



Ciência e Natura

ISSN: 0100-8307

cienciaenaturarevista@gmail.com

Universidade Federal de Santa Maria  
Brasil

Travassos Ichihara, José; Nunes da Silva, Patricia; Cardoso Pires de Abreu, Renata  
Quadrados mágicos: quando o método falha  
Ciência e Natura, vol. 37, núm. 3, 2015, pp. 419-425  
Universidade Federal de Santa Maria  
Santa Maria, Brasil

Disponível em: <http://www.redalyc.org/articulo.oa?id=467547643035>

- Como citar este artigo
- Número completo
- Mais artigos
- Home da revista no Redalyc

redalyc.org

Sistema de Informação Científica  
Rede de Revistas Científicas da América Latina, Caribe, Espanha e Portugal  
Projeto acadêmico sem fins lucrativos desenvolvido no âmbito da iniciativa Acesso Aberto

## Quadrados mágicos: quando o método falha

### Magic squares: when the method fails

José Travassos Ichihara<sup>1</sup>, Patricia Nunes da Silva<sup>2</sup> e Renata Cardoso Pires de Abreu<sup>3</sup>

<sup>1</sup> Universidade do Estado do Rio de Janeiro, PROFMAT/UERJ - RJ, Brasil

joseichihara@hotmail.com

<sup>2</sup> Doutorado em Matemática Aplicada, Professora Associada da Universidade do Estado do Rio de Janeiro, Brasil  
nunes@ime.uerj.br

<sup>3</sup> Mestrado em Ciências Computacionais, Professora de Matemática (Aposentada) da Escola Municipal Presidente Arthur da Costa e Silva, Brasil  
rcpabreu@gmail.com

#### Resumo

Nesse artigo, discutimos o comportamento das soluções de um sistema linear de congruência 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 (1929). Sua análise foi dividida em várias etapas. Na primeira delas, envolvendo a discussão de condições necessárias e suficientes para o preenchimento do quadrado pelo método, Lehmer afirma que se dois números guardam entre si uma certa relação, eles serão designados a ocupar a mesma célula do quadrado causando seu não preenchimento. Concluímos que tais números nunca ocupam a mesma célula. Ou seja, o que Lehmer afirma não é verdade.

**Palavras-chave:** Quadrados mágicos, Congruências, Método do passo uniforme.

#### Abstract

In this article, we discuss the behavior of the solutions of a system of linear congruences related to the uniform step method. This is a method for constructing magic squares of odd order proposed and mathematically analyzed by Lehmer (1929). His analysis has several steps. In the first, involving the discussion of necessary and sufficient conditions for filling the square, Lehmer says that if two numbers keep a certain relationship to each other, they will be designated to occupy the same cell of the square. We conclude here that numbers that fulfill the mentioned relationship never occupy the same cell. In other words, what Lehmer says is not true.

**Keywords:** Magic squares, Congruences, Uniform step method.

## 1 Introdução

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. Como a soma de todos os elementos da matriz é a soma dos  $n^2$  primeiros termos de uma progressão aritmética com termo inicial  $a_1 = 1$  e razão  $r = 1$ , a soma dos elementos de qualquer coluna ou linha será igual a  $\frac{(1+n^2)n}{2}$  quando o quadrado for mágico.

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 foi analisado matematicamente por Lehmer (1929). Ele consiste em atribuir, um de cada vez, ordenadamente, a sequência dos números  $1, 2, 3, \dots, n^2$  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. O método do passo uniforme apenas pode ser usado para gerar quadrados mágicos de ordem ímpar, uma vez que se a ordem é par necessariamente pelo menos uma das condições necessárias e suficientes para preenchimento, obtenção de colunas mágicas ou obtenção de linhas mágicas é violada (para mais detalhes, ver Lehmer (1929)). No entanto, na discussão do preenchimento do quadrado pelo método, essa restrição não se faz necessária.

