

Quadrados mágicos: matrizes fantásticas e onde habitam Parte 1

CAIO HENRIQUE SILVA DE SOUZA*

caiohsouza36@gmail.com

Universidade Federal de São Carlos

Resumo

Neste artigo vamos buscar métodos de construção para quadrados mágicos de algumas ordens baseados em matrizes conhecidas como quadrados latinos e em duas importantes estruturas algébricas. O artigo está dividido em duas partes. Na Parte 1 apresentaremos nosso problema e utilizaremos os grupos para construirmos quadrados mágicos regulares de ordem n ímpar. Para o caso par precisaremos de outra estrutura algébrica, os corpos finitos, que será apresentada na Parte 2, onde ainda será feita uma extensão do conceito de quadrados mágicos para k dimensões.

1. INTRODUÇÃO

UM **quadrado mágico** é uma matriz $n \times n$ em que suas linhas, colunas e diagonais (principal e secundária) somam um mesmo valor S . Para n dá-se o nome de **ordem** do quadrado. Um quadrado mágico é dito **regular** quando é preenchido pelos números de 1 a n^2 , cada um deles admitido uma única vez.

Como dito, é pedido um valor constante de soma nas linhas, colunas e diagonais. A esse valor denominamos **constante mágica**. Em um quadrado mágico regular ela é dada por

$$C_n = \frac{n(n^2 + 1)}{2}$$

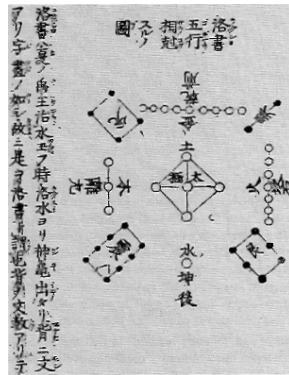
6	1	8
7	5	3
2	9	4

Figura 1: Quadrado mágico de ordem 3.

Na Figura 2 temos o Quadrado Luo Shu, que é um quadrado mágico regular de ordem 3 com constante mágica igual 15. Este quadrado fazia parte da espiritualidade chinesa e tem como

*Agradecimentos ao Prof. Dr. João Nivaldo Tomazella, meu orientador no início da graduação, por apoiar minhas ideias.

primeira aparição impressa no século X de nossa era, mas ele já aparecia talhado em instrumentos astronômicos chineses que datam do Século II A.C.



4	9	2
3	5	7
8	1	6

Figura 2: Quadrado Luo Shu [10].

Os quadrados mágicos foram muito utilizados como amuletos e talismãs, como objetos místicos. Na obra *Practica arithmetice & mensurandi singularis* (1539) de Girolamo Cardano (1501 - 1576) os quadrados mágicos regulares de ordem 3, 4, 5, 6, 7, 8, 9 são associados, respectivamente, aos sete corpos celeste Lua, Mercúrio, Vênus, Sol, Marte, Júpiter e Saturno, seguindo a física de Aristóteles.

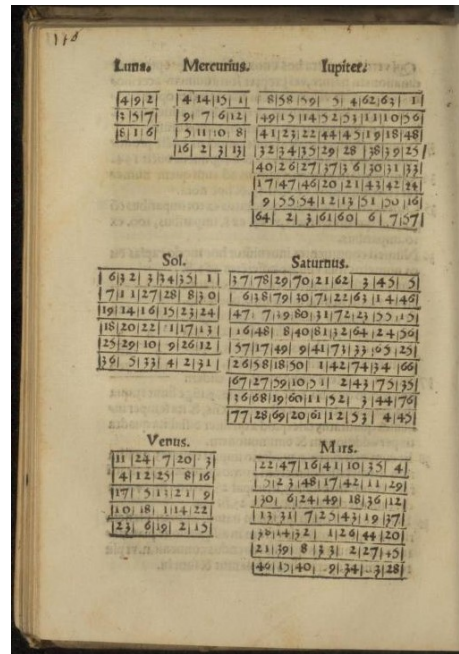


Figura 3: *Practica arithmetice & mensurandi singularis*, Capítulo 42, p.116 [9].

Podemos encontrar também quadrados mágicos na Arte: na obra *Melancolia* (Figura 4) do artista alemão Albrecht Dürer (1471 - 1528) temos um quadrado mágico regular de ordem 4, com constante mágica 34. Um detalhe interessante é que na última linha do quadrado mágico tem-se a

data em que a obra foi concluída, em 1514. O quadrado mágico da obra ficou conhecido como Quadrado de Dürer.

