Quadrados mágicos: matrizes fantásticas e onde habitam Parte 2

Caio Henrique Silva de Souza*
caiohsouza36@gmail.com
Universidade Federal de São Carlos

Resumo

Na Parte 1 deste artigo construímos quadrados mágicos regulares de ordem n ímpar a partir dos grupos $(\mathbb{Z}_n, +_n)$. Na Parte 2 vamos buscar métodos de construção para quadrados mágicos de ordem par a partir de uma outra estrutura algébrica: os corpos finitos. Falaremos por fim de quadrados mágicos em k dimensões.

1. Quadrados Mágicos de ordem $n = 2^s$

1.1 Corpos

Consideremos o conjunto $\mathbb{Z}$ dos números inteiros. Sabemos que $(\mathbb{Z}, +)$ é um grupo com elemento neutro 0. Como $a + b = b + a$ para todos $a, b \in \mathbb{Z}$, temos que a operação soma é comutativa e o grupo $(\mathbb{Z}, +)$ é abeliano. Já a estrutura $(\mathbb{Z}^*, \cdot)$, mesmo sendo uma estrutura com elemento neutro 1, esta não é grupo pois nem todos os elementos possuem um inverso com relação ao produto.

No entanto, as duas estruturas $(\mathbb{Z}, +)$ e $(\mathbb{Z}^*, \cdot)$ podem ser interligadas. As operações binárias soma e produto de $\mathbb{Z}$ conversam através da seguinte propriedade:

- distributividade: se a, b e c são números inteiros então $a \cdot (b + c) = ab + ac$ e $(b + c) \cdot a = ba + ca$.

Vamos voltar ao nosso grupo $(\mathbb{Z}_3, +_3)$ e acrescentar uma segunda operação, procurando alcançar a propriedade distributiva.

Exemplo 1.1. *Definimos um produto $\cdot_3 : \mathbb{Z}_3 \times \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$ de maneira que,*

$$\overline{a} \cdot_3 \overline{b} = \overline{a \cdot b}$$

onde $\overline{a \cdot b}$ é a classe de $a\dot{b}$ na relação de equivalência $\sim_3$. Por exemplo, $\overline{1} \cdot_3 \overline{2} = \overline{2}$ e $\overline{2} \cdot_3 \overline{2} = \overline{2 \cdot 2} = \overline{4} = \overline{1}$. Temos a tabela desta operação binária na Figura 1.

Da mesma maneira que fizemos com a soma $+_3$ é preciso verificar que a operação $\cdot_3$ está bem definida, isto é, o resultado de $\overline{a} \cdot_3 \overline{b}$ não se altera se escolhermos outros representantes para $\overline{a}$ e $\overline{b}$. Essa verificação é

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

$\cdot_3$	$\bar{\mathbf{0}}$	$\bar{\mathbf{1}}$	$\bar{\mathbf{2}}$
$\bar{\mathbf{0}}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{\mathbf{1}}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{\mathbf{2}}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Figura 1: *Tabela da operação* $\cdot_3$.

análoga a que foi feita com a soma $+_3$ *na Parte 1.*

Vejamos que vale a propriedade distributiva: sejam $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_3$. *Utilizando que vale a propriedade distributiva em* $\mathbb{Z}$, *obtemos*

$$\overline{a} \cdot_3 (\overline{b} +_3 \overline{c}) = \overline{a} \cdot_3 (\overline{b+c}) = \overline{a \cdot (b+c)} = \overline{a \cdot b + a \cdot c} = \overline{a \cdot b} +_3 \overline{a \cdot c} = \overline{a} \cdot_3 \overline{b} +_3 \overline{a} \cdot_3 \overline{c}$$

De maneira parecida mostramos que $(\overline{b} +_3 \overline{c}) \cdot_3 \overline{a} = \overline{b} \cdot_3 \overline{a} +_3 \overline{c} \cdot_3 \overline{a}$.

▼

Vemos que essa nova operação em $\mathbb{Z}_3$ não nos fornece um grupo. Porém, se consideramos $\mathbb{Z}_3^* = \{\overline{1}, \overline{2}\}$, vemos que $(\mathbb{Z}_3^*, \cdot_3)$ é um grupo (Figura 2). De fato, a operação $\cdot_3$ em $\mathbb{Z}_3^*$ é associativa, $\overline{1}$ o elemento neutro e, como $\overline{1} \cdot_3 \overline{1} = \overline{1}$ e $\overline{2} \cdot_3 \overline{2} = \overline{1}$, todo elemento possui inverso.

$\cdot_3$	$\bar{\mathbf{1}}$	$\bar{\mathbf{2}}$
$\bar{\mathbf{1}}$	$\bar{1}$	$\bar{2}$
$\bar{\mathbf{2}}$	$\bar{2}$	$\bar{1}$

Figura 2: *Tabela de grupo de* $(\mathbb{Z}_3^*, \cdot_3)$.

A tabela de grupo de $(\mathbb{Z}_3^*, \cdot_3)$ é simétrica com relação a diagonal principal, logo a operação $\cdot_3$ é comutativa. $(\mathbb{Z}_3, +_3, \cdot_3)$ forma uma estrutura que nomearemos na próxima definição.

Definição 1.2. *Sejam* $\mathbb{F}$ *um conjunto,* $+ : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F}$ *e* $\cdot : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F}$ *duas operações binárias chamadas, respectivamente, soma e produto. A tripla* $(\mathbb{F}, +, \cdot)$ *é dita um* ***corpo*** *se*

(i) $(\mathbb{F}, +)$ *é um grupo abeliano, com elemento neutro* 0*;*

(ii) $(\mathbb{F}^*, \cdot)$ *é um grupo abeliano com elemento neutro* 1, *sendo* $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$*;*

(iii) ***distributividade:*** *para todo* $a, b, c \in \mathbb{F}$ *vale* $a \cdot (b + c) = a \cdot b + a \cdot c$ *e* $(b + c) \cdot a = b \cdot a + c \cdot a$.

■

Exemplo 1.3. *Os conjuntos numéricos* $\mathbb{Q}$ *(números racionais),* $\mathbb{R}$ *(números reais) e* $\mathbb{C}$ *(números complexos) juntamente com a soma e produto tradicionais, isto é,* $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ *e* $(\mathbb{C}, +, \cdot)$, *são corpos. No entanto,* $(\mathbb{Z}, +, \cdot)$ *não é um corpo pois, como vimos,* $(\mathbb{Z}^*, \cdot)$ *não é grupo.*

▼

Exemplo 1.4. *Como mostrado acima,* $(\mathbb{Z}_3, +_3, \cdot_3)$ *é um corpo. Veremos agora que se* p *é primo então* $(\mathbb{Z}_p.+_p, \cdot_p)$ *é corpo. Aqui a operação* $\cdot_p$ *é definida de maneira semelhante a operação* $\cdot_3$. *Como já dito na seção anterior,* $(\mathbb{Z}_n, +_n)$ *é grupo abeliano para todo inteiro* $n \geq 0$. *Em particular então* $(\mathbb{Z}_p, +_p)$ *é grupo abeliano para* p *primo. A distributividade que liga as operações* $+_p$ *e* $\cdot_p$ *pode ser verificada como no Exemplo 1.1.*

Precisamos mostrar que $(\mathbb{Z}_p^*, \cdot_p)$ *é grupo abeliano. A associatividade e a comutatividade são decorrentes principalmente do fato de que o produto de números inteiros é associativo e comutativo. O elemento neutro da operação* $\cdot_p$ *é* $\overline{1}$. *Dessa forma, nos concentraremos em mostrar que para todo* $\overline{a} \in \mathbb{Z}_p$ *existe* $\overline{a}'$ *tal que* $\overline{a} \cdot \overline{a}' = \overline{1}$. *Primeiramente veremos que em* $(\mathbb{Z}_p, +_p, \cdot_p)$ *vale a seguinte propriedade:*

- ***integridade:*** $\overline{a} \cdot_p \overline{b} = \overline{0} \Rightarrow \overline{a} = \overline{0}$ *ou* $\overline{b} = \overline{0}$

