

Se promener sur la sphère, mai 2015.

Vibrations de disque, mai 2015.

Petites idées, juin 2015.

Petites idées, juin 2015.

Discret / continu, juin 2015.

Discret / découverte merveilleuse d'Euler, juin 2015.

Epingler les restes modulaires sur le tore, juillet 2015.

A tore ou à raison ?, juillet 2015.

Discret / continu, somme de sommes de cos dans matrices, juillet.

Sommes de diviseurs ou bien produits de restes, juillet 2015.

Matrices, sommes de diviseurs, produits de restes, juillet 2015.

Matrices et divisibilité, juillet 2015.

Spectres, juillet 2015.

Matrices et indicateur d'Euler, août 2015.

Distance suprême, août 2015.

Etrangeté de certaines opérations matricielles, septembre 2015.

Revenir au maillage, septembre 2015.

Cherche maille de taille 4 pour le tissage, septembre 2015.

Modéliser, octobre 2015.

Projections, novembre 2015.

Infinité du nombre de couples de nombres premiers jumeaux, novembre 2015.

Jumeaux et automates, décembre 2015.

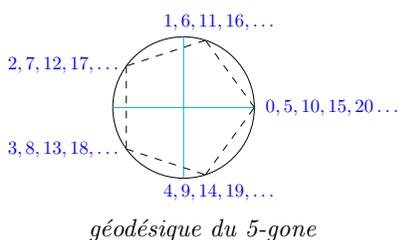
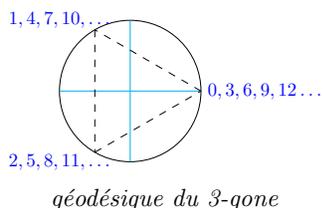
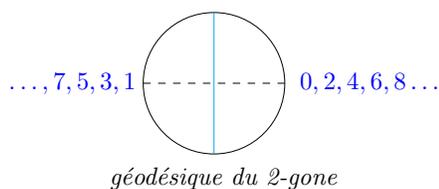
## Se promener sur la sphère (DV, 11/5/2015)

On aimerait associer à chaque entier son "mot de restes modulaires", i.e. le mot constitué de ses restes dans les divisions par l'infinité des nombres premiers. Par exemple, le mot associé à 11 est 1, 2, 1, 4, 0, 11, 11, 11, ... (1<sup>er</sup> reste mod 2, 2<sup>ème</sup> reste mod 3, 3<sup>ème</sup> reste mod 5, 4<sup>ème</sup> reste mod 7, 5<sup>ème</sup> reste mod 11 (donc 0), puis restes suivants mod tout premier strictement supérieur à 11 tous égaux à 11).

On "positionne" les différents restes d'un nombre entier  $n$  sur la sphère de la façon suivante :

- à chaque premier  $p$ , on associe un plan vertical passant par les pôles, séparé du plan de Greenwich par un angle de rotation de  $\frac{1}{p}$  ;
- sur ce plan vertical, on dessine sur la géodésique qui est l'intersection de ce plan et de la sphère un  $p$ -gone (un segment de droite pour  $p = 2$ , un triangle pour  $p = 3$ , un pentagone pour  $p = 5$ , un heptagone pour  $p = 7$ ,...). Tous ces  $p$ -gones ont un sommet sur le point  $(1, 0)$  (enfin, qui serait  $(1, 0)$  si on tournait ce plan pour le ramener sur le plan de Greenwich) qui "codera" tous les entiers divisibles par  $p$  (et puis sur le point suivant du  $p$ -gone, les nombres congrus à 1, sur le point suivant les congrus à 2, ..., sur le  $p - 1$ <sup>ème</sup> point les congrus à  $p - 1 \pmod{p}$ .

Exemples de géodésiques :



Ainsi, chaque entier est représenté par une infinité de points de la sphère dans l'infinité des "plans de restes". Du coup, les nombres premiers, n'étant divisibles que par eux-mêmes, ont leur ensemble de points qui ne contient qu'un seul point sur l'équateur.

Utiliser les nombres complexes

A un nombre complexe  $a + ib$ , on peut faire correspondre une matrice

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

On peut aussi voir le nombre complexe  $\cos\theta + i\sin\theta$  comme codant la combinaison d'une rotation d'angle  $\theta$  et d'une homothétie qui multiplie les normes des vecteurs par la norme du complexe  $\sqrt{\cos^2\theta + \sin^2\theta}$ .

Si on utilise la représentation proposée ci-dessus, on peut voir chaque nombre entier comme une composition infinie d'homothéties et rotations sur la sphère. Il faudrait pousser plus avant pour comprendre à quelles transformations correspond le fait d'avoir comme on l'a vu "un seul point sur l'équateur", dans la mesure où cette caractéristique suffit à distinguer les nombres premiers des nombres composés. Il faudrait voir aussi si cette représentation permet de modéliser "agréablement" l'addition et la multiplication des entiers.

## Vibrations de disque (DV, le 2 mai 2015)

On essaie d'imaginer deux procédés physiques pour "voir" les nombres premiers comme les noeuds de vibrations stationnaires qui seraient imprimées à un disque dans le premier cas ou bien qui passeraient par des fentes de Young dans le second cas.

On a réalisé (sans le démontrer) dans une autre note que les nombres premiers inférieurs ou égaux à  $n$  sont les zéros de la fonction  $sumsumcos(n)$  définie ainsi :

$$sumsumcos(n) = \sum_{i=2}^{n-1} \sum_{j=1}^i \cos \frac{2\pi n j}{i}$$

### 1) Première méthode : Figures de Chladni

Il faudrait que les nombres premiers "se lisent" sur des figures de Chladni qui s'obtiennent en faisant vibrer une plaque de cuivre saupoudrée de sable. La plaque aurait la forme d'un disque et on ferait imprimer des vibrations à la plaque par des archets frottant son bord.

Admettons qu'on se fixe simplement comme objectif de réussir à visualiser les 25 nombres premiers inférieurs ou égaux à 100, au nombre de 25. Ces nombres premiers peuvent être obtenus en testant la division des nombres de 8 à 100 par les 4 premiers nombres premiers 2, 3, 5 et 7 (puisque  $11^2 = 121$  et  $121 > 100$ ). On pourrait faire vibrer le premier archet à la fréquence  $1/2$ , le deuxième à la fréquence  $1/3$ , le troisième à la fréquence  $1/5$  et le quatrième à la fréquence  $1/7$ .

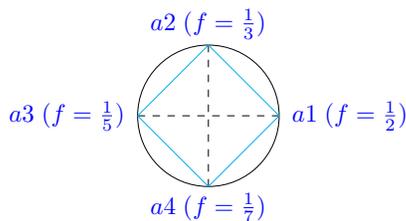
*Problème 1* : faudrait-il disposer les 4 archets (notés  $a_1, a_2, a_3, a_4$ ) aux 4 coins d'un carré inscrit dans le bord du disque ou bien faudrait-il les faire vibrer depuis 4 positions très proches les unes des autres, en se disant que  $2\pi$  correspondant au nombre 100, il faudrait placer le premier archet à la position  $7.2^\circ$  correspondant au nombre 2, le second archet à la position  $10.8^\circ$  correspondant au nombre 3, le troisième archet à la position  $18^\circ$  correspondant au nombre 5 et le quatrième archet à la position  $25.2^\circ$  correspondant au nombre 7 ?

