Universidade Federal de Uberlândia
Faculdade de Matemática
Programa de Mestrado Profissional em Matemática em Rede Nacional

CONSTRUÇÃO DOS QUADRADOS MÁGICOS E APLICAÇÃO NA CRIPTOGRAFIA COMO FERRAMENTAS EDUCACIONAIS.

Eustáquio Morais de Oliveira

Uberlândia-MG
2023

Eustáquio Morais de Oliveira

CONSTRUÇÃO DOS QUADRADOS MÁGICOS E APLICAÇÃO NA CRIPTOGRAFIA COMO FERRAMENTAS EDUCACIONAIS.

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para a obtenção de título de **MESTRE EM MATEMÁTICA**.

Área de concentração: Matemática
Linha de pesquisa: Álgebra Linear

Orientador(a): Dr. Ariosvaldo Marques Jatobá.

Uberlândia-MG
2023

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU, MG, Brasil.

O48c
2023

Oliveira, Eustáquio Morais de, 1978-
Construção dos quadrados mágicos e aplicação na criptografia como ferramentas educacionais [recurso eletrônico] / Eustáquio Morais de Oliveira. - 2023.

Orientador: Ariosvaldo Marques Jatobá.
Dissertação (mestrado profissional) - Universidade Federal de Uberlândia, Programa de Pós-Graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2023.7105
Inclui bibliografia.

1. Matemática. I. Jatobá, Ariosvaldo Marques, 1975-, (Orient.). II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Matemática. III. Título.

CDU: 51

Glória Aparecida
Bibliotecária Documentalista - CRB-6/2047

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática em Rede Nacional
Av. João Naves de Ávila, 2121, Bloco 1F - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3230-9452 - www.famat.ufu.br - profmat@famat.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Mestrado Profissional em Matemática em Rede Nacional - PROFMAT UFU				
Defesa de:	Dissertação de Mestrado Profissional, 04, PROFMAT				
Data:	Oito de setembro de dois mil e vinte e Três	Hora de início:	10hs	Hora de encerramento:	12hs
Matrícula do Discente:	12112PFT004				
Nome do Discente:	Eustáquio Morais de Oliveira				
Título do Trabalho:	Construção dos quadrados mágicos e aplicação na criptografia como ferramentas educacionais.				
Área de concentração:	Matemática				
Linha de pesquisa:	Álgebra				
Projeto de Pesquisa de vinculação:	Não há				

Reuniu-se em webconferência pela plataforma *Google Meet* a Banca Examinadora, aprovada pelo Colegiado do Programa de Pós-graduação em Matemática - Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), assim composta pelos professores doutores: Leonardo de Amorim e Silva - UFTM; Lígia Laís Fêmina - FAMAT/UFU e Ariosvaldo Marques Jatobá - FAMAT/UFU, orientador do candidato.

Iniciando os trabalhos, o presidente da mesa, Prof. Dr. Ariosvaldo Marques Jatobá, apresentou a Comissão Examinadora e juntamente com o candidato agradeceram a presença de todos. Posteriormente, o presidente concedeu ao Discente a palavra para a exposição do seu trabalho. A duração da apresentação do Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

Dando continuidade, o senhor presidente concedeu a palavra para os examinadores que passaram a arguir o candidato. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final considerando o candidato:

Aprovado

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Leonardo de Amorim e Silva**, **Usuário Externo**, em 08/09/2023, às 11:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Ligia Lais Femina**, **Professor(a) do Magistério Superior**, em 08/09/2023, às 11:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Ariosvaldo Marques Jatoba**, **Professor(a) do Magistério Superior**, em 08/09/2023, às 11:42, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4759454** e o código CRC **3DE0BF66**.

Referência: Processo nº 23117.060800/2023-72 SEI nº 4759454

"Você me deve entender! De Um você faz Dez, jogue fora Dois, combine Três, e você ficará rico. Que você crie Quatro! Cinco e Seis, diz a bruxa, faça Sete e Oito. Está tudo feito. Se Nove é isso. Um, dez é nenhum. Esta é a tabuada da bruxa!"(Johann Wolfgang von Goethe)

Agradecimentos

Em primeiro lugar agradeço a Deus, que me concedeu o dom da vida bem como a oportunidade de concluir esse curso, mesmo diante de tantas adversidades que foram todas vencidas. "Ao Rei eterno, ao Deus único, imortal e invisível, sejam honra e glória para todo o sempre. Amém."(ITimóteo 1:17) À minha querida esposa Michelle e as minhas filhas Mirella e Micaelly, pessoas especiais em minha vida, que me apoiaram a todo instante e compreenderam o motivo da minha ausência durante a longa jornada. Aos meus pais, que sempre me incentivaram a estudar como forma de crescer e vencer na vida. Aos meus alunos que participaram desta pesquisa. Ao meu orientador Ariosvaldo Marques Jatobá ao confiar em mim para realizar este trabalho. Agradeço não só por cada detalhe que me orientou neste trabalho, mas também pela paciência que teve. Aos meus colegas de Mestrado, pelos momentos agradáveis e pela força nas situações difíceis, principalmente durante a preparação para o ENQ onde durante os grupos de estudos pudemos cultivar nossas amizades. Não posso deixar de agradecer ao colega Adelmo que tanto ajudou durante esta jornada. Muito obrigado!

OLIVEIRA, E. M. *.Construção dos quadrados mágicos e aplicação na criptografia como ferramentas educacionais.*. **2023. 115p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.**

Resumo

Neste projeto investiga-se a utilização dos quadrados mágicos e robótica educacional no ensino e aprendizagem da matemática como um motivador para alunos. A aplicação da robótica, mais especificamente, a criação e montagem de experiências práticas em laboratório, que permita o desenvolvimento de maneira lúdica, podem promover a interação entre conceitos e aplicações. A educação é um campo prolífero para o uso da tecnologia, tendo em vista o conjunto de possibilidades que apresenta, tornando a aprendizagem mais dinâmica e motivadora. A partir dessa constatação, os quadrados mágicos e a robótica educacional é uma proposta de aprendizagem no qual os alunos aplicam o método científico e desenvolvem habilidades, competências, a capacidade crítica, o senso de saber para contornar as dificuldades na resolução. Assim, o vigente trabalho tem como objetivo investigar o uso dos quadrados mágicos aliado a Robótica Educacional como recurso pedagógico. Destacaremos, ainda, a importância do uso da tecnologia na educação, fundamentando o trabalho nas visões de alguns autores consagrados da atualidade, definiremos historicamente o quadrado mágico e descreveremos o kit educacional 9797 da mindstorms utilizado para esse projeto. No que concerne à aquisição do conhecimento, a principal evidência da pesquisa foi a de que o trabalho pedagógico, orientado pelos pressupostos básicos descritos no referencial teórico, favoreceu efetivamente, a aprendizagem dos alunos.

Palavras-chave: História, quadrado mágico, criptografia, robótica.

OLIVEIRA, E. M. .***Construction of magic squares and application in cryptography as educational tools.*. 2023. 115p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.**

Abstract

This project investigates the use of magic squares and educational robotics in teaching and learning mathematics as a motivator for students. The application of robotics, more specifically, the creation and assembly of practical experiences in the laboratory, which allows development in a playful way, can promote interaction between concepts and applications. Education is a prolific field for the use of technology, in view of the set of possibilities it presents, making learning more dynamic and motivating. Based on this observation, magic squares and educational robotics is a learning proposal in which students apply the scientific method and develop skills, competences, critical capacity, a sense of knowledge to overcome difficulties in solving. Thus, the current work aims to investigate the use of magic squares combined with Educational Robotics as a pedagogical resource. We will also highlight the importance of the use of technology in education, basing the work on the visions of some renowned authors of the present time, we will historically define the magic square and describe the mindstorms educational kit 9797 used for this project. With regard to the acquisition of knowledge, the main evidence of the research was that the pedagogical work, guided by the basic assumptions described in the theoretical framework, effectively favored the students' learning.

Keywords: History, magic square, cryptography, robotics .

Sumário

INTRODUÇÃO

A ideia principal deste projeto é propor a utilização dos QUADRADOS MÁGICOS e do kit de robótica NXT dentro de um plano de aula para auxiliar o professor a ensinar os alunos de maneira lúdica desenvolvendo nos mesmos a curiosidade e a oportunidade de ver além de conteúdo teórico, o funcionamento prático através de programações que permitem ao robô executar tarefas de acordo com o assunto abordado, ou seja, possibilitar vivência da situação de aplicação do conteúdo teórico em meios tecnológicos educativos. Este trabalho intenta aumentar o aproveitamento dos alunos, acelerando a curva de aprendizado e disponibilizando maior envolvimento do aluno com o professor e o assunto, podendo assim o aluno vivenciar a situação, almejando-se alcançar maior eficiência do que lhe foi ensinado ao passar de alguns dias, ou seja, aumentando assim também a sua retenção de conhecimento. A utilização de ferramentas não convencionais no ensino da matemática torna-se interessante quando aplicados conceitos teóricos na realização de experimentos práticos, estimulando assim o interesse ao aprendizado no aluno. Neste contexto, foi realizado um estudo de possíveis projetos utilizando quadrados mágicos juntamente com o kit lego NXT.

Adotaremos uma perspectiva predominantemente histórica para salientar as dificuldades inerentes ao entendimento desta estrutura e ressaltar as ideias que estão por trás destas definições. Para uma melhor compreensão do trabalho dividimos em cinco partes. Primeiro será feito um passeio pela história dos quadrados mágicos, desde seu surgimento lendário até sua aparição em obras de arte ao longo dos séculos. Em seguida classificaremos e apresentaremos algumas propriedades dos quadrados mágicos. Terceira parte do nosso projeto apresentaremos alguns métodos clássicos e outros bem elaborados por vários personagens históricos na construção dos quadrados mágicos. A quarta parte discutiremos a aplicação dos quadrados mágicos na criptografia, utilizaremos as cifra pigpen, RSA e Vigenère, mesclando aos quadrados mágicos tornando-as mais robusta, aumentando a segurança. A proposta ou ação educativa desse projeto é contribuir com ensino-aprendizagem da matemática, propondo uma experiência (situação-problema), na qual utilizaremos duas ferramentas: o kit lego mindstorms (robótica educacional) e o auxílio dos quadrados mágicos para solução e validação da situação didática concebida. Para melhor compreensão do projeto será criada uma ponte de significados e concepções entre a robótica educacional (fazer) é os quadrados mágicos (pensar ou raciocinar). Assim, no primeiro momento, é desenvolvido predominantemente o raciocínio tecnológico do discente, e no segundo momento, desenvolve-se predominantemente o raciocínio lógico. O nosso projeto se respalda na necessidade humana de assimilar e interferir nos fenômenos que a cercam, a Modelagem Matemática está proposta como um sistema de ensino-aprendizagem que tem por finalidade não somente fazer com que os alunos compreendam melhor o conteúdo matemático, porém aquilo que lhe é transmitido, mas, principalmente, coloca-se como um procedimento de ensino em que o aluno deixa de ser um sujeito passivo para ser ativo no processo de aprendizagem.

CAPÍTULO 1

QUADRADOS MÁGICOS NA HISTÓRIA

Na formulação da situação-problema para o desenvolvimento do presente projeto, buscamos contemplar a origem histórica do objeto de estudo, quadrados mágicos, objetivando de forma agradável, lúdica e simples a sanar as dificuldades de aprendizagem dos alunos.

Segundo Meirieu (1998, p.192)[20]:

“uma situação-problema é uma situação didática contextualizada a partir da história do conteúdo.”

De acordo com Miguel e Miorin (2004, p.45)[21] a história deve ser o caminho que conduz as respostas dadas aos porquês da matemática. Da mesma forma pensam que a história pode alavancar o ensino aprendizagem da matemática, por meio da compreensão e da significação. Assim, possibilita ao discente compreender também que o conhecimento matemático é construído historicamente.

Conforme D’ Ambrósio (1999, p.97)[28]:

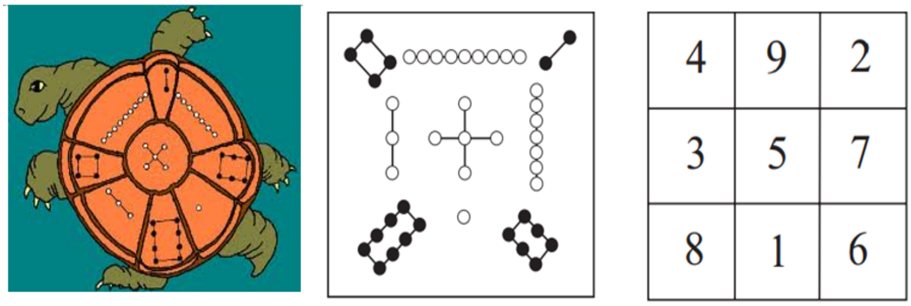
"*As ideias matemáticas comparecem em toda a evolução da humanidade, definindo estratégias de ação para lidar com o ambiente, criando e desenhando instrumentos para esse fim, e buscando explicações sobre os fatos e fenômenos da natureza e para a própria existência. Em todos os momentos da história e em todas as civilizações, as ideias matemáticas estão presentes em todas as formas de fazer e de saber.”*

Para melhor compreensão da proposta do trabalho faremos um breve resumo sobre a história do quadrado mágico, pois sabemos que a história da matemática tem capacidade para fazer a junção fundamental entre os conteúdos da matemática e desta com as outras disciplinas, uma vez que ela acompanha a história.

1.0.1 A Origem dos Quadrados Mágicos

Os quadrados mágicos têm uma rica história que data de cerca de 2200 a.C. Um mito chinês afirma que, enquanto o Imperador chinês Yü caminhava ao longo das margens do Rio Amarelo (Huang-Ho), ele notou uma tartaruga com um diagrama único em seu casco. O Imperador decidiu chamar o padrão numérico incomum de Lo Shu.

Figura 1.1: Quadrado de Lo Shu



Fonte:https://serluminoso.blogspot.com/

O quadrado mágico mais antigo registrado, no entanto, apareceu no livro do primeiro século "*Da-Dai Liji*".[24] Os quadrados mágicos na China têm sido usados em várias áreas do conhecimento, incluindo astrologia, adivinhação, interpretação da filosofia, fenômenos naturais e comportamento humano. Os Quadrados mágicos também permearam outras áreas da cultura chinesa. Por exemplo, pratos de porcelana chinesa expostos em museus e coleções particulares foram decorados com inscrições árabes e quadrados mágicos. Os quadrados mágicos muito provavelmente viajaram da China para Índia e depois para os países árabes. Dos países árabes, os quadrados mágicos chegaram a Europa, depois para o Japão. Os quadrados mágicos na Índia serviram a múltiplos propósitos além da disseminação do conhecimento matemático. Por exemplo, Varahamihira (astrônomo, matemático e astrólogo indiano que viveu em Ujjain.) utilizou um quadrado mágico de quarta ordem para especificar as receitas para fazer perfumes no seu livro. O quadrado mágico de 3ª ordem mais antigo da Índia aparece no trabalho do médico Vrnda Siddhayoga (900 d.C), como um meio para facilitar o parto.
Pouco se sabe sobre o início da pesquisa sobre quadrados mágicos na matemática islâmica. Tratados nos séculos IX e X revelaram que as propriedades matemáticas dos quadrados mágicos já estavam desenvolvidas entre as nações árabes. Além disso, a história sugere que a introdução dos quadrados mágicos foi completamente baseada em princípios matemáticos e não em mitos e superstições. A antiga designação árabe para os quadrados mágicos, "*wafq ala'dad*", significa "disposição harmoniosa dos números". Mais tarde, durante os séculos XI e XII, os matemáticos islâmicos deram um grande salto ao propor uma série de regras simples para criar quadrados mágicos. O século XIII testemunhou

o ressurgimento dos quadrados mágicos, que se tornaram associados à magia e à adivinhação. Esta ideia é ilustrada na seguinte citação de Cammann,(Prussin 1986, p.75)[7] que fala da importância espiritual dos quadrados mágicos: *"Se os quadrados mágicos eram, em geral, pequenos modelos do Universo, agora podiam ser vistos como representações simbólicas da vida em um processo de fluxo constante, renovando-se constantemente pelo contato com uma fonte divina no centro do cosmos."*

Um interesse considerável em quadrados mágicos também era evidente na África Ocidental. Quadrados mágicos foram entrelaçados em toda a cultura da África Ocidental. Os quadrados mágicos tinham uma importância espiritual particular e estavam inscritos em roupas, máscaras e artefatos religiosos. Eles influenciaram até mesmo os projetos arquitetônicos. No início do século XVIII, Muhammad, um conhecido astrônomo, matemático, místico e astrólogo da África Ocidental, interessou-se pelos quadrados mágicos de 3ª ordem. Em um de seus textos, ele deu exemplos de como construir quadrados de ordem ímpar. Durante o século XV, o escritor bizantino Manuel Moschopoulos introduziu os quadrados mágicos na Europa, onde, como em outras culturas, os quadrados mágicos estavam ligados à adivinhação, à alquimia e à astrologia. A primeira evidência de um quadrado mágico impresso na Europa foi revelada em uma famosa gravura do artista alemão Albrecht Durer. Em 1514, Durer incorporou um quadrado mágico em sua gravura em uma placa de cobre chamado de Melancolia[10]. Chen Dawei da China deu início ao estudo dos quadrados mágicos no Japão com a importação de seu livro "*Suan Fa Tong Zog*", publicado em 1592. Como os quadrados mágicos eram um tema popular, eles foram estudados pela maioria dos famosos "*wasan*", que eram especialistas japoneses em matemática.
Na história do Japão, o registro mais antigo de quadrados mágicos ficou evidente no livro "*Kuchi-Zusam*", que descreve um quadrado 3 por 3. Em 1687-88, um aristocrata francês, Antoine de La Loubere, estudou a teoria matemática da construção de quadrados mágicos. Em 1686, Adamas Kochansky entendeu os critérios para resolverem quadrados de 3ª ordem[10]. Durante a última parte do século XIX, os matemáticos aplicaram os quadrados a problemas de probabilidade e análise. Hoje, os quadrados mágicos são estudados em análise, combinatória, matrizes, aritmética e geometria. A magia, porém, ainda permanece nos quadrados mágicos.

1.0.2 China o Berço do Quadrado Mágico

A primeira referência do quadrado mágico de 3ª ordem é observado num antigo texto do *Yi Jing*[**iching**] um tratado de ritos e ensinamentos ancestrais, outra menção explícita do quadrado mágico aparece no capítulo chamado *MingTang* (Salão Brilhante) do livro "*Da Dai Liji*" (Livro de Ritos do

Ancião Dai), para descrever os rituais da Dinastia Zhou na China antiga.[24] Uma terceira referência é constatada em um texto matemático do livro "*Shushu jiyi*" (Memórias e tratados da arte matemática), que se diz ter sido escrito em 190 a.C. Provavelmente é a primeira ocorrência registrada do quadrado mágico em uma obra matemática. O quadrado mágico 3×3 foi chamado de "Nove Salas ou Nove Salões"pelos primeiros matemáticos chineses. No século XII a representação tabular ou gráfica do quadrado mágico 3×3 como conhecemos e o lendário quadrado de Lo Shu fica claramente associados e a partir de então passa a ser chamado de quadrado de Lo Shu.

4	9	2
3	5	7
8	1	6

Tabela 1.1: Quadrado Mágico

O matemático e escritor chines Yang Hui no ano de 1275 d.C, durante a dinastia Song, publicou dois livros. Em uma de suas obras, "*Xugu zheqi suanfa*"(Livro das Permutações), Hui exibe a construção de quadrados mágicos de terceira e quarta ordem. O livro de "*Yang Hui*" é considerado o registro matemático mais antigo ao se tratar de quadrados mágicos, sua obra foi baseada em trabalhos anteriores tanto nacionais quanto exteriores. Posteriormente a "*Yang Hui*", quadrados mágicos sistematicamente ocorreram na matemática chinesas de acordo com as publicações cronológicas das obras: *Ding Yidong Dayan suoyin (1300), Cheng Dawei's Suanfa tongzong (1593), de Fang Zhongtong Shuduyan (1661)*, podemos observar os círculos mágicos, cubos e esferas, *Xinzhai zazu de Zhang Chao (1650)*, que divulgou o primeiro quadrado mágico de ordem dez da China e, finalmente, *Binaishanfang ji de Bao Qishou(1880)*, apresentou várias configurações tridimensionais do quadrado mágico. Por outro lado, além de ser o primeiro a conhecer os quadrados mágicos e adquirir uma dianteira por vários séculos, o desenvolvimento chinês dos quadrados mágicos é muito inferior em comparação com desenvolvimentos da Índia, do Oriente Médio ou da Europa.

O clímax da matemática chinesa sobre os quadrados mágicos parece estar contido na obra de Yang Hui; mesmo como uma coleção de métodos mais antigos, esta obra é primitiva, carecendo de métodos gerais para a construção de quadrados mágicos de qualquer ordem, em comparação com uma coleção semelhante escrita na mesma época pelo estudioso bizantino *Manuel Moschopoulos*. Isso é possivelmente devido a admiração dos estudiosos chineses com o princípio Lo Shu, por vários anos, matemáticos chineses tentaram adaptar o método de 3ª ordem para solucionar os quadrados mágicos de ordem superior.

1.0.3 Quadrado Mágico e o conto de Lo Shu

Segundo uma das versões da estória do “Lo Shu” menciona que, por volta do ano 650 a.C., sucessivas inundações ocorreram no rio Lo, um afluente do rio Amarelo, na China, destruindo plantações, campos e deixando as pessoas desesperadas. A fim de aplacar a ira do deus do rio, as pessoas colocavam várias oferendas na margem do rio. A cada sacrifício, uma tartaruga aparecia no rio, contornava a oferenda e desaparecia no rio, mas as enchentes continuavam para o desespero da população ribeirinha. Por fim, alguém notou um padrão no casco da tartaruga que emergia da água, em cujo casco inferior viam-se desenhados 9 números em 3 colunas de 3 números cada, formando um quadrado. Pode ser visto na figura 1.1.

Somando esses números, por linha, por coluna ou na diagonal, obtinha-se sempre o mesmo número: 15.

		2	**7**	**6**	$\Rightarrow$	15
		9	**5**	**1**	$\Rightarrow$	15
		4	**3**	**8**	$\Rightarrow$	15
	$\swarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\searrow$	
15		15	15	15		15

Tabela 1.2: Constante Mágica.

Então, soube-se que 15 era o número de oferendas que precisavam ser feitas e assim procedeu-se. A tartaruga reapareceu e contornou aquela oferta, para surpresa das pessoas. O deus do rio ficou satisfeito com a quantidade exata de oferendas, aplacando assim a sua ira, e então o deus garantiu que o rio não inundaria os campos novamente. O número 15 é considerado um número poderoso porque corresponde ao número de dias em cada um dos 24 ciclos do ano solar chinês. Em outras palavras, é o número de dias no ciclo da lua nova até a lua cheia. O "Lo Shu square"ou “Quadrado de Lo Shu”, também chamado de Quadrado Mágico, é a base da antiga astrologia do *Feng Shui*, da escola *Xuan Kong Fei Xing*, bem como do *I-Ching*. Como pode ser visto na imagem (Tabela 1.2), em "Lo Shu Square"o número 5 está no centro, com números pares e ímpares alternando em sua periferia.

A maioria dos historiadores acredita que a lenda de Lo Shu se originou na China por volta de 2800 a.C, e depois se espalhou para a Índia e Egito e posteriormente para a Europa, e tem sido associada ao misticismo e superstição até hoje. Os padrões exibidos nos cascos das tartarugas são chamados de quadrados mágicos ou quadrados de Lo Shu. Este é considerado o quadrado mágico mais antigo, usado no Oriente e na Europa para práticas mágicas e como talismã para atrair boa sorte e afastar doenças. Acredita-se que este símbolo reúne os princípios fundamentais que compõem o universo, com números pares simbolizando o princípio feminino, *yin*, e números ímpares, o princípio masculino, *yang*. Num quadrado mágico 3x3, considerava-se que os números de 1 a 9 representavam todo o conhecimento, sendo que cada número representava um caminho no estágio espiritual com um significado próprio. O número 5 representava a Terra e ao seu redor estavam distribuídos os quatro elementos principais, a água 1 e 6, o fogo 2 e 7, a madeira 3 e 8 e os metais 4 e 9. Acreditava-se que quem possuísse um quadrado mágico teria sorte e felicidade para toda a vida. A ideia do presente projeto e mergulhar nesse mundo fantástico dos quadrados mágicos e discutir a luz da matemática e seus segredos.

CAPÍTULO 2

O QUE É UM QUADRADO MÁGICO?

2.1 Quadrados Mágicos: Definições

Nesta subsecção veremos algumas definições atribuídas por vários estudiosos e pesquisadores na área.

A maioria dos autores define-se quadrado mágico, como sendo uma matriz quadrada de números, geralmente naturais, é chamada de quadrado mágico se as somas dos números em cada linha, cada coluna e ambas as diagonais forem iguais. A ordem de um quadrado mágico é o número de inteiros ao longo de um lado (n), e a soma é chamada de <u>constante mágica</u>. Se a matriz contém apenas os inteiros positivos 1, 2, 3, ...,n^2, o quadrado mágico é considerado normal.

Kraitchik (1942)[19] e Gardner (1961)[18] definem que um quadrado mágico de ordem n é uma matriz quadrada de ordem n com n^2 inteiros, de modo que a soma dos números de qualquer linha, qualquer coluna e as diagonais têm o mesmo valor.

Os Quadrados Mágicos são matrizes que obedecem a uma determinada ordem, onde a sequência numérica informada precisa ser distribuída de forma a construir uma soma pré-estabelecida nas três possíveis posições: horizontal, vertical e diagonal.

Para Machado (2013)[27] - uma matriz $n \times n$ chama-se um quadrado mágico de ordem n quando a soma dos elementos de cada uma de suas linhas, de cada coluna, da diagonal principal e da diagonal secundária (ao todo $2n + 2$ somas) são iguais. Essa soma será chamada de constante mágica ou soma mágica.