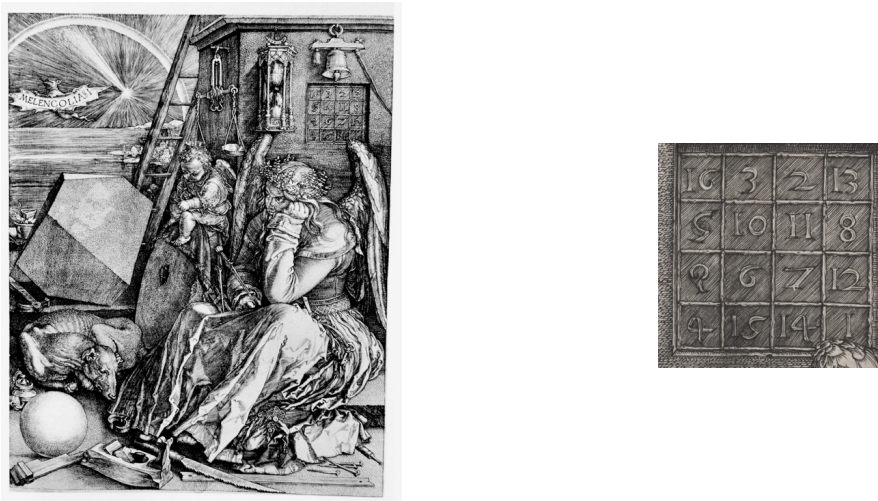


Figura 4: *Melancholia* (1514) de Albrecht Dürer e detalhe do Quadrado de Dürer [5].

E, é claro, os quadrados mágicos podem ser encontrados na Matemática! A partir de agora, sempre que dissermos quadrados mágicos estaremos nos referindo aos quadrados mágicos regulares. Uma primeira pergunta matemática sobre estas matrizes é: será que existem para qualquer $n \geq 2$? De imediato temos a resposta: não. Para $n = 2$ é impossível arranjar os números 1, 2, 3 e 4 de maneira que as somas das linhas, colunas e diagonais sejam sempre iguais a $2(2^2 + 1)/2 = 5$.

Tudo bem, e se excluirmos o caso $n = 2$? Existe um quadrado mágico de ordem n para todo $n \geq 3$? Neste caso, a resposta é afirmativa. Existem alguns métodos para construir quadrados mágicos: por exemplo, o Método LUX (quando $n = 4m + 2$), o Método Siamês (quando n ímpar) e a Troca de diagonais (quando $n = 4m$) que podem ser aprendidos em [1]. Porém pouco é dito sobre o por quê destes algoritmos funcionarem. De certa maneira, aplica-se o algoritmo e de forma “mágica” tem-se a matriz satisfazendo as condições exigidas.

O que faremos no que se segue é buscar algoritmos de construção para quadrados mágicos de algumas ordens de forma que possamos entender cada um dos passos. Para tal, utilizaremos conceitos da Álgebra e uma família de matrizes igualmente curiosas.

2. QUADRADOS MÁGICOS DE ORDEM n ÍMPAR

2.1 Grupos

Na Matemática estamos muitas vezes interessados em entender as estruturas dos nossos objetos de estudo, isto é, quais as propriedades fundamentais destes. Estas estruturas nos ajudam a classificar e a interligar os objetos matemáticos. E uma vez descritas as propriedades de certa estrutura, temos uma grande vantagem: todos os objetos aos quais for possível associar uma determinada estrutura terão, necessariamente, as propriedades desta estrutura.

Vamos trabalhar, em um primeiro momento, com um conjunto e uma função especial e ver que propriedades (i.e. que estrutura) a combinação destes nos fornece. Por exemplo, tomemos o conjunto dos números inteiros \mathbb{Z} . Em \mathbb{Z} temos uma operação de soma $+$, que é uma função que associa dois números inteiros a e b ao número $a + b$, isto é,

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$(a, b) \longmapsto +(a, b) := a + b$$

A operação $+$ é um exemplo do que chamamos **operação binária**. Dizer $+$: $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ é o mesmo que dizer que \mathbb{Z} é fechado na operação $+$. Dessa forma, reformulando a primeira frase do parágrafo anterior, vamos trabalhar, em um primeiro momento, com um conjunto e uma operação binária de tal forma que o conjunto seja fechado na operação e ver que propriedades a combinação destes nos fornece.

A operação binária $+$, no conjunto \mathbb{Z} , possui as seguintes propriedades:

- associatividade: se a, b e c são números inteiros então $(a + b) + c = a + (b + c)$ (ou seja, podemos rearranjar os parênteses sem alterar o valor final da soma);
- elemento neutro: o número 0 tem uma propriedade especial uma vez que $a + 0 = 0 + a = a$ qualquer que seja o número a ;
- inverso (oposto) aditivo: para qualquer número inteiro a , existe o número $b = -a$ que satisfaz $a + (-a) = (-a) + a = 0$.

Portanto, o conjunto \mathbb{Z} com a operação binária $+$ possui uma estrutura descrita pelas propriedades acima.

As propriedades que conseguiremos no conjunto dependem fortemente da operação binária escolhida, por isso a estrutura será descrita a partir do par (*conjunto, operação binária*). No exemplo acima, temos a estrutura $(\mathbb{Z}, +)$.

Vamos ver o que acontece quando trocamos o conjunto \mathbb{Z} por $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ (inteiros não nulos) e a operação $+$ pela operação binária \cdot , que é o conhecido produto de números inteiros. Primeiramente, como o produto de dois números inteiros nos retorna também um número inteiro, de fato \mathbb{Z}^* é fechado na operação \cdot . Temos as seguintes propriedades:

- associatividade: se a, b e c são números inteiros então $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, ou seja, podemos rearranjar os parênteses sem alterar o valor final do produto;
- elemento neutro: o número 1 possui a propriedade especial de que $a \cdot 1 = 1 \cdot a = a$, qualquer que seja o número $a \in \mathbb{Z}^*$.