De fato, suponhamos que $\overline{a} \cdot_p \overline{b} = \overline{0}$. *Assim,* $\overline{a \cdot b} = \overline{0}$, *isto é,* p *divide* ab. *O Lema de Euclides, presente na magnífica obra Os Elementos, Livro VII, Proposição 30, nos diz que se* p *é um primo e* p *divide o produto de dois números inteiros então* p *deve dividir pelo menos um dos fatores. Isto é, se* p *divide* ab *então* p *divide* a *ou* p *divide* b. *Isso significa que* $\overline{a} = \overline{0}$ *ou* $\overline{b} = \overline{0}$ *na relação de equivalência* $\sim_p$. *Logo* $(\mathbb{Z}_p, +_p, \cdot_p)$ *possui a propriedade de integridade.*

Vamos agora mostrar que todo elemento de $\mathbb{Z}_p^*$ *possui inverso com relação a operação* $\cdot_p$. *Seja* $\overline{a} \in \mathbb{Z}_p^*$. *Consideremos a função* $f : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ *dada por* $f(\overline{x}) = \overline{a} \cdot_p \overline{x}$. *Tal função é injetora pois*

$$\overline{a} \cdot_p \overline{x} = \overline{a} \cdot_p \overline{y} \Leftrightarrow \overline{a} \cdot_p \overline{x} +_p (-\overline{a} \cdot_p \overline{y}) = \overline{0} \Leftrightarrow \overline{a} \cdot_p \overline{x} +_p \overline{a} \cdot_p (\overline{-y}) = \overline{0} \Leftrightarrow \overline{a} \cdot_p (\overline{x} +_p (\overline{-y})) = \overline{0}$$

e, como $\mathbb{Z}_p$ *possui a propriedade de integridade e* $\overline{a} \neq \overline{0}$, *então* $\overline{x} - \overline{y} = \overline{0} \Rightarrow \overline{x} = \overline{y}$. *A função* f *é também sobrejetora pois é injetora e* $\mathbb{Z}_p$ *tem um número finito de elementos. Assim* f *é uma bijeção de* $\mathbb{Z}_p$ *em* $\mathbb{Z}_p$. *Pela definição de sobrejetividade, para* $\overline{1} \in \mathbb{Z}_p$ *deve existir* $\overline{a}' \in \mathbb{Z}_p$ *tal que* $f(\overline{a}') = \overline{1}$. *Mas isso significa que existe* $\overline{a}'$ *tal que* $\overline{a}' \cdot_p \overline{a} = \overline{1}$. *Assim qualquer elemento não nulo de* $\mathbb{Z}_p$ *possui inverso com relação a operação* $\cdot_p$. *Concluímos dessa forma que* $(\mathbb{Z}_p^*, \cdot_p)$ *é grupo abeliano e portanto* $(\mathbb{Z}_p, +_p, \cdot_p)$ *é corpo para* p *primo.*

▼

Observação 1.5. *Todo corpo* $(\mathbb{F}, +, \cdot)$ *possui a propriedade de integridade, uma vez que se* $a \cdot b = 0$ *e* $b \neq 0$ *então, tomando o inverso* b' *de* b, *temos* $a \cdot b = 0 \Rightarrow a \cdot b \cdot b' = 0 \cdot b' \Rightarrow a \cdot 1 = 0 \Rightarrow a = 0$.

Exemplo 1.6. *Embora a propriedade de integridade pareça imediata, ela não está presente em todas as estruturas. Por exemplo, se considerarmos* $(\mathbb{Z}_4, +_4, \cdot_4)$ *então* $\overline{2} \cdot_4 \overline{2} = \overline{0}$, *porém* $\overline{2} \neq \overline{0}$, *ou seja,* $(\mathbb{Z}_4, +_4, \cdot_4)$ *não possui a propriedade de integridade. Concluímos também, devido a Observação 1.5, que* $(\mathbb{Z}_4, +_4, \cdot_4)$ *não é corpo.*

▼

Nos corpos temos uma propriedade interessante envolvendo a soma. Em um corpo $(\mathbb{F}, +, \cdot)$ qualquer, o menor número natural k tal que

$$k1 := \overbrace{1 + 1 + \ldots + 1}^{k \text{ vezes}} = 0$$

é chamado **característica** de $\mathbb{F}$ e denotado $char(\mathbb{F})$. Caso não haja tal número natural dizemos que a característica do corpo é 0.

Exemplo 1.7. *Para os corpos numéricos do Exemplo 1.3 como, por exemplo,* $(\mathbb{Q}, +, \cdot)$*, temos* $char(\mathbb{Q}) = 0$*.* ▼

Exemplo 1.8. *Consideremos os corpos finitos* $(\mathbb{Z}_p, +_p, \cdot_p)$*, p primo. Como* $\overbrace{\overline{1} + \overline{1} + \ldots + \overline{1}}^{p \text{ vezes}} = p$*, vemos que* $p\overline{1} = \overline{0}$*. Este é o menor número tal que isso acontece. Logo* $char(\mathbb{Z}_p) = p$*.* ▼

Apresentaremos alguns fatos envolvendo a característica de um corpo, mas (infelizmente) não demonstraremos todos eles. A prova dos fatos abaixo fazem parte uma área da Matemática chamada Teoria de Galois. Uma sugestão de referência para se iniciar nesta área é [14].

- A característica de um corpo $\mathbb{F}$ só pode ser igual a 0 ou a um primo p. Isso pois se supormos que $0 \neq char(\mathbb{F}) = k = mn$, com $1 < m, n < k$, então $m1 \neq 0$ e $n1 \neq 0$ (pois k, sendo a característica, é o menor número que satisfaz isso) porém, com isso, $(m1) \cdot (n1) = (mn)1 = k1 = 0$, o que não pode ocorrer pois um corpo possui a propriedade de integridade;
- se $char(\mathbb{F}) = 0$ então $\mathbb{F}$ possui infinitos elementos. Logo a característica de um corpo finito é sempre um número primo p;
- se $\mathbb{F}$ é um corpo finito de característica p então $\mathbb{F}$ possui p^s elementos, para algum inteiro $s \geq 1$;
- para qualquer primo p e inteiro $s \geq 1$ existe um corpo com p^s elementos. Denotamos tal corpo por $\mathbb{F}_{p^s}$.

Focaremos mais adiante nos corpos finitos pois poderemos exibir suas tabelas de soma e produto e, a partir delas, construir quadrados mágicos. Para encontrar tais tabelas, utilizaremos polinômios.

Seja $\mathbb{F}$ um corpo. Vamos denotar por $\mathbb{F}[x]$ o conjunto de todos os **polinômios** na variável x e coeficientes em $\mathbb{F}$, que são expressões da forma

$$p(x) = \sum_{i=0}^{t} a_i x^i = a_t x^t + \ldots + a_1 x + a_0$$

com $a_i \in \mathbb{F}$, $t \in \mathbb{Z}^{\geq 0}$ e $a_t \neq 0$ se $t \neq 0$. Aos elementos a_i damos o nome de coeficientes. O número inteiro positivo t é dito grau do polinômio e denotado $gr(p(x))$. Um polinômio de grau $t = 0$ é chamado constante.

Exemplo 1.9. *O corpo* $(\mathbb{F}_2, +, \cdot)$ *é formado por dois elementos, ou seja,* $\mathbb{F}_2 = \{0, 1\}$*. Assim,*

$$\mathbb{F}_2[x] = \{0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1,\ x^3,\ x^3+1, \ldots\}$$

▼

É possível somar e multiplicar polinômios. Sendo $p(x) = a_n x^n + \ldots + a_1 x + a_0$ e $q(x) = b_m x^m + \ldots + b_1 x + b_0$ com $n > m$ e considerando $b_k = 0$ para $n \geq k > m$, a soma e produto de polinômios são escritos formalmente como

$$p(x) + q(x) := \sum_{i=0}^{n} (a_i + b_i) x^i \text{ e } p(x) \cdot q(x) := \sum_{i=0}^{n+m} d_i x^i$$

onde $d_i = \sum_{j+h=i} a_j b_h$, com $0 \leq j, h \leq n+m$ ou, equivalentemente, $d_i = \sum_{j=0}^{i} a_j b_{i-j}$. Se o corpo $\mathbb{F}$ possui característica k, então a soma de k vezes o mesmo polinômio resulta no polinômio constante igual a 0.

