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

On revient à une matrice, notée M dans la suite, contenant sur sa diagonale des matrices circulantes de taille 2, 3, 4, etc. On avait eu l'idée de cette matrice en juillet 2019 pour "simuler le crible d'Eratosthène"[1].

$$M = \begin{pmatrix}
0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 0 & 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 0 & 0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 1 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 1 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 0 & 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 1 & 0 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 1 & 0 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 1 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 1 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 0 & 1 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 1 & 0 & 0 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots
\end{pmatrix}$$

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 $\mathrm{Tr}(M^p) = p$, alors p est un nombre premier.

Au rang k, la matrice 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 cycliques sur la diagonale de M sont les matrices de permutation des groupes cycliques C_2, C_3, C_4, etc. Si on observe la diagonale de chacune de ces petites matrices, par exemple, la diagonale de la matrice 3×3, lorsqu'on les élève à différentes puissances correspondant aux entiers successifs

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

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

on comprend que suivant l'exposant de la matrice (la puissance à laquelle on l'élève), une fois sur 3, pour les puissances multiples de 3, les 3 chiffres 1 se retrouveront sur la diagonale, et la puissance de

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

la matrice en question aura pour trace 3. Cette cyclicité correspond au fait de “barrer un nombre sur 3” dans l'algorithme de criblage 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 quand on est sur une puissance M^q avec $q \neq p$.

Ci-dessous, le programme qui élève M aux diverses puissances successives et en calcule une valeur propre.

```
import math
import numpy as np
import numpy.linalg as alg

for k in range(2,50):
      print(k,end='')
      m=int(k*(k+1)/2-1)
      a = np.zeros((m,m))
      for u in range(k-1):
            i = int(((u+1)**2+3*(u+1)-2)/2)
            j = int(((u+3)**2-3*(u+3))/2)
            a[i,j] = 1
      for u in range(m-1):
            a[u,u+1] = 1
      for u in range(k-2):
            i = int(((u+1)**2+3*(u+1)-2)/2)
            j = int(((u+1)**2+3*(u+1)-2)/2+1)
            a[i,j] = 0
      grise = alg.matrix_power(a,k)
      valpropres = alg.eigvals(grise)
      print(valpropres[2:3])
      if (np.trace(grise) == k):
            print(k, 'est un nombre premier.'),
```

On utilise la bibliothèque python numpy.alg pour calculer l'une des valeurs propres des matrices pour un rang variant de 2 à 100.

```
2[] 2 est un nombre premier.
3[1.]  3 est un nombre premier.
4[1.+0.j]
5[-0.5+0.8660254j] 5 est un nombre premier.
6[0.30901699+0.95105652j]
7[-0.5+0.8660254j] 7 est un nombre premier.
```

```
8[-0.22252093+0.97492791j]
9[-1.+0.j]
10[-0.5+0.8660254j]
11[-0.5+0.8660254j] 11 est un nombre premier.
12[0.30901699+0.95105652j]
13[-0.5+0.8660254j] 13 est un nombre premier.
14[-0.74851075+0.66312266j]
15[-1.+0.j]
16[-0.80901699+0.58778525j]
17[-0.5+0.8660254j] 17 est un nombre premier.
18[-0.70710678-0.70710678j]
19[-0.5+0.8660254j] 19 est un nombre premier.
20[-0.5+0.8660254j]
21[-1.+0.j]
22[-0.90096887+0.43388374j]
23[-0.5+0.8660254j] 23 est un nombre premier.
24[-0.65486073+0.75574957j]
25[-0.5+0.8660254j]
26[-0.92977649+0.36812455j]
27[-1.+0.j]
28[-0.93969262+0.34202014j]
29[-0.5+0.8660254j] 29 est un nombre premier.
30[-0.90096887-0.43388374j]
31[-0.5+0.8660254j] 31 est un nombre premier.
32[-0.95413926+0.29936312j]
33[-1.+0.j]
34[-0.95949297+0.28173256j]
35[-0.5+0.8660254j]
36[-0.85021714+0.52643216j]
37[-0.5+0.8660254j] 37 est un nombre premier.
38[-0.96773295+0.25197806j]
39[-1.+0.j]
40[-0.87947375+0.47594739j]
41[-0.5+0.8660254j] 41 est un nombre premier.
42[-0.95105652-0.30901699j]
43[-0.5+0.8660254j] 43 est un nombre premier.
44[-0.97607588+0.21743018j]
45[-1.+0.j]
46[-0.9781476+0.20791169j]
47[-0.5+0.8660254j] 47 est un nombre premier.
48[-0.9172113+0.39840109j]
49[-0.5+0.8660254j]
```

