Regularidades associadas ao método do passo uniforme*

J. I. TRAVASSOS † P. N. SILVA ‡

Resumo

Nesse artigo, discutimos o comportamento das soluções de um sistema linear módulo n relacionado ao método do passo uniforme. Trata-se de um método para construção de quadrados mágicos de ordem ímpar proposto e analisado matematicamente por Lehmer [2]. Exploramos aqui o não preenchimento do quadrado e as regularidades associadas a esse processo.

Abstract

In this article, we discuss the behavior of solutions of a linear system module n related to the uniform step method. It is a method for constructing magic squares of odd order proposed and analyzed mathematically by Lehmer [2]. We investigate what happens when the method fails and we analyze the regularities associated with this process.

1 Introdução

Segundo Lehmer [2], uma matriz quadrada de ordem n preenchida com todos os números naturais de 1 até n^2, sem repetição, é chamada de quadrado mágico se a soma dos números de qualquer linha ou coluna for a mesma. Nesse caso, dizemos que o quadrado é mágico nas linhas e mágico nas colunas, respectivamente.

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 a certos aspectos do *método do passo uniforme* (MPU). Esse método[1] foi analisado matematicamente por Lehmer [2]. Ele consiste em atribuir, um de cada vez, ordenadamente, a sequência dos números $1, 2, 3, ..., n^2$ às células do quadrado seguindo uma regularidade de movimentos para a direita e para cima. Lehmer dividiu sua análise em várias etapas. Ele investigou sob quais hipóteses: (a) o método preenche o quadrado; (b) as colunas resultam mágicas e (c) as linhas resultam mágicas.

Ao analisar o preenchimento do quadrado, Lehmer [2] nos instigou a investigar o não preenchimento.

*Palavras chave: Quadrados Mágicos, Método do Passo Uniforme, não-preenchimento

†discente PROFMAT/UERJ, joseichihara@hotmail.com

‡Departamento de Análise Matemática, IME/UERJ, nunes@ime.uerj.br

[1] O método do passo uniforme apenas pode ser usado para gerar quadrados mágicos de ordem ímpar. No entanto, na discussão do preenchimento do quadrado pelo método, essa restrição não se faz necessária.

2 O método do passo uniforme

Cada célula do quadrado de ordem n será identificada por suas coordenadas (A, B) que indicam, respectivamente, a coluna e a linha que a ela correspondem. As linhas são numeradas de baixo para cima e as colunas, da esquerda para direita. Assim temos a seguinte disposição:

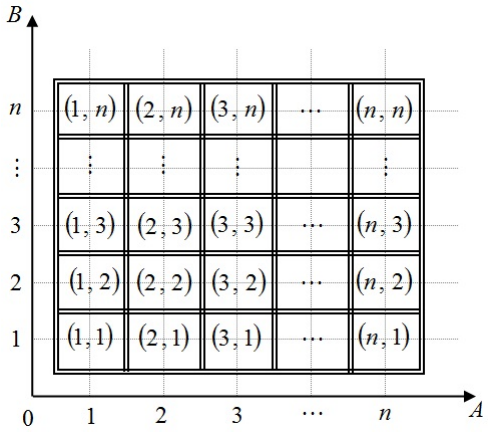


Figura 1: Coordenadas das células
Fonte: dados da pesquisa

2.1 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. Esses passos serão mantidos, por isso, α e β são chamadas de *constantes do passo uniforme*. A "saída" da matriz é evitada utilizando-se a congruência módulo n para determinar as coordenadas de cada célula. Com efeito, ao considerarmos $(A, B) \equiv (x, y) \pmod{n}$ se e somente se $A \equiv x \pmod{n}$ e $B \equiv y \pmod{n}$, os valores para as coordenadas podem ser obtidos de 1 a n. Para tornar o texto mais leve vamos omitir a escrita do $\pmod{n}$. 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 2.1.

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 2(a).

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 numa outra célula, com coordenadas $(2+1, 3+2) \equiv (3, 5)$. Os números de 7 até 10 poderão, então, ser alocados fechando o 2º ciclo, Figura 2(b). Esse procedimento se repete para o 3º ciclo, Figura 2(c) e prossegue com o 4º e 5º ciclos até que todos os 25 números tenham sido distribuídos, Figura 2(d).