No conjunto dos inteiros $\mathbb{Z}$ vimos o algoritmo da divisão de Euclides. Esse algoritmo também possui um análogo quando lidamos com polinômios com coeficientes em um corpo. Uma demonstração para o teorema a seguir pode ser vista em [7].

Teorema 1.10. *Para quaisquer polinômios $a(x), b(x) \in \mathbb{F}[x]$ existem únicos polinômios $q(x)$ e $r(x)$ tais que*

$$a(x) = b(x) \cdot q(x) + r(x)$$

onde $r(x) = 0$ ou $gr(r(x)) < gr(b(x))$. ■

Por exemplo, em $\mathbb{F}_2[x]$ temos $x^3 = (x+1) \cdot (x^2 + x + 1) + 1$ ($a(x) = x^3, b(x) = x+1, q(x) = x^2 + x + 1, r(x) = 1$).

Um polinômio não constante $p(x)$ é **redutível** quando $p(x) = f(x) \cdot g(x)$, ambos $f(x)$ e $g(x)$ não constantes. Caso isso não seja possível, $p(x)$ é dito **irredutível**. Decidir se um polinômio qualquer é redutível ou irredutível não é uma tarefa fácil, porém em alguns casos específicos podemos desenvolver algorítimos simples. Por exemplo, o próximo teorema pode ser utilizado para encontrar polinômios irredutíveis de grau 2 ou 3.

O elemento $\alpha \in \mathbb{F}$ será uma **raiz** de $p(x) = a_t x^t + \ldots + a_1 x + a_0 \in \mathbb{F}[x]$ se $p(\alpha) = a_t \alpha^t + \ldots + a_1 \alpha + a_0 = 0$.

Teorema 1.11. *Sejam $\alpha \in \mathbb{F}$ e $p(x) \in \mathbb{F}[x]$. Temos que α é uma raiz de $p(x)$ se, e somente se, $p(x) = (x - \alpha) \cdot q(x)$, com $q(x) \in \mathbb{F}[x]$.*

Demonstração. ($\Rightarrow$) Suponhamos que α seja raiz de $p(x)$. Pelo algoritmo da divisão, existem $q(x), r(x) \in \mathbb{F}[x]$ tais que $p(x) = (x - \alpha) \cdot q(x) + r(x)$, onde $r(x) = 0$ ou $deg(r(x)) < gr(x - \alpha) = 1$. Nessa segunda situação, $r(x)$ é um polinômio constante c. Avaliando em α, temos que

$$0 = p(\alpha) = 0 \cdot q(\alpha) + c \Leftrightarrow c = 0,$$

portanto $p(x) = (x - \alpha) \cdot q(x)$.
($\Leftarrow$) Agora se $p(x) = (x - \alpha) \cdot q(x)$ então basta fazer a avaliação em α para $p(\alpha) = 0$.

■

Exemplo 1.12. *Se um polinômio $p(x) \in \mathbb{F}[x]$ tem grau 3 ou 2, então este será redutível se, e somente se, possuir um fator linear que, conforme o teorema, significa que $p(x)$ possui uma raiz em $\mathbb{F}$. Assim podemos verificar que $x^2 + x + 1, x^3 + x + 1$ e $x^3 + x^2 + 1$ são irredutíveis em $\mathbb{F}_2[x]$ pois têm grau 2 ou 3 e não possuem raiz em $\mathbb{F}_2$.* ▼

Observação 1.13. *De forma alguma podemos generalizar o critério do exemplo anterior para polinômios de grau maior que* 3*: um contra-exemplo é* $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ *que não possui raiz em* $\mathbb{F}_2$*, mas é produto de dois polinômios não constantes.*

Exemplo 1.14. *Ainda em* $\mathbb{F}_2[x]$*, se um polinômio* $p(x)$ *possui grau* 4 *ou* 5*, para mostrar que este é irredutível é suficiente mostrar que este não possui fatores de grau* 1 *ou* 2*. Para mostrar que* $p(x)$ *não possui fatores lineares, podemos o usar o critério da raiz do Exemplo 1.12. Os polinômios de grau 4 que não possuem raiz em* $\mathbb{F}_2$ *são*

$$x^4 + x^3 + x^2 + x + 1,\ x^4 + x^3 + 1,\ x^4 + x^2 + 1 \text{ e } x^4 + x + 1.$$

Os polinômio de grau 5 *que não possuem raiz são*

$$x^5 + x^4 + x^3 + x^2 + 1,\ x^5 + x^4 + x^3 + x + 1,\ x^5 + x^4 + x^2 + x + 1,$$

$$x^5 + x^3 + x^2 + x + 1,\ x^5 + x^4 + 1,\ x^5 + x^2 + 1 \text{ e } x^5 + x + 1.$$

Indo agora para os fatores de grau 2*, como o único polinômio irredutível de grau 2 em* $\mathbb{F}_2[x]$ *é* $x^2 + x + 1$*, basta fazermos a divisão dos polinômios acima por este. Encontramos dessa forma que os polinômios irredutíveis de grau* 4 *são*

$$x^4 + x^3 + x^2 + x + 1,\ x^4 + x^3 + 1 \text{ e } x^4 + x + 1.$$

Os polinômios irredutíveis de grau 5 *em* $\mathbb{F}_2[x]$ *são*

$$x^5 + x^4 + x^3 + x^2 + 1,\ x^5 + x^4 + x^3 + x + 1,\ x^5 + x^4 + x^2 + x + 1,$$

$$x^5 + x^3 + x^2 + x + 1 \text{ e } x^5 + x^2 + 1.$$

▼

Se para qualquer primo p e inteiro $s \geq 1$ existe um corpo com p^s elementos, vamos buscar as tabelas de soma e produto do corpo com 4 elementos $\mathbb{F}_{2^2} = \mathbb{F}_4$, que utilizaremos para construir um quadrado mágico de ordem $n = 4$. Para tal, o polinômio $x^2 + x + 1 \in \mathbb{F}_2[x]$ e o algoritmo da divisão serão nossos aliados.

Exemplo 1.15. *Na divisão por* $p(x) = x^2 + x + 1$ *temos como possíveis restos* $0, 1, x$ *e* $x + 1$*. Tomando a relação* $\sim_{p(x)}$ *dada por* $a(x) \sim_{p(x)} b(x)$ *se, e somente se,* $a(x)$ *e* $b(x)$ *deixam o mesmo resto na divisão por* $p(x)$*, esta relação é de equivalência. As classes são*

$$\overline{0} = \{q(x) \cdot (x^2 + x + 1) \,|\, q(x) \in \mathbb{F}_2[x]\}^1$$

$$\overline{1} = \{q(x) \cdot (x^2 + x + 1) + 1 \,|\, q(x) \in \mathbb{F}_2[x]\}$$

$$\overline{x} = \{q(x) \cdot (x^2 + x + 1) + x \,|\, q(x) \in \mathbb{F}_2[x]\}$$

$$\overline{x+1} = \{q(x) \cdot (x^2 + x + \overline{1}) + (x + 1) \,|\, q(x) \in \mathbb{F}_2[x]\}.$$

Todo polinômio de $\mathbb{F}_2[x]$ *deve pertencer a um e apenas um destes conjuntos. Definido então a soma* $+_{p(x)}$ *e o produto* $\cdot_{p(x)}$ *como feito em* $\mathbb{Z}_3$*, via operação com classes, obtemos um conjunto e duas operações. Por exemplo,* $\overline{x} +_{p(x)} \overline{x+1} = \overline{1}$ *pois* $x + (x + 1) = (x + x) + 1 = 1$ *em* $\mathbb{F}_2[x]$ *(lembre-se da característica* 2 *de*

[1] não confundir com o elemento neutro da soma de $\mathbb{Z}_2$ (em relação aos elementos destes conjuntos), embora o príncipio de criação destes seja o mesmo (e isso é o que deve ser levado em conta). Utilizaremos a mesma notação para evitar que a mesma fique muito carregada.