*Problème 1 bis* : dans le cas où on dispose les archets en carré, ne serait-il pas plus judicieux que l'archet de fréquence  $1/2$  soit en face de l'archet de fréquence  $1/3$ , histoire d'équilibrer en quelque sorte les tempos lents, et de mettre les deux autres archets de fréquences  $1/5$  et  $1/7$  aux deux autres coins? Quand on généralise à une infinité de fréquences (chacune inverse d'un élément de l'ensemble infini des nombres premiers), comment faudrait-il disposer les archets ?

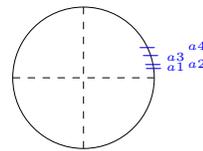
*Problème 2* : fixer les conditions au bord. Comment faut-il faire pour imposer qu'au bord du disque les fonctions valent bien 1 (pour que ça "corresponde" bien aux cosinus souhaités) ?

*Problème 3* : Où se liraient les nombres premiers ?

Le sable se disposerait-il par paquets, délimités par des lignes de sable, dessinant des sortes de bandes circulaires concentriques contenant justement 11, puis 13, puis 17, etc. zones délimitées ?



Archets aux 4 coins



Archets à leur "position numérique"

### 2) Deuxième méthode : Fentes de Young

On imagine un bac plein d'eau (comme une piscine à vagues mais en plus petit). On peut se reporter à ce dessin animé, à son instant une minute :

<https://www.youtube.com/watch?v=La64iUHfqs>

On place une plaque verticale dans le bac, percée de 4 fentes qui laisse passer l'eau. On est capable d'imposer à l'eau depuis 4 sources, disposées face aux 4 fentes, des fréquences différentes pour les vagues issues des 4 trous sous l'eau exactement comme dans le dispositif précédent (fréquence des vagues  $f = 1/2$  pour la première source,  $f = 1/3$  pour la seconde,  $f = 1/5$  pour la troisième et  $f = 1/7$  pour la quatrième).

On mesure au bout de la piscine la hauteur des vagues obtenues par interférences de ces 4 ondes aquatiques imposées et les nombres premiers pourraient peut-être apparaître au sein des différentes mesures.

A nouveau, de multiples problèmes techniques : La distance entre les fentes et le bout de la piscine, où on mesure les interférences obtenues a-t-elle de l'importance ? Où doit-on prendre les mesures sur le bord opposé de la piscine où viennent frapper les vagues ? La profondeur à laquelle sont situés les trous qui génèrent les ondes sous l'eau interfère-t-elle avec les résultats du dispositif ?

Rêve sonore, rêve aquatique, après un rêve, on se réveille. De toute façon, on n'a pas de piscine.

1) Sommes de cosinus

On a proposé la fonction  $sumsumcos(n)$  dont les zéros sont les nombres premiers<sup>12</sup>.

$$sumsumcos(n) = \sum_{b=2}^{n-1} \sum_{o=1}^b \cos\left(\frac{2\pi no}{b}\right)$$

On est très tenté d'utiliser la fonction d'Euler  $\cos(x) = \frac{e^{ix} + e^{-ix}}{2}$  pour réécrire cette formule en :

$$sumsumcos(n) = \sum_{b=2}^{n-1} \sum_{o=1}^b \frac{1}{2} (e^{i\frac{2\pi no}{b}} + e^{-i\frac{2\pi no}{b}})$$

On aimerait établir un lien entre cette vision des nombres premiers comme zéros d'une fonction simple et une modélisation à base d'opérateurs matriciels.

Pour cela, on peut définir une matrice qui contient ligne par ligne les cosinus à additionner, y compris pour les deux indices exclus pour le calcul des zéros qui correspondent aux bornes  $b = 1$  et  $b = n$ . Cette matrice  $M$  est triangulaire (haute-gauche) et contient à la position  $b, o$  l'élément  $a_{b,o} = \cos\left(\frac{2\pi no}{b}\right)$ . En multipliant cette matrice par la matrice triangulaire haute-gauche pleine de 1, on obtient sur la diagonale les différentes sommes de cosinus à additionner et dont il faut tester l'égalité à  $1 + n$  pour savoir si  $n$  est un nombre premier (on pourrait par un artifice rajouter ce  $1 + n$  à l'une des extrémités de la diagonale par exemple). On appelle trace la somme des éléments diagonaux.

Montrons sur un exemple de matrices de lettres qu'on obtient bien les sommes souhaitées sur la diagonale.

$$\text{Si } M = \begin{pmatrix} q & r & s & t \\ u & v & w & 0 \\ x & y & 0 & 0 \\ z & 0 & 0 & 0 \end{pmatrix} \text{ et } T = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \text{ alors}$$

$$MT = \begin{pmatrix} q+r+s+t & q+r+s & q+r & q \\ u+v+w & u+v+w & u+v & u \\ x+y & x+y & x+y & x \\ z & z & z & z \end{pmatrix}$$

On trouve naturel de relier cette matrice de cosinus à une vision des nombres qu'on a proposée à base d'ondes (co)sinusoïdales de divisibilité par les entiers qui leur sont inférieurs (*tous* ceux qui leur sont inférieurs, comme proposé ici, ou bien seulement les nombres premiers qui sont inférieurs à leur racine).

Informatiquement, la double somme "se code" par deux boucles *for* imbriquées et c'est peut-être là que réside la non-commutativité. Il faut définir d'abord l'indice de la somme externe pour pouvoir définir ensuite l'indice de la somme interne dont la dernière valeur dépend. Il faut avoir à l'esprit qu'on peut penser soit qu'une énorme matrice infinie contiendrait directement toutes les valeurs soit qu'il faut construire cette matrice petit à petit, au fur et à mesure que  $n$  grandit et ceci incrémentalement. Du point de vue informatique, la non-commutativité résiderait alors dans la séquentialité du déroulement des instructions d'un programme en général (et dans ce cas précis, elle interviendrait notamment dans la définition des variables utilisées dans les instructions des deux boucles *for*).

2) Suites infinies alternées

Chacun des cosinus dans la somme de sommes ci-dessus est égal à une suite infinie alternée.

$$\cos(x) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} x^{2n}$$

Pour la fonction  $\zeta$  de Riemann aussi, on dispose d'une définition faisant intervenir une suite infinie alternée : on peut étendre  $\zeta$  sur  $Re(s) > 0$  à partir de la définition de la série alternée appelée fonction

<sup>1</sup>La démonstration d'une égalité similaire portant sur la somme des diviseurs est à trouver dans un livre de Jean-Marie De Koninck. La somme des diviseurs d'un nombre premier  $p$  vaut  $p + 1$ .

<sup>2</sup>Les noms d'indice ont été choisis pour que soit perçue subliminalement l'expression poétique "deux pianos sur baie".

