UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
LICENCIATURA EM MATEMÁTICA

MARIANA VASCONCELOS NEGRINI

# QUADRADOS LATINOS

TRABALHO DE CONCLUSÃO DE CURSO

CORNÉLIO PROCÓPIO
2018

MARIANA VASCONCELOS NEGRINI

# QUADRADOS LATINOS

Trabalho de Conclusão de Curso de Graduação, apresentado à disciplina trabalho de conclusão de curso 2, do curso de Licenciatura em Matemática da Universidade Tecnológica Federal do Paraná — UTFPR, como requisito parcial para a aprovação da disciplina.

Orientador: Prof. Dr. Anderson Paiao Dos Santos

CORNÉLIO PROCÓPIO
2018

Ministério da Educação
**Universidade Tecnológica Federal do Paraná**
Câmpus Cornélio Procópio
Diretoria de Graduação
Departamento de Matemática
Curso de Licenciatura em Matemática

## FOLHA DE APROVAÇÃO

**BANCA EXAMINADORA**

Prof. Anderson Paião dos Santos
(Orientador)

Prof. Josimar da Silva Rocha

Prof. Débora Aparecida Francisco Albanez

"A Folha de Aprovação assinada encontra-se na Coordenação do Curso"

## RESUMO

NEGRINI, Mariana. **Quadrados Latinos**. 2018. 33 f. Trabalho de Conclusão de Curso (Graduação) – Licenciatura em Matemática. Universidade Tecnológica Federal do Paraná. Cornélio Procópio, 2018

O objetivo deste trabalho é fazer uma apresentação da teoria de Quadrados Latinos, que foi inicialmente estudada pelo matemático Leonard Euler. Também será introduzida a teoria de Quadrados Latinos Ortogonais, apresentando os principais resultados. Discutiremos também a teoria de Corpos Finitos, que como veremos, é parte importante da construção dos resultados da teoria de Quadrados Latinos. Apresentaremos algumas aplicações desta teoria, como delineamento experimental e teoria de grafos.



**Palavras-chave:** Quadrados Latinos. Teoria de Corpos. Grafos.

**ABSTRACT**

NEGRINI, Mariana. **Latim Square**. 2018. 33 f. Trabalho de Conclusão de Curso (Graduação) – Licenciatura em Matemática. Universidade Tecnológica Federal do Paraná. Cornélio Procópio, 2018

The purpose of this work is to present. Latin Square theory, which was initially studied by the mathematician Leonard Euler, we will also introduce the theory of Latin Orthogonal Squares, presenting the main results. In adition we discuss the theory of finite field, which as we shall see, is an important part of the construction of the results of the Latin Square theory. We will present some applications of this theory, such as experimental design and graph theory.

**Keywords:** Latin squares. Theory of Fields. Graphs.

## LISTA DE FIGURAS

FIGURA 1 – Puzzle Sudoku . . . . . 16
FIGURA 2 – Puzzle Sudoku Completo . . . . . 17
FIGURA 3 – Grafo . . . . . 26
FIGURA 4 – Grafo Bipartido . . . . . 27
FIGURA 5 – Grafo . . . . . 29

**SUMÁRIO**


**1 INTRODUÇÃO . . . . . 11**
**2 REFERENCIAL TEÓRICO . . . . . 13**
2.1 CORPOS . . . . . 13
2.2 QUADRADOS LATINOS . . . . . 16
2.2.1 Quadrados Latinos Ortogonais . . . . . 18
**3 APLICAÇÕES DE QUADRADOS LATINOS . . . . . 25**
3.1 DELINEAMENTO EXPERIMENTAL . . . . . 25
3.2 TEORIA DE GRAFOS . . . . . 25
3.2.1 Grafo Bipartido . . . . . 26
3.2.2 Grafo de Hamming . . . . . 28
**4 CONCLUSÃO . . . . . 31**
**REFERÊNCIAS . . . . . 33**

# 1 INTRODUÇÃO

O principal objetivo deste trabalho é abordar a teoria de Quadrados Latinos que, segundo (CARDOSO; SZYMANSKI; ROSTAMI, 2009), foi estudada inicialmente por Leonard Euler, importante matemático suíço do século XVIII. Os seus primeiros resultados foram apresentados à Academia de Ciências de São Petersburgo em 1779. Porém só recentemente é que este tema tem atraído a atenção dos matemáticos, devido às diversas aplicações como por exemplo na teoria de códigos, teoria de grafos, formação de desenhos estatísticos entre outras.

Podemos considerar o estudo de Quadrados Latinos como tendo duas ênfases principais que são abordadas neste texto. Por um lado, é o estudo das propriedades de quadrados latinos simples e por outro, o estudo de conjuntos de quadrados latinos mutuamente ortogonais.

Para se trabalhar com a teoria Quadrados Latinos, definições e propriedades, é necessário um estudo do conceito de corpo. A teoria de corpos foi inicialmente introduzida em 1820 pelo norueguês N.H Abel.

No presente trabalho, faremos um breve estudo da teoria de corpos, em especial da teoria de corpos finitos e um pouco de extensões de corpos, abordando algumas definições e propriedades que serão utilizadas no texto. Neste estudo espera-se que o leitor tenha um prévio conhecimento de Álgebra, em especial da teoria de anéis. Para um estudo mais aprofundado, sugerimos ao leitor as referências: (IEZZI; DOMINGUES, 2003) e (LIDL; NIEDERREITER, 2008). Tais assuntos serão tratados na primeira parte Capítulo 2.

Na segunda parte do Capítulo 2, faremos uma discussão sobre a teoria de Quadrados Latinos, apresentando algumas definições, exemplos e resultados, principalmente sobre Quadrados Latinos Ortogonais.

No Capítulo 3 deste trabalho, apresentaremos aplicações da teoria de Quadrados Latinos, como por exemplo na teoria de estatística por meio de delineamento experimental e também na teoria de grafo abordando grafo bipartido e grafo de Hamming.

Por último, apresentaremos a conclusão.

# 2 REFERENCIAL TEÓRICO

Neste capítulo apresentaremos algumas definições e resultados da teoria de corpos e da teoria de Quadrados Latinos. As principais referências utilizadas foram: (IEZZI; DOMINGUES, 2003), (LIDL; NIEDERREITER, 2008) e (MULLEN, 2008). Para a leitura deste capítulo, é necessário conhecimentos básicos de álgebra abstrata, como teoria de grupos e anéis.

## 2.1 CORPOS

O conceito de corpo segundo (MILIES, 2004), aparece no trabalho de Galois[1] sobre resolução de equações polinomiais, intitulado "Sur la theórie des nombres", publicado no Bulletin des Sciences de Férussac em 1830. Essencialmente, ele usa a ideia de Gauss de considerar congruências módulo um primo $p$ e constrói o que hoje denotamos como $\mathbb{Z}_p$, o corpo dos inteiros módulo $p$.

Ernst Steinitz tentou um estudo compreensivo da teoria abstrata de corpos. Em seu trabalho ele introduz as noções de corpo primo e de característica de um corpo e prova um resultado fundamental que afirma que "todo corpo pode ser obtido do seu corpo primo pela adjunção de uma série (eventualmente infinita) de elementos transcendentes e depois a adjunção de uma série de elementos algébricos". Também neste trabalho ele introduz a noção de polinômio separável, que ele chama de vollkommen ou completo, e prova que sobre um corpo, todo polinômio é irredutível ou se decompõe num produto de fatores lineares se, e somente se, é extensão de um corpo dado pela adjunção de um número finito de raízes de polinômios separáveis.

