Journal de Théorie des Nombres
de Bordeaux **8** *(1996), 243–249*

Le semi-groupe libre des carrés magiques

par Lionel COZAR

Résumé. Nous étudions une loi de composition sur les carrés magiques, qui a déjà été introduite dans la litterature, qui munit l'ensemble de tous les carrés magiques d'une structure de semi-groupe (monoïde). Nous prouvons ensuite une conjecture de Adler et Li, ce semi-groupe est libre.

Abstract. We study a law of composition upon magic squares, already introduced in literature, that provides the set of all magic squares with a structure of semi-group. We then prove a conjecture of Adler and Li, this semi-group is free.

1. Introduction

Carré semi-magique :

Un carré semi-magique de coté n est une matrice $A = (a_{i,j})_{i,j \in \mathbb{Z}/n\mathbb{Z}}$ de $\mathcal{M}_n(\mathbb{N})$ telle que :

(i) $\{a_{i,j}\}_{i,j \in \mathbb{Z}/n\mathbb{Z}} = \{1, \cdots, n^2\} = [1, n^2]$,

(ii) $\forall i \in \mathbb{Z}/n\mathbb{Z} \displaystyle\sum_{j \in \mathbb{Z}/n\mathbb{Z}} a_{i,j} = \frac{n(n^2+1)}{2}$,

(iii) $\forall j \in \mathbb{Z}/n\mathbb{Z} \displaystyle\sum_{i \in \mathbb{Z}/n\mathbb{Z}} a_{i,j} = \frac{n(n^2+1)}{2}$.

On peut aussi dire que les éléments de $[1, n^2]$ apparaissent une fois et une seule dans A et que la somme des éléments de chaque ligne et de chaque colonne est la même, soit nécessairement $\dfrac{n(n^2+1)}{2} = \dfrac{1}{n}(\displaystyle\sum_{k=1}^{n^2} k)$.

Manuscrit reçu le 15 janvier 1995

Carré magique:

Si, de plus, cette matrice vérifie les deux relations supplémentaires suivantes :

$$\text{(iv)} \sum_{i\in\mathbb{Z}/n\mathbb{Z}} a_{i,i} = \frac{n(n^2+1)}{2} \quad \text{et} \sum_{i\in\mathbb{Z}/n\mathbb{Z}} a_{i,n+1-i} = \frac{n(n^2+1)}{2},$$

on dit qu'elle est un carré magique. Elle est caractérisée par le fait que chacune des sommes des éléments des deux diagonales principales est la même que la somme des lignes et des colonnes.

Carré panmagique :

Si, par rapport aux équations consenties par les carrés semi-magiques, une matrice vérifie aussi les suivantes :

$$\text{(v)}\ \forall k \in \mathbb{Z}/n\mathbb{Z} \sum_{i\in\mathbb{Z}/n\mathbb{Z}} a_{i,i+k} = \frac{n(n^2+1)}{2}\ ,$$

$$\text{(vi)}\ \forall k \in \mathbb{Z}/n\mathbb{Z} \sum_{i\in\mathbb{Z}/n\mathbb{Z}} a_{i,1+k-i} = \frac{n(n^2+1)}{2}\ ,$$

on dit alors que cette matrice est un carré panmagique, on voit que les carrés panmagiques sont magiques ($k = 0$). La manière de voir ces carrés panmagiques est de considérer le carré comme un tore (on recolle ensembles les deux parois verticales et les deux parois horizontales), et de remarquer ensuite que ces équations reviennent à dire que toutes les diagonales sur le tore ont la même somme que les lignes et les colonnes.

Trois ensembles :

Notons $\mathcal{S}_n$ (resp. $\mathcal{C}_n$ et $\mathcal{P}_n$) l'ensemble de tous les carrés semi-magiques (resp. magiques et panmagiques) de coté n et $\mathcal{S} = \bigsqcup_{n\in\mathbb{N}^*} \mathcal{S}_n$ (resp. $\mathcal{C} = \bigsqcup\limits_{n\in\mathbb{N}^*} \mathcal{C}_n$ et $\mathcal{P} = \bigsqcup\limits_{n\in\mathbb{N}^*} \mathcal{P}_n$) leur réunion disjointe suivant n.