Ao analisar o preenchimento do quadrado, Lehmer nos instigou a investigar o não preenchimento. Na literatura, encontramos recorrentemente a descrição do método de La Loubère que é um caso particular do método do passo uniforme (ver, por exemplo, Ball (2004) e Pickover (2002)). Um tratamento através de reticulados desse método pode ser encontrado em Kraitichik (2006). Em Apostol e Zuckerman (1951), os autores generalizam o método do passo uniforme em circunstâncias especiais em que certas hipóteses de primalidade são violadas.

## 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, conforme Figura 1. Assim temos a seguinte disposição:

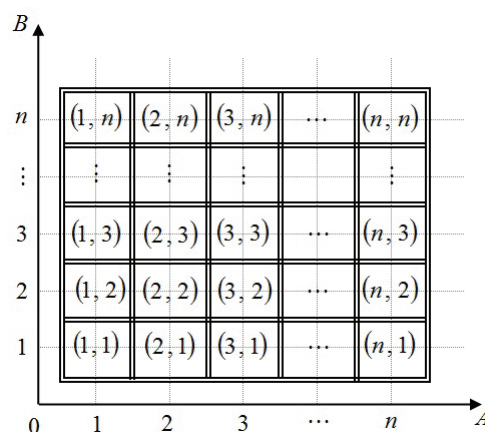


Figura 1: Coordenadas das células

Fonte: dados da pesquisa

No método do passo uniforme, inicia-se com o número 1 sendo atribuído a uma célula qualquer  $(p, q)$ . Em seguida, vem o número 2, colocado na célula  $(p + \alpha, q + \beta)$  sendo  $\alpha$  o deslocamento ou “passo” para a direita e  $\beta$  o passo para cima e assim por diante. Esses passos serão mantidos, por isso,  $\alpha$  e  $\beta$  são chamados de *constantes do passo uniforme*. Os sucessivos passos dados para a direita e para cima poderiam nos levar para “fora” da matriz. 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. No próximo exemplo, veremos claramente o papel de cada um dos parâmetros  $\alpha, \beta, a$  e  $b$ .

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

Partindo ordenadamente do número 1, cada grupo de  $n$  números será considerado um ciclo. A primeira quebra de passo será requerida, ao término do 1º ciclo, na inserção do número 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 número 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, conforme Figura 2(b). Esse procedimento se repete para o 3º ciclo, conforme Figura 2(c) e prossegue com o 4º e 5º ciclos até que todos os 25 números tenham sido distribuídos, conforme Figura 2(d).

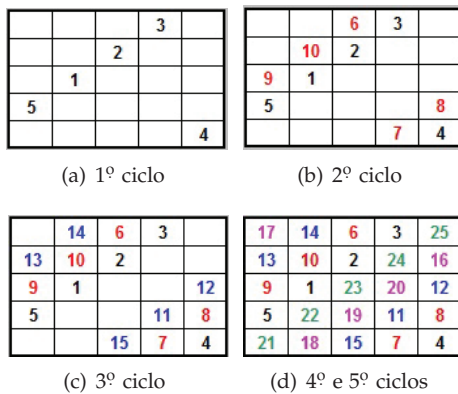


Figura 2: Inserção de 1 a 25 pelo MPU  
Fonte: dados da pesquisa

## 2.1 Congruências associadas

O processo descrito no exemplo foi resumido em duas congruências fundamentais para determinar as coordenadas  $(A, B)$  da célula na qual cada número  $x \in \{1, \dots, n^2\}$  deve ser alocado:

$$A \equiv p + \alpha(x - 1) + a \left\lfloor \frac{x-1}{n} \right\rfloor \pmod{n} \quad (1)$$

$$B \equiv q + \beta(x - 1) + b \left\lfloor \frac{x-1}{n} \right\rfloor \pmod{n} \quad (2)$$

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

No método do passo uniforme, o coeficiente  $(x - 1)$  de  $\alpha$  e  $\beta$  é um contador da quantidade de passos. O

coeficiente  $\left\lfloor \frac{x-1}{n} \right\rfloor$  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 aos coeficientes de  $a$  e  $b$  os quais se mantêm constantes durante os ciclos.