			3	
		2		
	1			
5				
				4

(a) 1º ciclo

		6	3	
	10	2		
9	1			
5				8
			7	4

(b) 2º ciclo

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

(c) 3º ciclo

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

(d) 4º e 5º ciclos

Figura 2: Inserção de 1 a 25 pelo MPU
Fonte: dados da pesquisa

2.2 Congruências associadas

O processo descrito no exemplo pode ser resumido nas congruências fundamentais propostas por Lehmer [2], para determinar as coordenadas (A, B) da célula na qual cada número $x \in \{1, \ldots, n^2\}$ deve ser alocado:

$$A \equiv p + \alpha\,(x-1) + a\left[\frac{x-1}{n}\right] \pmod n \tag{2.1}$$

$$B \equiv q + \beta\,(x-1) + b\left[\frac{x-1}{n}\right] \pmod n \tag{2.2}$$

onde (p, q) são as coordenadas da célula ocupada pelo 1 e $[w]$ representa a parte inteira do número real w. Estas congruências nos indicam que as coordenadas A e B de um número x no quadrado, pelo método do passo uniforme, dependem dos seis parâmetros α, β, a, b, p e q.

No método do passo uniforme, o coeficiente $(x-1)$ de α e β é um contador da quantidade de passos. O coeficiente $\left[\frac{x-1}{n}\right]$ de a e b é um contador das quebras de passos. De fato, após cada ciclo (de n alocações), há uma quebra de passo, sendo adicionada uma unidade ao coeficiente de a e b que se mantém constante durante os ciclos.

Para nossa análise, será conveniente observar que o teorema da Divisão Euclidiana garante que um número natural $x \in \{1, 2, 3, \cdots, n^2\}$ pode ser escrito, de maneira única, na forma

$$x = 1 + w + kn \tag{2.3}$$

com $0 \leq w, k \leq n-1$. Mais precisamente, k é o quociente da divisão de $x-1$ por n,

$$k = \left[\frac{x-1}{n}\right] \tag{2.4}$$

e, w é o resto dessa divisão,

$$w \equiv x - 1 \pmod{n}. \tag{2.5}$$

O conceito de congruência módulo n foi utilizado para formalizar matematicamente o procedimento indicado pelo método do passo uniforme. Foi possível estabelecer uma relação algébrica entre cada número x e as coordenadas da célula que será ocupada por ele.

3 O método preenche o quadrado?

Nesta seção, apresentamos o resultado de Lehmer [2] para preenchimento do quadrado pelo método do passo uniforme. Lehmer [2] estabelece o seguinte resultado

Teorema 3.1 (Lehmer [2, p. 530])**.** *Dados α, β, a e b todos primos com n, uma condição necessária e suficiente para que o método do passo uniforme preencha o quadrado é que $\alpha b - \beta a$ seja primo com n.*

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 as mesmas coordenadas (A, B). A prova de Lehmer [2] explora esse fato.

Sejam x_1 e x_2 dois números do conjunto $\{1, 2, 3, \ldots, n^2\}$. Vamos denotar respectivamente por (A_1, B_1) e por (A_2, B_2) suas coordenadas dadas por (2.1) e (2.2). 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,

$$\begin{cases} \alpha\,(x_1 - x_2) + a\left(\left[\dfrac{x_1-1}{n}\right] - \left[\dfrac{x_2-1}{n}\right]\right) \equiv 0 \pmod{n} & (3.6) \\ \beta\,(x_1 - x_2) + b\left(\left[\dfrac{x_1-1}{n}\right] - \left[\dfrac{x_2-1}{n}\right]\right) \equiv 0 \pmod{n} & (3.7) \end{cases}$$

Utilizando propriedades de congruência[2] em (3.6)-(3.7), Lehmer deduz o sistema (3.8)-(3.9), associado à condição de dois números x_1 e x_2 ocuparem a mesma célula, pelo método do passo uniforme.

$$\begin{cases} \Delta\,(x_1 - x_2) \equiv 0 \pmod{n} & (3.8) \\ \Delta\left\{\left[\dfrac{x_1-1}{n}\right] - \left[\dfrac{x_2-1}{n}\right]\right\} \equiv 0 \pmod{n} & (3.9) \end{cases}$$

onde $\Delta = \alpha b - \beta a$.