De acordo com William Symes Andrews (1960)[3], um quadrado mágico se resume em uma sucessão de números agrupados em um quadrado, de maneira que cada linha, coluna e ambas as diagonais devem ter o mesmo resultado, ou seja, a mesma soma. Essa soma é chamada constante mágica $\sigma(M)$.

Para Lehmer (1929)[16], um quadrado é denominado "mágico" nas filas se a soma dos números em cada linha, coluna e diagonais for a mesma soma.

Um quadrado mágico de ordem n pode ser definido como sendo uma matriz $(a_{ij})_{nxn}$ onde os elementos a_{ij} pertencem ao subconjunto de $\mathbb{N} = \{1, 2, 3, ..., n\}$, são dois a dois distintos e a soma dos números de qualquer linha, qualquer coluna e de qualquer uma das duas diagonais é igual a uma constante $\sigma(M)$.[2]

2.2 Classificação dos Quadrados Mágicos

Os quadrados mágicos podem ser classificados de várias maneiras, dependendo das propriedades específicas que podem ter. Uma das classificações mais comuns é dividida em três classes: **Simples, Associado e Pandiagonal.**

No entanto, se remover ou adicionar certas propriedades a eles, também podemos considerar os seguintes: **Semimágico, Semipandiagonal e Natural.**

Quando apresentam determinadas características, assumem outros significados como: **Bimágico,Concêntrico, Alfamágico, Latino, Serrilhado.**

As oito classificações mencionadas abaixo são definidas por Quadrados Mágicos de Ordem n, colocaremos na ordem de maior dificuldade de suas estruturas.

- **Quadrado semimágico** - Um quadrado semimágico, também conhecido como quadrado mágico parcial, é uma matriz quadrada de números (normalmente números inteiros positivos) em que a soma dos números em cada linha e em cada coluna é a mesma, mas a soma dos números ao longo de algumas diagonais não atinge esse mesmo valor.

Em contraste, um quadrado mágico regular (ou simplesmente quadrado mágico) é uma matriz onde a soma dos números em cada linha, coluna e diagonal principal é a mesma.

Portanto, em um quadrado semimágico, a propriedade principal de igualdade de soma para todas as linhas e colunas é mantida, mas essa igualdade não se estende a todas as diagonais da matriz.

Isso o diferencia dos quadrados mágicos tradicionais, onde todas as diagonais também têm a mesma soma.

11	6	1	21	16	**55**
17	12	7	2	22	**60**
23	18	13	8	3	**65**
4	24	19	14	9	**70**
10	5	25	20	15	**75**
65	**65**	**65**	**65**	**65**	**65**

Tabela 2.1: Quadrado semimágico.

• **Quadrado Mágico, Numérico, Normal, Puro, Natural e Simples de Ordem n ou simplesmente Quadrado Mágico** - Matriz de $n \times n$ Células (n linhas x n colunas) preenchidas, cada uma, por um determinado número que conduza a que as somas de cada linha, de cada coluna e das duas diagonais tenham todas o mesmo valor $\sigma(M)$, designado por constante mágica ou soma mágica. A satisfação das propriedades acima mencionadas, constitui o mínimo dos requisitos para obter a qualificação de quadrado mágico.[30]

				34
1	**14**	**15**	**4**	**34**
12	**7**	**6**	**9**	**34**
8	**11**	**10**	**5**	**34**
13	**2**	**3**	**16**	**34**
34	**34**	**34**	**34**	**34**

Tabela 2.2: Quadrado mágico Normal ou Puro.

• **Quadrado mágico concêntrico** – Quadrado mágico concêntrico é um quadrado mágico composto de outros quadrados mágicos ou semimágicos dentro dele, de modo que a soma de cada quadrado seja um número quadrado perfeito.[30]

Constante mágica 80

Soma do quadrado 400.

					80
14	**7**	**20**	**13**	**26**	**80**
27	**15**	**8**	**21**	**9**	**80**
10	**28**	**16**	**4**	**22**	**80**
23	**11**	**24**	**17**	**5**	**80**
6	**19**	**12**	**25**	**18**	**80**
80	**80**	**80**	**80**	**80**	**80**

Tabela 2.3: Quadrado Mágico Concêntrico.

• **Quadrado Mágico Semipandiagonal ou Semidiabólico ou SemiNasik** – Quadrado mágico com as seguintes propriedades:

Ordem Par: A soma de um par de diagonais curtas opostas com n células é igual à soma mágica, $\sigma(M)$.

Ordem Ímpar: A soma de um par de diagonais curtas opostas com $n - 1$ Células mais a célula central é igual à soma mágica, $\sigma(M)$;
A soma de um par de diagonais curtas opostas com $n + 1$ Células menos a célula central é igual à soma mágica, $\sigma(M)$.

Num quadrado mágico de Ordem n, a soma mágica $\sigma(M)$ é sempre calculada levando em consideração as n células, linhas, colunas e diagonais pandiagonais. Daí a necessidade de adicionar ou subtraír a célula do centro do quadrado às células que constituem o par de diagonais curtas opostas, quando estas são, respectivamente, $n - 1$ e $n + 1$.

1	**14**	**12**	**7**
4	**15**	**9**	**6**
13	**2**	**8**	**11**
16	**3**	**5**	**10**

1	**14**	**12**	**7**
4	**15**	**9**	**6**
13	**2**	**8**	**11**
16	**3**	**5**	**10**

Tabela 2.4: Quadrado Mágico Semi-Nasik.

Veja as tabelas 2.4:

Tabela 1	**Tabela 2**
	1 + 15 + 4 + 14 = 34
14 + 4 + 11 + 5 = 34	**13 + 3 + 16 + 2 = 34**
12 + 6 + 13 + 3 = 34.	**12 + 6 + 9 + 7 = 34**
	8 + 10 + 5 + 11 = 34.

• **Quadrado mágico pandiagonal ou diabólico ou Nasik ou contínuo** – Quadrado mágico em que a soma de cada par de diagonais quebradas é igual à soma mágica, $\sigma(M)$. O quadrado mágico pandiagonal é considerado um dos mais sofisticados entre as classes de Quadrados Mágicos. Não existem Quadrados mágicos pandiagonais quando n é par.[30]

					65
20	**8**	**21**	**14**	**2**	**65**
11	**4**	**17**	**10**	**23**	**65**
7	**25**	**13**	**1**	**19**	**65**
3	**16**	**9**	**22**	**15**	**65**
24	**12**	**5**	**18**	**6**	**65**
65	**65**	**65**	**65**	**65**	**65**

Tabela 2.5: Quadrado mágico pandiagonal ou diabólico ou Nasik ou contínuo.

Observando o quadrado mágico acima (Tabela 2.5) as linhas, colunas e diagonais, nota os quatro modos do quadrado, essas formas são chamados de "*quincunx*", no exemplo acima, temos:

• $\sigma(M)$**:** $17 + 25 + 13 + 1 + 9 = 65$ (centro mais linha adjacente e quadrados da coluna);

• $\sigma(M)$**:** $21 + 7 + 13 + 19 + 5 = 65$ (centro mais linhas restantes e quadrados da coluna;)

• $\sigma(M)$**:** $4 + 10 + 13 + 16 + 22 = 65$ (centro mais quadrados diagonalmente adjacentes);

• $\sigma(M)$**:**$20 + 2 + 13 + 24 + 6 = 65$ (centro mais quadrados restantes na diagonal).

Cada um desses quincúncios pode ser transformado em outro ponto do quadrado por um arranjo circular (envelope) de linhas e colunas, que em um quadrado mágico pandiagonal não afeta a igualdade dos números mágicos. Isso resulta em uma soma de 100 quincunces, incluindo quincunces quebrados que se assemelham a diagonais quebradas.

• **Um Quadrado Bimágico** – Um quadrado bimágico é um quadrado mágico que permanece mágico quando todos os seus números são substituídos por seus quadrados.[11]

16	**41**	**36**	**5**	**27**	**62**	**55**	**18**
26	**63**	**54**	**19**	**13**	**44**	**33**	**8**
1	**40**	**45**	**12**	**22**	**51**	**58**	**31**
23	**50**	**59**	**30**	**4**	**37**	**48**	**9**
38	**3**	**10**	**47**	**49**	**24**	**29**	**60**
52	**21**	**32**	**57**	**39**	**2**	**11**	**46**
43	**14**	**7**	**34**	**64**	**25**	**20**	**53**
61	**28**	**17**	**56**	**42**	**15**	**6**	**35**

Tabela 2.6: Um Quadrado Bimágico 8×8.

O quadrado mágico acima é bimágico, pois substituindo os quadros dos números acima ele contínua um quadrado mágico de ordem 8×8 com constante mágica $\sigma(M) = 11180$ e antes era $\sigma(M) = 260$.

256	**1681**	**1296**	**25**	**729**	**3844**	**3025**	**324**
676	**3969**	**2916**	**361**	**169**	**1936**	**1089**	**64**
1	**1600**	**2025**	**144**	**484**	**2601**	**3364**	**961**
529	**2500**	**3481**	**900**	**16**	**1369**	**2304**	**81**
1444	**9**	**100**	**2209**	**2401**	**576**	**841**	**3600**
2704	**441**	**1024**	**3249**	**1521**	**4**	**121**	**2116**
1849	**196**	**49**	**1156**	**4096**	**625**	**400**	**2809**
3721	**784**	**289**	**3136**	**1764**	**225**	**36**	**1225**

Tabela 2.7: Quadrado de quadrado

- **Quadrado Latino** - Quadrado latino (de ordem n) é uma matriz n por n de n símbolos distintos de modo que cada símbolo apareça uma vez em cada linha e coluna.[15] O nome quadrado latino vem de Leonhard Euler, que usava caracteres latinos como símbolos.

1	2	3
3	1	2
2	3	1

4	3	1	2
3	4	2	1
1	2	4	3
2	1	3	4

1	2	4	3	5
4	5	2	1	3
3	4	1	5	2
2	3	5	4	1
5	1	3	2	4

Tabela 2.8: Quadrado Latino de ordem 3, 4 e 5.

• **Um Quadrado Alfamágico** - Um quadrado alfamágico é um quadrado mágico que permanece mágico quando seus números são substituídos pelo número de letras que ocorrem no nome de cada número. Portanto, 3 seria substituído por 5, o número de letras em "três". Uma vez que idiomas diferentes terão um número diferente de letras para soletrar o mesmo número, os quadrados alfamágicos dependem do idioma.[26] Os quadrados alfamágicos foram inventados por Lee Sallows em 1986.[18]

O exemplo abaixo é alfamágico

Para descobrir se um quadrado mágico também é um quadrado alfamágico, converta-o na matriz de palavras numéricas correspondentes.

5	22	18
28	15	2
12	8	25

five	twenty-two	eighteen
twenty-eight	fifteen	two
twelve	eight	twenty-five

4	9	8
11	7	3
6	5	10

Tabela 2.9: Quadrado Alfamágico

• **Quadrados mágicos compostos** - Um quadrado mágico de ordem $m \times n$ é chamado de composto, quando pode ser decomposto em m^2 subquadrados mágicos, cada um de ordem n.

Deve-se notar que o quadrado mágico composto mínimo deve ser de ordem $n = 9$. Este é o número mínimo com dois divisores, para o qual existem quadrados mágicos compostos.

$$m \cdot n = 9, m = 3 \text{ e } n = 3.$$

Isso significa que o quadrado mágico fundamental pode ser decomposto em $m^2 = 3^2 = 9$ subquadrados mágicos, cada um deles de ordem $n = 3$. Claro que é impossível que todos os subquadrados sejam normalizados, ou seja, sejam compostos de inteiros consecutivos $1, 2, \ldots, n^2$.

71	66	67	20	25	24	29	34	33
64	68	72	27	23	19	36	32	28
69	70	65	22	21	26	31	30	35
8	3	4	40	39	44	74	79	78
1	5	9	45	41	37	81	77	73
6	7	2	38	43	42	76	75	80
47	54	49	56	63	58	11	16	15
52	50	48	61	59	57	18	14	10
51	46	53	60	55	62	13	12	17

Tabela 2.10: Quadrado Mágico Composto de ordem 9, com 9 subquadrados mágicos de ordem 3.

O próximo quadrado mágico composto é encontrado para a ordem $m \cdot n = 12$. Essa ordem pode ser dividida da seguinte maneira:

$$m \cdot n = 12, m = 3 \text{ e } n = 4.$$

Isso significa que o quadrado composto pode ser decomposto em $m^2 = 3^2 = 9$ subquadrados mágicos de ordem $n = 4$.

17	31	30	20	132	142	143	129	61	56	60	49
28	22	23	25	137	135	134	140	51	58	54	63
24	26	27	21	133	139	138	136	50	59	55	62
29	19	18	32	144	130	131	141	64	53	57	52
100	105	101	112	68	73	69	80	36	41	37	48
110	103	107	98	78	71	75	66	46	39	43	34
111	102	106	99	79	70	74	67	47	38	42	35
97	108	104	109	65	76	72	77	33	44	40	45
84	89	85	96	4	14	15	1	116	121	117	128
94	87	91	82	9	7	6	12	126	119	123	114
95	86	90	83	5	11	10	8	127	118	122	115
81	92	88	93	16	2	3	13	113	124	120	125

Tabela 2.11: Quadrado Mágico Composto de ordem 12, com 9 subquadrados mágicos de ordem 4.

Mas, também outra decomposição é possível.

$$m \cdot n = 12, m = 4 \text{ e } n = 3.$$

Este quadrado mágico composto é decomposto em $m^2 = 4^2 = 16$ subquadrados mágicos, cada um de ordem $n = 3$.

8	3	4	119	124	123	130	135	128	29	36	31
1	5	9	126	122	118	129	131	133	34	32	30
6	7	2	121	120	125	134	127	132	33	28	35
105	106	101	58	57	62	49	54	47	74	81	76
100	104	108	63	59	55	48	50	52	79	77	75
107	102	103	56	61	60	53	46	51	78	73	80
71	64	69	92	99	94	89	84	85	44	37	42
66	68	70	97	95	93	82	86	90	39	41	43
67	72	65	96	91	98	87	88	83	40	45	38
114	115	110	13	12	17	26	21	22	137	142	141
109	113	117	18	14	10	19	23	27	144	140	136
116	111	112	11	16	15	24	25	20	139	138	143

Tabela 2.12: Quadrado mágico composto de ordem 12, com 16 subquadrados mágicos de ordem 3.

2.3 Propriedades dos Quadrados Mágicos

2.3.1 Constante Mágica

De acordo com William Symes Andrews (1960)[3], um quadrado mágico se resume em uma sucessão de números agrupados em um quadrado, de maneira que cada linha, coluna e ambas as diagonais devem ter o mesmo resultado, ou seja, a mesma soma. **Essa soma é chamada constante mágica $\sigma(M)$.**

Verifica-se, num **Quadrado Mágico Normal** de ordem n, a soma de seus termos é dado por,

$$\sigma(M) = \frac{\left(n^2+1\right)n}{2}$$

Proposição 2.3.1. *Dado um quadrado Mágico Normal de ordem n, então $\sigma(M) = \frac{\left(n^2+1\right)n}{2}$.*

Demonstração. De fato, sejam 1, 2, 3,..., n^2 os n^2 primeiros números inteiros positivos. Sabemos que

$$\text{S(n)} = 1 + 2 + 3 + \ldots + (n^2-2) + (n^2-1) + n^2,$$

é a soma de uma progressão aritmética de razão $r = 1$ com n^2 termos, onde o primeiro termo é a_1 e o último termo é $a_n = n^2$, utilizando a fórmula da soma dos termos de uma progressão aritmética finita, temos:

$$S(n) = \frac{\left(n^2+1\right)n^2}{2},$$

Como a soma dos termos de um quadrado mágico de ordem n é

$$n.\sigma(M) = S(n)$$

pois são n linhas e cada linha tem soma dos termos igual a $\sigma(M)$, ou seja

$$\sigma(M) = \frac{\left(n^2+1\right)n}{2}.$$

□

Por exemplo, considere o quadrado 3×3 formado por números de 1 a 9, então

$$\sigma(M) = \frac{\left(3^2+1\right)3}{2} = 15.$$

No quadrado mágico

4	9	2
3	5	7
8	1	6

temos para as linhas, colunas e diagonais a soma dos elementos são iguais a 15, o qual se refere a **constante mágica.**

$$\frac{4+5+6=2+5+8}{Total\ das\ diagonais}=\frac{8+1+6=3+5+7=4+9+2}{Total\ da\ 1^a,\ 2^a\ e\ 3^a\ linha}=\frac{8+3+4=1\ \ 5+9=6+7+2}{Total\ da\ 1^a,\ 2^a\ e\ 3^a\ coluna}$$

Você pode notar também que 1 e 9, 2 e 8, 3 e 7, 4 e 6 somados dão 10 e complementado com 5 temos o total 15.

Veja a tabela abaixo para constante mágica e soma dos termos de acordo com a ordem do quadrado mágico.

Quadrados Mágicos e características Numéricas		
Quadrado Mágico	**Constante Mágica**	**Soma dos Termos**
3 x 3	**15**	**45**
4 x 4	**34**	**136**
5 x 5	**65**	**325**
6 x 6	**111**	**666**
7 x 7	**175**	**1225**
8 x 8	**260**	**2080**
9 x 9	**369**	**3321**
...	**...**	**...**
n x n	$\sigma(M)=\frac{(n^2+1)n}{2}$	$S(n)=\frac{(n^2+1)n^2}{2}$

Tabela 2.13: Constante Mágica e a Soma dos Termos

2.3.2 Forma Geral de um Quadrado Mágico de 3ª Ordem

Apresentamos uma maneira para construção de um quadrado mágico normal de ordem 3 com $\sigma(M)$ como sendo sua constante mágica. Nas representações dos elementos dos quadrados mágicos, utilizamos a forma abaixo

a	**b**	**c**
d	**e**	**f**
g	**h**	**i**

Tabela 2.14: Quadrado mágico 3×3 Geral

Proposição 2.3.2. *Dado um quadrado mágico qualquer de ordem* 3 *com constante mágica* $\sigma(M)$*, então o termo central é dado por*

$$e = \frac{\sigma(M)}{3}.$$

Demonstração. Sabemos que a soma de duas linhas são iguais a soma de duas diagonais, então

a + b + c + g + h + i = a + e + i + c + e + g

b + h = 2e

Também temos que a soma da segunda coluna e $\sigma(M)$, ou seja

$$\sigma(M) = b + e + h = (b + h) + e = 2e + e = 3e.$$

Assim,

$$e = \tfrac{\sigma(M)}{3}$$

□

Agora, podemos estabelecer a forma geral para o quadrado mágico de ordem 3 em função de três valores fixos. Fixaremos a, b e a constante mágica $\sigma(M)$.

Proposição 2.3.3. *Dado um quadrado mágico qualquer de ordem* 3*. Fixamos* a*,* b *e a constante mágica* $\sigma(M)$*. Então o quadrado mágico tem a forma geral dada por*

a	**b**	$\sigma(M)-a-b$
$\frac{4}{3}\sigma(M)-2a-b$	$\frac{\sigma(M)}{3}$	$2a+b-\frac{2}{3}\sigma(M)$
$a+b-\frac{\sigma(M)}{3}$	$\frac{2}{3}\sigma(M)-b$	$\frac{2}{3}\sigma(M)-a$

Do quadrado mágico geral, temos que, $\begin{cases} c=\sigma(M)-a-b \\ h=\sigma(M)-b-e \\ g=\sigma(M)-c-e \\ i=\sigma(M)-a-e \end{cases}$

utilizando que $e=\frac{\sigma(M)}{3}$ concluímos,

$$\begin{cases} c=\sigma(M)-a-b \\ h=\frac{2}{3}\sigma(M)-b \\ g=a+b-\frac{\sigma(M)}{3} \\ i=\frac{2}{3}\sigma(M)-a \end{cases}$$

Vejamos d e f em função de $a, b, \sigma(M)$.

Utilizando g acima temos que

$$\begin{cases} d=\sigma(M)-a-g=\sigma(M)-a-\left(a+b-\frac{\sigma(M)}{3}\right)=\frac{4}{3}\sigma(M)-2a-b \\ f=\sigma(M)-e-d=\sigma(M)-\frac{\sigma(M)}{3}-\left(\frac{4}{3}\sigma(M)-2a-b\right)=2a+b-\frac{2}{3}\sigma(M) \end{cases}$$

Utilizaremos o quadrado abaixo

a	**b**	$\sigma(M)-a-b$
$\frac{4}{3}\sigma(M)-2a-b$	$\frac{\sigma(M)}{3}$	$2a+b-\frac{2}{3}\sigma(M)$
$a+b-\frac{\sigma(M)}{3}$	$\frac{2}{3}\sigma(M)-b$	$\frac{2}{3}\sigma(M)-a$

para obter todos os quadrados mágicos normal de ordem 3.

Já temos que num quadrado mágico normal o

$$\sigma(M)=\frac{\left(3^2\ +\ 1\right)3}{2}=15.$$

assim quadrado geral fica

a	**b**	$15-a-b$
$20-2a-b$	5	$2a+b-10$
$a+b-5$	$10-b$	$10-a$

Podemos fazer algumas escolhas de a e b para obtermos alguns exemplos. Para caso que $a = 2, b = 7$ temos

$$\begin{array}{c|c|c|c|cc}
\cline{2-4}
 & \mathbf{2} & \mathbf{7} & \mathbf{6} & \Rightarrow & 15 \\
\cline{2-4}
 & \mathbf{9} & \mathbf{5} & \mathbf{1} & \Rightarrow & 15 \\
\cline{2-4}
 & \mathbf{4} & \mathbf{3} & \mathbf{8} & \Rightarrow & 15 \\
\cline{2-4}
\multicolumn{1}{c}{\swarrow} & \multicolumn{1}{c}{\Downarrow} & \multicolumn{1}{c}{\Downarrow} & \multicolumn{1}{c}{\Downarrow} & \searrow & \\
\multicolumn{1}{c}{15} & \multicolumn{1}{c}{15} & \multicolumn{1}{c}{15} & \multicolumn{1}{c}{15} & & 15
\end{array}$$

Caso que $a = 4, b = 3$ temos

4	**3**	**8**
9	**5**	**1**
2	**7**	**6**

Caso que $a = 8, b = 3$ temos

8	**3**	**4**
1	**5**	**9**
6	**7**	**2**

Vejamos que num quadrado mágico normal os valores de a e b são restritos. Vejamos o seguinte resultado

Proposição 2.3.4. *Em um quadrado mágico normal de ordem* 3 *da forma*

a	**b**	**c**
d	**e**	**f**
g	**h**	**i**

temos

$$e = 5, \quad \{a, c, g, i\} = \{2, 4, 6, 8\} \quad e \quad \{b, d, f, h\} = \{1, 3, 7, 9\}.$$

Demonstração. Já sabemos que $e = 5$ e $\sigma(M) = 15$. Então fica da seguinte forma geral

a	**b**	$15-a-b$
$20-2a-b$	5	$2a+b-10$
$a+b-5$	$10-b$	$10-a$

Vamos supor que a é um número ímpar. Assim

$a+5+10-a=15$, ou seja $10-a$ seria ímpar. Então já utilizamos 3 números ímpares e ainda temos que posicionar mais dois, pois os números utilizados são: $1,2,3,4,5,6,7,8,9$. Vamos supor que b seja ímpar.

Então $a+b$ seria par, logo teríamos $15-a-b$, $10-b$ números ímpares. Portanto 5, a, b , $10-a$, $15-a-b$, e $10-b$ seriam ímpares o que é um absurdo, pois só dispomos de 5 números ímpares.

Portanto, se a for ímpar, b terá que ser par. Vamos supor que a ímpar e b par. Então teríamos

b, $10-b$, $15-a-b$, $2a+b-10$, $a+b-5$ seriam par. Mas isto é um absurdo, pois só dispomos de 4 números pares. Então a não pode ser ímpar, isto é, a é par.

Vejamos que b não pode ser par. Suponhamos que b seja par, então

a, b, $10-a$, $10-b$, $20-2a-b$ seriam 5 números pares. O que é um absurdo. Portanto a é par e b é ímpar.

Neste caso temos: $\{a, a+b-5, 10-a, 15-a-b\}$ são pares e $\{b, 10-b, 20-2a-b, 2a+b-10\}$ são ímpares.

$\square$

2.3.3 Rotação e Reflexão do Quadrado Mágico Puro de 3ª Ordem

Os quadrados mágicos possíveis devem variar de acordo com o fatorial de $(n^2)!$. Qualquer um tentando montar a matriz mostrada na figura abaixo no caso do quadrado mágico de 3ª ordem, é surpreendente, pois provavelmente chegará a um número de matrizes na ordem do fatorial de nove, (9!) isto é, $9\times8\times7\times6\times5\times4\times3\times2\times1=362.800$ possibilidades de colocação dos dígitos na matriz. Todos os quadrados são imperfeitos, menos um, que é o quadrado em questão.

8	1	6
3	5	7
4	9	2

Em geral, qualquer quadrado mágico que satisfaça a Proposição 2.3.3 é chamado de quadrado mágico perfeito. Um quadrado que não atende a essa condição é chamado de quadrado imperfeito, ou mais precisamente, não é considerado um quadrado mágico.

Nas propriedades do quadrado mágico, você pode girar o quadrado mágico no sentido horário ou anti-horário para obter um novo quadrado mágico **rotação**. Rotações de $90°$, $180°$ ou $270°$ resultam em outros três quadrados mágicos de terceira ordem, enquanto rotações de $360°$ naturalmente resultam no quadrado inicial.

0°

8	1	6
3	5	7
4	9	2

90°

4	3	8
9	5	1
2	7	6

180°

2	9	4
7	5	3
6	1	8

270°

6	7	2
1	5	9
8	3	4

360°

8	1	6
3	5	7
4	9	2

Tabela 2.15: Quadrados Mágicos:rotação no sentido horário.