êta de Dirichlet.

$$\eta(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}$$
$$\zeta(s) = \frac{\eta(s)}{1 - 2^{1-s}}$$

3) *Exprimer la récurrence merveilleuse à l'aide de matrices*

Mais l'idée qu'il me plairait vraiment d'amener à son terme, c'est l'idée de coder la récurrence extraordinaire de la somme des diviseurs dans le formalisme matriciel par des matrices triangulaires et d'utiliser le fait qu'un nombre premier  $p$  a sa somme des diviseurs qui vaut  $p + 1$  pour établir peut-être d'une autre manière encore que la non-commutativité est nécessaire pour appréhender l'ensemble des nombres premiers.

On a lu qu'une récurrence élémentaire (celle de Fibonacci,  $u_0 = 1, u_1 = 1, u_{n+2} = u_{n+1} + u_n$ , se code simplement avec des matrices, et le nombre d'or apparaît dans la matrice dont on peut calculer les puissances) et on pense qu'il doit ainsi y avoir un ou plusieurs nombres qui "dirigent" la répartition des nombres premiers<sup>3</sup>.

La récurrence extraordinaire est :

$$\sigma(x) = \frac{12}{x^2(x-1)} \sum_{k=1}^{x-1} (-x^2 + 5kx - 5k^2) \sigma(k) \sigma(x-k)$$

---

<sup>3</sup>On a lu que les vecteurs propres d'un opérateur fournissent la direction des transformations quand les valeurs propres en fournissent la vitesse en quelque sorte.

1) Opérateur

Où en est-on ? On commence lentement à essayer de raisonner en terme de matrices. On a plusieurs éléments qui semblent peut-être intéressants :

- il faudrait disposer d'une matrice triangulaire d'exponentielles. Les arguments des exponentielles seraient de la forme  $\frac{2\pi n o}{b}$ ,  $o$  variant de 1 à  $b$ ,  $b$  variant de 2 à  $n - 1$  ;
- il faudrait déterminer si la matrice infinie contenant les exponentielles est donnée d'emblée ou bien si elle est construite incrémentalement. Pour augmenter la taille d'une matrice petit à petit, on a l'idée d'utiliser des matrices rectangulaires, comme ci-dessous, mais les contenus successifs laissent vraiment à désirer. Par exemple, pour obtenir une matrice  $3 \times 3$ , puis une matrice  $4 \times 4$ , on peut procéder ainsi mais on aimerait que les matrices résultantes restent triangulaires :

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

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 5 & 5 & 3 & 0 \\ 5 & 5 & 3 & 0 \\ 3 & 3 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

- on avait eu l'idée en avril 2014 d'amener l'axe des abscisses sur la droite du plan complexe de partie réelle  $1/2$  mais on utilisait des fonctions. Ce n'était pas du tout ce qu'il faudrait faire : il faudrait trouver un opérateur du plan complexe dans lui-même qui effectue la rotation.
- une rotation qui amènerait l'axe des abscisses sur l'axe des ordonnées et qui semblerait judicieuse de prime abord serait la rotation qui envoie l'angle  $\theta$  sur l'angle  $\pi/4 - \theta$ . En inversant *cosinus* et *sinus* d'un angle, on dirait qu'elle "symétriserait bien". De plus, comme par extraordinaire, le cosinus et le sinus de  $\pi/4$  valent  $\sqrt{2}/2$  dont le carré vaut  $1/2$ .

Le problème est qu'avec un tel opérateur, les zéros de l'axe des abscisses se retrouveraient sur l'axe des ordonnées alors qu'il faudrait également qu'ils subissent un décalage de leur partie réelle d' $1/2$  à droite pour se retrouver sur "la bonne droite" mais peut-être qu'alors, par ce "shift", on perd la linéarité ?

1) On a deux opérateurs représentés par des matrices, l'une contenant des réels, l'autre contenant des entiers, sur lesquels se focaliser :

- La matrice de réels contient des éléments de la forme  $\cos \frac{2\pi no}{b}$  ; par exemple, la matrice associée à  $n = 10$  est :

$$\begin{pmatrix} \cos \frac{20\pi 1}{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{2} & \cos \frac{20\pi 2}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{3} & \cos \frac{20\pi 2}{3} & \cos \frac{20\pi 3}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{4} & \cos \frac{20\pi 2}{4} & \cos \frac{20\pi 3}{4} & \cos \frac{20\pi 4}{4} & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{5} & \cos \frac{20\pi 2}{5} & \cos \frac{20\pi 3}{5} & \cos \frac{20\pi 4}{5} & \cos \frac{20\pi 5}{5} & 0 & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{6} & \cos \frac{20\pi 2}{6} & \cos \frac{20\pi 3}{6} & \cos \frac{20\pi 4}{6} & \cos \frac{20\pi 5}{6} & \cos \frac{20\pi 6}{6} & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{7} & \cos \frac{20\pi 2}{7} & \cos \frac{20\pi 3}{7} & \cos \frac{20\pi 4}{7} & \cos \frac{20\pi 5}{7} & \cos \frac{20\pi 6}{7} & \cos \frac{20\pi 7}{7} & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{8} & \cos \frac{20\pi 2}{8} & \cos \frac{20\pi 3}{8} & \cos \frac{20\pi 4}{8} & \cos \frac{20\pi 5}{8} & \cos \frac{20\pi 6}{8} & \cos \frac{20\pi 7}{8} & \cos \frac{20\pi 8}{8} & 0 & 0 \\ \cos \frac{20\pi 1}{9} & \cos \frac{20\pi 2}{9} & \cos \frac{20\pi 3}{9} & \cos \frac{20\pi 4}{9} & \cos \frac{20\pi 5}{9} & \cos \frac{20\pi 6}{9} & \cos \frac{20\pi 7}{9} & \cos \frac{20\pi 8}{9} & \cos \frac{20\pi 9}{9} & 0 \\ \cos \frac{20\pi 1}{10} & \cos \frac{20\pi 2}{10} & \cos \frac{20\pi 3}{10} & \cos \frac{20\pi 4}{10} & \cos \frac{20\pi 5}{10} & \cos \frac{20\pi 6}{10} & \cos \frac{20\pi 7}{10} & \cos \frac{20\pi 8}{10} & \cos \frac{20\pi 9}{10} & \cos \frac{20\pi 10}{10} \end{pmatrix}$$

La somme des éléments de la ligne  $d$  vaut  $d$  si  $d \mid n$  et vaut 0 sinon.

La somme de tous les éléments de la matrice vaut donc  $\sigma(n)$ , qui est la somme des diviseurs de  $n$ .

- La matrice d'entiers contient des éléments  $M_{n,d} = d$  si  $d \mid n$  et 0 sinon.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 8 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 9 & 0 \\ 1 & 2 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 10 \end{pmatrix}$$

Ici,  $\sigma(n)$  est la somme des éléments de la dernière ligne.

On est plutôt portée, depuis le début de ces recherches, vers une modélisation discrète, booléenne (binaire) étant l'idéale.

2) Comme cela est visible sur les tables de vérité logique de  $\wedge$  et  $\vee$  ci-dessous, si on pose que  $1 + 1 = 1$ ,  $min$  équivaudrait à  $\wedge$  et  $+$  équivaudrait à  $\vee$ .