Porém, (\mathbb{Z}^*, \cdot) não possui a propriedade do inverso valendo para qualquer número, uma vez que se quisermos que para $a \in \mathbb{Z}^*$ exista $b \in \mathbb{Z}^*$ satisfazendo $a \cdot b = b \cdot a = 1$, então precisamos que $b = 1/a$, que é um número inteiro somente se $a = 1$. Dessa forma, a estrutura (\mathbb{Z}^*, \cdot) não possui uma propriedade que a estrutura $(\mathbb{Z}, +)$ possui.

As estruturas que satisfazem as três propriedades que tratamos até agora são classificadas conforme a Definição 2.1:

Definição 2.1. Sejam G um conjunto e uma operação binária $*$: $G \times G \rightarrow G$. O par $(G, *)$ é dito um **grupo** se satisfaz as seguintes propriedades:

- (i) **associatividade**: para todo $a, b, c \in G$ vale que $(a * b) * c = a * (b * c)$;
- (ii) **existência de elemento neutro**: existe $e \in G$ satisfazendo $e * a = a * e = a$, para qualquer que seja $a \in G$;
- (iii) **elemento inverso (oposto)**: para todo $a \in G$ existe $a' \in G$, chamado inverso, tal que $a * a' = a' * a = e$.

■

Quando utilizarmos a notação aditiva para a operação (ou seja, escrevermos $+$ ao invés de $*$), preferiremos dizer oposto ao invés de inverso e utilizaremos a notação $a' = -a$.

Em um grupo qualquer $(G, *)$, o elemento neutro $e \in G$ é único. De fato se e' é outro elemento neutro então $e * e' = e' * e = e'$ (pois e é elemento neutro) e $e * e' = e' * e = e$, (pois e' é suposto elemento neutro), assim $e = e'$. Consequentemente, o inverso a^{-1} de um elemento $a \in G$ também é único. Além disso as equações $a * x = b$ e $y * a = b$ possuem única solução pois, sendo a' inverso de a , temos $a * x = b \Rightarrow a' * a * x = a' * b \Rightarrow x = a' * b$ e análogo para a segunda equação.

Vamos construir um grupo relacionado ao conjunto dos números inteiros e dar uma estrutura a ele a partir de uma operação binária derivada do **algoritmo de divisão de Euclides**, que está enunciado no teorema a seguir, cuja demonstração pode ser encontrada em [4].

Teorema 2.2. Para quaisquer inteiros a e b , com $b \neq 0$, existem únicos inteiros q e r , chamados quociente e resto respectivamente, tais que

$$a = q \cdot b + r$$

com $0 \leq r < |b|$.

■

Exemplo 2.3. Temos $-12 = 5 \cdot (-3) + 3$ ($a = -12, b = 5, q = -3, r = 3$) e $16 = 5 \cdot 3 + 1$ ($a = 16, b = 3, q = 5, r = 1$).

▼

Definiremos uma relação de equivalência em \mathbb{Z} utilizando o algoritmo da divisão de Euclides. Uma **relação de equivalência** é um conceito matemático que, intuitivamente, nos permite relacionar elementos de um conjunto de maneira que possamos generalizar a ideia de igualdade. Mais formalmente, se X é um conjunto não vazio, uma relação \sim em X é de equivalência se for, para todo $x, y, z \in X$, (i) **reflexiva**, i.e., $x \sim x$; (ii) **simétrica**, i.e., se $x \sim y$ então $y \sim x$; (iii) **transitiva**, i.e., se $x \sim y$ e $y \sim z$ então $x \sim z$. O conjunto $\bar{x} = \{y \in X \mid y \sim x\}$ é denominado classe de equivalência de x . Se $x \sim y$ então $\bar{x} = \bar{y}$, donde x e y são chamados representantes da classe. As classes de uma relação de equivalência separam nosso conjunto X em partes disjuntas. Vejamos um exemplo.

Exemplo 2.4. No conjunto \mathbb{Z} dos números inteiros vamos definir a seguinte relação: para $a, b \in \mathbb{Z}$ diremos que $a \sim_3 b$ se, e somente se, a e b deixam o mesmo resto na divisão por 3. Como um inteiro a deixa o mesmo resto na divisão por três que si mesmo, a relação é reflexiva. Também de forma direta vemos que a relação é simétrica e transitiva. Logo \sim_3 é uma relação de equivalência. O algoritmo da divisão de Euclides nos diz que as possibilidades para resto r na divisão por 3 são 0, 1 ou 2. Assim, temos três classes de equivalência distintas nessa relação. Tomando os representantes dessas três classes como sendo 0, 1 ou 2, podemos escrever

$$\bar{0} = \{\dots, -3, 0, 3, 6, \dots\},$$

$$\bar{1} = \{\dots, -2, 1, 4, 7, \dots\},$$

$$\bar{2} = \{\dots, -1, 2, 5, 8, \dots\}.$$

Nessa relação $\bar{0} = \bar{3} = \bar{6} = \bar{-3}$, bem como $\bar{1} = \bar{-2} = \bar{4} = \bar{7}$ e $\bar{2} = \bar{-1} = \bar{5} = \bar{8}$. Denotamos por $\mathbb{Z}_3 := \{\bar{0}, \bar{1}, \bar{2}\}$ o chamado conjunto dos **inteiros módulo 3**

