Universidade do Estado do Rio de Janeiro
Centro de Tecnologia e Ciências
Instituto de Matemática e Estatística

José Travassos Ichihara

Construção de quadrados mágicos pelo método do passo uniforme

Rio de Janeiro
2014

José Travassos Ichihara

Construção de quadrados mágicos pelo método do passo uniforme

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), da Universidade do Estado do Rio de Janeiro.

Orientadora: Profª Dra. Patrícia Nunes da Silva

Rio de Janeiro

2014

CATALOGAÇÃO NA FONTE
UERJ / REDE SIRIUS / BIBLIOTECA CTC-A

I16 Ichihara, José Travassos.
Construção de quadrados mágicos pelo método do passo uniforme / José Travassos Ichihara. – 2014.
100 f. : il.

Orientadora: Patrícia Nunes da Silva.
Dissertação (Mestrado Profissional em Matemática em Rede Nacional / PROFMAT) - Universidade do Estado do Rio de Janeiro, Instituto de Matemática e Estatística.

1. Teoria dos números. 2.Quadrados mágicos. I. Silva, Patrícia Nunes da. II. Universidade do Estado do Rio de Janeiro. Instituto de Matemática e Estatística. III. Título.

CDU 512.12

_____ _____

Assinatura Data

José Travassos Ichihara

Construção de quadrados mágicos pelo método do passo uniforme

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), da Universidade do Estado do Rio de Janeiro.

Aprovada em 27 de Novembro de 2014.
Banca Examinadora:

Profª Dra. Patrícia Nunes da Silva (Orientadora)
Instituto de Matemática e Estatística – UERJ

Prof. Dr. Silas Fantin
Departamento de Matemática e Estatística – UNIRIO

Prof. Dr. Roberto Alfonso de Olivares Jara
Instituto de Matemática e Estatística – UERJ

Rio de Janeiro
2014

DEDICATÓRIA

Ao meu pai Toshio (in memoriam), à minha mãe Danza.

AGRADECIMENTOS

Agradeço aos meus pais Toshio e Danza por terem me passado muitos valores entre eles o valor do conhecimento e da sabedoria.

Agradeço às amigas Fátima de Azevedo e Fátima Neto por terem sido o estopim e a força impulsionadora para fazer o PROFMAT na UERJ.

Agradeço a CAPES pela bolsa que me ajudou a custear despesas e necessidades que foram surgindo desde o início do mestrado até a conclusão deste trabalho.

Agradeço ao amigo Luis Oliveira, colega de profissão e amigo de longa data com o qual tenho compartilhado as muitas alegrias e as eventuais tristezas da profissão, pela paciente escuta e troca.

Agradeço aos amigos da minha turma do PROFMAT em especial Marcos Assumpção pelos momentos de estudo e convivência fraterna.

Agradeço aos amigos e amigas do Focolare com o qual compartilho o Ideal da Unidade de Chiara Lubich.

Agradeço a todos os amigos que direta ou indiretamente me ajudaram de alguma forma a realizar este trabalho.

Agradeço aos meus irmãos e irmãs Carolina, Ana, Yury, Antônio e Telma e a todos os meus familiares aos quais sempre serei um reconhecido devedor.

Agradeço aos meus professores da UERJ envolvidos no PROFMAT que me ajudaram com suas aulas, atenção e comprometimento na realização desse objetivo.

Agradeço à professora Renata Abreu pelas preciosas dicas, pelo interesse em me ajudar.

Agradeço à minha orientadora Patrícia Nunes pela dedicação, pela paciência e entrega. Quando escolhi este tema, não foi pelo orientador como muitos fazem, nem mesmo pelo tema apesar do meu despertado interesse em Aritmética, mas foi sobretudo pela proposta de trabalho, a meu ver, pouco pedagógica e muito matemática. Mas, passados alguns meses, na conclusão deste TCC posso dizer que não podia ter escolhido melhor orientador.

O menino pergunta: “Vovô, é fácil pegar um tatu?” O avô, medita alguns segundos e responde: ”Antes de tudo, tem que ter o tatu!”

Fonte: O autor, 2014.

RESUMO

ICHIHARA, José Travassos. *Construção de quadrados mágicos pelo método do passo uniforme*. 2014. 100 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional / PROFMAT) – Universidade do Estado do Rio de Janeiro, Instituto de Matemática e Estatística.

Lehmer (1929) analisa matematicamente o método do passo uniforme para construção de quadrados mágicos de ordem ímpar. Ele divide sua análise em várias etapas. Na primeira delas, envolvendo a discussão de condições necessárias e suficientes para o preenchimento do quadrado pelo método, o autor afirma que se dois números guardarem entre si uma certa relação, eles serão designados a ocupar a mesma célula do quadrado causando seu não preenchimento. A análise do preenchimento pelo método do passo uniforme envolve a resolução de um sistema linear módulo n. Nesse trabalho, discutimos o comportamento das soluções desse sistema quando o método falha no preenchimento. Como consequência, concluímos que números que guardam a relação mencionada nunca ocupam a mesma célula. A análise das condições necessárias e suficientes para obter quadrados mágicos segundo a definição de Lehmer (1929) envolve a resolução de equações de congruências lineares a duas variáveis. Nesse trabalho, detalhamos os resultados de Lehmer (1929). A análise das condições necessárias e suficientes para obtenção de quadrados mágicos, como são reconhecidos usualmente, também envolve a resolução de equações de congruências lineares a duas variáveis. Discutimos o comportamento das soluções dessas equações para obter diagonais principais mágicas. Como consequência, mostramos que diagonais principais mágicas são obtidas se e somente se as coordenadas iniciais guardarem certas relações.

Palavras-chave: Quadrados mágicos. Método do passo uniforme. Regularidades.

ABSTRACT

ICHIHARA, José Travassos. *Construction of magic squares by the uniform step method.* 2014. 100 f. Dissertação (Mestrado profissional em Matemática em Rede Nacional / PROFMAT) – Universidade do Estado do Rio de Janeiro, Instituto de Matemática e Estatística.

Lehmer (1929) mathematically analyzes the uniform step method for constructing magic squares of odd order. He divides his analysis into several steps. In the first, involving a discussion of necessary and sufficient conditions for completing the square, the author states that if two numbers keep a certain relationship to each other, they will be designated to occupy the same cell of the square causing its non fullfillment. The analysis of the uniform step method involves solving a linear system module n. In this monograph, we discuss the behavior of solutions of this system when the method fails in fulfilling the square. Consequently, we conclude that numbers guarding the mentioned relationship never occupy the same cell. The analysis of necessary and sufficient conditions for obtaining magic square (as defined by Lehmer (1929)) involves solving linear congruences in two variables. In this work, we detail the results of Lehmer (1929). The analysis of the necessary and sufficient conditions for magic squares (as usually defined) also involves solving linear congruences in two variables. We discuss the behavior of solutions of these equations to obtain magic main diagonals. Then, we show that magic main diagonals are obtained if and only if the initial coordinates keep certain relationships.

Keywords: Magic squares. Uniform step method. Regularities.

LISTA DE ILUSTRAÇÕES

Figura 1 - Melancolia, gravura de 1514 de Albrecht Dürer 11
Figura 2 - Detalhe da gravura Melancolia 11
Figura 3 - Sistema de coordenadas (A, B) 17
Figura 4 - Quadrado de ordem n 17
Figura 5 - Cilindro de ordem n 18
Figura 6 - Toro de ordem n 18
Figura 7 - Inserção de 1 a 25 pelo MPU 20
Figura 8 - Matriz $M(w', k')$ 32
Figura 9 - Estrutura das matrizes do exemplo 2. 33
Figura 10 - Localização do número 133, $M(2, 3)$. 34
Figura 11 - $M(2, 3)$ do Ex. 3. 36
Figura 12 - Regularidades. 38
Figura 13 - Regularidades. 40
Figura 14 - Elementos e suas coordenadas, matriz $M(1, 1)$, do Exemplo 4. 42
Figura 15 - x_1 e x_2 em uma mesma coluna l de $M(w', k')$ tem coordenadas (A, B) diferentes. . 44
Figura 16 - x_1 e x_2 em uma mesma linha t de $M(w', k')$ tem coordenadas (A, B) diferentes. . . 44
Figura 17 - $M(2, 3)$ elementos e coordenadas. Exemplo 5. 45
Figura 18 - Elementos e suas coordenadas, da matriz $M(1, 1)$, do Exemplo 6. . . . 47
Figura 19 - Números de $M(2, 0)$ que ocupam a mesma célula que 138. 48
Figura 20 - Matriz$(2, 0)$, Exemplo 7. 49
Figura 21 - Ciclos do quadrado do Exemplo 7. 51
Figura 22 - Diagonais positivas. 61
Figura 23 - Diagonais negativas. 62
Figura 24 - $n = 9$, $\alpha = 4$, $\beta = 1$, $a = 5$, $b = 1$, $p = 2$ e $q = 4$. DPN não mágica. . . 72
Figura 25 - $n = 9$, $\alpha = 4$, $\beta = 1$, $a = 5$, $b = 1$. 73
Figura 26 - $n = 9$, $\alpha = 4$, $\beta = 1$, $a = 5$, $b = 1$. 83
Figura 27 - Coordenadas iniciais para DPP e DPN mágicas (parâmetros: $n = 55$, $\alpha = 7$, $\beta = 4$, $a = 6$, $b = 1$). 89
Figura 28 - Coordenadas iniciais para DPP e DPN mágicas (parâmetros: $n = 105$, $\alpha = 11$, $\beta = 2$, $a = 31$, $b = 11$). 92

SUMÁRIO

	INTRODUÇÃO	11
1	**RESULTADOS PRELIMINARES**	13
2	**REPRESENTAÇÃO MATEMÁTICA DE UM QUADRÁDO MÁGICO**	16
2.1	**Coordenadas das células**	17
3	**MÉTODO DO PASSO UNIFORME**	19
3.1	**Um Exemplo**	19
3.2	**Descrição e formalização do método**	20
3.3	**Congruências fundamentais do método do passo uniforme**	22
3.4	**Análise do método do passo uniforme**	24
4	**O MÉTODO PREENCHE O QUADRADO?**	25
4.1	**A condição suficiente para o preenchimento**	26
4.2	**Se preenche, o determinante é primo com n?**	27
4.2.1	A condição necessária para o preenchimento segundo Lehmer (1929)	29
4.2.1.1	O parágrafo de Lehmer (1929, p. 531)	29
4.2.2	O ponto crucial no caminho da volta	31
4.3	**Como ocorre o não preenchimento?**	32
4.3.1	Coordenadas dos elementos de $M(w', k')$	35
4.3.2	As coordenadas A' e B'	37
4.3.3	Regularidade das coordenadas A e B entre matrizes	37
4.3.4	Regularidade das coordenadas A e B ao longo de uma linha de $M(w', k')$	39
4.3.5	Regularidade das coordenadas A e B ao longo de uma coluna de $M(w', k')$	40
4.3.6	Padrão dos números em $M(w', k')$ que ocupam uma mesma célula no quadrado	43
4.3.7	Duas soluções de interesse que ocupam a mesma célula	46
5	**MÁGICO NAS COLUNAS OU LINHAS**	52
5.1	**A condição é necessária?**	53
5.1.1	Calculando a soma das colunas	53
5.1.2	Calculando a soma das linhas	57
5.1.3	Condição necessária para que colunas e linhas sejam mágicas	59
6	**DIAGONAIS PRINCIPAIS POSITIVA E NEGATIVA MÁGICAS**	61
6.1	**Condições para que a diagonal principal negativa seja mágica**	62
6.1.1	Calculando a soma da diagonal	64
6.1.2	Condição necessária e suficiente	66
6.1.3	Onde começar para que a DPN seja mágica?	68

6.2 **Condições para que a diagonal principal positiva seja mágica** . . . 76
6.2.1 Calculando a soma da diagonal . . . 77
6.2.2 Condição necessária e suficiente . . . 78
6.2.3 Onde começar para que a DPP seja mágica? . . . 79
6.3 **Onde começar para que a DPP e a DPN sejam ambas mágicas?** . 86
7 **MÉTODO DE LA LOUBÈRE** . . . 95
CONCLUSÃO . . . 99
REFERÊNCIAS . . . 100

INTRODUÇÃO

Na literatura, raramente encontram-se referências sobre quaisquer aplicações práticas para quadrados mágicos. Em geral, são objeto de curiosidade e diversão. No Brasil, os livros didáticos de matemática endereçados ao ensino fundamental costumam apresentar questões com quadrados mágicos de ordem 3. No entanto, os quadrados mágicos oferecem uma variedade interessante de propriedades matemáticas.

Um famoso exemplo de quadrado mágico aparece na gravura Melancolia de Albrecht Dürer (Figura 1). Sobre a parede atrás do anjo que pondera sobre o universo, vê-se um quadrado mágico de ordem 4 (Figura 2) que apresenta a mesma soma 34 em cada

Figura 1 - Melancolia, gravura de 1514 de Albrecht Dürer

Fonte: CHABERT; BARBIN, 1999.

Figura 2 - Detalhe da gravura Melancolia

Fonte: Adaptado de CHABERT; BARBIN, 1999.

linha, coluna e nas duas diagonais principais:

$$\begin{bmatrix} 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 12 \\ 4 & 15 & 14 & 1 \end{bmatrix}$$

A soma 34 também se verifica nas quatro casas centrais, nas quatros casas dos cantos, nas duas casas do meio da linha superior com as duas casas do meio da linha inferior, nas duas casas centrais da coluna da esquerda com as duas casas centrais da coluna da direita. Ainda, a data da gravura, 1514, aparece nas duas células centrais da linha inferior.

Há muitas maneiras de gerar quadrados mágicos. Existem vários métodos de construção. Quadrados de ordem ímpar são construídos com métodos diferentes dos quadrados de ordem par. Este trabalho tem como objetivo principal a análise matemática do método do passo uniforme para construção de quadrados mágicos que será descrito mais adiante. Estudaremos as condições necessárias e suficientes para garantir que um quadrado construído pelo método do passo uniforme seja mágico.

1 RESULTADOS PRELIMINARES

Apresentamos nessa seção alguns resultados e conceitos de Teoria dos Números que serão utilizados ao longo do trabalho.

Como em Hefez (2006), denotaremos por $\mathbb{N}$ o conjunto dos números naturais:

$$\mathbb{N} = \{0, 1, 2, \ldots\}$$

Definição 1. Dados dois números naturais a e b com $a \neq 0$, diremos que a divide b, escrevendo $a \mid b$, quando existir $c \in \mathbb{N}$ tal que $b = a \cdot c$. Neste caso, diremos também que a é um divisor ou um fator de b ou, ainda, que b é um múltiplo de a.

Observe que essa definição pode ser naturalmente estendida para os inteiros (ver Definição 1.1, (SANTOS, 1998), p. 3).

Teorema 1 (Divisão Euclidiana, Teorema 3.2.1 (HEFEZ, 2006, p. 35))**.** *Sejam a e b dois números naturais com $0 < a < b$. Existem dois únicos números naturais q e r tais que $b = a \cdot q + r$, com $r < a$.*

Definição 2 (Máximo Divisor Comum, (HEFEZ, 2006, p. 53))**.** Dizemos que d é um *máximo divisor comum* (mdc) de a e b se possuir as seguintes propriedades:

(i) d é um divisor comum de a e b, e

(ii) d é divisível por todo divisor comum de a e b.

Dados dois números naturais a e b, denotaremos seu máximo divisor comum por $\text{mdc}(a, b)$.

Teorema 2 (Teorema 5.2.2 (HEFEZ, 2006, p. 60))**.** *Sejam a, b e c números naturais. Se $a \mid b \cdot c$ e $\text{mdc}(a, b) = 1$, então $a \mid c$.*

Proposição 1 (Proposição 5.2.2 (HEFEZ, 2006, p. 61))**.** *Dados números naturais $a_1, \ldots, a_n$, não todos nulos, existe o seu* mdc *e*

$$\text{mdc}(a_1, \ldots, a_n) = \text{mdc}(a_1, \ldots, \text{mdc}(a_{n-1}, a_n))$$

Definição 3 (Definição 2.1 (SANTOS, 1998, p. 32))**.** Se a e b são inteiros dizemos que a é CONGRUENTE a b módulo m ($m > 0$) se $m \mid (a - b)$. Denotamos isto por $a \equiv b \pmod{m}$. Se $m \nmid (a - b)$, dizemos que a é INCONGRUENTE a b módulo m e denotamos $a \not\equiv b \pmod{m}$.

Proposição 2 (Proposição 9.1.1 (HEFEZ, 2006, p. 110)). *Seja $m \in \mathbb{N}$, com $m > 1$. Para todos $a, b, c \in \mathbb{N}$, tem-se que:*

(i) $a \equiv a \pmod{m}$,

(ii) Se $a \equiv b \pmod{m}$, *então* $b \equiv a \pmod{m}$,

(iii) Se $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m}$, *então* $a \equiv c \pmod{m}$.

Proposição 3 (Proposição 9.1.3 (HEFEZ, 2006, p. 111)). *Sejam a, b, c, d,* $m \in \mathbb{N}$, *com* $m > 1$,

(i) Se $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$, *então* $a + c \equiv b + d \pmod{m}$,

(ii) Se $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$, *então* $a \cdot c \equiv b \cdot d \pmod{m}$.

Proposição 4 (Do cancelamento aditivo, Proposição 9.1.4 (HEFEZ, 2006, p. 113)). *Sejam a, b, c,* $m \in \mathbb{N}$, *com* $m > 1$. *Tem-se que*

$$a + c \equiv b + c \pmod{m} \iff a \equiv b \pmod{m}.$$

Proposição 5 (Do cancelamento multiplicativo, Proposição 9.1.5 (HEFEZ, 2006, p. 114)). *Sejam a, b, c,* $m \in \mathbb{N}$, *com* $c \neq 0$ *e* $m > 1$. *Temos que*

$$a \cdot c \equiv b \cdot c \pmod{m} \iff a \equiv b \pmod{\frac{m}{\mathrm{mdc}(c, m)}}.$$

Corolário 1 (HEFEZ, p. 114). *Sejam a, b, c,* $m \in \mathbb{N}$, *com* $m > 1$ *e* $\mathrm{mdc}(c, m) = 1$. *Temos que*

$a \cdot c \equiv b \cdot c \pmod{m} \Leftrightarrow a \equiv b \pmod{m}$.

Observamos que todos os resultados de congruência enunciados para naturais também são válidos para inteiros (veja Capítulo 2, (SANTOS, 1998)).

Definição 4. Chamamos de equação de congruência linear (ECL) na variável $x \in \mathbb{Z}$ a uma congruência na forma $ax \equiv b \pmod{m}$, onde x é a incógnita.

Teorema 3 (Existência e quantidade de soluções da ECL, Teorema 2.8 (SANTOS, 1998, p. 37)). *Se* $d = \mathrm{mdc}(a, m)$ *e* $d \mid b$, *então a equação* $ax \equiv b \pmod{m}$ *tem d soluções incongruentes* $\bmod m$.

Teorema 4 (ECL em uma variável, prova do Teorema 2.8 (SANTOS, 1998, p. 37)). *Sejam a, c,* $m \in \mathbb{N}$, *com* $m > 1$ *e* $\mathrm{mdc}(c, m) \mid c$. *Se* x_0 *é a solução minimal (isto é, a menor solução não negativa) da congruência* $ax \equiv c \pmod{m}$, *então*

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d},$$

onde $d = \mathrm{mdc}(a, m)$, *são as soluções incongruentes* $\bmod m$ *da ECL.*

Definição 5 (Seção 5.5 (SIVARAMAKRISHNAN, 2006, p. 124))**.** Uma ECL em n variáveis $x_1, x_2, \ldots, x_n$ é da forma

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{m}, \tag{1}$$

$b, m, a_i \in \mathbb{Z}, i = 1, 2, \ldots, n$ e $m > 1$. Uma n-upla $(x_1, x_2, \ldots, x_n)$ que satisfaz (1) será chamada de solução de (1). Duas soluções $(x_1, x_2, \ldots, x_n)$ e $(x'_1, x'_2, \ldots, x'_n)$ serão contadas como a mesma solução se, e somente se,

$$x_i \equiv x'_i \pmod{m}, \quad i = 1, \ldots, n.$$

Teorema 5 (Existência de soluções de uma ECL com n variáveis, Theorem 36 (SIVARAMAKRISHNAN, 2006, p. 124))**.** *A congruência linear* $a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{m}$ *tem solução se, e somente se,* $\text{mdc}(a_1, a_2, \ldots, a_n, m) \mid b$.

Teorema 6 (Número de soluções de uma ECL com n variáveis, Theorem 36 (SIVARAMAKRISHNAN, 2006, p. 124))**.** *A congruência linear* $a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{m}$*, com* $\text{mdc}(a_1, a_2, \ldots, a_n, m) = d \mid b$ *tem* $d \cdot m^{n-1}$ *soluções distintas.*

2 REPRESENTAÇÃO MATEMÁTICA DE UM QUADRÁDO MÁGICO

Para Lehmer (1929), um quadrado é denominado *"mágico" nas linhas* se a soma dos números em cada linha for a mesma. Será chamado de quadrado *"mágico" nas colunas* se a soma dos números em cada coluna for a mesma. Se um quadrado for mágico simultaneamente nas linhas e nas colunas será dito *"quadrado mágico"*. Um quadrado é reconhecido *"mágico nas diagonais positivas"* se a soma em cada diagonal estendida, paralela à diagonal principal, for a mesma soma da diagonal principal. Se for também *"mágico nas diagonais negativas"* será denominado *"diabólico"*. Um quadrado mágico é *"simétrico"* se a soma entre quaisquer duas células localizadas simetricamente em relação ao centro do quadrado for a mesma. As definições de Lehmer (1929) para quadrados mágicos serão adotadas nesse trabalho.

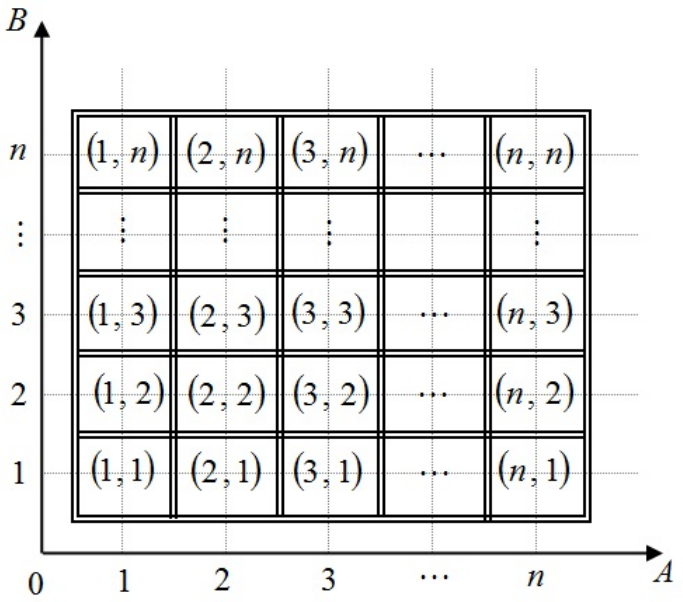
Para montar um quadrado mágico, uma matriz quadrada de ordem n deve ser preenchida, completamente, sem repetição, com os números naturais de 1 até n^2. Portanto, a soma de todos os elementos da matriz será a soma de uma progressão aritmética com $a_1 = 1$, $r = 1$, $a_{n^2} = n^2$ e n^2 elementos, que é igual a $^{(1+n^2)n^2}/_2$. Então se o quadrado for mágico a soma dos elementos de qualquer coluna ou linha será igual a esse valor dividido por n, teremos

$$\frac{(1+n^2)n}{2}. \tag{2}$$

2.1 **Coordenadas das células**

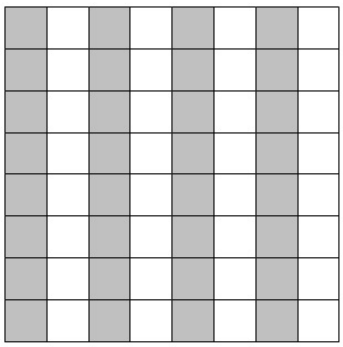
Cada célula do quadrado será identificada por suas coordenadas (A, B) que indicam respectivamente a coluna e a linha que ocupa (Figura 3) A primeira dificuldade a ser contornada na tentativa de preencher um quadrado de ordem n com algum método de passo regular, é a existência de um contorno. Em outras palavras movendo-se pelas células de uma linha para a esquerda ou para a direita ou pelas células de uma coluna para cima ou para baixo, vamos nos deparar com uma célula na borda que ultrapassada levará para fora do quadrado (Figura 4).

Figura 3 - Sistema de coordenadas (A, B)



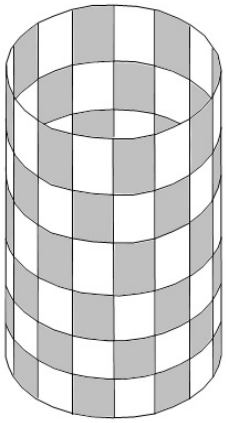
Fonte: O autor, 2014.

Figura 4 - Quadrado de ordem n



Fonte: O autor, 2014.

Figura 5 - Cilindro de ordem n



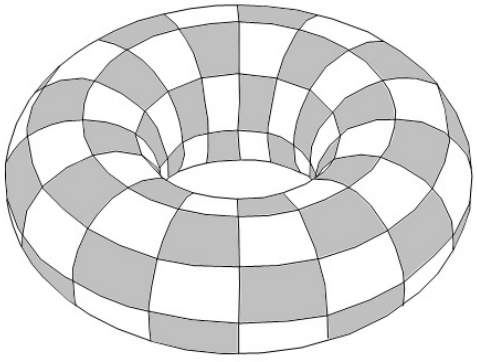
Fonte: O autor, 2014.

Uma solução seria colar as bordas direita e esquerda do quadrado obtendo-se um cilindro. Agora, movendo-se por uma linha qualquer para a direita ou para a esquerda não se sai mais do quadrado pois as células, não estão mais dispostas em um segmento de reta horizontal com duas extremidades mas dispostas de maneira circular (Figura 5).

De maneira análoga, as extremidades superior e inferior de cada coluna são coladas obtendo-se um toro. Assim, movendo-se por uma coluna qualquer para cima ou para baixo não se sai mais da matriz pois as células, não estão mais dispostas em um segmento de reta vertical com duas extremidades mas dispostas de maneira circular (Figura 6).

Algebricamente, o efeito "toro" de mover-se sem sair da matriz, é obtido tratando as coordenadas de cada célula da matriz como congruências módulo n, sendo n a ordem da matriz. Com efeito, o movimento de uma célula (p, q) para uma célula $(p+\alpha, q+\beta)$ sempre poderá ser associado, através de congruência módulo n, a uma célula de coordenadas com valores de 1 a n.

Figura 6 - Toro de ordem n



Fonte: O autor, 2014.

3 MÉTODO DO PASSO UNIFORME

Há muitas maneiras de gerar quadrados mágicos. Existem vários métodos de construção. Quadrados de ordem ímpar são construídos com métodos diferentes dos quadrados de ordem par. No presente trabalho vamos nos deter exclusivamente ao *método do passo uniforme* (MPU). Ele consiste em atribuir, um de cada vez, ordenadamente, a sequência dos números $1, 2, 3, ..., n^2$ às células seguindo uma regularidade de movimento para a direita e para cima que será detalhada a seguir.

3.1 Um Exemplo

No método do passo uniforme, inicia-se com o 1 sendo atribuído a uma célula qualquer (p, q). Em seguida, vem o 2, colocado na célula $(p+\alpha, q+\beta)$ sendo α o deslocamento ou "passo" para a direita e β o passo para cima[1]. Esses passos serão mantidos, por isso, α e β são chamadas de *constantes do passo uniforme*. Ao término de cada alocação de n números, será necessário fazer uma quebra de passo (através da introdução de parâmetros a e b) para evitar a sobreposição de números em uma mesma célula.

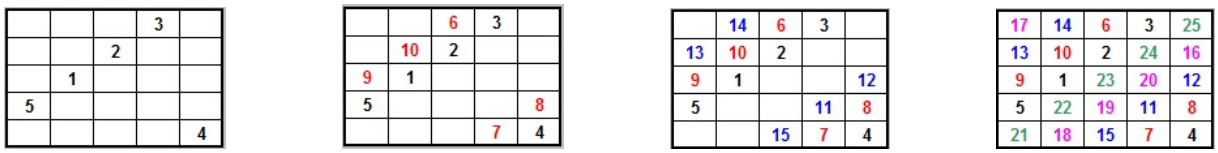
Exemplo 1. Seja o quadrado de ordem $n = 5$ construído pelo método do passo uniforme com os seguintes parâmetros: $\alpha = 1$, $\beta = 1$, $a = 1$, $b = 2$, $p = 2$ e $q = 3$.

O 1 é alocado na célula inicial $(p, q) = (2, 3)$, escolhida arbitrariamente, prossegue-se colocando 2 na célula situada 1 passo para a direita e um passo para cima, ou seja, $(2 + 1, 3 + 1) \equiv (3, 4)$. Da mesma forma, 3 é alocado em $(3 + 1, 4 + 1) \equiv (4, 5)$, 4 em $(4 + 1, 5 + 1) \equiv (5, 1)$ e 5 em $(5 + 1, 1 + 1) \equiv (1, 2)$, Figura 7a.

A primeira *quebra de passo* será requerida, ao término do 1º ciclo, na inserção de 6. De fato, partindo da coordenada $p = 2$ ao serem somados 5 passos horizontais $\alpha = 1$ voltaremos à coordenada 2, isto é, $2 + 5 \cdot 1 \equiv 2 \pmod 5$. Da mesma maneira, a partir da coordenada $q = 3$, acrescentados 5 passos verticais $\beta = 1$ volta-se à coordenada 3, ou seja, $3 + 5 \cdot 1 \equiv 3 \pmod 5$. Então, o método propõe uma *quebra de passo* que consiste em deslocar-se a passos para a direita e b passos para cima, isto é, somar $a = 1$ e $b = 2$, respectivamente, às coordenadas $p = 2$ e $q = 3$. O 2º ciclo, é iniciado, com a primeira quebra de passo introduzida, permitindo que o número 6 seja alocado não mais na célula $(2, 3)$ ocupada pelo 1 mas em uma outra célula, com coordenadas $(2 + 1, 3 + 2) \equiv (3, 5)$.

[1] Mais precisamente, os passos para a direita e para cima estão associados a parâmetros α e β positivos. No entanto, não há perda de generalidade em descrevermos apenas esse caso. Se α ou β for negativos, a congruência módulo n sempre permite redefini-los de modo que possam ser considerados positivos.

Figura 7 - Inserção de 1 a 25 pelo MPU



(a) (b) (c) (d)

Legenda: (a) 1º ciclo; (b) 2º ciclo; (c) 3º ciclo; (d) 4º e 5º ciclos.
Fonte: O autor, 2014.

Os números de 7 até 10 poderão, então, ser alocados fechando o 2º ciclo, Figura 7b. Esse procedimento se repete para o 3º ciclo, Figura 7c e prossegue com o 4º e 5º ciclos até que todos os 25 números tenham sido distribuídos, Figura 7d.