Nesta seção iremos abordar algumas definições e resultados preliminares da teoria corpos e corpos finitos. O leitor pode consultar (LIDL; NIEDERREITER, 2008) para um aprofundamento no assunto.

**Definição 1.** *Um sistema matemático constituído de um conjunto não vazio A e um par de operações sobre A, respectivamente, uma adição* $(x, y) \longmapsto x+y$ *e uma multiplicação* $(x, y) \longmapsto x \cdot y$ *é chamado de* **anel comutativo com unidade** *se:*

*(i)* $(A, +)$ *é um grupo abeliano, ou seja, se* $a, b, c \in A$*, então:*

- *(a)* $a + (b + c) = (a + b) + c$ *(associatividade).*
- *(b)* $a + b = b + a$ *(comutatividade).*
- *(c) Existe um elemento* $0_A \in A$ *tal que,* $a + 0_A = a$ *(existência do elemento neutro).*
- *(d) Existe um elemento em* $A$*, denotado por* $-a$*, tal que* $a + (-a) = 0_A$ *(existência de oposto).*

*(ii) A multiplicação goza da propriedade associativa, isto é, se* $a, b, c \in A$*, então*

$$a(bc) = (ab)c.$$

[1] Évariste Galois foi um importante matemático francês do século XIX. Galois criou um domínio inteiramente novo da álgebra abstrata: a teoria dos grupos determinou a condição necessária e para que um polinômio pudesse ser resolvido por raízes, morreu num duelo com a idade de 20 anos.

*(iii) A multiplicação é distributiva em relação à adição, isto é; se* $a, b, c \in A$*, então*

$$a(b+c) = ab + ac \ \text{ e } \ (a+b)c = ac + bc.$$

*(iv) A multiplicação goza da propriedade comutativa, isto é, se* $a, b \in A$*, então*

$$ab = ba.$$

*(v) Existe um elemento* $1_A \in A$*,* $1_A \neq 0_A$*, tal que*

$$a \cdot 1_A = 1_A \cdot a = a \ \text{ (elemento neutro multiplicativo).}$$

*Um elemento* $a$ *de um anel com unidade* $A$ *diz-se* **invertível** *se existe um elemento, que denotaremos por* $a^{-1} \in A$*, e chamaremos seu* **inverso***, tal que*

$$aa^{-1} = a^{-1}a = 1_A.$$

**Notação.** *Denotaremos por* $U(A)$ *o conjunto dos elementos do anel com unidade* $A$ *que têm inverso.*

**Definição 2.** *Um anel comutativo com unidade* $\mathbb{F}$ *é chamado de* **corpo** *se* $U(\mathbb{F}) = \mathbb{F}^* = \mathbb{F} - \{0\}$.

Caso o corpo $\mathbb{F}$ seja finito, dizemos que $\mathbb{F}$ é um **corpo finito**.

**Exemplo 1.** *Os conjuntos* $\mathbb{Q}, \mathbb{R}$ *e* $\mathbb{C}$*, com a soma e produto usuais, são exemplos de corpos. Note que* $\mathbb{Z}$ *não é um corpo, pois* $U(\mathbb{Z}) = \{1, -1\} \neq \mathbb{Z}^*$.

Em 1820, o norueguês N.H.Abel (1802-1829) em seus trabalhos sobre equações algébricas, introduziu o conceito de corpo, porém toda essa teoria só se tornou conhecida quando o alemão R. Dedekind (1831-1916) introduziu a teoria de corpos finitos, teoria essa que discutiremos a seguir.

**Exemplo 2.** *Um exemplo é o corpo* $\mathbb{Z}_3$*. Construiremos sua tábua de operações (respetivamente soma e produto).*

| $+$ | $0$ | $1$ | $2$ |
|---|---|---|---|
| $0$ | $0$ | $1$ | $2$ |
| $1$ | $1$ | $2$ | $0$ |
| $2$ | $2$ | $0$ | $1$ |

| $\cdot$ | $0$ | $1$ | $2$ |
|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $2$ |
| $2$ | $0$ | $2$ | $1$ |

**Definição 3.** *Um subconjunto* $\mathbb{K}$ *de um corpo* $\mathbb{F}$ *diz-se um* **subcorpo** *de* $\mathbb{F}$ *se* $\mathbb{K}$ *é fechado em relação às operações de* $\mathbb{F}$ *e em relação à inversão, isto é, se para todo par de elementos* $x, y \in \mathbb{K}$ *tem-se que:*

*(i)* $x \pm y \in \mathbb{K}$*;*

*(ii)* $xy \in \mathbb{K}$*;*

*(iii)* $x^{-1} \in \mathbb{K}$.

Vamos agora apresentar um pequeno resumo de alguns resultados principais da teoria de corpos finitos, visto que nos restringiremos a esse tipo de corpo no nosso trabalho.

**Definição 4.** *Seja $\mathbb{F}$ um corpo. Chama-se* **subcorpo primo** *de $\mathbb{F}$ ao menor subcorpo de $\mathbb{F}$, em relação à inclusão. Um corpo diz-se* **primo** *se coincide com seu subcorpo primo; isto é, se não existe nenhum subcorpo propriamente contido nele.*

Denotaremos por $\mathbb{F}_n$ um corpo com $n$ elementos.

**Proposição 1.** *Todo corpo primo finito $\mathbb{F}$ é isomorfo a $\mathbb{Z}_p$, para algum p primo.*

Um corpo $\mathbb{E}$ é **extensão de um corpo** $\mathbb{F}$ se $\mathbb{F} \subset \mathbb{E}$. A partir disso, todos os corpos finitos são vistos como extensões de $\mathbb{Z}_p$.

Uma extensão $\mathbb{F}$ de um corpo $\mathbb{E}$ é também um espaço vetorial sobre $\mathbb{E}$, o que nos diz que se $\mid \mathbb{E} \mid = q$, então $\mid \mathbb{F} \mid = q^n$, onde $n$ é a dimensão desse espaço vetorial. Olhando para essa afirmação, considerando que todo corpo finito é uma extensão de um corpo $\mathbb{Z}_p$, temos que todo corpo tem precisamente $p^n$ elementos para um $p$ primo.

**Exemplo 3.** *Considere o corpo $\mathbb{F}_3$ e o polinômio $f = x^2 + 1$ irredutível de grau dois em $\mathbb{F}_3[x]$. Seja $\alpha$ uma raiz deste polinômio. Sabemos que se estendermos $\mathbb{F}_3$ com o elemento $\alpha$, obtemos o corpo $\mathbb{F}_9$, ou seja, $\mathbb{F}_3[\alpha] \cong \mathbb{F}_9$. Então, $\mathbb{F}_9 = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$.*