A proposição "Se o quadrado preenche, então $\alpha b - \beta a$ é primo com n." é equivalente à sua contrapositiva "Se $\alpha b - \beta a$ não é primo com n, então o quadrado não preenche". Lehmer toma a contrapositiva.

[2] Veja Proposições 9.1.4 e 9.1.5 em Hefez [1, pp. 113–114]

Essencialmente, ele quer exibir dois números x_1 e x_2 que satisfazem (3.8)–(3.9), que ocupem a mesma célula, isto é, que também satisfaçam (3.6)-(3.7).

Para provar que a condição de primalidade de $\alpha b - \beta a$ e n é necessária, Lehmer parte do sistema (3.8)-(3.9) e argumenta da seguinte maneira:

> Se[3] o $\text{mdc}(\alpha b - \beta a, n) = \delta$, então
>
> $$\left[\frac{x_1 - 1}{n}\right] \equiv \left[\frac{x_2 - 1}{n}\right] \left(\text{mod } \frac{n}{\delta}\right)$$
>
> e $x_1 \equiv x_2 \left(\text{mod } \frac{n}{\delta}\right)$. 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
>
> $$\left[\frac{x_1 - 1}{n}\right] \equiv \left[\frac{x_1 - 1}{n} + \frac{n}{\delta}\right] \left(\text{mod } \frac{n}{\delta}\right).$$
>
> 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 passo uniforme na mesma célua e o quadrado não será preenchido. (Lehmer [2, p. 531]).

Lehmer [2], assume que os parâmetros α, β, a, b do método do passo uniforme sejam todos primos com n e ainda que o $\text{mdc}(\alpha b - \beta a, n) = \delta \neq 1$. Lehmer [2] exibe dois números $x_2 - x_1 = \frac{n^2}{\delta}$ que satistazem ao sistema equivalente a (3.8)–(3.9)[4]

$$\begin{cases} x_1 \equiv x_2 \left(\text{mod } \dfrac{n}{\delta}\right) & (3.10) \\ \left[\dfrac{x_1 - 1}{n}\right] \equiv \left[\dfrac{x_2 - 1}{n}\right] \left(\text{mod } \dfrac{n}{\delta}\right) & (3.11) \end{cases}$$

e afirma que vão cair na mesma célula e por isto o quadrado não será preenchido.

Essa afirmação é equivocada. Veremos mais adiante que se x_1 e x_2 tais que, $x_1 - x_2 = \frac{n^2}{\delta}$ não satisfazem (3.6)-(3.7)

A possibilidade de haver dois números x_1 e x_2 que satisfaçam as congruências do sistema (3.10)–(3.11) mas não ocupem a mesma célula do quadrado nos instigou a entender como se configura o não preenchimento pelo método do passo uniforme. O fato de Lehmer [2] ter pensado que soluções não triviais de (3.8)-(3.9) são também soluções de (3.6)-(3.7), ou seja, ocupam a mesma célula, nos levou a fazer uma análise da relação entre esses sistemas.

---

[3] *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.

[4] A Proposição 9.1.5 [1, p. 114] garante a equivalência dos sistemas (3.8)–(3.9) e (3.10)–(3.11)

3.1 O ponto crucial no caminho da volta

O ponto crucial na prova da condição necessária encontra-se na passagem, de (3.6)-(3.7) para (3.8)-(3.9), 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 (3.8)-(3.9) para (3.6)-(3.7) observamos algo que nos surpreendeu. Vamos, adotar aqui, a notação com $w's$ e $k's$. O sistema (3.8)-(3.9) pode ser reescrito como

$$\begin{cases} (\alpha b - \beta a)(w_1 - w_2) \equiv 0 \,(\text{mod } n) & (3.12) \\ (\alpha b - \beta a)(k_1 - k_2) \equiv 0 \,(\text{mod } n) & (3.13) \end{cases}$$

e é equivalente a

$$\begin{cases} b[\alpha(w_1 - w_2) + a(k_1 - k_2)] - a[\beta(w_1 - w_2) + b(k_1 - k_2)] \equiv 0 \,(\text{mod } n) & (3.14) \\ \alpha[\beta(w_1 - w_2) + b(k_1 - k_2)] - \beta[\alpha(w_1 - w_2) - a(k_1 - k_2) \equiv 0 \,(\text{mod } n) & (3.15) \end{cases}$$

