REVISEM

Revista Sergipana de Matemática e Educação Matemática

SOBRE SUDOKUS E GRUPOS

Mateus Alegri
DMAI/Universidade Federal de Sergipe
allegri.mateus@gmail.com

Samuel Brito Silva
DMAI/Universidade Federal de Sergipe
s.complexo@hotmail.com

Resumo

Neste trabalho exibiremos algumas relações entre a teoria matemática que abrange o jogo Sudoku, os quadrados latinos, e a teoria de grupos finitos. Na terceira seção exibiremos um critério que estabelece se um quadrado latino de ordem n é a tabela de Cayley de um grupo de igual ordem. Na última seção trabalharemos com o conceito de ortogonalidade entre quadrados latinos, e utilizando o conceito de grupos finitos, exibiremos um contra-exemplo para uma famosa conjectura de Euler. Ressaltamos que o único pré-requisito para o perfeito entendimento deste artigo é o teorema de Cayley para grupos finitos, de modo que a teoria desenvolvida aqui é aplicável no ensino universitário.

Palavras-chaves: Sudoku; Quadrados Latinos; Grupos; Teorema de Cayley; Quadrados Latinos Ortogonais.

Abstract

In this work we will show some relationships between the mathematical theory that covers the Sudoku game, the Latin squares, and finite group theory. In the third section we will show a criterion that establishes if a Latin square of order n is the Cayley table of a group of equal order. In the last section we will work with the concept of orthogonality between Latin squares, and using the concept of finite groups we will show a counterexample to a famous Euler conjecture. We emphasize that the only prerequisites for the perfect understanding of this article is Cayley's theorem for finite groups, so that the theory developed here is applicable in university teaching.

Keywords: Sudoku; Latin Squares; Groups; Cayley's Theorem; Orthogonal Latin Squares.

1 INTRODUÇÃO

Provavelmente você já jogou, ou ouviu falar de um jogo popularmente chamado Sudoku[1]. É um jogo bem simples de raciocínio lógico que trata de organização posicional de números. No caso, o jogo é disposto em forma de um quadrado 9×9 de números em $\{1, 2, \ldots, 9\}$ com alguns pré-alocados em que o jogador deve completá-los de modo que um mesmo número não se repita na mesma linha ou coluna. A origem do jogo está associada ao conceito de quadrados latinos de ordem n, com $n = 1, 2, 3, \ldots$. Neste artigo exploraremos o conceito de quadrados latinos e relacionaremos esta estrutura com grupos finitos, de modo a estabelecer um critério para saber se um quadrado latino é a tabela de Cayley de um grupo. Na última seção trataremos de relações envolvendo grupos e pares de quadrados latinos mutualmente ortogonais, sendo este assunto importante para aplicações como teoria de códigos corretores de erros, por exemplo. Ao leitor deste texto é requerido apenas o conhecimento básico de grupos de permutação e o teorema de Cayley.

2 QUADRADOS LATINOS

A primeira vez de que se tem registro de que alguém pensou em quadrados latinos foi em 1639 em um jogo de cartas. O primeiro matemático que publicou um texto sobre quadrados latinos[2] foi Leonhard Euler em 1783, texto que se referia à aplicações à estatística. Segue a definição matemática de um quadrado latino de ordem n.

Definição 2.1. Um *quadrado latino* de ordem n é uma quádrupla (R, C, S, L) onde R, C, S são conjuntos com n elementos e L é uma aplicação $L : R \times C \to S$ tal que para cada i de R e j de C, a equação $L(i, j) = x$ tem uma única solução, isto é, fixando qualquer duas coordenadas de (i, j, x) encontra-se a terceira de forma única.

De maneira informal, um quadrado latino é uma maneira de dispor $n \times n$ elementos onde em uma determinada linha i e coluna j o elemento i, j não se repete nesta mesma linha e na mesma coluna.