3.2 Descrição e formalização do método

No que segue, as coordenadas de cada célula sempre serão reduzidas módulo n, exceto quando forem igual a n, pois não existe coordenada igual a 0. Genericamente, inicia-se com o 1 sendo atribuído a uma célula qualquer (p, q). Em seguida, vem o 2, colocado na célula $(p+\alpha, q+\beta)$. Prosseguindo, temos: Ao final do 1º ciclo de n números (Tabela 1), a inserção de $n+1$ exigirá uma alteração no procedimento. De fato, partindo da coordenada p ao serem somados n passos horizontais α voltaremos à coordenada p, isto é, $p+n\alpha \equiv p \pmod{n}$. Da mesma maneira, a partir da coordenada q, acrescentados n passos verticais β volta-se à coordenada q, ou seja, $q+n\beta \equiv q \pmod{n}$. Portanto, após terem sido inseridos com sucesso os números $1, 2, 3, \ldots, n$ nos n primeiros passos, tropeçamos na inserção do número $n+1$, destinado a uma célula necessariamente já ocupada, pois $(p+n\alpha, q+n\beta) \equiv (p, q) \pmod{n}$, sendo (p, q) as coordenadas da célula

Tabela 1 - Alocação dos números no 1º ciclo

x	(A, B)
1	(p, q)
2	$(p+\alpha, q+\beta)$
3	$(p+2\alpha, q+2\beta)$
$\vdots$	$\vdots$
$n-1$	$(p+(n-2)\alpha, q+(n-2)\beta)$
n	$(p+(n-1)\alpha, q+(n-1)\beta)$

Fonte: O autor, 2014.

Tabela 2 - Alocação dos números no 2º ciclo

x	(A, B)
$n+1$	$(p+a, q+b)$
$n+2$	$(p+\alpha+a, q+\beta+b)$
$n+3$	$(p+2\alpha+a, q+2\beta+b)$
$\vdots$	$\vdots$
$n+(n-1)$	$(p+(n-2)\alpha+a, q+(n-2)\beta+b)$
$n+n$	$(p+(n-1)\alpha+a, q+(n-1)\beta+b)$

Fonte: O autor, 2014.

Tabela 3 - Alocação dos números no 3º ciclo

x	(A, B)
$2n+1$	$(p+2a, q+2b)$
$2n+2$	$(p+\alpha+2a, q+\beta+2b)$
$2n+3$	$(p+2\alpha+2a, q+2\beta+2b)$
$\vdots$	$\vdots$
$2n+(n-1)$	$(p+(n-2)\alpha+2a, q+(n-2)\beta+2b)$
$2n+n$	$(p+(n-1)\alpha+2a, q+(n-1)\beta+2b)$

Fonte: O autor, 2014.

ocupada pelo 1.

Então, o método propõe uma quebra de passo que consiste em somar as constantes a e b, respectivamente, às coordenadas p e q. O 2º ciclo, é iniciado, com a primeira quebra de passo introduzida, permitindo que o número $n+1$ seja alocado não mais na célula (p, q) ocupada pelo 1 mas em uma outra célula deslocada por a unidades para à direita e por b unidades para cima em relação a esta com coordenadas $(p+a, q+b)$
O restante dos números do 2º ciclo, de $n+1$ até $2n$ poderá, então, ser alocado como anteriormente.

Analogamente, uma segunda quebra de passo é requerida após a conclusão do 2º ciclo (Tabela 2). De fato, tendo já sido alocados os números $n+1, n+2, n+3, \ldots, 2n$ ao tentar alocar o número $2n+1$, como foram dados, novamente, n passos horizontais α e veticais β a partir da célula $(p+a, q+b)$ voltamos a ela novamente, uma vez que, $p+a+n\alpha \equiv p+a \pmod{n}$ e $q+b+n\beta \equiv q+b \pmod{n}$. Dessa forma, o número $2n+1$ seria destinado à célula $(p+\alpha, q+\beta)$ que já estaria ocupada pelo número $n+1$. Então, o método propõe uma segunda quebra de passo que é executada, alocando o número $2n+1$ na célula $(p+2a, q+2b)$. Segue-se, normalmente, a alocação dos restantes dos números do 3º ciclo (Tabela 3).

Tabela 4 - Alocação dos números no nº ciclo

x	(A, B)
$(n-1)n+1$	$(p+(n-1)a, q+(n-1)b)$
$(n-1)n+2$	$(p+\alpha+(n-1)a, q+\beta+(n-1)b)$
$(n-1)n+3$	$(p+2\alpha+(n-1)a, q+2\beta+(n-1)b)$
$\vdots$	$\vdots$
$(n-1)n+(n-1)$	$(p+(n-2)\alpha+(n-1)a, q+(n-2)\beta+(n-1)b)$
$(n-1)n+n$	$(p+(n-1)\alpha+(n-1)a, q+(n-1)\beta+(n-1)b)$

Fonte: O autor, 2014.

O n-ésimo ciclo pode ser visto na Tabela 4.

3.3 **Congruências fundamentais do método do passo uniforme**

Após a descrição do método do passo uniforme, Lehmer (1929) resume o processo descrito nas seguintes congruências fundamentais, para determinar as coordenadas (A, B) da célula na qual o número x deve ser alocado:

$$A \equiv p + \alpha\,(x-1) + a\left[\frac{x-1}{n}\right] \pmod{n}, \tag{3}$$

$$B \equiv q + \beta\,(x-1) + b\left[\frac{x-1}{n}\right] \pmod{n}, \tag{4}$$

onde $\left[\dfrac{x-1}{n}\right]$ indica a parte inteira da divisão de $x-1$ por n.

As congruências fundamentais são apresentadas por Lehmer (1929) sem nenhum detalhamento. Vimos na descrição do método do passo uniforme que o coeficiente de α e β "conta" a quantidade de passos. O coeficiente de a e b "conta" a quantidade de quebras de passos. De fato, após cada ciclo (n passos) há uma quebra de passo, sendo adicionada uma unidade ao coeficiente de a e b que se mantém constante durante o ciclo. Assim, no 1º ciclo, o coeficiente de a e b é 0. No 2º ciclo, o coeficiente é 1. No 3º ciclo, é 2 e assim sucessivamente. No n-ésimo ciclo, é $n-1$. Logo, em (3) e (4), $(x-1)$ é o "contador de passos" e $\left[\dfrac{x-1}{n}\right]$ é o "contador de quebra de passos".

Para entender melhor, a primeira coisa que iremos fazer é definir uma forma para o número x. O teorema da Divisão Euclidiana (Teorema 1, página 13) garante que um

número natural $x \in \{1, 2, 3, \ldots, n^2\}$ pode ser escrito, de uma única maneira, na forma

$$x = 1 + w + kn$$

com $0 \leq k, w \leq n - 1$. Segue que k é a parte inteira da divisão de $x - 1$ por n,

$$k = \left[\frac{x-1}{n}\right]$$

e que

$$w \equiv x - 1 \pmod{n}$$

Dessa forma, k é o quociente da divisão de $x - 1$ por n. E, w é o resto dessa divisão. Então, é imediato perceber que k assume o valor 0, enquanto w assume os valores $0, 1, 2, \ldots, n - 1$ para $x \in \{0, 1, 2, \ldots, n - 1\}$; k assume o valor 1, enquanto w assume, novamente, os valores $0, 1, 2, \ldots, n - 1$ para $x \in \{n, n + 1, n + 2, \ldots, 2n - 1\}$; k assume o valor 2, enquanto w assume, novamente, os valores $0, 1, 2, \ldots, n - 1$ para $x \in \{2n, 2n + 1, 2n + 2, \ldots, 3n - 1\}$ e, assim por diante.

Portanto, para $x = 1+w+kn$ e $x \in \{1, 2, 3, \ldots, n^2\}$, k e w assumem, por n vezes, os valores $\{0, 1, 2, 3, \ldots, n-1\}$. Mas, vimos que k e w variam no conjunto $\{0, 1, 2, 3, \ldots, n-1\}$ com "velocidades" diferentes. Fazendo uma analogia com um relógio (de 0 a $n - 1$), k seria o ponteiro das horas e w, o dos minutos. Assim, escrevendo x na forma $1 + w + kn$, w se identifica com o coeficiente de α e de β, e k se identifica com o coeficiente de a e de b.

Observação 1. Um número $x \in \{1, 2, \ldots, n^2\}$ pode sempre ser escrito, de modo único, na forma $x = 1+w+kn$, com $0 \leq k, w \leq n-1$, e alocado pelo método do passo uniforme na célula de coordenadas $(p + w\alpha + ka, q + w\beta + kb)$.

Esquematicamente[2]:

$$x = 1 + w + kn \mapsto (p + \alpha w + ak, q + \beta w + bk)$$

[2] Esta notação para o número x e suas coordenadas, não foi utilizada por Lehmer mas será empregada neste trabalho sempre que trouxer facilidade.

Mas, como $k = \left[\frac{x-1}{n}\right]$ e $w \equiv (x-1) \pmod{n}$, segue da Proposição 2, página 14:

$$p + \alpha w + ak \equiv p + \alpha(x-1) + a\left[\frac{x-1}{n}\right] \pmod{n}$$
$$q + \beta w + bk \equiv q + \beta(x-1) + b\left[\frac{x-1}{n}\right] \pmod{n}$$

As congruências (3) e (4) indicam que as coordenadas A e B de um número x no quadrado, dadas pelo método do passo uniforme, dependem apenas dos seis parâmetros α, β, a, b, p e q.

Na descrição que foi feita do método, a quebra do passo é requerida ao término de cada ciclo de n números. Isso é bem expresso nas congruências fundamentais (3) e (4) pelo "contador de ciclos" $\left[\frac{x-1}{n}\right]$. Mas, dependendo da escolha dos referidos parâmetros, é possível[3] que um número seja atribuído a uma célula já ocupada antes mesmo da quebra de passo, ou seja, antes de se completar n passos. Isso pode ocorrer no caso de algum dos parâmetros α, β, a e b não ser primo com n. Quando α, β, a e b são todos primos com n, um número só seria atribuído a uma célula já ocupada apenas ao final de cada ciclo de n passos.

3.4 **Análise do método do passo uniforme**

Até agora, usamos o conceito de congruência módulo n para formalizar matematicamente o método do passo uniforme: estabelecemos uma relação algébrica entre cada número x e as coordenadas da célula que será ocupada por ele. Note que essa formalização já nos permite determinar a posição de qualquer número sem que necessitemos posicionar todos os anteriores a ele. Vamos prosseguir nossa investigação matemática sobre o método respondendo a algumas perguntas. O método do passo uniforme se propõe a gerar quadrados mágicos. Para que ele funcione, uma condição inicial básica é que o procedimento por ele proposto garanta o preenchimento do quadrado. Por isso, iniciamos nossa investigação respondendo à pergunta: o método preenche o quadrado?

[3] Por exemplo: $n = 10$, $\alpha = 4$, $\beta = 2$, $a = 3$ e $b = 3$. Iniciamos com 1 na célula (1, 1), 2 na célula (5, 3), 3 na célula (9, 5), 4 na célula (3, 7), 5 na célula (7, 9), 6 na célula (1, 1) já ocupada pelo 1. A quebra de passo não evitará que o quadrado não seja preenchido.
Outro exemplo com n ímpar: $n = 9$, $\alpha = 3$, $\beta = 3$, $a = 2$ e $b = 1$. Iniciamos com 1 na célula (2, 3), 2 na célula (5, 6), 3 na célula (8, 9), 4 na célula (2, 3) já ocupada pelo 1. Novamente, a quebra de passo não evitará que o quadrado não seja preenchido.

4 O MÉTODO PREENCHE O QUADRADO?

O método do passo uniforme garante que nenhum número $1 \leq x \leq n^2$ caia fora do quadrado. Sendo assim, a única maneira do quadrado não ser preenchido pelo método é existirem dois números x_1 e x_2 que tenham a mesma coordenada (A, B). Vamos assumir esta condição.

Sejam x_1 e x_2, dois números do conjunto $\{1, 2, 3, \ldots, n^2\}$, alocados em um quadrado de ordem n pelo método do passo uniforme respectivamente nas células de coordenadas (A_1, B_1) e (A_2, B_2) dadas por (3) e (4).

Se x_1 e x_2 estão em uma mesma célula, temos $A_1 \equiv A_2 \pmod{n}$ e $B_1 \equiv B_2 \pmod{n}$. Isto é,

$$\begin{cases} p + \alpha\,(x_1 - 1) + a\left[\dfrac{x_1 - 1}{n}\right] \equiv p + \alpha\,(x_2 - 1) + a\left[\dfrac{x_2 - 1}{n}\right] & (\text{mod } n) \\ \\ q + \beta\,(x_1 - 1) + b\left[\dfrac{x_1 - 1}{n}\right] \equiv q + \beta\,(x_2 - 1) + b\left[\dfrac{x_2 - 1}{n}\right] & (\text{mod } n) \end{cases}$$

Pela Proposição 4 (página 14), efetuamos os devidos cancelamentos aditivos, obtendo:

$$\begin{cases} \alpha\,(x_1 - x_2) + a\left\{\left[\dfrac{x_1 - 1}{n}\right] - \left[\dfrac{x_2 - 1}{n}\right]\right\} \equiv 0 \pmod{n} & (5) \\ \beta\,(x_1 - x_2) + b\left\{\left[\dfrac{x_1 - 1}{n}\right] - \left[\dfrac{x_2 - 1}{n}\right]\right\} \equiv 0 \pmod{n} & (6) \end{cases}$$

Os procedimentos a seguir são justificados pela Proposição 3 (página 14). Multiplicamos a equação (5) por b, a equação (6) por a e subtraimos uma da outra.

$$(\alpha b - \beta a)\,(x_1 - x_2) \equiv 0 \pmod{n}$$

Multiplicamos a equação (5) por β, a equação (6) por α e subtraimos uma da outra.

$$(\alpha b - \beta a)\left\{\left[\frac{x_1 - 1}{n}\right] - \left[\frac{x_2 - 1}{n}\right]\right\} \equiv 0 \pmod{n}$$

Portanto, chegamos ao sistema abaixo, que é determinado pela condição de dois números x_1 e x_2 ocuparem a mesma célula, pelo método do passo uniforme.

$$\begin{cases} (\alpha b - \beta a)\,(x_1 - x_2) \equiv 0 \pmod{n} & (7) \\ (\alpha b - \beta a)\left\{\left[\dfrac{x_1 - 1}{n}\right] - \left[\dfrac{x_2 - 1}{n}\right]\right\} \equiv 0 \pmod{n} & (8) \end{cases}$$

4.1 A condição suficiente para o preenchimento

Vamos mostrar que se $\text{mdc}(\alpha b - \beta a, n) = 1$, então o método do passo uniforme preenche o quadrado. De fato, se $\text{mdc}(\alpha b - \beta a, n) = 1$, então, pelo Colorário 1 (página 14), temos:

$$\begin{cases} x_1 \equiv x_2 \pmod{n} & (9) \\ \left[\frac{x_1 - 1}{n}\right] \equiv \left[\frac{x_2 - 1}{n}\right] \pmod{n} & (10) \end{cases}$$

Segue de (10) e da Defnição 3 na página 13 que:

$$\left[\frac{x_1 - 1}{n}\right] \equiv \left[\frac{x_2 - 1}{n}\right] \pmod{n} \Leftrightarrow n \mid \left[\frac{x_1 - 1}{n}\right] - \left[\frac{x_2 - 1}{n}\right].$$

Temos:

$$n \mid \left[\frac{x_1 - 1}{n}\right] - \left[\frac{x_2 - 1}{n}\right] \Leftrightarrow k_1 = k_2 + tn, \quad t \in \mathbb{Z}$$

onde $x_1 = 1 + w_1 + k_1 n$ e $x_2 = 1 + w_2 + k_2 n$. Uma vez que $0 \leq k_1, k_2 \leq n - 1$, então[4] $t = 0$ e

$$k_1 = k_2. \tag{11}$$

Analogamente, segue de (9) que

$$x_1 \equiv x_2 \pmod{n} \Leftrightarrow x_1 = x_2 + ln, \quad l \in \mathbb{Z}$$

Substituindo, $x_1 = 1 + w_1 + k_1 n$ e $x_2 = 1 + w_2 + k_2 n$, na igualdade $x_1 = x_2 + ln$, e considerando a igualdade (11), obtemos:

$$1 + w_1 + k_1 n = 1 + w_2 + k_2 n + ln \Leftrightarrow w_1 = w_2 + ln, \quad l \in \mathbb{Z}$$

Uma vez que $0 \leq w_1, w_2 \leq n - 1$, então $l = 0$ e $w_1 = w_2$.
Esses resultados, $k_1 = k_2$ e $w_1 = w_2$, mostram que

$$x_1 = 1 + w_1 + k_1 n = 1 + w_2 + k_2 n = x_2.$$

[4] (11) mostra que x_1 e x_2 são de um mesmo ciclo n.

Isto é, se $\text{mdc}(\alpha b - \beta a, n) = 1$, dois números não poderão ser alocados em uma mesma célula, pelo método do passo uniforme, a não ser que sejam iguais. Ora, nesse caso o método preenche o quadrado[5].

Teorema 7 (Condição suficiente para o preenchimento)**.** *Dados os parâmetros α, β, a e b (números inteiros) a condição suficiente para que o método do passo uniforme preencha o quadrado de ordem n é que o determinante* $\begin{vmatrix} \alpha & a \\ \beta & b \end{vmatrix}$ *seja primo com n.*

Recapitulando: Até aqui, vimos que para preencher o quadrado pelo método do passo uniforme é suficiente escolher os parâmetros α, β, a e b tais que $\begin{vmatrix} \alpha & a \\ \beta & b \end{vmatrix} = \alpha b - \beta a$ seja primo com n. Ou seja, se o determinante $\alpha b - \beta a$ for primo com n o quadrado preenche. Observamos, que não são relevantes para o preenchimento, as coordenadas da célula inicial que alocará o 1. Tanto faz. Além disso, não é necessário que os parâmetros α, β, a e b sejam primos[6] com n. Antes de dar prosseguimento, vamos nos deter um pouco, diante da pergunta natural que se põe agora: se o método preenche o quadrado então o determinante $\alpha b - \beta a$ é primo com n?

4.2 Se preenche, o determinante é primo com n?

A proposição "Se o quadrado é preenchido, então o determinante $\alpha b - \beta a$ é primo com n." é equivalente à sua contrapositiva "Se o determinante $\alpha b - \beta a$ não é primo com n, então o quadrado não é preenchido". Aqui, vamos tomar a contrapositiva.

A condição necessária de dois números x_1 e x_2 ocuparem uma mesma célula, está determinada pelo sistema (7)–(8). Evidente que se n e $(\alpha b - \beta a)$ têm um divisor comum $\delta \neq 1$, efetuando-se o cancelamente multiplicativo, vamos obter o seguinte sistema equivalente a (7)–(8):

$$\begin{cases} x_1 \equiv x_2 \left(\text{mod } \dfrac{n}{\delta}\right) & (12) \\ \left[\dfrac{x_1 - 1}{n}\right] \equiv \left[\dfrac{x_2 - 1}{n}\right] \left(\text{mod } \dfrac{n}{\delta}\right) & (13) \end{cases}$$

[5] Em cada coluna ou linha, tanto w quanto k assumirão os valores de um sistema completo de resíduos módulo n.

[6] Em seu artigo, ao estabelecer uma condição necessária e suficiente para o preenchimento, Lehmer (1929) supõe que α, β, a e b sejam primos com n. No entanto, ao provar que essa condição é suficiente, ele não faz uso dessa hipótese.

Por $k \equiv \left[\frac{x-1}{n}\right]$, a equação $\left[\frac{x_1-1}{n}\right] \equiv \left[\frac{x_2-1}{n}\right] \left(\mathrm{mod}\ \frac{n}{\delta}\right)$ pode ser reescrita:

$k_1 \equiv k_2 \left(\mathrm{mod}\ \frac{n}{\delta}\right)$

De acordo com $x = 1 + w + kn$, a equação $x_1 \equiv x_2 \left(\mathrm{mod}\ \frac{n}{\delta}\right)$ pode ser escrita:

$1 + w_1 + k_1 n \equiv 1 + w_2 + k_2 n \quad \left(\mathrm{mod}\ \frac{n}{\delta}\right)$
$w_1 + k_1 \left(\delta \cdot \frac{n}{\delta}\right) \equiv w_2 + k_2 \left(\delta \cdot \frac{n}{\delta}\right) \quad \left(\mathrm{mod}\ \frac{n}{\delta}\right)$
$w_1 \equiv w_2 \left(\mathrm{mod}\ \frac{n}{\delta}\right)$

O sistema (12)–(13) pode, então, ser reescrito:

$$\begin{cases} w_1 \equiv w_2 \left(\mathrm{mod}\ \frac{n}{\delta}\right) & (14) \\ k_1 \equiv k_2 \left(\mathrm{mod}\ \frac{n}{\delta}\right) & (15) \end{cases}$$

Como queremos investigar números $x_1, x_2 \in \{1, 2, \ldots, n^2\}$ que ocupam a mesma célula no quadrado, estamos interessados em soluções de (12)–(13) tais que

$x_j = 1 + w_j + k_j n \in \{1, 2, \ldots, n^2\}$.

Vamos nos referir a tais soluções como *soluções de interesse*. Faremos o mesmo com soluções (w_1, k_1) e (w_2, k_2) do sistema (14)–(15) correspondentes respectivamente a x_1, x_2. Obviamente, duas soluções de interesse w_1 e w_2 de (14) deixam o mesmo resto w' na divisão por $\frac{n}{\delta}$. De um modo geral, as soluções de interesse de (14) são dadas por

$$w = w' + l \cdot \frac{n}{\delta} \tag{16}$$

com $0 \leq l \leq \delta - 1$ e $0 \leq w' \leq \frac{n}{\delta} - 1$. Observe que, se $l \geq \delta$ então $w \geq n$, o que é um absurdo, pois $0 \leq w \leq n - 1$, página 23, Observação 1.

Analogamente, as soluções de interesse de (15) são dadas por

$k = k' + t \cdot \frac{n}{\delta}$

com $0 \leq t \leq \delta - 1 \quad$ e $\quad 0 \leq k' \leq \frac{n}{\delta} - 1$. Portanto, as soluções de interesse do sistema

(12)–(13) são dadas por

$$x = 1 + w' + k'n + l \cdot \frac{n}{\delta} + t \cdot \frac{n^2}{\delta} \tag{17}$$

com w' e k' varrendo o conjunto de resíduos[7] módulo $\frac{n}{\delta}$, l e t varrendo o conjunto de resíduos[8] módulo δ. Para obter a condição necessária para o preenchimento, resta exibir $x_1 \neq x_2$ dados por (17) que sejam soluções de (5)–(6), isto é, que ocupem a mesma célula, o que será feito na Subseção 4.3.7.

4.2.1 A condição necessária para o preenchimento segundo Lehmer (1929)

Nesta seção, após a descrição do método do passo uniforme, do estabelecimento das suas congruências fundamentais e do teorema da condição suficiente para o preenchimento, vamos discutir um parágrafo, da página 531, do artigo de Lehmer (1929) que trata da prova de sua condição necessária.

Teorema 8 (Condição necessária para o preenchimento – Lehmer)**.** *Dados os parâmetros α, β, a e b, primos com n, a condição necessária para que o método do passo uniforme preencha o quadrado de ordem n é que o determinante* $\begin{vmatrix} \alpha & a \\ \beta & b \end{vmatrix}$ *seja primo com n.*

Para Lehmer (1929), a condição necessária para o preenchimento requer, além da condição $\text{mdc}(\alpha b - \beta a, n) = 1$, também a primalidade dos parâmetros α, β, a e b com n.

4.2.1.1 O parágrafo de Lehmer (1929, p. 531)

Se[9] o $\text{mdc}(\alpha b - \beta a, n) = \delta$, então

$$\left[\frac{x_1 - 1}{n}\right] \equiv \left[\frac{x_2 - 1}{n}\right] \left(\text{mod } \frac{n}{\delta}\right)$$

[7] $w', k' \in \{0, 1, 2, \ldots, \frac{n}{\delta} - 1\}$.

[8] $l, t \in \{0, 1, 2, \ldots, \delta - 1\}$.

[9] *tradução livre de:* If however n and $(\alpha b - \beta a)$ have a common divisor δ then we have $\left[\frac{x_1-1}{n}\right] \equiv \left[\frac{x_2-1}{n}\right] \left(\text{mod } \frac{n}{\delta}\right)$ and $x_1 \equiv x_2 \left(\text{mod } \frac{n}{\delta}\right)$. If then we put $x_2 = x_1 + \left(\frac{n}{\delta}\right) n$ this last congruence is satisfied. Put this value of x_2 in the other congruence and we have $\left[\frac{x_1-1}{n}\right] \equiv \left[\frac{x_1-1}{n} + \frac{n}{\delta}\right] \left(\text{mod } \frac{n}{\delta}\right)$ and since $\frac{n}{\delta}$ is an integer the congruence is clearly satisfied. Two values of x which differ by $\frac{n^2}{\delta}$ will then fall in the same cell by this rule for filling the square and the square will therefore not be filled.

> e $x_1 \equiv x_2 \left(\mathrm{mod}\ \frac{n}{\delta}\right)$. Se consideramos então $x_2 = x_1 + \left(\frac{n}{\delta}\right) n$ a última congruência se verifica. Substitua esse valor de x_2 na outra congruência e obtenha
>
> $$\left[\frac{x_1 - 1}{n}\right] \equiv \left[\frac{x_1 - 1}{n} + \frac{n}{\delta}\right] \left(\mathrm{mod}\ \frac{n}{\delta}\right).$$
>
> Como $\frac{n}{\delta}$ é um inteiro, a congruência claramente se verifica. Dois valores de x que difiram por $\frac{n^2}{\delta}$ serão alocados pelo método do passo uniforme na mesma célula e o quadrado não será preenchido. (LEHMER, 1929, p. 531).

Lehmer (1929) assume que os parâmetros do método do passo uniforme, α, β, a, b sejam todos primos com n e ainda que o $\mathrm{mdc}(\alpha b - \beta a, n) = \delta \neq 1$. Lehmer (1929) exibe duas soluções $x_1 - x_2 = \dfrac{n^2}{\delta}$ que satistazem (12)-(13) e afirma que vão cair na mesma célula e por isto o quadrado não será preenchido. Essa afirmação é equivocada pois duas soluções $x_1 - x_2 = \dfrac{n^2}{\delta}$ não satisfazem (5)-(6), como mostrado a seguir:

$$\begin{cases} \alpha\left(\dfrac{n^2}{\delta}\right) + a\left\{\left[\dfrac{x_2 - 1}{n} + \dfrac{n}{\delta}\right] - \left[\dfrac{x_2 - 1}{n}\right]\right\} \equiv 0 \pmod{n} \\ \beta\left(\dfrac{n^2}{\delta}\right) + b\left\{\left[\dfrac{x_2 - 1}{n} + \dfrac{n}{\delta}\right] - \left[\dfrac{x_2 - 1}{n}\right]\right\} \equiv 0 \pmod{n} \end{cases}$$

Como $\dfrac{n}{\delta}$ é inteiro, segue:

$$\begin{cases} \alpha n\left(\dfrac{n}{\delta}\right) + a\left(\dfrac{n}{\delta}\right) \equiv 0 \pmod{n} \\ \beta n\left(\dfrac{n}{\delta}\right) + b\left(\dfrac{n}{\delta}\right) \equiv 0 \pmod{n} \end{cases}$$

$$\begin{cases} a\left(\dfrac{n}{\delta}\right) \equiv 0 \pmod{n} \\ b\left(\dfrac{n}{\delta}\right) \equiv 0 \pmod{n} \end{cases}$$

Como $(a, n) = (b, n) = 1$, temos $\dfrac{n}{\delta} \equiv 0 \pmod{n}$ que é falso!

Diferentemente das equações algébricas, multiplicando-se congruências lineares com duas variáveis módulo n, por um número não primo com n, soluções espúrias podem ser introduzidas. Dividindo-se congruências lineares com duas variáveis módulo n, por um número não primo com n, soluções podem ser perdidas. Por exemplo, $4x+2y \equiv 0 \pmod{6}$ tem 12 soluções: $(0,0), (1,1), (2,2), (3,3), (4,4), (5,5), (0,3), (3,0), (4,1), (1,4), (5,2), (2,5)$. Dividindo-se por 2, obtém-se a equação $2x + y \equiv 0 \pmod{3}$ que tem apenas 3 soluções: $(0,0), (1,1), (2,2)$. Porém, multiplicando-se ou dividindo-se congruências lineares módulo n, por um número primo com n, não se perdem nem se ganham soluções. O fato de Lehmer (1929) ter pensado que podia voltar, ou seja, que as duas soluções apresentadas de

(12)-(13) são também soluções de (5)-(6), nos levou a fazer uma análise das implicações dos caminhos de ida e de volta.

4.2.2 O ponto crucial no caminho da volta

O ponto crucial na prova da condição necessária encontra-se na passagem, de (5)-(6) para (7)-(8), onde as equações lineares foram multiplicadas pelos parâmetros α, β, a e b presumidamente primos. Logo, nessa passagem não haveria ganho nem perda de soluções, portanto haveria uma equivalência. No entanto, voltando, de (7)-(8) para (5)-(6) observamos algo que nos surpreendeu. Vamos, adotar aqui, a notação com $w's$ e $k's$. O sistema (7)-(8) pode ser reescrito como

$$\begin{cases} (\alpha b - \beta a)(w_1 - w_2) \equiv 0 \pmod{n} & (18) \\ (\alpha b - \beta a)(k_1 - k_2) \equiv 0 \pmod{n} & (19) \end{cases}$$

e é equivalente a

$$\begin{cases} b[\alpha(w_1 - w_2) + a(k_1 - k_2)] - a[\beta(w_1 - w_2) + b(k_1 - k_2)] \equiv 0 \pmod{n} & (20) \\ \alpha[\beta(w_1 - w_2) + b(k_1 - k_2)] - \beta[\alpha(w_1 - w_2) - a(k_1 - k_2) \equiv 0 \pmod{n} & (21) \end{cases}$$

Multiplicando (20) por α e (21) por a e somando, vamos obter:

$$(\alpha b - \beta a)[\alpha(w_1 - w_2) + a(k_1 - k_2)] \equiv 0 \pmod{n}$$

Multiplicando (20) por β e (21) por b e somando, vamos obter:

$$(\alpha b - \beta a)[\beta(w_1 - w_2) + b(k_1 - k_2)] \equiv 0 \pmod{n}$$

Portanto, o sistema (18)-(19) implica em:

$$\begin{cases} (\alpha b - \beta a)[\alpha(w_1 - w_2) + a(k_1 - k_2)] \equiv 0 \pmod{n} \\ (\alpha b - \beta a)[\beta(w_1 - w_2) + b(k_1 - k_2)] \equiv 0 \pmod{n} \end{cases}$$

Se $\alpha b - \beta a$ for primo com n então:

$$\begin{cases} \alpha(w_1 - w_2) + a(k_1 - k_2) \equiv 0 \pmod{n} \\ \beta(w_1 - w_2) + b(k_1 - k_2) \equiv 0 \pmod{n} \end{cases}$$

Portanto, o que impede a equivalência entre os sistemas (5)-(6) e (7)-(8) é apenas, a não primalidade, do determinante $\alpha b - \beta a$ com n. Veremos que a condição necessária e suficiente do preenchimento do quadrado pelo método do passo uniforme depende unicamente da primalidade do determinante e não exige a primalidade dos parâmetros com n diferentemente do que havia estabelecido Lehmer (1929).