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

$$x = 1 + w + kn \quad (3)$$

com  $w$  e  $n$  inteiros não negativos, satisfazendo  $0 \leq w, k \leq n - 1$ . Mais precisamente,  $k$  é a parte inteira do quociente da divisão de  $x - 1$  por  $n$ ,

$$k = \left\lfloor \frac{x-1}{n} \right\rfloor \quad (4)$$

e,  $w$  é o resto dessa divisão,

$$w \equiv x - 1 \pmod{n}. \quad (5)$$

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 um resultado para preenchimento do quadrado pelo método do passo uniforme e discutimos aspectos de sua prova.

**Teorema 1** (Lehmer (1929), p. 530). *Dados  $\alpha, \beta, a$  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  $(A, B)$ . Esse fato é explorado na prova do teorema.

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

$$\begin{cases} \alpha(x_1 - x_2) + a \left( \left\lfloor \frac{x_1-1}{n} \right\rfloor - \left\lfloor \frac{x_2-1}{n} \right\rfloor \right) \equiv 0 \pmod{n} \\ \beta(x_1 - x_2) + b \left( \left\lfloor \frac{x_1-1}{n} \right\rfloor - \left\lfloor \frac{x_2-1}{n} \right\rfloor \right) \equiv 0 \pmod{n} \end{cases} \quad (6)$$

Utilizando propriedades de congruência (veja Proposições 9.1.4 e 9.1.5 em Hefez (2006), pp. 113–114) em (6), foi deduzido o sistema de congruências lineares (7), associado à condição de dois números  $x_1$  e  $x_2$  ocuparem a mesma célula, pelo método do passo uniforme.

$$\begin{cases} \Delta(x_1 - x_2) \equiv 0 & (\text{mod } n) \\ \Delta\left\{\left[\frac{x_1-1}{n}\right] - \left[\frac{x_2-1}{n}\right]\right\} \equiv 0 & (\text{mod } n) \end{cases} \quad (7)$$

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”. A prova foi feita pela contrapositiva. Essencialmente, foram exibidos dois números  $x_1$  e  $x_2$  que satisfazem (7) e que ocupam a mesma célula, isto é, que também satisfazem (6).

A prova da necessidade da condição de primalidade de  $\alpha b - \beta a$  e  $n$  partiu do sistema (7) e se estruturou como indicado a seguir.

Se o  $\text{mdc}(\alpha b - \beta a, n) = \delta$  ( $\delta \neq 1$ ), então

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

e  $x_1 \equiv x_2 \pmod{\frac{n}{\delta}}$ . 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

$$\left[\frac{x_1-1}{n}\right] \equiv \left[\frac{x_1-1}{n} + \frac{n}{\delta}\right] \pmod{\frac{n}{\delta}}.$$

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 célula e o quadrado não será preenchido. (Lehmer, 1929, p. 531).

Sob a hipótese de que os parâmetros  $\alpha$ ,  $\beta$ ,  $a$ ,  $b$  do método do passo uniforme sejam todos primos com  $n$  e ainda que o  $\text{mdc}(\alpha b - \beta a, n) = \delta \neq 1$ , foram exibidos dois números  $x_1$  e  $x_2$ , tais que  $x_2 - x_1 = \frac{n^2}{\delta}$ , que satisfazem ao sistema equivalente a (7) (A Proposição 9.1.5 Hefez (2006), p. 114, garante a equivalência dos sistemas (7) e (8))

$$\begin{cases} x_1 \equiv x_2 & (\text{mod } \frac{n}{\delta}) \\ \left[\frac{x_1-1}{n}\right] \equiv \left[\frac{x_2-1}{n}\right] & (\text{mod } \frac{n}{\delta}) \end{cases} \quad (8)$$

e afirmou-se que vão cair na mesma célula e por isto o quadrado não seria preenchido.