Como $R, C, S = X = \{1, 2, \ldots, n\}$, abreviaremos a quádrupla $(X, X, X, *)$ para $(X, \cdot)$. Um exemplo de um quadrado latino de ordem n é:

[1] A palavra Sudoku é a abreviação para a frase: suuji wa dokushin ni kagiru, que em português significa: os dígitos devem permanecer únicos.

[2] O nome quadrados latinos se dá ao fato de que Euler usou letras latinas para os seus quadrados nesta obra.

$$L = \begin{array}{cccc} 1 & 2 & \cdots & n \\ 2 & 3 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ n & 1 & \cdots & 2 \end{array}$$

Notemos que esse quadrado corresponde a tabela de Cayley de $(\mathbb{Z}_n, +)$, identificando k com $\bar{k}$, para $1 \leq k \leq n$. Tal fato nos leva a pensar em uma possível relação existente da teoria de quadrados latinos e a teoria dos grupos. Veremos na seção seguinte um teorema que conecta de maneira técnica estas estruturas.

De fato, quadrados latinos apresentam uma estrutura combinatória muito singular, e dela derivam-se muitas propriedades e aplicações. Ademais, há resultados que são influenciados por várias áreas dentro e fora da análise combinatória, como álgebra, geometria finita, estatística dentre outras.

Definição 2.2. Dados dois quadrados latinos de ordem n, $L_1 = (l_{ij})$ e $L_2 = (m_{ij})$, definimos $L_1 \odot L_2$ como sendo o quadrado formado pelos pares (l_{ij}, m_{ij}) na linha i e coluna j.

Exemplo 2.3. Considere os quadrados latinos L_1 e L_2 como abaixo.

$$L_1 = \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array} \qquad L_2 = \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{array}$$

$L_1 \odot L_2$ é dado como a seguir:

$$L_1 \odot L_2 = \begin{array}{ccc} 11 & 22 & 33 \\ 23 & 31 & 12 \\ 32 & 13 & 21 \end{array}$$

Definição 2.4. Dois quadrados latinos de ordem n, $L_1 = (l_{ij})$ e $L_2 = (m_{ij})$, são ditos ortogonais se o par (l_{ij}, m_{ij}) ocorre apenas uma vez em $L_1 \odot L_2$.

Os quadrados latinos no exemplo anterior são ortogonais. A importância do estudo de quadrados latinos mutualmente ortogonais está vinculada ao fato de que com conjuntos grandes de quadrados latinos mutualmente ortogonais pode-se obter códigos baseados em quadrados latinos considerados ótimos, em certo sentido (maiores informações podem ser encontradas em [4] e [1]).

A origem do estudo de quadrados latinos ortogonais vêm da tentativa de solução do problema dos 36 oficiais de Euler. O problema consiste em encontrar uma tabela 6×6

em que se possa distribuir os oficiais em 6 regimentos distintos com 6 patentes distintas de modo que cada regimento tenha exatamente um oficial de uma das 6 patentes. Por exemplo, não pode se ter dois tenentes na cavalaria. A solução deste problema requer dois quadrados latinos de ordem 6 ortogonais, onde, um referente à patentes e outro referente aos regimentos. Euler conjecturou que não existem tais quadrados e ainda que não existe um par de quadrados latinos ortogonais de ordem $2(2k-1)$, para k natural. Fora provado em 1900 por Gaston Tarry, que, de fato, não existem quadrados latinos mutuamente ortogonais de ordem 6, porém a forma mais geral da conjectura foi refutada na década de 1950 por Bose, Parker e Shrikhande [2].

Definição 2.5. Seja $A = \{L_1, L_2, \ldots, L_k\}$ um conjunto de quadrados latinos de ordem n. O conjunto A é dito ser um conjunto mutuamente ortogonal se para cada $i \neq j$, L_i é ortogonal a L_j, $1 \leq i, j \leq k$.