Afirmamos que é possivel haver dois números x_1 e x_2 que satisfaçam as congruências do sistema (12)–(13) mas não ocupem a mesma célula do quadrado. Em vista disso, antes de dar prosseguimento, achamos importante nos deter um pouco, para entender como se configura, o não preenchimento pelo método do passo uniforme.

4.3 Como ocorre o não preenchimento?

Vimos na página 29, que as soluções de interesse do sistema (12)-(13) são números da forma

$$x = x' + l \cdot \frac{n}{\delta} + t \cdot \frac{n^2}{\delta}, \qquad 0 \leq l,\ t \leq \delta - 1,$$

sendo $x' = 1 + w' + k'n$, com $0 \leq w',\ k' \leq \frac{n}{\delta} - 1$. Fixados w' e k', estes números podem ser dispostos em δ linhas e δ colunas, Figura 8, formando uma matriz $M(w', k')$. Mais precisamente, para $0 \leq w',\ k' \leq \frac{n}{\delta} - 1$, temos

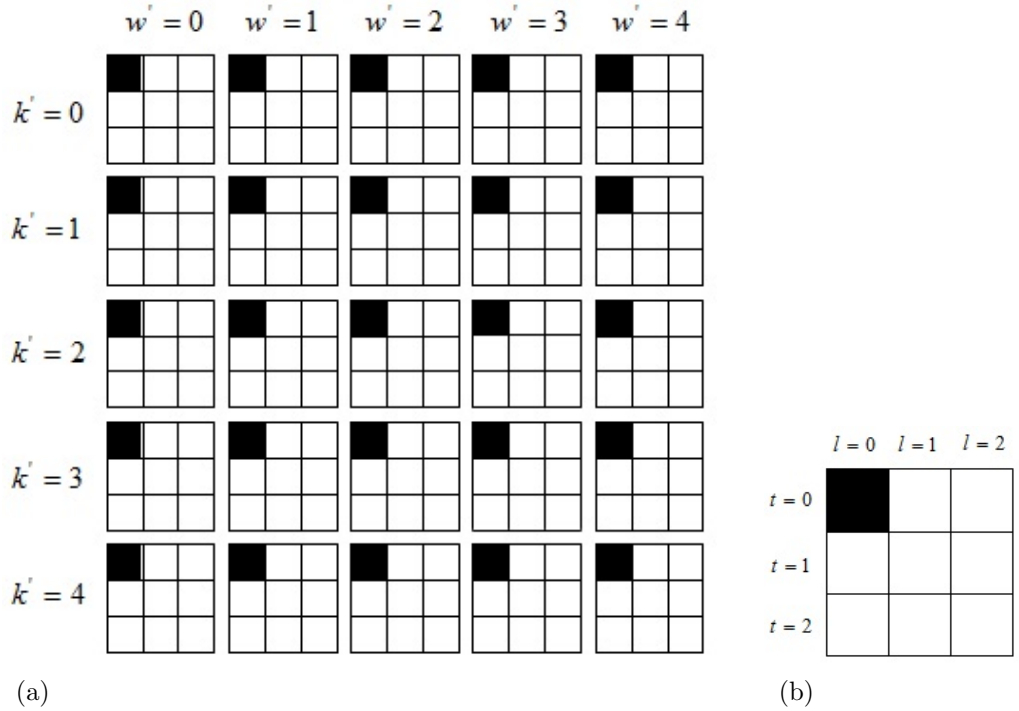
$$M(w', k') = (m_{t+1,l+1}), \quad m_{t+1,l+1} = x_{tl} = x' + l \cdot \frac{n}{\delta} + t \cdot \frac{n^2}{\delta}, \qquad 0 \leq l,\ t \leq \delta - 1$$

Figura 8 - Matriz $M(w', k')$

t \ l	0	1	2	$\cdots$	$\delta - 1$
0	$x' + 0 \cdot \frac{n}{\delta} + 0 \cdot \frac{n^2}{\delta}$	$x' + 1 \cdot \frac{n}{\delta} + 0 \cdot \frac{n^2}{\delta}$	$x' + 2 \cdot \frac{n}{\delta} + 0 \cdot \frac{n^2}{\delta}$	$\cdots$	$x' + (\delta - 1) \cdot \frac{n}{\delta} + 0 \cdot \frac{n^2}{\delta}$
1	$x' + 0 \cdot \frac{n}{\delta} + 1 \cdot \frac{n^2}{\delta}$	$x' + 1 \cdot \frac{n}{\delta} + 1 \cdot \frac{n^2}{\delta}$	$x' + 2 \cdot \frac{n}{\delta} + 1 \cdot \frac{n^2}{\delta}$	...	$x' + (\delta - 1) \cdot \frac{n}{\delta} + 1 \cdot \frac{n^2}{\delta}$
2	$x' + 0 \cdot \frac{n}{\delta} + 2 \cdot \frac{n^2}{\delta}$	$x' + 1 \cdot \frac{n}{\delta} + 2 \cdot \frac{n^2}{\delta}$	$x' + 2 \cdot \frac{n}{\delta} + 2 \cdot \frac{n^2}{\delta}$	$\cdots$	$x' + (\delta - 1) \cdot \frac{n}{\delta} + 2 \cdot \frac{n^2}{\delta}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
$\delta - 1$	$x' + 0 \cdot \frac{n}{\delta} + (\delta - 1) \cdot \frac{n^2}{\delta}$	$x' + 1 \cdot \frac{n}{\delta} + (\delta - 1) \cdot \frac{n^2}{\delta}$	$x' + 2 \cdot \frac{n}{\delta} + (\delta - 1) \cdot \frac{n^2}{\delta}$	$\cdots$	$x' + (\delta - 1) \cdot \frac{n}{\delta} + (\delta - 1) \cdot \frac{n^2}{\delta}$

Fonte: O autor, 2014.

Figura 9 - Estrutura das matrizes do exemplo 2.



Legenda: (a) 25 matrizes $M(w', k')$, 3×3.
(b) $M(w', k')$, 3×3.
Fonte: O autor, 2014.

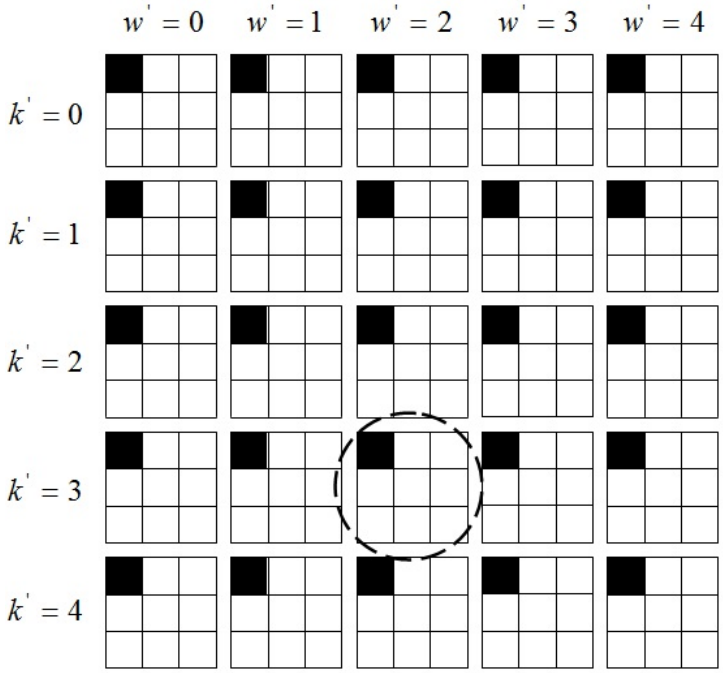
Segue que o conjunto de soluções de interesse do sistema (12)-(13) será constituído por $\left(\frac{n}{\delta}\right)^2$ matrizes, cada uma definida por um w' e um k' tais que $0 \leq w', k' \leq \frac{n}{\delta} - 1$, tendo cada uma δ^2 números.

A este ponto, somos capazes de dado um número qualquer $1 \leq x \leq n^2$ identificar a qual $M(w', k')$ ele pertence, e quais serão os outros números desta mesma matriz.

Por que é importante saber quais são os números de uma $M(w', k')$? Porque são números de uma $M(w', k')$ que vão ocupar uma mesma célula, ocasionando, o não preenchimento do quadrado.

Exemplo 2. Seja o quadrado de ordem $n = 15$ construído pelo método do passo uniforme com os seguintes parâmetros: $\alpha = 2$, $\beta = 1$, $a = 11$ e $b = 4$. Observe que $\begin{vmatrix} \alpha & a \\ \beta & b \end{vmatrix} = -3$ e $\text{mdc}(n, \alpha b - \beta a) = \delta = 3$. Assim, teremos $\left(\frac{n}{\delta}\right)^2 = \left(\frac{15}{3}\right)^2 = 25$ matrizes $M(w', k'), 3 \times 3$, Figura 9a, cada uma com $\delta^2 = 3^2 = 9$ elementos, Figura 9b.

Figura 10 - Localização do número 133, $M(2,3)$.



Fonte: O autor, 2014.

- Nessas condições, em qual $M(w', k')$ vai cair o número, digamos, 133?

  $133 = 1 + w + 15 \cdot k \Leftrightarrow k = 8$ e $w = 12$

  $k' \equiv k \left(\text{mod } \frac{n}{\delta}\right) \quad \Rightarrow \quad k' \equiv 8 \equiv 3 \pmod 5$

  $w' \equiv w \left(\text{mod } \frac{n}{\delta}\right) \quad \Rightarrow \quad w' \equiv 12 \equiv 2 \pmod 5$

  Desta forma, o número 133 está em $M(2,3)$, Figura 10.

4.3.1 Coordenadas dos elementos de $M\,(w', k')$

Um elemento genérico de $M(w', k')$ tem a forma

$$x = 1 + w' + k' \cdot n + l \cdot \frac{n}{\delta} + t \cdot \frac{n^2}{\delta}.$$

Vamos calcular as suas coordenadas A e B. Para isso retomamos a equação (3). Substituindo a expressão de x, vamos obter a seguinte congruência módulo n:

$$A \equiv p + \alpha \left(w' + k' \cdot n + l \cdot \frac{n}{\delta} + t \cdot \frac{n^2}{\delta} \right) + a \left[\frac{w' + k' \cdot n + l \cdot \frac{n}{\delta} + t \cdot \frac{n^2}{\delta}}{n} \right] \pmod{n}$$

Temos:

$$\alpha \cdot k' \cdot n \equiv 0 \pmod{n} \quad \text{e} \quad \alpha \cdot t \cdot \frac{n^2}{\delta} \equiv 0 \pmod{n}$$

Portanto, ambos podem ser eliminados.

$$A \equiv p + \alpha \left(w' + l \cdot \frac{n}{\delta} \right) + a \left[\frac{w' + k' \cdot n + l \cdot \frac{n}{\delta} + t \cdot \frac{n^2}{\delta}}{n} \right] \pmod{n}.$$

O termo multiplicado por a pode ser decomposto:

$$A \equiv p + \alpha \left(w' + l \cdot \frac{n}{\delta} \right) + a \left\{ \left[\frac{w' + l \cdot \frac{n}{\delta}}{n} \right] + \left[\frac{k' \cdot n}{n} \right] + \left[\frac{t \cdot \frac{n^2}{\delta}}{n} \right] \right\} \pmod{n}.$$

E, considerando que:

$$\left[\frac{w' + l \cdot \frac{n}{\delta}}{n} \right] = 0, \quad \text{uma vez que } w = w' + l \cdot \frac{n}{\delta} \text{ e } 0 \leq w \leq n - 1.$$

$$\left[\frac{k' \cdot n}{n} \right] = k' \qquad \text{e} \qquad \left[\frac{t \cdot \frac{n^2}{\delta}}{n} \right] = \left[\frac{t \cdot n}{\delta} \right] = \frac{t \cdot n}{\delta}, \quad \text{uma vez que } \delta \mid n,$$

a congruência se reduz a:

$$A \equiv p + \alpha w' + a \cdot k' + l \cdot \frac{\alpha n}{\delta} + t \cdot \frac{an}{\delta} \pmod{n} \tag{22}$$

Figura 11 - $M(2,3)$ do Ex. 3.

	$l=0$	$l=1$	$l=2$
$t=0$	48 $(p+7, q+14)$	53 $(p+2, q+4)$	58 $(p+12, q+9)$
$t=1$	123 $(p+2, q+4)$	128 $(p+12, q+9)$	133 $(p+7, q+14)$
$t=2$	198 $(p+12, q+9)$	203 $(p+7, q+14)$	208 $(p+2, q+4)$

Fonte: O autor, 2014.

Analogamente, segue de (4) que a coordenada B de x é dada por

$$B \equiv q + \beta w' + b \cdot k' + l \cdot \frac{\beta n}{\delta} + t \cdot \frac{bn}{\delta} \pmod{n} \tag{23}$$

Exemplo 3. Seja o quadrado de ordem $n = 15$ construído pelo método do passo uniforme com os seguintes parâmetros: $\alpha = 2$, $\beta = 1$, $a = 11$ e $b = 4$. Quais são as coordenadas (A, B), de cada elemento da matriz $M(2,3)$?
Obs.: p e q são as coordenadas da célula inicial, onde é alocado o 1.

A Figura 11 mostra os resultados obtidos quando usamos (22) e (23). Verificamos que os números

- 48, 133 e 203 vão ocupar a célula do quadrado de coordenadas $(p+7, q+14)$;
- 53, 123 e 208; a célula de coordenadas $(p+2, q+4)$ e
- 58, 128 e 198 irão cair na célula de coordenadas $(p+12, q+9)$,

confirmando que dois valores de x que correspondam a soluções de interesse do sistema (12)-(13) podem não ocupar a mesma célula.

Com relação à afirmação de Lehmer (4.2.1.1), Pág.29, *"que dois valores de x que diferem de $\frac{n^2}{\delta}$ vão ocupar a mesma célula"*, a Figura 11, oferece vários pares de valores de x que a contradizem, por exemplo, 53 e 128, que diferem de $\frac{15^2}{3}$ mas ocupam células diferentes.

4.3.2 As coordenadas A' e B'

O elemento x_{00} se localiza na 1ª linha e na 1ª coluna de $M(w', k')$. Então, fazendo $l = 0$ e $t = 0$, temos:

$$x_{00} = 1 + w' + k' \cdot n + 0 \cdot \frac{\beta n}{\delta} + 0 \cdot \frac{bn}{\delta} = 1 + w' + k' \cdot n = x'$$

Vamos denotar suas coordenadas por A' e B'. Temos

$$A' \equiv p + \alpha w' + ak' \pmod{n}$$
$$B' \equiv q + \beta w' + bk' \pmod{n}$$

Então, as congruências (22) e (23) podem ser reescritas:

$$A \equiv A' + l \cdot \frac{\alpha n}{\delta} + t \cdot \frac{an}{\delta} \pmod{n} \tag{24}$$
$$B \equiv B' + l \cdot \frac{\beta n}{\delta} + t \cdot \frac{bn}{\delta} \pmod{n} \tag{25}$$

As coordenadas dentro de uma matriz $M(w', k')$ dependem de (A', B') que são as coordenadas do elemento x_{00}. A partir destas coordenadas todas as outras coordenadas dos demais elementos da matriz são obtidas somando-se

$$l \cdot \frac{\alpha n}{\delta} + t \cdot \frac{an}{\delta} \qquad \text{e} \qquad l \cdot \frac{\beta n}{\delta} + t \cdot \frac{bn}{\delta}$$

respectivamente a A' e a B'. Ou seja todas são obtidas regularmente a partir de (A', B').

4.3.3 Regularidade das coordenadas A e B entre matrizes

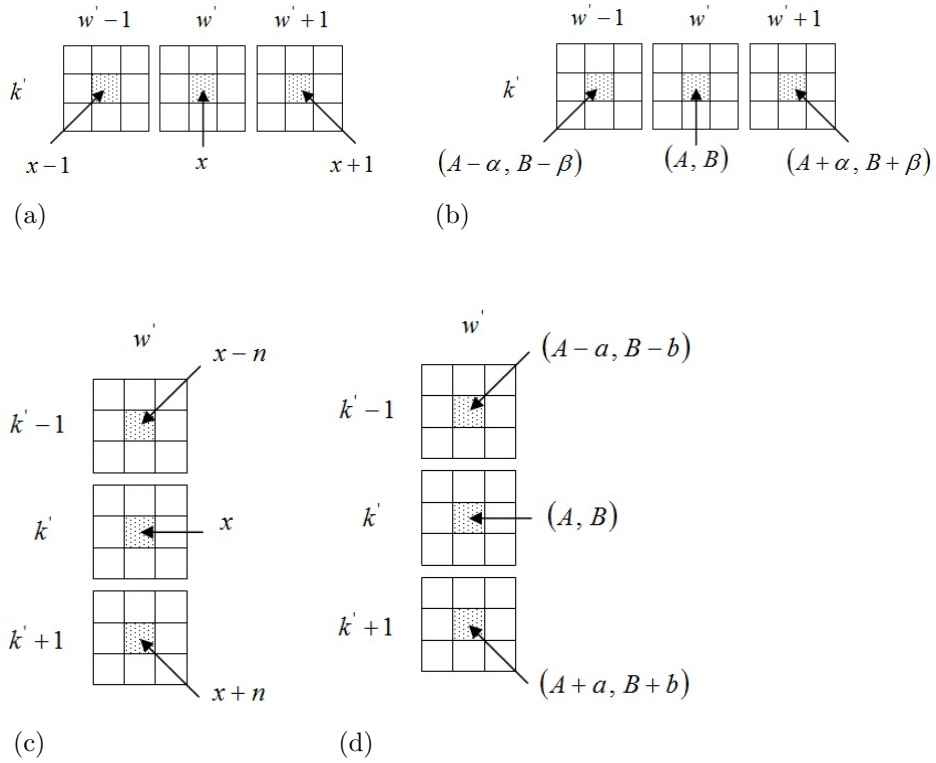
Seja

$$x = 1 + w' + k'n + l\frac{n}{\delta} + t\frac{n^2}{\delta}.$$

Note que a diferença entre números, localizados na mesma linha e coluna, mas em matrizes vizinhas $M(w' \pm 1, k')$ será de 1. E, em matrizes vizinhas da forma $M(w', k' \pm 1)$, a diferença será de n como mostram as figuras 12a e 12c.

Sejam (A, B) as coordenadas do elemento x localizado na t^{a} linha e l^{a} coluna de $M(w', k')$. A coordenada $A_{w' \pm 1, k'}$ de um elemento na mesma posição, mas localizado em

Figura 12 - Regularidades.



Legenda: (a) Elementos de mesma posição, em matrizes vizinhas, à esquerda e à direita; (b) Coordenadas de mesma posição, em matrizes vizinhas, à esquerda e à direita; (c) Elementos de mesma posição, em matrizes vizinhas, acima e abaixo; (d) Coordenadas de mesma posição, em matrizes vizinhas, acima e abaixo.

Fonte: O autor, 2014.

uma matriz vizinha $M(w' \pm 1, k')$, será determinada por:

$$A_{w'\pm1,k'} \equiv p + \alpha(w' \pm 1) + ak' + l \cdot \frac{\alpha n}{\delta} + t \cdot \frac{an}{\delta} \pmod{n}$$

$$A_{w'\pm1,k'} \equiv \left(p + \alpha w' + ak' + l \cdot \frac{\alpha n}{\delta} + t \cdot \frac{an}{\delta}\right) \pm \alpha \pmod{n}$$

$$A_{w'\pm1,k'} \equiv A \pm \alpha \pmod{n}$$

Analogamente

$$B_{w'\pm1,k'} \equiv B \pm \beta \pmod{n}$$

Portanto, a partir das coordenadas (A, B) de x, podemos determinar as coordenadas de um elemento localizado na mesma posição, em uma matriz vizinha à esquerda ou à direita

$M(w' \pm 1, k')$, simplesmente, somando $\pm\alpha$ à coordenada A e $\pm\beta$ à coordenada B, Figura 12b

A coordenada $A_{w',k'\pm1}$ de um elemento na mesma posição, mas localizado em uma matriz vizinha $M(w', k' \pm 1)$, será determinada por:

$$A_{w',k'\pm1} \equiv p + \alpha w' + a(k' \pm 1) + l \cdot \frac{\alpha n}{\delta} + t \cdot \frac{an}{\delta} \pmod{n}$$
$$A_{w',k'\pm1} \equiv \left(p + \alpha w' + ak' + l \cdot \frac{\alpha n}{\delta} + t \cdot \frac{an}{\delta}\right) \pm a \pmod{n}$$
$$A_{w',k'\pm1} \equiv A \pm a \pmod{n}$$

Analogamente

$$B_{w',k'\pm1} \equiv B \pm b \pmod{n}$$

Portanto, a partir das coordenadas (A, B) de x, podemos determinar as coordenadas de um elemento localizado na mesma posição, em uma matriz vizinha acima ou abaixo $M(w' \pm 1, k')$, simplesmente, somando $\pm a$ à coordenada A e $\pm b$ à coordenada B, Figura 12d.

Observação 2 (A possibilidade de α ser múltiplo de n)**.** A única possibilidade de termos duas coordenadas (A, B) iguais em matrizes vizinhas seria se β também fosse múltiplo de n, pois teríamos $\alpha \equiv 0 \pmod{n}$ e $\beta \equiv 0 \pmod{n}$. Mas, esse problema é aparente, pois em caso dos dois serem múltiplos de n então o determinante também seria múltiplo de n e o máximo divisor comum $\delta = n$. Nesse caso, a quantidade de matrizes é dada por $\left(\frac{n}{\delta}\right)^2 = 1$. Então, teríamos apenas uma única matriz $n \times n$ que seria a $M(0, 0)$. É inteiramente análoga, a possibilidade de a ou b serem múltiplos de n.

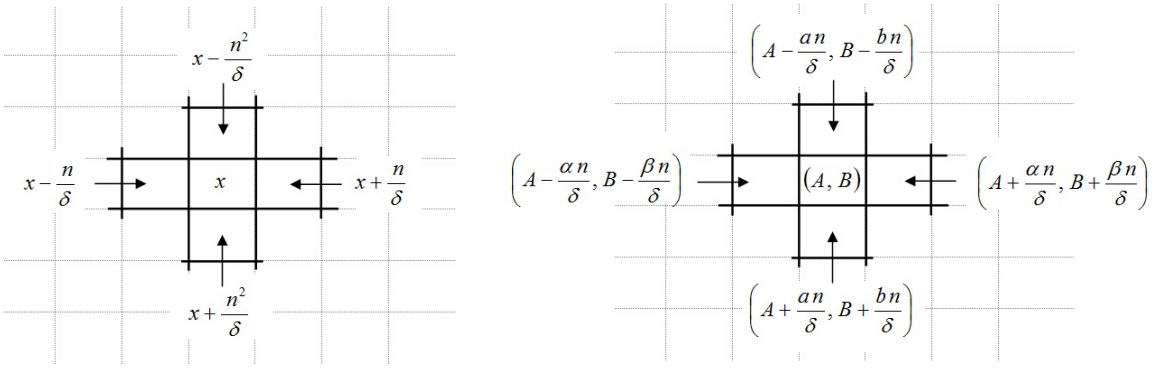
4.3.4 Regularidade das coordenadas A e B ao longo de uma linha de $M(w', k')$

Seja (A_{tl}, B_{tl}) as coordenadas do elemento x_{tl} localizado na linha t e coluna l de $M(w', k')$. As coordenadas de um elemento vizinho, localizado na mesma linha, $x_{t,l+1}$ ou $x_{t,l-1}$, serão determinadas por:

$$A_{t,l\pm1} \equiv \left(A' + l \cdot \frac{\alpha n}{\delta} + t \cdot \frac{an}{\delta}\right) \pm \frac{\alpha n}{\delta} \equiv A_{t,l} \pm \frac{\alpha n}{\delta} \pmod{n}$$
$$B_{t,l\pm1} \equiv \left(B' + l \cdot \frac{\beta n}{\delta} + t \cdot \frac{bn}{\delta}\right) \pm \frac{\beta n}{\delta} \equiv B_{t,l} \pm \frac{\beta n}{\delta} \pmod{n}$$

Portanto, a partir das coordenadas (A, B) de x, podemos determinar as coordenadas dos elementos vizinhos em uma mesma linha, simplesmente, somando $\pm\frac{\alpha n}{\delta}$ à coordenada A

Figura 13 - Regularidades.



(a) (b)

Legenda: (a) Elementos vizinhos de x; (b) Coordenadas vizinhas de (A, B).
Fonte: O autor, 2014.

e $\pm\frac{\beta n}{\delta}$ à coordenada B.

4.3.5 Regularidade das coordenadas A e B ao longo de uma coluna de $M(w', k')$

Seja (A_{tl}, B_{tl}) as coordenadas do elemento $x_{t,l}$ localizado na linha t e coluna l de $M(w', k')$. As coordenadas de um elemento vizinho, localizado na mesma coluna, $x_{t+1,l}$ ou $x_{t-1,l}$, serão determinadas por:

$$A_{t\pm1,l} \equiv \left(A' + l \cdot \frac{\alpha n}{\delta} + t \cdot \frac{an}{\delta}\right) \pm \frac{\alpha n}{\delta} \equiv A_{t,l} \pm \frac{an}{\delta} \pmod{n}$$
$$B_{t\pm1,l} \equiv \left(B' + l \cdot \frac{\beta n}{\delta} + t \cdot \frac{bn}{\delta}\right) \pm \frac{\beta n}{\delta} \equiv B_{t,l} \pm \frac{bn}{\delta} \pmod{n}$$

Portanto, a partir das coordenadas (A, B) de x, podemos determinar as coordenadas dos elementos vizinhos em uma mesma coluna somando $\pm\frac{an}{\delta}$ à coordenada A e $\pm\frac{bn}{\delta}$ à coordenada B. As figuras 13a e 13b mostram os vizinhos de um elemento genérico, x, em uma $M(w', k')$, assim como suas respectivas coordenadas.

Recapitulando: Até aqui, vimos que as soluções de interesse do sistema (12)-(13) são números da forma $x = 1 + w' + k' \cdot n + l \cdot \frac{n}{\delta} + t \cdot \frac{n^2}{\delta}$ e podem ser organizados em matrizes $M(w', k')$. São os números que estão em uma mesma matriz $M(w', k')$ que vão compartilhar células, causando o não preenchimento do quadrado pelo método do passo uniforme. Também observamos um padrão: à medida em que nos movemos, horizontalmente, para a direita ou esquerda, em $M(w', k')$, os elementos variam de $\pm\frac{n}{\delta}$ e suas, respectivas coordenadas, variam de $\pm\frac{\alpha n}{\delta}$ e $\pm\frac{\beta n}{\delta}$. Se o movimento for, verticalmente,

para cima ou para baixo, os elementos variam de $\pm\frac{n^2}{\delta}$ e suas, respectivas coordenadas, são acrescidas de $\pm\frac{an}{\delta}$ e $\pm\frac{bn}{\delta}$.

Exemplo 4. Seja o quadrado construído pelo método do passo uniforme definido pelos parâmetros $n = 15$, $\alpha = 4$, $\beta = 5$, $a = 1$ e $b = 2$.

Aplicando as regularidades da matriz $M(w', k')$, vamos determinar quais são os números, com suas respectivas coordenadas, que estão na mesma matriz que 102.
$\alpha b - \beta a = 4 \cdot 2 - 5 \cdot 1 = 3$ e $\delta = \text{mdc}(15, 3) = 3$

$102 = 1 + w + 15 \cdot k \Leftrightarrow k = 6$ e $w = 11$
$k' \equiv k \left(\text{mod } \frac{n}{\delta}\right) \quad \Rightarrow \quad k' \equiv 6 \equiv 1 \pmod 5$
$w' \equiv w \left(\text{mod } \frac{n}{\delta}\right) \quad \Rightarrow \quad w' \equiv 11 \equiv 1 \pmod 5$

Então, 102 está em $M(1, 1)$. O elemento x_{00} que está na 1ª linha e 1ª coluna de $M(1, 1)$ é dado por

$x_{00} = x' = 1 + w' + k'n = 1 + 1 + 1 \cdot 15 = 17$

Suas coordenadas são:

$A_{00} = A' \equiv p + \alpha w' + ak' \equiv p + 4 \cdot 1 + 1 \cdot 1 \equiv p + 5 \pmod{15}$
$B_{00} = B' \equiv q + \beta w' + bk' \equiv q + 5 \cdot 1 + 2 \cdot 1 \equiv q + 7 \pmod{15}$

Então, a partir de $x_{00} = 17$, $A_{00} = p + 5$ e $B_{00} = q + 7$, podemos determinar, respectivamente, x_{01}, A_{01} e B_{01}:

$x_{01} = 17 + 5 = 22$ $\qquad$ $A_{01} \equiv (p + 5) + 5 \equiv p + 10 \pmod{15}$
$\qquad\qquad\qquad\qquad$ $B_{01} \equiv (q + 7) + 10 \equiv q + 2 \pmod{15}$

A partir de $x_{01} = 22$, $A_{01} = p + 10$ e $B_{01} = q + 2$, podemos determinar, respectivamente, x_{02}, A_{02} e B_{02}:

$x_{02} = 22 + 5 = 27$ $\qquad$ $A_{02} \equiv (p + 10) + 5 \equiv p \pmod{15}$
$\qquad\qquad\qquad\qquad$ $B_{02} \equiv (q + 2) + 10 \equiv q + 12 \pmod{15}$

Assim, a 1ª linha foi concluída.

Continuando, de $x_{00} = 17$, $A_{00} = p + 5$ e $B_{00} = q + 7$, podemos determinar, respectivamente, x_{10}, A_{10} e B_{10}:

$x_{10} = 17 + 75 = 92$ $\qquad$ $A_{10} \equiv (p + 5) + 5 \equiv p + 10 \pmod{15}$
$\qquad\qquad\qquad\qquad$ $B_{10} \equiv (q + 7) + 10 \equiv q + 2 \pmod{15}$

De $x_{10} = 92$, $A_{10} = p + 10$ e $B_{10} = q + 2$, podemos determinar, respectivamente, x_{11}, A_{11} e B_{11}:

$$x_{11} = 92 + 5 = 97 \qquad A_{11} \equiv (p + 10) + 5 \equiv p \pmod{15}$$
$$B_{11} \equiv (q + 2) + 10 \equiv q + 12 \pmod{15}$$

De $x_{11} = 97$, $A_{11} = p$ e $B_{11} = q + 12$, podemos determinar, respectivamente, x_{12}, A_{12} e B_{12}:

$$x_{12} = 97 + 5 = 102 \qquad A_{12} \equiv p + 5 \equiv p + 5 \pmod{15}$$
$$B_{12} \equiv (q + 12) + 10 \equiv q + 7 \pmod{15}$$

Assim, a 2ª linha foi concluída.