*Assim obtemos as seguintes tábuas de operações para $\mathbb{F}_9$:*

| $+$ | $0$ | $1$ | $2$ | $\alpha$ | $\alpha+1$ | $\alpha+2$ | $2\alpha$ | $2\alpha+1$ | $2\alpha+2$ |
|---|---|---|---|---|---|---|---|---|---|
| $0$ | $0$ | $1$ | $2$ | $\alpha$ | $\alpha+1$ | $\alpha+2$ | $2\alpha$ | $2\alpha+1$ | $2\alpha+2$ |
| $1$ | $1$ | $2$ | $0$ | $\alpha+1$ | $\alpha+2$ | $\alpha$ | $2\alpha+1$ | $2\alpha+2$ | $2\alpha$ |
| $2$ | $2$ | $0$ | $1$ | $\alpha+2$ | $\alpha$ | $\alpha+1$ | $2\alpha+2$ | $2\alpha$ | $2\alpha+1$ |
| $\alpha$ | $\alpha$ | $\alpha+1$ | $\alpha+2$ | $2\alpha$ | $2\alpha+1$ | $2\alpha+2$ | $0$ | $1$ | $2$ |
| $\alpha+1$ | $\alpha+1$ | $\alpha+2$ | $\alpha$ | $2\alpha+1$ | $2\alpha+2$ | $2\alpha$ | $1$ | $2$ | $0$ |
| $\alpha+2$ | $\alpha+2$ | $\alpha$ | $\alpha+1$ | $2\alpha+2$ | $2\alpha$ | $2\alpha+1$ | $2$ | $0$ | $1$ |
| $2\alpha$ | $2\alpha$ | $2\alpha+1$ | $2\alpha+2$ | $0$ | $1$ | $2$ | $\alpha$ | $\alpha+1$ | $\alpha+2$ |
| $2\alpha+1$ | $2\alpha+1$ | $2\alpha+2$ | $2\alpha$ | $1$ | $2$ | $0$ | $\alpha+1$ | $\alpha+2$ | $\alpha$ |
| $2\alpha+2$ | $2\alpha+2$ | $2\alpha$ | $2\alpha+1$ | $2$ | $0$ | $1$ | $\alpha+2$ | $\alpha$ | $\alpha+1$ |

| $.$ | $0$ | $1$ | $2$ | $\alpha$ | $\alpha+1$ | $\alpha+2$ | $2\alpha$ | $2\alpha+1$ | $2\alpha+2$ |
|---|---|---|---|---|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $2$ | $\alpha$ | $\alpha+1$ | $\alpha+2$ | $2\alpha$ | $2\alpha+1$ | $2\alpha+2$ |
| $2$ | $0$ | $2$ | $1$ | $2\alpha$ | $2\alpha+2$ | $2\alpha+1$ | $\alpha$ | $\alpha+2$ | $\alpha+1$ |
| $\alpha$ | $0$ | $\alpha$ | $2\alpha$ | $2$ | $\alpha+2$ | $2\alpha+2$ | $1$ | $\alpha+1$ | $2\alpha+1$ |
| $\alpha+1$ | $0$ | $\alpha+1$ | $2\alpha+2$ | $\alpha+2$ | $2\alpha$ | $1$ | $2\alpha+1$ | $2$ | $\alpha+2$ |
| $\alpha+2$ | $0$ | $\alpha+2$ | $2\alpha+1$ | $2\alpha+2$ | $1$ | $\alpha$ | $\alpha+1$ | $2\alpha+2$ | $2$ |
| $2\alpha$ | $0$ | $2\alpha$ | $\alpha$ | $1$ | $2\alpha+1$ | $\alpha+1$ | $\alpha$ | $2\alpha+1$ | $\alpha+2$ |
| $2\alpha+1$ | $0$ | $2\alpha+1$ | $\alpha+2$ | $\alpha$ | $2$ | $2\alpha+2$ | $\alpha+2$ | $\alpha$ | $1$ |
| $2\alpha+2$ | $0$ | $2\alpha+2$ | $\alpha+1$ | $2\alpha+1$ | $\alpha+2$ | $2$ | $\alpha+2$ | $1$ | $2\alpha$ |

*Note que para a construção desta tábua, consideramos que $\alpha$ é uma raiz de $f = x^2 + 1$, ou seja, $f(\alpha) = \alpha^2 + 1 = 0$. Assim, $\alpha^2 = 2$.*

## 2.2 QUADRADOS LATINOS

O Quadrado Latino foi estudado por Leonard Euler, que o identificou como um "novo tipo de quadrado mágico". Ele fundamentou a teoria dos Quadrados Latinos em 1782, quando apresentou o problema que ficou conhecido como o "problema dos 36 oficiais" que apresenta a seguinte formulação: *"Admita-se a existência de seis destacamentos em cada um dos quais ficam seis oficiais com patentes distintas, dentre seis possíveis. Pretende-se fazer uma parada militar envolvendo estes trinta e seis oficiais, de tal forma que eles apareçam, seis em cada linha, sem que existam dois oficiais com a mesma patente ou pertencentes ao mesmo destacamento numa mesma linha."* Euler conjecturou que este problema não teria solução, porém só foi provada por Tarry Gaston em 1900, por análise exaustiva de todas as possibilidades. (CARDOSO; SZYMANSKI; ROSTAMI, 2009)

**Definição 5.** *Um* **Quadrado Latino** *de ordem $n$ é uma matriz $n \times n$ cujas entradas tem $n$ símbolos distintos e não há repetição de símbolos em nenhuma linha ou coluna.*

**Exemplo 4.** *Um Quadrado Latino de ordem 5:*

$$\begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 0 & 2 \\ 2 & 4 & 0 & 1 & 3 \\ 3 & 2 & 1 & 4 & 0 \\ 4 & 0 & 3 & 2 & 1 \end{array}$$

Nota-se que qualquer permutação de colunas ou de linhas de um quadrado latino gera um novo quadrado latino.

Outro exemplo clássico de Quadrado Latino é o Sudoku. O nome Sudoku vem da abreviação japonesa *suuji wa dokushin ni kagiru* que significa "os números devem ser únicos". Embora pareça ser um jogo de origem japonesa, teve sua primeira publicação em $1970$ na revista americana Math Puzzles and Logic Problems, com a designação Number Place e só mais tarde foi levado para o Japão onde, rapidamente, atingiu grande popularidade. (TEIXEIRA, 2014)

O Sudoku é um puzzle que se baseia na completação de quadrados latinos, no qual consiste uma grelha $9 \times 9$ que são agrupadas em blocos $3 \times 3$ e que devem ser completamente preenchidos com números inteiros entre $1$ e $9$. A princípio, algumas das entradas já estão preenchidas e o objetivo é preencher as entradas restantes, de tal forma que em cada linha, coluna e bloco, não existam números repetidos. A seguir uma representação do puzzle antes e depois de ser preenchido, respectivamente.

**Figura 1 – Puzzle Sudoku**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 8 | | | 7 | |
| | 2 | 7 | 9 | | 5 | | | |
| 6 | | | | | | | | |
| | | | | | | 4 | | 7 |
| 4 | 9 | | 2 | | | | 5 | |
| 3 | | 2 | 8 | 5 | | | | |
| | | | | | | 6 | | |
| | 3 | | | 7 | 9 | | | |
| 8 | | | 6 | 4 | | | 9 | |

**Figura 2 – Puzzle Sudoku Completo**

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

**Exemplo 5.** *Se tomarmos a tábua de operação de um grupo qualquer, temos que não existe repetição em nenhuma linha ou coluna (garantida pela existência e unicidade da solução de equações do tipo* $a * x = b$ *e* $y * a = b$*) . Se considerarmos essa tábua como uma matriz quadrada (ignorando a linha e coluna fundamentais) temos um quadrado latino. Como para qualquer inteiro* $n$ *existe pelo menos um grupo com* $n$ *elementos (tome* $(\mathbb{Z}_n, +)$*, por exemplo) temos que existe pelo menos um quadrado latino de ordem* $n$*.*

A seguir apresentamos alguns resultados preliminares da teoria de Quadrados Latinos.

