Comment une valeur propre de matrice peut permettre de distinguer les nombres premiers des nombres composés ? (Denise Vella-Chemla, 21.5.2023)

1. Exposition du problème

On revient à une matrice par blocs (idéalement infinie mais on va ici considérer des matrices de taille finie), notée M_k dans la suite, contenant sur sa diagonale des matrices circulantes de taille 2, 3, 4, ..., k. On avait eu l'idée de cette matrice en juillet 2019 pour "simuler le crible d'Ératosthène"[1]. On écrit M_5 ci-dessous pour illustrer.

$$M_5 = \begin{pmatrix} \boxed{\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}} & 0 & 0 & 0 \\ 0 & \boxed{\begin{matrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{matrix}} & 0 & 0 \\ 0 & 0 & \boxed{\begin{matrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{matrix}} & 0 \\ 0 & 0 & 0 & \boxed{\begin{matrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{matrix}} \end{pmatrix}$$

Dans la note de 2019, on avait utilisé cet opérateur (cette matrice) pour distinguer les nombres premiers des nombres composés par le fait suivant : si la trace de la puissance de matrice $\mathrm{Tr}(M^p)$ est égale à p, alors p est un nombre premier.

La matrice M_k est une matrice carrée de taille $n \times n$ avec $n = \dfrac{k(k+1)}{2} - 1$. Comme elle ne contient que des 0 et des 1 et que chaque ligne et chaque colonne ne contient qu'un seul 1, cette matrice est une matrice de permutation.

Les mini-matrices circulantes, sur la diagonale de M_k sont les matrices de permutation des groupes cycliques C_2, C_3, C_4, ..., C_k. Si on observe la diagonale de chacune de ces petites matrices, par exemple, la diagonale de la matrice 3×3, lorsqu'on l'élève à différentes puissances correspondant aux entiers successifs

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^4 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^5 = \ldots,$$

[1] Voir http://denise.vella.chemla.free.fr/enstransfotrace.pdf.

on comprend que suivant l'exposant de la matrice (la puissance à laquelle on l'élève), une fois sur 3, pour les $3k$, les 3 chiffres 1 se retrouveront sur la diagonale, et la puissance de la matrice en question aura pour trace 3. Cette cyclicité correspond au fait de "barrer un nombre sur 3" dans l'algorithme du crible d'Ératosthène pour trouver les nombres premiers.

Il en est de même pour la matrice "géante" contenant *toutes* les mini-matrices circulantes parce toutes les matrices autres que la matrice p lorsque p est un nombre premier ont leur diagonale pleine de 0 (et la trace étant la somme des éléments diagonaux, elle ne cumulera rien pour les petites matrices circulantes en question) quand on est sur une puissance M^q avec $q \neq p$.

On fait calculer par programme les valeurs propres des matrices $(M_k)^k$ pour k les entiers successifs. On constate que la liste des valeurs propres de $(M_p)^p$ pour p un nombre premier est le cumul des listes des racines de l'unité pour $2 \leq k \leq p$ alors que pour les nombres composés, la liste des valeurs propres contient de nombreux 1, ainsi que "quelques" complexes racines de l'unité.

2. Tentative d'explication

La trace de la matrice $\mathrm{Tr}((M_k)^k)$ est égale à $\sigma(k) - 1$, où $\sigma(k)$ dénote la somme des diviseurs de k. En effet, par la cyclicité des sous-matrices, l'élévation à la puissance k de la matrice M_k "ramène" les 1 sur la diagonale seulement pour les diviseurs de k et l'opérateur trace, qui calcule la somme des éléments diagonaux de $(M_k)^k$, qui ici compte les 1 qui sont revenus sur la diagonale, en compte d pour un diviseur d de k dans la matrice $(M_k)^k$ (*rappel* : la matrice $(M_k)^k$ est de taille $\left(\frac{k(k+1)}{2} - 1\right) \times \left(\frac{k(k+1)}{2} - 1\right)$).

Le déterminant de cette même matrice est égal à -1 pour les nombres de la forme $4k+3$ et 1 pour les nombres de la forme $4k+1$, $4k$ et $4k+2$[2].

Voyons les valeurs propres ; écrivons les premières listes : on sépare par ci par là les valeurs propres par des ";" bleus au lieu d'utiliser les ",", pour bien séparer certains groupes de valeurs propres que l'on pense devoir être "lues ensembles".