▼

Exemplo 2.5. Vamos definir uma operação binária para o conjunto $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. Definimos a operação $+_3 : \mathbb{Z}_3 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$ de maneira que

$$\bar{a} +_3 \bar{b} := \overline{a + b},$$

isto é, a classe de $a + b$ na relação de equivalência \sim_3 . Por exemplo

$$\bar{0} +_3 \bar{2} = \overline{0 + 2} = \bar{2}$$

e

$$\bar{2} +_3 \bar{2} = \overline{2 + 2} = \bar{4} = \bar{1}$$

pois 4 deixa o mesmo resto que 1 na divisão por 3. Temos uma função bem definida? Para que a resposta seja sim, precisamos que o resultado da operação de $\bar{a} +_3 \bar{b}$ não se altere caso troquemos o representante da classe \bar{a} e da classe \bar{b} . De fato isso ocorre pois se c é outro representante para \bar{a} (ou seja, $\bar{a} = \bar{c}$) e d é outro representante para \bar{b} , então a e c deixam o mesmo resto r_1 , enquanto b e d deixam o mesmo resto r_2 na divisão por 3. Sendo $a = q_a \cdot 3 + r_1$, $c = q_c \cdot 3 + r_1$, $b = q_b \cdot 3 + r_2$ e $d = q_d \cdot 3 + r_2$, temos

$$\bar{a} +_3 \bar{b} := \overline{a + b} = \overline{q_a \cdot 3 + r_1 + q_b \cdot 3 + r_2} := \overline{3(q_a + q_b) + r_1 + r_2} = \overline{0 + r_1 + r_2} = \overline{r_1 + r_2}$$

Fazendo esta mesma conta para $\bar{c} +_3 \bar{d}$, obtemos que $\bar{c} +_3 \bar{d} = \overline{r_1 + r_2} = \bar{a} +_3 \bar{b}$, ou seja, a operação está bem definida. Veremos que $(\mathbb{Z}_3, +_3)$ é um grupo. Como o conjunto \mathbb{Z}_3 é finito, podemos descrever a operação $+_3$ através da seguinte tabela:

$+_3$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Figura 5: Tabela de grupo de $(\mathbb{Z}_3, +_3)$.

Com esta tabela podemos verificar as propriedades de grupo diretamente: fazendo as combinações adequadas observamos que vale a associatividade, o $\bar{0}$ é o elemento neutro da operação $+_3$ e todos os elementos possuem oposto. Tal tabela é chamada **tabela de grupo** e determina completamente a operação binária.

▼

Observação 2.6. Também podemos escrever $a \equiv b \pmod{3}$ (lê-se “ a é congruente à b módulo 3”) para dizer $\bar{a} = \bar{b}$ na relação de equivalência \sim_3 .

Observação 2.7. A simetria da tabela de grupo com a relação a diagonal principal é devido a propriedade *comutativa* da operação $+_3$, isto é $\bar{a} +_3 \bar{b} = \bar{b} +_3 \bar{a}$. Grupos cuja operação possui a propriedade comutativa são chamados *grupos abelianos*.

A tabela de grupo de $(\mathbb{Z}_3, +_3)$ possui algumas características que nos serão muito úteis na construção de quadrados mágicos.

2.2 Construindo quadrados mágicos a partir de grupos

Consideremos a matriz $L'_{1,3}$ ilustrada na Figura 6, produzida a partir da tabela de grupo da Figura 5 tomando os representantes 0, 1 e 2 dos conjuntos $\bar{0}$, $\bar{1}$ e $\bar{2}$ respectivamente.

0	1	2
1	2	0
2	0	1

Figura 6: Matriz $L'_{1,3}$.

Cada linha e coluna desta matriz contém os números 0, 1 e 2 sem repetição. Isso na verdade ocorre com toda tabela de grupo, pois se duas entradas de uma linha (ou coluna) referente ao elemento a forem iguais então $x * a = y * a \Rightarrow x * a * a' = y * a * a' \Rightarrow x = y$ (o mesmo para $a * x = a * y$). Matrizes com esta configuração são conhecidas como **quadrados latinos**. A definição geral destas matrizes é a que se segue.

Definição 2.8. Um *quadrado latino de ordem n* é uma matriz $n \times n$ em que cada linha e coluna é uma permutação de n símbolos distintos de maneira que cada símbolo ocorra uma única vez em cada linha e em cada coluna. ■

Pela propriedade de ser quadrado latino, a matriz $L'_{1,3}$ da Figura 6 satisfaz que cada linha e cada coluna tem a soma de seus elementos constante igual a 3, uma propriedade que nos remete aos quadrados mágicos. Mais que isso, a tabela de grupo ainda nos deu que a diagonal principal tem esta mesma soma constante. Nosso objetivo será utilizar os quadrados latinos para construir quadrados mágicos. Porém, a diagonal secundária não satisfaz a mesma propriedade de soma. Notemos que esta está preenchida com todos os elementos iguais a 2. Se quisermos que esta diagonal secundária tenha a mesma soma que as linhas e colunas, então uma possibilidade é que esta esteja preenchida pelo número 1. Será possível encontrar um quadrado latino cuja diagonal secundária tenha a mesma soma que as linhas, colunas e diagonal principal?