**Definição 6.** *Um quadrado latino é denominado* **reduzido** *se as letras se dispõem por ordem alfabética na primeira linha e na primeira coluna ou se os números estiverem na sua ordem natural. O número total de quadrados latinos reduzidos de ordem* $n$ *será denotado por* $l_n$*.*

O número total de quadrados latinos de ordem $n$ será denotado por $L_n$ e o próximo teorema nos dá uma fórmula para se obter $L_n$ em função $l_n$.

**Teorema 1.** $L_n = n!(n-1)!l_n$*, para todo* $n \geq 2$*.*

*Demonstração.* Pode-se observar facilmente que qualquer permutação de colunas ou de linhas de um quadrado latino gera um novo quadrado latino. Assim, dado um quadrado latino de

ordem $n$ com permutação de colunas pode-se obter $n!$ quadrados latinos cujas primeiras linhas são distintas. Fixada a primeira linha, permutando as outras linhas, pode-se obter $(n-1)!$ quadrados latinos distintos entre si e distintos dos obtidos por permutação das colunas. Dado um quadrado latino reduzido, pode-se obter $n!(n-1)!$ quadrados latinos distintos, e portanto, para $l_n$ quadrados latinos reduzidos, podemos obter $n!(n-1)!l_n$ quadrados latinos distintos. Como para qualquer quadrado latino, com permutações de linhas e colunas pode-se obter somente um quadrado latino reduzido, temos que $L_n = n!(n-1)!l_n$. □

Segue abaixo a tabela com os valores de $l_n$ conhecidos:

| $n$ | $l_n$ |
|---|---|
| 2 | 1 |
| 3 | 1 |
| 4 | 4 |
| 5 | 56 |
| 6 | 9408 |
| 7 | 16942080 |
| 8 | 535281401856 |
| 9 | 377597570964258816 |
| 10 | 7580721483160132811489280 |
| 11 | 5363937773277371298119673540771840 |

### 2.2.1 Quadrados Latinos Ortogonais

**Definição 7.** *Sejam $H$ e $K$ quadrados latinos de ordem $n$.*

$$H = \begin{matrix} h_{1,1} & h_{1,2} & \cdots & h_{1,n} \\ h_{2,1} & h_{2,2} & \cdots & h_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n,1} & h_{n,2} & \cdots & h_{n,n} \end{matrix} \quad \textit{e} \quad K = \begin{matrix} k_{1,1} & k_{1,2} & \cdots & k_{1,n} \\ k_{2,1} & k_{2,2} & \cdots & k_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n,1} & k_{n,2} & \cdots & k_{n,n} \end{matrix}$$

*A* **sobreposição** *de H sobre K é definida como uma matriz de ordem $n$, cujas entradas são pares ordenados formados pelas entradas dos quadrados latinos $H$ e $K$. Vejamos abaixo a sobreposição dos quadrados latinos $H$ e $K$:*

$$\begin{matrix} (h_{1,1},k_{1,1}) & (h_{1,2},k_{1,2}) & ... & (h_{1,n},k_{1,n}) \\ (h_{2,1},k_{2,1}) & (h_{2,2},k_{2,2}) & ... & (h_{2,n},k_{2,n}) \\ \vdots & \vdots & \ddots & \vdots \\ (h_{n,1},k_{n,1}) & (h_{n,2},k_{n,2}) & ... & (h_{n,n},k_{n,n}) \end{matrix} .$$

**Exemplo 6.** *Considerando os quadrados latinos A e B.*

$$A = \begin{matrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{matrix} \qquad B = \begin{matrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{matrix}$$

*Temos que a sobreposição deles é dada por:*

$$\begin{array}{cccc} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,2) & (0,3) & (3,0) & (2,1) \\ (2,3) & (3,2) & (0,1) & (1,0) \\ (3,1) & (2,0) & (1,3) & (0,2) \end{array}$$

Note que para a matriz de sobreposição temos $n^2$ entradas e também $n^2$ pares ordenados distintos. No exemplo anterior, cada par ordenado apareceu uma única vez, porém isso não necessariamente acontece, como podemos observar no seguinte exemplo.

**Exemplo 7.** *Dados os Quadrados Latinos C e D,*

$$C = \begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \qquad D = \begin{array}{ccc} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{array},$$

*temos que a sobreposição de $C$ e $D$ é:*

$$\begin{array}{ccc} (0,0) & (1,2) & (2,1) \\ (1,2) & (2,1) & (0,0) \\ (2,1) & (0,0) & (1,2) \end{array}$$

**Definição 8.** *Dois quadrados latinos são ditos* **ortogonais** *se sua sobreposição tem somente pares ordenados distintos. Uma coleção de quadrados latinos é dita* **mutuamente ortogonal** *se dados dois quadrados latinos quaisquer desta coleção, eles são ortogonais. Para simplificar a notação, iremos denotar uma coleção de quadrados latinos mutuamente ortogonais por* **MOLS** *(Mutually Orthogonal Latin Squares). Será denotado por $N(n)$ a quantidade de conjuntos de MOLS possíveis de ordem $n$.*

No exemplo 6, os quadrados latinos $A$ e $B$ são ortogonais e no exemplo 7, os quadrados latinos $C$ e $D$ não são ortogonais.

Veremos nos próximos resultados que determinar o valor de $N(n)$ para $n$ qualquer, é um problema em aberto, assim como o valor de $l_n$, e vem sendo estudado por vários matemáticos a séculos.

**Teorema 2.** $N(n) \leq n-1$*, para todo* $n \geq 2$*.*

*Demonstração.* Observe que dados dois quadrados latinos ortogonais, podemos trocar um determinado símbolo por outro, sem afetar a ortogonalidade (Veja o exemplo 8). E consequentemente, num conjunto de MOLS, a troca de símbolos dentro de cada quadrado latino não afeta a ortogonalidade. Assim, dado uma ordem $n$, considere um conjunto $\{A_1, A_2, ..., A_r\}$ de MOLS. Cada quadrado latino pode ser modificado para que a sua primeira linha esteja com os elementos na ordem padrão, $0, 1, ..., n-1$, e ainda teremos um conjunto de MOLS, digamos $\{B_1, B_2, ..., B_r\}$.

Vamos denotar por $[a_{ij}]_{B_k}$ o elemento localizado na linha $i$ e coluna $j$ do quadrado latino $B_k$, com $i, j \in \{1, 2, ..., n\}$ e $1 \leq k \leq r$. Considere os elementos $[a_{21}]_{B_k}$. Temos que

$[a_{21}]_{B_k} \neq 0$ para todo $k$, pois caso contrário, teríamos dois zeros na coluna um, o que contradiz a hipótese de que todos são quadrados latinos. Assim, temos $n-1$ elementos possíveis para a entrada $[a_{21}]_{B_k}$. Como todas as matrizes têm a primeira linha na ordem padrão, a entrada $[a_{21}]_{B_k} \neq [a_{21}]_{B_l}$, para todo $k \neq l$, para que a ortogonalidade de cada par de quadrados latinos de $\{B_1, B_2, ..., B_r\}$ seja preservada. Temos assim que $|\{B_1, B_2, ..., B_r\}| \leq n-1$ e portanto $N(n) \leq n-1$. □