Si l'on prend la seconde valeur propre, on trouve que pour les rangs correspondant aux nombres premiers, mais pas seulement pour ces rangs-là, la seconde valeur propre est le complexe $0.5 + \frac{\sqrt{3}}{2}\, i$,

correspondant à l'angle $\frac{\pi}{3}$ sur le cercle trigonométrique. On est "ennuyée" par le fait que pour les rangs 10, 25, 35 ou 49, la seconde valeur propre est aussi égale au complexe en question.

De ce fait, on décide de s'intéresser à une valeur propre "ultérieure", par exemple la $11^{\text{ième}}$ et là, surprise, les rangs qui sont des nombres premiers semblent être les seuls rangs pour lesquels la $11^{\text{ième}}$ valeur propre est égale à $e^{\frac{-2i\pi}{5}}$, mais en y regardant bien, 49 n'est pas discriminé des nombres premiers.

Le résultat du programme :

```
2[] 2 est un nombre premier.
3[] 3 est un nombre premier.
4[]
5[1.+0.j] 5 est un nombre premier.
6[1.+0.j]
7[0.30901699+0.95105652j] 7 est un nombre premier.
8[-0.80901699-0.58778525j]
9[-0.80901699-0.58778525j]
10[1.+0.j]
11[0.30901699+0.95105652j] 11 est un nombre premier.
12[0.41541501+0.909632j]
13[0.30901699+0.95105652j] 13 est un nombre premier.
14[0.88545603+0.46472317j]
15[0.6234898+0.78183148j]
16[0.66913061-0.74314483j]
17[0.30901699+0.95105652j] 17 est un nombre premier.
18[-0.80901699-0.58778525j]
19[0.30901699+0.95105652j] 19 est un nombre premier.
20[-0.87947375+0.47594739j]
21[-1.66533454e-16+1.j]
22[0.07473009-0.9972038j]
23[0.30901699+0.95105652j] 23 est un nombre premier.
24[-0.80901699+0.58778525j]
25[-0.96592583-0.25881905j]
26[-0.18738131-0.98228725j]
27[-0.35460489+0.93501624j]
28[-0.28680323-0.95798951j]
29[0.30901699+0.95105652j] 29 est un nombre premier.
30[1.+0.j]
31[0.30901699+0.95105652j] 31 est un nombre premier.
32[-0.44039415-0.89780454j]
33[-0.55557023+0.83146961j]
34[-0.5-0.8660254j]
35[-0.9829731-0.18374952j]
```

```
36[0.44573836-0.89516329j]
37[0.30901699+0.95105652j] 37 est un nombre premier.
38[-0.59463318-0.80399713j]
39[-0.67728157+0.73572391j]
40[0.24548549-0.96940027j]
41[0.30901699+0.95105652j] 41 est un nombre premier.
42[0.30901699+0.95105652j]
43[0.30901699+0.95105652j] 43 est un nombre premier.
44[-0.6940742-0.71990347j]
45[-0.75574957+0.65486073j]
46[-0.7193398-0.69465837j]
47[0.30901699+0.95105652j] 47 est un nombre premier.
48[-0.06824241-0.99766877j]
49[0.30901699+0.95105652j]
```