Para responder esta pergunta, consideremos a bijeção φ dada por

$$\begin{aligned} 0 &\longmapsto 2 \\ 1 &\longmapsto 0 \\ 2 &\longmapsto 1 \end{aligned}$$

Aplicando-a nos elementos da matriz $L'_{1,3}$, obtemos a matriz $L_{1,3}$ representada na Figura 7 que, graças a injetividade da bijeção, é novamente um quadrado latino.

2	0	1
0	1	2
1	2	0

Figura 7: Matriz $L_{1,3}$.

Portanto respondemos nossa pergunta afirmativamente, pois a diagonal secundária tem todos os elementos iguais a 1 e assim todas as linhas, colunas e diagonais somam o valor 3. Esta será a primeira matriz que utilizaremos na construção do quadrado mágico de ordem 3. Precisaremos ainda de um segundo quadrado latino.

Voltando para o grupo $(\mathbb{Z}_3, +_3)$, vamos descrever também a tabela de subtração da operação $+_3$, isto é, a tabela obtida fazendo-se $a -_3 b := a +_3 (-b) = \overline{a - b}$, para $a, b \in \mathbb{Z}$, considerando $-b$ o oposto com relação à operação $+$. Por exemplo, $\overline{0 -_3 1} := \overline{0 - 1} = \overline{-1} = \overline{2}$, pois -1 e 2 deixam o mesmo resto na divisão por 3. A tabela com todas as subtrações em \mathbb{Z}_3 está exposta na Figura 8.

$-_3$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{2}$
$\overline{2}$	$\overline{2}$	$\overline{1}$	$\overline{0}$

Figura 8: Tabela de subtração de $(\mathbb{Z}_3, +_3)$.

A matriz $L'_{2,3}$ obtida por esta tabela (Figura 9, à esquerda) possui nas linhas, colunas e diagonal secundária soma constante. Porém aqui a diagonal principal está preenchida com o número 0. Precisamos desta diagonal preenchida pelo número 1. Análogo ao que fizemos com a matriz $L'_{1,3}$, aplicando a bijeção ψ (que é a inversa de φ) dada por

$$2 \mapsto 0$$

$$0 \mapsto 1$$

$$1 \mapsto 2$$

obtemos a matriz $L_{2,3}$, que é um quadrado latino e possui soma constante em todas linhas, colunas e diagonais.

As matrizes $L_{1,3}$ e $L_{2,3}$ possuem uma propriedade muito importante quando tratamos de quadrados latinos. Se considerarmos o conjunto dos pares cuja primeira coordenada provém de $L_{1,3}$ e a segunda coordenada provém de $L_{2,3}$, isto é,

$$\{(\alpha_{ij}, \beta_{ij}) \mid 0 \leq i, j \leq 2, \alpha_{ij} \in L_{1,3} \text{ e } \beta_{ij} \in L_{2,3}\}$$

todos os pares deste conjunto são distintos. Ou seja, se $(\alpha_{ij}, \beta_{ij}) = (\alpha_{i'j'}, \beta_{i'j'})$ então $(i, j) = (i', j')$. De fato, se $(\alpha_{ij}, \beta_{ij}) = (\alpha_{i'j'}, \beta_{i'j'})$, então $\alpha_{ij} = \alpha_{i'j'}$ e $\beta_{ij} = \beta_{i'j'}$. Mas $\alpha_{ij} = \varphi(a_{ij})$ e $\alpha_{i'j'} = \varphi(a_{i'j'})$,

0	2	1
1	0	2
2	1	0

1	0	2
2	1	0
0	2	1

Figura 9: Matriz $L'_{2,3}$ e matriz $L_{2,3}$, respectivamente.

com $a_{ij}, a_{i'j'} \in L'_{1,3}$ e, por φ ser bijeção, temos $a_{ij} = a_{i'j'}$. Com isso na tabela de grupo de $(\mathbb{Z}_3, +_3)$ teremos $\bar{a}_{ij} = \bar{i} +_3 \bar{j}$ e $\bar{a}_{i'j'} = \bar{i}' +_3 \bar{j}'$, implicando que $\bar{i} +_3 \bar{j} = \bar{i}' +_3 \bar{j}'$. Analogamente, a partir de $\beta_{ij} = \beta_{i'j'}$ e utilizando a bijeção ψ , obtemos $\bar{i} -_3 \bar{j} = \bar{i}' -_3 \bar{j}'$. Temos então o sistema

$$\begin{cases} \bar{i} +_3 \bar{j} = \bar{i}' +_3 \bar{j}' \\ \bar{i} -_3 \bar{j} = \bar{i}' -_3 \bar{j}' \end{cases}$$

Somando as duas equações obtemos que $\bar{i} +_3 \bar{i} = \bar{i}' +_3 \bar{i}'$ e, como em \mathbb{Z}_3 vale que $\bar{0} + \bar{0} = \bar{0}$, $\bar{1} + \bar{1} = \bar{2}$ e $\bar{2} + \bar{2} = \bar{1}$, a única forma da igualdade ocorrer é se $\bar{i} = \bar{i}' \Rightarrow i = i'$ (pois $0 \leq i, i' \leq 2$). Substituindo agora em uma das equações do sistema vemos que $j = j'$.