$\mathbb{F}_2$*) e* $\overline{x} \cdot_{p(x)} \overline{x} = \overline{x+1}$ *pois* $x^2 = 1 \cdot (x^2 + x + 1) + (x + 1)$.

Afirmamos que $\{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$ *com estas duas operações formam o procurado corpo com quatro elementos* $\mathbb{F}_4$*. As tabelas das operações estão descritas na Figura 3 A associatividade, a distributividade e a comutatividade são decorrentes do fato de as operações com polinômios já terem estas propriedades. Como* $p(x) = x^2 + x + 1$ *é irredutível, o produto de dois polinômios não nulos de grau menor do que* 2 *não pode ser igual* $p(x)$*, logo vale a propriedade de integridade e podemos utilizar o mesmo argumento da função que vimos no Exemplo 1.4 para mostrar que os elementos diferentes de* $\overline{0}$ *possuem inverso com relação ao produto.*

$+_{p(x)}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\cdot_{p(x)}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

Figura 3: *Tabela de grupo de* $(\mathbb{F}_4, +_{p(x)})$ *e tabela de grupo de* $(\mathbb{F}_4^*, \cdot_{p(x)})$.

▼

1.2 Construindo quadrados mágicos a partir de corpos finitos

Obteremos duas tabelas a partir da tabela de grupo de $(\mathbb{F}_4, +_{p(x)})$. Novamente, como no caso n ímpar, a tabela de grupo de $(\mathbb{F}_4, +_{p(x)})$ já é um quadrado latino. Porém sua diagonal principal está preenchida pelo mesmo símbolo e o mesmo para a diagonal secundária.
Vamos ajeitar estas diagonais. Considerando a bijeção $\varphi : \mathbb{F}_4 \longrightarrow \mathbb{F}_4$ dada por $\varphi(\overline{a}) = \overline{x} \cdot_{p(x)} \overline{a}$ ou, explicitamente,

$$\begin{aligned} \overline{0} &\longmapsto \overline{0} \\ \overline{1} &\longmapsto \overline{x} \\ \overline{x} &\longmapsto \overline{x+1} \\ \overline{x+1} &\longmapsto \overline{1}, \end{aligned}$$

preenchemos a tabela à esquerda na Figura 4.

$+_{p(x)}$	$\overline{\mathbf{0}}$	$\overline{\mathbf{1}}$	$\overline{x}$	$\overline{x+1}$
$\varphi(\overline{0})$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\varphi(\overline{1})$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\varphi(\overline{x})$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$
$\varphi(\overline{x+1})$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$

$+_{p(x)}$	$\overline{\mathbf{0}}$	$\overline{\mathbf{1}}$	$\overline{x}$	$\overline{x+1}$
$\psi(\overline{0})$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\psi(\overline{1})$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$
$\psi(\overline{x})$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\psi(\overline{x+1})$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$

Figura 4: *Tabela de grupo de* $(\mathbb{F}_4, +_{p(x)})$ *com linhas trocadas pela função* φ *e tabela de grupo de* $(\mathbb{F}_4, +_{p(x)})$ *com linhas trocadas pela função* ψ.

Nesta tabela vemos que a bijeção fez uma troca nas linhas da tabela de grupo e, com isso conseguimos um quadrado latino cujas diagonais são preenchidas por 4 símbolos distintos. Considerando a bijeção $\psi : \mathbb{F}_4 \longrightarrow \mathbb{F}_4$ dada por $\psi(\overline{a}) = (\overline{x+1}) \cdot_{p(x)} \overline{a}$ ou, explicitamente,

$$\begin{aligned} \overline{0} &\longmapsto \overline{0} \\ \overline{1} &\longmapsto \overline{x+1} \\ \overline{x} &\longmapsto \overline{1} \\ \overline{x+1} &\longmapsto \overline{x}. \end{aligned}$$

conseguimos a segunda tabela, exposta na Figura 4.

Substituindo $\overline{0}$ por 0, $\overline{1}$ por 1, $\overline{x}$ por 2 e $\overline{x+1}$ por 3, obtemos dois quadrados latinos $L_{1,4}$ e $L_{2,4}$ (Figura 5). Estes quadrados latinos são ortogonais. De fato, suponhamos que $(\alpha_{ij}, \beta_{ij}) = (\alpha_{i'j'}, \beta_{i'j'})$, com $\alpha_{ij}, \alpha_{i'j'} \in L_{1,4}$ e $\beta_{ij}, \beta_{i'j'} \in L_{2,4}$. Assim, $\alpha_{ij} = \alpha_{i'j'}$ e $\beta_{ij} = \beta_{i'j'}$. Como $\alpha_{ij} = \overline{x} \cdot_{p(x)} \overline{a_1} + \overline{b_1}$ e $\alpha_{i'j'} = \overline{x} \cdot_{p(x)} \overline{a_2} + \overline{b_2}$ (semelhante para β) para alguma combinação de $a_1, a_2, b_1, b_2 \in \mathbb{F}_4$, obtemos o seguinte sistema

$$\begin{cases} \overline{x} \cdot_{p(x)} \overline{a_1} + \overline{b_1} = \overline{x} \cdot_{p(x)} \overline{a_2} + \overline{b_2} \\ (\overline{x+1}) \cdot_{p(x)} \overline{a_1} +_{p(x)} \overline{b_1} = (\overline{x+1}) \cdot_{p(x)} \overline{a_2} +_{p(x)} \overline{b_2} \end{cases}$$

Somando as equações

$$\overline{a_1} \cdot_{p(x)} (\overline{x} +_{p(x)} (\overline{x+1})) = \overline{a_2} \cdot_{p(x)} (\overline{x} +_{p(x)} (\overline{x+1})) \Leftrightarrow$$

$$\overline{a_1} \cdot_{p(x)} \overline{1} = \overline{a_2} \cdot_{p(x)} \overline{1} \Leftrightarrow \overline{a_1} = \overline{a_2}.$$

Em seguida, substituindo na primeira equação obtemos $\overline{b}_1 = \overline{b}_2$. Com isso, $\alpha_{ij} = \alpha_{i'j'}$ e $\beta_{ij} = \beta_{i'j'}$.

Conseguidos os dois quadrados latinos ortogonais, basta agora seguirmos o que fizemos no caso ímpar: multiplicamos os elementos da matriz $L_{2,4}$ por 4, obtendo a matriz $4L_{2,4}$ e então somamos $M_4^{'} = L_{1,4} + 4L_{2,4}$. Somando 1 a todas as entradas de $M_4^{'}$, obtemos um quadrado mágico

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

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

Figura 5: *Matriz $L_{1,4}$ e matriz $L_{2,4}$.*

de ordem $n = 4$ com constante 34.

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

Figura 6: *Quadrado mágico de ordem 4.*

Note que este quadrado mágico é diferente do Quadrado de Dürer. Esta construção pode ser generalizada através dos passos a seguir:

1. Tomamos um polinômio irredutível $p(x)$ de grau s em $\mathbb{F}_p[x]$. Consideramos o corpo $\mathbb{F}_{p^s}$ formados através dos conjuntos definidos pelos restos da divisão por $p(x)$ e a relação de equivalência $\sim_{p(x)}$ e as operações análogas as definidas anteriormente. Por exemplo, para $x^3 + x + 1 \in \mathbb{F}_2[x]$ (irredutível pois é de grau 3 e não possui raízes em $\mathbb{F}_2$) temos

$$\mathbb{F}_8 = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}, \overline{x^2}, \overline{x^2+1}, \overline{x^2+x}, \overline{x^2+x+1}\}.$$

2. Construímos a tabela de grupo para $(\mathbb{F}_{p^s}, +_{p(x)})$ e $(\mathbb{F}^*_{p^s}, \cdot_{p(x)})$.

3. A partir das bijeções $\varphi : \mathbb{F}_{p^s} \longrightarrow \mathbb{F}_{p^s}$ dada por $\varphi(\bar{a}) = \overline{x} \cdot_{p(x)} \bar{a}$ e $\psi : \mathbb{F}_{p^s} \longrightarrow \mathbb{F}_{p^s}$ dada por $\psi(\bar{a}) = \overline{x+1} \cdot_{p(x)} \bar{a}$, fazemos as trocas necessárias nas linhas da tabela de soma para obter dois quadrados latinos ortogonais L_{1,p^s} e L_{2,p^s}.