De $x_{10} = 92$, $A_{10} = p + 10$ e $B_{10} = q + 2$, podemos determinar, respectivamente, x_{20}, A_{20} e B_{20}:

$$x_{20} = 92 + 75 = 167 \qquad A_{20} \equiv (p + 10) + 5 \equiv p \pmod{15}$$
$$B_{20} \equiv (q + 2) + 10 \equiv q + 12 \pmod{15}$$

De $x_{20} = 167$, $A_{20} = p$ e $B_{20} = q + 12$, podemos determinar, respectivamente, x_{21}, A_{21} e B_{21}:

$$x_{21} = 167 + 5 = 172 \qquad A_{21} \equiv p + 5 \equiv p + 5 \pmod{15}$$
$$B_{21} \equiv (q + 12) + 10 \equiv q + 7 \pmod{15}$$

De $x_{21} = 172$, $A_{21} = p + 5$ e $B_{21} = q + 7$, podemos determinar, respectivamente, x_{22}, A_{22} e B_{22}:

$$x_{22} = 172 + 5 = 177 \qquad A_{22} \equiv (p + 5) + 5 \equiv p + 10 \pmod{15}$$
$$B_{22} \equiv (q + 7) + 10 \equiv q + 2 \pmod{15}$$

Os resultados obtidos estão na Figura 14.

Figura 14 - Elementos e suas coordenadas, matriz $M(1, 1)$, do Exemplo 4.

	$l = 0$	$l = 1$	$l = 2$
$t = 0$	17 $(p+5, q+7)$	22 $(p+10, q+2)$	27 $(p, q+12)$
$t = 1$	92 $(p+10, q+2)$	97 $(p, q+12)$	102 $(p+5, q+7)$
$t = 2$	167 $(p, q+12)$	172 $(p+5, q+7)$	177 $(p+10, q+2)$

Fonte: O autor, 2014.

4.3.6 Padrão dos números em $M(w', k')$ que ocupam uma mesma célula no quadrado

Vimos que ter o mesmo valor para w' e o mesmo valor para k' é condição necessária, mas não suficiente para que dois números ocupem a mesma célula do quadrado. Sejam $x_1 = x_{t_1,l_1}$ e $x_2 = x_{t_2,l_2}$ dois elementos em uma matriz $M\,(w', k')$. Suas coordenadas são dadas respectivamente por (24) e (25)

$$\begin{aligned}
A_1 &\equiv A' + l_1\frac{\alpha n}{\delta} + t_1\frac{an}{\delta} \pmod{n}\\
B_1 &\equiv B' + l_1\frac{\beta n}{\delta} + t_1\frac{bn}{\delta} \pmod{n}\\
A_2 &\equiv A' + l_2\frac{\alpha n}{\delta} + t_2\frac{an}{\delta} \pmod{n}\\
B_2 &\equiv B' + l_2\frac{\beta n}{\delta} + t_2\frac{bn}{\delta} \pmod{n}
\end{aligned}$$

Vamos assumir que x_1 e x_2 tenham coordenadas iguais, $A_1 \equiv A_2$ e $B_1 \equiv B_2$, temos:

$$\begin{cases}
\alpha(l_1 - l_2) \equiv a(t_2 - t_1) \pmod{\delta} & (26)\\
\beta(l_1 - l_2) \equiv b(t_2 - t_1) \pmod{\delta} & (27)
\end{cases}$$

Vamos agora rediscutir o exemplo dos *"dois números que diferem por* $\frac{n^2}{\delta}$*"*, citado por Lehmer. Até o fim dessa subseção, tal como Lehmer (1929), admitiremos que os parâmetros α, β, a e b são primos com n. Veremos que dois números com essa relação, embora em uma mesma $M(w', k')$, não caem em uma mesma célula (A, B). Vamos analisar o sistema (26)-(27) tendo em vista analisar o erro cometido por Lehmer sob uma nova perspectiva.

Segue do fato dos parâmetros α, β, a e b serem primos com n que o sistema (26)–(27) é equivalente a

$$\begin{cases}
\alpha(l_1 - l_2) \equiv a(t_2 - t_1) \pmod{\delta} & (28)\\
(\alpha b - \beta a)(t_2 - t_1) \equiv 0 \pmod{\delta} & (29)
\end{cases}$$

Observe que quaisquer inteiros t_1, t_2 satisfazem a (29). Consequentemente, basta resolver (28).

Considere (28). Se $l_1 = l_2$ então $0 \equiv a(t_2 - t_1) \pmod{\delta}$,

mas a é primo com n, então $t_1 \equiv t_2 \pmod{\delta}$,

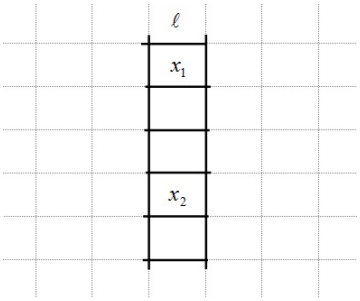
(mas $0 \leq t \leq \delta - 1$) então $t_1 = t_2$.

Por outro lado, se $t_1 = t_2$ então $\alpha(l_1 - l_2) \equiv 0 \pmod{\delta}$,

mas α é primo com n, então $l_1 \equiv l_2 \pmod{\delta}$,

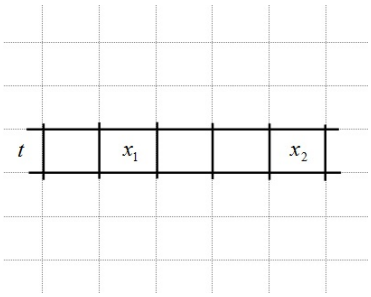
mas $0 \leq l \leq \delta - 1$, então $l_1 = l_2$.

Figura 15 - x_1 e x_2 em uma mesma coluna l de $M(w', k')$ tem coordenadas (A, B) diferentes.



Fonte: O autor, 2014.

Figura 16 - x_1 e x_2 em uma mesma linha t de $M(w', k')$ tem coordenadas (A, B) diferentes.



Fonte: O autor, 2014.

Portanto, podemos enunciar o seguinte:

Teorema 9. *Dados α, β, a e b todos primos com n. Se dois elementos distintos $x_1 = x_{t_1,l_1} = x' + l_1\frac{n}{\delta} + t_1\frac{n^2}{\delta}$ e $x_2 = x_{t_2,l_2} = x' + l_2\frac{n}{\delta} + t_2\frac{n^2}{\delta}$ da matriz $M(w', k')$ ocupam a mesma célula do quadrado, então $l_1 \neq l_2$ e $t_1 \neq t_2$.*

Isso significa que dois números que estão em uma mesma coluna l da matriz $M(w', k')$ não podem ocupar uma mesma célula do quadrado, Figura 15. Da mesma forma, dois números que estão em uma mesma linha t da matriz $M(w', k')$ não ocupam uma mesma célula do quadrado, Figura 16. Note que *"dois números que diferem por $\frac{n^2}{\delta}$"* sempre pertencem a uma mesma coluna. Portanto, não podem ocupar uma mesma célula do quadrado.

Substituindo os coeficientes de (28) pelos restos na divisão por δ, obtemos um sistema equivalente a (28)–(29)

$$\begin{cases} \alpha'(l_1 - l_2) + a'(t_1 - t_2) \equiv 0 \pmod{\delta} & (30) \\ (\alpha b - \beta a)(t_2 - t_1) \equiv 0 \pmod{\delta} & (31) \end{cases}$$

Figura 17 - $M(2,3)$ elementos e coordenadas. Exemplo 5.

	$l=0$	$l=1$	$l=2$
$t=0$	48 $(p+7, q+14)$	53 $(p+2, q+4)$	58 $(p+12, q+9)$
$t=1$	123 $(p+2, q+4)$	128 $(p+12, q+9)$	133 $(p+7, q+14)$
$t=2$	198 $(p+12, q+9)$	203 $(p+7, q+14)$	208 $(p+2, q+4)$

Fonte: O autor, 2014.

Note que a hipótese de primalidade nos diz que $\alpha' \neq 0$ e $a' \neq 0$. Pelo Teorema 5 na página 15, a equação de congruência linear com duas variáveis (30), tem solução, pois, $\text{mdc}(\alpha', a', \delta) = 1 \mid 0$. O Teorema 6 assegura que a equação (30) tem $\text{mdc}(\alpha', a', \delta) \cdot \delta^{2-1} = 1 \cdot \delta = \delta$ soluções distintas.

Seja $(\alpha', a') = \text{mdc}(\alpha', a')$. Para $0 \leq k \leq \delta - 1$, considere

$$l_1 - l_2 \equiv \frac{a'}{(\alpha', a')} \cdot k \pmod{\delta} \quad \text{e} \quad t_1 - t_2 \equiv \delta - \frac{\alpha'}{(\alpha', a')} \cdot k \pmod{\delta} \tag{32}$$

Note que se $0 \leq k_1 \neq k_2 \leq \delta - 1$,

$$\frac{a'}{(\alpha', a')} \cdot (k_1 - k_2) \not\equiv 0 \pmod{\delta} \quad \text{e} \quad \delta - \frac{\alpha'}{(\alpha', a')} \cdot (k_1 - k_2) \not\equiv 0 \pmod{\delta}.$$

Além disso, se l_1, t_1, l_2 e t_2 satisfazem (32), temos

$$\alpha'(l_1 - l_2) + a'(t_1 - t_2) \equiv \frac{a'\alpha'}{(\alpha', a')} \cdot k - \frac{a'\alpha'}{(\alpha', a')} \cdot k + a' \cdot \delta \equiv 0 \pmod{\delta}.$$

Consequentemente, (32) nos permite determinar todos os elementos de uma matriz $M(w', k')$ que cairão em uma mesma célula do quadrado. Note que os δ^2 elementos de $M(w', k')$ serão designados a δ células distintas. Além disso, cada uma dessas células será ocupada exatamente por δ elementos de $M(w', k')$.

Exemplo 5. Retomamos aqui o Exemplo 3 do quadrado de ordem $n = 15$ construído pelo método do passo uniforme com os seguintes parâmetros: $\alpha = 2$, $\beta = 1$, $a = 11$ e $b = 4$, para ilustrar o Teorema 9. A Figura 17 apresenta os elementos de $M(2,3)$ e suas respectivas coordenadas.

Recapitulando: Os números que ocupam uma mesma célula, estão distribuídos em $\left(\frac{n}{\delta}\right)^2$ matrizes $M(w', k')$, com $0 \leq w', k' \leq \frac{n}{\delta} - 1$, constituída de δ linhas e δ colunas.

Nesta subseção (Seção 4.3.6), vimos que o método do passo uniforme, com parâmetros α, β, a e b, primos um a um com n, porém com o determinante $\begin{vmatrix} \alpha & a \\ \beta & b \end{vmatrix} = \alpha b - \beta a$ tendo um divisor comum, δ, com n, (Seção 4.3 na página 32), não preenche o quadrado e caracterizamos os números que vão ocupar uma mesma célula. Mostramos que conhecidas a linha t e a coluna l de um número em $M(w', k')$, podemos calcular quais são todos os outros números que serão alocados na mesma célula do quadrado.

4.3.7 Duas soluções de interesse que ocupam a mesma célula

Nessa seção, não supomos que os parâmetros α, β, a e b sejam primos com n. Admitimos apenas de $\text{mdc}(\alpha b - \beta a, n) \neq 1$. Para obter a condição necessária para o preenchimento, resta exibir $x_1 \neq x_2$ dados por $x = 1 + w' + k'n + l \cdot \dfrac{n}{\delta} + t \cdot \dfrac{n^2}{\delta}$ que sejam soluções de (5)–(6). isto é, que ocupem a mesma célula no quadrado.

Já sabemos que duas soluções, x_1 e x_2, que ocupam a mesma célula (A, B) do quadrado, pertencem a uma mesma matriz $M(w', k')$ e têm suas coordenadas dadas por (26)–(27). Substituindo os coeficientes α, β, a e b do sistema pelos restos na divisão por $\text{mdc}(\alpha b - \beta a, n) = \delta \neq 1$, obtemos:

$$\begin{cases} \alpha'(l_1 - l_2) + a'(t_1 - t_2) \equiv 0 \pmod{\delta} & (33) \\ \beta'(l_1 - l_2) + b'(t_1 - t_2) \equiv 0 \pmod{\delta} & (34) \end{cases}$$

Interessam-nos soluções $l_1 - l_2 \neq 0$ ou $t_1 - t_2 \neq 0$. Observe que

$$\delta \mid (\alpha b - \beta a) \Rightarrow \alpha' b' - \beta' a' \equiv 0 \pmod{\delta}$$

Note que se todos os parâmetros α', β', a' e b' forem nulos, todos os elementos da matriz $M(w', k')$ ocupam a mesma célula do quadrado e não há o que demonstrar.

Vamos supor que pelo menos um dos parâmetros α', β', a' e b' é diferente de zero. Por inspeção, se tomamos

$$\begin{cases} l_1 - l_2 \equiv b' \pmod{\delta} \\ t_1 - t_2 \equiv \delta - \beta' \pmod{\delta} \end{cases}$$

o sistema (33)-(34) é satisfeito uma vez que $\beta'(b') + b'(\delta - \beta') \equiv 0 \pmod{\delta}$

O mesmo acontece se temos

$$\begin{cases} l_1 - l_2 \equiv \delta - b' \pmod{\delta} \\ t_1 - t_2 \equiv \beta' \pmod{\delta} \end{cases} \qquad \text{ou} \qquad \begin{cases} l_1 - l_2 \equiv \delta - a' \pmod{\delta} \\ t_1 - t_2 \equiv \alpha' \pmod{\delta} \end{cases}$$

Figura 18 - Elementos e suas coordenadas, da matriz $M(1,1)$, do Exemplo 6.

	$l=0$	$l=1$	$l=2$
$t=0$	11 (5, 1)	14 (5, 1)	17 (5, 1)
$t=1$	38 (8, 1)	41 (8, 1)	44 (8, 1)
$t=2$	65 (2, 1)	68 (2, 1)	71 (2, 1)

Fonte: O autor, 2014.

ou

$$\begin{cases} l_1 - l_2 \equiv a' \pmod{\delta} \\ t_1 - t_2 \equiv \delta - \alpha' \pmod{\delta} \end{cases}$$

Como a', b', α', $\beta' < \delta$, e pelo menos um deles é não nulo, em pelo menos um dos quatro sistemas acima, haverá uma escolha $l_1 \neq l_2$ ou $t_1 \neq t_2$. Portanto, podemos sempre exibir $x_1 \neq x_2$ dados por (17) que sejam soluções de (5)–(6), isto é, que ocupem a mesma célula (A, B) do quadrado.

Os argumentos acima estabelecem as condições necessárias para o preenchimento do quadrado pelo método do passo uniforme:

Teorema 10 (Condição necessária para o preenchimento)**.** *Dados os parâmetros α, β, a e b (números inteiros) a condição necessária para que o método do passo uniforme preencha o quadrado de ordem n é que o determinante* $\begin{vmatrix} \alpha & a \\ \beta & b \end{vmatrix}$ *seja primo com n.*

Exemplo 6. Considere $n = 9$, $\alpha = 3$, $\beta = 6$, $a = 1$, $b = 3$. O determinante $\alpha b - \beta a = 3$; $\delta = 3$. Teremos 9 matrizes 3×3. A Figura 18 exibe a matriz $M(1,1)$. Observamos, que neste caso existem elementos de uma mesma linha que ocupam a mesma célula do quadrado. Por exemplo, na linha $t = 0$, os elementos 11, 14 e 17 vão ocupar a mesma célula $(5, 1)$ do quadrado.

Exemplo 7. Seja um quadrado de ordem $n = 15$, construído pelo método do passo uniforme, com os seguintes parâmetros: $\alpha = 3$, $\beta = 1$, $a = 1$ e $b = 2$. Quais números ocupam a mesma célula que 138?
Como $\delta = \text{mdc}\,(\alpha b - \beta a, n) = (5, 15) = 5$ teremos $\left(\frac{n}{\delta}\right)^2 = 9$ matrizes $M(w', k')$, cada uma com $\delta^2 = 25$ elementos. Para escrever 138 como em (17):

$$138 = 1 + \left(w' + l \cdot \frac{15}{5}\right) + \left(k' + t \cdot \frac{15}{5}\right) 15.$$

Figura 19 - Números de $M(2,0)$ que ocupam a mesma célula que 138.

	$l=0$	$l=1$	$l=2$	$l=3$	$l=4$
$t=0$		6			
$t=1$					60
$t=2$			99		
$t=3$	138				
$t=4$				192	

Fonte: O autor, 2014.

Segue, do teorema da divisão euclidiana que

$(w' + 3 \cdot l) = 2 \quad \text{e} \quad (k' + 3 \cdot t) = 9.$

Portanto, $w' = 2$, $k' = 0$, $l = 0$ e $t = 3$. Isso significa que 138 está na linha $t = 3$ (4^{a} linha) e na coluna $l = 0$ (1^{a} coluna) da matriz $M(2,0)$ (Figura 19).

Ainda que tenhamos $\text{mdc}(\alpha, n) \neq 1$, pelo fato dos demais parâmetros β, a e b serem primos com n e ainda $\text{mdc}(\alpha, a, n) = 1$, com um raciocínio análogo ao da Subseção 4.3.6, todos os outros números que compartilham a mesma célula do quadrado com 138, podem ser determinados. Vamos tomar (30),

$3\,(l_1 - l_2) + (t_1 - t_2) \equiv 0 \pmod 5$

Como $\text{mdc}(\alpha, a, n) = \text{mdc}(3, 1, 5) = 1 \mid 0 \Rightarrow$ então pelos Teoremas 5 e 6 a equação acima terá 5 soluções $(l_1 - l_2, t_1 - t_2)$ distintas. Por (32) segue:

$l_1 - l_2 \equiv k \pmod 5 \quad \text{e} \quad t_1 - t_2 \equiv 2k \pmod 5$

Sendo $k = 0, 1, 2, \ldots, \delta - 1 = 0, 1, 2, \ldots, 4$.

$$
\begin{aligned}
k = 0 \qquad & l_1 - l_2 \equiv 0 \pmod 5 \\
& t_1 - t_2 \equiv 0 \pmod 5 \\
k = 1 \qquad & l_1 - l_2 \equiv 1 \pmod 5 \\
& t_1 - t_2 \equiv 2 \pmod 5 \\
k = 2 \qquad & l_1 - l_2 \equiv 2 \pmod 5 \\
& t_1 - t_2 \equiv 4 \pmod 5 \\
k = 3 \qquad & l_1 - l_2 \equiv 3 \pmod 5 \\
& t_1 - t_2 \equiv 1 \pmod 5 \\
k = 4 \qquad & l_1 - l_2 \equiv 4 \pmod 5 \\
& t_1 - t_2 \equiv 3 \pmod 5
\end{aligned}
$$

Para 138, temos $l = 0$ e $t = 3$. Fazendo $(l_2, t_2) = (0, 3)$, os elementos que compartilham a mesma célula do quadrado com 138, têm localizações em $M(2, 0)$ dadas por

$$(l, t) \equiv (0, 3) + (l_1, t_1) \pmod 5, \quad \text{tais que} \quad (l_1, t_1) \in \{(0, 0), (1, 2), (2, 4), (3, 1), (4, 3)\}$$

Assim, podemos determinar os números

$$x_{tl} = 1 + w' + k'n + l \cdot \frac{n}{\delta} + t \cdot \frac{n^2}{\delta} = 1 + 2 + 0 \cdot 15 + l \cdot \frac{15}{5} + t \cdot \frac{15^2}{5}$$

que vão ocupar a mesma célula do quadrado que 138:

$$x_{30} = 138, \quad x_{01} = 6, \quad x_{22} = 99, \quad x_{43} = 192, \quad x_{14} = 60.$$

Por (22) e (23), as coordenadas (A, B) de 138 são

$$(p + 6 + 0 + 0 \cdot 9 + 3 \cdot 3,\ q + 2 + 0 + 0 \cdot 3 + 3 \cdot 6) \equiv (p, q + 5) \pmod{15}$$

Assim, 6, 60, 99, 138 e 192 compartilham a mesma célula do quadrado de coordenadas $(p, q + 5)$. A Figura 20a, exibe a matriz $M(2, 0)$ completa. Na Figura 20b temos todas as respectivas coordenadas.

Figura 20 - Matriz$(2, 0)$, Exemplo 7.

	$l = 0$	$l = 1$	$l = 2$	$l = 3$	$l = 4$
$t = 0$	3	6	9	12	15
$t = 1$	48	51	54	57	60
$t = 2$	93	96	99	102	105
$t = 3$	138	141	144	147	150
$t = 4$	183	186	189	192	195

(a)

	$l = 0$	$l = 1$	$l = 2$	$l = 3$	$l = 4$
$t = 0$	(7,3)	(1,6)	(10,9)	(4,12)	(13,15)
$t = 1$	(10,9)	(4,12)	(13,15)	(7,3)	(1,6)
$t = 2$	(13,15)	(7,3)	(1,6)	(10,9)	(4,12)
$t = 3$	(1,6)	(10,9)	(4,12)	(13,15)	(7,3)
$t = 4$	(4,12)	(13,15)	(7,3)	(1,6)	(10,9)

(b)

Legenda: (a) – Números; (b) – Respectivas coordenadas (A, B).
Fonte: O autor, 2014.

Na página 51, a Figura 21a, mostra como ficará o quadrado após os três primeiros ciclos. A figura 21b, mostra que do 4º ao 7º ciclos, os números serão alocados nas mesmas células já preenchidas anteriormente. As figuras 21c, 21d e 21e mostram, que nos ciclos restantes, sucederá o mesmo e, assim, o quadrado não será preenchido. De fato, após todos os 225 números terem sido alocados pelo método do passo uniforme o quadrado ficará como mostra a última figura 21e, com céluas vazias. Tínhamos visto que em cada $M(w', k')$, os δ^2 números x vão ocupar apenas δ células. Esse percentual que se mantém para o quadrado, corresponde a $\frac{1}{\delta} = \frac{1}{5} = 0,2$, ou, 20% de preenchimento. Os resultados apresentados até aqui, estabelecem o seguinte teorema.

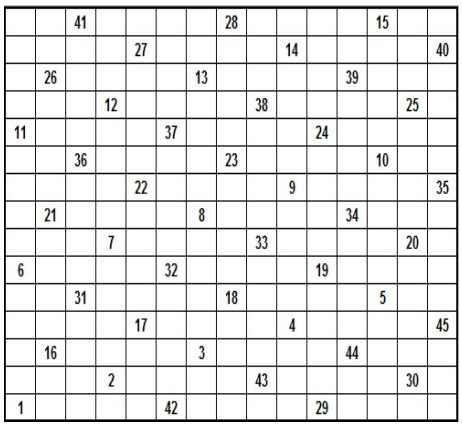
Teorema 11 (Condição necessária para o preenchimento)**.** *Dados os parâmetros α, β, a e b (números inteiros) a condição necessária para que o método do passo uniforme preencha o quadrado de ordem n é que o determinante* $\begin{vmatrix} \alpha & a \\ \beta & b \end{vmatrix}$ *seja primo com n.*

Ao suprimir a hipótese de primalidade com n sobre os parâmetros α, β, a e b, os Teoremas 7 e 11 generalizam o resultado apresentado por Lehmer:

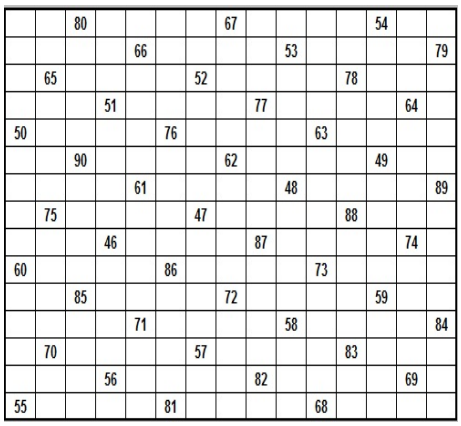
Teorema 12 (LEHMER, 1929, p. 530)**.** *Dados*[10] *α, β, a, b, todos primos com n, a condição necessária e suficiente para que o método do passo uniforme preencha o quadrado é que o determinante* $\begin{vmatrix} \alpha & a \\ \beta & b \end{vmatrix}$ *seja primo com n.*

[10] tradução livre de: *Given α, β, a, b, all prime to n, the necessary and sufficient condition that the uniform step process shall fill the square is that the determinant* $\begin{vmatrix} \alpha & a \\ \beta & b \end{vmatrix}$ *shall be prime to n.*

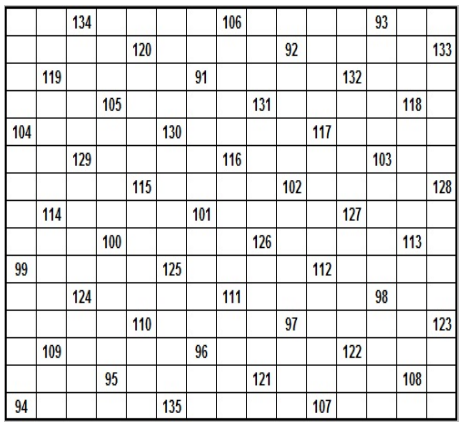
Figura 21 - Ciclos do quadrado do Exemplo 7.



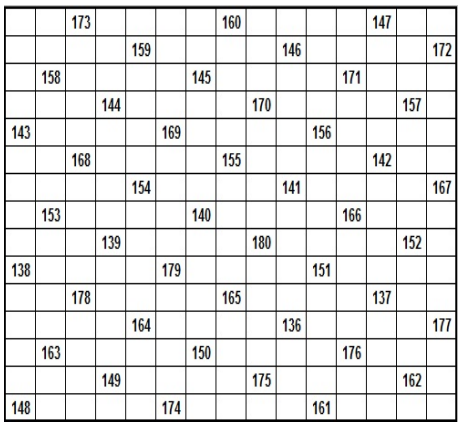
(a)



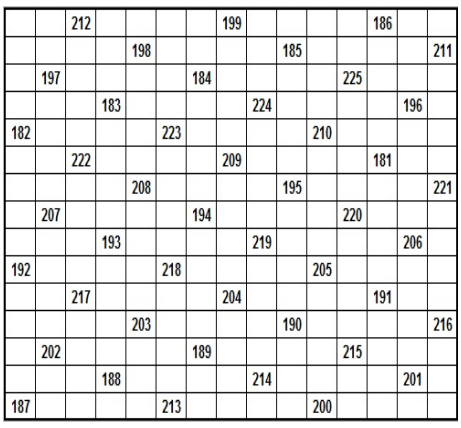
(b)



(c)



(d)



(e)

Legenda: (a) 1º ao 3º ciclos: de 1 até 45; (b) 4º ao 6º ciclos: de 46 até 90; (c) 7º ao 9º ciclos: de 91 até 135; (d) 10º ao 12º ciclos: de 136 até 180; (e) 13º ao 15º ciclos: de 181 até 225.

Fonte: O autor, 2014.

5 MÁGICO NAS COLUNAS OU LINHAS

Teorema 13 (LEHMER, 1929, p. 531)**.** *Se os coeficientes α, a e o determinante $\alpha b - \beta a$ forem primos com n então o quadrado é mágico nas colunas.*

Demonstração. Como o $\text{mdc}(\alpha b - \beta b, n) = 1$, pelo Teorema 7, página 27, o quadrado será preenchido. Vamos tomar dois números distintos x_1 e x_2 quaisquer de uma coluna do quadrado. Sendo assim, a congruência $A_1 \equiv A_2$ deve ser verdadeira. Logo,

$$p + w_1\alpha + k_1 a \equiv p + w_2\alpha + k_2 a \pmod{n}$$
$$w_1\alpha + k_1 a \equiv w_2\alpha + k_2 a \pmod{n}$$

Se $k_1 = k_2$, então $w_1\alpha \equiv w_2\alpha \pmod{n}$. Como α e n são primos entre si, então $w_1 \equiv w_2 \pmod{n}$. Como $0 \leq w \leq n-1$, então $w_1 = w_2$. Isto é, se dois números distintos x_1 e x_2 pertencem a uma mesma coluna do quadrado e $w_1 \neq w_2$, então $k_1 \neq k_2$.

Se $w_1 = w_2$, então $k_1\alpha \equiv k_2\alpha \pmod{n}$. Como α e n são primos entre si, então $k_1 \equiv k_2 \pmod{n}$. Como $0 \leq k \leq n-1$, então $k_1 = k_2$. Isto é, se dois números distintos x_1 e x_2 pertencem a uma mesma coluna do quadrado e $k_1 \neq k_2$, então $w_1 \neq w_2$. Vimos que

$$k_1 \neq k_2 \Leftrightarrow w_1 \neq w_2 \tag{35}$$

Sejam $x_1 \neq x_2$, em uma mesma coluna, segue que $(1 + w_1 + k_1 n) - (1 + w_2 + k_2 n) = (w_1 - w_2) + (k_1 - k_2)n \neq 0$. Daí, sendo $n \neq 0$, teríamos três possibilidades: Ou $w_1 \neq w_2$ e $k_1 = k_2$; ou $w_1 = w_2$ e $k_1 \neq k_2$; ou $w_1 \neq w_2$ e $k_1 \neq k_2$.

Mas, levando em conta o resultado (35) apenas a última relação vai se verificar sob as hipóteses do teorema. Portanto, se dois números distintos x_1 e x_2, pertencem a uma mesma coluna, de um quadrado preenchido pelo método do passo uniforme, com as condições dadas, então $w_1 \neq w_2$ e $k_1 \neq k_2$. Isso significa que os $w's$ são distintos, os $k's$ também são distintos e portanto, cada um vai assumir todos os valores do conjunto $\{0, 1, 2, \ldots, n-1\}$. Sendo, assim, se somarmos os elementos de uma coluna, temos:

$$\begin{aligned}\sum_{i=1}^{n} x_i &= \sum_{i=1}^{n} (1 + w_i + k_i n) = \sum_{i=1}^{n} 1 + \sum_{i=1}^{n} w_i + \sum_{i=1}^{n} k_i n \\ &= n + \frac{0 + n - 1}{2} \cdot n + \frac{0 + n - 1}{2} \cdot n^2 \\ &= \frac{2n + n^2 - n + n^3 - n^2}{2} = \frac{n\,(n^2 + 1)}{2},\end{aligned}$$

que é igual à soma mágica (veja (2), na página 16). Logo, o quadrado é *mágico nas*

colunas. □

Essa propriedade, válida para uma coluna genérica, que acabamos de demonstrar é, obviamente, verdadeira também para uma linha genérica. A demonstração é inteiramente análoga.

Teorema 14 (LEHMER, 1929, p. 532)**.** *Se os coeficientes β, b e o determinante $\alpha b - \beta a$ forem primos com n então o quadrado é mágico nas linhas.*

5.1 A condição é necessária?

Vamos considerar em todos os casos a seguir que o determinante $\alpha b - \beta a$ seja primo com n, assim garantimos o preenchimento.

5.1.1 Calculando a soma das colunas

Um número $x = 1 + w + kn$ cujas coordenadas são (A, B) está na j-ésima coluna se, e somente se, w e k forem soluções de[11]

$$\alpha w + ak \equiv j - p \pmod{n} \tag{36}$$

Se $\text{mdc}(\alpha, a, n) = 1$, então pelos Teoremas 5 e 6 a equação acima sempre terá n soluções (w, k) distintas.

Observação 3. Observe que se $\text{mdc}(\alpha b - \beta a, n) = 1$, então $\text{mdc}(\alpha, a, n) = 1$.