Denota-se conjuntos mutuamente ortogonais por M.O.L.S. (sigla em inglês da expressão *Mutually Orthogonal Latin Squares*). Seja $N(n)$ o número de M.O.L.S. de ordem n. A proposição a seguir fornece uma limitação para a função $N(n)$.

Proposição 2.6. *Para cada* $n \geq 2$, $N(n) \leq n-1$

Demonstração: Seja $A = \{L_1, L_2, \ldots, L_k\}$ um conjunto de quadrados latinos mutuamente ortogonais. Dados L_1 e L_2 em A, os n símbolos de L_1 podem ser permutados de qualquer maneira sem afetar a sua ortogonalidade com o quadrado L_2. Podemos reordenar os símbolos na primeira linha de cada quadrado para ficar na forma:$(1, 2..., n)$. Sejam L_1 e L_2, como abaixo, são dois elementos do conjunto A.

$$L_1 = \begin{array}{cccc} 1 & 2 & \cdots & n \\ x & - & \cdots & - \\ \vdots & \vdots & \ddots & \vdots \\ - & - & \cdots & - \end{array} \qquad L_2 = \begin{array}{cccc} 1 & 2 & \cdots & n \\ y & - & \cdots & - \\ \vdots & \vdots & \ddots & \vdots \\ - & - & \cdots & - \end{array}$$

Nem o símbolo x, nem y podem ser 1, de modo que L_1 e L_2 são quadrados latinos. Além do mais $x \neq y$, pois se $x = y = i$, o par (i, i) já existe na primeira linha de $L_1 \odot L_2$. Então existem no máximo $n-1$ símbolos que podem aparecer na primeira posição da segunda linha de $L_1 \odot L_2$. Logo $N(n) \leq n-1$. ■

No exemplo abaixo mostraremos um conjunto de 3 M.O.L.S. de ordem 4. Um conjunto de $n-1$ M.O.L.S. de ordem n é chamado de um *conjunto completo*.

Exemplo 2.7. Considere os quadrados latinos:

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{array} \quad \begin{array}{cccc} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{array} \quad \begin{array}{cccc} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{array}$$

Por simples inspeção, estes quadrados formam um conjunto completo. Há uma classe infinita onde a cota superior $n-1$ é atingida, como descrito na última seção.

3 QUANDO UM QUADRADO LATINO É A TABELA DE UM GRUPO

Nesta seção exibiremos uma condição técnica, que se satisfeita, possa garantir que quadrados latinos possuam as propriedades de um grupo. Nem sempre um quadrado latino é a tabela de um grupo com uma certa operação, porém a tabela de um grupo sempre tem a estrutura de um quadrado latino. Basta notar que os elementos do grupo nunca se repetem nas mesmas linhas e colunas de um quadrado pois a operação do grupo é binária, e todo elemento do grupo possui inversa, ou seja a lei do cancelamento (tanto a direita como a esquerda) está assegurada nesta tabela. Podemos associar um quadrado latino à uma estrutura mais simples que a de grupos.

Definição 3.1. Dada $*$ uma operação binária em um conjunto Q, o par $(Q,*)$ é um quasigrupo se para todo par $a,b \in Q$, as equações $a*x=b$ e $y*a=b$ são unicamente solúveis para x e y em Q.

A partir da definição de um quasigrupo, podemos estabelecer que um quadrado latino L de ordem n é equivalente a uma tabela de um quasigrupo $(X=\{1,2,\ldots,n\},*)$.

A proposição a seguir nos diz que o que difere um grupo de um quasigrupo é a associatividade de elementos, ou seja, "um quasigrupo é um grupo não associativo".