A titre d'exemple :

$\mathcal{S}_1 = \{(1)\}$, $\mathcal{S}_2 = \emptyset$, $\mathrm{card}(\mathcal{S}_3) = 72$.

$\mathcal{C}_1 = \{(1)\}$, $\mathcal{C}_2 = \emptyset$, $\mathrm{card}(\mathcal{C}_3) = 8$ et $\mathrm{card}(\mathcal{C}_4) = 7040$.

$\mathcal{P}_1 = \{(1)\}$, $\mathcal{P}_2 = \emptyset$, $\mathcal{P}_3 = \emptyset$ et $\mathrm{card}(\mathcal{P}_4) = 384$.

On a toujours $\mathcal{P}_n \subset \mathcal{C}_n \subset \mathcal{S}_n$, d'où $\mathcal{P} \subset \mathcal{C} \subset \mathcal{S}$.

Structure de semi-groupes :

On va introduire une structure de semi-groupe sur les ensembles $\mathcal{S}, \mathcal{C}$ et $\mathcal{P}$; en effet, considérons la loi de composition suivante valable pour les trois ensembles :

$$\begin{aligned} \mathcal{S}_n \times \mathcal{S}_m &\longrightarrow \mathcal{S}_{nm} \\ (A, B) &\longrightarrow C = A \times B. \end{aligned}$$

Soit $(r, s) \in [1, nm]^2$ alors il existe d'uniques i, j, k, l tels que $1 \leq i, j \leq n$ et $1 \leq k, l \leq m$ avec $r = i + (k-1)n$ et $s = j + (l-1)n$, alors, on définit C par : $c_{r,s} = a_{i,j} + n^2(b_{k,l} - 1)$.

On vérifie facilement que ces expressions définissent bien un nouveau carré semi-magique et que le produit ainsi introduit est bien associatif (voir [1]) même si on dit le contraire dans [2]. On peut aussi contrôler que si les deux matrices à multiplier sont magiques (resp. panmagiques) alors le produit est comme attendu magique (resp. panmagique). Comme le carré de $\mathcal{S}_1 = \mathcal{C}_1 = \mathcal{P}_1 = (1)$ est élément neutre à droite et à gauche, $(\mathcal{S}, \times)$, $(\mathcal{C}, \times)$ et $(\mathcal{P}, \times)$ sont bien des semi-groupes. Ils sont bien évidemment non commutatifs.

Exemple :

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

$$\left(\begin{array}{cccccccccccc} 8 & 1 & 6 & 134 & 127 & 132 & 125 & 118 & 123 & 35 & 28 & 33 \\ 3 & 5 & 7 & 129 & 131 & 133 & 120 & 122 & 124 & 30 & 32 & 34 \\ 4 & 9 & 2 & 130 & 135 & 128 & 121 & 126 & 119 & 31 & 36 & 29 \\ 107 & 100 & 105 & 53 & 46 & 51 & 62 & 55 & 60 & 80 & 73 & 78 \\ 102 & 104 & 106 & 48 & 50 & 52 & 57 & 59 & 61 & 75 & 77 & 79 \\ 103 & 108 & 101 & 49 & 54 & 47 & 58 & 63 & 56 & 76 & 81 & 74 \\ 71 & 64 & 69 & 89 & 82 & 87 & 98 & 91 & 96 & 44 & 37 & 42 \\ 66 & 68 & 70 & 84 & 86 & 88 & 93 & 95 & 97 & 39 & 41 & 43 \\ 67 & 72 & 65 & 85 & 90 & 83 & 94 & 99 & 92 & 40 & 45 & 38 \\ 116 & 109 & 114 & 26 & 19 & 24 & 17 & 10 & 15 & 143 & 136 & 141 \\ 111 & 113 & 115 & 21 & 23 & 25 & 12 & 14 & 16 & 138 & 140 & 142 \\ 112 & 117 & 110 & 22 & 27 & 20 & 13 & 18 & 11 & 139 & 144 & 137 \end{array}\right)$$

D'autres exemples sont proposés dans [4].

Carrés premiers :

On appelle carré semi-magique (resp. magique et panmagique) premier un carré semi-magique (resp. magique et panmagique) qui ne peut pas s'écrire comme produit de deux carrés semi-magiques (resp. magiques et panmagiques) dont aucun n'est le carré unité (1). (1) n'est donc pas un carré premier.