**Exemplo 8.** *Considere os quadrados latinos ortogonais $A$ e $B$:*

$$A = \begin{matrix} 1 & 2 & 3 & 0 \\ 2 & 1 & 4 & 3 \\ 3 & 0 & 1 & 2 \\ 0 & 3 & 2 & 1 \end{matrix} \qquad B = \begin{matrix} 2 & 1 & 0 & 3 \\ 0 & 3 & 2 & 1 \\ 3 & 0 & 1 & 2 \\ 1 & 2 & 3 & 0 \end{matrix}.$$

*Note que no quadrado $A$, se realizarmos a seguinte substituição:*

$$\begin{matrix} 1 \longmapsto 0 \\ 2 \longmapsto 1 \\ 3 \longmapsto 2 \\ 0 \longmapsto 3 \end{matrix}$$

*Teremos um novo quadrado latino $A'$ que ainda é ortogonal a $B$.*

$$A' = \begin{matrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{matrix}.$$

*Fazendo a mesma substituição em $B$, obtemos $B'$, que também é ortogonal a $A$ e $A'$.*

$$B' = \begin{matrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{matrix}.$$

O próximo resultado nos dá um valor exato para $N(q)$, quando $q$ é uma potência prima, e para tanto utilizamos resultados da Teoria de Corpos, como o fato de que $\mathbb{F}_q$ é um corpo.

**Teorema 3.** *(BOSE, 1938) Se $q$ é uma potência de um número primo, então $N(q) = q-1$.*

*Demonstração.* Considere o corpo $\mathbb{F}_q = \{0, a_1, a_2, ..., a_{q-1}\}$. Enumere cada linha e cada coluna de uma matriz $q \times q$ com elementos de $\mathbb{F}_q$. Definimos então a função $f_k(x, y) = a_k x + y$, onde $k \in \mathbb{F}_q^*$ e $x, y \in \mathbb{F}_q$. Considere agora a matriz $B_k$, onde cada entrada é definida como:

$$[b_{xy}]_{B_k} = f_k(x, y).$$

*Afirmação*: $B_k$ é um quadrado latino para todo $k \in \mathbb{F}_q^*$. Fixado um $k$, suponha por absurdo que existam dois elementos iguais numa linha de $B_k$. Assim temos que existem $x, y_1, y_2 \in \mathbb{F}_q$ tais que

$$f_k(x, y_1) = f_k(x, y_2), \text{ com } y_1 \neq y_2.$$

E portanto,

$$a_k x + y_1 = a_k x + y_2 \Rightarrow y_1 = y_2,$$

o que é um absurdo. Claramente, se supormos elementos iguais numa coluna de $B_k$ chegaremos ao mesmo resultado. Portanto, $B_k$ é um quadrado latino.
*Afirmação*: $B_k$ é ortogonal a $B_l$ para todo $k \neq l$ com $k, l \in \mathbb{F}_q^*$.

Considere a matriz da sobreposição de $B_k$ e $B_l$ e seja $(b_1, b_2)$ uma das entradas desta matriz. Temos que existem $x, y \in \mathbb{F}_q$ tais que:

$$\begin{aligned} a_k x + y &= b_1 \\ a_l x + y &= b_2. \end{aligned}$$

Tomando a matriz de coeficientes deste sistema, temos:

$$\begin{pmatrix} a_k & 1 \\ a_l & 1 \end{pmatrix}.$$

Como $a_k \neq a_l$, temos que ela é inversível, logo a solução é única. Portanto, o par $(b_1, b_2)$ é único na matriz de sobreposição de $B_k$ e $B_l$ e consequentemente $B_k$ e $B_l$ são ortogonais. Como tomamos $B_k$ e $B_l$ arbitrários, temos que qualquer par de matrizes do conjunto $\{B_1, B_2, ..., B_{q-1}\}$ é ortogonal.

□

**Exemplo 9.** *Considere o corpo $\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{0, 1, \alpha, 1 + \alpha\}$, onde o polinômio minimal de $\alpha$ é $m_\alpha = X^2 + X + 1$. Denotando $\alpha = 2$ e $\alpha + 1 = 3$ e utilizando a construção descrita na demonstração do Teorema 3, temos:*
*para cada $k \in \mathbb{F}_4^*$, defina $[b_{xy}]_{B_k} = f_k(x, y) = kx + y$. Assim,*

$$B_1 = \begin{matrix} f_1(0,0) & f_1(0,1) & f_1(0,2) & f_1(0,3) \\ f_1(1,0) & f_1(1,1) & f_1(1,2) & f_1(1,3) \\ f_1(2,0) & f_1(2,1) & f_1(2,2) & f_1(2,3) \\ f_1(3,0) & f_1(3,1) & f_1(3,2) & f_1(3,3) \end{matrix} = \begin{matrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{matrix}$$

$$B_2 = \begin{matrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{matrix}$$

$$B_3 = \begin{matrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 0 & 1 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{matrix}.$$

*Facilmente se verifica que o conjunto $\{B_1, B_2, B_3\}$ é um conjunto de MOLS.*

Apresentaremos na sequência três conjecturas acerca da função $N(n)$ para outros valores de $n$. Como veremos adiante, uma delas ainda é um problema em aberto, as outras duas foram resolvidas.

Este primeiro resultado foi conjecturado por Leonard Euller.

**Conjectura 1.** *(EULER, 1782) Se $n$ é um múltiplo ímpar de 2, ou seja, se existe $k \in \mathbb{Z}_+$ tal que $n = (2k+1)2$, então $N(n) = 1$.*

Atualmente sabe-se que esta conjectura é válida somente para $k = 0$ e $k = 1$. Veremos adiante alguns resultados que provam esta afirmação.

**Teorema 4.** *(TARRY, 1900)* $N(6) = 1$.

A prova original deste teorema pode ser encontrada em (TARRY, 1900) . Existe também uma prova em termos mais atuais em (MULLEN, 1995). Como já se sabia que a conjectura de Euler era válida para $k = 0$, este Teorema reforçou a conjectura, mostrando que ela também é válida para $k = 1$. Note que este resultado é equivalente a dizer que o Problema dos 36 oficiais de fato, não tem solução.

**Conjectura 2.** *(MACNEISH, 1922) Seja $n = q_1 q_2 \cdots q_r$, onde $q_i$ são potências de primos distintos e ainda $q_1 < q_2 < ... < q_r$. Então, $N(n) = q_1 - 1$.*

Esta conjectura foi provada por MacNeish no ano de 1922 e é uma tentativa de generalizar a Conjectura de Euler, que nesse ano, não se sabia que estava incorreta. Note que se $q_1 = 2$, temos exatamente a Conjectura de Euler, que foi resolvida em 1959.

Na sequência apresentamos os conceitos de números de Fermat e de Mersenne, que podem ser encontrados com mais detalhes na referência (HEFEZ, 2011).

Os **números de Fermat** são os números da forma

$$F_n = 2^{2^n} + 1.$$

Fermat achava que esses números eram todos primos, baseado na observação de que $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ são primos. Em 1732, Leonhard Euler mostrou que

$$F_5 = 2^{2^5} + 1 = 4.294.967.297 = 641 \cdot 6700417,$$

desmentindo assim a afirmação de Fermat.

Os números de Fermat primos são chamados de **primos de Fermat.** Até hoje, não se sabe se existem outros primos de Fermat além dos quatro primeiros. Conjecturou-se (Hardy e Wright) que os primos de Fermat são em número finito.

Os **números de Mersenne** são os números da forma

$$M_p = 2^p - 1,$$

onde $p$ é um número primo.