Lema 1. *Sejam n, α, β, a e b inteiros tais que* $\text{mdc}(\alpha b - \beta a, n) = 1$. *Seja* $\text{mdc}(\alpha, n) = \delta_\alpha$. *Para cada coluna j do quadrado, existe $0 \leq k_j \leq \delta_\alpha - 1$ tal que para qualquer um dos n elementos $x = 1 + w + k \cdot n$ alocados na j-ésima coluna, temos $k = k_j + l \cdot \delta_\alpha$, sendo $0 \leq l \leq \dfrac{n}{\delta_\alpha} - 1$. Além disso, para cada $l \in \left\{0, 1, \ldots, \dfrac{n}{\delta_\alpha} - 1\right\}$, há exatamente δ_α repetições de $k = k_j + l \cdot \delta_\alpha$ dentre as soluções de interesse (w, k) de (36).*

Demonstração. Como $\text{mdc}(\alpha b - \beta a, n) = 1$, o quadrado é preenchido e a j-ésima coluna do quadrado possui exatamente n valores da forma

$$x_i = 1 + w_i + nk_i, \quad 0 \leq w_i, k_i \leq n - 1.$$

[11] $A \equiv j \pmod{n} \Rightarrow p + \alpha w + ak \equiv j \pmod{n} \Rightarrow \alpha w + ak \equiv j - p \pmod{n}$

Vamos tomar k_j como o menor valor de k_i dentre tais pares (w_i, k_i). Certamente, existe $w_j \in \{0, 1, 2, \ldots, n-1\}$ tal que (w_j, k_j) satisfaz (36). Isto é

$$\alpha w_j + a k_j \equiv j - p \pmod{n}.$$

Observe que para cada l tal que $0 \leq l \leq \dfrac{n}{\delta_\alpha} - 1$, pelo Teorema 5, a ECL

$$\alpha w_i + a\left(k_j + l\delta_\alpha\right) \equiv j - p \pmod{n}. \tag{37}$$

admite solução. Pelo Teorema 6, há δ_α valores de w_i.

Observe ainda que $0 \leq k_j \leq \delta_\alpha - 1$. De fato, se $k_j \geq \delta_\alpha$, tomando $l = \frac{n}{\delta_\alpha} - 1$ em (37), vemos que existe $\tilde{w}$ tal que $x = 1 + \tilde{w} + (k_j - \delta_\alpha)n$ pertence à j-ésima coluna contrariando o fato de k_j ser mínimo.
Consequentemente, dentre os n elementos da diagonal, os k_i's assumem $\dfrac{n}{\delta_\alpha}$ valores distintos e cada um deles se repete δ_α vezes. □

Corolário 2. *Se em* $\alpha w + ak \equiv j - p \pmod{n}$, $\mathrm{mdc}(\alpha, n) = 1$, *então os* k*'s formam um sistema completo de resíduos.*

Observação 4. Observe que k_j depende de j e é o menor valor de $k \in \{0, 1, \ldots, n-1\}$ que torna $j - p - ak_j$ divisível por δ_α. Conforme j varia de 1 a n, como $\mathrm{mdc}(a, \delta_\alpha) = 1$, k_j irá assumir (em alguma ordem) todos os valores de 0 a $\delta_\alpha - 1$.

Um resultado análogo é válido se $\mathrm{mdc}(a, n) = \delta_a$.

Lema 2. *Sejam* n, α, β, a *e* b *inteiros tais que* $\mathrm{mdc}(\alpha b - \beta a, n) = 1$. *Seja* $\mathrm{mdc}(a, n) = \delta_a$. *Para cada coluna* j *do quadrado, existe* $0 \leq w_j \leq \delta_a - 1$ *tal que para qualquer um dos* n *elementos* $x = 1 + w + k \cdot n$ *alocados na* j*-ésima coluna, temos* $w = w_j + t \cdot \delta_a$, *sendo* $0 \leq t \leq \dfrac{n}{\delta_a} - 1$. *Além disso, para cada* $t \in \left\{0, 1, \ldots, \dfrac{n}{\delta_a} - 1\right\}$, *há exatamente* δ_a *repetições de* $w = w_j + t \cdot \delta_a$ *dentre as soluções de interesse* (w, k) *de (36).*

Corolário 3. *Se em* $\alpha w + ak \equiv j - p \pmod{n}$, $\mathrm{mdc}(a, n) = 1$ *então os* w*'s formam um sistema completo de resíduos.*

Observação 5. Observe que w_j depende de j e é o menor valor de $w \in \{0, 1, \ldots, n-1\}$ que torna $j - p - \alpha w_j$ divisível por δ_a. Conforme j varia de 1 a n, como $\mathrm{mdc}(\alpha, \delta_a) = 1$, w_j irá assumir (em alguma ordem) todos os valores de 0 a $\delta_a - 1$.

Sejam $\mathrm{mdc}(a, n) = \delta_a$ e $\mathrm{mdc}(\alpha, n) = \delta_\alpha$ e x_i, $i = 1, \ldots, n$ os elementos da j-ésima coluna do quadrado. Inicialmente, vamos calcular a soma de todos os k's associados a esses elementos. Uma vez que $\mathrm{mdc}(\alpha, n) = \delta_\alpha$, pelo Lema 1, os k's poderão assumir $\dfrac{n}{\delta_\alpha}$ valores no conjunto

$$\{0, 1, 2, \ldots, n-1\}.$$

Esses valores dependem de $j - p$ e pertencem a um dos seguintes conjuntos disjuntos

$$\left\{0, \delta_\alpha, 2\delta_\alpha, \ldots, \left(\frac{n}{\delta_\alpha} - 1\right)\delta_\alpha\right\},$$
$$\left\{1, 1+\delta_\alpha, 1+2\delta_\alpha, \ldots, 1+\left(\frac{n}{\delta_\alpha} - 1\right)\delta_\alpha\right\},$$
$$\left\{2, 2+\delta_\alpha, 2+2\delta_\alpha, \ldots, 2+\left(\frac{n}{\delta_\alpha} - 1\right)\delta_\alpha\right\},$$
$$\vdots$$
$$\left\{\delta_\alpha - 1, 2\delta_\alpha - 1, 3\delta_\alpha - 1, \ldots, \frac{n}{\delta_\alpha}\cdot\delta_\alpha - 1\right\}.$$

O conjunto que inicia com 0 terá como soma dos seus elementos:

$$0 + \delta_\alpha + 2\delta_\alpha + \cdots + \left(\frac{n}{\delta_\alpha} - 1\right)\delta_\alpha = \frac{n}{2}\left(\frac{n}{\delta_\alpha} - 1\right)$$

Indutivamente, é possível mostrar que para cada inteiro k_j tal que $0 \leq k_j \leq \delta_\alpha - 1$, o conjunto que inicia com k_j terá soma:

$$\frac{n}{2}\left(\frac{n}{\delta_\alpha} - 1\right) + \frac{k_j n}{\delta_\alpha}$$

Vimos no Lema 1 que cada um desses conjuntos se repete δ_α vezes, logo a soma dos k_i's, de uma coluna, será

$$\sum_{i=1}^{n} k_i = \frac{n}{2}\left(n - \delta_\alpha\right) + k_j n$$

Analogamente, é possível mostrar que se x_i, $i = 1, \ldots, n$ são os elementos da j-ésima coluna, os w's associados a esses elementos poderão assumir $\dfrac{n}{\delta_a}$ valores no conjunto

$\{0, 1, 2, \ldots, n-1\}$.

Esses valores dependem de $j - p$ e pertencem a um dos seguintes conjuntos disjuntos

$$\left\{0, \delta_a, 2\delta_a, \ldots, \left(\frac{n}{\delta_a} - 1\right)\delta_a\right\},$$
$$\left\{1, 1+\delta_a, 1+2\delta_a, \ldots, 1+\left(\frac{n}{\delta_a} - 1\right)\delta_a\right\},$$
$$\left\{2, 2+\delta_a, 2+2\delta_a, \ldots, 2+\left(\frac{n}{\delta_a} - 1\right)\delta_a\right\},$$
$$\vdots$$
$$\left\{\delta_a - 1, 2\delta_a - 1, 3\delta_a - 1, \ldots, \frac{n}{\delta_a}\cdot\delta_a - 1\right\}.$$

O conjunto que inicia com 0 terá como soma de seus elementos:

$$0 + \delta_a + 2\delta_a + \cdots + \left(\frac{n}{\delta_a} - 1\right)\delta_a = \frac{n}{2}\left(\frac{n}{\delta_a} - 1\right)$$

Indutivamente, é possível mostrar que para cada inteiro w_j tal que $0 \leq w_j \leq \delta_a - 1$, o conjunto que inicia com w_j terá soma:

$$\frac{n}{2}\left(\frac{n}{\delta_a} - 1\right) + \frac{w_j n}{\delta_a}$$

Vimos no Lema 1 que cada um desses conjuntos se repete δ_α vezes, logo a soma dos w_i's, de uma coluna, será

$$\sum_{i=1}^{n} w_i = \frac{n}{2}(n - \delta_a) + w_j n.$$

A soma dos elementos x_i da j-ésima coluna é

$$\begin{aligned}
C_j &= \sum_{i=1}^{n} x_i = \sum_{i=1}^{n}(1 + w_i + k_i \cdot n) \\
&= \sum_{i=1}^{n} 1 + \sum_{i=1}^{n} w_i + \sum_{i=1}^{n} k_i \cdot n \\
&= n + \left[\frac{n}{2}\cdot(n - \delta_a) + w_j n\right] + \left[\frac{n}{2}\cdot(n - \delta_\alpha) + k_j n\right]\cdot n \\
&= n + n\cdot w_j + \frac{n^2}{2} - \delta_a \cdot \frac{n}{2} + n^2 \cdot k_j + \frac{n^3}{2} - \delta_\alpha \cdot \frac{n^2}{2} \\
&= \frac{n}{2} + \frac{n^3}{2} + \frac{n}{2} + n\cdot w_j + n^2 \cdot k_j + \frac{n^2}{2} - \delta_a \cdot \frac{n}{2} - \delta_\alpha \cdot \frac{n^2}{2}
\end{aligned}$$

Isto é

$$C_j = \left(\frac{1+n^2}{2}\right) n + \left(w_j - \frac{\delta_a - 1}{2}\right) n + \left(k_j - \frac{\delta_\alpha - 1}{2}\right) n^2 \tag{38}$$

Os resultados estabelecidos para as colunas se estendem naturalmente para as linhas.

5.1.2 Calculando a soma das linhas

Um número $x = 1 + w + kn$ cujas coordenadas são (A, B) está na m-ésima linha se, e somente se, w e k forem soluções de

$$\beta w + bk \equiv m - q \pmod{n} \tag{39}$$

Se $\text{mdc}(\beta, b, n) = 1$, então pelos Teoremas 5 e 6 a equação acima sempre terá n soluções (w, k) distintas.

Observação 6. Observe que se $\text{mdc}(\alpha b - \beta a, n) = 1$, então $\text{mdc}(\beta, b, n) = 1$.

Lema 3. *Sejam n, α, β, a e b inteiros tais que $\text{mdc}(\alpha b - \beta a, n) = 1$. Seja $\text{mdc}(\beta, n) = \delta_\beta$. Para cada linha m do quadrado, existe $0 \leq k_m \leq \delta_\beta - 1$ tal que para qualquer um dos n elementos $x = 1 + w + k \cdot n$ alocados m-ésima linha, temos $k = k_m + l \cdot \delta_\beta$, sendo $0 \leq l \leq \dfrac{n}{\delta_\beta} - 1$. Além disso, para cada $l \in \left\{0, 1, \ldots, \dfrac{n}{\delta_\beta} - 1\right\}$, há exatamente δ_β repetições de $k = k_m + l \cdot \delta_\beta$ dentre as soluções de interesse (w, k) de (39).*

Corolário 4. *Se em $\beta w + bk \equiv m - q \pmod{n}$, $\text{mdc}(\beta, n) = 1$ então os k's formam um sistema completo de resíduos.*

Observação 7. Observe que k_m depende de m e é o menor valor de $k \in \{0, 1, \ldots, n-1\}$ que torna $m - q - bk_m$ divisível por δ_β. Conforme m varia de 1 a n, como $\text{mdc}(b, \delta_\beta) = 1$, k_m irá assumir (em alguma ordem) todos os valores de 0 a $\delta_\beta - 1$.

Um resultado análogo é válido se $\text{mdc}(b, n) = \delta_b$.

Lema 4. *Sejam n, α, β, a e b inteiros tais que $\text{mdc}(\alpha b - \beta a, n) = 1$. Seja $\text{mdc}(b, n) = \delta_b$. Para cada linha m do quadrado, existe $0 \leq w_m \leq \delta_b - 1$ tal que para qualquer um dos n elementos $x = 1 + w + k \cdot n$ alocados m-ésima linha, temos $w = w_m + t \cdot \delta_b$, sendo $0 \leq t \leq \dfrac{n}{\delta_b} - 1$. Além disso, para cada $t \in \left\{0, 1, \ldots, \dfrac{n}{\delta_b} - 1\right\}$, há exatamente δ_b repetições de $w = w_m + t \cdot \delta_b$ dentre as soluções de interesse (w, k) de (39).*

Corolário 5. *Se em* $\beta w + bk \equiv m - q \pmod{n}$, $\mathrm{mdc}(b, n) = 1$ *então os* w*'s formam um sistema completo de resíduos.*

Observação 8. Observe que w_m depende de m e é o menor valor de $w \in \{0, 1, \ldots, n-1\}$ que torna $m - q - \beta w_m$ divisível por δ_b. Conforme m varia de 1 a n, como $\mathrm{mdc}(\alpha, \delta_b) = 1$, w_m irá assumir (em alguma ordem) todos os valores de 0 a $\delta_b - 1$.

Sejam $\mathrm{mdc}(b, n) = \delta_b$ e $\mathrm{mdc}(\beta, n) = \delta_\beta$ e x_i, $i = 1, \ldots, n$ os elementos da m-ésima linha do quadrado. Inicialmente, vamos calcular a soma de todos os k's associados a esses elementos. Uma vez que $\mathrm{mdc}(\beta, n) = \delta_\beta$, pelo Lema 3, os k's poderão assumir $\dfrac{n}{\delta_\beta}$ valores no conjunto

$$\{0, 1, 2, \ldots, n-1\}.$$

Esses valores dependem de $m - q$ e pertencem a um dos seguintes conjuntos disjuntos

$$\begin{gathered}
\left\{0, \delta_\beta, 2\delta_\beta, \ldots, \left(\frac{n}{\delta_\beta} - 1\right)\delta_\beta\right\}, \\
\left\{1, 1+\delta_\beta, 1+2\delta_\beta, \ldots, 1+\left(\frac{n}{\delta_\beta} - 1\right)\delta_\beta\right\}, \\
\left\{2, 2+\delta_\beta, 2+2\delta_\beta, \ldots, 2+\left(\frac{n}{\delta_\beta} - 1\right)\delta_\beta\right\}, \\
\vdots \\
\left\{\delta_\beta - 1, 2\delta_\beta - 1, 3\delta_\beta - 1, \ldots, \frac{n}{\delta_\beta}\cdot\delta_\beta - 1\right\}.
\end{gathered}$$

e sua soma será dada por

$$\sum k = \frac{n}{2}(n - \delta_\beta) + k_m n, \quad 0 \leq k_m \leq \delta_\beta - 1. \tag{40}$$

Analogamente, é possível mostrar que se x_i, $i = 1, \ldots, n$ são os elementos da m-ésima linha, os w's associados a esses elementos poderão assumir $\dfrac{n}{\delta_b}$ valores no conjunto

$$\{0, 1, 2, \ldots, n-1\}.$$

Esses valores dependem de $m-q$ e pertencem a um dos seguintes conjuntos disjuntos

$$\left\{0, \delta_b, 2\delta_b, \ldots, \left(\frac{n}{\delta_b} - 1\right)\delta_b\right\},$$
$$\left\{1, 1+\delta_b, 1+2\delta_b, \ldots, 1+\left(\frac{n}{\delta_b} - 1\right)\delta_b\right\},$$
$$\left\{2, 2+\delta_b, 2+2\delta_b, \ldots, 2+\left(\frac{n}{\delta_b} - 1\right)\delta_b\right\},$$
$$\vdots$$
$$\left\{\delta_b - 1, 2\delta_b - 1, 3\delta_b - 1, \ldots, \frac{n}{\delta_b}\cdot\delta_b - 1\right\}.$$

e sua soma é dada por

$$\sum w = \frac{n}{2}(n - \delta_b) + w_m n, \quad 0 \leq w_m \leq \delta_b - 1. \tag{41}$$

Por (40) e (41), podemos deduzir que a soma dos elementos x_i da m-ésima linha é dada por

$$C_m = \left(\frac{1+n^2}{2}\right)n + \left(w_m - \frac{\delta_b - 1}{2}\right)n + \left(k_m - \frac{\delta_\beta - 1}{2}\right)n^2.$$

5.1.3 Condição necessária para que colunas e linhas sejam mágicas

Teorema 15. *Sejam n, α, β, a e b inteiros tais que* $\mathrm{mdc}(\alpha b - \beta a, n) = 1$. *Suponha o quadrado gerado com tais parâmetros pelo método do passo uniforme seja mágico nas colunas. Então,* $\mathrm{mdc}(a, n) = \mathrm{mdc}(\alpha, n) = 1$.

Demonstração. Sejam $\mathrm{mdc}(a, n) = \delta_a$ e $\mathrm{mdc}(\alpha, n) = \delta_\alpha$. Como as colunas são mágicas, para todo $j \in \{1, \ldots, n\}$, por (38), temos

$$w_j - \frac{\delta_a - 1}{2} = n\left(\frac{\delta_\alpha - 1}{2} - k_j\right).$$

O lado direito é um múltiplo de n e o esquerdo é um inteiro entre $-n$ e n. Consequentemente, para todo $j \in \{1, \ldots, n\}$,

$$w_j - \frac{\delta_a - 1}{2} = \frac{\delta_\alpha - 1}{2} - k_j = 0.$$

Pelas Observações 4 e 5, se δ_α ou δ_a for diferente de 1, existe j tal que

$$w_j - \frac{\delta_a - 1}{2} \neq 0 \qquad \text{ou} \qquad \frac{\delta_\alpha - 1}{2} - k_j \neq 0.$$

Portanto, se todas as colunas são mágicas temos, $\delta_a = \delta_\alpha = 1$. □

Analogamente,

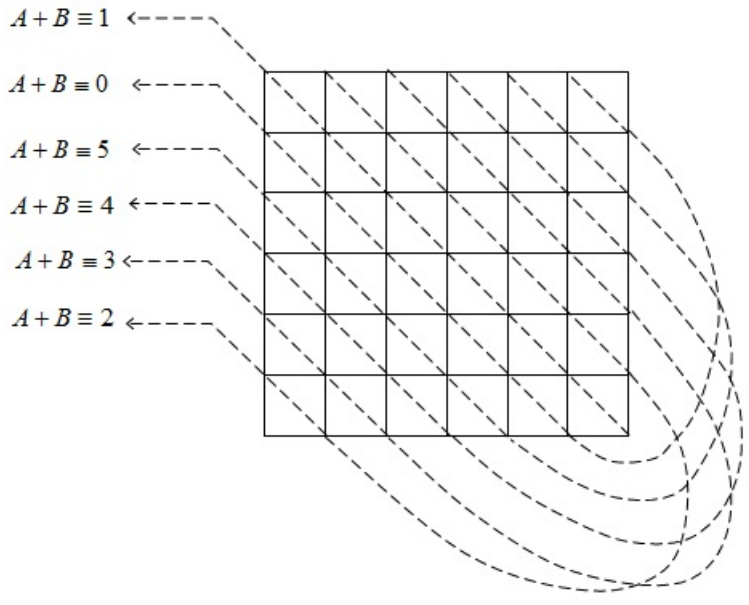
Teorema 16. *Sejam n, α, β, a e b inteiros tais que* $\text{mdc}(\alpha b - \beta a, n) = 1$. *Suponha o quadrado gerado com tais parâmetros pelo método do passo uniforme seja mágico nas linhas. Então,* $\text{mdc}(b, n) = \text{mdc}(\beta, n) = 1$.

A este ponto, podemos afirmar que o método do passo uniforme não gera quadrados mágicos nas linhas e nas colunas, ao mesmo tempo, quando n for par. De acordo como os Teoremas 15 e 16, para que todas as linhas e todas as colunas sejam mágicas é necessário que os parâmetros α, β, a e b sejam, um a um, primos com n. Ora, se n for par, então todos têm de ser ímpar. Mas se todos forem ímpar, o determinante $\alpha b - \beta a$ é par, consequentemente tendo um divisor comum diferente de 1 com n e portanto, de acordo com o Teorema 10, não preenchendo o quadrado.

6 DIAGONAIS PRINCIPAIS POSITIVA E NEGATIVA MÁGICAS

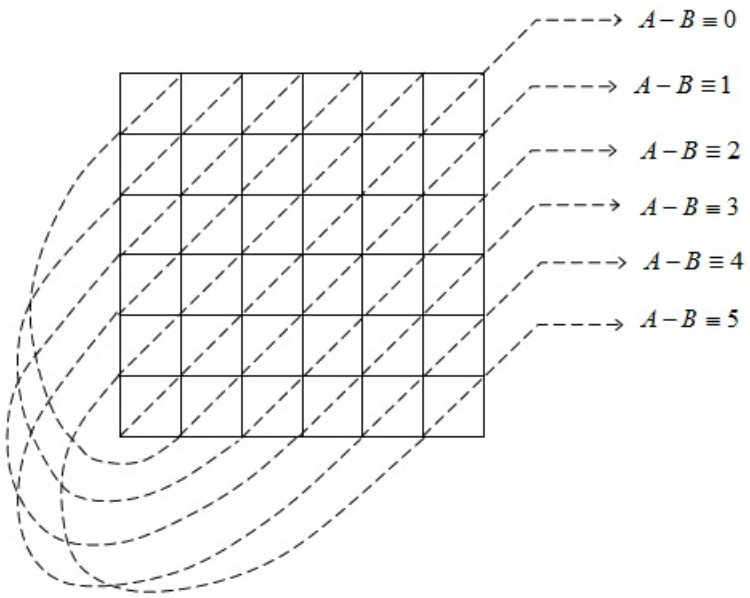
Sejam A e B as coordenadas de uma célula do quadrado. Vamos denominar *diagonal principal positiva* a diagonal regida por $A + B \equiv 1 \pmod{n}$ e *diagonal principal negativa* a diagonal regida por $A - B \equiv 0 \pmod{n}$. Note que a reta r que passa pelo canto inferior direito do quadrado e por seu canto superior esquerdo intercepta todos os pontos de coordenadas (A, B) tais que $A + B \equiv 1$. Além disso, vemos em cada linha e em cada coluna do quadrado há apenas uma célula que satisfaz $A + B \equiv 1$. O termo *diagonal* pode ser generalizado da seguinte maneira: considere a reta paralela a r que passa pela célula da n-ésima linha e que está na p-ésima coluna contada a partir da direita e a reta paralela a r que passa pela célula da primeira coluna e p-ésima linha. Ao todo, essas duas retas interceptam n células do quadrado, e apenas uma de linha e de cada coluna. Tais diagonais são chamadas de diagonais positivas do quadrado. (KRAITCHIK, 1942, p. 143) As diagonais positivas do quadrado preenchidas pelo método do passo uniforme são determinadas pela equação $A + B \equiv j$, Figura 22. As diagonais negativas podem

Figura 22 - Diagonais positivas.



Fonte: O autor, 2014.

Figura 23 - Diagonais negativas.



Fonte: O autor, 2014.

ser definidas de modo análogo. As diagonais negativas por $A - B \equiv j$, Figura 23, com $j = 0, 1, 2, \ldots, n-1$. Antes de prosseguir, devemos enfatizar que em todos os casos desta seção estaremos considerando que o determinante $\alpha b - \beta a$ seja primo com n, o que irá garantir o preenchimento do quadrado, e também cada parâmetro α, β, a e b primo com n o que garantirá linhas e colunas mágicas. Essas duas condições juntas, como já visto anteriormente[12], descartam todos os quadrados de ordem par. Portanto, só serão considerados, os quadrados de ordem ímpar.

6.1 Condições para que a diagonal principal negativa seja mágica

Nosso interesse agora é obter condições para que a diagonal principal negativa seja mágica. Um número $x = 1 + w + kn$ está na diagonal principal negativa se, e somente se, w e k forem soluções de $A - B \equiv 0$.

$$A \equiv B \pmod{n} \quad \Rightarrow \quad p + w\alpha + ka \equiv q + w\beta + kb \pmod{n}$$

[12] A condição para o preenchimento é o determinante $\alpha b - \beta a$ ser primo com n. Se n for par então o determinante $\alpha b - \beta a$ deverá ser ímpar, o que implica em pelo menos um dos parâmetros α ou β ou a ou b ser par o que implica por sua vez em algumas colunas ou linhas não mágicas.

Segue,

$$(\alpha - \beta)w + (a - b)k \equiv q - p \pmod{n} \tag{42}$$

Se $\text{mdc}(\alpha - \beta, a - b, n) = 1$ então pelos Teoremas 5 e 6 a equação acima sempre terá n soluções (w, k) distintas.

Observação 9. Se o método preenche o quadrado, então n números são dispostos na diagonal principal negativa. Isto é, (42) tem n soluções pertencentes ao conjunto $\{1, 2, \ldots, n^2\}$.

Observação 10. Observe que se $\text{mdc}(\alpha b - \beta a, n) = 1$, então $\text{mdc}(\alpha - \beta, a - b, n) = 1$.

De fato, vamos supor que $\text{mdc}(\alpha - \beta, a - b, n) = \delta \neq 1$. Então, $\delta \mid \alpha - \beta$, $\delta \mid a - b$ e $\delta \mid n$.

Agora

$$\delta \mid \alpha - \beta \Rightarrow \delta \mid \alpha b - \beta b$$
$$\delta \mid a - b \Rightarrow \delta \mid a\beta - b\beta$$

Subtraindo uma da outra, temos:

$$\delta \mid (\alpha b - \beta b) - (a\beta - b\beta) \Rightarrow \delta \mid \alpha b - \beta a$$

Logo, como $\delta \mid n$ e $\delta \mid \alpha b - \beta a$, temos $\text{mdc}(\alpha b - \beta a, n) \neq 1$. □

Lema 5. *Sejam n, α, β, a e b inteiros tais que $\text{mdc}(\alpha b - \beta a, n) = 1$. Seja $\text{mdc}(\alpha - \beta, n) = \delta_k^-$. Existe $0 \leq k_0 \leq \delta_k^- - 1$ tal que para qualquer uma das n soluções (w, k), com $0 \leq w, k \leq n - 1$ da equação $(\alpha - \beta)w + (a - b)k \equiv q - p \pmod{n}$, temos $k = k_0 + l \cdot \delta_k^-$, sendo $0 \leq l \leq \dfrac{n}{\delta_k^-} - 1$. Além disso, para cada $l \in \left\{0, 1, \ldots, \dfrac{n}{\delta_k^-} - 1\right\}$, há exatamente δ_k^- repetições de $k = k_0 + l \cdot \delta_k^-$ dentre essas n soluções (w, k) de (42).*

Demonstração. Como $\text{mdc}(\alpha b - \beta a, n) = 1$, o quadrado é preenchido e a diagonal do quadrado possui exatamente n valores da forma

$$x_i = 1 + w_i + nk_i, \quad 0 \leq w_i, k_i \leq n - 1.$$

Consequentemente, há exatamente n pares (w_i, k_i) (com $0 \leq w_i, k_i \leq n-1$) que satisfazem $(\alpha - \beta)w + (a - b)k \equiv q - p \pmod{n}$. Vamos tomar k_0 como o menor valor de k_i dentre tais pares (w_i, k_i). Certamente, existe $w_0 \in \{0, 1, 2, \ldots, n - 1\}$ tal que (w_0, k_0) satisfaz $(\alpha - \beta)w + (a - b)k \equiv q - p \pmod{n}$. Isto é

$$(\alpha - \beta)w_0 + (a - b)k_0 \equiv q - p \pmod{n}.$$

Observe que para cada l tal que $0 \leq l \leq \dfrac{n}{\delta_k^-} - 1$, pelo Teorema 5, a ECL

$$(\alpha - \beta)w_i + (a - b)\left(k_0 + l\delta_k^-\right) \equiv q - p \pmod{n}. \tag{43}$$

admite solução. Pelo Teorema 6, há δ_k^- valores de w_i.
Observe ainda que $0 \leq k_0 \leq \delta_k^- - 1$. De fato, se $k_0 \geq \delta_k^-$, tomando $l = \frac{n}{\delta_k^-} - 1$ em (43), vemos que existe $\tilde{w}$ tal que $x = 1 + \tilde{w} + (k_0 - \delta_k^-)n$ pertence à diagonal negativa contrariando o fato de k_0 ser mínimo.
Consequentemente, dentre os n elementos da diagonal, os k's assumem $\dfrac{n}{\delta_k^-}$ valores distintos e cada um deles se repete δ_k^- vezes. □

Corolário 6. *Se em* $(\alpha - \beta)w + (a - b)k \equiv q - p \pmod{n}$, $\mathrm{mdc}(\alpha - \beta, n) = 1$, *então os* k*'s formam um sistema completo de resíduos módulo* n.

Um resultado análogo é válido se $\mathrm{mdc}(a - b, n) = \delta_w^-$.

Lema 6. *Sejam* n, α, β, a *e* b *inteiros tais que* $\mathrm{mdc}(\alpha b - \beta a, n) = 1$. *Seja* $\mathrm{mdc}(a - b, n) = \delta_w^-$. *Existe* $0 \leq w_0 \leq \delta_w^- - 1$ *tal que para qualquer uma das* n *soluções* (w, k), *com* $0 \leq w, k \leq n - 1$ *da equação (42), temos* $w = w_0 + t \cdot \delta_w^-$, *sendo* $0 \leq t \leq \dfrac{n}{\delta_w^-} - 1$. *Além disso, para cada* $t \in \left\{0, 1, \ldots, \dfrac{n}{\delta_w^-} - 1\right\}$, *há exatamente* δ_w^- *repetições de* $w = w_0 + t \cdot \delta_w^-$ *dentre essas* n *soluções* (w, k) *de (42).*

Corolário 7. *Se em* $(\alpha - \beta)w + (a - b)k \equiv q - p \pmod{n}$, $\mathrm{mdc}(a - b, n) = 1$, *então os* w*'s formam um sistema completo de resíduos módulo* n.

6.1.1 Calculando a soma da diagonal

Sejam $\mathrm{mdc}(a - b, n) = \delta_w^-$ e $\mathrm{mdc}(\alpha - \beta, n) = \delta_k^-$ e x_i, $i = 1, \ldots, n$ os elementos da diagonal principal negativa. Inicialmente, vamos calcular a soma de todos os k's associados a esses elementos. Uma vez que $\mathrm{mdc}(\alpha - \beta, n) = \delta_k^-$, pelo Lema 5, os k's poderão assumir $\dfrac{n}{\delta_k^-}$ valores no conjunto

$\{0, 1, 2, \ldots, n - 1\}$.