Par exemple, soit p un nombre premier, tous les carrés semi-magiques (resp. magiques et panmagiques) de coté p ou $2p$ sont des carrés premiers, de plus, les carrés panmagiques de coté $3p$ sont aussi premiers.

Je me propose maintenant, considérant les structures et les définitions précédemment introduites, de démontrer le résultat suivant, qui a été conjecturé par Allan Adler et Shuo-Yen Robert Li dans [1] et récemment démontré par Allan Adler lui-même dans [5].

THÉORÈME. *Le semi-groupe des carrés semi-magiques (resp. magiques et panmagiques) $\mathcal{S}$ (resp. $\mathcal{C}$ et $\mathcal{P}$) est un semi-groupe libre de base les carrés semi-magiques (resp. magiques et panmagiques) premiers.*

2. Preuve du théorème principal

Interprétation par blocs et application :

On voit sur cet exemple, mais on pourrait le formaliser, que cette composition consiste à diviser la matrice C de taille $nm \times nm$ en m^2 blocs $n \times n$ et à placer dans le bloc (k, l) $(1 \leq k, l \leq m)$ la matrice $A + (b_{k,l} - 1)n^2$.

Avec l'interprétation par blocs de cette loi de composition, on montre très facilement que $(\mathcal{S}, \times)$ (resp. $(\mathcal{C}, \times)$ et $(\mathcal{P}, \times)$) est régulier à droite et à gauche ; c'est-à-dire, soient A, B, C des éléments de $\mathcal{S}$ (resp. $\mathcal{C}$ et $\mathcal{P}$) , alors :

$$A \times B = A \times C \Longleftrightarrow B = C$$
$$B \times A = C \times A \Longleftrightarrow B = C$$

Notons $|A|$ la taille d'un carré magique ; c'est-à-dire $|A| = n$ est équivalent à $A \in \mathcal{S}_n$.

PROPOSITION. *Soient A, B, C, D des carrés semi-magiques (resp. magiques et panmagiques), si $A \times B = C \times D$ avec $|A| \geq |C|$ alors il existe un unique X élément de $\mathcal{S}$ (resp. $\mathcal{C}$ et $\mathcal{P}$) tel que $A = C \times X$ et $D = X \times B$.*

Preuve : notons $E = A \times B = C \times D$, on peut voir E comme une matrice divisée en $|B|^2$ blocs $|A| \times |A|$ ou comme une matrice divisée en $|D|^2$ blocs $|C| \times |C|$.

Notons maintenant $n = |A|$ et $m = |C|$ et supposons que m ne divise pas n, alors n = qm+r est la division euclidienne de n par m avec $r \neq 0$. L'hypothèse de la proposition se traduit sur ces nouvelles notations par $n \geq m$.

Considérons dans la matrice E les 4 éléments suivants :

$$e_{n,n}, e_{n,n+1}, e_{n+1,n}, e_{n+1,n+1}.$$

Ils appartiennent à 4 blocs différents relativement au produit $A \times B$.

$$\begin{cases} e_{n,n} & = & a_{n,n} & + & (b_{1,1} - 1)n^2 \\ e_{n+1,n} & = & a_{1,n} & + & (b_{2,1} - 1)n^2 \\ e_{n,n+1} & = & a_{n,1} & + & (b_{1,2} - 1)n^2 \\ e_{n+1,n+1} & = & a_{1,1} & + & (b_{2,2} - 1)n^2 \end{cases}$$

Pourtant ils sont tous dans le même bloc relativement au produit $C \times D$, en effet, puisque $n = qm + r$, si on applique la définition de la matrice E relativement au produit $C \times D$, on a :

$$\begin{cases} e_{n,n} & = & c_{r,r} & + & (d_{q+1,q+1} - 1)m^2 \\ e_{n+1,n} & = & c_{r+1,r} & + & (d_{q+1,q+1} - 1)m^2 \\ e_{n,n+1} & = & c_{r,r+1} & + & (d_{q+1,q+1} - 1)m^2 \\ e_{n+1,n+1} & = & c_{r+1,r+1} & + & (d_{q+1,q+1} - 1)m^2 \end{cases}$$