0°

8	1	6
3	5	7
4	9	2

90°

6	7	2
1	5	9
8	3	4

180°

2	9	4
7	5	3
6	1	8

270°

4	3	8
9	5	1
2	7	6

360°

8	1	6
3	5	7
4	9	2

Tabela 2.16: Quadrados Mágicos:rotação no sentido anti-horário.

Podemos também espelhar o quadrado seguindo a mediana horizontal ou vertical ou uma das diagonais para obter um novo quadrado mágico **reflexão**. Veja as imagens abaixo:

8	1	6
3	5	7
4	9	2

8	1	6
3	5	7
4	9	2

8	1	6
3	5	7
4	9	2

8	1	6
3	5	7
4	9	2

$\Downarrow$ $\Downarrow$ $\Downarrow$ $\Downarrow$

4	9	2
3	5	7
8	1	6

6	1	8
7	5	3
2	9	4

2	7	6
9	5	1
4	3	8

8	3	4
1	5	9
6	7	2

Tabela 2.17: Quadrados Mágicos: reflexão.

Os arranjos entre si não são considerados diferentes, mas sim variações do mesmo quadrado mágico de ordem 3. Sendo assim, qualquer quadrado mágico de ordem 3 é uma variação de um único quadrado.

Por outro lado, sabe-se que para quadrados mágicos de ordem 4 há 880 quadrados distintos, excluindo os obtidos através de rotações e reflexões. Os 880 quadrados foram enumerados por Frénicle de Bessy em 1693. O número de quadrados distintos de ordem 5 somam $275.305.224$, computados por R. Schroeppel em 1973. Já o número de quadrados de ordem 6 é desconhecido, mas Pinn e Wieczerkowski, em 1998, estimaram cerca de $(1.7745 \pm 0.0016) \cdot 10^{19}$, usando uma simulação e métodos estatísticos de Monte Carlo [34].

O estado atual do conhecimento é dado na tabela a seguir

$N(n)$: o número de quadrados mágicos de ordem n sem análise de simetrias.
$P(n)$: o número de quadrados mágicos de ordem n, onde os quadrados que diferem apenas por rotação ou reflexão são contados apenas uma vez.

Ordem	$N(n)$	$P(n)$
1	**1**	**1**
2	**0**	**0**
3	**8**	**1**
4	**7040**	**880**
5	2202441792	275305224
6	**?**	**?**

2.3.4 Momento de Inércia de um quadrado mágico

Define o momento de inércia, I_n, de um quadrado mágico de ordem n, como sendo a soma dos elementos nas células equidistantes multiplicado pelo quadrado da distância do centro das células ao centro do quadrado mágico; aqui a unidade de medida é a largura de uma célula. (Assim, por exemplo, uma célula de canto de um quadrado 3×3 tem uma distância de $\sqrt{2}$, uma célula de borda não-canto tem uma distância de 1, e a célula do centro tem uma distância zero).[17]

Veja a figura abaixo,

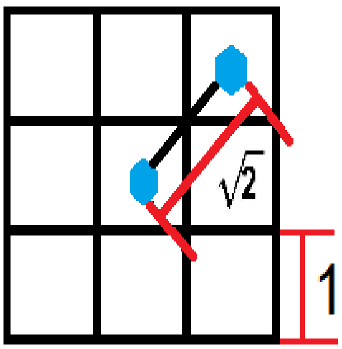


Figura 2.1: As dimensões do quadrado magico.

Então todos os quadrados mágicos de uma dada ordem têm o mesmo momento de inércia entre si.

Para o quadrado mágico de 3ª ordem, o momento de inércia é sempre 60.

Vamos observar os dois exemplos abaixo:

Exemplo 1:

4	**3**	**8**
9	**5**	**1**
2	**7**	**6**

vejamos,

$$\begin{aligned} I_3 &= [1+3+7+9]\cdot(1)^2+[2+4+6+8]\cdot(\sqrt{2})^2 \\ &= [20]\cdot(1)+[20]\cdot(2) \\ &= 60 \end{aligned}$$

Exemplo 2:

6	**1**	**8**
7	**5**	**3**
2	**9**	**4**

analogamente $I_3 = 60$.

Utilizando Proposição 2.3.4 temos que

$$\begin{aligned} I_3 &= [b+d+f+h]\cdot(1)^2+[a+c+g+h]\cdot(\sqrt{2})^2 \\ &= [20](1)+[20]\cdot(2) \\ &= 60 \end{aligned}$$

e também isso ocorre devido ao fato que só existe um quadrado mágico de ordem 3, os demais são simples rotação e reflexão.

Proposição 2.3.5. *Dado um quadrado mágico natural de ordem n, então o momento de inércia é dado por*

$$I_n = \frac{1}{12}n^2(n^4-1).$$

Demonstração. Os momentos de inércia em relação aos eixos horizontal e vertical, que passam pelo centro, são ambos 30. Isso nos lembra do teorema do eixo perpendicular, que afirma que a soma desses momentos de inércia é igual ao momento de inércia em torno do eixo que passa pelo centro e é perpendicular ao plano. Veja a **figura 2.2**, $I_x = 3+5+7 = 15$, $I_y = 1+5+9 = 15$, então, $I_x + I_y = 30$.

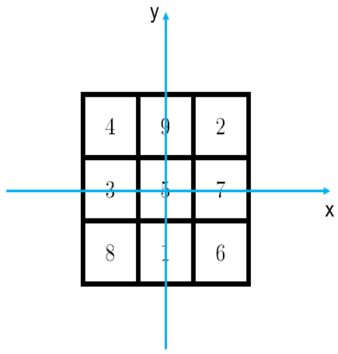


Figura 2.2: Quadrado mágico centrado no plano cartesiano.

O teorema do eixo perpendicular significa que só temos que calcular o momento de inércia em relação a um eixo horizontal I_x ou vertical I_y no plano do quadrado através de seu centro de massa (localizado no centro do quadrado), e então dobre para obter Iz. Como cada linha (ou coluna) tem a mesma massa (linha soma, $\sigma(M)$) o cálculo de I_x se reduz a somar as distâncias quadradas das linhas a partir do centro do quadrado. Além disso, se calcularmos I_x sobre o borda superior (ou inferior) do quadrado:

Temos o seguinte,

$$I_{borda} = \sigma(M)[0^2+1^2+3^2+...+(n-1)^2],$$

segue,

$$[0^2+1^2+3^2+...+(n-1)^2] = \sum_{k=1}^{n} k^2 \;-\; n^2$$

Façamos:

$$(n+1)^3 - 1 = \sum_{k=1}^{n}[(k+1)^3 - k^3]$$

$$(n+1)^3 - 1 = \sum_{k=1}^{n}\sum_{m=0}^{3}\binom{3}{m}k^m - k^3$$

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

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

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

$$(n+1)^3 - 1 = n + \tfrac{3n(n+1)}{2} + 3\sum_{k=1}^{n}k^2$$

$$\sum_{k=1}^{n}k^2 = \frac{2n^3\ +\ 3n^2\ +\ n}{6}$$

então,

$$[0^2 + 1^2 + 3^2 + \ldots + (n-1)^2] = \tfrac{2n^3\ +\ 3n^2\ +\ n}{6}\ -\ n^2$$

$$[0^2 + 1^2 + 3^2 + \ldots + (n-1)^2] = \tfrac{2n^3 - 3n^2 + n}{6}$$

logo,

$$I_{borda} = \sigma(M)[\tfrac{2n^3 - 3n^2 + n}{6}].$$

Teorema dos eixos paralelos nos permite obter I_x através do centro do quadrado subtraindo a massa do quadrado multiplicada pelo quadrado da distância entre o centro e uma borda.

Massa do quadrado mágico de ordem n: $n\sigma(M)$

Distância centro do quadrado a borda: $\frac{n-1}{2}$

Constante mágica: $\sigma(M) = \frac{n^3 + n}{2}$

Então,

$$I_n \equiv I_Z = 2[I_{borda} - n\sigma(M)(\tfrac{n-1}{2})^2],$$

Substituindo,

$$\begin{aligned} I_n &= 2[(\frac{n^3+n}{2})(\frac{2n^3-3n^2+n}{6}) - n(\frac{n^3+n}{2})(\frac{n^2-2n+1}{4})] \\ &= [(\frac{2n^6-3n^5+3n^4-3n^3+n^2}{6}) - (\frac{n^6-2n^5+2n^4-2n^3+n^2}{4})] \end{aligned}$$

$$I_n = [\frac{4n^6-6n^5+6n^4-6n^3+2n^2-3n^6+6n^5-6n^4+6n^3-3n^2}{12}]$$

$$I_n = [\frac{n^6-n^2}{12}]$$

concluímos,

$$I_n = \frac{1}{12}n^2(n^4-1).$$

$\square$

CAPÍTULO 3

MÉTODOS DE CONSTRUÇÃO DE QUADRADOS MÁGICOS

O alemão Heinrich Cornelius Agrippa $(1486-1535)$, físico e teólogo, escreveu o *“De Occulta Philosophia”* onde falava de quadrados mágicos de ordem 3 até à ordem 9 associando cada ordem à um planeta, atribuindo, assim, um significado astronômico a esses quadrados que representavam simbolicamente os sete planetas conhecidos por Cornelius, incluindo o Sol e a Lua (Mercúrio, Vênus, Marte, Júpiter, Saturno, o Sol e a Lua).[22]

Astro	**Ordem**
Saturno	3×3
Júpiter	4×4
Marte	5×5
Sol	6×6
Vênus	7×7
Mercúrio	8×8
Lua	9×9

Fonte: The Occult Encyclopedia of Magick Squares.

Autor: Nineveh Shadrach.

4	9	2
3	5	7
8	1	6

Saturno

4	14	15	1
9	7	6	12
5	11	10	8
16	2	3	13

Júpiter

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

Marte

22	47	16	41	10	35	4
5	23	48	17	42	11	29
30	6	24	49	18	36	12
13	31	7	25	43	19	37
38	14	32	1	26	44	20
21	39	8	33	2	27	45
46	15	40	9	34	3	28

Vênus

8	58	59	5	4	62	63	1
49	15	14	52	53	11	10	56
41	23	22	44	45	19	18	48
32	34	35	29	28	38	39	25
40	26	27	37	36	30	31	33
17	47	46	20	21	43	42	24
9	55	54	12	13	51	50	16
64	2	3	61	60	6	7	57

Mercúrio

6	32	3	34	35	1
7	11	27	28	8	30
19	14	16	15	23	24
18	20	22	21	17	13
25	29	10	9	26	12
36	5	33	4	2	31

Sol

37	78	29	70	21	62	13	54	5
6	38	79	30	71	22	63	14	46
47	7	39	80	31	72	23	55	15
16	48	8	40	81	32	64	24	56
57	17	49	9	41	73	33	65	25
26	58	18	50	1	42	74	34	66
67	27	59	10	51	2	43	75	35
36	68	19	60	11	52	3	44	76
77	28	69	20	61	12	53	4	45

Lua

Mas como se deu a construção desses quadrados? Seguiu-se uma certa ordem ou foram tentativas que acabaram dando certo?

Como os quadrados mágicos são tão populares nos mais diversos ambientes, várias técnicas foram desenvolvidas para construí-los. Esses métodos e suas variantes podem ser encontrados, por exemplo, nas obras de jacques Sesiano[29], Frank J. Swetz[32], jim Moran[22], Dame Kathleen Ollerenshaw e P. K. Srinivasan[31], e serão demonstrados e discutidos ao longo do trabalho. É natural encontrar técnicas inteligentes ao construir quadrados mágicos, observando o comportamento posicional das entradas das células. Algumas técnicas são muito exigentes, enquanto outras são quase rotineiras e simples. Os métodos de construção são decompostos de acordo com a ordem n. Há algumas técnicas que englobam um grupo de ordens, como os quadrados de ordem ímpar ($n = 2m+1$), mas também há os casos específicos para um determinado valor n.

3.1 Métodos Principais

Existem três métodos que podem ser considerados bases por darem origem aos outros, que nada mais são do que variações dos primeiros. Cada um desses métodos são específicos para um certo grupo de valores de n, que reunidos, permitem a construção de qualquer quadrado mágico, seja qual for sua ordem n.

- O método **"cross-jump"** que é específico para quadrados de ordem $n = 2m + 1$, ($n = 3, 5, 7, 9...$);
- O método **"doubly even"** é específico para quadrados de ordem $n = 4m$, ($n = 4, 8, 12, 16...$);
- O método **"Lux"** que é específico para quadrados de ordem $n = 4m + 2$, ($n = 6, 10, 14, 18...$).

Será demonstrado cada um desses métodos e, mais a diante, suas variações.

3.1.1 Método "cross-jump".

Diplomata francês Simom de La Loubère, em missão para o rei Luiz XIV, em companhia do matemático jesuíta Guy Tachard e do representante da Companhia Francesa das Índias Orientais viajaram para Sião (Tailândia), onde escreveu uma obra intitulada **"Du Royaume de Siam"** (Do Reino do Sião) em 1693, onde descreve um método de construção para quadrados mágicos de ordem ímpar[12].

Figura 3.1: Simom de La Loubère.

Fonte:https://alchetron.com/Simon-de-la-Loubère, acessado em:07/08/2023.

Método **"cross-jump"**, conhecido também como método La Loubère ou método Siamês. Este método consiste em construir um quadrado mágico com números sucessivos deslocando-os diagonalmente para cima e para direita.

O que aconteceria se colocássemos o número 1 na célula média da linha superior ou inferior, coluna esquerda ou direita, e nos movêssemos transversalmente?

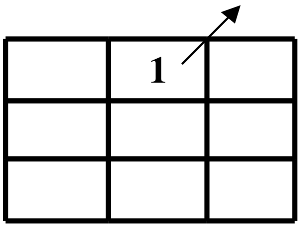
Observe que com 1 no meio da linha superior, um movimento transversal ou um salto cruzado significa um passo para a direita seguido por um passo para cima.

Ao seguir essa técnica, você descobre duas situações e deve seguir as seguintes regras:

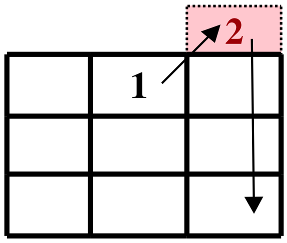
1. sempre que se tem que ir para fora, a entrada é feita na célula final da linha correspondente ou coluna.

2. sempre que for bloqueado por se encontrar com uma célula já preenchida ou virada para o canto de uma célula, a entrada é obtida na célula vizinha localizada oposta ao lado para o movimento transversal.

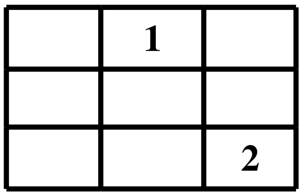
Veja as ilustrações abaixo mostrando movimento por movimento, usando como exemplo um quadrado mágico de ordem $n = 3$.



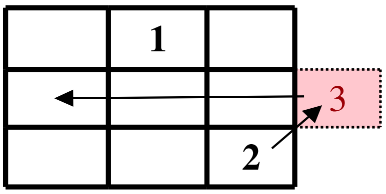
(I)



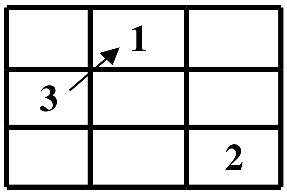
(II)



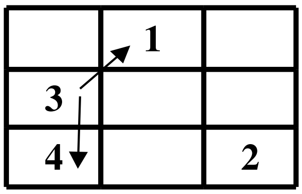
(III)



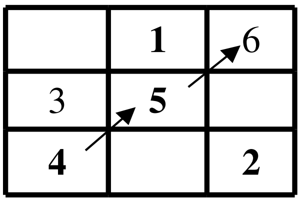
(IV)



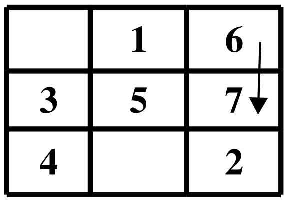
(V)



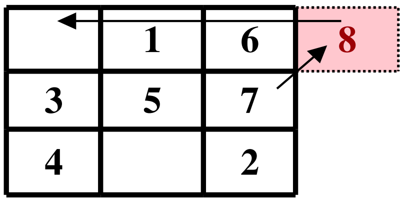
(VI)



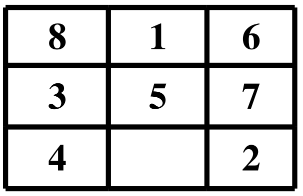
(VII)



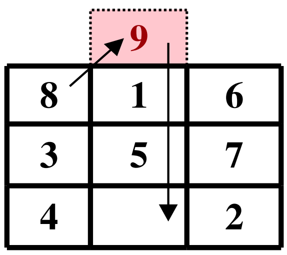
(VIII)



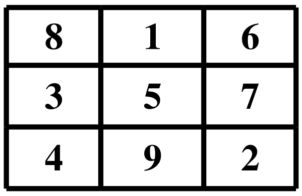
(IX)



(X)



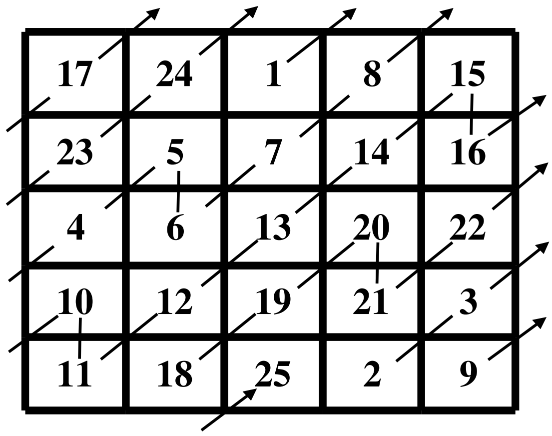
(XI)



(XII)

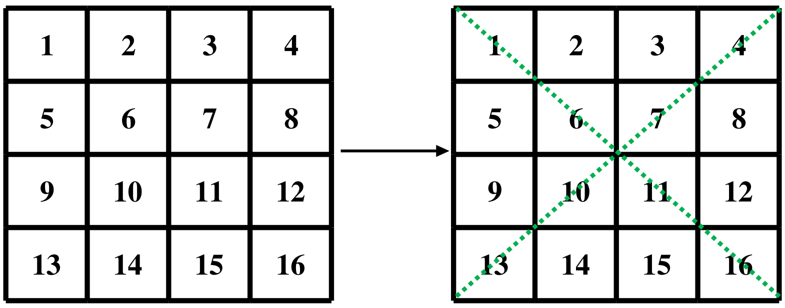
- **Ordem $n = 5$:**

O método é válido para qualquer quadrado mágico de ordem $n = 2m + 1$, ou seja, para qualquer n ímpar, porém não será demonstrado.



3.1.2 Método "doubly even".

O método para de construir quadrados mágicos de ordem $n = 4m$ consiste em preencher todas as entradas em ordem e desenhar Xs através de cada quadrado 4 × 4 interno, como mostrado abaixo:



Feito isso, substitui-se cada entrada a_{ij} na diagonal cruzada formada pelo X por $(n^2 + 1) - a_{ij}$, ou seja, inverte-se a ordem das entradas da região cruzada. No exemplo com $n = 4$, os números cruzados são originalmente $1, 6, 11, 16$ e $4, 7, 10, 13$, desse modo a entrada 1 será substituída pelo número 16 e vice-versa, o 6 pelo 11, o 4 pelo 13 e o 7 pelo 10.

O quadrado mágico obtido está representado abaixo.

16	**2**	**3**	**13**
5	**11**	**10**	**8**
9	**7**	**6**	**12**
4	**14**	**15**	**1**

- **Ordem** $n = 8$**:**

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Resultará:

64	2	3	61	60	6	7	57
9	55	54	12	13	51	50	16
17	47	46	20	21	43	42	24
40	26	27	37	36	30	31	33
32	34	35	29	28	38	39	25
41	23	22	44	45	19	18	48
49	15	14	52	53	11	10	56
8	58	59	5	4	62	63	1

3.1.3 Método "LUX".

Um método muito elegante para construir quadrados mágicos de ordem $n = 4m+2$ com $m \geq 1$ (não há quadrado mágico de ordem 2) é devido ao matemático britânico John Horton Conway, que o chama de **método "LUX"**.

Deve-se seguir as seguintes instruções:

• Crie uma matriz composta por $m+1$ linhas de **Ls**, 1 linha de **Us**, e $m-1$ linhas de **Xs**, todas de comprimento $\frac{n}{2} = 2m+1$;

• Intercale o **U** médio com o **L** acima dele. Agora gere o quadrado mágico de ordem $2m+1$, começando no quadrado central da linha superior;

• Preencha cada conjunto de quatro quadrados que circundam uma letra sequencialmente de acordo com a ordem prescrita pela letra.

Obs: As "*formas*" das letras ***L, U*** e ***X*** sugerem naturalmente a ordem de preenchimento, daí o nome do algoritmo.

$(\mathbf{m+1})$ $(\mathbf{1})$ $(\mathbf{m - 1})$

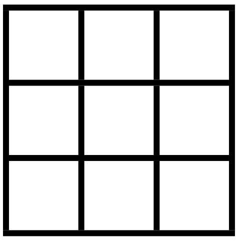
68	65	96	93	4	1	32	29	60	57
66	67	94	95	2	3	30	31	58	59
92	89	20	17	28	25	56	53	64	61
90	91	18	19	26	27	54	55	62	63
16	13	24	21	49	52	80	77	88	85
14	15	22	23	50	51	78	79	86	87
37	40	45	48	76	73	81	84	9	12
38	39	46	47	74	75	82	83	10	11
41	44	69	72	97	100	5	8	33	36
43	42	71	70	99	98	7	6	35	34

3.2 Método Staircase.

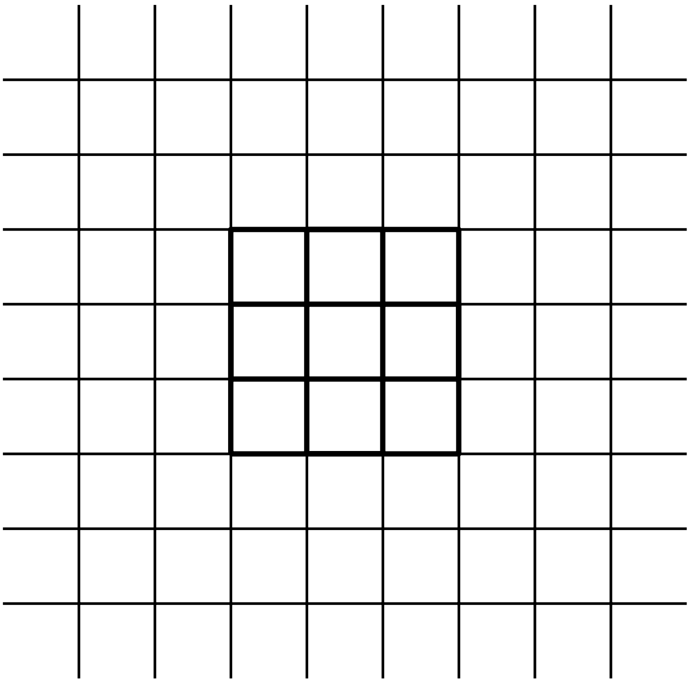
Esse método é usado para a construção de quadrados mágicos de ordem $n = 2m + 1$ (ímpar) e segue o mesmo princípio do método **"cross-jump"** já discutido, porém o princípio é demonstrado de outra forma.