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

Le 9 janvier 2008, on avait posté une petite note dont le paragraphe 2 fournissait des éléments en lien avec un article sublime d'Euler intitulé "Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs". Dans cette note en français<sup>1</sup>, Euler fournit une récurrence surprenante qui lie entre elles les sommes des diviseurs des entiers successifs.

$$\sigma(n) = \sigma(n-1) + \sigma(n-2) - \sigma(n-5) - \sigma(n-7) + \sigma(n-12) + \sigma(n-15) - \dots$$

Monsieur Dominique Giard fournit sur la toile, dans les annexes de la séquence A000203 de l'OEIS (la On-Line Encyclopedia of Integer Sequences) concernant la somme des diviseurs d'un entier, une autre récurrence, non moins surprenante, pour calculer la somme des diviseurs d'un entier.

$$\sigma(x) = \frac{12}{x^2(x-1)} \sum_{k=1}^{x-1} (-x^2 + 5kx - 5k^2)\sigma(k)\sigma(x-k)$$

On avait vérifié avec surprise en 2008 que cette récurrence calculait bien la somme des diviseurs. Il s'agit de multiplier les éléments de deux triangles de nombres, qui rappellent le triangle de Pascal.

Le premier triangle contient les nombres :

1								
1	1							
-1	4	-1						
-5	5	5	-5					
-11	4	9	4	-11				
-19	1	11	11	1	-19			
-29	-4	11	16	11	-4	-29		
-41	-11	9	19	19	9	-11	-41	
-55	-20	5	20	25	20	5	-20	-55

Ce triangle contient les coefficients multiplicatifs  $p(n, k) = -n^2 + 5kn - 5k^2$  pour  $n$  variant de 2 à 10 et pour  $k$  variant dans chaque ligne de 1 à  $n-1$ .

Le deuxième triangle, quant à lui, contient :

1								
3	3							
4	9	4						
7	12	12	7					
6	21	16	21	6				
12	18	28	28	18	12			
8	36	24	49	24	36	8		
15	24	48	42	42	48	24	15	
13	45	32	84	36	84	32	45	13

Pour trouver le premier élément de chaque ligne de ce deuxième triangle, on multiplie terme à terme les éléments des lignes précédentes dans les deux triangles et on multiplie le résultat par  $\frac{12}{n^2(n-1)}$ .

Pour trouver les autres éléments d'une ligne, on se sert des premiers éléments de chaque ligne, en les multipliant deux à deux.

Les premiers éléments des lignes de ce deuxième triangle sont les sommes des diviseurs des entiers successifs.

---

<sup>1</sup>Le fait qu'Euler ait écrit cette note en français est assez exceptionnel, ses notes étant plutôt écrites habituellement en latin ou allemand. La note est trouvable à l'adresse [http://portail.mathdoc.fr/cgi-bin/oetoc?id=OE\\_EULER12](http://portail.mathdoc.fr/cgi-bin/oetoc?id=OE_EULER12)

Montrons comment trouver les éléments des triangles en multipliant des matrices.  
 On utilise la matrice d'entiers  $M_n$  qui contient les éléments  $M_{n,d} = d$  si  $d \mid n$  et 0 sinon.

$$M_9 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 0 & 0 & 6 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 8 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 9 \end{pmatrix}$$

Ici,  $\sigma(9) = 13$  est la somme des éléments de la dernière ligne.

On écrit la matrice "à l'envers" en la multipliant à gauche par une matrice diagonale de 1 "inversée", dans le sens où les 1 sont sur la diagonale nord-est / sud-ouest.

$$M_{diag} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$M_{9-tourne} = M_{diag} \cdot M_9 = \begin{pmatrix} 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 9 \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 8 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 \\ 1 & 2 & 3 & 0 & 0 & 6 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Puis on multiplie  $M_{9-tourne}$  par une matrice triangulaire pleine de 1.

$$M2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Le positionnement des éléments dans les matrices est important car la multiplication matricielle s'effectue, comme l'écriture manuscrite, d'abord de la gauche vers la droite, puis du haut vers le bas.

On obtient par cette première multiplication  $M_{9-tourne} \cdot M2$  une matrice dans laquelle les sommes des diviseurs des entiers successifs sont dans la première colonne.

$$M_{9-tourne}.M2 = \begin{pmatrix} 13 & 4 & 4 & 4 & 4 & 4 & 4 & 1 & 1 \\ 15 & 15 & 7 & 7 & 7 & 7 & 3 & 3 & 1 \\ 8 & 8 & 8 & 1 & 1 & 1 & 1 & 1 & 1 \\ 12 & 12 & 12 & 12 & 6 & 6 & 6 & 3 & 1 \\ 6 & 6 & 6 & 6 & 6 & 1 & 1 & 1 & 1 \\ 7 & 7 & 7 & 7 & 7 & 7 & 3 & 3 & 1 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 1 & 1 \\ 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Puis, on multiplie à nouveau le résultat par la matrice triangulaire pleine de 1.  
On obtient la matrice ci-dessous :

$$M_{9-tourne}.M2.M2 = \begin{pmatrix} 39 & 38 & 37 & 33 & 29 & 25 & 21 & 17 & 13 \\ 65 & 64 & 61 & 58 & 51 & 44 & 37 & 30 & 15 \\ 30 & 29 & 28 & 27 & 26 & 25 & 24 & 16 & 8 \\ 70 & 69 & 66 & 60 & 54 & 48 & 36 & 24 & 12 \\ 34 & 33 & 32 & 31 & 30 & 24 & 18 & 12 & 6 \\ 49 & 48 & 45 & 42 & 35 & 28 & 21 & 14 & 7 \\ 30 & 29 & 28 & 24 & 20 & 16 & 12 & 8 & 4 \\ 25 & 24 & 21 & 18 & 15 & 12 & 9 & 6 & 3 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

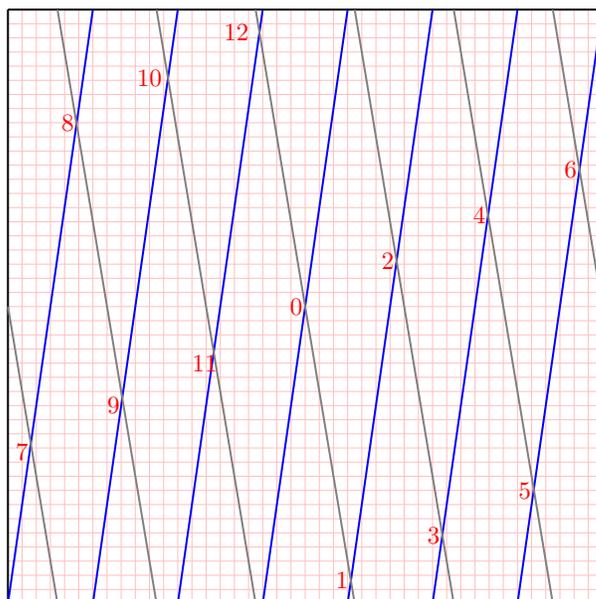
Cette fois-ci on voit apparaître dans la dernière colonne les sommes de diviseurs qui nous intéressent. On voit aussi apparaître, comme par magie, un certain nombre des autres valeurs du deuxième triangle qui nous intéressent également considérablement puisqu'elles interviennent dans tous les calculs intermédiaires (les lire de bas en haut, par exemple du 3 tout en bas au 24 de la colonne, en remontant, ou bien du 4 tout en bas au 48 de cette même colonne, etc).