Multiplicando (3.14) por α e (3.15) por a e somando, vamos obter:

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

Multiplicando (3.14) por β e (3.15) por b e somando, vamos obter:

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

Portanto, sob as hipóeteses de α, β, a e b serem primos com n, o sistema (3.12)-(3.13) é equivalente a:

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

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

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

Portanto, o que impede a equivalência entre os sistemas (3.6)-(3.7) e (3.8)-(3.9) 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 [2].

Afirmamos que é possivel haver dois números x_1 e x_2 que satisfaçam as congruências do sistema (3.10)–(3.11) mas não ocupem a mesma célula do quadrado. Compreender essa afirmação exigiu o entendimento de como se configura o não preenchimento pelo método do passo uniforme. Como consequência dessa investigação, deduzimos e identificamos várias regularidades associadas ao não preenchimento do quadrado pelo método do passo uniforme.

3.1.1 Se o método preenche, $\alpha b - \beta a$ é primo com n?

Para compreender o equívoco de Lehmer, é necessário analisar cuidadosamente o sistema (3.10)–(3.11).

Por (2.4), a equação (3.11) pode ser reescrita:

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

De acordo com (2.3), a equação (3.10) pode ser escrita:

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

O sistema (3.10)–(3.11) pode, então, ser reescrito:

$$\begin{cases} w_1 \equiv w_2 \left(\mathrm{mod}\ \dfrac{n}{\delta}\right) & (3.16) \\ k_1 \equiv k_2 \left(\mathrm{mod}\ \dfrac{n}{\delta}\right) & (3.17) \end{cases}$$

Seja S_I o subconjunto de $\{1, \ldots, n^2\}$ tal que para todo $x_1, x_2 \in S_I$, tenhamos x_1, x_2 é solução de (3.10)–(3.11).

Como queremos investigar números $x_1, x_2 \in \{1, 2, \ldots, n^2\}$ que ocupam a mesma célula no quadrado, estamos interessados em determinar os elementos x_j de S_I. Por (2.3), podemos representá-los na forma

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

Vamos nos referir a tais elementos como *soluções de interesse* do sistema (3.10)–(3.11). A cada solução de interesse x_j do sistema (3.10)–(3.11), podemos associar uma solução de interesse (w_j, k_j) do sistema (3.16)–(3.17). A coordenada w_j será chamdade de solução de interesse de (3.16) e k_j, de solução de interesse de (3.17). Obviamente, duas soluções de interesse w_1 e w_2 de (3.16) deixam o mesmo resto w' na divisão por $\frac{n}{\delta}$. De um modo geral, duas soluções de interesse w_1 e w_2 de (3.16) são dadas por

$$w_j = w' + l_j \cdot \frac{n}{\delta}, \quad j = 1, 2, \tag{3.18}$$

para algum w' tal que $0 \leq w' \leq \frac{n}{\delta} - 1$. Como w_j é tal que $0 \leq w_j \leq n - 1$, temos $0 \leq l_j \leq \delta - 1$.

Analogamente, duas soluções de interesse k_1 e k_2 de (3.17) são dadas por

$$k_j = k' + t_j \cdot \frac{n}{\delta}, \quad j = 1, 2, \tag{3.19}$$

com $0 \leq t_j \leq \delta - 1$ e para algum k' tal que $0 \leq k' \leq \frac{n}{\delta} - 1$.

Portanto, as soluções de interesse do sistema (3.10)–(3.11) podem ser agrupadas em função dos pares (w', k'). Para cada w' e k' pertencentes ao conjunto de resíduos[5] módulo $\frac{n}{\delta}$, (3.18) e (3.19) nos mostram

[5] $w', k' \in \left\{0, 1, 2, \cdots, \frac{n}{\delta} - 1\right\}$.

que há δ^2 soluções de interesse (w_j, k_j) do sistema (3.16)–(3.17). Além disso, sendo x_1 e x_2 duas soluções do sistema (3.10)–(3.11), por (3.18) e (3.19), temos

$$x_j = 1 + w' + k'n + l_j \cdot \frac{n}{\delta} + t_j \cdot \frac{n^2}{\delta}, \quad j = 1, 2. \tag{3.20}$$

para algum l_j e t_j pertencentes ao conjunto de resíduos[6] módulo δ.