Esses valores dependem de $q-p$ e pertencem a um dos seguintes conjuntos disjuntos

$$\left\{0, \delta_k^-, 2\delta_k^-, \ldots, \left(\frac{n}{\delta_k^-} - 1\right)\delta_k^-\right\},$$
$$\left\{1, 1+\delta_k^-, 1+2\delta_k^-, \ldots, 1+\left(\frac{n}{\delta_k^-} - 1\right)\delta_k^-\right\},$$
$$\left\{2, 2+\delta_k^-, 2+2\delta_k^-, \ldots, 2+\left(\frac{n}{\delta_k^-} - 1\right)\delta_k^-\right\},$$
$$\vdots$$
$$\left\{\delta_k^- - 1, 2\delta_k^- - 1, 3\delta_k - 1, \ldots, \frac{n}{\delta_k^-}\cdot\delta_k^- - 1\right\}.$$

O conjunto que inicia com 0 terá soma:

$$0 + \delta_k^- + 2\delta_k^- + \cdots + \left(\frac{n}{\delta_k^-} - 1\right)\delta_k^- = \frac{n}{2}\left(\frac{n}{\delta_k^-} - 1\right)$$

Indutivamente, é possível mostrar que para cada inteiro r_k tal que $0 \leq r_k \leq \delta_k^- - 1$, o conjunto que inicia com r_k terá soma:

$$\frac{n}{2}\left(\frac{n}{\delta_k^-} - 1\right) + \frac{r_k n}{\delta_k^-}$$

Vimos no Lema 5 que cada um desses conjuntos se repete δ_k^- vezes, logo a soma dos k's, será dada por

$$\sum k = \frac{n}{2}\left(n - \delta_k^-\right) + r_k n \tag{44}$$

Veremos que p e q devem ser escolhidos de modo que os valores de k na diagonal principal negativa sejam os do conjunto

$$R_k = \left\{r_k, r_k + \delta_k^-, r_k + 2\delta_k^-, \ldots, r_k + \left(\frac{n}{\delta_k^-} - 1\right)\delta_k^-\right\}$$

onde

$$r_k = \frac{\delta_k^- - 1}{2}.$$

Analogamente, é possível mostrar que se x_i, $i = 1, \ldots, n$ são os elementos da diagonal principal negativa, os w's associados a esses elementos poderão assumir $\dfrac{n}{\delta_w^-}$ valores no conjunto

$$\{0, 1, 2, \ldots, n-1\}.$$

Esses valores dependem de $q-p$ e pertencem a um dos seguintes conjuntos disjuntos

$$\begin{gathered}
\left\{0, \delta_w^-, 2\delta_w^-, \ldots, \left(\frac{n}{\delta_w^-} - 1\right)\delta_w^-\right\}, \\
\left\{1, 1+\delta_w^-, 1+2\delta_w^-, \ldots, 1+\left(\frac{n}{\delta_w^-} - 1\right)\delta_w^-\right\}, \\
\left\{2, 2+\delta_w^-, 2+2\delta_w^-, \ldots, 2+\left(\frac{n}{\delta_w^-} - 1\right)\delta_w^-\right\}, \\
\vdots \\
\left\{\delta_w^- - 1, 2\delta_w^- - 1, 3\delta_w^- - 1, \ldots, \frac{n}{\delta_w^-}\cdot\delta_w^- - 1\right\}.
\end{gathered}$$

e sua soma é dada por

$$\sum w = \frac{n}{2}\left(n - \delta_w^-\right) + r_w n \tag{45}$$

onde r_w é um inteiro tal que $0 \leq r_w \leq \delta_w^- - 1$.
Veremos também que p e q devem ser escolhidos de modo que os valores de w na diagonal principal negativa sejam os do conjunto

$$R_w = \left\{r_w, r_w + \delta_w^-, r_w + 2\delta_w^-, \ldots, r_w + \left(\frac{n}{\delta_w^-} - 1\right)\delta_w^-\right\}$$

onde

$$r_w = \frac{\delta_w^- - 1}{2}.$$

Por (44) e (45), podemos deduzir que a soma dos elementos x_i da diagonal principal positiva é dada por

$$\begin{aligned}
\sum_i x_i &= \sum_i 1 + \sum w + n\sum k \\
&= n + \frac{n}{2}\left(n - \delta_w^-\right) + r_w n + \frac{n^2}{2}\left(n - \delta_k^-\right) + r_k n^2 \\
&= n + r_w n + \frac{n}{2}\left(n - \delta_w^-\right) + r_k n^2 + \frac{n^2}{2}\left(n - \delta_k^-\right)
\end{aligned} \tag{46}$$

6.1.2 Condição necessária e suficiente

Teorema 17. *Sejam $x_i = 1 + w_i + nk_i$, $0 \leq w_i, k_i \leq n-1$, $i = 1, \ldots, n$, os elementos da diagonal principal negativa. Sejam $\mathrm{mdc}(a-b, n) = \delta_w^-$ e $\mathrm{mdc}(\alpha - \beta, n) = \delta_k^-$. Para que a diagonal principal negativa seja mágica é necessário e suficiente que p e q sejam*

escolhidos de modo que

$$r_k = \frac{\delta_k^- - 1}{2} \quad e \quad r_w = \frac{\delta_w^- - 1}{2}$$

sejam respectivamente o menor k e o menor w dentre todas os elementos x_i da diagonal.

Demonstração. Vamos mostrar que se

$$r_w = \frac{\delta_w^- - 1}{2} \quad \text{e} \quad r_k = \frac{\delta_k^- - 1}{2}$$

então $\sum x_i$ será igual à soma mágica $\left(\frac{1+n^2}{2}\right) n$.

Por (46), temos

$$\sum_i x_i = n + r_w n + \frac{n}{2}\left(n - \delta_w^-\right) + r_k n^2 + \frac{n^2}{2}\left(n - \delta_k^-\right)$$

Substituindo $r_w = \frac{\delta_w^- - 1}{2}$ e $r_k = \frac{\delta_k^- - 1}{2}$, temos:

$$\begin{aligned}\sum_i x_i &= n + \left(\frac{\delta_w^- - 1}{2}\right) n + \frac{n}{2}\left(n - \delta_w^-\right) + \left(\frac{\delta_k^- - 1}{2}\right) n^2 + \frac{n^2}{2}\left(n - \delta_k^-\right) \\ &= n + \frac{\delta_w^-}{2} n - \frac{n}{2} + \frac{n^2}{2} - \frac{\delta_w^-}{2} n + \frac{\delta_k^-}{2} n^2 - \frac{n^2}{2} + \frac{n^3}{2} - \frac{\delta_k^-}{2} n^2\end{aligned}$$

Após os devidos cancelamentos, temos:

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

Pelo Lema 5, sabemos que o menor r_{k_1} associado aos elementos da diagonal é tal que

$$r_{k_1} = \frac{\delta_k^- - 1}{2} \pm t = r_k \pm t,$$

sendo $0 \leq t \leq \frac{\delta_k^- - 1}{2} - 1$. Mostraremos então a soma $\sum k$ irá variar de $\pm tn$ em relação à soma de um sistema completo de resíduos módulo n. De fato, por (44)

$$\begin{aligned}\sum k &= \frac{n}{2}\left(n - \delta_k^-\right) + r_{k_1} n = \left[(r_k \pm t)n + \frac{n}{2}(n - \delta_k^-)\right] = \left[r_k n + \frac{n}{2}(n - \delta_k^-)\right] \pm tn \\ &= \left[\left(\frac{\delta_k^- - 1}{2}\right) n + \frac{n}{2}(n - \delta_k^-)\right] \pm tn = \frac{n(n-1)}{2} \pm tn\end{aligned}$$

Analogamente, se o menor r_{w_1} associado aos elementos da diagonal é tal que

$$r_{w_1} = \frac{\delta_w^- - 1}{2} \pm l = r_w \pm l,$$

então a soma $\sum w$ irá variar de $\pm ln$ em relação à soma de um sistema completo de resíduos módulo n. Isto é,

$$\sum w = \left[\left(\frac{\delta_w^- - 1}{2}\right) n + \frac{n}{2}(n - \delta_w^-)\right] \pm ln = \frac{n(n-1)}{2} \pm ln.$$

Consequentemente, a soma dos elementos da diagonal principal será dada por

$$\sum x = n + \frac{n(n-1)}{2} \pm ln + n\left(\frac{n(n-1)}{2} \pm tn\right) = \left(\frac{1+n^2}{2}\right) n \pm ln \pm tn^2.$$

Claramente, $\sum x$ será mágica se, se somente se, $l = t = 0$. Isto é, se e somente se o menor k e o menor w dentre todas os elementos x da diagonal sejam respectivamente

$$r_k = \frac{\delta_k^- - 1}{2} \quad \text{e} \quad r_w = \frac{\delta_w^- - 1}{2}.$$

□

Corolário 8. *Sejam n, α, β, a e b inteiros tais que* $\text{mdc}(\alpha b - \beta a, n) = 1$. *Sejam* $\text{mdc}(\alpha - \beta, n) = \delta_k^-$ *e* $\text{mdc}(a - b, n) = \delta_w^-$. *Se p e q são tais que*

$$q - p \equiv (\alpha - \beta)\left(\frac{\delta_w^- - 1}{2}\right) + (a - b)\left(\frac{\delta_k^- - 1}{2}\right) \pmod{n}$$

então a soma dos elementos da diagonal principal negativa do quadrado gerado pelo método do passo uniforme é igual a $\frac{n(n^2+1)}{2}$.

6.1.3 Onde começar para que a DPN seja mágica?

Vimos nas seções anteriores que os elementos da diagonal principal negativa (DPN) foram caracterizados como soluções de (42). Além disso, vimos que é possível associar à DPN únicos conjuntos R_w e R_k tais que se $x = 1 + w + kn$ é um elemento da DPN, temos $w \in R_w$ e $k \in R_k$. Consequentemente, se há na DPN algum x da forma

$$x = 1 + \frac{\delta_w^- - 1}{2} + l \cdot \delta_w^- + \left(\frac{\delta_k^- - 1}{2} + t \cdot \delta_k^-\right) \cdot n$$

com $0 \leq l \leq \frac{n}{\delta_w^-} - 1, 0 \leq t \leq \frac{n}{\delta_k^-} - 1$, então

$$R_w = \left\{ r_w, r_w + \delta_w^-, r_w + 2\delta_w^-, \ldots, r_w + \left(\frac{n}{\delta_w^-} - 1 \right) \delta_w^- \right\}, \quad \text{onde } r_w = \frac{\delta_w^- - 1}{2}$$

e

$$R_k = \left\{ r_k, r_k + \delta_k^-, r_k + 2\delta_k^-, \ldots, r_k + \left(\frac{n}{\delta_k^-} - 1 \right) \delta_k^- \right\}, \quad \text{onde } r_k = \frac{\delta_k^- - 1}{2}$$

Portanto, pelo Teorema 17, a DPN é mágica.

Reciprocamente, se a DPN é mágica, pelo Teorema 17, ela contém elementos x da forma

$$x = 1 + \frac{\delta_w^- - 1}{2} + l \cdot \delta_w^- + \left(\frac{\delta_k^- - 1}{2} + t \cdot \delta_k^- \right) \cdot n$$

com $0 \leq l \leq \frac{n}{\delta_w^-} - 1, 0 \leq t \leq \frac{n}{\delta_k^-} - 1$.

Essas considerações nos permitem estabelecer a seguinte proposição.

Proposição 6. *Sejam α, β, a, b e n números inteiros tais que α, β, a, b e $\alpha b - \beta a$ são primos com n. A DPN do quadrado de ordem n construído pelo método do passo uniforme é mágica se e somente se as coordenadas (p, q) da célula inicial satisfazem*

$$(\alpha - \beta) \left(\frac{\delta_w^- - 1}{2} + l \cdot \delta_w^- \right) + (a - b) \left(\frac{\delta_k^- - 1}{2} + t \cdot \delta_k^- \right) \equiv q - p \pmod{n} \tag{47}$$

para algum $0 \leq l \leq \frac{n}{\delta_w^-} - 1, 0 \leq t \leq \frac{n}{\delta_k^-} - 1$ e onde $\delta_w^- = \text{mdc}(a-b, n)$ e $\delta_k^- = \text{mdc}(\alpha - \beta, n)$.

Note que se $\alpha - \beta$ e $a - b$ forem primos com n, a diagonal principal negativa sempre será mágica. De fato, pelos Corolários 6 e 7, a soma dos elementos x_i da diagonal principal negativa, será mágica:

$$\begin{aligned} x_1 + x_2 + \cdots + x_n &= \sum_{i=1}^{n} 1 + \sum_{i=1}^{n} w_i + n \sum_{i=1}^{n} k_i \\ &= n + (0 + 1 + 2 + \cdots + n - 1) + n(0 + 1 + 2 + \cdots + n - 1) \\ &= \left(\frac{1 + n^2}{2} \right) n \end{aligned}$$

Portanto, se os coeficientes $\alpha - \beta$ e $a - b$ da equação linear (42) com duas variáveis w e

k, módulo n, que determina a diagonal principal negativa forem primos[13] com n, ela será mágica, independentemente dos valores iniciais (p, q). Esse resultado também pode ser obtido a partir da Proposição 6. Se os coeficientes $\alpha - \beta$ e $a - b$ forem primos com n, (47) é dada por

$$(\alpha - \beta)l + (a - b)t \equiv q - p \pmod{n}$$

com $0 \leq l, t \leq n-1$. É fácil ver que podemos escolher (l, t) de modo que $(\alpha-\beta)l+(a-b)t$ gere um conjunto completo de resíduos. Isso resulta em p e q quaisquer.

Exemplo 8. O quadrado preenchido pelo método do passo uniforme com $n = 7$, $\alpha = 4$, $\beta = 2$, $a = 3$ e $b = 6$, será mágico nas linhas, nas colunas e na diagonal principal negativa, uma vez que os coeficientes $\alpha-\beta = 2$ e $a-b = -3$ são ambos primos com 7. A condição de primalidade de $\alpha-\beta$ e $a-b$ com n garante que todas as diagonais negativas sejam mágicas.

Segue da Proposição 6 que todos os possíveis valores de $q-p$ que determinam uma DPN mágica pertencem ao conjunto

$$O = \left\{ m \in \mathbb{Z},\ m \equiv m_{tl} \pmod{n}, 0 \leq l \leq \frac{n}{\delta_w^-} - 1,\ 0 \leq t \leq \frac{n}{\delta_k^-} - 1 \right\}$$

onde

$$m_{tl} = (\alpha - \beta)\left(\frac{\delta_w^- - 1}{2} + l \cdot \delta_w^-\right) + (a - b)\left(\frac{\delta_k^- - 1}{2} + t \cdot \delta_k^-\right). \tag{48}$$

Vamos investigar agora estratégias para determinar os elementos do conjunto O. Fixados t e l, pela Proposição 6, o elemento m_{tl} pode ser associado a uma DPN mágica. Consequentemente, pelo Teorema 17, deve haver um elemento x da forma

$$x = 1 + \frac{\delta_w^- - 1}{2} + \left(\frac{\delta_k^- - 1}{2} + t \cdot \delta_k^-\right) \cdot n.$$

Além disso, temos

$$(\alpha - \beta) \cdot \frac{\delta_w^- - 1}{2} + (a - b)\left(\frac{\delta_k^- - 1}{2} + t \cdot \delta_k^-\right) \equiv m_{tl} \equiv q - p \pmod{n}.$$

[13] Na verdade, com tal condição (argumentando como na prova do Teorema 13), podemos deduzir que o quadrado é mágico em todas as diagonais negativas. Isto é, nas diagonais em que

$A - B \equiv j \pmod{n},\ j = 0, 1, 2, \ldots, n-1$

Consequentemente, temos

$$O = \left\{ m \in \mathbb{Z},\ m \equiv m_{t0}, \quad 0 \leq t \leq \frac{n}{\delta_k} - 1 \right\}, \tag{49}$$

onde m_{tl} é dado por (48). Analogamente, temos

$$O = \left\{ m \in \mathbb{Z},\ m \equiv m_{0l}, \quad 0 \leq l \leq \frac{n}{\delta_w} - 1 \right\}, \tag{50}$$

onde m_{tl} é dado por (48).

Vamos ilustrar essa caracterização do conjunto O em alguns casos especiais.

Suponha $\text{mdc}(\alpha - \beta, n) = \delta \neq 1$ e $\text{mdc}(a - b, n) = 1$. Pelo Corolário 7, os w's associados às soluções de (42) formam um sistema completo de resíduos cuja soma é dada por

$$\sum_{i=1}^{n} w = \left(\frac{n-1}{2} \right) n.$$

Para obter uma DPN mágica, pelo Teorema 17, sabemos que p e q devem ser escolhidos de modo que os valores de k na diagonal principal negativa sejam os do conjunto

$$R = \left\{ r_0, r_0 + \delta, r_0 + 2\delta, \ldots, r_0 + \left(\frac{n}{\delta} - 1 \right) \delta \right\} \tag{51}$$

onde

$$r_0 = \frac{\delta - 1}{2}. \tag{52}$$

Como os w's formam um sistema completo de resíduos, por (49), para cada $k \in R$ obtemos pela congruência

$$(\alpha - \beta) \cdot 0 + (a - b) \cdot k \equiv q - p \pmod{n}$$

uma relação entre p e q para obter todas as possíveis diagonais principais negativas mágicas.

Suponha agora $\text{mdc}(\alpha - \beta, n) = 1$ e $\text{mdc}(a - b, n) = \delta \neq 1$. Esse caso é análogo ao caso anterior, apenas trocando k por w. Então, fazendo $k = 0$, para cada $w \in R$ (ver (51) e (52)), por (50), obtemos pela congruência

$$(\alpha - \beta) \cdot w + (a - b) \cdot 0 \equiv q - p \pmod{n}$$

uma relação entre p e q para obter todas as possíveis diagonais principais negativas mágicas.

Figura 24 - $n = 9$, $\alpha = 4$, $\beta = 1$, $a = 5$, $b = 1$, $p = 2$ e $q = 4$.
DPN não mágica.

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

Fonte: O autor, 2014.

Exemplo 9. Sejam $n = 9$, $\alpha = 4$, $\beta = 1$, $a = 5$ e $b = 1$. Para quais valores de p e q a diagonal negativa será mágica?

Temos

$$\alpha - \beta = 3 \qquad \text{e} \qquad a - b = 4.$$

Substituindo os valores dos coeficientes em (42), temos:

$$3w + 4k \equiv q - p \pmod 9.$$

Além disso, $\text{mdc}(3, 9) = 3 = \delta$, logo por (52), $r_0 = \dfrac{3-1}{2} = 1$, e por (51), $k \in \{1, 4, 7\}$
Por outro lado, temos $\text{mdc}(4, 9) = 1$, logo $w \in \{0, 1, 2, \ldots, 7, 8\}$

Os valores de $q - p$ são calculados fazendo $w = 0$ e k assumindo os valores do conjunto $R = \{1, 4, 7\}$, logo:

$$k = 1, \quad q - p \equiv 4 \pmod 9,$$
$$k = 4, \quad q - p \equiv 16 \pmod 9,$$
$$k = 7, \quad q - p \equiv 28 \pmod 9.$$

Logo, a diagonal principal negativa será mágica se $q - p \equiv 1$, $q - p \equiv 4$ ou $q - p \equiv 7 \pmod 9$.

Na Figura 24 o quadrado foi preenchido com as coordenadas iniciais $p = 2$ e $q = 4$. A DPN não será mágica, uma vez que $q - p \equiv 2$.

$$23 + 81 + 49 + 26 + 75 + 52 + 20 + 78 + 46 = 450 \neq 369.$$

Figura 25 - $n = 9$, $\alpha = 4$, $\beta = 1$, $a = 5$, $b = 1$.

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

(a)

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

(b)

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

(c)

Legenda: (a) DPN mágica, $p = 2$ e $q = 6$.
(b) DPN mágica, $p = 1$ e $q = 2$.
(c) DPN mágica, $p = 1$ e $q = 8$.

Fonte: O autor, 2014.

Na Figura 25a, o quadrado foi preenchido com as coordenadas iniciais $p = 2$ e $q = 6$. Uma DPN mágica será obtida, pois $q - p = 4$.

$13 + 71 + 39 + 16 + 65 + 42 + 10 + 68 + 45 = 369$.

Na Figura 25b, $p = 1$ e $q = 2$, atende a condição $q - p = 1$, uma DPN mágica será obtida:

$41 + 18 + 67 + 44 + 12 + 70 + 38 + 15 + 64 = 369$.

Na Figura 25c, $p = 1$ e $q = 8$, atende a condição $q - p = 7$, uma DPN mágica é obtida:

$11 + 69 + 37 + 14 + 72 + 40 + 17 + 66 + 43 = 369$.

Prosseguindo, vamos tentar investigar quantos valores incongruentes de $q-p$ geram DPN mágicas. Seja $q_0 - p_0$ o gerador de DPN mágicas associado a m_{00}. Isto é

$$q_0 - p_0 \equiv (\alpha - \beta) \cdot \frac{\delta_w^- - 1}{2} + (a - b) \cdot \frac{\delta_k^- - 1}{2} \pmod{n}. \tag{53}$$

Note que para qualquer outro valor $q - p$ gerador de DPN mágicas, teremos

$$q - p - (q_0 - p_0) \equiv (\alpha - \beta) \cdot l \cdot \delta_w^- + (a - b) \cdot t \cdot \delta_k^- \pmod{n}.$$

para algum $0 \leq l \leq \frac{n}{\delta_w^-} - 1$ e $0 \leq t \leq \frac{n}{\delta_k^-} - 1$. Isto nos diz que podemos obter todos os demais geradores de DPN mágicas a partir de $q_0 - p_0$ através de acréscimos da forma $(\alpha - \beta) \cdot l \cdot \delta_w^- + (a - b) \cdot t \cdot \delta_k^-$. Para identificar todos os geradores incongruentes, basta identificar quantos valores incongruentes módulo n podem ser gerados por

$$(\alpha - \beta) \cdot l \cdot \delta_w^- + (a - b) \cdot t \cdot \delta_k^- \quad \text{para} \quad 0 \leq l \leq \frac{n}{\delta_w^-} - 1 \quad \text{e} \quad 0 \leq t \leq \frac{n}{\delta_k^-} - 1.$$

Pela Observação 10 e pela Proposição 1, temos

$$\text{mdc}(\delta_k^-, \delta_w^-) = \text{mdc}(\text{mdc}(\alpha - \beta, n), \text{mdc}(a - b, n)) = \text{mdc}(\alpha - \beta, a - b, n) = 1.$$

Pelo Teorema 2, temos $\delta_k^- \cdot \delta_w^- \mid n$. Seja r_{tl} o resíduo módulo n de $(\alpha-\beta)\cdot l\cdot\delta_w^- + (a-b)\cdot t\cdot\delta_k^-$. Temos

$$(\alpha - \beta) \cdot l \cdot \delta_w^- + (a - b) \cdot t \cdot \delta_k^- \equiv r_{tl} \pmod{n}. \tag{54}$$

Sejam $M_{\alpha\beta}$ e M_{ab} naturais tais que

$$\alpha - \beta = M_{\alpha\beta} \cdot \delta_k^- \quad \text{e} \quad a - b = M_{ab} \cdot \delta_w^-.$$

Podemos reescrever (54) da seguinte maneira

$$M_{\alpha\beta} \cdot \delta_k^- \cdot \delta_w^- \cdot l + M_{ab} \cdot \delta_w^- \cdot \delta_k^- \cdot t \equiv r_{tl} \pmod{n}. \tag{55}$$

Como $\delta_k^- \cdot \delta_w^- \mid n$, temos

$$\text{mdc}(\delta_k^- \cdot \delta_w^-, n) = \delta_k^- \cdot \delta_w^-.$$

Pelo Teorema 5, $\delta_k^- \cdot \delta_w^- \mid r_{tl}$. Como $0 \leq r_{tl} \leq n - 1$, existe um inteiro r'_{tl} tal que

$$r_{tl} = r'_{tl} \cdot \delta_k^- \cdot \delta_w^-, \quad 0 \leq r'_{tl} \leq \frac{n}{\delta_k^- \delta_w^-} - 1$$

Pela Proposição 5, (55) é equivalente a

$$M_{\alpha\beta} \cdot l + M_{ab} \cdot t \equiv r'_{tl} \quad \left(\mod \frac{n}{\delta_k^- \delta_w^-} \right) \tag{56}$$

Segue de $\text{mdc}(\alpha - \beta, a - b, n) = 1$ que $\text{mdc}\left(M_{\alpha\beta}, M_{ab}, \frac{n}{\delta_k^- \cdot \delta_w^-}\right) = 1$. Pelo Teorema 5, para todo $0 \leq r'_{tl} \leq \frac{n}{\delta_k^- \delta_w^-} - 1$, (56) admite soluções. Portanto, esse é o total de geradores $q - p$ incongruentes módulo n de DPN mágicas. E para determiná-los, basta resolver

$$q - p - (q_0 - p_0) \equiv r \cdot \delta_k^- \cdot \delta_w^- \pmod{n} \tag{57}$$

para cada $r \in \left\{0, 1, \ldots, \frac{n}{\delta_k^- \delta_w^-} - 1\right\}$. Essa congruência nos diz que podemos obter todos os possíveis geradores de DPN mágicas adicionando (módulo n) ao gerador $q_0 - p_0$ a quantidade $\delta_k^- \cdot \delta_w^-$ por $\frac{n}{\delta_k^- \delta_w^-} - 1$ vezes.

Exemplo 10. Considere $\alpha = 11, \beta = 2, a = 31, b = 11$ e $n = 105$. Temos

$\text{mdc}(\alpha b - \beta a, n) = \text{mdc}(59, 105) = 1$
$\text{mdc}(\alpha, n) = \text{mdc}(\beta, n) = \text{mdc}(a, n) = \text{mdc}(b, n) = 1$
$\delta_k^- = \text{mdc}(\alpha - \beta, n) = \text{mdc}(9, 105) = 3$
$\delta_w^- = \text{mdc}(a - b, n) = \text{mdc}(20, 105) = 5$

Temos

$$R_w = \{2, 7, 12, 17, \ldots, 102\}, \qquad r_w = \frac{\delta_w^- - 1}{2} = 2$$

e

$$R_k = \{1, 4, 7, 10, \ldots, 103\}, \qquad r_k = \frac{\delta_k^- - 1}{2} = 1$$

Além disso, vimos que temos $\frac{n}{\delta_k^- \delta_w^-} = 7$ geradores de DPN mágicas incongruentes que podem ser obtidos a partir do gerador

$$q_0 - p_0 \equiv (\alpha - \beta) \cdot \frac{\delta_w^- - 1}{2} + (a - b) \cdot \frac{\delta_k^- - 1}{2} \equiv 38 \pmod{105}$$

por 6 adições módulo 105 de $\delta_k^- \cdot \delta_w^- = 15$. Temos

$q - p \in \{8, 23, 38, 53, 68, 83, 98\}$.

Esse resultado é o mesmo obtido pelo método de tomarmos, por exemplo, o primeiro

elemento de R_k e considerar

$$q - p \equiv 38 + (\alpha - \beta) \cdot l \pmod{105}, \quad l \in R_w.$$

6.2 Condições para que a diagonal principal positiva seja mágica

Nosso interesse agora é obter condições para que a diagonal principal positiva seja mágica. Um número $x = 1 + w + kn$ está na diagonal principal positiva se, e somente se, w e k forem soluções de $A + B \equiv 1$.

$$A + B \equiv 1 \pmod{n} \quad \Rightarrow \quad p + w\alpha + ka + q + w\beta + kb \equiv 1 \pmod{n}$$

Segue,

$$(\alpha + \beta)w + (a + b)k \equiv 1 - p - q \pmod{n} \tag{58}$$

Se $\text{mdc}(\alpha + \beta, a + b, n) = 1$ então pelos Teoremas 5 e 6, a equação acima sempre terá n soluções (w, k).

Observação 11. Se o método preenche o quadradro, então n números são dispostos na diagonal principal positiva. Isto é, $(\alpha+\beta)w+(a+b)k \equiv 1-p-q \pmod{n}$ tem n soluções pertencentes ao conjunto $\{1, 2, \ldots, n^2\}$.

Observação 12. Observe que se $\text{mdc}(\alpha b - \beta a, n) = 1$, então $\text{mdc}(\alpha + \beta, a + b, n) = 1$.

De fato, vamos supor que $\text{mdc}(\alpha + \beta, a + b, n) = \delta \neq 1$. Então, $\delta \mid \alpha + \beta$, $\delta \mid a + b$ e $\delta \mid n$. Agora

$$\delta \mid \alpha + \beta \Rightarrow \delta \mid \alpha b + \beta b$$
$$\delta \mid a + b \Rightarrow \delta \mid a\beta + b\beta$$

Subtraindo uma da outra, temos:

$$\delta \mid (\alpha b + \beta b) - (a\beta + b\beta) \Rightarrow \delta \mid \alpha b - \beta a$$

Logo, como $\delta \mid n$ e $\delta \mid \alpha b - \beta a$, temos $\text{mdc}(\alpha b - \beta a, n) \neq 1$. □

Lema 7. *Sejam n, α, β, a e b inteiros tais que $\text{mdc}(\alpha b - \beta a, n) = 1$. Seja $\text{mdc}(\alpha + \beta, n) = \delta_k^+$. Existe $0 \leq k_0 \leq \delta_k^+ - 1$ tal que para qualquer uma das n soluções (w, k), com $0 \leq w, k \leq n-1$ da equação $(\alpha+\beta)w+(a+b)k \equiv 1-p-q \pmod{n}$, temos $k = k_0 + l \cdot \delta_k^+$, sendo $0 \leq l \leq \dfrac{n}{\delta_k^+} - 1$. Além disso, para cada $l \in \left\{0, 1, \ldots, \dfrac{n}{\delta_k^+} - 1\right\}$, há exatamente δ_k^+*

repetições de $k = k_0 + l \cdot \delta_k^+$ *dentre essas n soluções* (w, k) *de* $(\alpha+\beta)w+(a+b)k \equiv 1-p-q \pmod{n}$.

Demonstração. Análoga à do Lema 5 □

Corolário 9. *Se na equação* $(\alpha+\beta)w+(a+b)k \equiv 1-p-q \pmod{n}$, $\text{mdc}(\alpha+\beta, n) = 1$, *então os k's formam um sistema completo de resíduos.*

Um resultado análogo é válido se $\text{mdc}(a+b, n) = \delta_w^+$.

Lema 8. *Sejam* n, α, β, a *e* b *inteiros tais que* $\text{mdc}(\alpha b - \beta a, n) = 1$. *Seja* $\text{mdc}(a+b, n) = \delta_w^+$. *Existe* $0 \leq w_0 \leq \delta_w^+ - 1$ *tal que para qualquer uma das n soluções* (w, k), *com* $0 \leq w, k \leq n-1$ *da equação* $(\alpha+\beta)w+(a+b)k \equiv 1-p-q \pmod{n}$, *temos* $w = w_0 + t \cdot \delta_w^+$, *sendo* $0 \leq t \leq \dfrac{n}{\delta_w^+} - 1$. *Além disso, para cada* $t \in \left\{0, 1, \ldots, \dfrac{n}{\delta_w^+} - 1\right\}$, *há exatamente* δ_w^+ *repetições de* $w = w_0 + t \cdot \delta_w^+$ *dentre essas n soluções* (w, k) *de* $(\alpha+\beta)w+(a+b)k \equiv 1-p-q \pmod{n}$.

Corolário 10. *Se na equação* $(\alpha+\beta)w+(a+b)k \equiv 1-p-q \pmod{n}$, $\text{mdc}(a+b, n) = 1$, *então os w's formam um sistema completo de resíduos.*

6.2.1 Calculando a soma da diagonal

Sejam $\text{mdc}(a+b, n) = \delta_w^+$ e $\text{mdc}(\alpha+\beta, n) = \delta_k^+$.