Si on arrive à positionner les sommes de diviseurs des nombres sur la diagonale de la matrice d'un opérateur, un nombre premier présentant cette particularité d'avoir sa somme de diviseurs qui vaut  $p+1$ , les nombres premiers seront "presque" les valeurs propres de l'opérateur en question.

On essaie d'appréhender l'espace des nombres premiers. On est attachée à une modélisation qui code chaque nombre entier par le n-uplet infini de ses restes modulaires selon l'infinité des nombres premiers. *Exemple* : 11 est codé par (1,2,1,4,0,11,11,11,11...).

L'objectif consiste à associer à chaque reste modulaire  $a \bmod p$  un point du tore. Pour ça, on fixe un point du tore origine et on s'intéresse aux 2 courbes  $y = \left\lceil \frac{p}{2} \right\rceil x$  et  $y = -\left\lfloor \frac{p}{2} \right\rfloor x$ . Par exemple, si  $p = 13$ , on s'intéresse aux deux courbes  $y = 7x$  et  $y = -6x$ . Ces 2 courbes se croisent  $p$  fois sur le tore. A chaque point d'intersection, on associe l'un des restes modulaires selon le module  $p$ .

Voici la représentation plane des 13 points d'intersection des courbes pour  $p = 13$ .



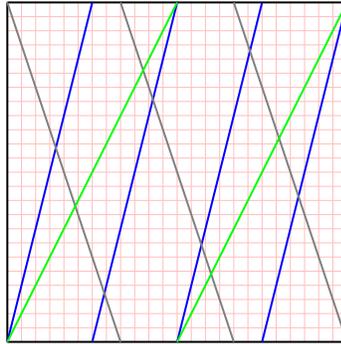
Un nombre entier étant caractérisé par l'infinité de ses restes modulaires selon l'infinité des nombres premiers peut ainsi être modélisé par une infinité de points du tore. On rappelle que chacun de ses restes est un point particulier de l'ensemble des intersections de 2 courbes du tore.

Un nombre premier ayant un seul de ses restes modulaires selon l'ensemble infini des nombres premiers qui est nul, aura un seul de ses points associés épinglé à l'origine.

On ne sait pas si une telle modélisation présente un intérêt. En particulier, on ne sait pas passer du reste modulaire  $a \bmod p$  au reste modulaire  $a \bmod q$  ( $a$  entier,  $p$  et  $q$  premiers).

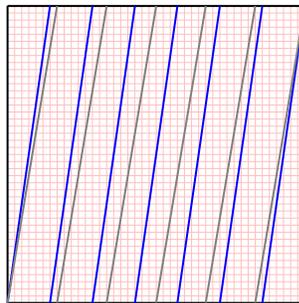
Je remercie les intervenants du forum les-mathematiques.net qui ont pour pseudos *remarque* et *GaBuZoMeu* pour l'aide qu'ils m'ont apportée au sujet du tore <http://www.les-mathematiques.net/phorum/read.php?4,1109447>.

Voici la représentation plane des 12 points d'intersection des courbes pour  $p = 7$ .

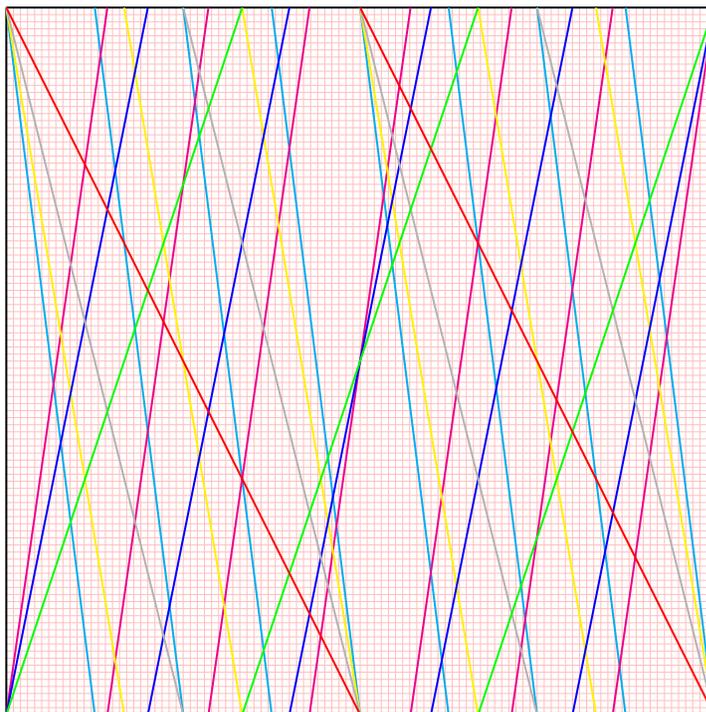


Les 3 courbes  $y = 4x$ ,  $y = -3x$ ,  $y = 2x$  montrent les  $4 + 3 = 7$  et les  $3 + 2 = 5$  points d'intersection d'un coup.

Ci-dessous la représentation de l'unique point d'intersection des courbes  $y = 7x$  et  $y = -6x$ .



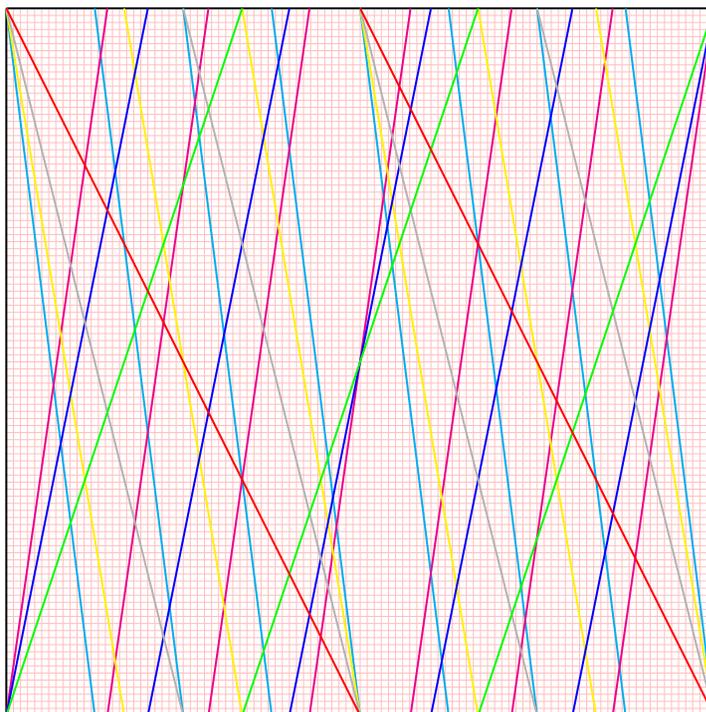
Autre exemple, le nombre 15, fonctions  $y = 8x$  (cyan),  $y = -7x$  (magenta),  $y = 6x$  (jaune),  $y = -5x$  (bleu),  $y = 4x$  (gris),  $y = -3x$  (vert),  $y = 2x$  (rouge). Les nombres de points d'intersection sont  $8+7 = 15$ ,  $7+6 = 13$ ,  $6+5 = 11$ ,  $5+4 = 9$ ,  $4+3 = 7$  et  $3+2 = 5$ .