4. Fazendo uma bijeção entre $\mathbb{F}_{p^s}$ e o conjunto $\{0, 1, 2, \ldots, p^s - 1\}$, trocamos cada elemento das matrizes obtidas através do passo anterior pelo sua imagem por esta bijeção. Por exemplo em $\mathbb{F}_8$ podemos fazer

$$\begin{aligned}
\overline{0} &\longmapsto 0\\
\overline{1} &\longmapsto 1\\
\overline{x} &\longmapsto 2\\
\overline{x+1} &\longmapsto 3\\
\overline{x^2} &\longmapsto 4\\
\overline{x^2+1} &\longmapsto 5\\
\overline{x^2+x} &\longmapsto 6\\
\overline{x^2+x+1} &\longmapsto 7.
\end{aligned}$$

5. Seguimos o que é feito nos Passos 6. , 7. e 8. da construção para n ímpar na Parte 1.

Na Figura 7 temos um quadrado mágico de ordem $n = 8$ construído com este método. Assim temos um método que nos permite construir os quadrados mágicos de ordem $n = 2^s$.

1	10	19	28	37	46	55	65
27	20	9	2	63	56	45	38
53	62	39	48	17	26	3	12
47	40	61	54	11	4	25	18
60	51	42	33	32	23	14	5
34	41	52	59	6	13	24	31
16	7	30	21	44	35	58	49
22	29	8	15	50	57	36	43

Figura 7: *Quadrado mágico de ordem 8.*

2. Quadrados mágicos de ordem $n = 2^s m$

Após encontrarmos um par de quadrados latinos ortogonais e ajeitarmos suas diagonais, podemos dizer que todo o trabalho para se construir um quadrado mágico terminou. Já sabemos construir pares ortogonais de ordem ímpar e de ordem 2^s. O próximo teorema nos diz que é possível então obter pares ortogonais de outras ordens utilizando estes que já conhecemos.

Teorema 2.1. *Se existe um par de quadrados latinos ortogonais de ordem n e se existe um par de quadrados latinos ortogonais de ordem m, então existe um par de quadrados latinos ortogonais de ordem nm.*

Demonstração. Sejam $A^{(1)}$ e $A^{(2)}$ um par de quadrados latinos ortogonais de ordem m e $B^{(1)}$ e $B^{(2)}$ um par de quadrados latinos ortogonais de ordem n. Vamos definir, para cada $e = 1, 2$ as matrizes $(a_{ij}^{(e)}, B^{(e)})$ formada pelos pares $(a_{ij}^{(e)}, b_{hk}^{(e)})$ com $1 \leq h, k \leq n$. Por exemplo, para $A^{(1)}$ e $A^{(2)}$ par

ortogonal de ordem $m = 4$ (Figura 5) e $B^{(1)}$ e $B^{(2)}$ par ortogonal de ordem $n = 3$ temos $(a_{11}^{(1)}, B^{(1)})$ igual a matriz da Figura 8. Seja então $C^{(e)}$ a matriz $mn \times mn$ representada na Figura 9.

$(0,2)$	$(0,0)$	$(0,1)$
$(0,0)$	$(0,1)$	$(0,2)$
$(0,1)$	$(0,2)$	$(0,0)$

Figura 8: *Matriz* $(a_{11}^{(1)}, B^{(1)})$

$(a_{11}^{(e)}, B^{(e)})$	$(a_{12}^{(e)}, B^{(e)})$	$\cdots$	$(a_{1m}^{(e)}, B^{(e)})$
$(a_{21}^{(e)}, B^{(e)})$	$(a_{22}^{(e)}, B^{(e)})$	$\cdots$	$(a_{2m}^{(e)}, B^{(e)})$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
$(a_{m1}^{(e)}, B^{(e)})$	$(a_{m2}^{(e)}, B^{(e)})$	$\cdots$	$(a_{mm}^{(e)}, B^{(e)})$

Figura 9: *Matriz* $C^{(e)}$.

As matrizes $C^{(1)}$ e $C^{(2)}$ formam um par de quadrados latinos de ordem mn. Para vermos que estes são de fato quadrados latinos tome dois elementos em uma mesma linha, $(a_{ij}^{(e)}, b_{hk}^{(e)})$ e $(a_{il}^{(e)}, b_{hw}^{(e)})$. Como $A^{(e)}$ e $B^{(e)}$ são quadrados latinos, então $a_{ij}^{(e)} \neq a_{il}^{(e)}$ e $b_{hk}^{(e)} \neq b_{hw}^{(e)}$, provando que os elementos nas linhas de $C^{(e)}$ são distintos. O mesmo vale para as colunas.

Agora, suponhamos que

$$((a_{ij}^{(1)}, b_{hk}^{(1)}), (a_{ij}^{(2)}, b_{hk}^{(2)})) = ((a_{pq}^{(1)}, b_{st}^{(1)}), (a_{pq}^{(2)}, b_{st}^{(2)}))$$

Assim, pela igualdade destes pares ordenados (compostos por pares ordenados) temos

$$(a_{ij}^{(1)}, a_{ij}^{(2)}) = (a_{pq}^{(1)}, a_{pq}^{(2)})$$

e, pela ortogonalidade de $A^{(1)}$ e $A^{(2)}$, $i = p$ e $j = q$. De forma similar obtemos que $h = s$ e $k = t$, o que mostra que $C^{(1)}$ e $C^{(2)}$ são ortogonais. ■

A demostração do teorema acima nos dá um meio de construir estes pares ortogonais $C^{(1)}$ e $C^{(2)}$. Porém, este método se mostra muito trabalhoso para ser efetuado à mão, visto que por exemplo para $m = 4$ e $n = 3$ são necessárias 16 matrizes 3×3 $(a_{ij}^{(e)}, B^{(e)})$ (ou 9 matrizes 4×4, se trocarmos m e n). Assim, decidimos aproveitar o caráter matricial desta demonstração e, utilizando a linguagem Python, criamos o Algoritmo 2, presente no Apêndice, que executa este processo.

Portanto podemos construir pares de quadrados latinos ortogonais de ordem $2^s m$ onde m é ímpar e $s \geq 2$. Mais que isso, fazendo a associação

$$(a_{ij}^{(e)}, b_{hk}^{(e)}) \leftrightarrow n \cdot a_{ij}^{(e)} + b_{hk}^{(e)}$$

podemos transformar as matrizes $C^{(1)}$ e $C^{(2)}$ em quadrados latinos preenchidos agora pelos números $0, 1, 2, \ldots, mn - 1$. Se escolhermos $A^{(1)}$ e $A^{(2)}$ para serem as matrizes de ordem 2^s, então por estes quadrados latinos já terem, pela nossa construção na seção anterior, suas diagonais preenchidas por elementos distintos, também $C^{(1)}$ e $C^{(2)}$ terão as diagonais preenchidas por elementos distintos. Ou seja, $C^{(1)}$ e $C^{(2)}$ já estão prontas para que possamos usá-las na construção de quadrados mágicos. Continuando a linha de código do Algoritmo 2 com o que foi dito neste parágrafo obtemos o Algoritmo 3 (vide Apêndice) que nos dá um meio de construir quadrados mágicos de ordem $n = 2^s m$, onde m é ímpar e $s \geq 2$.