Argumentando como no caso da diagonal principal negativa, o Lema 8 nos mostra que os k's poderão assumir $\dfrac{n}{\delta_k^+}$ valores no conjunto

$\{0, 1, 2, \ldots, n-1\}$.

Esses valores dependem de $1-p-q$ e a soma dos k's, será dada por

$$\sum k = \frac{n}{2}\left(n - \delta_k^+\right) + r_k n, \tag{59}$$

com $0 \leq r_k \leq \delta_k^+ - 1$.
Veremos que p e q devem ser escolhidos de modo que os valores de k na diagonal principal positiva sejam os do conjunto

$$R_k = \left\{r_k, r_k + \delta_k^+, r_k + 2\delta_k^+, \ldots, r_k + \left(\frac{n}{\delta_k^+} - 1\right)\delta_k^+\right\} \tag{60}$$

onde

$$r_k = \frac{\delta_k^+ - 1}{2}. \tag{61}$$

Analogamente, é possível mostrar que se x_i, $i = 1, \ldots, n$ são os elementos da diagonal principal positiva, os w's associados a esses elementos poderão assumir $\frac{n}{\delta_w^+}$ valores no conjunto

$\{0, 1, 2, \ldots, n-1\}$.

Esses valores dependem de $1 - p - q$ e sua soma é dada por

$$\sum w = \frac{n}{2}\left(n - \delta_w^+\right) + r_w n \tag{62}$$

onde r_w é um inteiro tal que $0 \leq r_w \leq \delta_w^+ - 1$.
Veremos também que p e q devem ser escolhidos de modo que os valores de w na diagonal principal positiva sejam os do conjunto

$$R_w = \left\{ r_w, r_w + \delta_w^+, r_w + 2\delta_w^+, \ldots, r_w + \left(\frac{n}{\delta_w^+} - 1\right)\delta_w^+ \right\}$$

onde

$$r_w = \frac{\delta_w^+ - 1}{2}.$$

Por (59) e (62), podemos deduzir que a soma dos elementos x_i da diagonal principal positiva é dada por

$$\begin{aligned}\sum_i x_i &= \sum_i 1 + \sum w + n\sum k \\ &= n + \frac{n}{2}\left(n - \delta_w^+\right) + r_w n + \frac{n^2}{2}\left(n - \delta_k^+\right) + r_k n^2 \\ &= n + r_w n + \frac{n}{2}\left(n - \delta_w^+\right) + r_k n^2 + \frac{n^2}{2}\left(n - \delta_k^+\right)\end{aligned}$$

6.2.2 Condição necessária e suficiente

Teorema 18. *Sejam $x_i = 1 + w_i + nk_i$, $0 \leq w_i, k_i \leq n-1$, $i = 1, \ldots, n$, os elementos da diagonal principal positiva. Sejam $\mathrm{mdc}(a+b, n) = \delta_w^+$ e $\mathrm{mdc}(\alpha+\beta, n) = \delta_k^+$. Para que a diagonal principal positiva seja mágica é necessário e suficiente que p e q sejam escolhidos de modo que*

$$r_k^+ = \frac{\delta_k^+ - 1}{2} \quad e \quad r_w^+ = \frac{\delta_w^+ - 1}{2}$$

sejam respectivamente o menor k e o menor w dentre todas os elementos x_i da diagonal.

Demonstração. Análoga à prova do Teorema 17. □

Corolário 11. *Sejam* n, α, β, a *e* b *inteiros tais que* $\text{mdc}(\alpha b+\beta a, n) = 1$. *Sejam* $\text{mdc}(\alpha+\beta, n) = \delta_k^+$ *e* $\text{mdc}(a+b, n) = \delta_w^+$. *Se* p *e* q *são tais que*

$$1 - q - p \equiv (\alpha+\beta)\left(\frac{\delta_w^+ - 1}{2}\right) + (a+b)\left(\frac{\delta_k^+ - 1}{2}\right) \pmod{n}$$

então a soma dos elementos da diagonal principal positiva do quadrado gerado pelo método do passo uniforme é igual a $\frac{n(n^2+1)}{2}$.

6.2.3 Onde começar para que a DPP seja mágica?

Vimos nas seções anteriores que os elementos da diagonal principal positiva (DPP) foram caracterizados como soluções de (58). Além disso, vimos que é possível associar à DPP únicos conjuntos R_w e R_k tais que se $x = 1 + w + kn$ é um elemento da DPP, temos $w \in R_w$ e $k \in R_k$. Consequentemente, se há na DPP algum x da forma

$$x = 1 + \frac{\delta_w^+ - 1}{2} + l \cdot \delta_w^+ + \left(\frac{\delta_k^+ - 1}{2} + t \cdot \delta_k^+\right) \cdot n$$

com $0 \leq l \leq \frac{n}{\delta_w^+} - 1, 0 \leq t \leq \frac{n}{\delta_k^+} - 1$, então

$$R_w = \left\{ r_w, r_w + \delta_w^+, r_w + 2\delta_w^+, \ldots, r_w + \left(\frac{n}{\delta_w^+} - 1\right)\delta_w^+ \right\}, \quad \text{onde } r_w = \frac{\delta_w^+ - 1}{2}$$

e

$$R_k = \left\{ r_k, r_k + \delta_k^+, r_k + 2\delta_k^+, \ldots, r_k + \left(\frac{n}{\delta_k^+} - 1\right)\delta_k^+ \right\}, \quad \text{onde } r_k = \frac{\delta_k^+ - 1}{2}.$$

Portanto, pelo Teorema 18, a DPP é mágica.

Reciprocamente, se a DPP é mágica, pelo Teorema 18, ela contém elementos x da forma

$$x = 1 + \frac{\delta_w^+ - 1}{2} + l \cdot \delta_w^+ + \left(\frac{\delta_k^+ - 1}{2} + t \cdot \delta_k^+\right) \cdot n$$

com $0 \leq l \leq \frac{n}{\delta_w^+} - 1, 0 \leq t \leq \frac{n}{\delta_k^+} - 1$.

Essas considerações nos permitem estabelecer a seguinte proposição.

Proposição 7. *Sejam* α, β, a, b *e* n *números inteiros tais que* α, β, a, b *e* $\alpha b - \beta a$ *são primos com* n. *A DPP do quadrado de ordem* n *construído pelo método do passo uniforme*

é mágica se e somente se as coordenadas (p, q) *da célula inicial satisfazem*

$$(\alpha+\beta)\left(\frac{\delta_w^+-1}{2}+l\cdot\delta_w^+\right)+(a+b)\left(\frac{\delta_k^+-1}{2}+t\cdot\delta_k^+\right)\equiv 1-q-p \pmod{n} \tag{63}$$

para algum $0\leq l\leq \frac{n}{\delta_w^+}-1, 0\leq t\leq \frac{n}{\delta_k^+}-1$ *e onde* $\delta_w^+=\mathrm{mdc}(a+b,n)$ *e* $\delta_k^+=\mathrm{mdc}(\alpha+\beta,n)$.

Note que se $\alpha+\beta$ e $a+b$ forem primos com n, a diagonal principal positiva sempre será mágica. De fato, pelos Corolários 9 e 10, a soma dos elementos x_i da diagonal principal positiva, será mágica:

$$x_1+x_2+\cdots+x_n=\sum_{i=1}^{n}1+\sum_{i=1}^{n}w_i+n\sum_{i=1}^{n}k_i=\left(\frac{1+n^2}{2}\right)n$$

Portanto, se os coeficientes $\alpha+\beta$ e $a+b$ da equação linear (58) com duas variáveis w e k, módulo n, que determina a diagonal principal positiva forem primos[14] com n, ela será mágica, independentemente dos valores iniciais (p, q). Esse resultado também pode ser obtido a partir da Proposição 7. Se os coeficientes $\alpha+\beta$ e $a+b$ forem primos com n, (63) é dada por

$$(\alpha+\beta)l+(a+b)t\equiv 1-q-p \pmod{n}$$

com $0\leq l,t\leq n-1$. É fácil ver que podemos escolher (l, t) de modo que $(\alpha+\beta)l+(a+b)t$ gere um conjunto completo de resíduos. Isso resulta em p e q quaisquer.

Exemplo 11. *Tomando o mesmo quadrado do exemplo 8, Página 70,* $n=7$, $\alpha=4$, $\beta=2$, $a=3$ *e* $b=6$, *verificamos que será mágico também nas diagonais positivas uma vez que* $\alpha+\beta=6$ *e* $a+b=9$ *são ambos primos com* 7.

A condição de primalidade de $\alpha+\beta$ e $a+b$ com n garante que todas as diagonais positivas sejam mágicas.

Segue da Proposição 7 que todos os possíveis valores de $1-q-p$ que determinam uma DPP mágica pertencem ao conjunto

$$O=\left\{m\in\mathbb{Z},\ m\equiv m_{tl} \pmod{n}, 0\leq l\leq\frac{n}{\delta_w^+}-1,\ 0\leq t\leq\frac{n}{\delta_k^+}-1\right\}$$

[14] Na verdade, com tal condição (argumentando como na prova do Teorema 13, podemos deduzir que o quadrado é mágico em todas as diagonais positivas. Isto é, nas diagonais em que

$A+B\equiv j \pmod{n},\ j=0,1,2,\ldots,n-1$

onde

$$m_{tl} = (\alpha + \beta)\left(\frac{\delta_w^+ - 1}{2} + l \cdot \delta_w^+\right) + (a + b)\left(\frac{\delta_k^+ - 1}{2} + t \cdot \delta_k^+\right). \tag{64}$$

Vamos investigar agora estratégias para determinar os elementos do conjunto O. Fixados t e l, pela Proposição 7, o elemento m_{tl} pode ser associado a uma DPP mágica. Consequentemente, pelo Teorema 18, deve haver um elemento x da forma

$$x = 1 + \frac{\delta_w^+ - 1}{2} + \left(\frac{\delta_k^+ - 1}{2} + t \cdot \delta_k^+\right) \cdot n.$$

Além disso, temos

$$(\alpha + \beta) \cdot \frac{\delta_w^+ - 1}{2} + (a + b)\left(\frac{\delta_k - 1}{2} + t \cdot \delta_k^+\right) \equiv m_{tl} \equiv 1 - q - p \pmod{n}.$$

Consequentemente, temos

$$O = \left\{m \in \mathbb{Z},\ m \equiv m_{t0}, \quad 0 \leq t \leq \frac{n}{\delta_k^+} - 1\right\}, \tag{65}$$

onde m_{tl} é dado por (64). Analogamente, temos

$$O = \left\{m \in \mathbb{Z},\ m \equiv m_{0l}, \quad 0 \leq l \leq \frac{n}{\delta_w^+} - 1\right\}, \tag{66}$$

onde m_{tl} é dado por (64).

Vamos ilustrar essa caracterização do conjunto O em alguns casos especiais.

Suponha $\text{mdc}(\alpha + \beta, n) = \delta \neq 1$ e $\text{mdc}(a + b, n) = 1$. Pelo Corolário 7, os w's associados às soluções de (58) formam um sistema completo de resíduos cuja soma é dada por

$$\sum_{i=1}^{n} w = \left(\frac{n-1}{2}\right) n.$$

Para obter uma DPP mágica, pelo Teorema 17, sabemos que p e q devem ser escolhidos de modo que os valores de k na diagonal principal positiva sejam os do conjunto

$$R = \left\{r_0, r_0 + \delta, r_0 + 2\delta, \ldots, r_0 + \left(\frac{n}{\delta} - 1\right)\delta\right\} \tag{67}$$

onde

$$r_0 = \frac{\delta - 1}{2}. \tag{68}$$

Como os w's formam um sistema completo de resíduos, por (65), para cada $k \in R$ obtemos pela congruência

$$(\alpha+\beta)\cdot 0 + (a+b)\cdot k \equiv 1-q-p \pmod{n}$$

uma relação entre p e q para obter todas as possíveis diagonais principais positivas mágicas.

Suponha agora $\text{mdc}(\alpha+\beta, n) = 1$ e $\text{mdc}(a+b, n) = \delta \neq 1$. Esse caso é análogo ao caso anterior, apenas trocando k por w. Então, fazendo $k = 0$, para cada $w \in R$ (ver (67) e (68)), por (66), obtemos pela congruência

$$(\alpha+\beta)\cdot w + (a+b)\cdot 0 \equiv 1-q-p \pmod{n}$$

uma relação entre p e q para obter todas as possíveis diagonais principais positivas mágicas.

Exemplo 12. Sejam $n = 9$, $\alpha = 4$, $\beta = 1$, $a = 5$ e $b = 1$, verificamos que será mágico na diagonal principal positiva para determinados valores de p e q. Que valores são esses? Temos

$$\alpha+\beta = 5 \qquad \text{e} \qquad a+b = 6.$$

Substituindo em (58), temos:

$$5w + 6k \equiv 1-q-p \pmod{9}.$$

Além disso, $\text{mdc}(5, 9) = 1$, logo $k \in \{0, 1, 2, \ldots, 7, 8\}$. Por outro lado, $\text{mdc}(6, 9) = 3 = \delta$, logo por (68), $r_0 = \dfrac{3-1}{2} = 1$, e por (67), $w \in \{1, 4, 7\}$.
Os valores de $1-q-p$ são calculados fazendo $k = 0$ e w assumindo os valores do conjunto $R = \{1, 4, 7\}$, logo:

$$w = 1, \quad q+p \equiv -4 \equiv 5 \pmod{9},$$
$$w = 4, \quad q+p \equiv -1 \equiv 8 \pmod{9},$$
$$w = 7, \quad q+p \equiv -7 \equiv 2 \pmod{9}.$$

Logo, a diagonal principal positiva será mágica se $q+p \equiv 2$, $q+p \equiv 5$ ou $q+p \equiv 8$.

Na Figura 26a o quadrado foi preenchido com as coordenadas iniciais $p = 2$ e $q = 4$. A DPP não será mágica, uma vez que $q+p \equiv 6$.

$$63+21+69+36+75+42+9+48+15 = 378 \neq 369.$$

Figura 26 - $n = 9$, $\alpha = 4$, $\beta = 1$, $a = 5$, $b = 1$.

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

(a)

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

(b)

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

(c)

Legenda: (a) DPP não mágica, $p = 2$ e $q = 4$.
(b) DPP mágica, $p = 1$ e $q = 1$.
(c) DPP mágica, $p = 5$ e $q = 3$.

Fonte: O autor, 2014.

Na Figura 26b, $p = 1$ e $q = 1$, atende a condição $q + p = 2$, uma DPP mágica será obtida

$41 + 8 + 47 + 14 + 62 + 20 + 68 + 35 + 74 = 369$.

Na Figura 26c, $p = 5$ e $q = 3$, atende a condição $p + q = 8$, uma DPP mágica é obtida.fig:

$80 + 38 + 5 + 53 + 11 + 59 + 26 + 65 + 32 = 369$.

Prosseguindo, vamos tentar investigar quantos valores incongruentes de $q+p$ geram DPP mágicas. Seja $q_0 + p_0$ o gerador de DPP mágicas associado a m_{00}. Isto é

$$q_0 + p_0 \equiv 1 - (\alpha + \beta) \cdot \frac{\delta_w^+ - 1}{2} - (a + b) \cdot \frac{\delta_k^+ - 1}{2} \pmod{n} \tag{69}$$

Note que para qualquer outro valor $q + p$ gerador de DPP mágicas, teremos

$$(q + p) - (q_0 + p_0) \equiv -(\alpha + \beta) \cdot l \cdot \delta_w^+ - (a + b) \cdot t \cdot \delta_k^+ \pmod{n}$$

para algum $0 \leq l \leq \frac{n}{\delta_w^+} - 1$ e $0 \leq t \leq \frac{n}{\delta_k^+} - 1$. Isto nos diz que podemos obter todos os demais geradores de DPN mágicas a partir de $q_0 - p_0$ através de acréscimos da forma $-(\alpha + \beta) \cdot l \cdot \delta_w^+ - (a + b) \cdot t \cdot \delta_k^+$. Para identificar todos os geradores incongruentes, basta identificar quantos valores incongruentes módulo n podem ser gerados por

$$-(\alpha + \beta) \cdot l \cdot \delta_w^+ - (a + b) \cdot t \cdot \delta_k^+$$

para $0 \leq l \leq \frac{n}{\delta_w^+} - 1$ e $0 \leq t \leq \frac{n}{\delta_k^+} - 1$.

Pela Observação 10 e pela Proposição 1, temos

$$\text{mdc}(\delta_k^+, \delta_w^+) = \text{mdc}(\text{mdc}(\alpha + \beta, n), \text{mdc}(a + b, n)) = \text{mdc}(\alpha + \beta, a + b, n) = 1.$$

Pelo Teorema 2, temos $\delta_k^+ \cdot \delta_w^+ \mid n$. Seja r_{tl} o resíduo módulo n de $(\alpha+\beta)\cdot l\cdot\delta_w^+ + (a+b)\cdot t\cdot\delta_k^+$. Temos

$$-(\alpha + \beta) \cdot l \cdot \delta_w^+ - (a + b) \cdot t \cdot \delta_k^+ \equiv r_{tl} \pmod{n}. \tag{70}$$

Sejam $M_{\alpha\beta}$ e M_{ab} naturais tais que

$$\alpha + \beta = M_{\alpha\beta} \cdot \delta_k^+ \quad \text{e} \quad a + b = M_{ab} \cdot \delta_w^+.$$

Podemos reescrever (70) da seguinte maneira

$$-M_{\alpha\beta} \cdot \delta_k^+ \cdot \delta_w^+ \cdot l - M_{ab} \cdot \delta_w^+ \cdot \delta_k^+ \cdot t \equiv r_{tl} \pmod{n}. \tag{71}$$

Como $\delta_k^+ \cdot \delta_w^+ \mid n$, temos

$$\text{mdc}(\delta_k^+ \cdot \delta_w^+, n) = \delta_k^+ \cdot \delta_w^+.$$

Pelo Teorema 5, $\delta_k^+ \cdot \delta_w^+ \mid r_{tl}$. Como $0 \leq r_{tl} \leq n - 1$, existe um inteiro r'_{tl} tal que

$$r_{tl} = r'_{tl} \cdot \delta_k^+ \cdot \delta_w^+, \quad 0 \leq r'_{tl} \leq \frac{n}{\delta_k^+ \delta_w^+} - 1$$

Pela Proposição 5, (71) é equivalente a

$$-M_{\alpha\beta} \cdot l - M_{ab} \cdot t \equiv r'_{tl} \quad \left(\mathrm{mod}\, \frac{n}{\delta_k^+ \delta_w^+}\right) \tag{72}$$

Segue de $\mathrm{mdc}(\alpha+\beta, a+b, n) = 1$ que $\mathrm{mdc}\left(M_{\alpha\beta}, M_{ab}, \frac{n}{\delta_k^+ \cdot \delta_w^+}\right) = 1$. Pelo Teorema 5, para todo $0 \leq r'_{tl} \leq \frac{n}{\delta_k^+ \delta_w^+} - 1$, (72) admite soluções. Portanto, esse é o total de geradores $q+p$ incongruentes módulo n de DPP mágicas. E para determiná-los, basta resolver

$$(q+p) - (q_0 + p_0) \equiv -r \cdot \delta_k^+ \cdot \delta_w^+ \pmod{n} \tag{73}$$

para cada $r \in \left\{0, 1, \ldots, \frac{n}{\delta_k^+ \delta_w^+} - 1\right\}$. Essa congruência nos diz que podemos obter todos os possíveis geradores de DPP mágicas adicionando (módulo n) ao gerador $q_0 + p_0$ a quantidade $-(\delta_k^+ \cdot \delta_w^+)$ por $\frac{n}{\delta_k^+ \delta_w^+} - 1$ vezes.

Exemplo 13. Sejam $n = 75$, $\alpha = 2$, $\beta = 7$, $a = 8$ e $b = 2$.

$\mathrm{mdc}(\alpha b - \beta a, n) = \mathrm{mdc}(-52, 75) = 1$
$\mathrm{mdc}(\alpha, n) = \mathrm{mdc}(\beta, n) = \mathrm{mdc}(a, n) = \mathrm{mdc}(b, n) = 1$
$\delta_k^+ = \mathrm{mdc}(\alpha+\beta, n) = \mathrm{mdc}(9, 75) = 3$
$\delta_w^+ = \mathrm{mdc}(a+b, n) = \mathrm{mdc}(20, 75) = 5$

Temos

$$R_w = \{2, 7, 12, 17, \ldots, 72\}, \qquad r_w = \frac{\delta_w^+ - 1}{2} = 2$$

e

$$R_k = \{1, 4, 7, 10, \ldots, 73\}, \qquad r_k = \frac{\delta_k^+ - 1}{2} = 1$$

Além disso, vimos que temos $\frac{n}{\delta_k^+ \delta_w^+} = 5$ geradores de DPP mágicas incongruentes que podem ser obtidos a partir do gerador

$$q_0 + p_0 \equiv 1 - (\alpha+\beta) \cdot \frac{\delta_w^+ - 1}{2} - (a+b) \cdot \frac{\delta_k^+ - 1}{2} \equiv -27 \pmod{75}$$

por 5 adições módulo 75 de $\delta_k^+ \cdot \delta_w^+ = 15$. Temos

$q + p \in \{48, 63, 3, 18, 33\}$.

Esse resultado é o mesmo obtido pelo método de tomarmos, por exemplo, o primeiro

elemento de R_w e considerar

$$q + p \equiv -17 - 10 \cdot r \pmod{75}, \quad r \in R_k$$

6.3 Onde começar para que a DPP e a DPN sejam ambas mágicas?

Para determinar os geradores $q-p$ incongruentes módulo n de DPN mágicas, basta resolver (57)

$$q - p - (q_0 - p_0) \equiv r^- \cdot \delta_k^- \cdot \delta_w^- \pmod{n} \tag{74}$$

para cada $r^- \in \left\{0, 1, \ldots, \frac{n}{\delta_k^- \delta_w^-} - 1\right\}$. Essa congruência nos diz que podemos obter todos os possíveis geradores de DPN mágicas adicionando (módulo n) ao gerador $q_0 - p_0$ a quantidade $\delta_k^- \cdot \delta_w^-$ por $\frac{n}{\delta_k^- \delta_w^-} - 1$ vezes.

Para determinar os geradores $q+p$ incongruentes módulo n de DPP mágicas, basta resolver (73)

$$(q + p) - (q_0 + p_0) \equiv -r^+ \cdot \delta_k^+ \cdot \delta_w^+ \pmod{n} \tag{75}$$

para cada $r^+ \in \left\{0, 1, \ldots, \frac{n}{\delta_k^+ \delta_w^+} - 1\right\}$. Essa congruência nos diz que podemos obter todos os possíveis geradores de DPP mágicas adicionando (módulo n) ao gerador $q_0 + p_0$ a quantidade $-(\delta_k^+ \cdot \delta_w^+)$ por $\frac{n}{\delta_k^+ \delta_w^+} - 1$ vezes.

Admitindo que (p_0, q_0) satisfaz a (53) e (69) e somando (74) com (75) temos:

$$2q \equiv 2q_0 + r^- \cdot \delta_k^- \cdot \delta_w^- - r^+ \cdot \delta_k^+ \cdot \delta_w^+ \pmod{n}$$

Seja $Q^- = \delta_k^- \cdot \delta_w^-$ se $2 \mid \delta_k^- \cdot \delta_w^-$ ou $Q^- = (\delta_k^- \cdot \delta_w^- - n)$ se $2 \nmid \delta_k^- \cdot \delta_w^-$.
Seja $Q^+ = \delta_k^+ \cdot \delta_w^+$ se $2 \mid \delta_k^+ \cdot \delta_w^+$ ou $Q^+ = (\delta_k^+ \cdot \delta_w^+ - n)$ se $2 \nmid \delta_k^- \cdot \delta_w^+$.
Uma vez que n é ímpar Q^- e Q^+ serão pares e podemos determinar o valor de q.

$$q \equiv q_0 + r^- \cdot \frac{Q^-}{2} - r^+ \cdot \frac{Q^+}{2} \pmod{n} \tag{76}$$

Subtraindo (74) de (75) temos:

$$2p \equiv 2p_0 - r^- \cdot \delta_k^- \cdot \delta_w^- - r^+ \cdot \delta_k^+ \cdot \delta_w^+ \pmod{n}$$

Uma vez que n é ímpar Q^- e Q^+ serão pares e podemos determinar o valor de p.

$$p \equiv p_0 - r^- \cdot \frac{Q^-}{2} - r^+ \cdot \frac{Q^+}{2} \pmod{n} \tag{77}$$

A congruência (77) para a coordenada inicial p é análoga a congruência (3) para a coordenada A. Observe que r^- e r^+ são contadores e $\frac{Q^-}{2}$ ou $\frac{Q^+}{2}$ podem ser escolhidos como "passo"ou "quebra de passo". Portanto, pode-se obter todas as coordenadas iniciais p a partir de p_0, acrescentando "passos", por exemplo, $\frac{Q^-}{2}$, por $\frac{n}{\delta_k^- \delta_w^-} - 1$ vezes, ao final do qual, soma-se a "quebra de passo", $\frac{Q^+}{2}$. Um novo ciclo é então iniciado, acrescentando-se $\frac{n}{\delta_k^- \delta_w^-} - 1$ passos $\frac{Q^-}{2}$, completando outro ciclo, então nova quebra de passo $\frac{Q^+}{2}$ é introduzida. E assim por diante até se completar $\frac{n}{\delta_k^+ \delta_w^+} - 1$ quebras de passos.

Da mesma maneira, pode-se obter todas as coordenadas iniciais q a partir de q_0, pois a congruência (76) para a coordenada inicial q é análoga a equação (4) para a coordenada B.

Exemplo 14. Sejam $n = 55$, $\alpha = 7$, $\beta = 4$, $a = 6$ e $b = 1$.

$\text{mdc}(\alpha b - \beta a, n) = \text{mdc}(-17, 55) = 1$

$\text{mdc}(\alpha, n) = \text{mdc}(\beta, n) = \text{mdc}(a, n) = \text{mdc}(b, n) = 1$

$\delta_k^+ = \text{mdc}(\alpha + \beta, n) = \text{mdc}(11, 55) = 11$

$\delta_w^+ = \text{mdc}(a + b, n) = \text{mdc}(7, 55) = 1$

$\delta_k^- = \text{mdc}(\alpha - \beta, n) = \text{mdc}(3, 55) = 1$

$\delta_w^- = \text{mdc}(a - b, n) = \text{mdc}(5, 55) = 5$

$$R_w^+ = \{0, 1, 2, 3, 4, \ldots, 54\}, \qquad r_w^+ = \frac{\delta_w^+ - 1}{2} = 0$$

$$R_k^+ = \{5, 16, 27, 38, 49\}, \qquad r_k^+ = \frac{\delta_k^+ - 1}{2} = 5$$

$$R_w^- = \{2, 7, 12, 17, \ldots, 52\}, \qquad r_w^- = \frac{\delta_w^- - 1}{2} = 2$$

$$R_k^- = \{0, 1, 2, 3, 4, \ldots, 54\}, \qquad r_k^- = \frac{\delta_k^- - 1}{2} = 0$$

Além disso,

$$q_0 + p_0 \equiv 1 - (\alpha + \beta) \cdot r_w^+ - (a + b) \cdot r_k^+ \pmod{n}$$

$$q_0 + p_0 \equiv 1 - 11 \cdot 0 - 7 \cdot 5 \equiv -34 \equiv 21 \pmod{55}$$

Tabela 5 - Coordenadas iniciais para DPP e DPN mágicas

	r^+	(p, q)
$r^- = 0$	0	$(35, 41)$
	1	$(35 + 22 \equiv 2, 41 + 22 \equiv 8)$
	2	$(2 + 22 \equiv 24, 8 + 22 \equiv 30)$
	3	$(24 + 22 \equiv 46, 30 + 22 \equiv 52)$
	4	$(46 + 22 \equiv 13, 52 + 22 \equiv 19)$

Fonte: O autor, 2014.

$$q_0 - p_0 \equiv (\alpha - \beta) \cdot r_w^- + (a - b) \cdot r_k^- \pmod{n}$$
$$q_0 - p_0 \equiv 3 \cdot 2 + 5 \cdot 0 \equiv 6 \pmod{55}$$

Segue que
$p_0 \equiv -20 \equiv 35 \pmod{55}$
$q_0 \equiv -14 \equiv 41 \pmod{55}$

Temos $\delta_w^+ \cdot \delta_k^+ = 11$ e $\delta_w^- \cdot \delta_k^- = 5$

Logo $\dfrac{Q^+}{2} \equiv \dfrac{11 - 55}{2} \equiv -22$ e $\dfrac{Q^-}{2} \equiv \dfrac{5 - 55}{2} \equiv -25$

$$p \equiv p_0 - r^- \cdot \frac{Q^-}{2} - r^+ \cdot \frac{Q^+}{2} \cdot \pmod{n}$$
$$p \equiv 35 + 25 \cdot r^- + 22 \cdot r^+ \pmod{55}$$
$$q \equiv q_0 + r^- \cdot \frac{Q^-}{2} - r^+ \cdot \frac{Q^+}{2} \pmod{n}$$
$$q \equiv 41 - 25 \cdot r^- + 22 \cdot r^+ \pmod{n}$$

Sendo
$r^- \in \left\{0, 1, \ldots, \frac{n}{\delta_k^- \delta_w^-} - 1\right\} = \{0, 1, \ldots, 10\}$
$r^+ \in \left\{0, 1, \ldots, \frac{n}{\delta_k^+ \delta_w^+} - 1\right\} = \{0, 1, 2, 3, 4\}$

Ao final do 1º ciclo de 5 números, Tabela 5, o próximo valor de (p, q) exigirá uma quebra de passo no procedimento. De fato, partindo das coordenadas iniciais (p_0, q_0) ao serem somados 4 passos horizontais $\dfrac{Q^-}{2}$ voltaremos à coordenada inicial (p_0, q_0). Então, adicionamos $\dfrac{Q^+}{2}$ à coordenada p e $-\dfrac{Q^+}{2}$ à coordenada q, obtendo $(13+25 \equiv 38, 19-25 \equiv -6 \equiv 49)$. Em seguida, voltamos ao procedimento dos passo até completar outro ciclo de

Tabela 6 - Coordenadas iniciais para DPP e DPN mágicas

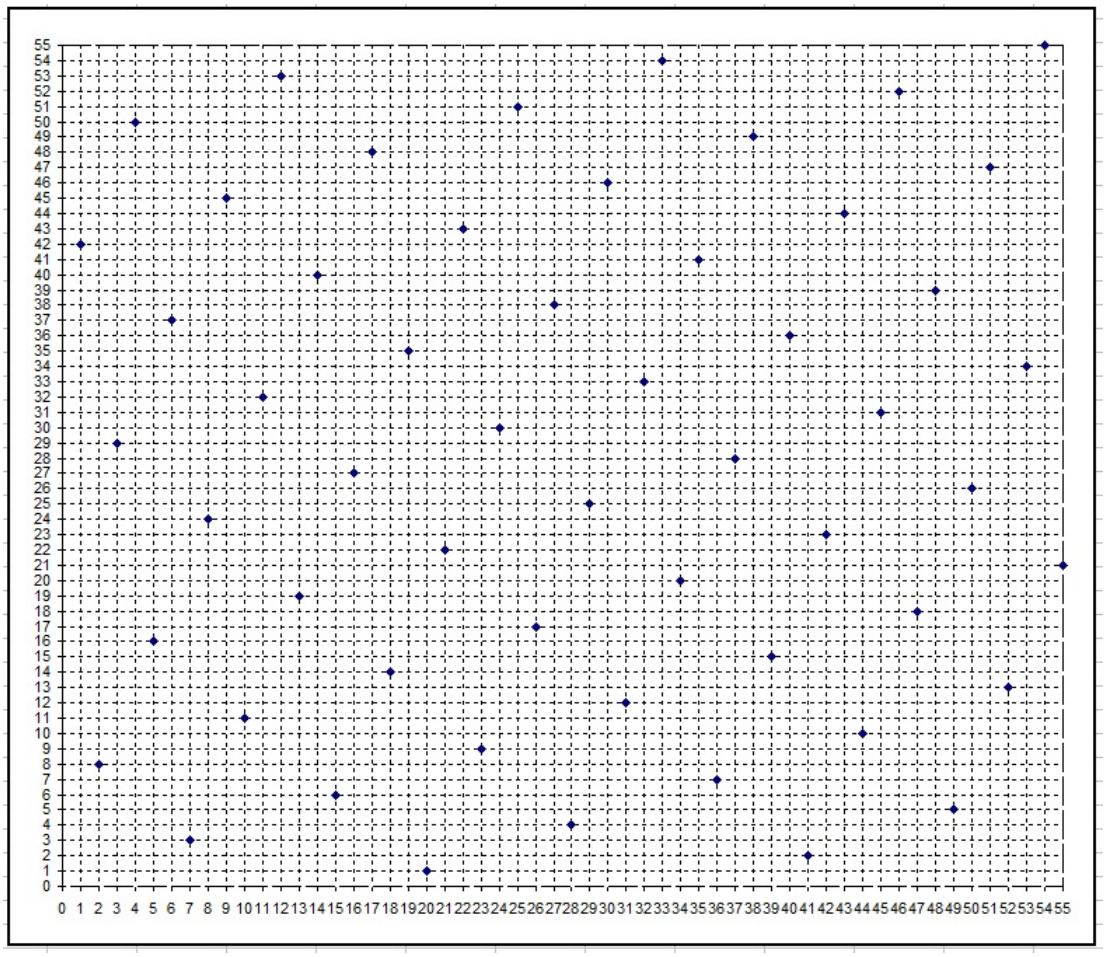
	r^+	(p, q)
$r^- = 1$	0	$(38, 49)$
	1	$(38 + 22 \equiv 5, 49 + 22 \equiv 16)$
	2	$(5 + 22 \equiv 27, 16 + 22 \equiv 38)$
	3	$(27 + 22 \equiv 49, 38 + 22 \equiv 5)$
	4	$(49 + 22 \equiv 16, 5 + 22 \equiv 27)$

Fonte: O autor, 2014.