Proposição 3.2. *Seja $(Q,*)$ um quasigrupo. Se esta estrutura é associativa então $(Q,*)$ é um grupo.*

Demonstração: Primeiramente vamos provar que $(Q,*)$ possui identidade. Sejam $e_1,e_2,x \in Q$, tais que $x*e_1=x=e_2*x$. Então $x*e_1^2=x*e_1=x$, logo $e_1^2=e_1$. Se $a \in Q$ é tal que $e_1*a=x$, então $e_2*e_1*a=e_2*x=x=e_1*a$, e assim $e_2*e_1=e_1=e_1^2$, implicando em $e_1=e_2$. Colocando $e=e_1$, temos que para qualquer $y \in Q$, $e*y=e*y^2$, implicando que $y=e*y$ e de maneira análoga obtemos $y=y*e$. Devido a arbitrariedade das escolhas de x e y, podemos estabelecer que e é a identidade em Q.

Provaremos agora que todo elemento de Q possui inverso em Q. Para todo $x \in Q$, existem únicos $a, b \in Q$, tais que $x * a = e = b * x$. Então $a = e * a = (b * x) * a = b * (x * a) = b * e = b$, e deste modo podemos denotar $x^{-1} = a = b$. ■

Como todo grupo é um quasigrupo, toda tabela de Cayley de um grupo finito é um quadrado latino, deste modo obtemos o seguinte resultado.

Corolário 3.3. *A tabela de multiplicação de um grupo finito de ordem n é um quadrado latino de ordem n.*

Exemplo 3.4. Considere os dois quadrados a seguir.

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

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

O quadrado latino da esquerda representa a tabela do grupo de Klein, $V = \mathbb{Z}_2 \times \mathbb{Z}_2$, obtida seguindo o isomorfismo entre V e $X = \{1, 2, 3, 4\}$, via a associação $1 \leftrightarrow (\bar{0}, \bar{0}), 2 \leftrightarrow (\bar{0}, \bar{1}), 3 \leftrightarrow (\bar{1}, \bar{0})$, e $4 \leftrightarrow (\bar{1}, \bar{1})$. O quadrado latino da direita não é a tabela de Cayley de um grupo. Observe que esta estrutura não é associativa, pois $(1.2).3 = 1$ e $1.(2.3) = 2$.

Como vimos no exemplo anterior, a recíproca do corolário nem sempre é verdadeira. Utilizando o próximo teorema teremos condições de julgar quando um quadrado latino tem a estrutura de grupo. O próximo teorema faz uso do famoso teorema de Cayley que diz que todo grupo finito é isomorfo a um subgrupo do grupo de permutações S_n, ou seja todo elemento de um grupo finito de n elementos é uma permutação de n elementos.

Considerando a tabela do grupo de Klein (V), se tomarmos duas linhas quaisquer desta e considerarmos estas como permutações, a composição destas linhas será uma linha da tabela de V. Por exemplo se permutarmos a segunda e quarta linhas, temos

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

que é a terceira linha da tabela do grupo de Klein (V). Podemos obter esta linha calculando $(2*4)*x = 2*(4*x)$, para todo $x \in X = \{1, 2, 3, 4\}$. De maneira equivalente, podemos realizar esta tarefa calculando $\phi_2 \circ \phi_4(x) = \phi_{2*4}(x)$, onde ϕ_g é a translação, $\phi_g(x) = g * x$. Em geral, para todos os quadrados latinos em que a composição de

duas de suas linhas é uma linha do quadrado, teremos que este quadrado é a tabela de Cayley de um grupo, resultado que será demonstrado logo a seguir, chamado de método de Siu. Este método é creditado ao matemático chinês Man-Keung Siu em seu artigo *Which Latin Squares are Cayley Tables?, publicado na revista The American Mathematical Monthly em 1991. Ver [5].*

Teorema 3.5 (Método de Siu)**.** *Um quadrado latino é a tabela de um grupo se, e somente se, a composição de duas linhas é uma linha do quadrado.*