Segue as instruções do método:

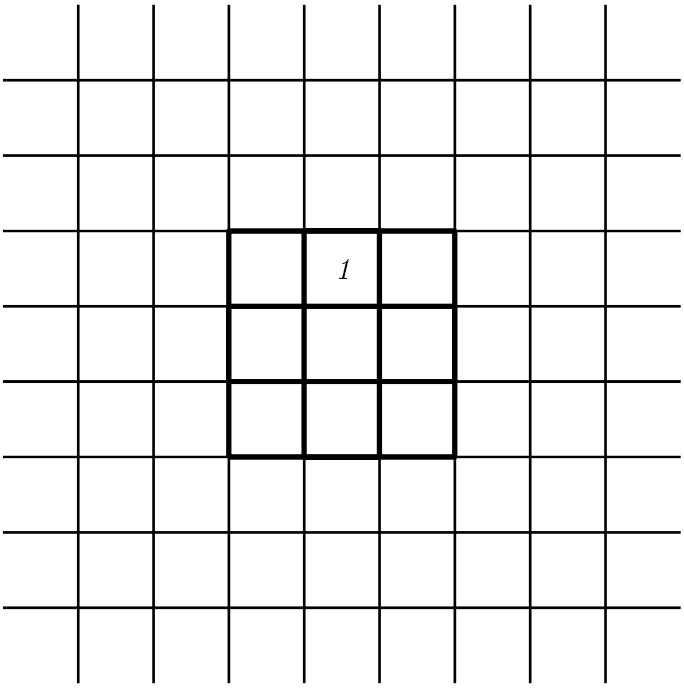
1. Construa um diagrama, da ordem de interesse, em branco (nesse caso, usaremos um quadrado mágico de ordem n = 3);



2. Imagine o diagrama cercado de outros diagramas idênticos;

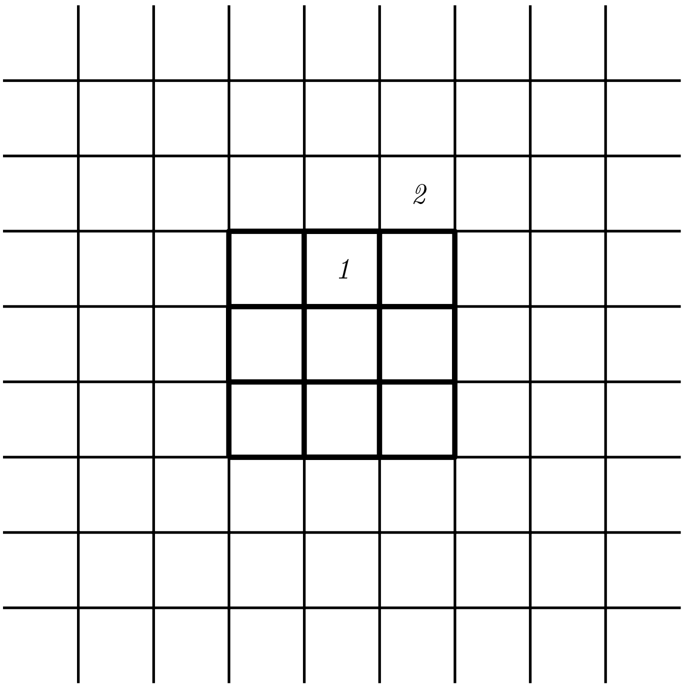


3. Regra número 1: sempre comece colocando o número 1 na primeira linha, coluna do meio do quadrado a ser construído;



4. Regra número 2: coloque o próximo número na diagonal acima à direita, a menos que este lugar já esteja preenchido;

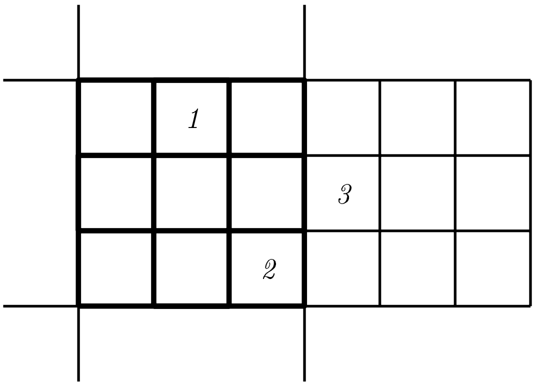
5. Desde que as duas primeiras regras tenham sido obedecidas, o número 2 se encontrará disposto na última linha e última coluna do quadrado logo acima (extensão imaginária do diagrama);



6. Colocado o número 2 fora do quadrado de interesse, tem-se que encontrar um lugar apropriado para o número dentro do diagrama;

7. Deve-se então, preencher a entrada correspondente do quadrado em construção em relação ao quadrado da extensão imaginária, com o número 2;

8. Seguindo a regra 2, o número 3 deve ser colocado como mostrado:



9. Para trazê-lo para dentro do quadrado, basta preencher a entrada correspondente, como foi feito anteriormente;

	1	
3		
		2

10. No caso do número 4, encontra-se um problema ao se seguir a regra 2 visto que a entrada na diagonal acima e à direita de 3 encontra-se preenchida. Isso nos remete à terceira regra;

11. Regra número 3: quando a entrada na diagonal acima e à direita já estiver ocupada, colocar o próximo número na entrada diretamente abaixo do número passado, logo o 4 passa a ficar embaixo do 3;

	1	
3		
4		2

12. Seguindo a regra 2, coloca-se os números 5 e 6, como mostrado:

	1	6
3	5	
4		2

13. Já o número 7 volta a entrar no caso de ser colocado em alguma entrada fora do quadrado de interesse, mas basta encontrar a entrada correspondente dentro do quadrado como já foi descrito. Porém a entrada já se encontra preenchida pelo número 4, então se segue a regra 3 e o número 7 é colocado na entrada logo abaixo do 6;

	1	6
3	5	7
4		2

14. Para os número 8 e 9, o preenchimento segue a regra 2 como mostrado:

8	1	6
3	5	7
4	9	2

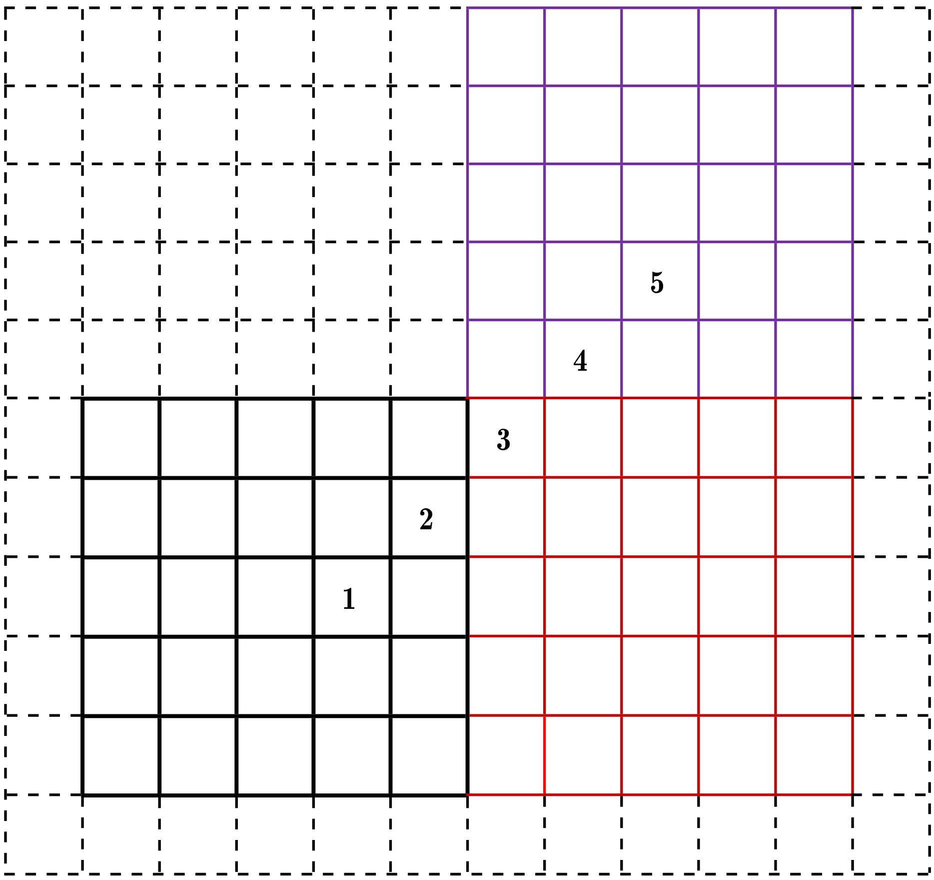
3.2.1 Variação 1 do método Staircase

Este método é uma das muitas variações com base no sistema de escada de avançar os números para cima, diagonalmente para a direita.

- Coloque o número 1 na caixa horizontalmente à direita da caixa central;

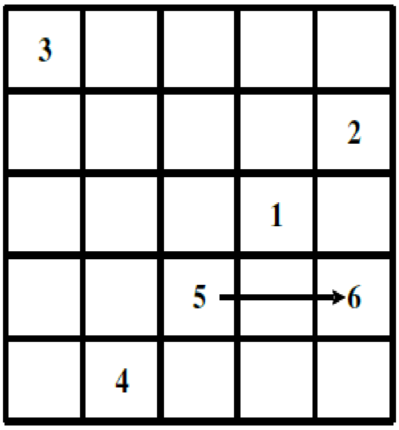
			1	

- Preencha as caixas avançando diagonalmente para cima e a direita até ser bloqueado por um número previamente colocado;

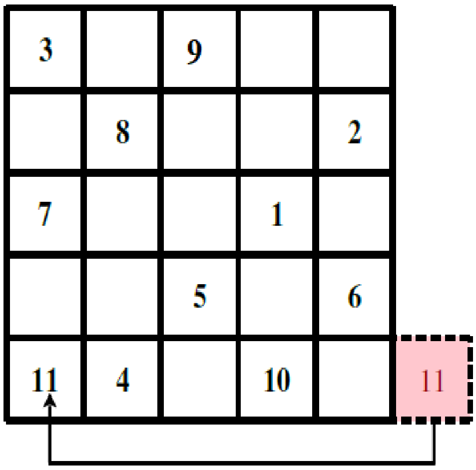


- Quando um movimento é bloqueado, coloque o próximo número da série duas caixas horizontalmente à direita do último número colocado. O movimento bloqueado ocorrerá a cada cinco movimentos em um quadrado de ordem 5×5, a cada sete movimentos em um quadrado de ordem 7×7, e assim por diante. Quando o movimento bloqueado ocorre, use os conceitos de extensão imaginária dos quadrados para continuar preenchendo.

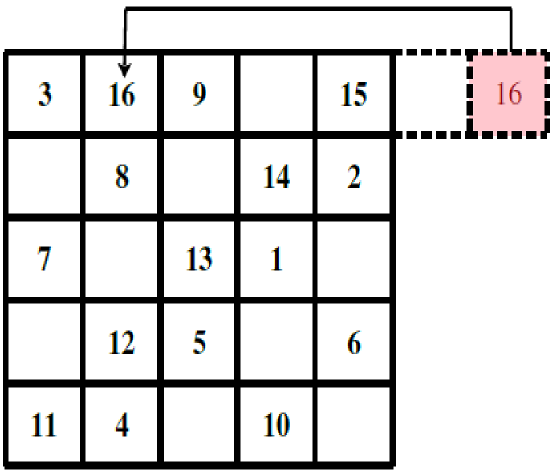
Os passos estão demonstrados:



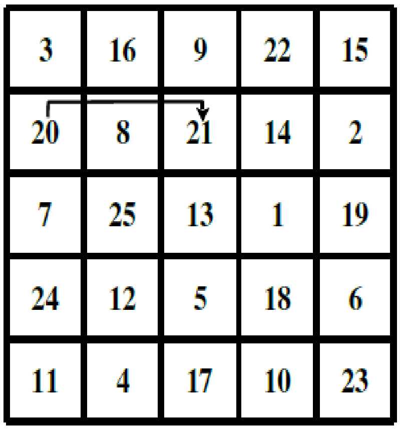
Primeiro movimento bloqueado



Segundo movimento bloqueado



Terceiro movimento bloqueado



Quarto movimento bloqueado

3.2.2 Variação 2 do método Staircase

Para entender corretamente a construção desse método deve-se pensar de uma maneira diferente. Não se trata apenas um quadrado de ordem 9×9 contendo 81 célula, mas também um arranjo de nove quadrados de ordem 3, cada um contendo nove caixas como mostrado abaixo.

	8			1			6	
	3			5			7	
	4			9			2	

Basta dividir a sequência de 1 a 81 em nove unidades iguais e numerá-las mentalmente da seguinte maneira:

Unidade $1 : 1 - 9$	Unidade $4 : 28 - 36$	Unidade $7 : 55 - 63$
Unidade $2 : 10 - 18$	Unidade $5 : 37 - 45$	Unidade $8 : 64 - 72$
Unidade $3 : 19 - 27$	Unidade $6 : 46 - 54$	Unidade $9 : 73 - 81$

Em seguida, considerando cada unidade como um único número, coloque a primeira unidade, $1 - 9$ (como se estivesse fazendo um quadrado mágico 3×3), no espaço 3×3 acima, onde você escreveu no número 1, seguindo a sequência do método "*cross-jump*" para continuar completando o quadrado, com a segunda unidade de $10 - 18$ e assim por diante.

			8	1	6			
			3	5	7			
			4	9	2			

Passo 1

			8	1	6			
			3	5	7			
			4	9	2			
						17	10	15
						12	14	16
						13	18	11

Passo 2

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

Passo 3

			8	1	6			
			3	5	7			
			4	9	2			
26	19	24						
21	23	25						
22	27	20						
35	28	33				17	10	15
30	32	34				12	14	16
31	36	29				13	18	11

Passo 4

			8	1	6			
	8		3	5	7		**6**	
			4	9	2			
26	19	24	44	37	42			
21	23	25	39	41	43		**7**	
22	27	20	40	45	38			
35	28	33				17	10	15
30	32	34		**9**		12	14	16
31	36	29				13	18	11

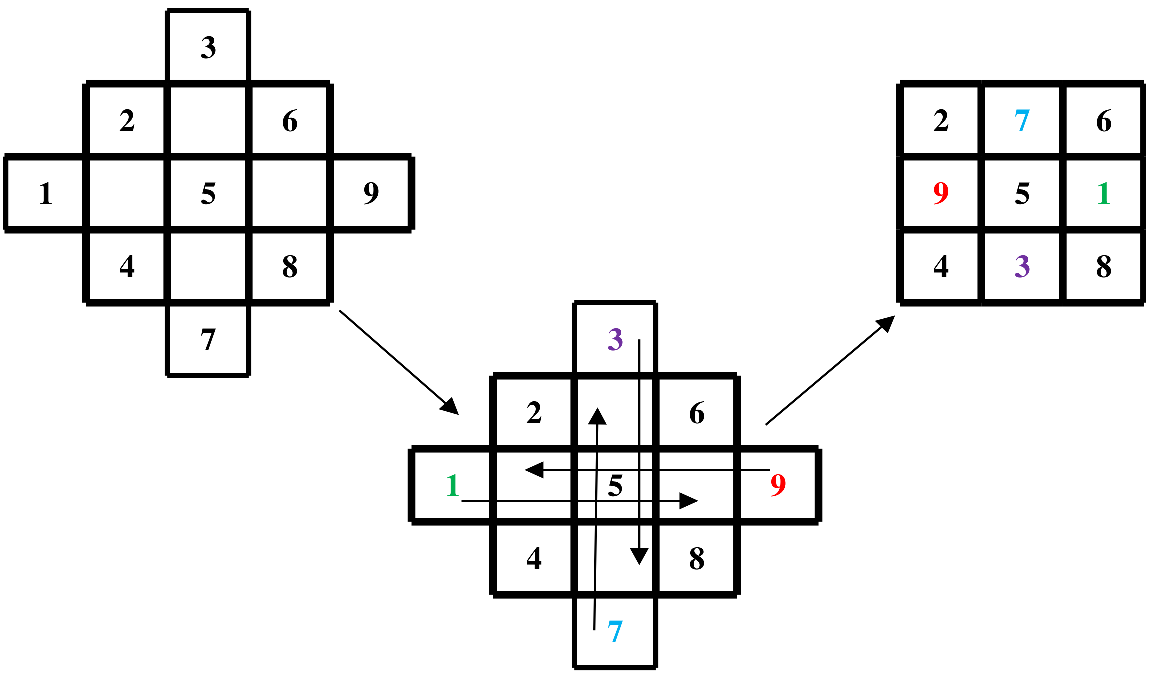
Passo 5

71	64	69	8	1	6	53	46	51
66	68	70	3	5	7	48	50	52
67	72	65	4	9	2	49	54	47
26	19	24	44	37	42	62	55	60
21	23	25	39	41	43	57	59	61
22	27	20	40	45	38	58	63	56
35	28	33	80	73	78	17	10	15
30	32	34	75	77	79	12	14	16
31	36	29	76	81	74	13	18	11

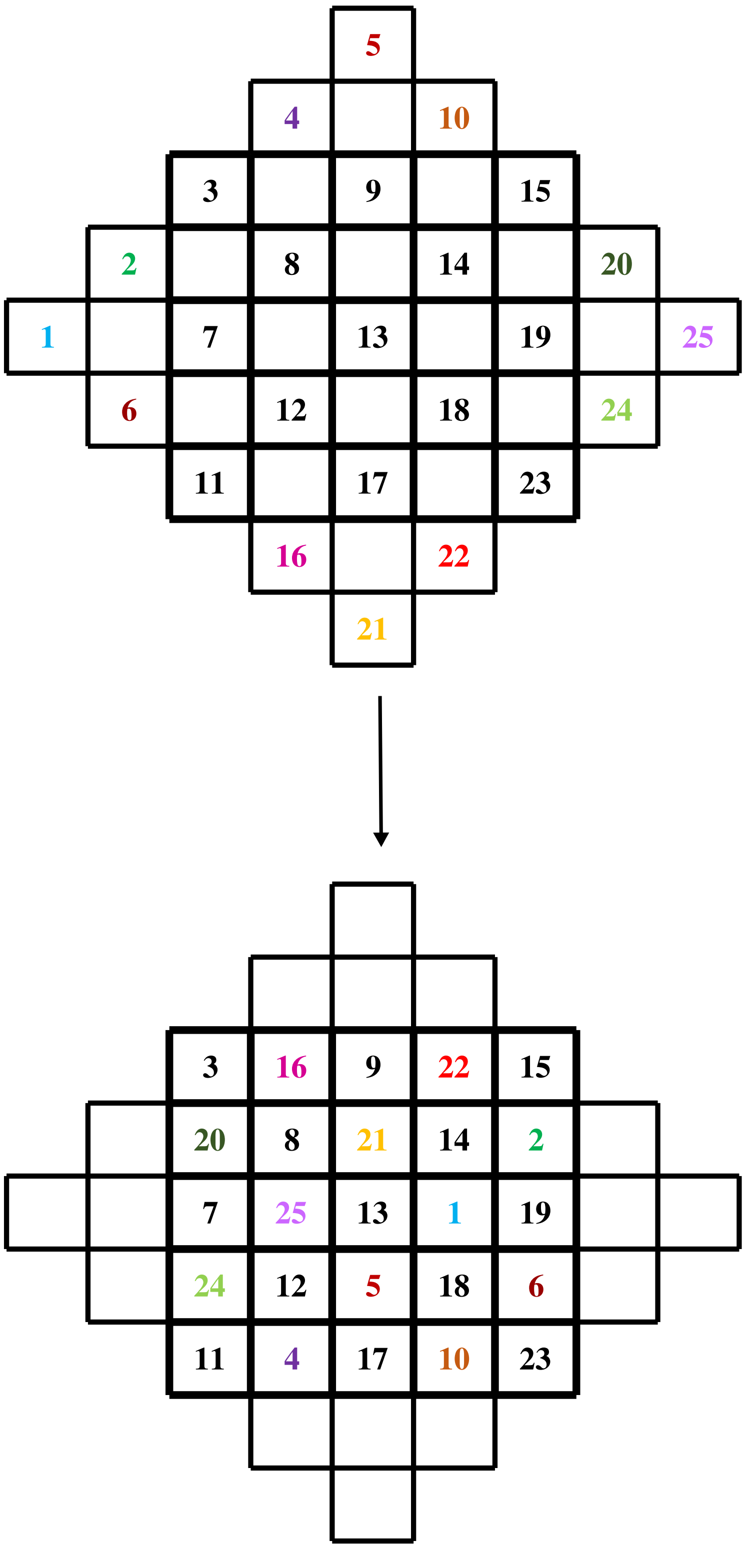
Passo 6

3.3 Método Pirâmide

Apresentaremos um antigo procedimento de composição de quadrados mágicos, ou seja, quadrados com ordem ($n = 2m + 1$), ímpar: 3×3, 5×5, 7×7, etc. Esse processo foi proposto no século $XVII$ pelo matemático francês Bachet [25]. Como o procedimento de Bachet é utilizado, entre outras coisas, para um quadrado de 9 células, é conveniente iniciar sua descrição com este exemplo, pois é mais simples. Então, começamos a compor o quadrado mágico de 9 células pelo procedimento de Bachet. Depois de traçar uma pirâmide quadriculada em treze quadrados, escrevemos em ordem crescente os números de 1 a 9, dispondo-os em fileiras oblíquas, três em cada fileira, como pode ser visto nas figuras abaixo. Na segunda pirâmide os números que estão no vértice, são colocadas nas células opostas, configurando a formação do quadrado mágico.



A aplicação deste método para o quadrado de ordem 5×5 é mostrada abaixo:



3.4 Método do Cavalo

Como qualquer enxadrista sabe, um quadrado mágico de ordem 8 tem o mesmo número de células que um tabuleiro de xadrez. Essa semelhança significa que podemos criar um tipo especial de quadrado mágico com base nos movimentos de uma peça de xadrez.

O cavalo é uma peça interessante, porque ao contrário das outras peças, não se move verticalmente, horizontalmente ou diagonalmente ao longo de uma linha reta. Em vez disso, o cavalo se move em forma de L, conforme mostrado no diagrama.

	X		**X**	
X				**X**
		K		
X				**X**
	X		**X**	

Tabela 3.1: cavalo (K) pode se mover em forma de L para qualquer um dos quadrados marcados com um X

Veja as ilustrações abaixo mostrando movimento por movimento, usando como exemplo um quadrado mágico de ordem $n = 3$.

•**1º Passo:** defina o número 1 na casa do meio da fileira superior.

_	**1**	_
_	_	_
_	_	_

•**2º Passo:** a partir do número 1, subindo uma fileira acima do número 1. Nota-se que o número 1 encontra-se na fileira superior, nesse caso deve-se continuar na fileira inferior. Em seguida, move-se uma coluna à direita, onde estará à casa do número 2.

_	**1**	_
_	_	_
_	_	**2**

•**3º Passo:** a partir do número 2, subindo uma fileira superior, a seguir movimenta-se uma coluna à direita, nesse caso desloca-se para coluna do lado esquerdo e coloca-se o número 3.

	1	
3		
		2

•**3º Passo:** do número 3, sobe-se uma fileira superior e move-se uma coluna à direita, como existe o número 1 na casa indicada, o próximo número estará na casa imediatamente abaixo do número 3, onde colocaremos o número 4.

	1	
3		
4		**2**

•**4º Passo:** para encontrar a casa do número 5, a partir do número 4, sobe-se uma fileira superior e move-se uma coluna à direita.

	1	
3	**5**	
4		**2**

•**5º Passo:** seguindo a regra do cavalo ($\uparrow \rightarrow$) a célula do número 5, chega-se ao número 6.

	1	**6**
3	**5**	
4		**2**

•**6º Passo:** a partir do número 6, sobe-se uma fileira superior, nesse caso deve-se continuar na fileira inferior. Em seguida, move-se uma coluna à direita, nesse caso desloca-se para coluna do lado esquerdo, como existe o número 4 na casa indicada, o próximo número estará na casa imediatamente abaixo do número 6, onde alocaremos o número 7.

	1	**6**
3	**5**	**7**
4		**2**

•**7º Passo:** do número 7 e seguindo a regra do cavalo ($\uparrow \rightarrow$), similar ao 3º passo, chega-se ao número 8.

8	**1**	**6**
3	**5**	**7**
4		**2**

•**8º Passo:** a partir do número 8, sobe-se uma fileira superior, nesse caso deve-se continuar na fileira inferior. Em seguida, move-se uma coluna à direita e coloca-se o número 9.

8	**1**	**6**
3	**5**	**7**
4	**9**	**2**

Mas é possível para um cavalo que se move dessa maneira visitar todas as casas do tabuleiro exatamente uma vez?

Um dos primeiros matemáticos a investigar o passeio do cavaleiro (método do cavalo), como o problema ficou conhecido, foi o grande matemático suíço Leonhard Euler. Seu trabalho inspirou outros a aceitar o desafio.

Usando o método do cavalo, William Beverley conseguiu produzir um quadrado mágico, conforme mostrado abaixo. As células são numeradas em sequência, conforme o cavaleiro (cavalo) as visita. Embora todas as linhas e colunas somem 260, as diagonais principais não, portanto, estritamente falando, é um quadrado semimágico. Na verdade, um quadrado mágico baseado no passeio de um cavaleiro é frequentemente chamado de passeio mágico, então o que Beverley produziu em 1848 é um passeio semimágico![1]

1	**48**	**31**	**50**	**33**	**16**	**63**	**18**
30	**51**	**46**	**3**	**62**	**19**	**14**	**35**
47	**2**	**49**	**32**	**15**	**34**	**17**	**64**
52	**29**	**4**	**45**	**20**	**61**	**36**	**13**
5	**44**	**25**	**56**	**9**	**40**	**21**	**60**
28	**53**	**8**	**41**	**24**	**57**	**12**	**37**
43	**6**	**55**	**26**	**39**	**10**	**59**	**22**
54	**27**	**42**	**7**	**58**	**23**	**38**	**11**

À primeira vista, parece que o seguinte quadrado mágico de *Feisthamel* se encaixa no projeto. As linhas, colunas e diagonais somam 260. Infelizmente, é apenas uma volta parcial do cavaleiro, pois há um salto de 32 para 33.

5	**14**	**53**	**62**	**3**	**12**	**51**	**60**
54	**63**	**4**	**13**	**52**	**61**	**2**	**11**
15	**6**	**55**	**24**	**41**	**10**	**59**	**50**
64	**25**	**16**	**7**	**58**	**49**	**40**	**1**
17	**56**	**33**	**42**	**23**	**32**	**9**	**48**
34	**43**	**26**	**57**	**8**	**39**	**22**	**31**
27	**18**	**45**	**36**	**29**	**20**	**47**	**38**
44	**35**	**28**	**19**	**46**	**37**	**30**	**21**

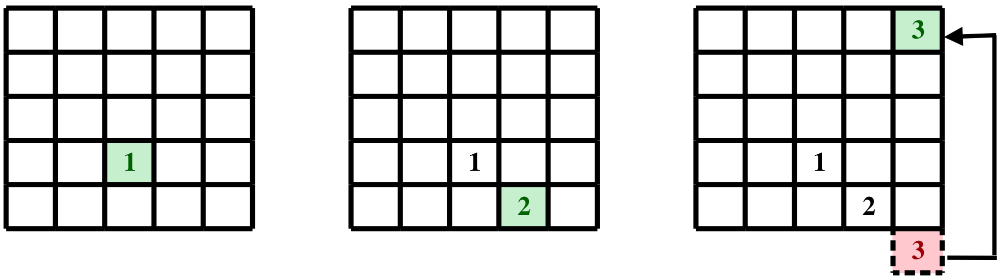
Então, quando é possível transformar o passeio de um cavaleiro em um quadrado mágico? Em 2003, Stertenbrink e Meyrignac [1] finalmente resolveram esse problema calculando todas as combinações possíveis. Eles encontraram 140 passeios semimágicos, mas nenhum passeio mágico. Xeque-mate!