5 números, Tabela 6. E assim por diante.

Com este procedimento são obtidas $\frac{n}{\delta_w^+ \cdot \delta_k^+} \cdot \frac{n}{\delta_w^- \cdot \delta_k^-} = 55$ coordenadas. A regularidade das 55 coordenadas iniciais (p, q) que garantem DPP e DPN mágicas é exibida na Figura 27).

Figura 27 - Coordenadas iniciais para DPP e DPN mágicas (parâmetros: $n = 55$, $\alpha = 7$, $\beta = 4$, $a = 6$, $b = 1$).



Fonte: O autor, 2014.

Exemplo 15. Considere $n = 105$, $\alpha = 11, \beta = 2, a = 31$ e $b = 11$.

$\text{mdc}(\alpha b - \beta a, n) = \text{mdc}(59, 105) = 1$
$\text{mdc}(\alpha, n) = \text{mdc}(\beta, n) = \text{mdc}(a, n) = \text{mdc}(b, n) = 1$
$\delta_w^+ = \text{mdc}(a + b, n) = \text{mdc}(42, 105) = 3$
$\delta_k^+ = \text{mdc}(\alpha + \beta, n) = \text{mdc}(13, 105) = 1$
$\delta_w^- = \text{mdc}(a - b, n) = \text{mdc}(20, 105) = 5$
$\delta_k^- = \text{mdc}(\alpha - \beta, n) = \text{mdc}(9, 105) = 3$

$R_w^+ = \{1, 4, 7, \ldots, 103\}, \qquad r_w^+ = \dfrac{\delta_w^+ - 1}{2} = 1$
$R_k^+ = \{0, 1, 2, 3, \ldots, 104\}, \qquad r_k^+ = \dfrac{\delta_k^+ - 1}{2} = 0$
$R_w^- = \{2, 7, 12, \ldots, 102\}, \qquad r_w^- = \dfrac{\delta_w^- - 1}{2} = 2$
$R_k^- = \{1, 4, 7, \ldots, 103\}, \qquad r_k^- = \dfrac{\delta_k^- - 1}{2} = 1$

Além disso,

$q_0 + p_0 \equiv 1 - (\alpha + \beta) \cdot r_w^+ - (a + b) \cdot r_k^+ \pmod{n}$
$q_0 + p_0 \equiv 1 - 13 \cdot 1 - 42 \cdot 0 \equiv -12 \pmod{105}$

$q_0 - p_0 \equiv (\alpha - \beta) \cdot r_w^- + (a - b) \cdot r_k^- \pmod{n}$
$q_0 - p_0 \equiv 9 \cdot 2 + 20 \cdot 1 \equiv 38 \pmod{105}$

Segue que

$p_0 \equiv -25 \equiv 80 \pmod{105}$
$q_0 \equiv 13 \pmod{105}$

Temos $\delta_w^- \cdot \delta_k^- = 15$ e $\delta_w^+ \cdot \delta_k^+ = 3$

Logo $\dfrac{Q^+}{2} \equiv \dfrac{3 - 105}{2} \equiv -51$ e $\dfrac{Q^-}{2} \equiv \dfrac{15 - 105}{2} \equiv -45$

$$p \equiv p_0 - r^- \cdot \frac{Q^-}{2} - r^+ \cdot \frac{Q^+}{2} \pmod{n}$$

$$p \equiv 80 + 45 \cdot r^- + 51 \cdot r^+ \pmod{105}$$

Tabela 7 - Coordenadas iniciais para DPP e DPN mágicas

	r^-	(p, q)
$r^+ = 0$	0	$(80, 13)$
	1	$(80 + 45 \equiv 20, 13 - 45 \equiv 73)$
	2	$(20 + 45 \equiv 65, 73 - 45 \equiv 28)$
	3	$(65 + 45 \equiv 5, 28 - 45 \equiv 88)$
	4	$(5 + 45 \equiv 50, 88 - 45 \equiv 43)$
	5	$(50 + 45 \equiv 95, 43 - 45 \equiv 103)$
	6	$(95 + 45 \equiv 35, 103 - 45 \equiv 58)$

Fonte: O autor, 2014.

$$q \equiv q_0 + r^- \cdot \frac{Q^-}{2} - r^+ \cdot \frac{Q^+}{2} \pmod{n}$$
$$q \equiv 13 - 45 \cdot r^- + 51 \cdot r^+ \pmod{105}$$

Sendo
$r^- \in \left\{0, 1, \ldots, \frac{n}{\delta_k^- \delta_w^-} - 1\right\} = \{0, 1, 2, 3, 4, 5, 6\}$
$r^+ \in \left\{0, 1, \ldots, \frac{n}{\delta_k^+ \delta_w^+} - 1\right\} = \{0, 1, 2, 3, \ldots, 34\}.$

Ao final do 1º ciclo de 7 números (Tabela 7), o próximo valor de (p, q) exigirá uma quebra de passo no procedimento. De fato, $(80 + 7 \cdot 45 \equiv 80 \pmod{105}, 13 - 7 \cdot 45 \equiv 13 \pmod{105})$. Então, adicionamos 51 à coordenada p e 51 à coordenada q, obtendo $(80 + 51 \equiv 26, 13 + 51 \equiv 64)$. Em seguida, voltamos ao procedimento dos passos até completar outro ciclo de 7 números, Tabela 8. E assim por diante. A próxima tabela terá $r^+ = 1$

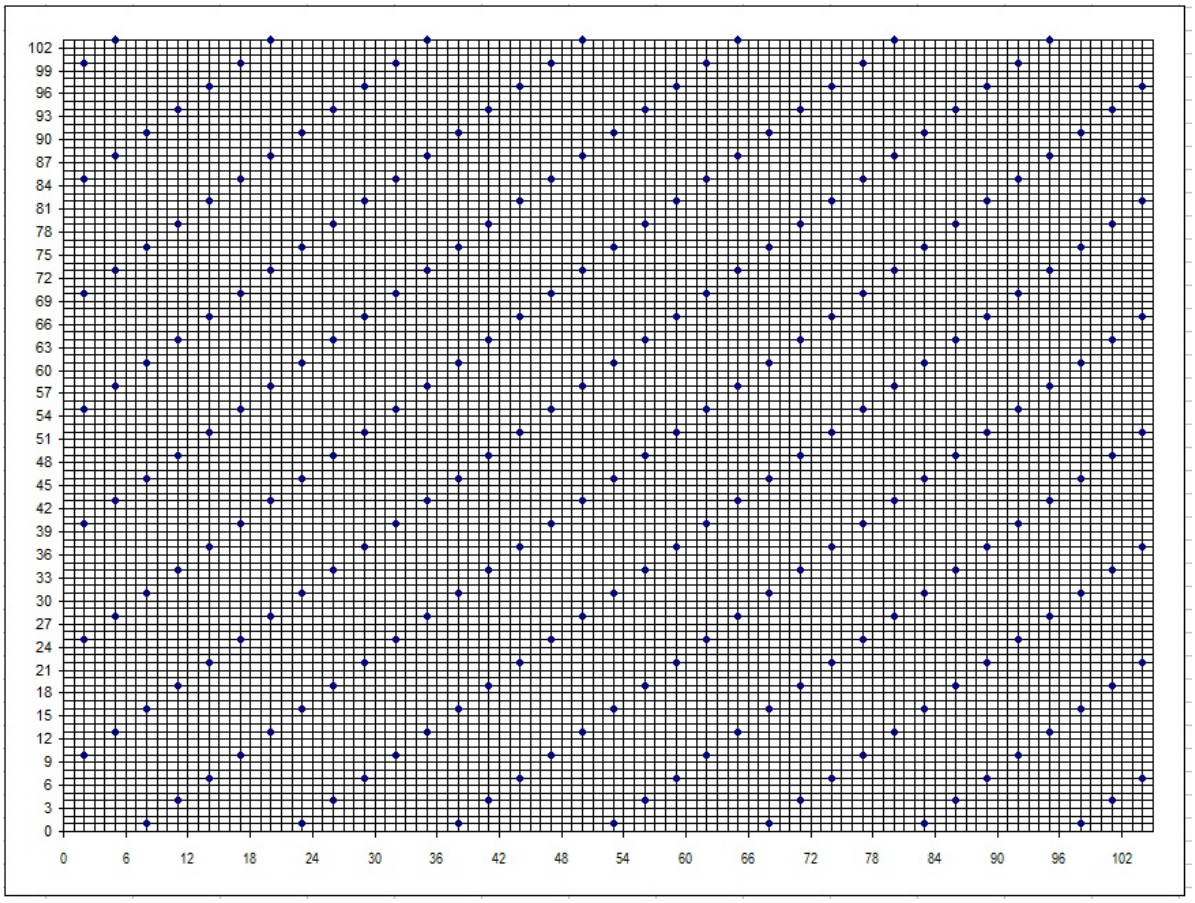
Tabela 8 - Coordenadas iniciais para DPP e DPN mágicas

	r^-	(p, q)
$r^+ = 1$	0	$(26, 64)$
	1	$(26 + 45 \equiv 71, 64 - 45 \equiv 19)$
	2	$(71 + 45 \equiv 11, 19 - 45 \equiv 79)$
	3	$(11 + 45 \equiv 56, 79 - 45 \equiv 34)$
	4	$(56 + 45 \equiv 101, 34 - 45 \equiv 94)$
	5	$(101 + 45 \equiv 41, 94 - 45 \equiv 49)$
	6	$(41 + 45 \equiv 86, 49 - 45 \equiv 4)$

Fonte: O autor, 2014.

A última tabela terá $r^+ = 34$. Com este procedimento são obtidas $\frac{n}{\delta_w^+ \cdot \delta_k^+} \cdot \frac{n}{\delta_w^- \cdot \delta_k^-} = 245$ coordenadas. A regularidade das 245 coordenadas iniciais (p, q) que garantem DPP e DPN mágicas é exibida na Figura 28.

Figura 28 - Coordenadas iniciais para DPP e DPN mágicas (parâmetros: $n = 105$, $\alpha = 11$, $\beta = 2$, $a = 31$, $b = 11$).



Fonte: O autor, 2014.

Exemplo 16. Alguns casos especiais – um coeficiente é múltiplo de n. Não podemos ter $\alpha+\beta\equiv 0$ e $a+b\equiv 0$. De fato,

$$\alpha+\beta\equiv 0\Rightarrow n\mid(\alpha+\beta)\quad\text{e}\quad(a+b)\equiv 0\Rightarrow n\mid(a+b)$$

Logo

$$n\mid b(\alpha+\beta)-\beta(a+b)\Rightarrow n\mid(\alpha b-\beta a)\Rightarrow \text{mdc}(\alpha b-\beta a,n)=n,$$

o que impede o preenchimento do quadrado. Conforme a introdução da seção 6 na página 61, $\text{mdc}(\alpha b-\beta a,n)$ tem de ser igual a 1, que é a condição para o preenchimento do quadrado.

Também não podemos ter $\alpha+\beta\equiv 0$ e $\text{mdc}(a+b,n)=\delta\neq 1$. De fato,

$$\alpha+\beta\equiv 0\Rightarrow n\mid(\alpha+\beta)\quad\text{e}\quad\text{mdc}(a+b,n)=\delta\Rightarrow\delta\mid(a+b),\quad\delta\mid n$$

Portanto

$$\begin{aligned}n\mid b(\alpha+\beta)\quad\text{e}\quad\delta\mid\beta(a+b)&\Rightarrow\delta\mid b(\alpha+\beta),\quad\delta\mid\beta(a+b)\\&\Rightarrow\delta\mid b(\alpha+\beta)-\beta(a+b)\\&\Rightarrow\delta\mid(\alpha b-\beta a)\\&\Rightarrow\text{mdc}(\alpha b-\beta a,n)=\delta,\end{aligned}$$

e o quadrado não preenche. Logo, nas equações que determinam as diagonais principais se um dos coeficientes for múltiplo de n o outro terá de ser primo com n.

- Vamos tomar $(\alpha+\beta)w+(a+b)k\equiv 1-q-p\pmod n$.

  $(\alpha+\beta)\equiv 0\Rightarrow\text{mdc}(\alpha+\beta,n)=n\Rightarrow k\in\left\{\dfrac{n-1}{2}\right\}$

  $\text{mdc}(a+b,n)=1\Rightarrow w\in\{0,1,2,\ldots,n-1\}$ w assume os valores de um sistema completo de resíduos módulo n mas k assume apenas um valor. Vamos determinar a variação de $1-q-p$ quando w aumenta 1. Observe que k aumenta 0 pois é constante.

  $$\begin{aligned}(\alpha+\beta)(w+1)+(a+b)(k+0)&\equiv(\alpha+\beta)w+(\alpha+\beta)+(a+b)k\\&\equiv(\alpha+\beta)w+(a+b)k+(\alpha+\beta)\\&\equiv(\alpha+\beta)w+(a+b)k.\end{aligned}$$

Logo, $1-q-p$ é constante, terá apenas um valor. Este valor será igual a

$$(\alpha+\beta)0+(a+b)\left(\frac{n-1}{2}\right)\equiv(a+b)\left(\frac{n-1}{2}\right).$$

Logo, a diagonal principal positiva será mágica se

$$1-q-p\equiv(a+b)\left(\frac{n-1}{2}\right)\pmod{n}.$$

- Vamos tomar $(\alpha-\beta)w+(a-b)k\equiv q-p\pmod{n}$.

  $(\alpha-\beta)\equiv 0\Rightarrow \text{mdc}(\alpha-\beta,n)=n\Rightarrow k\in\left\{\frac{n-1}{2}\right\}$

  $\text{mdc}(a-b,n)=1\Rightarrow w\in\{0,1,2,\ldots,n-1\}$ w assume os valores de um sistema completo de resíduos módulo n mas k assume apenas um valor. Vamos determinar a variação de $q-p$ quando w aumenta 1. Observe que k aumenta 0 pois é constante.

$$\begin{aligned}(\alpha-\beta)(w+1)+(a-b)(k+0)&\equiv(\alpha-\beta)w+(\alpha-\beta)+(a-b)k\\&\equiv(\alpha-\beta)w+(a-b)k+(\alpha-\beta)\\&\equiv(\alpha-\beta)w+(a-b)k.\end{aligned}$$

  Logo, $q-p$ é constante, terá apenas um valor. Este valor será igual a

$$(\alpha-\beta)0+(a-b)\left(\frac{n-1}{2}\right)\equiv(a-b)\left(\frac{n-1}{2}\right).$$

  Logo, a diagonal principal negativa será mágica se

$$q-p\equiv(a-b)\left(\frac{n-1}{2}\right)\pmod{n}.$$

Observação 13. A condição necessária do quadrado preenchido pelo método do passo uniforme ser mágico nas linhas e colunas é de n ser ímpar. Se[15] $n>3$ for ímpar e primo, podemos construir quadrados mágicos nas linhas e colunas e ainda diabólicos escolhendo os coeficientes α, β, a, b, $\alpha\pm\beta$, $a\pm b$ tais que nenhum seja múltiplo de n.

[15] Em seu artigo, Lehmer (1929) faz a seguinte afirmação: "...um quadrado diabólico não pode ser construído pelo método do passo uniforme quando n for múltiplo de 3. Pois se α e β forem primos com 3, $\alpha+\beta$ e $\alpha-\beta$ não poderiam ser ambos primos com 3. Contudo, isso não significa que um quadrado diabólico não possa ser obtido por outros métodos quando n for múltiplo de 3".

7 MÉTODO DE LA LOUBÈRE

De La Loubère apresentou o seguinte método de construção de quadrados mágicos de ordem ímpar.

> Coloque o número 1 no topo da coluna central. Em seguida, suba, sucessivamente, pela diagonal negativa que passa por 1, preenchendo, ordenadamente, com os números $2, \ldots, n$, todas as posições remanescentes. Quando essa diagonal tiver sido preenchida com os números $1, 2, \ldots, n$ escreva $n+1$ imediatamente abaixo da célula contendo n e preencha as células remanescentes da nova diagonal negativa com os números $n+2, \ldots, 2n$. Continue este procedimento. Cada vez que uma nova diagonal negativa for preenchida escreva o próximo número imediatamente abaixo do número anterior e suba novamente preenchendo as posições remanescentes da diagonal com os números sucessivos.

Usaremos os resultados obtidos no presente trabalho para fazer a análise do método de La Loubère para a construção de quadrados mágicos no sentido usual, isto é, linhas, colunas e as duas diagonais principais mágicas.

Um quadrado construído pelo método de La Loubère terá os parâmetros $\alpha = 1$, $\beta = 1$, $a = -1$, $b = -2$, $p = \dfrac{n+1}{2}$ e $q = n$. O determinante $\alpha b - \beta a = -1$, primo com n, vai garantir o preenchimento. Os parâmetros α, β, a e b serão sempre primos com n ímpar, o que garantirá o quadrado mágico nas linhas e colunas.

$\forall n$ ímpar, não múltiplo de 3, a diagonal principal positiva será mágica, independentemente de (p, q), uma vez que $\alpha + \beta = 2$ e $a + b = -3$ serão primos com n.

$\forall n$ ímpar, múltiplo de 3, $\delta_w^+ = \text{mdc}(a+b, n) = \text{mdc}(-3, n) = 3$ e $\delta_k^+ = \text{mdc}(\alpha + \beta, n) = \text{mdc}(2, n) = 1$. Segue:

$$q_0 + p_0 \equiv 1 - (\alpha+\beta) \cdot \left(\frac{\delta_w^+ - 1}{2}\right) - (a+b) \cdot \left(\frac{\delta_k^+ - 1}{2}\right) \pmod{n}$$

$$q_0 + p_0 \equiv 1 - 2 \cdot 1 - 3 \cdot 0 \equiv -1 \pmod{n}$$

Os valores de $q + p \pmod{n}$ que dão DPP mágicas são obtidos por:

$$q + p \equiv q_0 + p_0 + t \cdot \delta_w^+ \cdot \delta_k^+ \pmod{n}, \text{ onde } 1 \leq t \leq \frac{n}{\delta_w^+ \cdot \delta_k^+}$$

Escrevendo n na forma $n = 3(2s-1)$ com $s \in \{1, 2, 3, \ldots\}$, segue

$$\frac{n}{\delta_w^+ \cdot \delta_k^+} = \frac{3(2s-1)}{3} = 2s - 1$$

$$q + p \equiv -1 + t \cdot \delta_w^+ \cdot \delta_k^+ \pmod{n} \text{ com } t = 1, 2, 3, \ldots, 2s-1.$$

Evidentemente, $2s-1$ é ímpar, então $\forall n$, ímpar múltiplo de 3, há uma quantidade ímpar de somas $q+p \pmod{n}$, incongruentes, que nos dão DPP mágicas. A primeira destas somas

$q+p$, é obtida fazendo-se $t = 1$. Seu valor é $p+q \equiv -1+1\cdot 3 \equiv 2$ e a última soma $q+p$ é obtida fazendo $t = 2s-1$. Seu valor é $q+p \equiv -1+(2s-1)\cdot 3 \equiv 6s-4 \equiv 6\left(\frac{n+3}{6}\right)-4 \equiv n-1 \pmod{n}$. Então, a soma central $q+p$, pode ser calculada simplesmente fazendo a média do primeiro $q+p$ com o último $q+p$, isto é, $\frac{2+n-1}{2} \equiv \frac{n+1}{2} \pmod{n}$.
Afirmamos que a soma das coordenadas sugeridas pelo método de La Loubère, $q = n$ e $p = \frac{n+1}{2}$ vai ser igual, $\forall n$ ímpar múltiplo de 3, à soma central $q+p \pmod{n}$ do conjunto de soluções $q+p$ que dão DPP mágicas. De fato, a soma das coordenadas módulo n, de La Loubère, vai dar $q+p \equiv n+\frac{n+1}{2} \equiv \frac{n+1}{2} \pmod{n}$. Portanto, $\forall n$ ímpar, o método de La Loubère vai construir quadrados com a diagonal principal positiva mágica.

A diagonal principal negativa será determinada por

$(\alpha-\beta)w+(a-b)k \equiv q-p \pmod{n}$
$(1-1)w+(-1+2)k \equiv n-\left(\frac{n+1}{2}\right) \pmod{n}$
$0w+k \equiv \left(\frac{n-1}{2}\right) \pmod{n}$
$k \equiv \left(\frac{n-1}{2}\right) \pmod{n}$

Dessa feita, os elementos x_i da DPN terão k_i constante igual a $\left(\frac{n-1}{2}\right)$, assumindo a forma $x_i = 1+w_i+\left(\frac{n-1}{2}\right)n$ com w_i varrendo os valores de um sistema completo de resíduos módulo n. Somando esses elementos temos

$$\sum_{i=1}^{n} x_i = \sum_{i=1}^{n}\left(1+w_i+\left(\frac{n-1}{2}\right)n\right) = \sum_{i=1}^{n}1+\sum_{i=1}^{n}w_i+\sum_{i=1}^{n}\left(\frac{n-1}{2}\right)n$$
$$= n+\left(\frac{n-1}{2}\right)n+\left(\frac{n-1}{2}\right)n^2 = \left(\frac{n^2+1}{2}\right)n \quad \text{(soma mágica)}$$

Portanto, $\forall n$ ímpar, o método de La Loubère vai construir quadrados com a diagonal principal negativa mágica.

Uma curiosidade do método: O número central, $\frac{n^2+1}{2}$ irá se localizar sempre no centro do quadrado $\left(\frac{n+1}{2}, \frac{n+1}{2}\right)$. Vamos mostrar porque isso acontece:
Substituindo $x = \frac{n^2+1}{2}$, $p = \frac{n+1}{2}$, $\alpha = 1$ e $a = -1$ na congruência
$A \equiv p+\alpha(x-1)+a\left[\frac{x-1}{n}\right] \pmod{n}$, vamos obter

$$A \equiv \frac{n+1}{2} + \left(\frac{n^2+1}{2} - 1\right) - \left[\frac{\frac{n^2+1}{2} - 1}{n}\right] \pmod{n}$$

$$A \equiv \frac{n+1}{2} + \left(\frac{n^2-1}{2}\right) - \left[\frac{\frac{n^2}{2} - \frac{n}{2} + \frac{n}{2} - \frac{1}{2}}{n}\right] \pmod{n}$$

$$A \equiv \frac{n+1}{2} + \left(\frac{n^2-1}{2}\right) - \left[\frac{n\left(\frac{n}{2} - \frac{1}{2}\right) + \left(\frac{n}{2} - \frac{1}{2}\right)}{n}\right] \pmod{n}$$

$$A \equiv \frac{n+1}{2} + \left(\frac{n^2-1}{2}\right) - \left[\left(\frac{n-1}{2}\right) + \left(\frac{n-1}{2n}\right)\right] \pmod{n}.$$

Como n é ímpar maior ou igual a 3, $\left[\left(\frac{n-1}{2}\right)\right] = \frac{n-1}{2}$ e $\left[\left(\frac{n-1}{2n}\right)\right] = 0$,

$$A \equiv \frac{n+1}{2} + \left(\frac{n^2-1}{2}\right) - \left(\frac{n-1}{2}\right) \pmod{n}$$

$$A \equiv \frac{n}{2} + \frac{n^2}{2} - \frac{n}{2} + \frac{1}{2} \pmod{n}$$

$$A \equiv n\left(\frac{n-1}{2}\right) + \frac{n+1}{2} \pmod{n}$$

$$A \equiv \frac{n+1}{2} \pmod{n} \Rightarrow A = \frac{n+1}{2}.$$

Analogamente, vamos substituir $x = \frac{n^2+1}{2}$, $q = n$, $\beta = 1$ e $b = -2$ na congruência $B \equiv q + \beta(x-1) + b\left[\frac{x-1}{n}\right] \pmod{n}$, vamos obter

$$B \equiv n + \left(\frac{n^2+1}{2} - 1\right) - 2\left[\frac{\frac{n^2+1}{2} - 1}{n}\right] \pmod{n}$$

$$B \equiv n + \left(\frac{n^2-1}{2}\right) - 2\left[\frac{\frac{n^2}{2} - \frac{n}{2} + \frac{n}{2} - \frac{1}{2}}{n}\right] \pmod{n}$$

$$B \equiv n + \left(\frac{n^2-1}{2}\right) - 2\left[\frac{n\left(\frac{n}{2} - \frac{1}{2}\right) + \left(\frac{n}{2} - \frac{1}{2}\right)}{n}\right] \pmod{n}$$

$$B \equiv n + \left(\frac{n^2-1}{2}\right) - 2\left[\left(\frac{n-1}{2}\right) + \left(\frac{n-1}{2n}\right)\right] \pmod{n}.$$

Como n é ímpar maior ou igual a 3, $\left[\left(\frac{n-1}{2}\right)\right] = \frac{n-1}{2}$ e $\left[\left(\frac{n-1}{2n}\right)\right] = 0$,

$$B \equiv n + \left(\frac{n^2-1}{2}\right) - 2\left(\frac{n-1}{2}\right) \pmod{n}$$

$$B \equiv \frac{n^2}{2} + \frac{1}{2} \pmod{n}$$

$$B \equiv \frac{n^2}{2} + \frac{1}{2} + \frac{n}{2} - \frac{n}{2} \pmod{n}$$

$$B \equiv n\left(\frac{n-1}{2}\right) + \frac{n+1}{2} \pmod{n}$$

$$B \equiv \frac{n+1}{2} \pmod{n} \Rightarrow B = \frac{n+1}{2}.$$

CONCLUSÃO

Quando fiz a disciplina Aritmética no PROFMAT pude redescobrir esse campo fecundo da matemática que bem explorado poderia proporcionar melhorias no ensino-aprendizagem da matemática. Por trabalhar com os números naturais, familiares às crianças desde as primeiras contagens, oferecia, ao meu ver, um campo vasto, seja para a investigação, seja para uma ampla variedade de problemas possibilitando, se bem explorados, uma sólida aprendizagem dos fundamentos para uma boa formação matemática, entendida aqui, não apenas como habilidade de fazer cálculos ou resolver problemas com sucesso e rapidez mas de adquirir a metodologia, a maneira matemática de se olhar para as coisas do mundo. Seria a capacidade não só de resolver o problema matematizado mas de matematizar o problema.

Pela primeira vez, pude refletir sobre a minha formação matemática. Retomando minhas lembranças da escola, incluindo a universidade, pareceu-me evidente uma predominância acentuada da matemática do contínuo: a resolução de equações, o estudo das funções, por exemplo, em detrimento da matemática discreta, em particular da Aritmética. A Álgebra com seus x's e y's e a Geometria com seus triângulos retângulos ocupavam quase toda a mesa relegando a Aritmética a um papel secundário ou até mesmo a ficar na gaveta. De um certo modo, poderia até ser compreensível que seja assim no ensino médio. Mas fica a pergunta, e a inquietação para os responsáveis do ensino nos primeiros anos do fundamental e sobretudo para o ensino de matemática nos anos iniciais.

A proposta para o TCC de detalhamento do artigo "Sobre congruências associadas a certos quadrados mágicos" de Lehmer (1929) me atraiu por atender a este novo interesse em Aritmética além da proposta que era digamos muito mais matemática do que pedagógica, tendo um objeto de algum modo afim com a matemática do fundamental nas escolas públicas além de não propor nenhum indesejável levantamento de dados com turmas.

Vale destacar o impasse causado pelo parágrafo de Lehmer (1929, p. 531) estar equivocado ou não. Por ter uma influência japonesa mais rígida em relação à autoridade moral, encontrei uma grande resistência em admitir que o mestre pudesse ter cometido um deslize. Mas foi justamente o querer defendê-lo que possibilitou o desenvolvimento deste trabalho. Pode-se afirmar que tomou um rumo bem diferente do previsto inicialmente, que era apenas detalhar e fundamentar cada passagem do artigo de Lehmer.

REFERÊNCIAS

CHABERT, J.; BARBIN, E. *A History of Algorithms: From the Pebble to the Microchip*. Berlin, Heidelberg, New York: Springer Verlag, 1999.

HEFEZ, A. *Elementos de aritmética*. Rio de Janeiro: SBM, 2006. (Textos Universitários).

KRAITCHIK, M. *Mathematical recreations*. [S.l.]: W.W. Norton & company inc., 1942.

LEHMER, D. N. On the congruences connected with certain magic squares. *Transactions of the American Mathematical Society*, v. 31, p. 529–551, 1929.

SANTOS, J. P. d. O. *Introduçao à teoria dos números*. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1998. (Coleçao Matemática Universiária).

SIVARAMAKRISHNAN, R. *Certain Number-Theoretic Episodes In Algebra*. Hoboken, NJ: Taylor & Francis, 2006. (Chapman & Hall/CRC Pure and Applied Mathematics).