Demonstração: Considere L um quadrado latino de ordem n, fechado em relação a composição de linhas. A fim de demonstrarmos este teorema, precisamos mostrar que a associatividade está assegurada para os elementos de $X = \{1, 2, \ldots, n\}$ via a operação $*$ explicitada no quadrado latino L. Vamos assumir que 1 seja a unidade de X, e consideremos a aplicação $\phi : X \to S_n$, que associa cada $g \in X$ em $\phi_g \in S_n$, onde $\phi_g(x) = g * x$, para todo $x \in X$. Primeiramente, ϕ está bem definida, pois se $g = h$, então $g*x = h*x$, implicando em $\phi_g(x) = \phi_h(x)$, para todo $x \in X$. A função é também injetora, devido ao fato da lei de cancelamento à esquerda, garantindo que ϕ_g é de fato bijetiva, e, por conseguinte, uma permutação de S_n.

Afirmamos que o quasigrupo $(X, *)$ é associativo (ou seja $(X, *)$ é um grupo), se e somente se, $\phi(X)$ é subgrupo de S_n.

De fato, se assumirmos $(X, *)$ associativo, temos $\phi_g \circ \phi_h(x) = g*(h*x) = (g*h)*x = \phi_{g*h}(x)$, para todo $x \in X$, e assim $\phi_g \circ \phi_h = \phi_{g*h}$, e temos que $\phi(X)$ é subgrupo de S_n. Reciprocamente, sendo $\phi(X)$ um subgrupo de S_n, temos $(a * b) * c = \phi_{a*b}(c) = \phi_a \circ \phi_b(c) = \phi_a(b * c) = a * (b * c)$, para quaisquer a, b e c em X.

Como S_n é um grupo finito, para provarmos que $(\phi(X), \circ)$ é subgrupo de S_n, basta verificarmos que a composição de quaisquer duas permutações de $\phi(X)$ está em $\phi(X)$, ou seja, basta provarmos que se $a, b \in X$, então $\phi_a \circ \phi_b = \phi_c$. Para tanto, basta verificarmos se a composição de duas linhas, digamos a e b, é uma linha do quadrado latino L. De fato, para qualquer $x \in X$, a linha a é $(\phi_a(1), \phi_a(2), \ldots, \phi_a(n))$, e assim a composição da linha a com a linha b é dada por

$$L_a \circ L_b = (\phi_a(1), \phi_a(2), \ldots, \phi_a(n)) \circ (\phi_b(1), \phi_b(2), \ldots, \phi_b(n)).$$

A composição $L_a \circ L_b$ é uma linha de L desde que $L_a \circ L_b = (\phi_c(1), \phi_c(2), \ldots, \phi_c(n))$, e isso é verdade se, e somente se, $\phi_a \circ \phi_b = \phi_c$. ■

Pode-se verificar que as linhas da tabela do grupo de Klein satisfazem a condição do critério de Siu. Na prática, para mostrar que um quadrado latino não é a tabela de um grupo, basta encontrar duas linhas de modo que a composição delas não é uma linha do quadrado latino.

Exemplo 3.6. Consideremos o quadrado latino

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \\ 3 & 1 & 2 & 5 & 4 \\ 4 & 3 & 5 & 2 & 1 \\ 5 & 4 & 1 & 3 & 2 \end{array}$$

Calculando a composição da terceira e segunda linhas, obtemos:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix}$$

A permutação resultante não é nenhuma linha do quadrado latino.

Para mostrarmos que um quadrado latino de ordem n tem estrutura de grupo, pelo teorema anterior, temos que testar as n^2 composições possíveis. Note que isto é muito mais simples do que testar as n^3 equações do tipo: $a * (b * c) = (a * b) * c$.

4 GRUPOS E M.O.L.S.

Definição 4.1. Um quadrado latino linha é um quadrado de ordem n em que cada linha é uma permutação de n elementos.

Observemos que um quadrado latino é um quadrado latino linha, mas a recíproca nem sempre é verdadeira.