4 Como ocorre o não preenchimento?

Vimos que as soluções de interesse do sistema (3.10)–(3.11) 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 3, formando uma matriz $M(w', k')$.

Figura 3: 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	$x' + 0 \cdot \frac{n}{\delta} + 1 \cdot \frac{n^2}{\delta}$	$x' + 1 \cdot \frac{n}{\delta} + 1 \cdot \frac{n^2}{\delta}$	$x' + 2 \cdot \frac{n}{\delta} + 1 \cdot \frac{n^2}{\delta}$	$\cdots$	$x' + (\delta - 1) \cdot \frac{n}{\delta} + 1 \cdot \frac{n^2}{\delta}$
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.

Mais precisamente, para $0 \leq w',\ k' \leq \frac{n}{\delta} - 1$, temos

$$M(w', k') = (m_{t+1,l+1}), \quad m_{t+1,l+1} = x_{tl} = x' + l \cdot \frac{n}{\delta} + t \cdot \frac{n^2}{\delta}, \qquad 0 \leq l,\ t \leq \delta - 1 \tag{4.21}$$

Segue que o conjunto de soluções de interesse do sistema (3.10)–(3.11) 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.

[6] $l_j, t_j \in \{0, 1, 2, \cdots, \delta - 1\}$.

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 4.1.

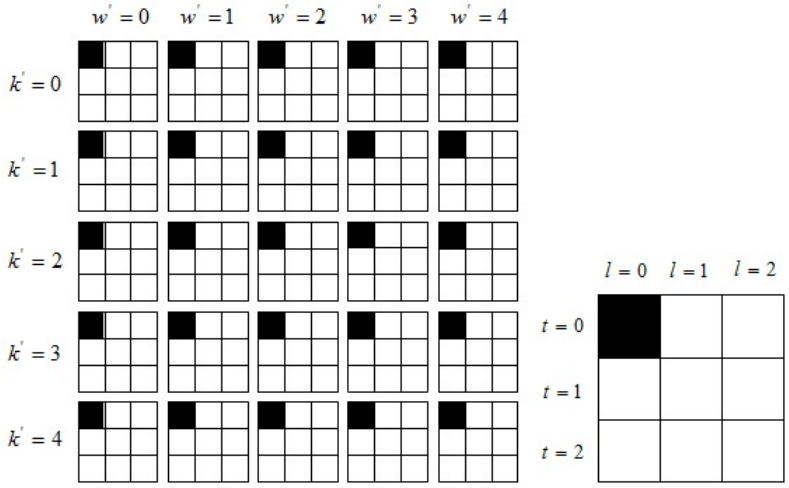
Seja o quadrado de ordem $n = 15$ construído pelo método do passo uniforme com os seguintes parâmetros: $\alpha = 2$, $\beta = 1$, $a = 11$ e $b = 4$. Observe que determinante $\begin{vmatrix} \alpha & a \\ \beta & b \end{vmatrix} = -3$ e $\text{mdc}(n, \alpha b - \beta a) = \delta = 3$. Assim, teremos $\left(\frac{n}{\delta}\right)^2 = \left(\frac{15}{3}\right)^2 = 25$ matrizes $M(w', k'), 3 \times 3$, (Figura 5(a), página 23), cada uma com $\delta^2 = 3^2 = 9$ elementos, Figura 5(b), na página 23.

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

$$133 = 1 + w + 15 \cdot k \Leftrightarrow k = 8 \text{ e } w = 12$$
$$k' \equiv k \left(\text{mod } \frac{n}{\delta}\right) \quad \Rightarrow \quad k' \equiv 8 \equiv 3 \pmod 5$$
$$w' \equiv w \left(\text{mod } \frac{n}{\delta}\right) \quad \Rightarrow \quad w' \equiv 12 \equiv 2 \pmod 5$$

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

Figura 4: Estrutura das matrizes do exemplo 4.1.