3.5 Método do Moschopoulos

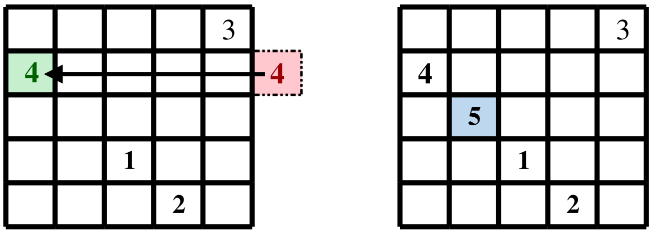
Um método muito simples para criar quadrados mágicos de ordem ímpar é conhecido como *Moschopoulos*. Mas hoje em dia, sabemos por um escrito de um autor desconhecido do século 12 que o algoritmo conhecido como Moschopoulos na verdade vem de *Ibn al-Haytham* (aprox. $965-1041$)[35]. Este método cria quadrados mágicos para todas as ordens ímpares n e foi o método mais comum nos anos posteriores à sua criação devido à sua simplicidade. Pode ser descrito com os seguintes passos.

- Coloque o primeiro número na célula logo abaixo da célula central do quadrado.
- Determine a próxima célula indo uma linha para baixo e uma coluna para a direita.
- Depois de exatamente n passos obliquamente, você chega a uma cela já ocupada. Em vez disso, dê um passo intermediário que o levará duas linhas abaixo da última célula ocupada.
- Sempre que sair do quadrado em uma extremidade, continue no lado oposto do quadrado.

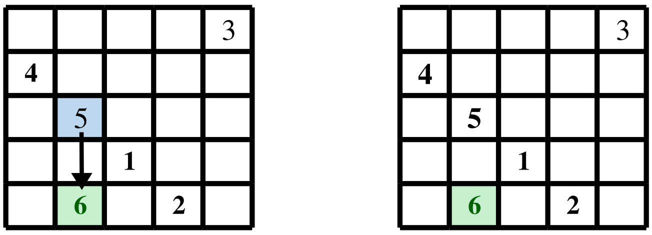
No início, colocamos o número 1 na célula diretamente abaixo do centro do quadrado. Para o segundo número, temos que descer uma linha e uma coluna à direita. Da mesma forma para o terceiro número, e obtenha uma posição fora do quadrado. Mas como olhamos para as linhas e colunas ciclicamente, podemos somar a ordem do quadrado a partir do número da linha e novamente obter um número de linha que esteja dentro do quadrado. Ou seja, contornamos o quadrado na mesma coluna e continuamos na ponta oposta.



Com a quarta etapa, há novamente um pequeno problema, pois saímos do quadrado para a direita.



O primeiro grupo de cinco números agora está posicionado corretamente. O próximo número, porém, já cria um novo problema, pois o número 6 levaria à célula já ocupada pelo número 1. Nesse ponto, a sequência de etapas dada deve ser interrompida com uma etapa intermediária especial, na qual simplesmente desça duas linhas a partir da última célula ocupada.



Você pode continuar com essas etapas e somente parar quando o quadrado estiver preenchido com os números $1, 2, 3, \ldots, n^2$.

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

3.6 Método Ralier des Ourmes

Um método um pouco mais complicado foi encontrado por Jean-Joseph Rallier des Ourmes [23], que primeiro colocou o número mediano no campo central do quadrado, incluindo o número 1 abaixo e a ordem n à esquerda do centro. As células que são simétricas ao centro são então preenchidas com seus números complementares.

Agora as células restantes na linha do meio estão preenchidas. A partir do número 25 no centro do quadrado, cada segunda célula agora é preenchida. O número atual é diminuído em $n-1$, progredindo para a direita, mas aumentado em $n-1$, progredindo para a esquerda. O mesmo procedimento é seguido começando do número vizinho esquerdo ou direito (7 ou 43) da célula central. No entanto, agora você só se move em uma direção.

O mesmo procedimento é seguido com a coluna do meio, exceto que os números são diminuídos em $n+1$ para cima, mas aumentados para baixo em $n+1$. O resultado é mostrado para a ordem $n = 7$.

			49			
		7	25	43		
			1			

			41			
			17			
			49			
13	31	7	25	43	19	37
			1			
			33			
			9			

Começando pelos números na linha ou coluna do meio, os campos vazios do quadrado agora são preenchidos na diagonal de acordo com o diagrama. No canto superior direito, o número atual é sempre diminuído em n, por outro lado, é aumentado em n no canto inferior esquerdo. Diminuiu em n no canto superior esquerdo e aumentou em $+1$ no canto inferior direito.

-1				-8				-7
				41				
				17				
				49				
6	13	31	7	25	43	19	37	-6
				1				
				33				
				9				
7				8				1

22			41			4
	23		17		11	
		24	49	18		
13	31	7	25	43	19	37
		32	1	26		
	39		33		27	
46			9			28

A figura a seguir mostra o quadrado mágico de ordem $n = 7$ finalizado por este método.

22	47	16	41	10	35	4
5	23	48	17	42	11	29
30	6	24	49	18	36	12
13	31	7	25	43	19	37
38	14	32	1	26	44	20
21	39	8	33	2	27	45
46	15	40	9	34	3	28

3.7 Método de De la Hire

Em um artigo publicado em 1705, Philippe de la Hire[13] descreve alguns métodos para criar quadrados mágicos de ordem $n = 4k$ a partir de dois quadrados auxiliares.

No primeiro quadrado auxiliar ele preenche a primeira metade da linha superior com qualquer número z do intervalo de 1 a n, a segunda metade com seu número complementar $n+1-z$. Na linha abaixo, ele troca as duas metades. É assim que ele procede com os números restantes nos outros pares de linhas até que todo o quadrado auxiliar seja preenchido.

O segundo quadrado auxiliar, por outro lado, é construído usando colunas com números ligeiramente alterados. Agora a metade superior é preenchida com um número arbitrário z do intervalo de 0 a $n-1$ e a metade inferior com seu número complementar, que é $n-1-z$ no intervalo de números alterado, pois o intervalo de números começa aqui em 0

Na próxima coluna, as duas metades são trocadas. De acordo com esse princípio, todos os outros pares de colunas são preenchidos com os números restantes, como na figura à direita.

8	8	8	8	1	1	1	1
1	1	1	1	8	8	8	8
5	5	5	5	4	4	4	4
4	4	4	4	5	5	5	5
7	7	7	7	2	2	2	2
2	2	2	2	7	7	7	7
6	6	6	6	3	3	3	3
3	3	3	3	6	6	6	6

7	0	6	1	5	2	4	3
7	0	6	1	5	2	4	3
7	0	6	1	5	2	4	3
7	0	6	1	5	2	4	3
0	7	1	6	2	5	3	4
0	7	1	6	2	5	3	4
0	7	1	6	2	5	3	4
0	7	1	6	2	5	3	4

Os números do segundo quadrado auxiliar são agora multiplicados por $n = 8$ e adicionados aos números do primeiro quadrado auxiliar. O resultado é o quadrado mágico abaixo.

64	8	56	16	41	17	33	25
57	1	49	9	48	24	40	32
61	5	53	13	44	20	36	28
60	4	52	12	45	21	37	29
7	63	15	55	18	42	26	34
2	58	10	50	23	47	31	39
6	62	14	54	19	43	27	35
3	59	11	51	22	46	30	38

Claro, o papel dos dois quadrados auxiliares pode ser trocado. Isso significa que as linhas do primeiro quadrado auxiliar foram preenchidas com os números de 0 a $n-1$, enquanto as linhas do segundo quadrado auxiliar foram preenchidas com os números de 1 a n.

6	6	6	6	1	1	1	1
1	1	1	1	6	6	6	6
4	4	4	4	3	3	3	3
3	3	3	3	4	4	4	4
7	7	7	7	0	0	0	0
0	0	0	0	7	7	7	7
5	5	5	5	2	2	2	2
2	2	2	2	5	5	5	5

6	3	8	1	5	4	7	2
6	3	8	1	5	4	7	2
6	3	8	1	5	4	7	2
6	3	8	1	5	4	7	2
3	6	1	8	4	5	2	7
3	6	1	8	4	5	2	7
3	6	1	8	4	5	2	7
3	6	1	8	4	5	2	7

Agora é claro que todos os números do primeiro quadrado auxiliar devem ser multiplicados por $n=8$, antes que os números do segundo quadrado auxiliar sejam adicionados. O resultado disso é o seguinte quadrado mágico.

54	**51**	**56**	**49**	**13**	**12**	**15**	**10**
14	**11**	**16**	**9**	**53**	**52**	**55**	**50**
38	**35**	**40**	**33**	**29**	**28**	**31**	**26**
30	**27**	**32**	**25**	**37**	**36**	**39**	**34**
59	**62**	**57**	**64**	**4**	**5**	**2**	**7**
3	**6**	**1**	**8**	**60**	**61**	**58**	**63**
43	**46**	**41**	**48**	**20**	**21**	**18**	**23**
19	**22**	**17**	**24**	**44**	**45**	**42**	**47**

CAPÍTULO 4

APLICAÇÕES DE QUADRADOS MÁGICOS

4.1 Quadrados mágicos em criptografia

Neste capítulo estudaremos as aplicações dos quadrados mágicos na criptografia e sua utilização como uma ferramenta lúdica no ensino aprendizagem.

O estudo de técnicas de comunicação segura que permitem apenas ao remetente e ao destinatário das mensagens ler seu conteúdo é conhecido como **criptografia**. A palavra "cryptos" vem da palavra grega "kryptos", que significa "oculto". Ele está intimamente ligado à criptografia, que é o processo de embaralhar texto simples em texto cifrado e, em seguida, voltar novamente quando é recebido.

Além disso, a criptografia inclui técnicas como micropontos e fusão para ofuscar informações em fotografias. Os antigos egípcios eram conhecidos por aplicar técnicas semelhantes em hieróglifos complicados, e uma das primeiras cifras modernas é atribuída ao imperador romano Júlio César.

Criptografia e Descriptografia

Em seu nível mais básico, a criptografia envolve duas etapas: Criptografia (codificação) e Descriptografia (decodificação). Para criptografar o texto simples e convertê-lo em texto cifrado, o processo de criptografia emprega uma cifra. A descriptografia, por outro lado, usa a mesma cifra para converter o texto cifrado em texto simples.

Criptografar e descriptografar e-mail e outras mensagens de texto simples é o uso mais comum de criptografia ao transmitir dados eletrônicos. A abordagem simétrica ou "chave secreta" é a forma mais básica.

Os dados são criptografados usando a chave secreta, e a mensagem codificada e a chave secreta são então entregues ao receptor para decodificação. Qual é o problema então? Um terceiro é tudo o que eles precisam para decodificar e ler a comunicação se ela for interceptada. Criptologistas inventaram o esquema assimétrico ou de "chave pública" para superar esse problema. Cada usuário tem duas chaves neste caso: uma pública e outra privada. Os remetentes criptografam a mensagem e a transmitem após solicitar a chave pública do destinatário. Portanto, a criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. É a arte dos “códigos secretos”.

Como funciona a criptografia?

Vejamos um exemplo de como a criptografia funciona.

Suponha que você queira criptografar uma mensagem básica como **"AMO O PROFMAT.”**

Podemos criptografar a mensagem usando "Cifra de César" (também conhecida como cifra de deslocamento), que é um dos tipos básicos de criptografia.

A mensagem **AMO O PROFMAT** seria codificado como **DPRRSURIPDW**.

Uma cifragem análoga a este foi usado, por exemplo, pelo imperador romano Júlio César para comunicar-se com as legiões romanas em batalha pela Europa. Este sugere ser o primeiro exemplo de um código secreto de que se tem relato. Cifragem como o de César amarga um grande problema: é muito fácil de “decodificar”

Decodificar um código significa ser capaz de ler a mensagem, mesmo não sendo seu destinatário real. Na verdade, qualquer código que envolva substituir cada letra sistematicamente por outro símbolo qualquer sofre do mesmo problema. Isto ocorre porque a frequência média com que cada letra aparece em um texto de uma dada língua é mais ou menos constante.

Tipos de Criptografia

Dependendo do processo que seguem para criptografar e descriptografar os dados, a criptografia pode ser categorizada em diferentes tipos, como "*hashing*", criptografia simétrica, criptografia assimétrica e algoritmos de troca de chaves.

- **Hashing**

Hashing é um tipo de criptografia na qual uma mensagem é convertida em uma sequência de texto ilegível com o objetivo de confirmar seu conteúdo, em vez de ocultá-lo.

Quando o editor dos arquivos ou software os fornece para download, esse tipo de criptografia é mais comumente empregado para proteger a transmissão de software e arquivos grandes. A razão para isso é que, embora o cálculo do hash seja simples, é bastante difícil encontrar uma entrada inicial que seja uma correspondência precisa para o resultado necessário.

- **Criptografia Simétrica**

A Criptografia Simétrica é talvez o tipo de criptografia mais clássico e também aquele com o qual você está mais familiarizado. Este método de criptografia, criptografa uma mensagem usando uma única chave e, em seguida, a descriptografa após ser recebida na outra extremidade. Exemplo: O método da **cifra pigpen** (cifra maçonica).

- **Criptografia assimétrica**

Em contraste com a criptografia simétrica, que emprega uma única chave para criptografar e descriptografar, a criptografia assimétrica usa duas chaves distintas para criptografar e descriptografar.

A primeira chave é uma chave pública usada para criptografar mensagens, enquanto a segunda chave é usada para decodificá-las. Este método é que ele só pode decifrar mensagens criptografadas recebidas de uma chave pública. Exemplo: O método **RSA**.

- **Algoritmos de Troca de Chaves**

Esse tipo de criptografia não é especialmente relevante para ninguém fora do campo da segurança cibernética. Para trocar chaves de criptografia com segurança com uma pessoa desconhecida, um algoritmo de troca de chaves como o "*Diffie-Hellman*" é utilizado.

Vamos conhecer alguns métodos de codificação de mensagem utilizando uma das categorias descritas acima.

4.1.1 Método da cifra pigpen

A cifra PIGPEN (às vezes chamada de cifra maçônica ou cifra do maçom) é uma cifra de substituição geométrica simples que troca letras por símbolos que são fragmentos de uma grade. A origem exata da cifra é incerta, mas foram encontrados registros desse sistema que remontam pelo menos ao século $XVIII$. Variações dessa cifra foram usadas tanto pela irmandade rosacruz quanto pelos maçons, embora os últimos a usassem com tanta frequência que o sistema é frequentemente chamado de cifra do maçom. Eles começaram a usá-lo no início do século $XVIII$ para manter seus registros de história e ritos privados e para correspondência entre líderes de lojas.[4]

A versão mais antiga conhecida é de Heinrich Cornelius Agrippa von Nettesheim que explica o método em seu "*De occulta philosophia*" publicado em 1533. Este trabalho foi reutilizado em 1586 por Blaise de Vigenère em seu tratado sobre criptografia. Existem muitas variações possíveis, mas qualquer criptoanalista treinado geralmente não terá problemas para decifrar as mensagens codificadas. A tradução literal do nome da cifra é Porco no Chiqueiro e vem do fato de que cada uma das letras (os porcos) é colocada numa "casa"(o chiqueiro).[4]

Veja o exemplo da codificação pigpen numa lápide maçônica de James Leeson ($1756-1794$) que está enterrado no "*Trinity Church Cemetery*", em Nova York. Sua lápide traz uma curiosa inscrição. Permaneceu um quebra-cabeça local até 1889, quando o Trinity Record descobriu que é o epitáfio e lido como LEMBRE-SE DA MORTE.

Figura 4.1: Lápide de James Leeson

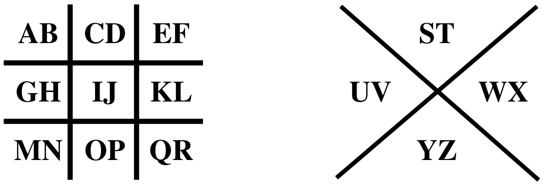
Fonte:http://lacustodeditombe.blogspot.com/2015/07/83-ricorda-la-morte.html , acessado em:19/03/2023.

Características do método pigpen

Origem:	Desenvolvida por Heinrich Cornelius Agrippa von Nettelsheim.
Classe:	Substituição simples.
Tipo:	Monoalfabética monogrâmica.
Metódo:	Substituição de letras por símbolos. O cifrante, ao invés de ser constituído por letras, é constituído por símbolos especiais.
Segurança:	Baixíssima.
Uso:	Apenas interesse histórico.
Criptoanálise:	Uma análise da frequência das letras é suficiente para quebrar a cifra.

Atribuição

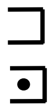
A cifra consiste em alojar as letras do alfabeto em "casas", como descrito no esquema abaixo.



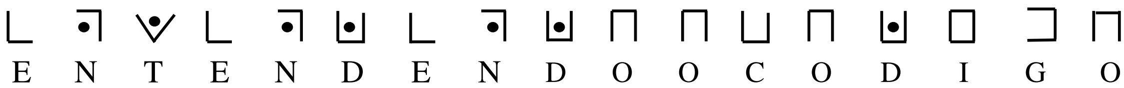
Dessa forma, cada letra tem um símbolo característico para representá-la. Como visto, cada "casa" possui duas letras e a forma de distinguí-las é adicionando um pontinho ao símbolo correspondente à "casa" para representar as segunda letra.

Por exemplo:

A letra **G** é representado por
A letra **H** é representado por

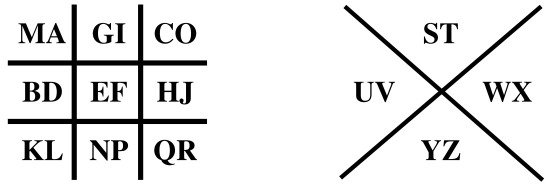


A frase "*Entendendo o código*", escrita utilizando a cifra ficaria da seguinte forma:

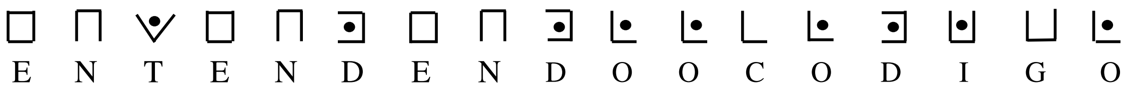


A maneira de tornar o código decifrável apenas para seu destinatário é embutir uma pequena sequência de letras ou mesmo um palavra, chamada de "segredo", de forma a não se repetir nenhuma letra, no início do esquema de letras e símbolos e assim modificar a relação entre eles, completando o resto do alfabeto na sequência de preenchimento e pulando as letras utilizadas na escrita da palavra escolhida.

Pegando por exemplo a palavra **MÁGICO** como sendo o "*segredo*", o esquema de letras e símbolos ficaria da seguinte forma:



Dessa forma, a mesma frase escrita anteriormente ficaria da seguinte forma:



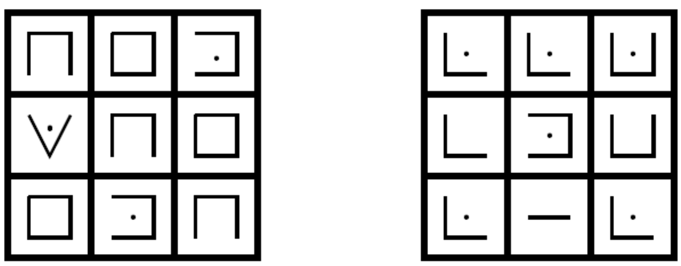
4.1.2 Mesclando quadrados mágicos e o códico Pigpen

Devido ao grande número de técnicas de criptografia e a facilidade com que códigos podem ser decifrados, surgiu a ideia de mesclar o código Pigpen com quadrados mágicos, levando em conta o princípio de construção e ordem de preenchimento destes, com o objetivo de dificultar que a mensagem enviada seja decifrada por alguém que não seja seu destinatário legítimo. Para isso, é necessário que se tenha um conhecimento prévio das técnicas de construção de quadrados mágicos, visto que os símbolos referentes às letras do alfabeto que compõe a mensagem a ser enviada serão agora dispostos nas entradas de um quadrado mágico, seguindo sua ordem de preenchimento. O que define a ordem do quadrado mágico escolhido e a quantidade de quadrados a serem utilizados está relacionado ao número de letras necessárias para escrever a mensagem. Porém o mais importante é que ambas as partes, tanto remetente quanto destinatários, devem estar cientes do quadrado mágico escolhido e da técnica utilizada na sua construção.
Por exemplo, para mandar uma mensagem com a frase "Entendendo o código", que possui 17 letras, pode-se utilizar dois quadrados mágicos de ordem 3×3, restando uma entrada sem preencher. Para demonstrar, utilizaremos o esquema de letras e símbolos com a palavra MÁGICO sendo o "segredo"do código, e a técnica utilizada para preencher os quadrados mágicos 3×3 sendo o método cross-jump.

8	1	6
3	5	7
4	9	2

8	1	6
3	5	7
4	9	2

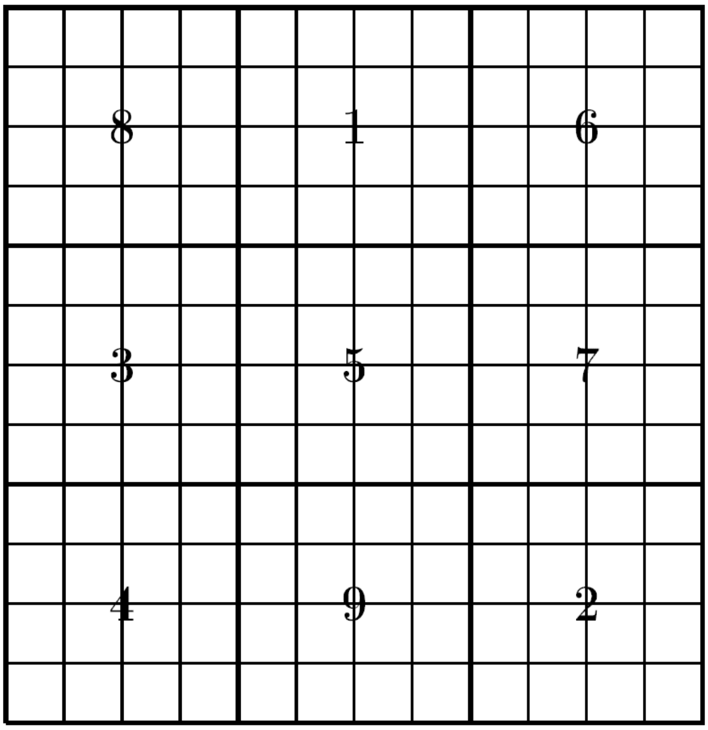
Ordem de preenchimento dos quadrados.



Quadrados preenchidos com os símbolos.

Outro exemplo, que pode complicar mais ainda que o código seja decifrado facilmente, é utilizar uma variação do método staircase como o apresentado no tópico 3.2 para mesclar com código Pigpen em frases que exijam um quadrado com muitas entradas devido ao número de caracteres que as compõem. Para criptografar a seguinte frase **"*Quadrados mágicos revelam brilhantemente a simetria de números. Com seu charme místico parecem atrair alguma inteligência e a ordem cósmica que domina toda a existência.*"** Utilizando o método staircase com um quadrado de ordem 12×12, subdividido em 9 quadrados internos 4×4, e o "segredo" sendo MÁGICO esquemas será apresentado abaixo:

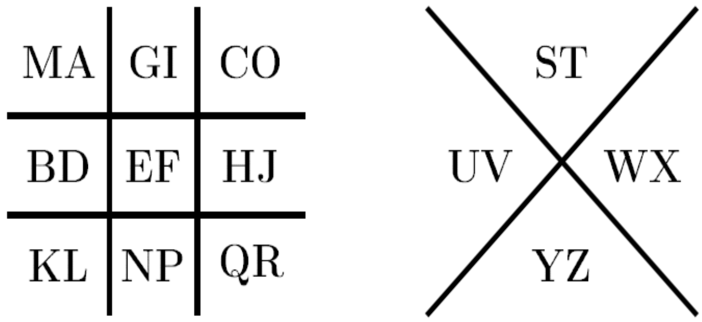
- Quadrado de ordem 12×12 subdividido em outros 9 quadrados internos de ordem 4×4.



- Ordem de preenchimento dos quadrados interior de ordem 4×4.

16	2	3	13
5	11	10	8
9	7	6	12
4	14	15	1

- Relação de letras e símbolos com o "segredo"sendo a palavra MÁGICO.