Essa afirmação é equivocada. Veremos mais adiante que se  $x_1$  e  $x_2$  são tais que  $x_1 - x_2 = \frac{n^2}{\delta}$ , eles não satisfazem ao sistema (6). Isto é, é possível haver dois números  $x_1$  e  $x_2$  que satisfaçam as congruências do sistema (8)

mas não ocupem a mesma célula do quadrado. Ao identificarmos o equívoco de Lehmer, fomos instigados a entender como se configura o não preenchimento pelo método do passo uniforme.

O fato de Lehmer ter pensado que soluções não triviais de (7) são também soluções de (6), ou seja, ocupam a mesma célula, nos levou a fazer uma análise da relação entre esses sistemas.

### 3.1 Entendendo o sistema (8)

Para compreender o equívoco de Lehmer, é necessário analisar cuidadosamente o sistema (8).

Por (4), a segunda equação do sistema (8) pode ser reescrita:

$$k_1 \equiv k_2 \pmod{\frac{n}{\delta}}$$

De acordo com (3), a primeira equação do sistema (8) pode ser escrita:

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

O sistema (8) pode, então, ser reescrito:

$$\begin{cases} w_1 \equiv w_2 & (\text{mod } \frac{n}{\delta}) \\ k_1 \equiv k_2 & (\text{mod } \frac{n}{\delta}) \end{cases} \quad (9)$$

Seja  $S_I$  o subconjunto de  $\{1, \dots, n^2\}$  tal que para todo  $x_1, x_2 \in S_I$ , tenhamos  $x_1, x_2$  é solução de (8).

Como queremos investigar números  $x_1, x_2 \in \{1, 2, \dots, n^2\}$  que ocupam a mesma célula no quadrado, estamos interessados em determinar os elementos  $x_j$  de  $S_I$ . Por (3), podemos representá-los na forma

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

Vamos nos referir a tais elementos como *soluções de interesse* do sistema (8). A cada solução de interesse  $x_j$  do sistema (8), podemos associar uma solução de interesse  $(w_j, k_j)$  do sistema (9). A coordenada  $w_j$  será chamada de de solução de interesse da primeira equação do sistema (9) e  $k_j$ , de solução de interesse da segunda equação do sistema (9). Obviamente, duas soluções de interesse  $w_1$  e  $w_2$  da primeira equação do sistema (9) deixam o mesmo resto  $w'$  na divisão por  $\frac{n}{\delta}$ . De um modo geral, duas soluções de interesse  $w_1$  e  $w_2$  da primeira equação do sistema (9) são dadas por

$$w_j = w' + l_j \cdot \frac{n}{\delta}, \quad j = 1, 2, \quad (10)$$

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  $k_2$  da segunda equação do sistema (9) são dadas por

$$k_j = k' + t_j \cdot \frac{n}{\delta}, \quad j = 1, 2, \quad (11)$$

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 (8) podem ser agrupadas em função dos pares  $(w', k')$ . Para cada  $w'$  e  $k'$  pertencentes ao conjunto de resíduos módulo  $\frac{n}{\delta}$ . Isto é,  $w', k' \in \{0, 1, 2, \dots, \frac{n}{\delta} - 1\}$ . As expressões (10) e (11) nos mostram que há  $\delta^2$  soluções de interesse  $(w_j, k_j)$  do sistema (9). Além disso, sendo  $x_1$  e  $x_2$  duas soluções do sistema (8), por (10) e (11), temos

$$x_j = 1 + w' + k'n + l_j \cdot \frac{n}{\delta} + t_j \cdot \frac{n^2}{\delta}, \quad j = 1, 2. \quad (12)$$

para algum  $l_j$  e  $t_j$  pertencentes ao conjunto de resíduos módulo  $\delta$ . Isto é,  $l_j, t_j \in \{0, 1, 2, \dots, \delta - 1\}$ .

### 3.2 Como ocorre o não preenchimento?

Sejam um par  $(w', k')$ , com  $0 \leq w', k' \leq \frac{n}{\delta} - 1$  e

$$x' = 1 + w' + k'n.$$

Por (12), as soluções de interesse do sistema (8) podem ser dispostas em  $\delta$  linhas e  $\delta$  colunas (Tabela 1).