On constate que 10, 25, 35 ont été "discriminés" des nombres premiers en prenant une valeur propre d'indice plus élevé, mais 49 s'envoie toujours sur le même complexe (en l'occurrence $e^{\frac{2i\pi}{5}}$) que les nombres premiers. Alors, on prend la $22^{\text{ième}}$ valeur propre et enfin, le nombre 49 s'avère ne pas avoir la même image que les nombres premiers (pour eux, c'est le complexe correspondant à l'angle 77.14 degrés) ; le résultat du programme est :

```
2[] 2 est un nombre premier.
3[] 3 est un nombre premier.
4[]
5[] 5 est un nombre premier.
6[]
7[1.+0.j] 7 est un nombre premier.
8[1.+0.j]
9[-0.90096887-0.43388374j]
10[-0.90096887+0.43388374j]
11[-0.22252093+0.97492791j] 11 est un nombre premier.
12[-0.90096887-0.43388374j]
13[-0.22252093+0.97492791j] 13 est un nombre premier.
14[-0.5-0.8660254j]
15[-0.22252093+0.97492791j]
16[-0.90096887-0.43388374j]
17[-0.22252093+0.97492791j] 17 est un nombre premier.
18[-0.27366299-0.96182564j]
19[-0.22252093+0.97492791j] 19 est un nombre premier.
20[0.54694816-0.83716648j]
21[1.+0.j]
22[-0.90096887-0.43388374j]
23[-0.22252093+0.97492791j] 23 est un nombre premier.
```

```
24[0.41541501+0.909632j]
25[0.25881905+0.96592583j]
26[0.96858316-0.24868989j]
27[0.74851075-0.66312266j]
28[1.+0.j]
29[-0.22252093+0.97492791j] 29 est un nombre premier.
30[0.22252093-0.97492791j]
31[-0.22252093+0.97492791j] 31 est un nombre premier.
32[0.68896692+0.72479279j]
33[0.38268343-0.92387953j]
34[0.58005691+0.81457595j]
35[-0.27366299+0.96182564j]
36[-0.90096887+0.43388374j]
37[-0.22252093+0.97492791j] 37 est un nombre premier.
38[0.37285648+0.92788903j]
39[0.08257935-0.99658449j]
40[-0.90096887+0.43388374j]
41[-0.22252093+0.97492791j] 41 est un nombre premier.
42[-0.95105652-0.30901699j]
43[-0.22252093+0.97492791j] 43 est un nombre premier.
44[0.10937121+0.99400098j]
45[-0.14231484-0.98982144j]
46[0.0348995+0.99939083j]
47[-0.22252093+0.97492791j] 47 est un nombre premier.
48[0.8544194-0.51958395j]
49[-0.99144486-0.13052619j]
```

On n'a pas encore d'explication d'un tel phénomène mais il reste surprenant car on n'a au départ "mis aucune information" dans la matrice M : elle contient *toutes* les matrices circulantes jusqu'à un certain rang, un peu comme une factorielle contient tous les entiers jusqu'à l'un certain d'entre eux.

Ce qui est étonnant dans le fait que telle valeur propre (par exemple la $22^{\text{ième}}$), qui a permis de discriminer les nombres premiers des nombres composés inférieurs à 50, soit la même pour deux nombres premiers, par exemple prenons $p_1 = 11$ et $p_2 = 37$ (pour tous les nombres premiers en fait), c'est le fait qu'on pense avoir calculé deux choses différentes : dans un cas la $22^{\text{ième}}$ valeur propre de la $11^{\text{ième}}$ puissance d'une matrice de taille $\frac{11 \times 12}{2} - 1$ et dans l'autre cas, la $22^{\text{ième}}$ valeur propre de la $37^{\text{ième}}$ puissance d'une matrice de taille $\frac{37 \times 38}{2} - 1$; il faudrait dans un premier temps au moins comprendre cela, peut-être ce partage d'une valeur propre de même rang est-il dû au fait que la première matrice est sous-matrice haute gauche de la seconde. On n'a pas d'explication parce qu'on imagine que les racines des nouveaux facteurs intégrés au polynôme caractéristique (par exemple les racines de $(x^k - 1)$), au fur et à mesure de l'augmentation de la taille de la matrice, devraient s'intercaler entre les racines des polynômes caractéristiques des niveaux inférieurs (les racines des produits successifs de $x^{k'} - 1$ avec $k' < k$.