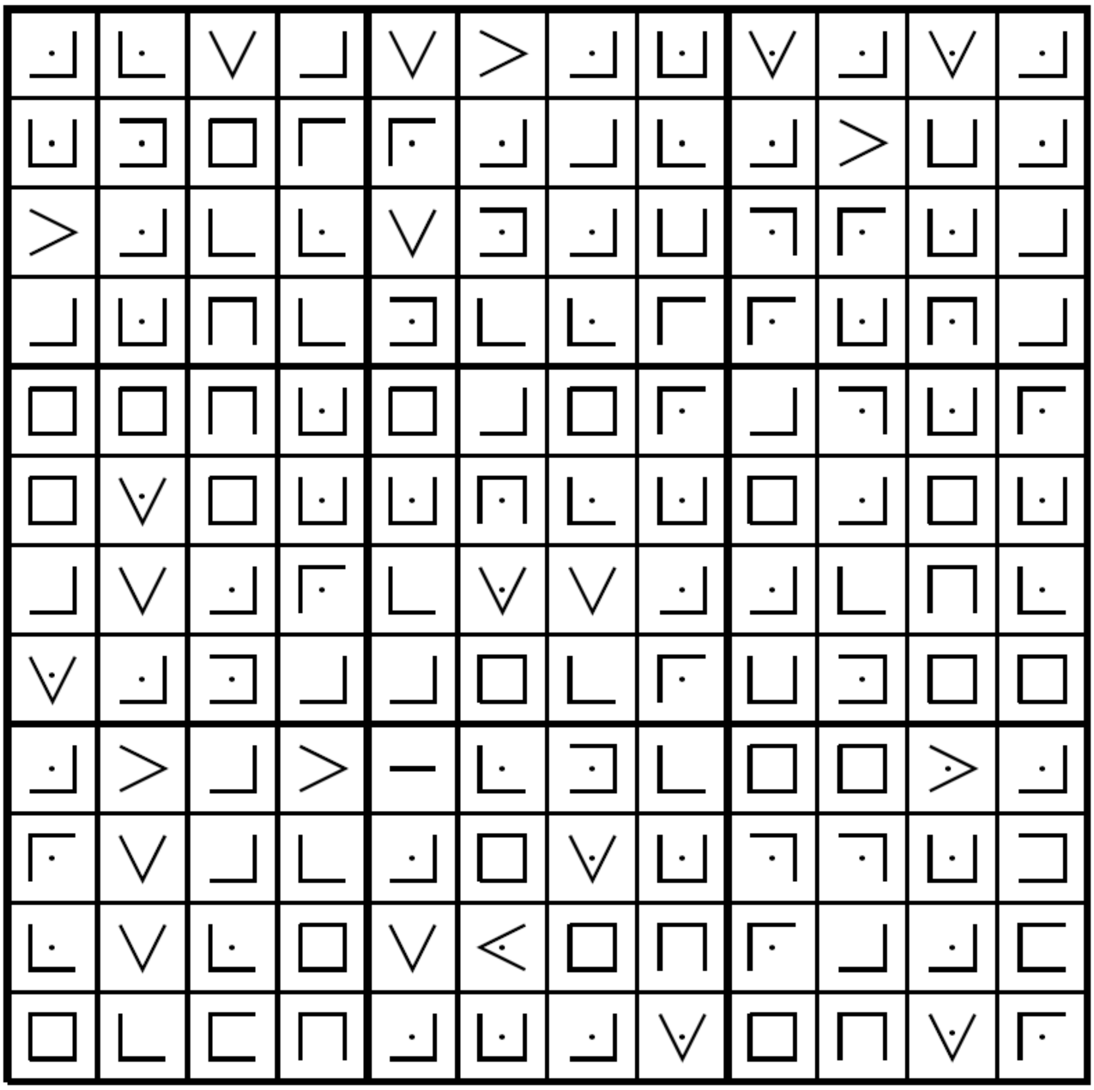
A sequência numérica do quadrado mágico que deve ser seguida no preenchimento é a seguinte:

128	114	115	125	16	2	3	13	96	92	83	93
117	123	122	120	5	11	10	8	85	91	90	88
121	119	118	124	9	7	6	12	89	87	86	92
116	126	127	113	4	14	15	1	84	94	95	81
48	34	35	45	80	66	67	77	112	98	99	109
37	43	42	40	69	75	74	72	101	107	106	104
41	39	38	44	73	71	70	76	105	103	102	108
36	46	47	33	68	78	79	65	100	110	111	97
64	50	51	61	144	130	131	141	32	18	19	29
53	59	58	56	133	139	138	136	21	27	26	24
57	55	54	60	137	135	134	140	25	23	22	28
52	62	63	49	132	142	143	129	20	30	31	17

O quadrado preenchido com as letras que compõem a frase deve ser da seguinte forma:

A	O	S	M	S	U	A	I	T	A	T	A
I	D	E	Q	R	A	M	O	A	U	G	A
U	A	C	O	S	D	A	G	L	R	I	M
M	I	N	C	D	C	O	Q	R	I	N	M
E	E	N	I	E	M	E	R	M	L	I	R
E	T	E	I	I	P	O	I	E	A	E	I
M	S	A	R	C	T	S	A	A	C	N	O
T	A	D	M	M	E	C	R	G	D	E	E
A	U	M	U	-	O	D	C	E	E	V	A
R	S	M	C	A	E	T	I	L	L	I	B
O	S	O	E	S	X	E	N	R	M	A	H
E	C	H	N	A	I	A	T	E	N	T	R

O quadrado preenchido pela mensagem já criptografada está representado a seguir:



O processo de decodificação segue da seguinte maneira:

- Dada a sequência de preenchimento, fazer o processo inverso e listar os símbolos na ordem;
- Fazer a correlação entre os símbolos e as letras a partir do "segredo" que foi previamente definido.

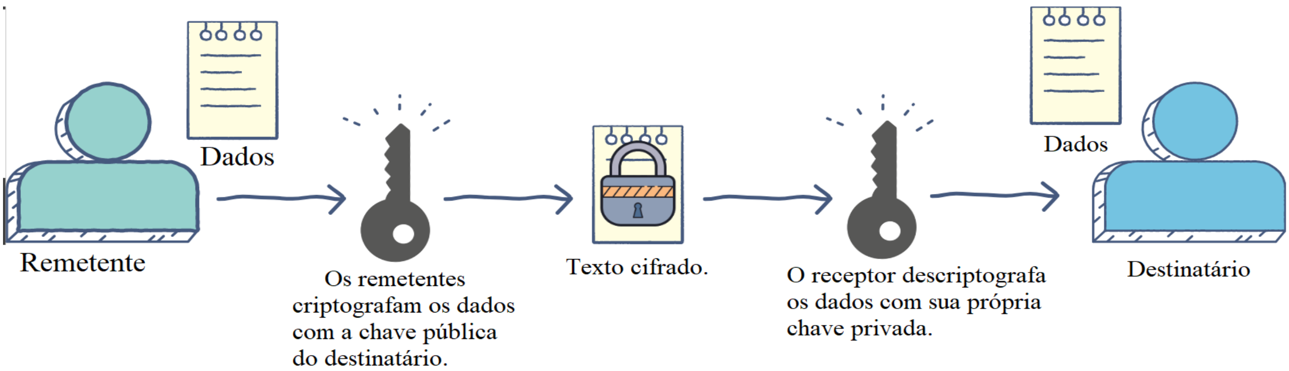
Por exemplo, decodificando a primeira parte do código :

4.1.3 Método da cifra RSA

O algoritmo RSA é um algoritmo de criptografia assimétrica; isso significa que ele usa uma chave pública e uma chave privada (ou seja, duas chaves diferentes matematicamente vinculadas). Como seus nomes sugerem, uma chave pública é compartilhada publicamente, enquanto uma chave privada é secreta e não deve ser compartilhada com ninguém. O algoritmo **RSA** recebeu o nome daqueles que o inventaram em 1978: "*Ron Rivest, Adi Shamir e Leonard Adleman*".

A ilustração a seguir destaca como a criptografia assimétrica funciona:

Figura 4.2: Algoritmo RSA



Fonte: Ilustração do próprio autor.

Como funciona

O algoritmo RSA garante que as chaves, na ilustração acima, sejam as mais seguras possíveis. As etapas a seguir destacam como funciona:

1. Gerando as chaves

I – Selecione dois números primos grandes, p e q. Os números primos precisam ser grandes para que seja difícil para alguém descobrir.

II – Calcular $n = p \cdot q$.

III – Calcular a função totiente; $\varphi(n) = (p-1)(q-1)$.

IV – Selecione um número inteiro e, de tal modo que e é coprimo com n para $1 < e < \varphi(n)$. O par de números (n, e) compõe a chave pública.

V – Calcular d de tal modo que $e \cdot d \equiv 1(mod\varphi(n))$. d pode ser encontrado usando o algoritmo euclidiano estendido. O par $< n, d >$ compõe a chave privada.

2. Criptografia

Dado um texto simples de chave P, representado como um número, o texto cifrado C é calculado como:

$$C \equiv P^e (mod n).$$

3. Descriptografia

Usando a chave privada $< n, d >$, o texto simples pode ser encontrado usando:

$$P \equiv C^d (mod n).$$

Vamos dar um exemplo de algoritmo de **criptografia RSA**:

Exemplo 4.1.1. *Este exemplo mostraremos como podemos criptografar um texto chave $P = 9$ simples usando o algoritmo de criptografia de chave pública RSA. Neste exemplo usaremos os números primos $p = 7$ e $q = 11$ para gerar as chaves pública e privada.*

Explicação:

Etapa 1: Selecione dois números primos grandes, $p = 7, q = 11$

Etapa 2: Multiplique esses números para encontrar $n = p \times q = 7 \times 11 = 77$.

Etapa 3: Calculamos

$$\varphi(n) = (p-1)(q-1) = (7-1)(11-1) = 60.$$

Etapa 4: Escolha um número e, tal que n seja relativamente primo de $\varphi(n) = 60$. Escolha e tal que $1 < e < \varphi(n)$, e é primo de 60. Tome $e = 7$. Assim, a chave pública é $< e, n >= (7, 77)$.

Etapa 5: Uma mensagem de texto simples P é criptografada usando a chave pública $< e, n >= (7, 77)$. Para encontrar o texto cifrado do texto simples, a seguinte fórmula é usada para obter o texto cifrado C.

$$\begin{aligned} C &\equiv P^e (mod n) \\ &\equiv 9^7 (mod 77) \\ &\equiv 37 (mod 77) \end{aligned}$$

Ou seja $C = 37$.

Etapa 6: A chave privada é $< d, n >$. Para determinar a chave privada, usamos a seguinte fórmula para d tal que:

$$\begin{aligned} e \cdot d &\equiv 1(mod \varphi(n)) \\ 7 \cdot d &\equiv 1(mod 60) \end{aligned}$$

ou seja $7d = 60k + 1$ isto é $d = \frac{60k+1}{7}$ para $k = 0, 1, 2, \ldots$.

Tomado $k = 5$ temos $d = 43$. A chave privada é $< d, n >= (43, 77)$.

Etapa 7: Uma mensagem de texto cifrado C é descriptografada usando a chave privada $< d, n >$. Para calcular o texto simples P a partir do texto cifrado C, a seguinte fórmula é usada para obter o texto simples.

$$\begin{aligned} P &\equiv C^d (modn) \\ &\equiv 37^{43}(mod 77) \\ &\equiv 9(mod 77) \end{aligned}$$

Neste exemplo, texto simples $P = 9$ e o texto cifrado $C = 37$.

Exemplo 4.1.2. *Em um sistema criptográfico RSA, um determinado A usa dois números primos, 13 e 17, para gerar as chaves pública e privada. Se o público de A é 35. Então a chave privada de A?*

Temos $p = 13, q = 17$ e $n = p \cdot q = 221$. E também $\varphi(221) = 192$. Tendo que $mdc(35, 192) = 1$ e foi dado que $e = 35$. Para determinar d utilizaremos

$$e \cdot d \equiv 1(mod \varphi(n)).$$

Logo

$$35 \cdot d \equiv 1 (mod 192)$$

Portanto

$$d = \frac{192k+1}{35} \quad k = 0, 1, 2, 3, \ldots$$

Para k = 0 : $d = \frac{1}{35}$.

Para k = 1 :$d = \frac{193}{35}$

Para k = 2: $d = \frac{385}{35} = 11$

A chave privada é $< d, n >= (11, 221)$.

Pré-codificação

Para simplificar, vamos supor que a mensagem original seja um texto onde não há números, apenas palavras, nas quais são formadas apenas por letras maiúsculas. Portanto, a mensagem é finalmente formada com as letras que compõem as palavras e os espaços entre as palavras. Chamamos esse primeiro passo de pré-codificação para distingui-lo do próprio processo de codificação. Na pré-codificação, usaremos um conjunto de caracteres que consiste em 128 valores ASCII (American Standard Code for Information Interchange), as letras são convertidas em números usando a seguinte tabela de conversão:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
65	**66**	**67**	**68**	**69**	**70**	**71**	**72**	**73**	**74**	**75**	**76**	**77**

N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
78	**79**	**80**	**81**	**82**	**83**	**84**	**85**	**86**	**87**	**88**	**89**	**90**

O espaço entre duas palavras será substituído pelo número 32, quando for feita a conversão. Por exemplo, a frase **PROFMAT NA UFU** é convertida no número:

P	R	O	F	M	A	T		N	A		U	F	U
80	82	79	70	77	65	84	32	78	65	32	85	70	85

Codificando e Decodificando uma Mensagem

Isso conclui o processo de pré-codificação e podemos continuar com codificação em si. Para cifrar a mensagem precisamos apenas de n, que é o produto de números primos. dizemos que n é a chave de codificação do sistema RSA que estamos usando. Esta chave pode ser tornada pública; isto é, podemos enviá-la a qualquer um que queira nos mandar uma mensagem, sem preocupação de mantê-la secreta. Por isso a chave de codificação também é conhecida como chave pública do sistema.

Codificação

Vamos a codificação usando uma chave RSA, para isso suponha $n = p \cdot q$, tal que, se escolhermos $p = 5$ e $q = 23$, então $n = 115$ e $e = 31$. Neste caso, a mensagem, cuja conversão numérica foi feita acima, pode ser quebrada nos seguintes blocos:

$$80-82-79-70-77-65-84-32-78-65-32-85-70-85$$

Codificando toda a mensagem passo a passo, temos o seguinte:

$C \equiv P^e (mod n)$
$80^{31} \equiv 65(mod 115);$
$82^{31} \equiv 3(mod 115);$
$79^{31} \equiv 89(mod 115);$
$70^{31} \equiv 70(mod 115);$
$77^{31} \equiv 78(mod 115);$
$65^{31} \equiv 10(mod 115);$
$84^{31} \equiv 14(mod 115);$
$32^{31} \equiv 48(mod 115);$
$78^{31} \equiv 2(mod 115);$
$65^{31} \equiv 10(mod 115);$
$32^{31} \equiv 48(mod 115);$
$85^{31} \equiv 100(mod 115);$

$70^{31} \equiv 70 (mod 115)$;

$85^{31} \equiv 100 (mod 115)$;

Reunindo todos os blocos, descobrimos que a mensagem codificada é

65 - 3 - 89 - 70 - 78 - 10 - 14 - 48 - 2 - 10 - 48 - 100 - 70 - 100

Decodificação

A informação que precisamos para decodificar consiste em dois números: n e o inverso de d tal que $d > 0$, então tomemos 31 de módulo $\varphi(115) = 88$. Pela definição utilizaremos

$$e \cdot d \equiv 1 (mod \varphi(n)).$$

ou seja

$$31 \cdot d \equiv 1 (mod 88).$$

Assim

$$d = \frac{[1 + 88 \cdot k]}{31}, \quad k = 0, 1, 2, 3, \ldots$$

Para $k = 0$, temos $d = \frac{1}{31}$.

Para $k = 1$, temos: $d = \frac{89}{31}$.

Para $k = 2$, temos: $d = \frac{177}{31}$.

Sucessivamente até $k = 25$, temos:

$$d = \frac{2201}{31} = 71.$$

Aplicando a receita dada anteriormente ao primeiro bloco da mensagem codificada, temos que $D(65)$ é igual ao resto da divisão de 65^{71} por $n = 115$.

$P = C^d (mod n)$

$65^{71} \equiv 80 (mod 115)$;

$3^{71} \equiv 82 (mod 115)$;

$89^{71} \equiv 79 (mod 115)$;

$70^{71} \equiv 70 (mod 115)$;

$78^{71} \equiv 77(mod 115);$

$10^{71} \equiv 65(mod 115);$

$14^{71} \equiv 84(mod 115);$

$48^{71} \equiv 32(mod 115);$

$2^{71} \equiv 78(mod 115);$

$10^{71} \equiv 65(mod 115);$

$48^{71} \equiv 32(mod 115);$

$100^{71} \equiv 85(mod 115);$

$70^{71} \equiv 70(mod 115);$

$100^{71} \equiv 85(mod 115);$

Todos os cálculos acimas pode ser verificados no link:https://rsa-calculator.netlify.app/

4.1.4 Mesclando quadrados mágicos e o códico RSA

Usando o algoritmo RSA, construímos um "quadrado mágico duplamente par (doubly even)" de ordem 32 que contém 1024 diferentes valores, como o conjunto de caracteres consiste em 128 valores ASCII, o quadrado mágico é dividido logicamente em 8 matrizes diferentes, cada uma com 128 valores correspondentes aos caracteres ASCII individual, para maior realização do assunto proposto.

1024	2	3	1021	1020	6	7	1017	1016	10	11	1013	1012	14	15	1009	1008	18	19	1005	1004	22	23	1001	1000	26	27	997	996	30	31	993	Matriz 1
33	991	990	36	37	987	986	40	41	983	982	44	45	979	978	48	49	975	974	52	53	971	970	56	57	967	966	60	61	963	962	64	
65	959	958	68	69	955	954	72	73	951	950	76	77	947	946	80	81	943	942	84	85	939	938	88	89	935	934	92	93	931	930	96	
928	98	99	925	924	102	103	921	920	106	107	917	916	110	111	913	912	114	115	909	908	118	119	905	904	122	123	901	900	126	127	897	
896	130	131	893	892	134	135	889	888	138	139	885	884	142	143	881	880	146	147	877	876	150	151	873	872	154	155	869	868	158	159	865	Matriz 2
161	863	862	164	165	859	858	168	169	855	854	172	173	851	850	176	177	847	846	180	181	843	842	184	185	839	838	188	189	835	834	192	
193	831	830	196	197	827	826	200	201	823	822	204	205	819	818	208	209	815	814	212	213	811	810	216	217	807	806	220	221	803	802	224	
800	226	227	797	796	230	231	793	792	234	235	789	788	238	239	785	784	242	243	781	780	246	247	777	776	250	251	773	772	254	255	769	
768	258	259	765	764	262	263	761	760	266	267	757	756	270	271	753	752	274	275	749	748	278	279	745	744	282	283	741	740	286	287	737	Matriz 3
289	735	734	292	293	731	730	296	297	727	726	300	301	723	722	304	305	719	718	308	309	715	714	312	313	711	710	316	317	707	706	320	
321	703	702	324	325	699	698	328	329	695	694	332	333	691	690	336	337	687	686	340	341	683	682	344	345	679	678	348	349	675	674	352	
672	354	355	669	668	358	359	665	664	362	363	661	660	366	367	657	656	370	371	653	652	374	375	649	648	378	379	645	644	382	383	641	
640	386	387	637	636	390	391	633	632	394	395	629	628	398	399	625	624	402	403	621	620	406	407	617	616	410	411	613	612	414	415	609	Matriz 4
417	607	606	420	421	603	602	424	425	599	598	428	429	595	594	432	433	591	590	436	437	587	586	440	441	583	582	444	445	579	578	448	
449	575	574	452	453	571	570	456	457	567	566	460	461	563	562	464	465	559	558	468	469	555	554	472	473	551	550	476	477	547	546	480	
544	482	483	541	540	486	487	537	536	490	491	533	532	494	495	529	528	498	499	525	524	502	503	521	520	506	507	517	516	510	511	513	
512	514	515	509	508	518	519	505	504	522	523	501	500	526	527	497	496	530	531	493	492	534	535	489	488	538	539	485	484	542	543	481	Matriz 5
545	479	478	548	549	475	474	552	553	471	470	556	557	467	466	560	561	463	462	564	565	459	458	568	569	455	454	572	573	451	450	576	
577	447	446	580	581	443	442	584	585	439	438	588	589	435	434	592	593	431	430	596	597	427	426	600	601	423	422	604	605	419	418	608	
416	610	611	413	412	614	615	409	408	618	619	405	404	622	623	401	400	626	627	397	396	630	631	393	392	634	635	389	388	638	639	385	
384	642	643	381	380	646	647	377	376	650	651	373	372	654	655	369	368	658	659	365	364	662	663	361	360	666	667	357	356	670	671	353	Matriz 6
673	351	350	676	677	347	346	680	681	343	342	684	685	339	338	688	689	335	334	692	693	331	330	696	697	327	326	700	701	323	322	704	
705	319	318	708	709	315	314	712	713	311	310	716	717	307	306	720	721	303	302	724	725	299	298	728	729	295	294	732	733	291	290	736	
288	738	739	285	284	742	743	281	280	746	747	277	276	750	751	273	272	754	755	269	268	758	759	265	264	762	763	261	260	766	767	257	
256	770	771	253	252	774	775	249	248	778	779	245	244	782	783	241	240	786	787	237	236	790	791	233	232	794	795	229	228	798	799	225	Matriz 7
801	223	222	804	805	219	218	808	809	215	214	812	813	211	210	816	817	207	206	820	821	203	202	824	825	199	198	828	829	195	194	832	
833	191	190	836	837	187	186	840	841	183	182	844	845	179	178	848	849	175	174	852	853	171	170	856	857	167	166	860	861	163	162	864	
160	866	867	157	156	870	871	153	152	874	875	149	148	878	879	145	144	882	883	141	140	886	887	137	136	890	891	133	132	894	895	129	
128	898	899	125	124	902	903	121	120	906	907	117	116	910	911	113	112	914	915	109	108	918	919	105	104	922	923	101	100	926	927	97	Matriz 8
929	95	94	932	933	91	90	936	937	87	86	940	941	83	82	944	945	79	78	948	949	75	74	952	953	71	70	956	957	67	66	960	
961	63	62	964	965	59	58	968	969	55	54	972	973	51	50	976	977	47	46	980	981	43	42	984	985	39	38	988	989	35	34	992	
32	994	995	29	28	998	999	25	24	1002	1003	21	20	1006	1007	17	16	1010	1011	13	12	1014	1015	9	8	1018	1019	5	4	1022	1023	1	

Figura 4.3: Quadrado Mágico Doubly Even 32x32

Suponha que $p = 13$, $q = 17$ e a chave pública $e = 11$, então $n = 221$, e $\varphi(221) = (p-1)(q-1) = 192$ logo a chave secreta $d = 35$. Para criptografar a mensagem **(UFU)**, os valores ASCII de **U** e **F** são 85 e 70 respectivamente, então para criptografar **U** que aparece na primeira e terceira posição no texto simples, os numerais que aparecem no 85º posição da primeira matriz e na 85ª posição da segunda matriz (Figura 4.5 que é dividido logicamente em 8 matrizes) são tomados respectivamente, tal que, $Np(U_1) = 939$, $Np(U_2) = 811$ e $Np(F) = 954$. E a cifra

$$C(U_1) \equiv 939^{11}(mod 221) \equiv 217,$$

$$C(U_2) \equiv 811^{11}(mod 221) \equiv 125,$$

$$C(F) \equiv 954^{11}(mod 221) \equiv 8$$

da mesma forma, usamos esta substituição para cada caractere repetido no texto simples, portanto, para cada caractere repetido de $A, B, C, \ldots$(que aparece mais de uma vez no texto simples), cifra diferente são geradas.

A comparação entre o algoritmo RSA comum e o RSA proposto com Quadrado Mágico Doubly Even.

Para ilustrar o resultado do algoritmo RSA com quadrado mágico, o texto simples **(PROFMAT NA UFU)** é primeiro criptografado usando RSA existente (se $p = 17, q = 23, n = 391, (p-1).(q-1) = 352$ e $e = 13$) e a saída é mostrada na tabela abaixo. É claro que os caracteres (A, F e U) aparecem duas vezes no texto simples, portanto, no RSA comum, o texto cifrado deles é o mesmo, enquanto no sugerido (RSA com QMDE), o valor do texto cifrado do primeiro (A) que é (959) é diferente do segundo (A) que é (831) e a mesma coisa com quaisquer caracteres repetidos no texto simples.

RSA COMUM			RSA NO QUADRADO MÁGICO DOUBLY EVEN		
TEXTO	ASCII VALOR	TEXTO CIFRADO	TEXTO	VALOR NO QUADRADO MÁGICO	TEXTO CIFRADO
P	80	201	P	81	98
R	82	192	R	942	91
O	79	245	O	80	201
F	70	185	F	954	270
M	77	110	M	947	269
A	65	260	A	959	210
T	84	373	T	85	187
N	78	334	N	946	262
A	65	260	A	831	308
U	85	187	U	939	191
F	70	185	F	826	249
U	85	187	U	811	82

O aspecto de segurança do RSA é melhorado porque não há valores duplicados no quadrado mágico, na cifra simples RSA, os mesmos valores de texto cifrado são gerados sempre que os mesmos caracteres, enquanto no proposto (RSA com QMDE) valores diferentes são produzidos no texto cifrado para cada ocorrência do mesmo caractere. Ele desempenha um papel importante no aumento da aleatoriedade e segurança do algoritmo.

4.1.5 Método da cifra Vigenère

A Cifra de Vigenére é um método de criptografia manual baseado em uma variação da Cifra de César. Ele funciona aplicando uma série de diferentes Cifras de César no texto simples, com base nas letras de uma chamada palavra- chave . Na verdade, é uma forma simples de substituição polialfabética.

A Cifra de Vigenère existe em diferentes formas, como uma matriz retangular com 26 alfabetos deslocados (tabula reta) e como dois discos concêntricos com um alfabeto completo cada. As letras da palavra-chave determinam quantos lugares o disco interno deve ser deslocado.

Ao longo da história, a cifra de Vigenère foi reinventada várias vezes. Foi falsamente atribuído a Blaise de Vigenère, como foi originalmente descrito em 1553 por Giovan Battista Bellaso em seu livro "*La cifra del*".

A primeira descrição bem documentada de uma cifra polialfabética, no entanto, foi feita por volta de 1467 por Leon Battista Alberti. A Cifra de Vigenère é, portanto, às vezes chamada de Disco de Alberti ou Cifra de Alberti. Em 1508, Johannes Trithemius inventou a chamada tabula reta (uma matriz de alfabetos deslocados) que mais tarde sofreria uma ferrenha crítica.[33] A cifra de Vigenère usa uma tabela de 26×26 com A a Z como cabeçalho de linha e cabeçalho de coluna. Essa tabela é geralmente chamada de Tabela de Vigenère, ou Quadrado de Vigenère. A primeira linha desta tabela tem as 26 letras do alfabeto latino. Começando com a segunda linha, cada linha tem as letras deslocadas para a esquerda uma posição de forma cíclica. Por exemplo, quando B é deslocado para a primeira posição na segunda linha, a letra A se move para o final.

Figura 4.4: tabela de Viginere

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

Fonte:https://crypto.interactive-maths.com/vigenegravere-cipher.html, acessado em:25/06/2023.

Dois métodos executam a cifra de Vigenère.

Método 1: CRIPTOGRAFIA

Vamos a um exemplo: O texto simples é "PROFMAT NA UFU"e a chave "ENQ".