On essaie d'appréhender l'espace des nombres premiers. On est attachée à une modélisation qui code chaque nombre entier par le n-uplet infini de ses restes modulaires selon l'infinité des nombres premiers. *Exemple* : 11 est codé par (1,2,1,4,0,11,11,11,11...).

L'objectif consiste à associer à chaque reste modulaire  $a \pmod p$  un point du tore. Pour ça, on fixe un point du tore origine et on s'intéresse aux 2 courbes  $y = \left[\frac{p}{2}\right]x$  et  $y = -\left[\frac{p}{2}\right]x$ . Par exemple, si  $p = 13$ , on s'intéresse aux deux courbes  $y = 7x$  et  $y = -6x$ . Ces 2 courbes se croisent  $p$  fois sur le tore. A chaque point d'intersection, on associe l'un des restes modulaires selon le module  $p$ .

Ci-dessous, les représentations des fonctions  $y = 8x$  (cyan),  $y = -7x$  (magenta),  $y = 6x$  (jaune),  $y = -5x$  (bleu),  $y = 4x$  (gris),  $y = -3x$  (vert),  $y = 2x$  (rouge). Les nombres de points d'intersection sont  $8+7 = 15$ ,  $7+6 = 13$ ,  $6+5 = 11$ ,  $5+4 = 9$ ,  $4+3 = 7$  et  $3+2 = 5$ .



Je remercie les intervenants du forum les-mathematiques.net qui ont pour pseudos *remarque* et *GaBuZoMeu* pour l'aide qu'ils m'ont apportée au sujet du tore <http://www.les-mathematiques.net/phorum/read.php?4,1109447>.

Il y aura 2 trucs qui m'auront bien plu et issus de cette discussion :

- le fait de compter les intersections de "droites" sur le tore, qui se résume ainsi :  $x, y \in [0, 1[, y = px, y = -qx \implies y = px = -qx \pmod 1 \implies (p + q)x = 0 \pmod 1 \iff (p + q)x = k, k \in \mathbb{Z} \implies k \in [0, p + q[$  si  $p + q \leq 0$ .

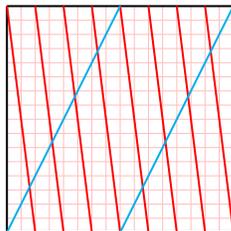
Je ne sais pas si c'est bien écrit, mais ce  $(\pmod 1)$  me parle enfin (je ne le comprenais pas précédemment, j'avais en tête que tout entier divisé par 1 donne un reste nul). On peut du coup (peut-être) mémoriser que les  $p$  éléments de  $\mathbb{Z}/p\mathbb{Z}$  peuvent être mis en bijection avec les  $p$  intersections sur le tore des droites d'équations  $y = \left[\frac{p}{2}\right]x$  et  $y = -\left[\frac{p}{2}\right]x$ , on a ainsi une vision géométrique des éléments de  $\mathbb{Z}/p\mathbb{Z}$  et de leur cyclicité ;

- on peut également "voir" sur le tore la divisibilité : si  $d \mid n$  alors, la droite du tore  $y = dx \pmod 1$  et la droite  $y = nx \pmod 1$  du tore se coupent (s'intersectent ?)  $d$  fois dans un plan de coupe horizontal du tore, par exemple, le plan équatorial.

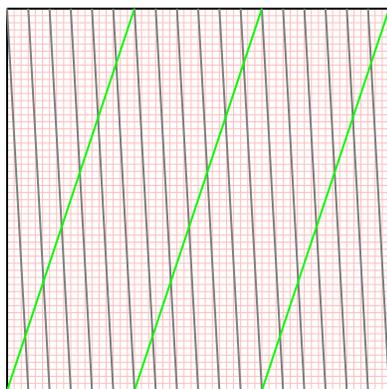
*Problème* : il faudrait peut-être savoir écrire ces idées matriciellement.

On essaie d'appréhender l'espace des nombres premiers. On va utiliser pour cela des solénoïdes du tore. On associe à chaque entier  $n$  le solénoïde qui effectue  $n$  tours du tore selon les méridiens pour 1 tour selon les parallèles avant de se refermer sur lui-même.

Par exemple, ci-dessous sont représentés sur la première représentation plane du tore les solénoïdes associés aux nombres 2 (cyan) et -8 (rouge), sur la seconde les solénoïdes associés aux nombres 3 (vert) et -18 (gris).



$$y = 2x \pmod{1}, y = -8x \pmod{1}$$



$$y = 3x \pmod{1}, y = -18x \pmod{1}$$

On compte les intersections des solénoïdes sur le tore en utilisant le fait que

$$\begin{cases} x, y \in [0, 1[ \\ y = px, \\ y = -qx \end{cases} \implies y = px = -qx \pmod{1} \implies (p+q)x = 0 \pmod{1}$$

équivalent à

$$(p+q)x = k, k \in \mathbb{Z} \implies k \in [0, p+q[ \text{ si } p+q \geq 0$$

Dans les dessins ci-dessus, on compte effectivement 6 intersections sur le premier tore et 15 sur le second. On peut "voir" sur le tore la divisibilité : si  $d \mid n$  alors, la droite du tore  $y = dx \pmod{1}$  et la droite  $y = -nx \pmod{1}$  du tore ont  $d$  intersections dans le plan équatorial (d'équation  $y = 0 \pmod{1}$ ).

On définit une fonction  $f$  qui à deux entiers  $n$  et  $m$  associe  $f(m, n)$  le nombre d'intersections de leur solénoïde qui appartiennent au parallèle d'équation  $y = 0 \pmod{1}$ .

$$\forall n > m \geq 1, f(n, m) = \text{pgcd}(n, m)$$

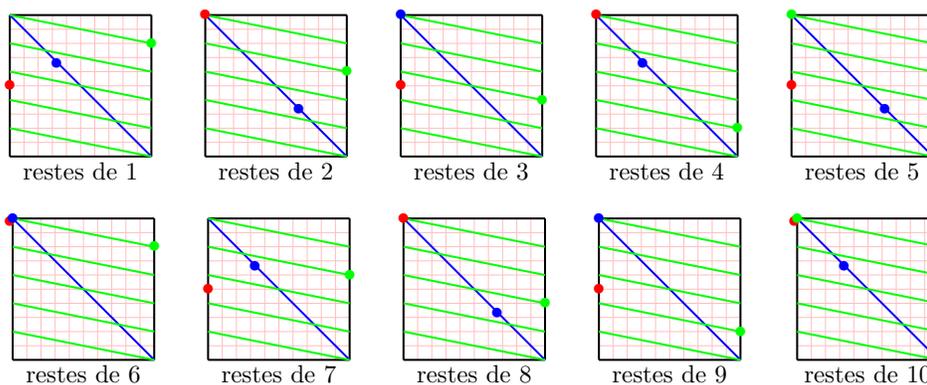
Cette fonction permet de lier géométriquement les nombres premiers. Le solénoïde d'un nombre premier  $p$  ne partage qu'un point sur le parallèle  $y = 0 \pmod{1}$  avec tout solénoïde associé à un nombre  $x$  avec lequel il est premier, que  $x$  soit premier lui-même, ou bien composé non divisible par  $p$ . La fonction  $f$  permet ainsi d'avoir une vision géométrique du treillis de la relation de divisibilité.