Exemplo 2.2. *Utilizando o Algoritmo 3 obtemos um quadrado mágico de ordem 12 com constante 870.*

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

▼

3. E os quadrados latinos das demais ordens?

As demais ordens compreendem os números pares n que não se escrevem como $2^s m$, $s \geq 2$ e m ímpar, isto é, os números pares que deixam resto 2 na divisão por 4. Se seguirmos a lógica de construção de quadrados mágicos que adotamos durante todo o texto, precisamos apenas descobrir como encontrar um par de quadrados latinos ortogonais. Essa questão foi discutida por Leonhard Euler (1707 - 1783) no trabalho *Recherches sur une nouvelle espace de quarries magiques*, quando este propôs o chamado Problema dos 36 Oficiais:

Problema dos 36 Oficiais: Arranjar 36 oficiais, 6 de cada um dos 6 regimentos, de 6 diferentes patentes, em um quadrado 6×6 de forma que cada fila e cada coluna contenha um oficial de cada patente e um oficial de cada regimento.

Ou seja, o que Euler estava propondo era encontrar um par de quadrados latinos ortogonais de ordem 6. Euler não conseguiu resolver o Problema dos 36 Oficiais e também não conseguiu provar que o problema era impossível. Ele então fez a seguinte conjectura:

Conjectura de Euler: *Não existem pares de quadrados latinos ortogonais de ordem* $n = 4q + 2$.

O Problema dos 36 Oficiais só foi resolvido em 1901 pelo matemático francês Gaston Tarry (1843 - 1913) que, após listar todos os 812.851.200 quadrados latinos de ordem 6, concluiu que nenhum par era ortogonal, portanto o problema é impossível. A Conjectura de Euler ficou em aberto por mais quase 60 anos até que R. C. Bose (1901 - 1987) e S. S. Shrikhande (1917 -) construíram um par ortogonal de ordem 22 [3] e E. T. Parker (1926 - 1991) encontrou um par de ordem 10 [13], ambos em 1959 e separadamente. No mesmo ano os três se juntaram e provaram que, na verdade, $n = 6$ é o único caso em que a conjectura é válida, isto é, existem pares de quadrados latinos ortogonais para todo $n = 4q + 2 \neq 6$ [2].

Por exemplo, temos o par de quadrados latinos ortogonais de ordem 10 encontrado por Parker na Figura 10.

0	4	1	7	2	9	8	3	6	5
8	1	5	2	7	3	9	4	0	6
9	8	2	6	3	7	4	5	1	0
5	9	8	3	0	4	7	6	2	1
7	6	9	8	4	1	5	0	3	2
6	7	0	9	8	5	2	1	4	3
3	0	7	1	9	8	6	2	5	4
1	2	3	4	5	6	0	7	8	9
2	3	4	5	6	0	1	8	9	7
4	5	6	0	1	2	3	9	7	8

0	7	8	6	9	3	5	4	1	2
6	1	7	8	0	9	4	5	2	3
5	0	2	7	8	1	9	6	3	4
9	6	1	3	7	8	2	0	4	5
3	9	0	2	4	7	8	1	5	6
8	4	9	1	3	5	7	2	6	0
7	8	5	9	2	4	6	3	0	1
4	5	6	0	1	2	3	7	8	9
1	2	3	4	5	6	0	9	7	8
2	3	4	5	6	0	1	8	9	7

Figura 10: *Primeiro par de quadrados latinos ortogonais de ordem 10 exibido por Parker em [13]*

Porém não podemos usar de imediato o par de quadrados latinos de Parker para construir um quadrado mágico de ordem 10 como o da Figura11, pois suas diagonais possuem muitos elementos repetidos e não é evidente uma troca de linhas que mantenha ortogonalidade e arrume as diagonais para a construção.

Assim vemos que nosso método não é suficiente para englobar todas as ordens de quadrados mágicos. Para amenizar este sentimento de incompletude, vamos para nossa última seção onde veremos que os quadrados latinos ainda podem ser úteis para construirmos outras formas mais elaboradas de quadrados mágicos.

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

Figura 11: *Quadrado mágico de ordem* 10 *com constante mágica 505 construído a partir de [17].*

4. Quadrados mágicos em k dimensões

4.1 Matrizes k-dimensionais

Pensemos o que é uma matriz. Seguindo [8], dados dois números naturais não nulos m e n, uma matriz m por n é uma tabela composta por mn números reais dispostos em m linhas e n colunas. Podemos localizar um elemento de uma matriz A sabendo em qual linha e em qual coluna este está, daí a notação utilizada a_{ij}. São necessários então duas informações para identificar um elemento, por isso diremos que uma matriz possui dimensão 2. As matrizes que utilizamos nas discussões da Parte 1 eram todas quadradas ($m = n$), assim podemos também visualizar a dimensão dois destas matrizes como a disposição dos números em um quadrado, uma figura geométrica de dimensão 2.

E se quisermos dispor os números em uma tabela onde são necessárias três informações para identificação dos elementos, ou melhor, dispor os números em um cubo? Poderíamos pensar em algo como na Figura 12.

Identificando um elemento na matriz cúbica como $a(i_1, i_2, i_3)$, apontamos na figura acima algumas posições. Estamos considerando uma matriz cúbica, isto é, todas as "arestas" da matriz cúbica possuem o mesmo número de elementos. No caso retratado na Figura 12 temos 3 elementos em cada aresta, logo as coordenadas variam no intervalo $1 \leq i_j \leq 3$ e diremos que esta matriz cúbica é de ordem $n = 3$.

Mais geralmente, podemos definir matrizes k-dimensionais de ordem n da seguinte maneira:

Definição 4.1. *Sejam $k, n \in \mathbb{Z}^{>0}$. Uma* ***matriz k-dimensional de ordem n*** *é uma tabela composta por n^k números cujas posições são determinadas por $a(i_1, \ldots i_k)$ com $1 \leq i_j \leq n$. Denotamos*

$$A_n^k = [a(i_1, \ldots i_k) \,|\, 1 \leq i_1, \ldots, i_k \leq n] = [a(i_1, \ldots i_k)].$$

■

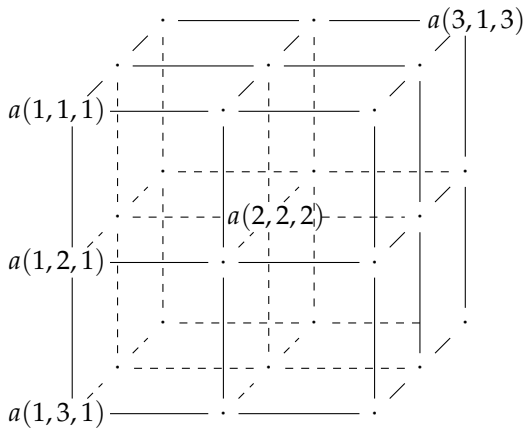

Figura 12: *Matriz 3-dimensional*

Uma linha/coluna em A_n^k é definida pelo conjunto

$$\{a(i_1, \ldots, i_{j-1}, x, i_{j+1}, \ldots, i_k) \,|\, 1 \leq x \leq n\}$$

onde $i_1, \ldots i_{j-1}, i_{j+1}, \ldots, i_k$ são fixadas. Por exemplo, na Figura 12 temos a coluna

$$\{a(1,1,1), a(1,2,1), a(1,3,1)\}.$$

Utilizando-se métodos de contagem, vemos que existem kn^{k-1} linhas/colunas em A_n^k.