$2 \to [1, 1]$

$3 \to [1, -1 \ ; \ 1, 1, 1]$

$4 \to [-\frac{1}{2} + \frac{\sqrt{3}}{2}i \ ; \ -\frac{1}{2} - \frac{\sqrt{3}}{2}i \ ; \ 1, 1, 1 \ ; \ 1, 1, 1, 1]$

$5 \to [1, -1 \ ; \ -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i, 1 \ ; \ -1, i, -i, 1 \ ; \ 1, 1, 1, 1, 1]$

$6 \to [-0.80 + 0.587i, -0.80 - 0.587i, 0.30 + 0.95i, 0.30 - 0.95i, 1 \ ; \ 1, -1, 1, -1 \ ; \ 1, 1 \ ; \ 1, 1, 1 \ ; \ 1, 1, 1, 1, 1, 1]$

$7 \to [1, -1 \ ; \ -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i, 1 \ ; \ -1, i, -i, 1 \ ; \ -0.80 + 0.587i, -0.80 - 0.587i, 0.30 + 0.95i, 0.30 - 0.95i, 1 \ ; \ -1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i, \frac{1}{2} + \frac{\sqrt{3}}{2}i, \frac{1}{2} - \frac{\sqrt{3}}{2}i, 1 \ ; \ 1, 1, 1, 1, 1, 1, 1]$

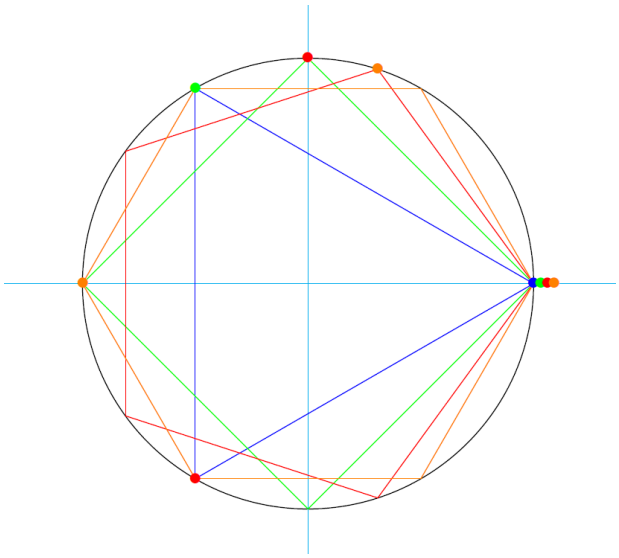
[2] On rappelle que Gauss remplaçait les $4k+3$ par des -1 dans les Recherches arithmétiques, dans sa démonstration de la loi de réciprocité quadratique.

On voit que ce n'est que pour les nombres premiers que la liste des valeurs propres est la liste des racines $k^{\text{ièmes}}$ de l'unité du plus petit polygone au plus grand en commençant par le polygone à 2 côtés (de sommets 1 et -1).

Ainsi, les nombres premiers ont des images qui sont des listes emboîtées : la liste des valeurs propres de la puissance p de leur matrice M_p (dont on rappelle qu'elle est de taille $\frac{p(p+1)}{2} - 1$) contient toutes les racines de l'unité pour $2 \leq k \leq p$. Les nombres composés n'ont pas ce genre d'image.

Regardons les valeurs propres pour le nombre composé 6 dans la liste fournie précédemment : on voit les $2 + 3 + 6 = \sigma(6) - 1 = 11$ occurrences de la valeur propre 1 correspondant aux 1 sur la diagonale de la sixième puissance de M_6, les autres valeurs propres sont celles du pentagone (car $6 \equiv 1 \pmod 5$).

Ci-dessous, le cercle unité sur lequel ont été positionnées les racines de l'unité des polygones réguliers ayant de 3 à 6 côtés.



3. Tentative de théorisation

La matrice M_k, qui contient toutes les circulantes sur sa diagonale, présente l'avantage, lorsqu'on l'élève à des puissances successives, de faire agir *simultanément* chacune des petites matrices circulantes indépendamment. Dans la suite, on notera les petites circulantes C_x pour ne pas se mélanger les pinceaux[3] avec la grosse matrice M_k.

La matrice M_k est une matrice de permutation :

- elle fait agir la mini-matrice C_2 sur les nombres de 1 à 2 ;
- elle fait agir la mini-matrice C_3 sur les nombres de 3 à 5 ;
- elle fait agir la mini-matrice C_4 sur les nombres de 6 à 9 ;

[3] C'est le cas de le dire..., puisque la théorie de tout ça en anglais parle de "shuffle".

- etc ;
- elle fait agir la mini-matrice C_k sur les nombres de $\frac{(k-1)k}{2}$ à $\frac{k(k+1)-2}{2}$.

Voyons les puissances des matrices circulantes indépendamment les unes des autres :

- $(C_k)^{0 \pmod k} = \mathrm{Id}_k$;
- $(C_k)^{+1 \pmod k} = C_k$;
- $(C_k)^{-1 \pmod k} = (C_k)^*$; il se trouve que dans le cas des matrices de permutations (ici cycliques), la transposée est également l'inverse. ;
- si k est pair, $(C_k)^{\frac{k}{2} \pmod m}$ est une matrice symétrique qui contient deux moitiés de diagonales, une au nord-est et une au sud-ouest (par exemple $(C_4)^6 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$.