On essaie d'appréhender l'espace des nombres premiers. On est attaché à une modélisation qui code chaque nombre entier par le n-uplet infini de ses restes modulaires selon l'infinité des nombres premiers. *Exemple* : 11 est codé par (1,2,1,4,0,11,11,11,...). L'objectif consiste à associer à chaque reste modulaire  $x \bmod p$  un point du tore. Pour fixer les idées, on ne va considérer que les restes modulo les 3 premiers nombres premiers 2, 3 et 5. Aux nombres de 1 à 30, on va associer leur triplet de restes modulo 2, 3 et 5 ainsi :

$x \rightarrow (x \bmod 2, x \bmod 3, x \bmod 5)$	$x \rightarrow (x \bmod 2, x \bmod 3, x \bmod 5)$
1 $\rightarrow$ (1, 1, 1)	29 $\rightarrow$ (1, 2, 4)
2 $\rightarrow$ (0, 2, 2)	28 $\rightarrow$ (0, 1, 3)
3 $\rightarrow$ (1, 0, 3)	27 $\rightarrow$ (1, 0, 2)
4 $\rightarrow$ (0, 1, 4)	26 $\rightarrow$ (0, 2, 1)
5 $\rightarrow$ (1, 2, 0)	25 $\rightarrow$ (1, 1, 0)
6 $\rightarrow$ (0, 0, 1)	24 $\rightarrow$ (0, 0, 4)
7 $\rightarrow$ (1, 1, 2)	23 $\rightarrow$ (1, 2, 3)
8 $\rightarrow$ (0, 2, 3)	22 $\rightarrow$ (0, 1, 2)
9 $\rightarrow$ (1, 0, 4)	21 $\rightarrow$ (1, 0, 1)
10 $\rightarrow$ (0, 1, 0)	20 $\rightarrow$ (0, 2, 0)
11 $\rightarrow$ (1, 2, 1)	19 $\rightarrow$ (1, 1, 4)
12 $\rightarrow$ (0, 0, 2)	18 $\rightarrow$ (0, 0, 3)
13 $\rightarrow$ (1, 1, 3)	17 $\rightarrow$ (1, 2, 2)
14 $\rightarrow$ (0, 2, 4)	16 $\rightarrow$ (0, 1, 1)
15 $\rightarrow$ (1, 0, 0)	

On représente le premier reste verticalement sur le tore (le reste 0 (mod 2) est le point (0,0) tandis que le reste 1 (mod 2) est le point (0,1/2)), le second reste sur la pente bleue et le troisième reste sur la pente verte. On imagine aisément qu'on pourrait ajouter un point à chaque triplet, le transformant en quadruplet, pour prendre en compte le reste modulo 7, et ainsi infiniment, selon l'infinité des nombres premiers.

Présentons sur 10 représentations planes de tores les points associés aux nombres de 1 à 10.



Comment passe-t-on de l'ensemble de points associés à un entier à l'ensemble de points associés à l'entier suivant (cf. la fonction *succ* de l'axiomatique de Peano) ? Il suffit d'appliquer à chacun des points associés à  $x$  la "bonne" rotation, selon le module sur lequel on est alors focalisé. Si le module est 3, il s'agit d'effectuer une rotation d'un tiers de tour dans la bonne direction. Modulo 5, la rotation est d'1/5 de tour, etc.

La représentation matricielle d'une rotation d'un tiers de tour en dimension 2 est la matrice

$$\begin{pmatrix} \cos \frac{2\pi}{3} & -\sin \frac{2\pi}{3} \\ \sin \frac{2\pi}{3} & \cos \frac{2\pi}{3} \end{pmatrix}$$

On lit dans un cours que la généralisation en dimension supérieure est faisable moyennant quelques ajustements : il faut utiliser plutôt une représentation des rotations comme s'effectuant selon un seul angle autour

d'un axe dirigé par un vecteur unitaire et une rotation quelconque est un produit de telles rotations axiales.

On imagine qu'il ne doit peut-être pas être compliqué de généraliser ces idées en dimension infinie (l'infinité de l'ensemble des nombres premiers).

On comprend que les nombres premiers ont leur ensemble associé de points du tore qui ne contient qu'une seule occurrence du point  $(0, 0)$  tandis que les nombres composés ont leur ensemble associé de points du tore qui contient plusieurs de telles occurrences.

### *Rêve éveillé*

On est également tenté de voir une sorte de symétrie entre les points de coordonnée  $y = \theta$  et  $y = 1 - \theta$ . Cela nous ramène à une analogie qu'on avait faite qui liait le  $1/2$  de la droite de partie réelle  $1/2$  et le  $n/2$  qui intervient sans arrêt lors de l'étude des décompositions de Goldbach d'un nombre  $n$ <sup>123</sup>.

---

<sup>1</sup>On n'a pas considéré ici les points du tore comme ayant des coordonnées complexes mais on pourrait imaginer que le point  $(x, y)$  représente le nombre complexe  $x + iy$ .

<sup>2</sup><http://denise.vella.chemla.free.fr/analogie.pdf>

<sup>3</sup>Cela nous fait également penser à un extrait d'un article feuilleté de Marc Rieffel "*C\*-algebras associated with irrational rotations*" (bien que les coordonnées des points du tore qui interviennent ici soient rationnelles, les rotations sur le tore sont irrationnelles). Cette note fournit un théorème de Rieffel qui énonce (il faudrait stipuler toutes les conditions correspondantes) " $\forall t \in (\mathbb{Z} + \theta\mathbb{Z}) \cap [0, 1]$ , il existe un projecteur de  $\mathcal{A}_0$  dont la trace est  $t$ " et plus loin, "échanger  $u$  et  $v$  change  $\theta$  en  $1 - \theta$ " ce qui entraîne l'apparition un peu plus loin dans la note de la formule

$$g(e^{2i\pi t}) = \sqrt{f(e^{2i\pi t})(1 - f(e^{2i\pi t}))}$$

On a proposé la fonction  $sumsumcos(n)$  dont les zéros sont les nombres premiers

$$sumsumcos(n) = \sum_{b=2}^{n-1} \sum_{o=1}^b \cos\left(\frac{2\pi no}{b}\right)$$

On souhaite calculer de telles doubles sommes en utilisant des matrices carrées  $M_n$  contenant des cosinus.