(a) 25 matrizes $M(w', k')$, 3×3 (b) $M(w', k')$, 3×3

Fonte: O autor, 2014.

4.1 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 (2.1). 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:

$$A \equiv p + \alpha w' + a \cdot k' + l \cdot \frac{\alpha n}{\delta} + t \cdot \frac{an}{\delta} \pmod{n} \tag{4.22}$$

Analogamente, segue de (2.2) que a coordenada B de x é dada por

$$B \equiv q + \beta w' + b \cdot k' + l \cdot \frac{\beta n}{\delta} + t \cdot \frac{bn}{\delta} \pmod{n} \tag{4.23}$$

Exemplo 4.2.

Seja o quadrado de ordem $n = 15$ construído pelo método do passo uniforme com os seguintes parâmetros: $\alpha = 2$, $\beta = 1$, $a = 11$ e $b = 4$. 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 10 mostra os resultados obtidos quando usamos (4.22) e (4.23). 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 (3.10)–(3.11) podem não ocupar a mesma célula.

Com relação à afirmação de Lehmer: *"que dois valores de x que diferem de* $\frac{n^2}{\delta}$ *vão ocupar a mesma célula"*, a Figura 10, 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.

Figura 5: $M(2, 3)$ do Ex. 4.4.

	$l = 0$	$l = 1$	$l = 2$
$t = 0$	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.

4.2 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 (4.22) e (4.23) podem ser reescritas:

$$A \equiv A' + l \cdot \frac{\alpha n}{\delta} + t \cdot \frac{an}{\delta} \pmod{n} \tag{4.24}$$

$$B \equiv B' + l \cdot \frac{\beta n}{\delta} + t \cdot \frac{bn}{\delta} \pmod{n} \tag{4.25}$$

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 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 7(a) e 7(c).

Sejam (A, B) as coordenadas do elemento x localizado na t^{a} linha e l^{a} coluna de $M(w', k')$. A coordenada $A_{w'\pm1,k'}$ de um elemento na mesma posição, mas localizado em 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 7(b)

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:

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

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

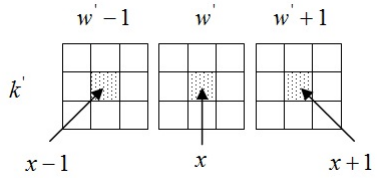
$$A_{w',k'\pm1} \equiv A \pm a \pmod{n}$$

Analogamente

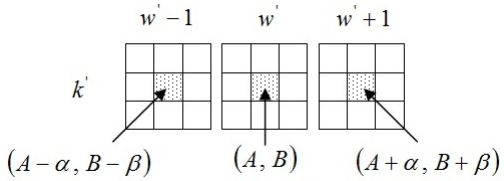
$$B_{w',k'\pm1} \equiv B \pm b \pmod{n}$$

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 7(d).

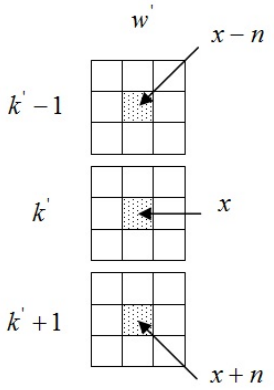
Figura 6: Regularidades.



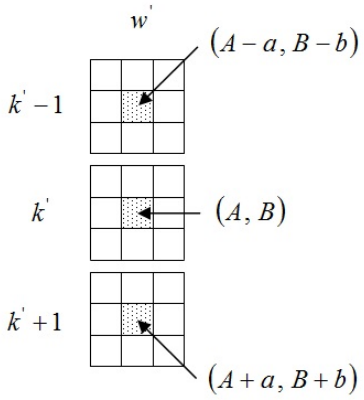
(a) Elementos de mesma posição, em matrizes vizinhas, à esquerda e à direita



(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.