Para gerar uma nova chave, a chave fornecida é repetida de maneira circular, desde que o comprimento do texto simples não seja igual ao da nova chave.

Texto simples	P	R	O	F	M	A	T	N	A	U	F	U
Chave	E	N	Q	E	N	Q	E	N	Q	E	N	Q
Texto cifrado	T	E	E	J	Z	Q	X	A	Q	Y	S	K

A primeira letra do texto simples é combinada com a primeira letra da chave. A coluna de texto simples "P" e a linha da chave "E" cruzam a tabela Vigenère em "T", então a primeira letra do texto cifrado é "T".

Da mesma forma, a segunda letra do texto simples é combinada com a segunda letra da chave. A coluna de texto simples "R" e a linha da chave "N" cruzam na na tabela Vigenère de "E", então a segunda letra do texto cifrado é "E".

Esse processo continua até que o texto simples seja concluído.

Texto Cifrado = TEEJZQXAQYSK

DESCRIPTOGRAFIA

A descriptografia é feita pela linha de chaves na tabela Vigenère. Primeiro, selecione a linha da letra-chave, encontre a posição da letra do texto cifrado nessa linha e, em seguida, selecione o rótulo da coluna do texto cifrado correspondente como texto simples.

Texto cifrado	T	E	E	J	Z	Q	X	A	Q	Y	S	K
Chave	E	N	Q	E	N	Q	E	N	Q	E	N	Q

Por exemplo, na linha da chave está "E"e o texto cifrado é "T"e esta letra do texto cifrado aparece na coluna "P", isso significa que a primeira letra do texto simples é "P".

Em seguida, na linha da chave está "N"e o texto cifrado é "E"e esta letra do texto cifrado aparece na coluna "R", isso significa que a segunda letra do texto simples é "R".

Esse processo continua continuamente até que o texto cifrado seja concluído.

Texto simples = PROFMAT NA UFU

Método 2:

Quando a tabela Vigenère não é fornecida, a criptografia e a descriptografia são feitas pela fórmula algébrica de Vigenère neste método (converter as letras (A-Z) em números (0-25)).

Fórmula de criptografia é,

$$Ei \equiv (P_i + K_i)(mod 26).$$

Fórmula de descriptografia é,

$$Di \equiv (E_i - K_i)(mod 26)$$

Se algum valor (D_i) do caso ficar negativo (-ve), neste caso, adicionaremos 26 no valor negativo.

Onde,

E: denota a criptografia.

D: denota a descriptografia.

P: denota o texto simples.

K: denota a chave.

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

O texto simples é "PROFMAT NA UFU"e a chave é "ENQ".

Criptografia: $Ei \equiv (P_i + K_i) mod 26$

Texto simples	P	R	O	F	M	A	T	N	A	U	F	U
Valor do texto simples (P)	15	17	14	05	12	00	19	13	00	20	05	20
Chave	E	N	Q	E	N	Q	E	N	Q	E	N	Q
Valor da chave (K)	04	13	16	04	13	16	04	13	16	04	13	16
Valor do texto cifrado (E)	19	04	04	09	25	16	23	00	16	24	18	10
Texto cifrado	T	E	E	J	Z	Q	X	A	Q	Y	S	K

Descriptografia:

$$Di = (E_i - K_i)(mod 26)$$

Se algum valor (Di) do caso ficar negativo (-ve), neste caso, adicionaremos 26 no valor negativo. Tipo, a terceira letra do texto cifrado; $T = 19$ e $E = 04$

$$\begin{aligned} Di &\equiv (E_i - K_i)(mod 26) \\ Di &\equiv 19 - 04(mod 26) \\ Di &\equiv 15(mod 26) \end{aligned}$$

Então,

Texto cifrado	**T**	**E**	**E**	**J**	**Z**	**Q**	**X**	**A**	**Q**	**Y**	**S**	**K**
Valor do texto cifrado (E)	**19**	**04**	**04**	**09**	**25**	**16**	**23**	**00**	**16**	**24**	**18**	**10**
Chave	**E**	**N**	**Q**	**E**	**N**	**Q**	**E**	**N**	**Q**	**E**	**N**	**Q**
Valor da chave (K)	**04**	**13**	**16**	**04**	**13**	**16**	**04**	**13**	**16**	**04**	**13**	**16**
Valor do texto (P)	**15**	**17**	**14**	**05**	**12**	**00**	**19**	**13**	**00**	**20**	**05**	**20**
Texto Simples	**P**	**R**	**O**	**F**	**M**	**A**	**T**	**N**	**A**	**U**	**F**	**U**

4.1.6 Mesclando quadrados mágicos e o códico Vigenère

Usando o algoritmo de Vigenère, construímos um "quadrado mágico usando o Método da Pirâmide" de ordem 5 que contém 25 diferentes valores, como o conjunto de caracteres consiste em 25 valores (1 a 25) cada carácter estará associado a um valor.

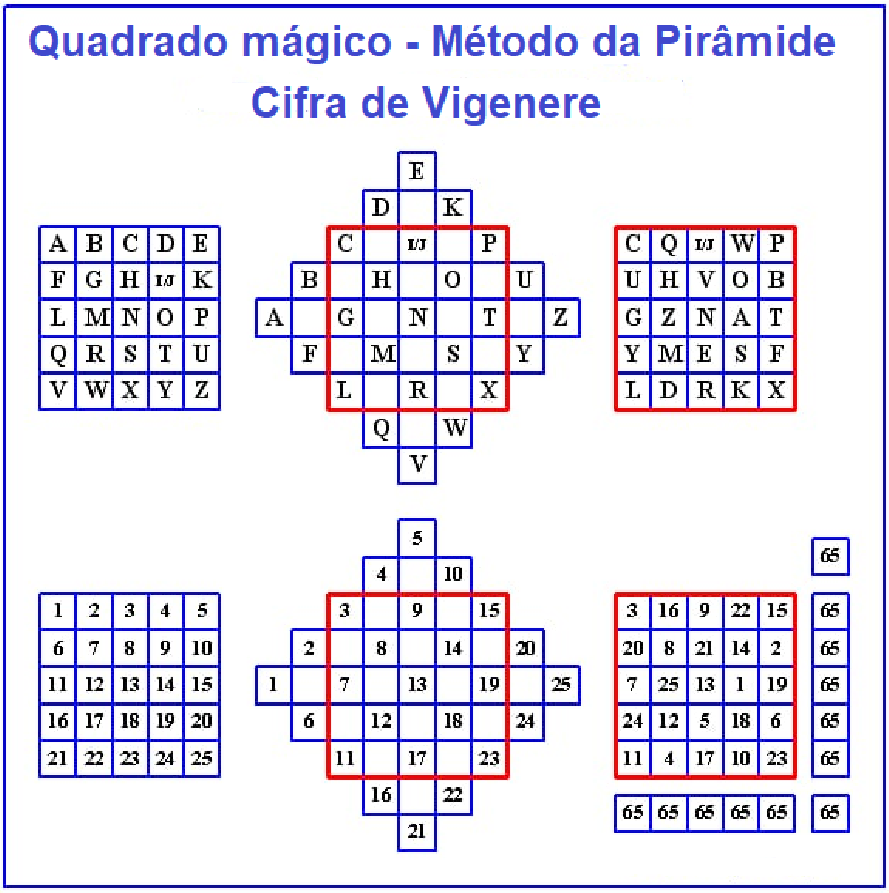


Figura 4.5: Método da Pirâmide

Exemplo 4.1.3.

Usando a Cifra da Pirâmide, **"PROFMAT NA UFU"** pode ser codificado como **"TMAUZCS NC FUF"**. Usando uma ou mais letras de preenchimento, a cifra pode se parecer com "TMAUZCSONCY-FUF" com 'J' e 'Q' como preenchimentos codificados ('O' e 'Y'). Lembre-se de que 'I' também pode ser codificado como 'O'. As letras podem ser substituídas por números para criar uma cifra numérica: **"**$19-12-1-20-25-3-1813-36-20-6$**".** Depois de adicionar os preenchimentos 'J' e 'Q', a cifra ficaria como **"**$19-12-1-20-25-3-18-14-13-3-24-6-20-6$**. "** Sabendo que os números de 1 a 25 representam as letras, uma mensagem cifrada poderia misturar números adicionais até 50 ou 100. A pessoa que fizesse a decodificação removeria todos os números acima de 25, deixando os números cifrados reais: **"**$33-19-12-49-28-1-41-20-26-25-37-29-3-28-48-18$**"** **= "**$19-12-1-20-25-3-18$**" ="PROFMAT"**.

CAPÍTULO 5

ROBÓTICA EDUCACIONAL E OS QUADRADOS MÁGICOS.

A proposta ou ação educativa desse projeto é contribuir com ensino-aprendizagem da matemática, propondo uma experiência (situação-problema), na qual utilizaremos duas ferramentas: o kit lego mindstorms (robótica educacional) e o auxílio dos quadrados mágicos para solução e validação da situação didática concebida. Para melhor compreensão do projeto será criada uma ponte de significados e concepções entre a robótica educacional (fazer) e os quadrados mágicos (pensar ou raciocinar). Assim, no primeiro momento, é desenvolvido predominantemente o raciocínio tecnológico do discente, e no segundo momento, desenvolve-se predominantemente o raciocínio lógico. É importante ressaltar que essas duas ferramentas estão imbricadas entre si e vão contribuir para o desenvolvimento de diversas habilidades e competências intelectuais dos alunos. Por sua vez, a fim de dar uma visão panorâmica, conceituaremos de forma linear essas duas ferramentas. A robótica educacional segundo (d'Abreu e Garcia, 2010)[14] é uma ferramenta tecnológica empregada na área pedagógica, sendo mais um dispositivo que possibilita:

• A aprendizagem colaborativa, o que faz com que todos compartilhem, em sala de aula, os conhecimentos, as competências e as habilidades adquiridas;

• Valorização da aprendizagem significativa, pois os alunos percebem a importância do que estão aprendendo;

• A realização do que foi aprendido em aula, tendo em vista que os alunos constroem protótipos que têm começo, meio e fim;

• A alfabetização quanto a inclusão digital dos alunos, enfatizando, nesse sentido, a responsabilidade social da escola.

5.1 Apresentação do kit robótica lego

A ferramenta utilizada para o desenvolvimento do trabalho é o kit lego mindstorms nxt, próprio para atividade de robótica. O qual permite o desenvolvimento de projetos de pequeno e médio porte, dependendo da quantidade de alunos e materiais, estimulando a criatividade e a solução de problemas. Ele e uma ferramenta tecnológica que proporciona uma aprendizagem das ciências exatas e conceitos técnicos de forma lúdica. O LEGO MINDSTORMS NXT, conforme a Figura 5.1 a seguir, trata-se de um kit com propósito educacional desenvolvido a partir de uma parceria entre a Lego Group com a Universidade Americana MIT (Massachusetts Institute of Technology).

Figura 5.1: LEGO NXT

A Figura 5.2 abaixo mostra o bloco programável do LEGO MINDSTORMS NXT.

Figura 5.2: Brick nxt

O NXT ou brick (bloco, devido ao seu formato) é a peça central do kit, sendo tido como o “cérebro” do robô. Essa parte tem a capacidade de “armazenar a programação para os movimentos do robô, o que torna possível a existência de montagens com motivos elucubrados” (CAMPOS,2011, P.12)[8].

5.2 Procedimentos Metodológicos

5.2.1 Problema da pesquisa.

Considerando-se o que foi fundamentada pelos pensamentos e pelas concepções encontradas nas referências bibliográficas pesquisadas, é proposto o seguinte problema de pesquisa: Construção dos quadrados mágicos e aplicação na criptografia como ferramentas educacionais.

5.2.2 A escolha do tema.

Essa etapa foi realizada durante a elaboração do projeto de pesquisa, quando o professor, durante a ministração de uma aula para OBMEP com tema: Quadrados mágico, percebendo as dificuldades encontradas por parte dos alunos em entender o método de construção do quadrado mágico.

5.2.3 Sujeitos da pesquisa.

O projeto foi desenvolvida com alunos da 1ª série do Ensino Médio, da Escola SESI Dolores Peres Gomes da Silva, na cidade de Ituiutaba, em Minas Gerais. A turma investigada e composta por 20 alunos. As aulas foram ministradas em quatro períodos semanais de 50 minutos cada, sendo dois períodos na terça-feira, um período na quinta-feira e o outro na sexta-feira, no turno da tarde.

As aulas foram divididas em seis momentos:

I) Apresentação da situação problema aos alunos;

II) Desenvolvimento do módulo de apoio para experiência prática;

III) Proposta de programação do robô;

IV) Exposição de cada grupo sobre a montagem realizada;

V) Realização das atividades propostas;

VI) Apresentação dos resultados e discussão.

5.2.4 Compreensão do problema.

Neste experimento, os alunos construíram um equipamento simples “um robô” usando o kit 9797 do lego mindstorms, figura 5.3, que é capaz de resolver quadrados mágicos 3x3, 5x5, 7x7 e 9x9, o manual da montagem do robô segue em anexo, usamos para a confecção do manual o **Lego studio** software que permite criar o passo a passo para montagem do equipamento.

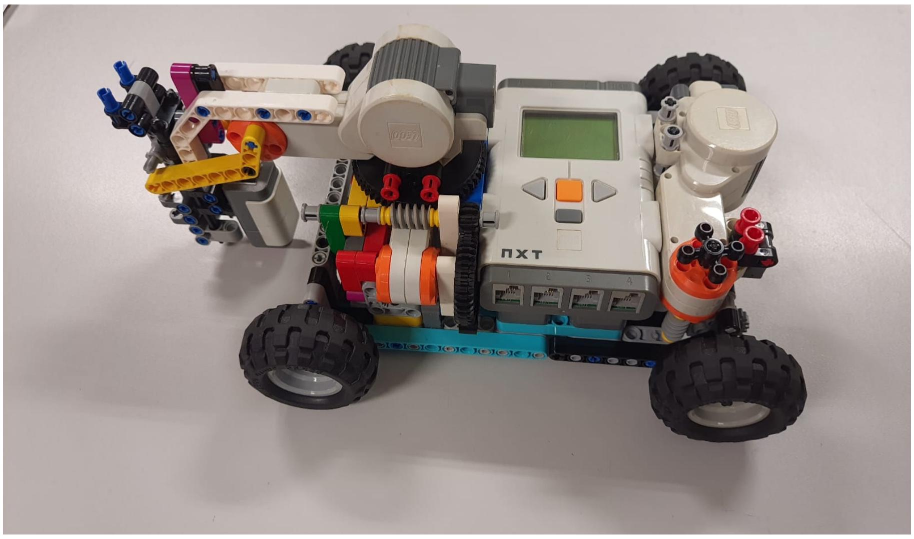


Figura 5.3: ROBÔ MÁGICO

Os alunos fizeram o uso das seguintes linguagens de programação python, C e lego mindstorms(linguagem em bloco), por serem linguagens de fácil entendimento, as linhas de programação foram baseadas no **Método Pirâmide** apresentado no capitulo 3. As programações seguem os mesmos algoritmos:

1º Detectar o tabuleiro: Utilização de sensor de cor para a identificação da posição inicial;
2º Analisar a configuração atual: o robô precisa identificar o tamanho do tabuleiro (quadrado magico) e as posição;
3º Escrever a solução em cada posição: O robô identifica a lacuna e a preenche com valor correto, isto e feito através de uma caneta presa em um braço mecânico do equipamento;
4º Verificar se o quadrado mágico foi formado: Após cada movimento, o robô deve verificar se o quadrado mágico foi alcançado. Isso pode ser feito somando os elementos de cada linha, coluna e diagonal comparando com a soma mágica esperada.
5º Repetir até a solução ser encontrada: O programa deve repetir os passos 3 e 4 até que a solução correta seja encontrada.

O envolvimento dos alunos com o tema como metodologia de ensino para trabalhar as situações-problema propiciou desenvolver os conteúdos estabelecidos pelo programa de forma mais criativa, contextualizada e motivadora para os alunos. O relatório a atividade proposto pelo professor no ponto 5.3 para melhor eficaz na aprendizagem dos alunos, conforme Biembengut (2011)[5] pode ser classificado como técnica, ao elaborar e formular expressões que possam ser válidas não apenas para uma solução particular, mas que também possam servir como estrutura para outras finalidades.

5.2.5 Local da execução do projeto.

A experiência foi vivenciada no laboratório de robótica educacional da escola SESI (figura 5.4),encontramos em tal local o ambiente perfeito para desenvolver a atividade de Robótica Educacional.

Figura 5.4: Laboratório de Robótica escola SESI

5.2.6 Apresentação dos métodos de soluções dos quadrados mágicos para turma.

Lembrando que a turma é do 1°ano do ensino médio, os mesmos já tinha o conhecimento prévio sobre os quadrados mágicos, porém, para um bom andamento das atividades propostas foram novamente abordado com os alunos alguns métodos de solução para os quadrados mágicos aqueles abordados no capitulo 3 deste trabalho,de acordo com Dante(2000)[9],

"*Devemos propor aos estudantes várias estratégias de resolução de problemas, mostrando-lhes que não existe uma única estratégia, ideal e infalível. Cada problema exige uma determinada estratégia. A resolução de problemas não deve se constituir em experiências repetitivas, através da* *aplicação dos mesmos problemas (com outros números) resolvidos pelas mesmas estratégias. O interessante é resolver diferentes problemas com uma mesma estratégia e aplicar diferentes estratégias para resolver um mesmo problema. Isso facilitará a ação futura dos alunos diante de um problema novo*".

A revisão é um momento muito importante, pois propicia uma depuração e uma abstração da solução do problema. A depuração tem por objetivo verificar os procedimentos utilizados, procurando simplificá-los ou, buscar outras maneiras de resolver o problema de forma mais simples. A abstração tem por finalidade refletir sobre o processo realizado procurando descobrir a essência do problema e do método empregado para resolvê-lo, de modo a favorecer uma transposição do aprendizado adquirido neste trabalho para a resolução de outras situações-problema. Abaixo segue uma imagem minha ministrando algumas demonstrações.

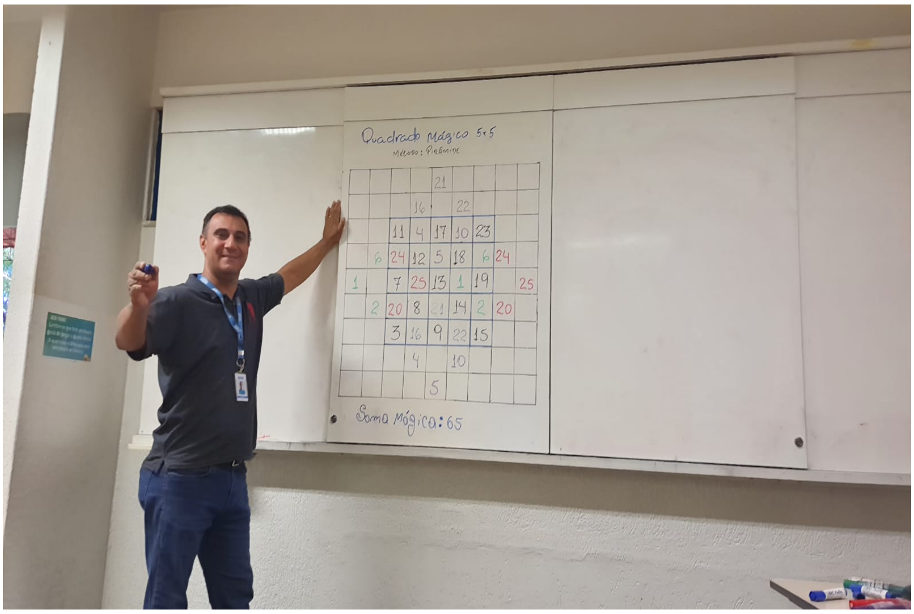


Figura 5.5: Construindo com os alunos quadrado 5x5.

5.3 RESULTADOS E DISCUSSÕES

Como o objetivo geral desta pesquisa era aplicar os quadrados mágicos na contribuição da metodológica na construção de conhecimentos matemáticos e lógicos pelos alunos da 1ª série do Ensino Médio com o tema: Construção dos quadrados mágicos e aplicação na criptografia como ferramentas educacionais, pode-se concluir que esse objetivo foi alcançado de maneira satisfatória. Sabe-se que fazer com que o aluno aprenda é uma tarefa muito difícil, pois, durante a vida escolar o aluno tem lacunas em sua bagagem de conhecimentos e isso dificulta a compreensão de novos conteúdos. Após serem concluídos os trabalhos com os alunos, utilizando-se a Modelagem Matemática, pôde-se constatar que a construção do conhecimento ocorreu de forma efetiva. Após ter encerrado os trabalhos com relatório, ocorreu uma conversa informal, por meio da qual o professor fez uma avaliação com os alunos sobre os trabalhos realizados. Abaixo, são transcritos os depoimentos de alguns alunos.

"*Foi muito bom fazer os trabalhos em grupo, pois alguns sabem mais umas coisas e outros sabem outras. Assim, cada um foi fazendo o que sabia mais, e um ia ajudando o outro. Eu adorei fazer o trabalho.*"

"*Adorei fazer os trabalhos, principalmente a parte prática, onde tivemos que fazer o robô. Assim aprendemos bastante sobre o tema.*"

"*Foi muito legal, nos divertimos bastante. E eu, que morava em Capinópolis e agora vim estudar aqui e morar com a avó, nunca tinha feito um trabalho desse tipo. Conseguimos enxergar na prática o que estudamos na sala de aula.*"

Foi possível constatar, pela fala dos alunos, que quando os conteúdos matemáticos surgem de suas realidades despertam maior interesse e motivação para a aprendizagem. Conforme afirma Caldeira (2004, p. 4)[6], “Grupos de trabalhos se fazem necessários para uma dinâmica mais participativa, onde o aluno passa da passividade das aulas explicativas, onde ele é mero espectador e ’depositário’ de informações, para uma dinâmica integração criativa”.

Logo abaixo segue a proposta de uma atividade final (na qual chamamos de Relatório de Atividades); relatório de atividades(consiste de 5 atividades) realizadas pelos grupos como a atividade desenvolvida com o robô mágico (atividade 5) que foi capaz de resolver um quadrado mágico de 9ª ordem. A montagem do robô passo a passo assim como as imagens da realização das tarefa segue no link: https://drive.google.com/drive/folders/19n2urXtenyD5JC1FKeoEBugTNYjIZMOk?usp=sharing

LEGO education

RELATÓRIO DE ATIVIDADES

SESI

Escola Sesi Dolores Peres Gomes da Silva		
Professor: Eustáquio Morais de Oliveira		
Projeto Desenvolvido: Quadrado Mágico		
Data: 20/06/2023	Equipe: Esparta	Nº do Kit: 9797
Alunos: Elisa Nunes Stefany Ferreira Alaíra Diniz Guilherme Augusto		

O projeto quadrado Mágico, vamos realizar cinco atividades, que fundamentará alguns conceitos matemáticos e por fim construiremos o **robô mágico.**

1ª Atividade

Calcule a soma mágica (constante mágica) dos seguintes quadrados mágicos:

Ordem do quadrado	Soma Mágica (Constante Mágica)
3x3	15
4x4	34
5x5	65
6x6	111
7x7	175

Quadrado $3\times 3 : S(m) : \frac{(3^2+1).3}{2} : \frac{(10).3}{2} : 15$

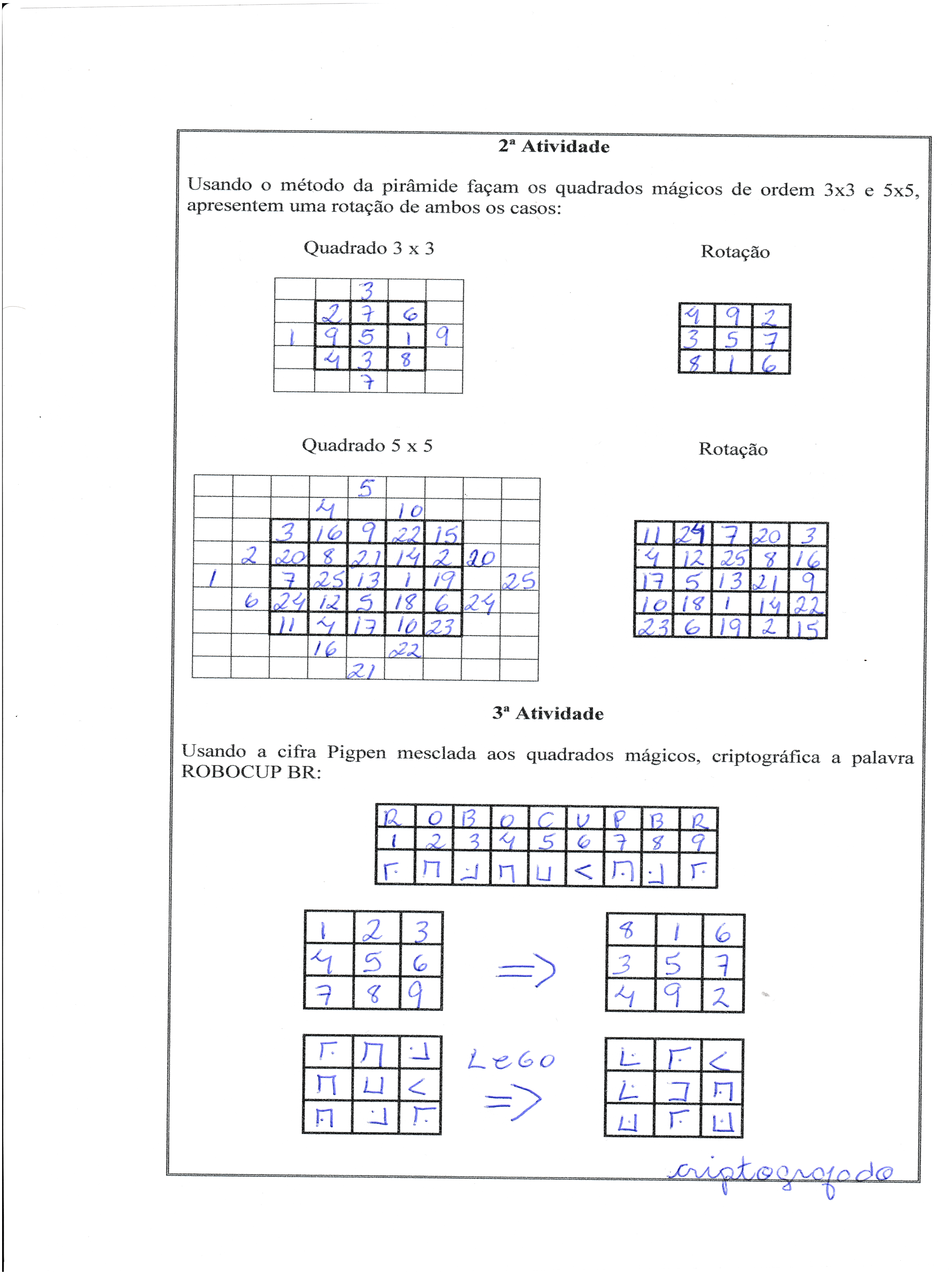
Quadrado $4\times 4 : S(m) : \frac{(4^2+1).4}{2} : \frac{(17).4}{2} : 34$

Quadrado $5\times 5 : S(m) : \frac{(5^2+1).5}{2} : \frac{(26).5}{2} : 65$

Quadrado $6\times 6 : S(m) : \frac{(6^2+1).6}{2} : \frac{(37).6}{2} : 111$

Quadrado $7\times 7 : S(m) : \frac{(7^2+1).7}{2} : \frac{(50).7}{2} : 175$

Figura 5.6: Atividade - página 1



2ª Atividade

Usando o método da pirâmide façam os quadrados mágicos de ordem 3x3 e 5x5, apresentem uma rotação de ambos os casos:

Quadrado 3 x 3

		3		
	2	7	6	
1	9	5	1	9
	4	3	8	
		7		

Rotação

4	9	2
3	5	7
8	1	6

Quadrado 5 x 5

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

Rotação

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

3ª Atividade

Usando a cifra Pigpen mesclada aos quadrados mágicos, criptográfica a palavra ROBOCUP BR:

R	O	B	O	C	U	P	B	R
1	2	3	4	5	6	7	8	9

1	2	3
4	5	6
7	8	9

=>

8	1	6
3	5	7
4	9	2

Lego

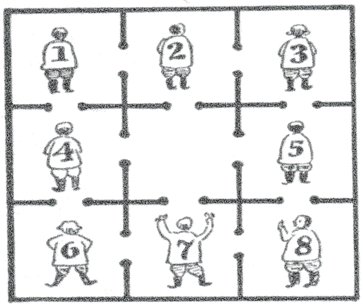
=>

criptografado

Figura 5.7: Atividade - página 2

4ª Atividade

OITO PRISIONEIROS ALEGRES.