Para definirmos uma diagonal em A_n^k vamos primeiro ver exemplos. Na Figura 12, onde $k = n = 3$, temos a diagonal

$$\{a(1,3,1), a(2,2,2), a(3,1,3)\} = \{a(x, i_2, i_3) \,|\, 1 \leq x \leq 3 \text{ e } i_2 = \overline{x}, i_3 = x\} = \{a(x, \overline{x}, x) \,|\, 1 \leq x \leq n\}.$$

onde $\overline{x} = n + 1 - x$. Outro exemplo seria o conjunto

$$\{a(x, i_2, i_3) \,|\, 1 \leq x \leq n \text{ e } i_2 = x, i_3 = \overline{x}\} = \{a(x, x, \overline{x}) \,|\, 1 \leq x \leq 3\}.$$

Assim, escolhemos se i_2 será igual a x ou a $\overline{x}$ e fixamos esta escolha, depois escolhemos se i_3 será igual a x ou a $\overline{x}$ e fixamos esta escolha. Feitas e fixadas as escolhas, basta variar $1 \leq x \leq 3$. Dessa forma uma diagonal em A_n^k é definida pelo conjunto

$$\{a(x, i_2, \ldots, i_k) \,|\, 1 \leq x \leq n \text{ e fixados } i_j = x \text{ ou } i_j = \overline{x} \text{ para cada } 1 \leq j \leq k\}$$

onde $\overline{x} = n + 1 - x$. Quando se escolhe se $i_j = x$ ou $i_j = \overline{x}$, deve-se manter esta escolha fixa em todos os elementos da diagonal, variando apenas o valor de x no intervalo de 1 a n.

Para estas matrizes k-dimensionais fazemos a mesma pergunta que para as matrizes tradicionais: será possível arranjar os números inteiros de 1 até n^k nestes cubos k-dimensionais de ordem n, cada número admitido uma única vez, de forma que todas as linhas, colunas e diagonais somem um mesmo valor? Isto é, existem quadrados mágicos em k dimensões?

4.2 Você disse ... quadrados mágicos em k dimensões?

Como no caso $k = 2$ (os quadrados mágicos regulares), não será possível construir cubos k-dimensionais de ordem $n = 2$ com as propriedades de quadrado mágico. Porém, para qualquer outra ordem $n \geq 3$ e qualquer dimensão $k \geq 2$ existe um quadrado mágico k-dimensional de ordem n. A prova geral foi elaborada por Marián Trenkler (1948 -) no final da década de 90 do século XX e está dividida em três casos: para n ímpar, para n par múltiplo de 4 [16] e para n par não múltiplo de 4 [17], quase como dividimos nossas construções nas seções anteriores. A prova em [17] continha alguns pontos que estavam incorretos e que foram corrigidos pelos autor deste texto e seu orientador Prof. Dr. João Nivaldo Tomazella, que se basearam em [18].

Para fecharmos, vamos apresentar no teorema a seguir a definição de um quadrado mágico k-dimensional de ordem n ímpar, fazendo em seguida alguns comentários sobre a mesma.

Teorema 4.2. *A matriz* $\mathrm{M}_n^k = [m(i_1, \ldots, i_k)]$ *de ordem n ímpar descrita por*

$$m(i_1, \ldots, i_k) = \sum_{l=0}^{k-1} \left[m_l(i_1, \ldots, i_k) n^l \right] + 1$$

onde

$$m_l(i_1, \ldots, i_k) = \left[\sum_{x=1}^{l} (-1)^{x-1} i_x + (-1)^l \sum_{x=l+1}^{k} i_x + C_l \right] (mod\, n) \; e$$

$$C_l = (-1)^{l+1} \left[k - l - (l+1)(mod\, 2) \right] \frac{n+1}{2} - 1$$

é um quadrado mágico k-dimensional de ordem n ímpar

O que os somatórios em $m_l(i_1, \ldots, i_k)$ fazem é relacionar os índices das posições, utilizando a soma em $\mathbb{Z}_n$ $(mod\, n)$ de modo que cada matriz $[m_l(i_1, \ldots, i_k)]$ seja um quadrado latino de dimensão k. Estes têm a propriedade de serem ortogonais entre si. A constante C_l é escolhida de forma que $m_l(\frac{n+1}{2}, \frac{n+1}{2}, \ldots, \frac{n+1}{2}) = \frac{n-1}{2}$ para todo $0 \leq l \leq k-1$, semelhante com o que fizemos nas diagonais do quadrado latino de ordem n ímpar. Assim, o teorema generaliza para matrizes k-dimensionais a construção que fizemos a partir dos grupos.

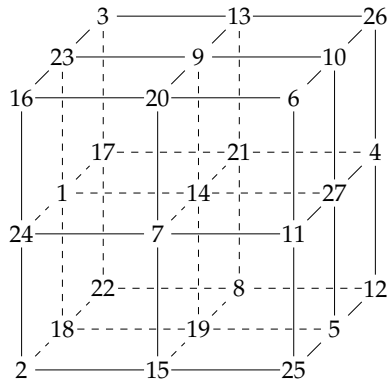

Figura 13: *Quadrado mágico em 3 dimensões de ordem 3 com constante* $C_3^3 = 42$.

Para mostrar que a matriz M_n^k definida desta forma é de fato um quadrado mágico k-dimensional é preciso verificar os seguintes quatro itens:

- Cada elemento de M_n^k pertence a $\left\{1, \ldots, n^k\right\}$;
- Todos os elementos $m(i_1, \ldots, i_k)$ de M_n^k são distintos;
- Todas as linhas/colunas somam o mesmo valor;
- As diagonais somam o mesmo valor das linhas/colunas.

As verificações dos pontos acima são técnicas e longas. Vamos verificar aqui apenas que cada elemento está no conjunto citado e que as linhas/colunas somam o mesmo valor.

Como $m_l(i_1, \ldots, i_k)$ pertence a um quadrado latino k-dimensional então ele é tal que $0 \leq m_l(i_1, \ldots, i_k) \leq n-1$. Multiplicando essa desigualdade por n^l, estritamente positivo, temos que $0 \leq m_l(i_1, \ldots, i_k)n^l \leq (n-1)n^l$. Tomemos agora

$$\sum_{l=0}^{k-1} m_l(i_1, \ldots, i_k)n^l = m_0(i_1, \ldots, i_k) + \ldots + m_{k-1}(i_1, \ldots, i_k)n^{k-1}$$

Como $m_l(i_1, \ldots, i_k)n^l \leq (n-1)n^l$ e por $0 \leq l \leq p-1$, observamos que

$$\begin{aligned}
m_{k-1}(i_1, \ldots, i_k)n^{k-1} &\leq (n-1)n^{k-1} = n^k - n^{k-1} \\
m_{k-2}(i_1, \ldots, i_k)n^{k-2} &\leq (n-1)n^{k-2} = n^{k-1} - n^{k-2} \\
&\vdots \\
m_1(i_1, \ldots, i_k)n &\leq (n-1)n = n^2 - n \\
m_0(i_1, \ldots, i_k)n^0 &\leq (n-1)n^0 = n-1
\end{aligned}$$

Somando membro a membro, vemos um cancelamento de fatores. Portanto

$$0 \leq \sum_{l=0}^{k-1} m_l(i_1, \ldots, i_k)n^l \leq n^k - 1$$

Adicionando 1, fechamos a primeira parte da prova, pois

$\sum_{l=0}^{k-1} \left[m_l(i_1, \ldots, i_k)n^l\right] + 1 = m(i_1, \ldots, i_k)$ e então segue que $1 \leq m(i_1, \ldots, i_k) \leq n^k$.

Agora consideremos o conjunto

$$S_l' = \{m_l(i_1 \ldots, i_{j-1}, i_j, i_{j+1}, \ldots, i_k) : i_j = 1, \ldots, n\} \text{ para } 0 \leq l \leq k-1.$$

Esse conjunto é formado pelos elementos de uma determinada linha/coluna da matriz $[m_l(i_1 \ldots, i_k)]$. Fixando todas as outras coordenadas, variamos i_j e, dessa forma, procuramos os elementos da linha/coluna. Como $m_l(i_1, \ldots, i_k)$ é um número entre 0 e $n-1$ (devido ao $mod\, n$),

o conjunto S'_l equivale, para cada l, a $\{0,1,2,\ldots,n-1\}$.