Observação 4.1 (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.*

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

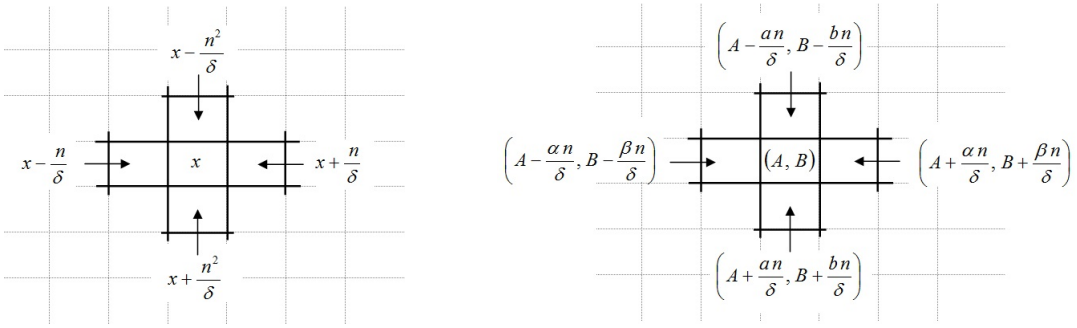
4.5 Regularidade das coordenadas A e B ao longo de uma coluna de $M(w', k')$

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 8(a) e 8(b) mostram os vizinhos de um elemento genérico, x, em uma $M(w', k')$, assim como suas respectivas coordenadas.

Figura 7: Regularidades.



(a) Elementos vizinhos de x (b) Coordenadas vizinhas de (A, B)

Fonte: O autor, 2014.

Até este ponto, vimos que as soluções de interesse do sistema (3.10)–(3.11) 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 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 4.3.

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. Temos

$$\begin{vmatrix} \alpha & a \\ \beta & b \end{vmatrix} = \alpha b - \beta a = 4 \cdot 2 - 5 \cdot 1 = 3$$

e $\delta = \text{mdc}(15, 3) = 3$.

Vamos identificar em qual matriz $M(w', k')$ está 102.

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

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:

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

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}:

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

$B_{01} \equiv (q + 7) + 10 \equiv q + 2 \pmod{15}$

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}:

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

$B_{02} \equiv (q + 2) + 10 \equiv q + 12 \pmod{15}$

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}:

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

$$B_{10} \equiv (q + 7) + 10 \equiv q + 2 \pmod{15}$$

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 8.

Figura 8: Elementos e suas coordenadas, da matriz $M(1, 1)$, do Exemplo 4.3.

	$l = 0$	$l = 1$	$l = 2$
$t = 0$	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.

4.6 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 (4.24) e (4.25)

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

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

$$\begin{cases} \alpha(l_1 - l_2) \equiv a(t_2 - t_1) \pmod{\delta} & (4.26) \\ \beta(l_1 - l_2) \equiv b(t_2 - t_1) \pmod{\delta} & (4.27) \end{cases}$$

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 [2], 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 numa mesma célula (A, B). Vamos analisar o sistema (4.26)-(4.27) 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 (4.26)–(4.27) é equivalente a

$$\begin{cases} \alpha(l_1 - l_2) \equiv a(t_2 - t_1) \pmod{\delta} & (4.28) \\ (\alpha b - \beta a)(t_2 - t_1) \equiv 0 \pmod{\delta} & (4.29) \end{cases}$$

Observe que quaisquer inteiros t_1, t_2 satisfazem a (4.29). Consequentemente, basta resolver (4.28).

Considere (4.28). 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 $l_1 \equiv l_2 \pmod{\delta}$

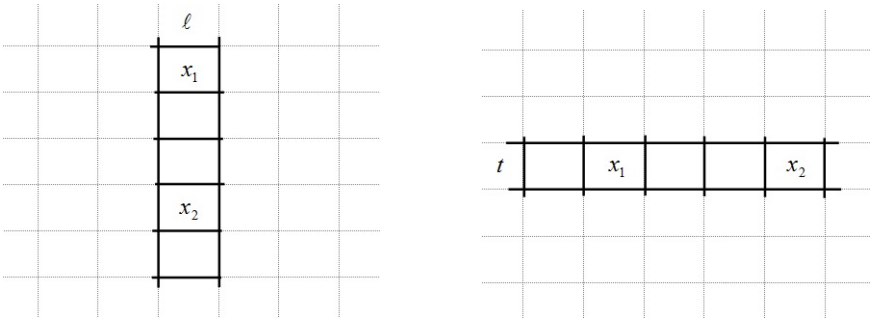
(mas $0 \leq l \leq \delta - 1$)

então $l_1 = l_2$

Portanto, podemos enunciar o seguinte:

Teorema 4.1. *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 9(a). 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 2. 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.