Quando dois quadrados latinos possuem a propriedade de que todos os elementos do conjunto de pares mencionado são distintos dizemos que estes quadrados são **ortogonais**. Vamos utilizar a propriedade de ortogonalidade de $L_{1,3}$ e $L_{2,3}$ como base da construção do quadrado mágico de ordem 3.

Tomamos a matriz $L_{2,3}$ e multiplicamos todos as suas entradas por 3, obtendo a matriz $3L_{2,3}$, que possui soma constante de suas linhas, colunas e diagonais igual a 9.

3	0	6
6	3	0
0	6	3

Figura 10: Matriz $3L_{2,3}$.

A matriz $3L_{2,3}$ está preenchida pelos números 0, 3 e 6, múltiplos de 3, e cada um destes aparece exatamente três vezes na matriz. Em seguida vamos somar as matrizes $L_{1,3}$ e $3L_{2,3}$, obtendo M'_3 . Os elementos $m'_{ij} = \alpha_{ij} + 3\beta_{ij}$ de M'_3 , graças a ortogonalidade, varrem todos os número entre 0 e 8.¹ Como as matrizes $L_{1,3}$ e $3L_{2,3}$ possuem soma constante, também M'_3 possui soma constante e esta vale $3 + 9 = 12$.

¹De fato o que estamos fazendo aqui é converter os números $\alpha_{ij}\beta_{ij}$ (ou seja 00, 01, 02, 10, 11, ...) da base 3 para a base 10.

5	0	7
6	4	2
1	8	3

Figura 11: Matriz M'_3 .

Por fim, somando 1 a todas as entradas de M'_3 obtemos um quadrado mágico de ordem 3, cuja constante mágica é 15.

6	1	8
7	5	3
2	9	4

Figura 12: Quadrado mágico de ordem 3.

Podemos generalizar a construção acima para todos os n ímpares através dos passos a seguir:

1. Iniciamos tomando a tabela de grupo de $(\mathbb{Z}_n, +_n)$. O conjunto $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ dos **inteiros módulo n** é descrito segundo o algoritmo de divisão de Euclides e a relação de equivalência \sim_n como fizemos para \mathbb{Z}_3 : $a \sim_n b$ se, e somente se, a e b deixam o mesmo resto na divisão por n e tomamos por representantes das classes de equivalência $\bar{0}$ (representando os inteiros que deixam resto 0 na divisão por n), $\bar{1}$ (representando os inteiros que deixam resto 1 na divisão por n) e assim sucessivamente até $n-1$. A operação $+_n$ é definida de maneira análoga a $+_3$.
2. Tomamos então a tabela $L'_{1,n}$ considerando os representantes fixados $0, 1, \dots, n-1$ de $\bar{0}, \bar{1}, \dots, \overline{n-1}$ respectivamente. Essa tabela, por ser fruto de uma tabela de grupo, é um quadrado latino e, portanto, todas as linhas, colunas e a diagonal principal somam

$$\sum_{k=0}^{n-1} k = \frac{n(n-1)}{2}.$$

Devido a matriz $L'_{1,n}$ vir de uma tabela de grupo, todos os elementos da diagonal secundária são iguais a $n-1$. Como queremos que esta diagonal tenha a soma mencionada anteriormente, precisamos que as n entradas da diagonal secundária (que serão iguais a x) somem esta constante, ou seja,

$$nx = \frac{n(n-1)}{2} \Rightarrow x = \frac{(n-1)}{2}.$$

Como n é ímpar, temos que $(n-1)/2$ é um número inteiro entre 0 e $n-1$.

3. Aplicamos então a bijeção φ dada por

$$\begin{aligned} n-1 &\mapsto \frac{n-1}{2} \\ \frac{n-1}{2} &\mapsto 0 \\ 0 &\mapsto n-1 \\ c &\mapsto c \text{ se } c \notin \left\{0, \frac{n-1}{2}, n-1\right\} \end{aligned}$$

nos elementos de $L'_{1,n}$ obtendo a matriz $L_{1,n}$, onde todas as linhas, colunas e diagonais somam o valor mencionado.

4. Tomamos a tabela de subtração da operação $\bar{a} -_n \bar{b} := \bar{a} +_n (-\bar{b}) = \overline{a-b}$, onde $\overline{a-b}$ é a classe de $a-b$ na relação \sim_n . Obtemos dessa forma outro quadrado latino $L'_{2,n}$. Através da bijeção ψ (inversa de φ)

$$\begin{aligned} \frac{n-1}{2} &\mapsto n-1 \\ 0 &\mapsto \frac{n-1}{2} \\ n-1 &\mapsto 0 \\ c &\mapsto c \text{ se } c \notin \left\{0, \frac{n-1}{2}, n-1\right\} \end{aligned}$$

obtemos $L_{2,n}$.