Consideremos agora o quadrado R de ordem 3,

$$R = \begin{array}{ccc} 2 & 1 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array}$$

Cada linha de R pode ser vista como a imagem de uma permutação, digamos,

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Se as linhas de um quadrado latino linha são dadas por $f_1, f_2, \ldots, f_n$, denotamos este quadrado por $(f_1, f_2, \ldots, f_n)$. O conjunto de todos os quadrados latinos linha de ordem n é denotado por RL_n. Definimos a seguinte operação: $\circ : RL_n \times RL_n \to RL_n$, tal que $A \circ B = (h_1, ..., h_n)$, onde $A = (f_1, ..., f_n), B = (g_1, ..., g_n)$, e $h_i(x) = f_i(g_i(x))$, para $x \in \{1, 2, \ldots, n\}$.

Teorema 4.2. *$(RL_n, .)$ é um grupo de ordem $(n!)^n$*

Demonstração: Sejam:

$A = (f_1, ..., f_n)$, $B = (g_1, ..., g_n)$ e $C = (h_1, ..., h_n)$ elementos em RL_n

(i) A operação é associativa, pois, $A \circ (B \circ C) = A \circ (h_1 g_1, ..., h_n g_n) = (f_1(h_1 g_1), ..., f_n(h_n g_n)) = ((f_1 h_1)g_1, ..., (f_n h_n)g_n) = (A \circ B) \circ C$

(ii) Para todo $A \in RL_n$ existe $E \in RL_n$ tal que $A \circ E = E \circ A = A$, basta tomar a matriz $E = (e, e, ..., e)$, onde e é a permutação identidade.

(iii) Para qualquer $A \in RL_n$ existe $B \in RL_n$ tal que $A \circ B = B \circ A = E$, basta tomar $B = (f_1^{-1}, ..., f_n^{-1})$. Costuma-se denotar B por A^{-1}.

Por (i), (ii), e (iii), temos que RL_n é um grupo com a operação $\circ$. O número de elementos de RL_n é igual a $(n!)^n$, pois dado $A = (f_1, ..., f_n)$ têm-se $n!$ possibilidades em cada entrada de A, e como A tem n entradas, segue o resultado. ■

Para os quadrados A e B em RL_n, denotaremos, de agora em diante $A \circ B$ por AB. Provaremos a seguir uma série de teoremas que são úteis na construção de conjuntos de quadrados latinos mutuamente ortogonais.

Teorema 4.3. *Sejam $R \in RL_n$ e $E = (e, ..., e)$, assim E e R são ortogonais se, e somente se, R é um quadrado latino.*

Demonstração: Como $R \in RL_n$, é suficiente provar que as colunas de R são permutações. Fixado j, basta provar que $a_{ij} \neq a_{kj}$ sempre que $i \neq k$. No quadrado $R \odot E$ temos que o par (a_{ij}, j) aparece na linha i e coluna j, enquanto o par (a_{ik}, j) aparece na coluna k e linha i. Como R e E são ortogonais e $(i, j) \neq (k, j)$ temos $(a_{ij}, j) \neq (a_{ik}, j)$ e assim $a_{ij} \neq a_{kj}$, como queríamos.

A outra implicação segue do fato de que, sendo R um quadrado latino, tomando o elemento a_{ij} de R, (a_{ij}, j) só pode ocorrer uma vez, e portanto R e E são mutuamente ortogonais.■

Teorema 4.4. *Seja $\{A_1, ..., A_n\}$ um conjunto de quadrados latinos linha mutuamente ortogonais. Para qualquer quadrado latino linha X, o conjunto $\{XA_1, ..., XA_m\}$ é composto de quadrados latinos linha mutuamente ortogonais.*

Demonstração: Vamos demonstrar que se A e B então XA e XB são ortogonais. Suponhamos que o par (u, v) ocorre na linha n e coluna p e também na linha n e coluna q em $XA \odot XB$. Sendo $x(m, p)$ elemento de X, $u = a(m, x(m, p)) = a(n, x(n, q))$ e $v = b(m, x(m, p)) = b(n, x(n, q))$, temos que o par $(a(n, x(n, q)), b(n, x(n, q)))$ só ocorre uma vez em $XA \odot XB$, devido a ortogonalidade de A e B.■