No intervalo $2 \leq p \leq 5000$ os números de Mersenne que são primos, chamados de **primos de Mersenne**, correspondem aos seguintes valores de $p$ :

$2, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253$ e $4423$. Até dezembro de 2001 o maior primo de Mersenne conhecido era $M_{13466917}$, que possui no sistema decimal $4053946$ dígitos, e é o trigésimo nono primo de Mersenne conhecido.

Na sequência apresentamos alguns resultados sem prová-los:

**Teorema 5.** *(DÉNES; KEEDWELLRY, 1974) Seja $m$ um numero. Se $m$ é um primo de Mersenne maior que três, ou $m+1$ um primo de Fermat, então existe um conjunto de $m$ MOLS de ordem $m^2+m+1$.*

**Exemplo 10.** *Note que tomando $m=4$, as hipóteses do teorema são respeitadas e portanto $N(21) \geq 4$. Temos então um contra-exemplo da Conjectura de MacNeish.*

**Teorema 6** (Bose e Shrikhande 1959)**.** *Seja $q$ uma potência de um primo tal que $q \equiv 3$ mod $4$, então existe um par de MOLS de ordem $(3q-1)/2$.*

**Exemplo 11.** *Note agora que se tomarmos $q=7$, as hipóteses do teorema são respeitadas e portanto $N(10) \geq 2$. Temos então um contra-exemplo da Conjectura de Euler.*

**Conjectura 3.** $N(n) = n-1$ *se, e somente se, $n$ é uma potência de um primo.*

A volta da Conjectura da Potência Prima é exatamente o Teorema 3. A ida, ainda é um problema em aberto e sua importância é tamanha, que em 1995, um ano após o Último Teorema de Fermat ser provado, Gary L. Mullen propôs em seu artigo intitulado *"A Candidate for the next Fermat Problem"* que a Conjectura da Potência Prima fosse o próximo problema de Fermat.

O próximo teorema é considerado o mais importante resultado desde o Teorema 3, na Teoria de Quadrados Latinos. O Teorema 6 já derrubará a Conjectura de Euler, mas este teorema nos mostrará mais, que a Conjectura de Euler está incorreta para todo $k \in \mathbb{Z}_+$, com exceção de $k=0$ e $k=1$.

**Teorema 7.** *(BOSE; SHRIKHANDE; PARKER, 1960)* $N(n) \geq 2$*, para todo $n$ com exceção de $n=2$ e $n=6$.*

# 3 APLICAÇÕES DE QUADRADOS LATINOS

## 3.1 DELINEAMENTO EXPERIMENTAL

Segundo (MONTGOMERY, 2008) cada execução experimental é um teste. Mais formalmente, podemos definir um experimento como uma série de execuções em que mudanças intencionais são feitas nas variáveis de entrada, de um processo ou sistema, de modo que possamos observar a resposta de saída. Delineamento experimental é uma ferramenta criticamente importante no mundo científico para melhorar o processo de realização do produto.

Esses delineamentos são separados em três categorias, que são: delineamento sem controle local, delineamento com controle local simples e delineamento com controle local duplo que são os quadrados latinos.

Os quadrados latinos são um delineamento muito aplicável, entretanto o número de tratamentos deve ser igual ao número de repetições, o que pode ser um problema quando são diferentes.

Em geral os quadrados latinos mais utilizados são os de ordens $5$ e $8$. Por outro lado, em grande parte dos casos não se usa mais de $8$ tratamentos pois o número de repetições seria grande, já por outro lado os quadrados latinos de ordens $3$ e $4$ formam poucas parcelas e por conseguinte só são utilizadas quando o experimento inclui vários quadrados latinos.

A seguir mostraremos um exemplo retirado do livro (GOMES, 1963).

**Exemplo 12.** *Queremos experimentar $5$ rações A,B,C,D e E em $5$ vacas e com $5$ capins. Nessa circunstância é aconselhável que cada ração seja experimentada em cada uma das vacas e com cada um dos capins. Desta forma usaremos um quadrado latino de ordem $5$.*

| | Vaca 1 | Vaca 2 | Vaca 3 | Vaca 4 | Vaca 5 |
|---|---|---|---|---|---|
| Capim 1 | A | B | C | D | E |
| Capim 2 | C | A | E | B | D |
| Capim 3 | B | E | D | C | A |
| Capim 4 | E | D | B | A | C |
| Capim 5 | D | C | A | E | B |

Note que as rações estão posicionadas numa matriz $5 \times 5$ tal que cada ração não se repete nenhuma vez em sua linha ou coluna, característica essa de um quadrado latino.

## 3.2 TEORIA DE GRAFOS

A teoria de grafos é muito utilizada na área da matemática aplicada, visto que é uma modelagem que se aplica em várias situações reais.

Para discutir a Teoria de Grafos, precisamos de algumas definições.

**Definição 9.** *Se $A$ é um conjunto não vazio, uma partição de $A$, com dois elementos, é um conjunto $\{X, Y\}$, onde $X \subset A$ e $Y \subset A$ e valem as seguintes condições:*

- $X \cup Y = A$ *e*

- $X \cap Y = \emptyset$.

**Observação 1.** *Em geral, pode-se definir partição de um conjunto A utilizando uma quantidade maior que dois de subconjuntos de $A$, mas no que segue vamos utilizar partições com somente dois subconjuntos.*

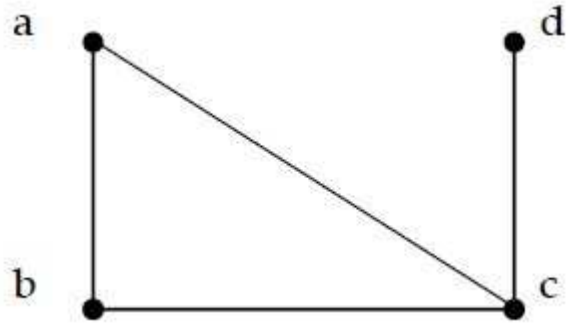
**Exemplo 13.** *Se P é o conjunto dos naturais pares e I é o conjunto dos naturais ímpares temos que $\{P, I\}$ é uma partição do conjunto $\mathbb{N}$ dos números naturais.*

**Definição 10.** *Um* **grafo** *é um conjunto não vazio $V$ juntamente com um conjunto $E$ em que seus elementos são denotados por $x - y$, com $x, y \in V$. Os elementos de $V$ serão designados por vértices e os elementos de $E$ (que são pares não ordenados de vértices, isto é, $x - y = y - x$) serão designados por arestas. Designaremos por $G = (V, E)$ um grafo em que o conjunto de vértices é $V$ e o conjunto de arestas é $E$.*

Os grafos são muitas vezes representados por figuras planas constituídas por pontos representando os vértices e segmento representando as arestas.

**Exemplo 14.** *Seja $G = (V, E)$ onde $V = \{a, b, c, d\}$ e $E$=$\{a - b, b - c, c - d, a - c\}$. Então, $G$ pode ser representado por:*

**Figura 3 – Grafo**




Pode-se utilizar o cartesiano para definir um grafo orientado, porém não vamos tratar de tais grafos neste trabalho.