5. Pelo mesmo argumento envolvendo os índices, as matrizes $L_{1,n}$ e $L_{2,n}$ são quadrados latinos ortogonais.

6. Multiplicamos os elementos da matriz $L_{2,n}$ por n . Dessa forma, a matriz $nL_{2,n}$ possui soma constante

$$\frac{n^2(n-1)}{2}$$

7. Somamos as matrizes $L_{1,n}$ e $nL_{2,n}$. Pela ortogonalidade, todos os números entre 0 e n^2-1 estão em $M'_n = L_{1,n} + nL_{2,n}$. Em M'_n todas as linhas, colunas e diagonais somam

$$\frac{n(n-1)}{2} + \frac{n^2(n-1)}{2} = \frac{n(n-1)}{2} \cdot (n+1) = \frac{n(n^2-1)}{2}.$$

8. Somando 1 a todas as entradas da matriz M'_n obtemos M_n um quadrado mágico de ordem n ímpar. Como somamos 1 a todas as entradas, adicionamos dessa forma n na soma das linhas, colunas e diagonais. Assim a constante mágica vale

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

Por exemplo, temos na Figura 13 os dois quadrados latinos ortogonais de ordem 5 utilizados na construção do quadrado mágico de ordem 5 da Figura 14.

4	1	0	3	2
1	0	3	2	4
0	3	2	4	1
3	2	4	1	0
2	4	1	0	3

2	0	3	4	1
1	2	0	3	4
4	1	2	0	3
3	4	1	2	0
0	3	4	1	2

Figura 13: Quadrados latinos ortogonais de ordem 5 utilizados na construção do quadrado mágico de ordem 5.

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

Figura 14: Quadrado mágico de ordem 5.

Na Seção Apêndice, o Algoritmo 1 é uma implementação utilizando a linguagem de programação Python dos passos da construção de um quadrado mágico de ordem n ímpar².

Exemplo 2.9. Testando com $n = 7$ obtemos um quadrado mágico de ordem 7 com constante 175.

Entre com um valor de ímpar de $n:7$
 [[28.0, 2, 38, 29, 47, 20, 11.0],
 [9, 24.0, 1, 40, 34, 46.0, 21],
 [17, 8, 26.0, 6, 39.0, 35, 44],
 [43, 19, 13, 25.0, 7, 37, 31],
 [33, 48, 18.0, 14, 23.0, 3, 36],
 [41, 32.0, 49, 16, 10, 22.0, 5],
 [4.0, 42, 30, 45, 15, 12, 27.0]]

▼

Os grupos $(\mathbb{Z}_n, +_n)$ podem ser construídos para qualquer n natural. Por exemplo, na Figura 15 temos a matriz $L'_{1,4}$ extraída da tabela de grupo de $(\mathbb{Z}_4, +_4)$. Esta matriz é um quadrado latino (pois toda tabela de grupo o é). No entanto $L'_{1,4}$ tem na sua diagonal principal números repetidos. Ainda, quanto a diagonal secundária, não é possível aplicar a bijeção do Passo 3 se n é par pois, nessa situação, $n - 1$ é ímpar logo $(n - 1)/2$ não é inteiro.

²O código foi implementado por Gabriel Longatto Clemente, meu fiel companheiro de graduação.

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

Figura 15: Matriz $L'_{1,4}$.

Assim a construção para quadrados mágicos apresentada anteriormente é válida somente quando n é ímpar. Mas e quando n for par? Na nossa introdução dissemos que estas matrizes existem para todo $n \geq 3$. Como poderemos então descrever construções para quadrados mágicos de ordem par?

Calma calma, não criemos pânico! Veremos na segunda parte desse artigo como utilizar os grupos juntamente com uma estrutura adicional e os quadrados latinos ortogonais para construir quadrados mágicos de ordem par.

REFERÊNCIAS

- [1] ANDRADE, L. N. de. **Mais sobre quadrados mágicos**. Rio de Janeiro: RPM, v.41. Disponível em: <<http://www.rpm.org.br/cdrpm/41/3.htm>>. Acesso em: 26 ago. 2019.
- [2] BOSE, R. C.; SHRIKHANDE, S. S.; PARKER, E.T. Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture. **Canadian Journal of Mathematics**, Canadá, v. 12, p. 189 - 203, ago. 1959.
- [3] BOSE, R. C.; SHRIKHANDE, S. S. On the Falsity of Euler's Conjecture About the Non-existence of Two Orthogonal Latin Squares of Order $4t + 2$, **Proceedings of the National Academy of Science**, Estados Unidos, v. 45, p. 734 - 737, mar. 1959.
- [4] CAETANO; SAMPAIO. **Introdução à Teoria dos Números**, São Carlos: EdUFSCar, 2008. 109 p.
- [5] COMES, R. **The Transmission of Azarquel's Magic Squares in Latin Europe**. In: WALLIS, F.; WISNOVSKY, R. **Medieval Textual Cultures: Agents of Transmission, Translation and Transformation**. Alemanha: Walter de Gruyter GmbH, 2016. p. 159 - 199.
- [6] EULER, L. Recherches sur une nouvelle espace de quarries magiques. **Verh. Genootsch. der wet. Vlissingen** v.9, p. 85 - 239, 1782.
- [7] FRALEIGH, J. B. **A first course in abstract algebra**. 7. ed. Londres: Pearson, 2002. 590 p.
- [8] HAZZAN, S.; IEZZI, G. **Fundamentos de Matemática elementar: sequências, matrizes, determinantes, sistemas**. 2. ed. São Paulo: Atual, 1977. 228 p. (Fundamentos de Matemática elementar).