Explication : la trace de la matrice $\mathrm{Tr}(M^k)$ est égal à $\sigma(k)$, la somme des diviseurs de k diminuée de 1. En effet, par la cyclicité des sous-matrices, l'élévation à la puissance "ramène les 1 sur la diagonale" et l'opérateur trace, qui calcule la somme des éléments diagonaux de M^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 (*rappel* : la matrice M^k est de taille $\left(\frac{k(k+1)}{2}-1\right)\times\left(\frac{k(k+1)}{2}-1\right)$).

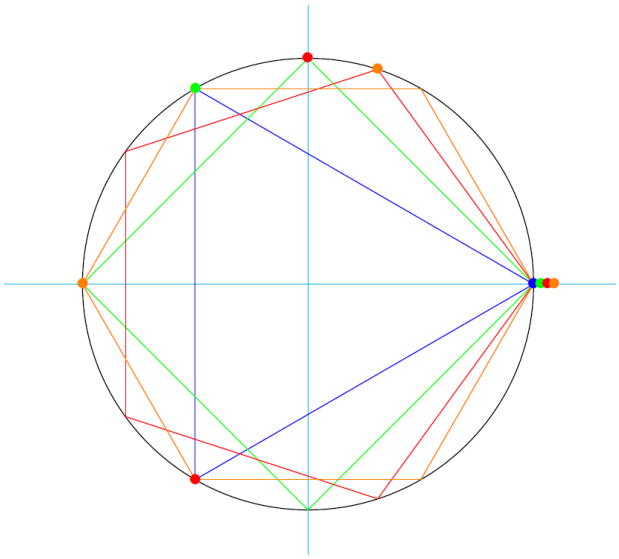
Le déterminant de cette même matrice est égal à -1 pour les nombres de la forme $4k+3$ et 1 pour les nombres de la forme $4k+1$, $4k$ et $4k+2$[2].

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 les groupes de 2, 3, 4, 5, etc. valeurs propres.

$2 \to [1, 1]$
$3 \to [1, -1\ ;\ 1, 1, 1]$
$4 \to [-\frac{1}{2}+\frac{\sqrt{3}}{2}i\ ;\ -\frac{1}{2}-\frac{\sqrt{3}}{2}i\ ;\ 1, 1, 1\ ;\ 1, 1, 1, 1]$
$5 \to [1, -1\ ;\ -\frac{1}{2}+\frac{\sqrt{3}}{2}i, -\frac{1}{2}-\frac{\sqrt{3}}{2}i, 1\ ;\ -1, i, -i, 1\ ;\ 1, 1, 1, 1, 1]$
$6 \to [-0.80+0.587i, -0.80-0.587i\ ;\ 0.30+0.95i, 0.30-0.95i, 1\ ;\ 1, -1, 1, -1\ ;\ 1, 1, 1, 1, 1\ ;\ 1, 1, 1, 1, 1, 1]$
$7 \to [1, -1\ ;\ -\frac{1}{2}+\frac{\sqrt{3}}{2}i, -\frac{1}{2}-\frac{\sqrt{3}}{2}i, 1\ ;\ -1, i, -i, 1\ ;\ -0.80+0.587i, -0.80-0.587i,$
$0.30+0.95i, 0.30-0.95i, 1\ ;\ -1, -\frac{1}{2}+\frac{\sqrt{3}}{2}i, -\frac{1}{2}-\frac{\sqrt{3}}{2}i, \frac{1}{2}+\frac{\sqrt{3}}{2}i, \frac{1}{2}-\frac{\sqrt{3}}{2}i], 1\ ;\ 1, 1, 1, 1, 1, 1, 1]$

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 dans l'ordre du plus petit polygone au plus grand en commençant par le polygone à 2 côtés (de sommets 1 et -1). C'est pour cette raison que la $22^{\text{ième}}$ valeur propre est toujours la même pour les nombres premiers et pas pour les nombres composés. Peut-être faut-il le démontrer, ou peut-être que c'est trivial.

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



[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.