(a) x_1 e x_2 em uma mesma coluna de $M(w', k')$ tem coordenadas diferentes.

(b) x_1 e x_2 em uma mesma linha de $M(w', k')$ tem coordenadas diferentes.

Figura 9: Coordenadas de x_1 e x_2
Fonte: O autor, 2014.

Substituindo os coeficientes de (4.28) pelos restos na divisão por δ, obtemos um sistema equivalente a (4.28)–(4.29)

$$\begin{cases} \alpha'(l_1 - l_2) + a'(t_1 - t_2) \equiv 0 \pmod{\delta} & (4.30) \\ (\alpha b - \beta a)(t_2 - t_1) \equiv 0 \pmod{\delta} & (4.31) \end{cases}$$

Note que a hipótese de primalidade nos diz que $\alpha' \neq 0$ e $a' \neq 0$. A equação de congruência linear com duas variáveis (4.30), tem solução, pois, $\text{mdc}(\alpha', a', \delta) = 1 \mid 0$. Mais ainda, a equação (4.30) tem $\text{mdc}(\alpha', a', \delta) \cdot \delta^{2-1} = 1 \cdot \delta = \delta$ soluções (veja Theorem 36, Sivaramakrishnan [3, p. 124]).

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

$$l_1 - l_2 \equiv \frac{a'}{(\alpha, a)} \cdot k \pmod{\delta} \quad \text{e} \quad t_1 - t_2 \equiv \delta - \frac{\alpha'}{(\alpha, a)} \cdot k \pmod{\delta} \tag{4.32}$$

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

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

Além disso, se l_1, t_1, l_2 e t_2 satisfazem (4.32), 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, (4.32) 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 4.4.

Seja o quadrado de ordem $n = 15$ construído pelo método do passo uniforme com os seguintes parâmetros: $\alpha = 2$, $\beta = 1$, $a = 11$ e $b = 4$. Vamos usar (4.21), (2.1) e (2.2) para calcular as coordenadas (A, B), de cada elemento da matriz $M(2, 3)$. A Figura 10 mostra os resultados obtidos. 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 $(p + 12, q + 9)$. Com relação à afirmação de Lehmer, a Figura 10, 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.

	$l = 0$	$l = 1$	$l = 2$
$t = 0$	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 $(p+2, q+4)$

Figura 10: Coordenadas dos elementos de $M(2, 3)$
Fonte: dados da pesquisa

5 Considerações finais

Vimos que 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. Vimos também que o método do passo

uniforme, com parâmetros α, β, a e b, primos um a um com n, porém com o determinante $\alpha b - \beta a$ tendo um divisor comum, δ, com n, 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. A arapuca que fez Lehmer tropeçar, se dá, justamente, na passagem do sistema (3.6)-(3.7) para (3.8)-(3.9). Ele exibiu dois números que satisfazem (3.8)-(3.9) e, ao afirmar que eles ocupariam a mesma célula, ele admitiu que eles também satisfariam (3.6)-(3.7). Mas isso nem sempre se verifica para quaisquer dois números que satisfazem (3.8)-(3.9). Mais precisamente, se o mdc$(\alpha b - \beta a, n) = \delta$, com $\delta \neq 1$, o método não preenche o quadrado e não há equivalência entre os referidos os sistemas (3.6)-(3.7) e (3.8)-(3.9). Sempre haverá em (3.8)-(3.9) soluções que não satisfazem (3.6)-(3.7). Mostramos que sob a hipótese de primalidade dos parâmetros α, β, a, b com n, várias regularidades estão associadas ao não preenchimento de um quadrado de ordem n pelo método do passo uniforme.

Referências

[1] HEFEZ, A. Elementos de Aritmética. Coleção Textos Universitários. SBM, 2005

[2] LEHMER, D.N. On the congruences connected with certain magic squares, Trans. Amer. Math. Soc. 31 (1929), no. 3, 529–551.

[3] SIVARAMAKRISHNAN, R. Certain number-theoretic episodes in algebra, Chapman & Hall/CRC, 2007.