### 3.2.1 Grafo Bipartido

**Definição 11.** *Um grafo $G = (V, E)$ diz-se* **bipartido completo** *se existe uma partição $\{X, Y\}$ do seu conjunto de vértices tal que não existe aresta entre qualquer par de vértices de $X$ nem entre qualquer par de vértices em $Y$, ou seja:*

- *Se* $a, b \in X \Rightarrow a - b \notin E$
- *Se* $a, b \in Y \Rightarrow a - b \notin E$
- *Se* $a \in X$ *e* $b \in Y \Rightarrow a - b \in E$.

*Esta partição $\{X, Y\}$ do conjunto $V$ designa-se por* **bipartição** *de vértices.*

Considere um Quadrado Latino $L = [a_{i,j}]_n$. Vamos construir um grafo bipartido completo rotulado[1] a partir deste Quadrado Latino. Considere o conjunto $U$ de linhas e $W$ de colunas de $L$, ou seja:

$$U = \{U_i = (a_{i,1}; a_{i,2}; \ldots; a_{i,n}), \forall i \in \{1, 2, \ldots n\}\} \text{ e}$$
$$W = \{W_i = (a_{1,i}; a_{2,i}; \ldots; a_{n,i}), \forall i \in \{1, 2 \ldots, n\}\}.$$

Considere $K = a_{ij}$, pela definição de Quadrado Latino, temos que $K \in \{1, \ldots, n\}$

Vamos construir um grafo bipartido completo, $G(V, E)$, onde cada vértice será associado a uma linha ou coluna de $L$, ou seja, $V := U \cup W$. Certamente $\{U, W\}$ define uma partição de $V$.

Desta forma definiremos o conjunto de arestas da seguinte forma:

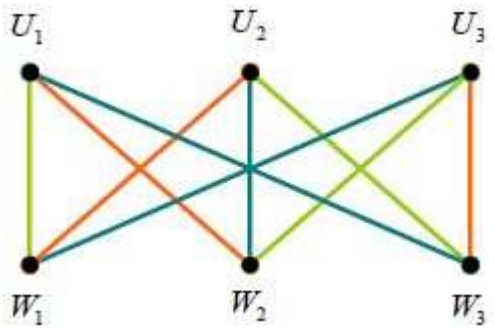
$$E = \{U_i - W_j; \forall i, j \in \{1, \ldots, n\}\}.$$

A definição de $V$ e $E$ nos diz que o grafo é bipartido completo.

Cada aresta $U_i - W_j$ será rotulado como o valor da entrada $a_{ij}$ do Quadrado Latino.

**Exemplo 15.** *Dado o quadrado latino* $L = \begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{matrix}$ *, este pode ser representado através do seguinte grafo bipartido, onde utilizamos a seguinte lista de cores para os rótulos: o número 1 refere-se a cor verde, o número 2 a cor laranja e o número 3 a cor azul.*

**Figura 4 – Grafo Bipartido**




*Desta forma, o grafo bipartido associado a um quadrado latino de ordem* $n$ *é um* $G(V, E)$ *em que cada aresta é colorida com* $n$ *cores contidas no quadrado latino e em cada vértice incide em uma aresta de cada cor.*

[1] Um grafo é dito rotulado quando são atribuídos rótulos a seus vértices ou arestas. Neste caso, refere-se a cor dada a cada aresta

### 3.2.2 Grafo de Hamming

Para que se possa ter um maior compreensão na aplicação de quadrados latinos na teoria de grafo de Hamming, a seguir são apresentados alguns conceitos sobre a teoria de grafo de Hamming segundo (CARDOSO; SZYMANSKI; ROSTAMI, 2009).

**Definição 12.** *Dadas duas sequências de $m$ dígitos $x = x_1x_2 \dots x_m$ e $y = y_1y_2 \dots y_m$ cada um dos quais pertencentes a um mesmo conjunto de $n$ símbolos, define-se por* ***distância de Hamming*** *entre $x$ e $y$, e denota-se por $d_{ham}(x, y)$, o número de posições em que $x$ e $y$ diferem.*

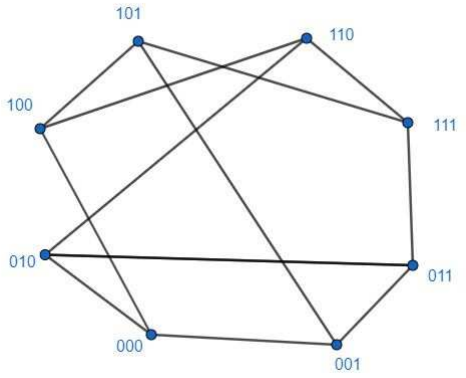
**Exemplo 16.** *Dadas as palavras de 8 letras do alfabeto latino*

*critério e criticam*

*Conclui-se que a distância de hamming dessas duas palavras é 4.*

**Definição 13.** *Designa-se por* **grafo de Hamming** *e denota-se por $H(m, n)$ o grafo cujos vértices são as sequências de $m$ dígitos pertencentes a um conjunto de $n$ símbolos e onde dois vértices são adjacentes se as correspondentes sequências estão a uma distância de Hamming igual a $1$.*

**Exemplo 17.** $H(3, 2) = \{100, 101, 110, 111, 010, 011, 001, 000\}$.




**Definição 14.** *Seja $G(V, A)$ um grafo e $S$ um subconjunto de vértices $S \subset V$. Diz-se que $S$ é um* **conjunto independente** *de $G$ se dois vértices quaisquer de $S$ não são adjacentes. Quando tal conjunto $S$ tem cardinalidade máxima, ou seja, coleciona a maior quantidade possível de vértices dois a dois não adjacentes, $S$ é denominado de* **conjunto independente máximo** *e a sua cardinalidade é denominada* **número de independência** *e denotada por $\alpha(G)$.*

A seguir abordamos um exemplo usando as definições anteriores.

**Exemplo 18.** *Transformar a determinação de um quadrado latino de ordem n na determinação de um independente máximo de um grafo de Hamming e com base nesta transformação determinar um quadrado latino de ordem três.*

*Sendo $X = [x_{ij}]$ um quadrado latino de ordem $n$ sobre o conjunto de símbolos $\{1, 2, ..., n\}$ e denotando cada entrada $x_{ij} = k$ por $x_{ijk}$, com $i$, $j$, $k \in \{1, 2, ..., n\}$, é claro que em $X$ não podem existir duas entradas determinadas por $x_{i_1j_1k_1}$ e $x_{i_2j_2k_2}$ cuja distância de*

*Hamming entre as sequências de três índices $i_1j_1k_1$ e $i_2j_2k_2$ seja igual a 1. Logo, construindo o correspondente grafo de Hamming, $H(3, n)$, que é um grafo de ordem $n^3$ tal que*

$$V = \{(ijk) : i, j, k \in [n]\}, E = \{(i_1j_1k_1)(i_2j_2k_2)\},$$

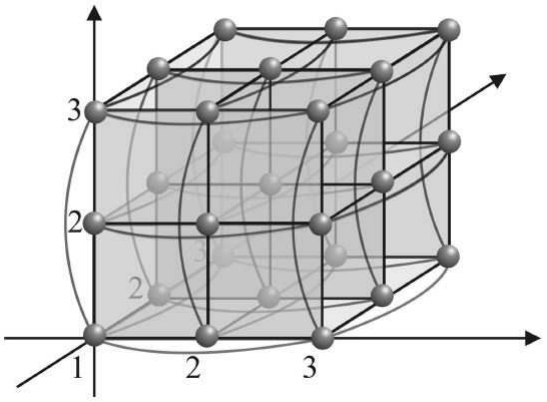
*conclui-se que a determinação de um quadrado latino $X$ de ordem $n$ é equivalente à determinação de um independente máximo de $H(3, n)$.*