Posons

$$x = \min(e_{n,n}; e_{n,n+1}; e_{n+1,n}; e_{n+1,n+1})$$
$$\text{et } y = \max(e_{n,n}; e_{n,n+1}; e_{n+1,n}; e_{n+1,n+1}),$$

alors, puisque ces 4 valeurs sont simultanément dans un même bloc de taille $m \times m$, et que ces 4 valeurs sont différentes, on a :

$$3 \leq y - x \leq m^2 - 1$$

Le premier système d'équations nous donne pourtant :

$y - x = \big(\max(b_{1,1}, b_{1,2}, b_{2,1}, b_{2,2}) - \min(b_{1,1}, b_{1,2}, b_{2,1}, b_{2,2})\big)n^2 + (a_{p,q} - a_{r,s})$ pour certaines valeurs p, q, r, s dans $\{1, n\}$, et comme $a_{p,q} - a_{r,s} \leq n^2 - 1$ et $\max(b_{1,1}, b_{1,2}, b_{2,1}, b_{2,2}) - \min(b_{1,1}, b_{1,2}, b_{2,1}, b_{2,2}) \geq 3$, on a :

$$y - x \geq 2n^2 + 1.$$

On aurait ainsi $2n^2 + 1 \leq m^2 - 1$ qui contredirait l'hypothèse de départ $n \geq m$. On en déduit donc que m divise n.

Il y a, d'après l'interprétation par blocs du produit, dans la matrice E un bloc de taille $n \times n$ où se trouve la matrice A elle-même. Comme E est aussi égal à $C \times D$ etque $|C|$ divide $|A|$, on trouve dans ce bloc de taille $n \times n$, donc dans la matrice A, le bloc C ainsi que $(n/m)^2 - 1$ de ses translatés, entendez des matrices de la forme $C + km^2$ avec $1 \leq k \leq (n/m)^2 - 1$.

On construit la matrice X de la manière suivante : on divise la matrice A en $(n/m)^2$ blocs de taille $m \times m$ et si dans un bloc (i, j) se trouve la matrice $C + km^2$, on pose $x_{i,j} = k$. Les propiétés de E et le fait que m divise n nous assure que cette définition est consistante, et l'interprétation par blocs du produit nous révèle que $A = C \times X$.

Le fait que A et C soient des carrés semi-magiques (resp. magiques et panmagiques) implique que X est aussi un carré semi-magique (resp. magique et panmagique).

Ainsi, $C \times X \times B = C \times D$, on peut donc simplifier par C et trouver : $D = X \times B$.

On a par conséquent prouvé l'existence du X désiré, son unicité découle de la régularité du produit.

Preuve du théorème : il suffit de voir que, pour tout carré, sa décomposition en carrés premiers est unique. L'existence de cette décomposition est tout d'abord évidente compte tenu de la définition des carrés premiers (on procède par récurrence sur le coté du carré).

Supposons maintenant :

$$A = P_1 \times \cdots \times P_n = Q_1 \times \cdots \times Q_m,$$

avec $P_1, \cdots, P_n, Q_1, \cdots, Q_n$ premiers.

On peut supposer $|P_1| \geq |Q_1|$, alors d'après la proposition précédente, il existe un carré X tel que $P_1 = X \times Q_1$, mais comme P_1 est premier et $Q_1 \neq (1)$, on obtient $X = (1)$ donc $P_1 = Q_1$.

On peut ainsi simplifier par P_1 et par une récurrence simple on déduit $n = m$ et pour tout i tel que $1 \leq i \leq n$ on a $P_i = Q_i$.

L'unicité de la décomposition est donc démontrée.

Bibliographie

[1] Adler Allan and Li, Shuo Yen Robert, *Magic cubes and Prouhet sequences*, Amer. Math. Monthly 84 **8** (1977), 618–627.

[2] Chee P.S., *Magic squares*, Menemui Mat. 5 **3** (1983), 111–121.

[3] Ku,Y.H. and Chen, Nan Xian, *Some theorems on construction of magic squares*, J. Franklin Inst. 322 **5-6** (1986), 253–266.

[4] Bouteloup Jacques, *Carrés magiques, carrés latins et eulériens* (1992), Editions du choix.

[5] Adler Allan, *Magic N-cubes form a free monoid*, à paraître dans European J. Combinatorics.

Lionel Cozar
Université Bordeaux I
351, cours de la Libération
33405 Talence Cedex