Portanto

$$\sum_{i_j=1}^{n} m_l(i_1,\ldots,i_k) = \frac{n(n-1)}{2}, \text{ para todo } 1 \leq j \leq k.$$

Temos então que em cada linha e coluna

$$\sum_{i_j=1}^{n} m(i_1,\ldots,i_k) = \sum_{i_j=1}^{n}\left[\sum_{l=0}^{k-1}\left[m_l(i_1,\ldots,i_p)n^l\right]+1\right] =$$

$$\sum_{l=0}^{k-1}\left[\sum_{i_j=1}^{n}\left[m_l(i_1,\ldots,i_k)n^l\right]\right] + \sum_{i_j=1}^{n} 1 = \sum_{l=0}^{k-1}\left[\frac{n(n-1)}{2}\cdot n^l\right] + n.$$

Observemos que esse somatório pode ser separado em partes, isto é,

$$\sum_{l=0}^{k-1}\left[\frac{n(n-1)}{2}\cdot n^l\right] = \frac{n(n-1)(1+n+\cdots+n^{k-1})}{2} = \frac{n(n^k-1)}{2}.$$

Segue por fim que

$$\sum_{l=0}^{k-1}\left[\frac{n(n-1)}{2}\cdot n^l\right] + n = \frac{n(n^k-1)}{2} + n = \frac{n^{k+1}-n-2n}{2} = \frac{n(n^k+1)}{2},$$

que é a fórmula da constante mágica no caso k-dimensional.

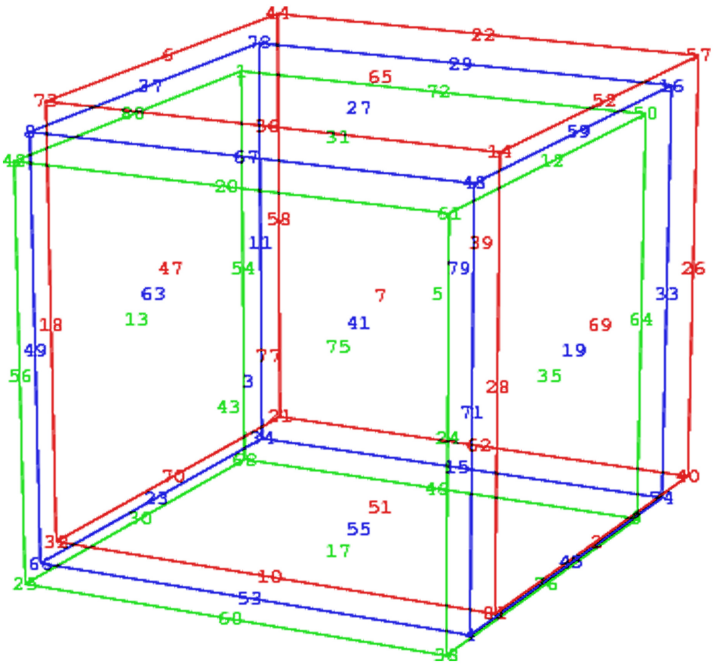

Figura 14: *Quadrado mágico em 4 dimensões de ordem 3 com constante* $C_3^4 = 123$ *[19].*

Concluindo, onde então habitam estas matrizes fantásticas? Onde podemos encontrá-las? Bom, após todas essas páginas, tudo nos leva a crer que estas matrizes fantásticas se encontram em algum lugar entre o misticismo e a Álgebra, entre a Arte e os algoritmos, entre o lúdico e a Teoria dos Números, entre os grupos e os corpos, entre as conjecturas e as impossibilidades, ou até perdidas em outras dimensões!

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 Lain 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 Azarquiel'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. Genoolsch. 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 t he 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 $n \not\equiv 2\,(mod\,4)$, **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.

5. Apêndice

Algoritmo 2 Dado um par de quadrados latinos ortogonais de ordem m e um par de quadrados latinos de ordem n, o algoritmo retorna um par de quadrados latinos ortogonais de ordem mn.

```
# par ortogonal de ordem 4
LA1 = [[0,1,2,3],[2,3,0,1],[3,2,1,0],[1,0,3,2]]
LA2 = [[0,1,2,3],[3,2,1,0],[1,0,3,2],[2,3,0,1]]

# par ortogonal de ordem 3
LB1 = [[2,0,1],[0,1,2],[1,2,0]]
LB2=[[1,0,2],[2,1,0],[0,2,1]]

# par ortogonal de ordem 5
#LB1 = [[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]]
#LB2 = [[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]]

# par ortogonal de ordem 7
#LB1 = [[6,1,2,0,4,5,3],[1,2,0,4,5,3,6],[2,0,4,5,3,6,1],
[0,4,5,3,6,1,2],[4,5,3,6,1,2,0],[5,3,6,1,2,0,4],[3,6,1,2,0,4,5]]
#LB2 = [[3,0,5,4,6,2,1],[1,3,0,5,4,6,2],[2,1,3,0,5,4,6],
[6,2,1,3,0,5,4],[4,6,2,1,3,0,5],[5,4,6,2,1,3,0],[0,5,4,6,2,1,3]]

m = len(LA1)
n = len(LB2)

Auxiliar = [ ]
Auxiliar2 = [ ]
for i in range(0, m, 1):
    for j in range(0, m, 1):
        Auxiliar = Auxiliar + [0]
    Auxiliar2 = Auxiliar2 + [Auxiliar]
    Auxiliar = []

for g in range(0,m,1):
    for h in range(0,m,1):
        A1B1 = []

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

```
            A1B1 = A1B1 + [Auxiliar]
            Auxiliar = []

        for i in range(0,n,1):
            for j in range(0,n,1):
                A1B1[i][j] = [LA1[g][h], LB1[i][j]]
        Auxiliar2[g][h] = A1B1

Auxiliar3 = []
for i in range(0, m, 1):
    for j in range(0, m, 1):
        Auxiliar = Auxiliar + [0]
    Auxiliar3 = Auxiliar3 + [Auxiliar]
    Auxiliar = []

for g in range(0,m,1):
    for h in range(0,m,1):
        A2B2 = []

        for i in range(0, n, 1):
            for j in range(0, n, 1):
                Auxiliar = Auxiliar + [0]
            A2B2 = A2B2 + [Auxiliar]
            Auxiliar = []

        for i in range(0,n,1):
            for j in range(0,n,1):
                A2B2[i][j] = [LA2[g][h], LB2[i][j]]
        Auxiliar3[g][h] = A2B2

C1=[]
for i in range(0, n*m, 1):
    for j in range(0, n*m, 1):
        Auxiliar = Auxiliar + [0]
    C1 = C1 + [Auxiliar]
    Auxiliar = []

for v in range(0,n,1):
    for u in range(0,n,1):
        for i in range(0,m,1):
            for j in range(0,m,1):
```

```
                C1[i+u*m][j+v*m]=Auxiliar2[i][j][u][v]

C2=[]
for i in range(0, n*m, 1):
    for j in range(0, n*m, 1):
        Auxiliar = Auxiliar + [0]
    C2 = C2 + [Auxiliar]
    Auxiliar = []

for v in range(0,n,1):
    for u in range(0,n,1):
        for i in range(0,m,1):
            for j in range(0,m,1):
                C2[i+u*m][j+v*m]=Auxiliar3[i][j][u][v]
```

Algoritmo 3 Complemento do algoritmo anterior. Dado um par de quadrados latinos ortogonais de ordem n com diagonais ajeitadas e um par de quadrados latinos ortogonais de ordem m com diagonais ajeitadas, o algoritmo retorna um quadrado mágico de ordem nm.

```
for i in range(0,m*n,1):
        for j in range(0,m*n,1):
                a = n*C1[i][j][0]+C1[i][j][1]
                C1[i][j]=a

for i in range(0,m*n,1):
        for j in range(0,m*n,1):
                a = n*C2[i][j][0]+C2[i][j][1]
                C2[i][j]=a

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

```
for i in range(0, m*n, 1):
        for j in range(0, m*n, 1):
                Matriz[i][j] = C1[i][j] + m*n * C2[i][j] + 1

print(Matriz)
```