Observamos que todos os números de uma tabela tem o mesmo  $w'$  e o mesmo  $k'$ . O que distingue dois quaisquer são os valores de  $l$  e  $t$  variando de 0 até  $\delta - 1$ . Sendo assim, os valores de  $w'$  e de  $k'$  determinam uma tabela de  $\delta^2$  números. Vamos nos referir a esse conjunto, naturalmente, como matriz  $M(w', k')$ . Mais precisamente, para  $0 \leq w', k' \leq \frac{n}{\delta} - 1$ , temos  $M(w', k') = (m_{t+1, l+1})$ , com

$$m_{t+1, l+1} = x_{tl} = x' + l \cdot \frac{n}{\delta} + t \cdot \frac{n^2}{\delta}, \quad 0 \leq l, t \leq \delta - 1 \quad (13)$$

Segue que o conjunto de todas as soluções de interesse do sistema (8) será constituído por  $(\frac{n}{\delta})^2$  matrizes, cada uma definida por um par  $(w', k')$ ,  $0 \leq w', k' \leq \frac{n}{\delta} - 1$ , tendo cada uma  $\delta^2$  números.

Observe que são os números de uma  $M(w', k')$  que vão ocupar uma mesma célula do quadrado, ocasionando, o não preenchimento do quadrado. De fato, para que  $x_1$  e  $x_2$  ocupem a mesma célula, é necessário que satisfaçam ao sistema de equações (6). Consequentemente, por (12), eles pertencem a uma mesma matriz  $M(w', k')$ . Por outro lado, usando resultados sobre existência de solução de equações de congruência linear (ver Teorema 36, Sivaramakrishnan (2006), p. 124), é possível mostrar que os  $\delta^2$  elementos de  $M(w', k')$  vão cair em  $\delta$  células do quadrado. Além disso, cada célula será ocupada por  $\delta$

elementos. Ademais, elementos pertencentes a matrizes  $M(w', k')$  distintas não caem na mesma célula.

#### 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  $b = 4$ . Logo,  $\text{mdc}(n, \alpha b - \beta a) = \delta = 3$ . Assim, teremos  $(\frac{n}{\delta})^2 = (\frac{15}{3})^2 = 25$  matrizes  $M(w', k')$ ,  $3 \times 3$ , (Figura 3(a)), cada uma com  $\delta^2 = 3^2 = 9$  elementos (Figura 3(b)).

	$w' = 0$	$w' = 1$	$w' = 2$	$w' = 3$	$w' = 4$
$k' = 0$					
$k' = 1$					
$k' = 2$					
$k' = 3$					
$k' = 4$					

(a) 25 matrizes  $M(w', k')$ ,  $3 \times 3$

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

(b)  $M(w', k')$ ,  $3 \times 3$

Figura 3: Estrutura das matrizes  
Fonte: dados da pesquisa

#### A qual $M(w', k')$ pertence o número 133?

Observe que

$$133 = 1 + w + 15 \cdot k, \text{ com } k = 8 \text{ e } w = 12.$$

Portanto, por (10) e (11), temos

$$k' = 3 \equiv k \pmod{\frac{n}{\delta}} \quad \text{e} \quad w' = 2 \equiv w \pmod{\frac{n}{\delta}}$$

Desta forma, o número 133 pertence a  $M(2, 3)$ .

Quais serão os outros elementos da matriz  $M(2, 3)$ ?

Tabela 1: Soluções de interesse dispostas em  $\delta$  linhas e  $\delta$  colunas  
Fonte: dados da pesquisa

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

Como  $x' = 1 + w' + k'n = 48$ , os demais elementos de  $M(2,3)$  são da forma

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

Nas tabelas abaixo, exibimos os elementos de  $M(2,3)$  que foram obtidos através da expressão acima para  $x_{tl}$ .