A ilustração mostra a planta de uma prisão de nove celas, todas se comunicando entre si por portas. Os oito presos têm seus números nas costas, e qualquer um deles pode se exercitar em qualquer cela que esteja vaga, sujeito à regra de que em nenhum momento dois presos podem estar na mesma cela. O alegre monarca em cujos domínios se situava a prisão ofereceu-lhes especiais confortos numa véspera de Natal se, sem infringir essa regra, pudessem colocar-se de modo que seus números formassem um quadrado mágico.

Ora, o prisioneiro número 7 sabia bastante sobre quadrados mágicos; então elaborou um esquema e naturalmente escolheu o método mais rápido — isto é, um que envolvesse o menor número possível de movimentos de cela para cela. Mas um homem era um sujeito grosseiro e obstinado (totalmente inadequado para a companhia de seus companheiros joviais) e recusou-se a sair de sua cela ou tomar parte nos procedimentos. Mas o nº 7 estava à altura da emergência e descobriu que ainda podia fazer o que era necessário com o menor número de movimentos possíveis, sem incomodar o bruto para sair de sua cela. O quebra-cabeça é mostrar como ele fez isso e, aliás, descobrir qual prisioneiro foi tão estupidamente obstinado. Você pode encontrar o sujeito?

Existem oito maneiras de formar o quadrado mágico - todos meramente aspectos diferentes de um arranjo fundamental. Assim, se você der um quarto de volta ao nosso primeiro quadrado, obterá o segundo quadrado;

Figura 5.8: Atividade - página 3

e como os quatro lados podem, por sua vez, serem levados ao topo, há quatro aspectos. Esses quatro, por sua vez, refletidos em um espelho, produzem os quatro aspectos restantes. Agora, desses oito arranjos, apenas quatro podem ser alcançados sob as condições, e apenas dois desses quatro podem ser alcançados com o menor número de movimentos possíveis, que são dezenove. Esses dois arranjos são mostrados. Mova os homens na seguinte ordem: 5, 3, 2, 5, 7, 6, 4, 1, 5, 7, 6, 4, 1, 6, 4, 8, 3, 2, 7, e você obtém o primeiro quadrado. Mova os assim: 4, 1, 2, 4, 1, 6, 7, 1, 5, 8, 1, 5, 6, 7, 5, 6, 7, 5, 6, 4, 2, 7, e você terá o arranjo no segundo quadrado.
No primeiro caso, todo homem se moveu, mas no segundo caso, o homem de numero 3 nunca saiu de sua cela.
Portanto, o nº 3 deve ser o prisioneiro obstinado e o segundo quadrado deve ser o arranjo necessário.

Figura 5.9: Atividade - página 4

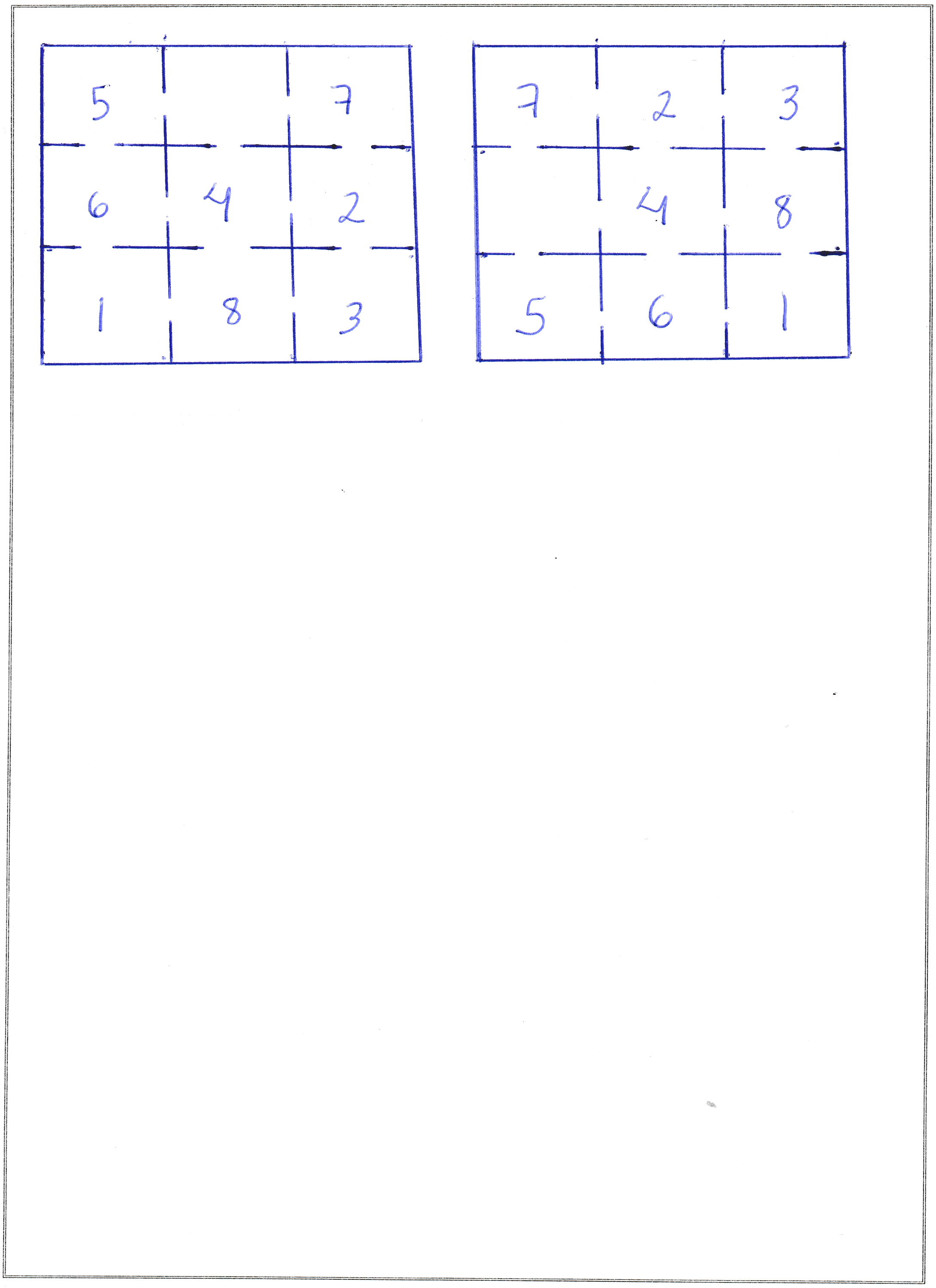
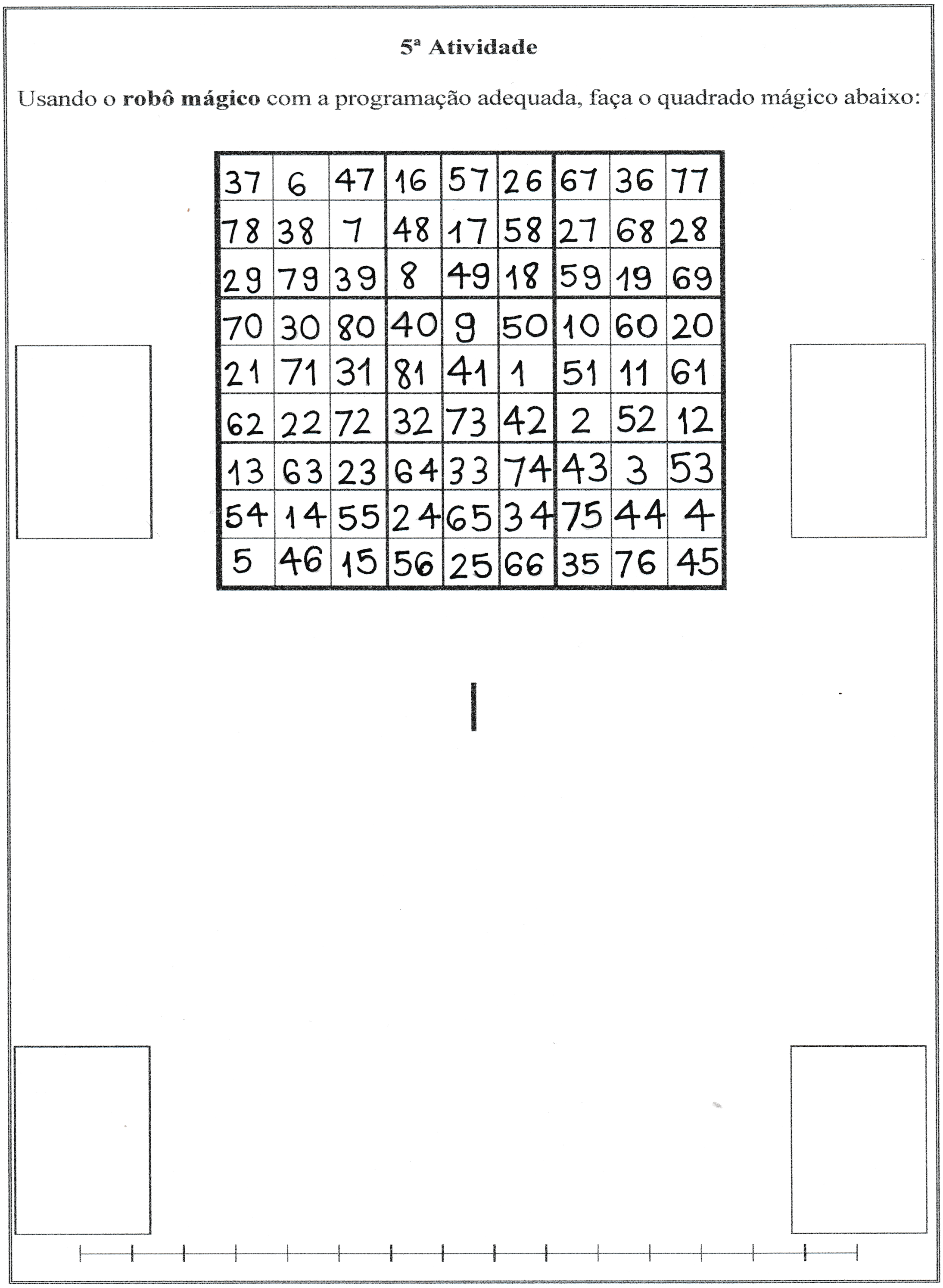


Figura 5.10: Atividade - página 5



5ª Atividade

Usando o **robô mágico** com a programação adequada, faça o quadrado mágico abaixo:

37	6	47	16	57	26	67	36	77
78	38	7	48	17	58	27	68	28
29	79	39	8	49	18	59	19	69
70	30	80	40	9	50	10	60	20
21	71	31	81	41	1	51	11	61
62	22	72	32	73	42	2	52	12
13	63	23	64	33	74	43	3	53
54	14	55	24	65	34	75	44	4
5	46	15	56	25	66	35	76	45

Figura 5.11: Atividade - página 6

Observando a análise das respostas dos alunos, evidencia-se a importância de contextualizar a Matemática. Isso nos mostra que a aprendizagem dos alunos está diretamente ligada à aplicabilidade dos conteúdos. Eles se interessam mais em aprender algo quando conseguem visualizar sua utilidade. Consequentemente, conseguem entender melhor os conceitos matemáticos vinculados.

Após ter encerrado os trabalho com os quadrados mágicos, ocorreu uma conversa informal, por meio da qual o professor fez uma avaliação com os alunos sobre os trabalhos realizados. Ele comentou que ficou muito satisfeito com os resultados, apenas lamentou o pouco tempo para realização das tarefas propostas. Nesse momento, houve espaço para que cada aluno colocasse a sua opinião sobre os trabalhos desenvolvidos.

Abaixo, são transcritos os depoimentos de alguns alunos.

"*Adorei fazer os trabalhos, principalmente a parte prática, onde tivemos que fazer o robô. Assim aprendemos bastante sobre o tema.*"

"*Muito bom, porque estreitou os vínculos com os colegas e o professor, podemos ter uma aprendizagem mais concreta e entender melhor.*"

'Como já disse anteriormente, o trabalho foi bom, devido a vários motivos, um deles foi a melhor compreensão da matéria. Além disso nos divertimos na realização deste trabalho..."

"*Foi bastante criativo, divertido e interessante. Gostei muito e espero que se repita nos próximos anos.*"

Foi possível constatar, pela fala dos alunos, que quando os conteúdos matemáticos surgem de suas realidades despertam maior interesse e motivação para a aprendizagem. Na presente investigação, com os 20 alunos do 1° ano do Ensino Médio, constatou-se que foi possível motivá-los.

Os quadrados mágicos e aplicação da robótica educacional propõe a construção do conhecimento matemático a partir do conhecimento do aluno, não desprezando este conhecimento, mas agregando-o e dando a ele uma forma acadêmica. Assim, como o processo de atingir o conhecimento se faz de forma construtiva, também o é a avaliação, que passa agora a não ser uma prova ou um questionário ou lista, mas sim um conjunto de informações, que vão desde o conhecimento inicial do aluno, sua postura investigativa e questionadora em relação ao fenômeno e aos resultados atingidos, como, é claro, a assimilação do conteúdo inicial que se pretendia trabalhar. Podendo atingir um nível satisfatória por parte do docente e alunos envolvidos no projeto aprendizagem.

5.4 CONCLUSÃO

Esta pesquisa apresentou o uso dos quadrados mágicos como uma poderosa ferramenta de auxílio no ensino de diversas áreas do conhecimento, as demonstrações que tornaram objeto de estudo, faz do aprendizado por parte do aluno mais agradável e estimulante. O objetivo inicial do trabalho foi relacionar a utilização dos quadrados mágicos e a robótica como estratagema de ensino-aprendizagem. Esse vínculo não só é conveniente, como também a utilização das propostas apresentadas pela Modelagem Matemática obedece criteriosamente, às diretrizes estabelecidas pela **didática da matemática**. Além disso, os quadrados como modelagem favorece, dentro de sua estratégia, atingir os propósitos do processo de ensino-aprendizagem de forma satisfatória. Pois compreende-se que empregar Modelagem e a robótica pode ser uma forma de solução para o déficit de aprendizagem que os alunos têm em relação à matemática.

O processo de ensino se caracteriza pela combinação de métodos, conteúdos e formas de organização do processo de ensino-aprendizagem que facilitem a função docente de fazer com que os alunos assimilem os conteúdos, aprimorem e desenvolvam suas capacidades e habilidades no estudo. Chama-se de método de ensino a sequência de ações desenvolvidas pelo professor ao dirigir e estimular o processo de ensino em função da aprendizagem dos alunos, utilizando, intencionalmente, o conjunto de ações, passo, condições externas e procedimentos. Objetivo satisfatoriamente alcançado por ambos os lados, além disso, constatamos que com a robótica é possível estabelecer uma relação diferenciada do conhecimento com a realidade, pois os robôs se mostraram excelentes ferramentas que auxiliam os alunos a compreender os conteúdos trabalhados. Vale destacar que não é a robótica que tem a capacidade de contextualizar determinados conteúdos, mas sim o seu uso de forma apropriada que potencializa o ensino de conceitos educacionais, de forma prática, divertida e contextualizada.

Ao se trabalhar com Robótica Educacional é possível que os alunos desenvolvam algumas competências, que às vezes em uma aula tradicional não seria possível alcançar com a mesma facilidade, tais como a organização, responsabilidade, capacidade de resolver problemas, raciocínio lógico, formulação de conjecturas, exposição de ideias, criatividade, etc. Pode-se concluir que as expectativas quanto à aprendizagem dos alunos foram alcançadas, pois, após a conclusão das atividades e apresentação dos trabalhos, pôde-se perceber que a maioria dos alunos teve suas dificuldades atendidas em relação ao conteúdo estudado. Acredita-se que isso se deva ao fato de que eles próprios tenham realizado as atividades, o que despertou interesse em estudar algo que estava relacionado com lúdico. Considerando esses aspectos, conclui-se que os quadrados mágicos aliada a robótica educacional é uma metodologia eficaz para o ensino de Matemática.

Referências Bibliográficas

[1] AIDEN, Hardeep. “**Anything but square: from magic squares to Sudoku**”. Em: (2006) (citado nas páginas 52, 53).

[2] ANDRADE, Lenimar Nunes de. “**Mais sobre os quadrados mágicos.**” Em: (1999) (citado na página 10).

[3] ANDREWS, William Symes. ***Magic Squares and cubes.*** 1ª ed. Vol. 1. ed. New York:Dover Publications, 1960 (citado nas páginas 9, 18).

[4] ANGEL, B Ann. ***Pigpen Cipher Journal: Write in code the easy way***. 1ª ed. Vol. 1. Independently Published, 2019 (citado na página 63).

[5] BIEMBEMGUT, Maria Salete. ***Modelagem matemática implicações no ensino e na aprendizagem de matemática.*** 1ª ed. Vol. 1. ed.2.Blumenau - Edfurb, 2004 (citado na página 90).

[6] CALDEIRA, Ademir Donizeti. ***Modelagem matemática na formação do professor de matemática: desaos e possibilidades.*** 1ª ed. Vol. 1. ANPED SUL. Anais, 2004 (citado na página 93).

[7] CAMMANN, Schuyler. “**Islamic and Indian Magic Squares**”. Em: (1969). DOI: https://doi.org/10.1086/462584 (citado na página 5).

[8] CAMPOS, Flavio Rodrigues. “**Robótica Pedagógica e Inovação Educacional: Uma Experiênciano Uso de Novas Tecnologias na Sala de Aula**”. Dissertação de Mestrado. Universidade Presbiteriana Mackenzie, São Paulo, 2005 (citado na página 88).

[9] DANTE., Luiz Roberto. ***Didática da resolução de problemas de matemática.*** 12ª ed. Vol. 1. Didática da resolução de problemas de matemática., 2000 (citado na página 91).

[10] EVES, Howard. ***Introdução a história da Matemática***. 5ª ed. Vol. 1. ed. da Unicamp, 2011 (citado na página 5).

[11] HARVEY HEINZ E EVELYN MATHESON STYAN. ***Quadrado mágico Bimágico.*** URL: www.multimagie.com/ (acesso em 08/12/2022) (citado na página 14).

[12] HIGGINS, Peter M. ***Number story : from counting to cryptography.*** 1ª ed. Vol. 1. Ed. Copernicus, Nova Iorque, 2008 (citado na página 33).

[13] HIRE, Philippe de la. ***Construction des quarrés magiques.*** 1ª ed. Vol. 1. Paris: Académie Royale des Sciences (France), 1705 (citado na página 57).

[14] J. V. V Garcia, M. F. d'Abreu. "**Robótica Pedagógica e Currículo**". Em: ***Workshop de Robótica EducacionalT***. SBIA-SBRN-JR. 2010 (citado na página 87).

[15] KLYVE, Dominic e STEMKOSKI, Lee. "**Graeco-Latin Squares and a Mistaken Conjecture of Euler**". Em: (2006). DOI: https://doi.org/10.1080/07468342.2006.11922160 (citado na página 14).

[16] LEHMER, D. N. ***On the congruences connected with certain magic squares.*** 1ª ed. Vol. 1. Transactions of the American Mathematical Society,v. 31, p. 529–551, 1929. DOI: https://doi.org/10.1090/S0002-9947-1929-1501498-X (citado na página 10).

[17] LOLY, Peter. "**The invariance of the moment of inertia of magic squares**". Em: (2004) (citado na página 26).

[18] M., Gardner. ***Magic Squares.*** 1ª ed. Vol. 1. ed. New York:Simon e Schuster, 1961 (citado nas páginas 9, 15).

[19] M., Kraitchik. ***Magic Squares.*** 1ª ed. Vol. 1. ed. New York:Norton, 1942 (citado na página 9).

[20] MEIRIEU, Philippe. **"*Aprender... sim, mas como?*** 1ª ed. Vol. 7. ed. Porto Alegre, 1998 (citado na página 3).

[21] MIGUEL, Antonio e MIORIM, Maria Ângela. ***A História na educação matemática: propostas e desafios.*** 1ª ed. Vol. 1. Belo Horizonte: Autêntica, 2004 (citado na página 3).

[22] MORAN, Jim. ***The wonders of magic of squares.*** 1ª ed. Vol. 1. Editora Vintage Books, 1982 (citado nas páginas 31, 33).

[23] OURMES, Rallier des e JEAN-JOSEPH. ***Mémoire sur les quarrés magiques.*** 1ª ed. Vol. 1. Paris: Académie Royale des Sciences (France), 1763 (citado na página 56).

[24] PENG, Ho. ***Encyclopedia of the History of Science, Technology, and Medicine***. 2ª ed. Vol. 1. Non-Western Cultures, 2008 (citado nas páginas 4, 6).

[25] PERELMÁN, Ya. I. ***Problemas y experimentos recreativos, traduzido para o espanhol de Antônio M. Garcia.*** 2ª ed. Vol. 1. Ed. Mir Moscú, 1983 (citado na página 48).

[26] SALLOWS, L. C. F. **"*Alpha Magic Squares."In The Lighter Side of Mathematics.*** 1ª ed. Vol. 1. Washington, DC: Math. Assoc. Amer., 1994 (citado na página 15).

[27] SANTINHO M. S.and MACHADO, R. M.. ***Os fascinantes Quadrados Mágicos.*** 1ª ed. Vol. 1. Belo Horizonte: Autêntica, 2006 (citado na página 9).

[28] SANTOS, Claudimar Abadio dos e D'AMBROSIO, Ubiratam. "**A história da matemática como ferramenta no processo de ensino-aprendizagem da matemática**". Em: (2007) (citado na página 3).

[29] SESIANO, Jacques. ***Their History and Construction from Ancient Times to AD 1600***. 1ª ed. Vol. 1. Springer, 2019. DOI: https://doi.org/10.1007/978-3-030-17993-9_1 (citado na página 33).

[30] SILVA, Ricardo José da. ***Quadrados Magicos e sequência Numérica***. 1ª ed. Vol. 1. ed. Digital, 2018 (citado nas páginas 11, 13).

[31] SRINIVASAN, P. K. ***Mathematics and magic squares.*** 2ª ed. Vol. 1. The association of mathematics teachers of India., 1992 (citado na página 33).

[32] SWETZ, Frank J. ***Legacy of the Luoshu.*** 2ª ed. Vol. 1. A K Peters, Ltd. Wellesley, Massachusetts, 2008. DOI: https://doi.org/10.1201/b10589 (citado na página 33).

[33] TKOTZ, V. ***Criptografia: segredos embalados para viagem.*** 1ª ed. Vol. 1. São Paulo: Novatec, 2005 (citado na página 81).

[34] TRUMP, Walter. ***Quantos quadrados mágicos existem?*** URL: http://www.trump.de/magic-squares/howmany.html (acesso em 09/01/2023) (citado na página 25).

[35] WALLIS, Faith e WISNOVSKY, Robert. ***Medieval Textual Cultures.*** 6ª ed. Vol. 1. De Gruyter, 2016. DOI: https://doi.org/10.1515/9783110467307-003 (citado na página 54).