4. Littérature

On peut se reporter à l'article 41 des Recherches arithmétiques de Gauss [1] pour trouver une démonstra-tion au sujet de permutations ainsi qu'aux manuscrits de Galois [2].

Valentin Bahier (à Toulouse) ou Nadia Lafrenière (à Montréal) ont présenté deux thèses sur les opérateurs de mélange aléatoires ([3], [4]).

5. Lien avec la conjecture de Goldbach

On a vu [5] qu'un nombre premier incongru à n (un nombre pair ≥ 6) selon tout module premier $\leq \lfloor \sqrt{n} \rfloor$ est un décomposant de Goldbach de n.

La reformulation de cette conjecture en terme de matrices est :

Conjecture de Goldbach :

$\forall n \geq 6, \exists p, p$ est un décomposant de Goldbach de n, i.e. p est premier et $n-p$ est premier.

$\forall n \geq 6, \exists p, \forall q$ premier, $2 \leq q \leq \lfloor \sqrt{n} \rfloor, (M_q)^p \neq (M_q)^n$.

On utilise la caractérisation trouvée pour les nombres premiers en terme de trace, on obtient :

$$\forall n \geq 6, \exists p \text{ tel que } \mathrm{Tr}(M_p)^p = p$$
$$\text{et } \forall q \text{ tel que }, 2 \leq q \leq \lfloor \sqrt{n} \rfloor \text{ et } \mathrm{Tr}(M_q)^q) = q,$$
$$\text{on a } (M_q)^p \neq (M_q)^n.$$

On peut préférer $(M_p)^p = \mathrm{Id}_p$ plutôt que $\mathrm{Tr}(M_p)^p = p$.

Illustration sur un exemple

Dans la table ci-dessous, on montre les puissances (exposants entêtes des colonnes) des matrices (dénomination choisie indiquée entêtes de ligne) qui montrent que 3 et 7 sont des décomposants de Golbach de 20. Pour alléger le tableau, on note ci-dessous les matrices de 20 :

$$(M_3)^{20} = \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix}, \quad (M_5)^{20} = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{pmatrix}, \quad (M_7)^{20} = \begin{pmatrix} & & & & & & 1 \\ 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 1 & \end{pmatrix}$$

Table des puissances impaires des matrices d'indices impairs :

	3	5	7	9
M_3	$\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$	$\begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix}$	$\begin{pmatrix} 1 & & \\ & & 1 \\ 1 & & \end{pmatrix}$	$\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$
M_5	$\begin{pmatrix} & & 1 & & \\ & & & & 1 \\ 1 & & & & \\ & 1 & & & \\ & & & 1 & \end{pmatrix}$	$\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{pmatrix}$	$\begin{pmatrix} & & 1 & & \\ & & & 1 & \\ & & & & 1 \\ 1 & & & & \\ & 1 & & & \end{pmatrix}$	$\begin{pmatrix} & & & & 1 \\ 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \end{pmatrix}$
M_7	$\begin{pmatrix} & & 1 & & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & & 1 \\ 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \end{pmatrix}$	$\begin{pmatrix} & & & & & & 1 \\ 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 1 & \end{pmatrix}$	$\begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & 1 \end{pmatrix}$	$\begin{pmatrix} & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & 1 \\ 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \end{pmatrix}$
M_9	$(7,8,9,1,2,3,4,5,6)$	$(5,6,7,8,9,1,2,3,4)$	$(3,4,5,6,7,8,9,1,2)$	$(1,2,3,4,5,67,8,9)$

Note : Pour la ligne des puissances $9^{\text{ièmes}}$, on utilise la notation standard des permutations (voir la diapositive 4/29 du diaporama de Nadia Lafrenière [6]). On a que $(M_x)^y = (x-y+1, \ldots, x, 1, \ldots, x-y)$.

Références.

[1] Carl Friedrich Gauss, Recherches arithmétiques, Brunswick, 1802, voir l'édition Jacques Gabay, Paris ici https://gallica.bnf.fr/ark:/12148/bpt6k29060d.

[2] Évariste Galois, Manuscrits, publiés par Jules Tannery, 1908, Gauthier-Villars, Paris ici https://gallica.bnf.fr/ark:/12148/bpt6k9610625f.

[3] Nadia Lafreniere, Thèse de doctorat, *Valeurs propres des opérateurs de mélange symétrisés*, 2019, Montréal, https://nadialafreniere.github.io/these.pdf.

[4] Valentin Bahier, Thèse de doctorat, *Spectre de matrices de permutation aléatoires*, 2018, http://thesesups.ups-tlse.fr/3973/1/2018TOU30069.pdf.

[5] Denise Vella-Chemla, *Réécrire* (aidée de Leila Schneps), http://denise.vella.chemla.free.fr/jade1.pdf.

[6] Nadia Lafrenière, *Derangements : Solving Problems by Counting (Certain Types Of) Permutations*, Dartmouth College, https://nadialafreniere.github.io/talks/Derangements.pdf