Proposição 4.5. *Sejam A e B dois quadrados latinos linha. Os quadrados A e B são ortogonais se, e somente se, existe um quadrado latino L tal que $AL = B$*

Demonstração: Considerando $L = A^{-1}B$, pelo teorema 4.2 , temos que L é um quadrado latino linha. Como A e B são ortogonais, temos que $L = A^{-1}B$ e $A^{-1}A = E$ são ortogonais pelo teorema 4.4. Pelo teorema 4.3 podemos concluir que L é um quadrado latino.

Reciprocamente, seja L um quadrado latino tal que $AL = B$. Pelo teorema 4.3, L é ortogonal a E, e assim, pelo teorema 4.4, $AL = B$ e $AE = A$ são ortogonais. ■

Proposição 4.6. *Seja A um quadrado latino e m o menor inteiro positivo tal que A^m não é latino, assim $\{A, A^2, \ldots, A^{m-1}\} = B$ é um conjunto ortogonal de quadrados latinos linha.*

Demonstração: Considerando $k, j < m$, temos que A^j e A^k são ortogonais, e pela proposição 4.5 existe um quadrado latino L tal que $A^j = LA^k$, sem perda de generalidade, consideremos $j < k$, e assim $L = A^{j-k}$ é um quadrado latino, e pela proposição anterior, podemos concluir que A^k e A^j são ortogonais. ■

Se os quadrados $A, A^2, ..., A^{m-1}$ formam um conjunto de quadrados latinos linha mutuamente ortogonais, A, A^j são ortogonais ($j \leq n$), pela proposição 4.1, existe um quadrado latino L, tal que $A^j = AL$ o que acarreta $L = A^{j-1}$. Deste modo, obtemos o seguinte resultado.

Corolário 4.7. *$\{A, A^2, \ldots, A^{m-1}\}$ é um conjunto de quadrados latinos linha mutuamente ortogonais se, e somente se, todos são quadrados latinos.*

Lema 4.8. *Se A é um quadrado latino, então A^{-1} também é um quadrado latino.*

Demonstração: Se A é um quadrado latino, pelo teorema 4.3 A e E são ortogonais. Pelo teorema 4.4, $E = AA^{-1}$ e $EA^{-1} = A^{-1}$ são ortogonais, implicando que A^{-1} é um quadrado latino. ■

Pelo corolário 4.7 e lema 4.8, podemos obter o seguinte corolário.

Corolário 4.9. *Se $A, A^2, ..., A^{m-1}$ são quadrados latinos, então $m-1$ quadrados consecutivos da coleção $A^{-m+1}, A^{-m+2}, \ldots, A, \ldots, A^{m-1}$ forma um conjunto de M.O.L.S..*

Agora vamos provar o principal teorema desta seção:

Teorema 4.10. *Se L é um quadrado latino de ordem n, com $n = p_1^{e_1}...p_r^{e_r}$, onde $p_1 < p_2 < ... < p_r$ são primos, então o conjunto*

$$\{L, L^2, \ldots, L^{p_1-1}\}$$

é conjunto de M.O.L.S. de ordem n.

Demonstração: Observemos que todos os positivos inteiros menores ou iguais a $p_1 - 1$ são relativamente primos com n, temos que $L, ..., L^{p_1-1}$ são quadrados latinos. Pelo corolário 4.7, estes quadrados são mutuamente ortogonais. ■

Corolário 4.11. *Se n é primo, existe um conjunto de potências de quadrados latinos contendo um conjunto completo de $n-1$ M.O.L.S. de ordem n.*

Corolário 4.12. *Se n é ímpar, então existe um conjunto de potências de quadrados latinos contendo ao menos dois M.O.L.S. de ordem n.*

Note que para n primo, o corolário 4.7 garante a existência de um conjunto de $n-1$ MOLS de ordem n, que de fato, ilustra a eficiência da procura de conjuntos de potências de quadrados latinos para encontrar conjuntos de M.O.L.S..