*Com efeito, uma vez que dentre as possíveis sequências de índices $ijk$, com $i, j, k \in \{1, 2, ..., n\}$, existem no máximo $n^2$ pares de índices distintos, podemos concluir, imediatamente, que $\alpha(H(3, n)) \leq n^2$.*

*Por outro lado, admitindo que existe um quadrado latino L de ordem $n$ é claro que o conjunto de sequências de três índices $\{ijk : L_{ij} = k\}$ tem cardinalidade $n^2$ (que é igual ao número de entradas de L) e define em H(3, n) um conjunto independente de vértices.*

*Tendo em conta as definições acima, $\alpha(H(3, n)) = n^2$. Concretizando esta redução da determinação de quadrados latinos à determinação de independentes máximos de grafos de Hamming, para $n = 3$, considerando o grafo de Hamming $H(3, 3)$ (que tem ordem 27), conforme referido anteriormente, temos*

**Figura 5 – Grafo**




$V(G)$= $\{(111), (112), (113), (121),(122), (123), (131), (132), (133), (211), (212), (213), (221), (222), (223), (231), (232), (233), (311), (312), (313), (321), (322), (323), (331), (332), (333)\}$.

$E(G)$= $\{(111)(112), (111)(113), (111)(121), (111)(131), (111)(211), (111)(311), (112)(113), (112)(122), (112)(132), (112)(212), (112)(312), (113)(123), (113)(213), (113)(313), (121)(122), (121)(123), (121)(131), (121)(221), (121)(321), (122)(123), (122)(222), (122)(322), (123)(133), (123)(223), (123)(323), (131)(132), (131)(133), (132)(332), (133)(233), (133)(333), (211)(212), (211)(213), (211)(221), (211)(231), (211)(311), (212)(213), (212)(222), (212)(232), (212)(312), (213)(223), (213)(233), (213)(223), (213)(233), (213)(313), (221)(222), (221)(223), (221)(231), (221)(321), (222)(223), (222)(232), (222)(322), (223)(323), (231)(232), (231)(233), (231)(331), (232)(233), (232)(332), (233)(333), (311)(312), (311)(313), (311)(321), (311)(331), (312)(313), (312)(322), (312)(323), (312)(332), (313)(323), (313)(333), (321)(322),$

$(321)(322)$, $(321)(323)$, $(321)(331)$, $(322)(323)$, $(322)(332)$, $(323)(333)$, $(331)(332)$, $(331)(333)$, $(332)(333)\}$.

*Analisando este grafo, obtêm-se, por exemplo, os conjuntos independentes máximos*

$$S_1 = \{(111), (122), (133), (212), (223), (231), (313), (321), (332)\} \quad \textit{e}$$

$$S_2 = \{(111), (122), (133), (213), (221), (232), (312), (323), (331)\}.$$

*Cada um dos quais define, naturalmente, um quadrado latino de ordem* $3$*.*

*Por exemplo, tomando o Quadrado Latino obtido por* $S_1$ *temos:*

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

# 4 CONCLUSÃO

Neste trabalho apresentamos uma discussão sobre a teoria de Quadrados Latinos, focando principalmente na definição na determinação de cardinalidade do maior conjunto de MOLS possíveis de ordem $n$.

Vimos que a teoria teve inicio no século XVIII, com Euler, mas diversos resultados importantes são mais recentes, já do século XX. Esses resultados, foram obtidos utilizando principalmente a teoria de Corpos Finitos. Daí a necessidade da breve discussão sobre Teoria de corpos finitos que fizemos no capítulo . Optamos por apresentar somente os resultados principais de tal teoria, por se tratar de uma teoria muito extensa e não ser o foco deste trabalho.

Apresentamos também, aplicações de Quadrados Latinos em estatística e em teoria de grafos relacionamos com Grafo de Hamming e Grafo Bipartido.

Fizemos as correções propostas pela banca e por esse motivo não nos aprofundamos na teoria de corpos que era uma perspectiva para essa segunda fase, desta forma nos restringindo apenas o que usaríamos na teoria de Quadrados Latinos , pois como dito anteriormente se trata de uma teoria muito extensa.

## REFERÊNCIAS


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. Canad. J. Math, 1960. Citado na página 23.

BOSE, R. C. On the application of properties of galois fields to the problem of construction of hyper-graeco-latin squares. **SankhyZ 3**, 1938. Citado na página 20.

CARDOSO, Domingos; SZYMANSKI, Jerzy; ROSTAMI, Mohammad. **Matemática Discreta: combinatória, teoria dos grafos e algoritmos**. [S.l.: s.n.], 2009. ISBN 978-972-592-237-8. Citado 3 vezes nas páginas 11, 16 e 28.

DÉNES, J.; KEEDWELLRY, A. D. **Latin Squares and Their Applications**. [S.l.: s.n.], 1974. 397-401 p. Citado na página 23.

EULER, L. Recherches sur une nouvelle espèce de quarrés magiques. **Verhandelingen uitgegeven door het zeeuwsch Genootschap der Wetenschappen te Vlissingen 9, Middelburg 1782**, 1782. Citado na página 22.

GOMES, F.P. **Curso de estatística experimental**. Universidade de S. Paulo, Escola Superior de Agricultura "Luiz de Queiroz, 1963. Disponível em: <https://books.google.com.br/books?id=ZckqGwAACAAJ>. Citado na página 25.

HEFEZ, Abramo. **Elementos da Aritmética**. [S.l.: s.n.], 2011. ISBN 978-85-85818-25-8. Citado na página 22.

IEZZI, Gelson; DOMINGUES, Hygino. **Álgebra Moderna**. 4º. ed. reform. ed. São Paulo: [s.n.], 2003. ISBN 85-357-010-9. Citado 2 vezes nas páginas 11 e 13.

LIDL, Rudolf; NIEDERREITER, Harald. **Finite Fields (Encyclopedia of Mathematics and its Applications**. [S.l.: s.n.], 2008. ISBN 0521065674. Citado 2 vezes nas páginas 11 e 13.

MACNEISH, Harris F. Euler squares. **Annals of Mathematics**, Annals of Mathematics, v. 23, n. 3, p. 221–227, 1922. ISSN 0003486X. Disponível em: <http://www.jstor.org/stable/1967920>. Citado na página 22.

MILIES, César Polcino. **Breve História da Algebra Abstrata**. 2004. Citado na página 13.

MONTGOMERY, D.C. **Design and Analysis of Experiments**. [s.n.], 2008. ISBN 9780471487357. Disponível em: <http://books.google.de/books?id=kMMJAm5bD34C>. Citado na página 25.

MULLEN, Gary. A candidate for the next fermat problem. v. 17, p. 18–22, 09 1995. Citado na página 22.

MULLEN, Gary L. Finite fields and their applications. 2008. Citado na página 13.

PARKER, E. T. Construction of some sets of mutually orthogonal latin squares. **Proc. Amer. Math. Soc.**, Series A 36, p. 946–949, 1959. Nenhuma citação no texto.

TARRY, G. Le probléme des 36 officiers. **Annals of Mathematics**, C. R. Assoc. Fr. Au. Sci., p. 122–123, 1900. Citado na página 22.

TEIXEIRA, Ricardo Cunha. O sudoku. **Tribunal das Ilhas**, 2014. Citado na página 16.