- [9] Internet Archive. **Practica arithmetice, et mensurandi singularis / [Girolamo Cardano]**. Disponível em: <<https://archive.org/details/hin-wel-all-00000134-001>>. Acesso em: 26 ago. 2019.
- [10] LEE, E.; LEUNG, D. K. S.; LI, K. L.; SO, A. T. P. Luo Shu: Ancient Chinese Magic Square on Linear Algebra, **SAGE Open**, v. 5 p. 1 - 12, 2015.
- [11] MACNEISH, H. F. Euler Squares, **Annals of Mathematics**, v. 23, p. 221 - 227, 1922.
- [12] PETROVIC, M. S. **Famous puzzles of great mathematicians**. Providence: AMS, 2009. 325 p.
- [13] PARKER, T. Orthogonal Latin squares, **Proc. of the National Academy of Sciences**, v.45, p. 859 - 862, 1959.
- [14] STEWART, I. **Galois Theory**. 4. ed. Londres: CRC Press, 2015. 314 p.
- [15] TARRY, G. Le problème des 36 officiers, **C.R. Assoc. France Av. Sci.**, v. 29 parte 2, p. 170 - 203, 1900.
- [16] TRENKLER, M. Magic p-dimensional cubes of order $n \not\equiv 2 \pmod{4}$, **Acta Arith.**, v.92, p. 189 - 194, 2001.
- [17] TRENKLER, M. Magic p-dimensional cubes, **Acta Arith.**, v. 96, p. 361 - 364, 2001.
- [18] TRENKLER, M. An algorithm for Magic Tesseracts, **Scientific Bulletin of Chelm**, p. 249 - 251, 2006.
- [19] Wolfram MathWorld. **Magic Tesseract**. Disponível em: <<http://mathworld.wolfram.com/MagicTesseract.html>>. Acesso em: 26 ago. 2019.

3. APÊNDICE

Algoritmo 1 Dado $n \geq 3$ inteiro ímpar, o algoritmo retorna uma quadrado mágico regular de ordem n .

```
n = int(input("Entre com um valor de impar de n:"))

if (n % 2) == 0:
    print("O valor de n fornecido eh par!")

else:
    Tabela1 = []
    Auxiliar = []
    for i in range(0, n, 1):
        for j in range(0, n, 1):
            Auxiliar = Auxiliar + [0]
            Tabela1 = Tabela1 + [Auxiliar]
            Auxiliar = []

    for i in range(0, n, 1):
        for j in range(0, n, 1):
            Tabela1[i][j] = i + j
            while Tabela1[i][j] - n >= 0:
                Tabela1[i][j] = Tabela1[i][j] - n

    for i in range(0, n, 1):
        for j in range(0, n, 1):
            if Tabela1[i][j] == (n-1)/2 or Tabela1[i][j] == 0 or Tabela1[i][j] == n-1:
                if Tabela1[i][j] == (n - 1)/2:
                    Tabela1[i][j] = 0
                elif Tabela1[i][j] == 0:
                    Tabela1[i][j] = n-1
                else:
                    Tabela1[i][j] = (n-1)/2
            else:
                continue

    Tabela2 = []
    Auxiliar = []
    for i in range(0, n, 1):
        for j in range(0, n, 1):
            Auxiliar = Auxiliar + [0]
```

```
Tabela2 = Tabela2 + [Auxiliar]
Auxiliar = []

for i in range(0, n, 1):
    for j in range(0, n, 1):
        Tabela2[i][j] = i - j
        if Tabela2[i][j] < 0:
            Tabela2[i][j] = Tabela2[i][j] + n
        else:
            continue

for i in range(0, n, 1):
    for j in range(0, n, 1):
        if Tabela2[i][j] ==(n-1)/2 or Tabela2[i][j] ==0 or Tabela2[i][j] ==n-1:
            if Tabela2[i][j] == (n - 1)/2:
                Tabela2[i][j] = n - 1
            elif Tabela2[i][j] == 0:
                Tabela2[i][j] = (n - 1)/2
            else:
                Tabela2[i][j] = 0
        else:
            continue

Matriz = []
Auxiliar = []
    for i in range(0, n, 1):
        for j in range(0, n, 1):
            Auxiliar = Auxiliar + [0]
            Matriz = Matriz + [Auxiliar]
            Auxiliar = []

for i in range(0, n, 1):
    for j in range(0, n, 1):
        Matriz[i][j] = Tabela1[i][j] + n * Tabela2[i][j] + 1
print(Matriz)
```