Exemplo 4.13. Neste exemplo vamos utilizar o teorema anterior para construir um conjunto $\{L, L^2\}$ contendo dois MOLS de ordem 10:

$$L = \begin{array}{cccccccccc} 1 & 3 & 4 & 2 & 6 & 7 & 5 & 9 & 10 & 8 \\ 10 & 2 & 5 & 4 & 4 & 8 & 6 & 7 & 1 & 9 \\ 9 & 10 & 3 & 5 & 8 & 1 & 2 & 4 & 6 & 7 \\ 7 & 9 & 1 & 4 & 10 & 5 & 3 & 2 & 8 & 6 \\ 3 & 8 & 10 & 7 & 5 & 2 & 9 & 6 & 4 & 1 \\ 5 & 1 & 8 & 9 & 2 & 6 & 4 & 10 & 7 & 3 \\ 8 & 4 & 6 & 10 & 1 & 9 & 7 & 5 & 3 & 2 \\ 2 & 7 & 9 & 6 & 3 & 10 & 1 & 8 & 5 & 4 \\ 4 & 6 & 2 & 8 & 7 & 3 & 10 & 1 & 9 & 5 \\ 6 & 5 & 7 & 1 & 9 & 4 & 8 & 3 & 2 & 10 \end{array}$$

$$L^2 = \begin{array}{cccccccccc} 1 & 4 & 2 & 3 & 7 & 5 & 6 & 10 & 8 & 9 \\ 9 & 2 & 4 & 5 & 3 & 7 & 8 & 6 & 10 & 1 \\ 6 & 7 & 3 & 8 & 4 & 9 & 10 & 5 & 1 & 2 \\ 3 & 8 & 7 & 4 & 6 & 10 & 1 & 9 & 2 & 5 \\ 10 & 6 & 1 & 9 & 5 & 8 & 4 & 2 & 7 & 3 \\ 2 & 5 & 10 & 7 & 1 & 6 & 9 & 3 & 4 & 8 \\ 5 & 10 & 9 & 2 & 8 & 3 & 7 & 1 & 6 & 4 \\ 7 & 1 & 5 & 10 & 9 & 4 & 2 & 8 & 3 & 6 \\ 8 & 3 & 6 & 1 & 10 & 2 & 5 & 4 & 9 & 7 \\ 4 & 9 & 8 & 6 & 2 & 1 & 3 & 7 & 5 & 10 \end{array}$$

Estes quadrados provêm um contra-exemplo para a conjectura de Euler (página 4) sobre a não existência de pares de M.O.L.S. de ordem 10. Como $L^3 = E$ e logo, $L^2 = L^{-1}$ e sabendo que se A é um quadrado latino A^{-1} (lema 4.8) também o é, pelo corolário 4.7, temos que L e L^2 são ortogonais.

Referências

[1] Alegri, M. *Quadrados Latinos e aplicações*. 2006.85f. Dissertação (Mestrado em Matemática Aplicada)-Instituto de Matemática Estatística e Computação Científica, Unicamp, Campinas, SP, 2006.

[2] Bose, R. C., Parker, E. T., Shrikhande, S. S. *Further results on the construction of mutually ortogonal Latin squares and the falsity of Euler's conjecture.* Canadian Journal of Mathematics, 19, 1960, 189-203.

[3] Bruck, R. H. *Some results in theory of quasigroups.* Trans. Amer. Math. Soc., 55, 1944, 19-52.

[4] Laywine, C.F., Mullen, G. L. *Discrete Mathematics Using Latin Squares*, Wiley interscience publication, New York, 1998. 305p.

[5] Siu, M-K, *Which Latin Squares are Cayley Tables?* The American Mathematical Monthly, Vol. 98, No.7, 1991, pp. 625-627.