	$l = 0$	$l = 1$	$l = 2$
$t = 0$	$x_{00}$	$x_{01}$	$x_{02}$
$t = 1$	$x_{10}$	$x_{11}$	$x_{12}$
$t = 2$	$x_{20}$	$x_{21}$	$x_{22}$

(a) Estrutura de  $M(2,3)$

	$l = 0$	$l = 1$	$l = 2$
$t = 0$	48	53	58
$t = 1$	123	128	133
$t = 2$	198	203	208

(b)  $M(2,3)$

Figura 4: Elementos de  $M(2,3)$   
Fonte: dados da pesquisa

## 4 A afirmação de Lehmer

Lehmer afirmou que “dois valores de  $x$  que difiram por  $\frac{n^2}{\delta}$  serão alocados pelo passo uniforme na mesma célula e o quadrado não será preenchido.” (Lehmer, 1929,

p. 531). Como  $0 \leq t_j, l_j \leq \delta - 1$  ( $j = 1, 2$ ), por (12), duas soluções de interesse  $x_1$  e  $x_2$  do sistema que difiram por  $\frac{n^2}{\delta}$ , são necessariamente da forma

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

Além disso, sem perda de generalidade, podemos admitir que  $t_2 - t_1 = 1$ . Substituindo os valores de  $x_1$  e  $x_2$  em (6), obtemos

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

Evidentemente falso, sob as hipóteses  $\delta \neq 1$ ,  $a$  e  $b$  primos com  $n$ .

### 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  $b = 4$ . Vamos usar (13), (1) e (2) para calcular as coordenadas  $(A, B)$ , de cada elemento da matriz  $M(2,3)$ . A Figura 5 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 5, 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 5: Coordenadas dos elementos de  $M(2, 3)$   
Fonte: dados da pesquisa

Esse exemplo ilustra a não-equivalência entre os sistemas de congruências (6) e (7). Ainda que toda solução do sistema (6) seja também solução do sistema (7), há solução do sistema (7) que não é solução do sistema (6).

## 5 Considerações finais

A arapuca que fez Lehmer tropeçar, se dá, justamente, na passagem do sistema de equações (6) para o sistema de equações (7). Ele exibiu dois números que satisfazem (7) e, ao afirmar que eles ocupariam a mesma célula, ele admitiu que eles também satisfariam (6). Mas isso nem sempre se verifica para quaisquer dois números que satisfazem (7). Mais precisamente, se o  $\text{mdc}(\alpha b - \beta a, n) = \delta$ , com  $\delta \neq 1$ , o método não preenche o quadrado e não há equivalência entre os referidos os sistemas (6) e (7). Sempre haverá em (7) soluções que não satisfazem (6). Sob a hipótese de primalidade dos parâmetros  $\alpha, \beta, a, b$  com  $n$ , várias regularidades estão associadas ao não preenchimento de um quadrado de ordem  $n$  pelo método do passo uniforme. Vimos aqui que os números que ocupam uma mesma célula estão distribuídos em  $(\frac{n}{\delta})^2$  matrizes constituídas de  $\delta$  linhas e  $\delta$  colunas.

## Referências

- Apostol, T. M., Zuckerman, H. S. (1951). On magic squares constructed by the uniform step method. Proc Amer Math Soc, 2(4), 557–565.
- Ball, W. (2004). Mathematical Recreations And Essays. Kessinger Publishing.
- Hefez, A. (2006). Elementos de aritmética. Textos Universitários, SBM, Rio de Janeiro.
- Kraitchik, M. (2006). Mathematical Recreations. Dover Recreational Math Series, Dover Pub..
- Lehmer, D. N. (1929). On the congruences connected with certain magic squares. Transactions of the American Mathematical Society, 31, 529–551.

Pickover, C. (2002). The Zen of Magic Squares, Circles, and Stars: An Exhibition of Surprising Structures Across Dimensions. Princeton University Press.

Sivaramakrishnan, R. (2006). Certain Number-Theoretic Episodes In Algebra. Chapman & Hall/CRC Pure and Applied Mathematics, Taylor & Francis, Hoboken, NJ.