Considérons la matrice  $10 \times 10$  :

$$M_{10} = \begin{pmatrix} \cos\frac{20\pi 1}{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos\frac{20\pi 1}{2} & \cos\frac{20\pi 2}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos\frac{20\pi 1}{3} & \cos\frac{20\pi 2}{3} & \cos\frac{20\pi 3}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos\frac{20\pi 1}{4} & \cos\frac{20\pi 2}{4} & \cos\frac{20\pi 3}{4} & \cos\frac{20\pi 4}{4} & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos\frac{20\pi 1}{5} & \cos\frac{20\pi 2}{5} & \cos\frac{20\pi 3}{5} & \cos\frac{20\pi 4}{5} & \cos\frac{20\pi 5}{5} & 0 & 0 & 0 & 0 & 0 \\ \cos\frac{20\pi 1}{6} & \cos\frac{20\pi 2}{6} & \cos\frac{20\pi 3}{6} & \cos\frac{20\pi 4}{6} & \cos\frac{20\pi 5}{6} & \cos\frac{20\pi 6}{6} & 0 & 0 & 0 & 0 \\ \cos\frac{20\pi 1}{7} & \cos\frac{20\pi 2}{7} & \cos\frac{20\pi 3}{7} & \cos\frac{20\pi 4}{7} & \cos\frac{20\pi 5}{7} & \cos\frac{20\pi 6}{7} & \cos\frac{20\pi 7}{7} & 0 & 0 & 0 \\ \cos\frac{20\pi 1}{8} & \cos\frac{20\pi 2}{8} & \cos\frac{20\pi 3}{8} & \cos\frac{20\pi 4}{8} & \cos\frac{20\pi 5}{8} & \cos\frac{20\pi 6}{8} & \cos\frac{20\pi 7}{8} & \cos\frac{20\pi 8}{8} & 0 & 0 \\ \cos\frac{20\pi 1}{9} & \cos\frac{20\pi 2}{9} & \cos\frac{20\pi 3}{9} & \cos\frac{20\pi 4}{9} & \cos\frac{20\pi 5}{9} & \cos\frac{20\pi 6}{9} & \cos\frac{20\pi 7}{9} & \cos\frac{20\pi 8}{9} & \cos\frac{20\pi 9}{9} & 0 \\ \cos\frac{20\pi 1}{10} & \cos\frac{20\pi 2}{10} & \cos\frac{20\pi 3}{10} & \cos\frac{20\pi 4}{10} & \cos\frac{20\pi 5}{10} & \cos\frac{20\pi 6}{10} & \cos\frac{20\pi 7}{10} & \cos\frac{20\pi 8}{10} & \cos\frac{20\pi 9}{10} & \cos\frac{20\pi 10}{10} \end{pmatrix}$$

La somme des éléments de la ligne  $d$  vaut  $d$  si  $d \mid n$  et vaut 0 sinon.

La somme de tous les éléments de la matrice vaut donc  $\sigma(n)$ , qui est la somme des diviseurs de  $n$ .

Pour le calcul des éléments d'une ligne, connaissant le premier élément de la ligne, on utilise les polynômes de Tchebychev de première espèce  $T_n(\cos(\theta)) = \cos(n\theta)$  définis par les relations

$$\begin{aligned} T_0 &= 1 \\ T_1 &= X \\ T_{n+2}(X) &= 2XT_{n+1}(X) - T_n(X) \end{aligned}$$

Chacun des éléments successifs d'une ligne est calculable en appliquant autant de fois que nécessaire la matrice  $\begin{pmatrix} 2x & -1 \\ 1 & 0 \end{pmatrix}$  au vecteur colonne  $\begin{pmatrix} x \\ 1 \end{pmatrix}$ .

$$M = \begin{pmatrix} 2x & -1 \\ 1 & 0 \end{pmatrix}, \quad M^2 = \begin{pmatrix} 4x^2 - 1 & -2x \\ 2x & -1 \end{pmatrix}, \quad M^3 = \begin{pmatrix} 8x^3 - 4x & -4x^2 + 1 \\ 4x^2 - 1 & -2x \end{pmatrix}, \quad M^4 = \begin{pmatrix} 16x^4 - 12x^2 + 1 & -8x^3 + 4x \\ 8x^3 - 4x & -4x^2 + 1 \end{pmatrix}$$

Si la matrice  $M_k$  (la puissance  $k^{ième}$  de la matrice  $M$ ) est de la forme  $\begin{pmatrix} a & b \\ -b & c \end{pmatrix}$ , alors sa puissance  $k+1^{ième}$

est de la forme  $\begin{pmatrix} 2ax + b & -a \\ a & b \end{pmatrix}$

Pour obtenir la somme de cosinus qui nous intéresse, il faut prendre la matrice initiale de cosinus  $M_{10}$ , la multiplier à gauche par une matrice d'inversion

$$Inv = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

et obtenir ainsi une matrice triangulaire avec un seul cosinus sur la dernière ligne.

$$InvM_{10} = \begin{pmatrix} \cos \frac{20\pi 1}{10} & \cos \frac{20\pi 2}{10} & \cos \frac{20\pi 3}{10} & \cos \frac{20\pi 4}{10} & \cos \frac{20\pi 5}{10} & \cos \frac{20\pi 6}{10} & \cos \frac{20\pi 7}{10} & \cos \frac{20\pi 8}{10} & \cos \frac{20\pi 9}{10} & \cos \frac{20\pi 10}{10} \\ \cos \frac{20\pi 1}{9} & \cos \frac{20\pi 2}{9} & \cos \frac{20\pi 3}{9} & \cos \frac{20\pi 4}{9} & \cos \frac{20\pi 5}{9} & \cos \frac{20\pi 6}{9} & \cos \frac{20\pi 7}{9} & \cos \frac{20\pi 8}{9} & \cos \frac{20\pi 9}{9} & 0 \\ \cos \frac{20\pi 1}{8} & \cos \frac{20\pi 2}{8} & \cos \frac{20\pi 3}{8} & \cos \frac{20\pi 4}{8} & \cos \frac{20\pi 5}{8} & \cos \frac{20\pi 6}{8} & \cos \frac{20\pi 7}{8} & \cos \frac{20\pi 8}{8} & 0 & 0 \\ \cos \frac{20\pi 1}{7} & \cos \frac{20\pi 2}{7} & \cos \frac{20\pi 3}{7} & \cos \frac{20\pi 4}{7} & \cos \frac{20\pi 5}{7} & \cos \frac{20\pi 6}{7} & \cos \frac{20\pi 7}{7} & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{6} & \cos \frac{20\pi 2}{6} & \cos \frac{20\pi 3}{6} & \cos \frac{20\pi 4}{6} & \cos \frac{20\pi 5}{6} & \cos \frac{20\pi 6}{6} & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{5} & \cos \frac{20\pi 2}{5} & \cos \frac{20\pi 3}{5} & \cos \frac{20\pi 4}{5} & \cos \frac{20\pi 5}{5} & 0 & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{4} & \cos \frac{20\pi 2}{4} & \cos \frac{20\pi 3}{4} & \cos \frac{20\pi 4}{4} & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{3} & \cos \frac{20\pi 2}{3} & \cos \frac{20\pi 3}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{2} & \cos \frac{20\pi 2}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Puis, il convient de la multiplier à droite par une matrice triangulaire de 1

$$Tri = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Cela permet d'obtenir sur la diagonale de la matrice résultat  $InvM_{10}Tri$  les sommes partielles ligne par ligne. La trace de la matrice résultat (la somme de ses éléments diagonaux) fournit la somme des diviseurs de  $n$ .

*Petite note concernant une matrice similaire à celle dont on doit chercher les puissances :* la matrice

$\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$  est rigolote : par multiplication, elle ajoute. On a ainsi :

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

$$\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} 4 & -3 \\ 3 & -2 \end{pmatrix}$$

$$\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} n+1 & -n \\ n & -n+1 \end{pmatrix}$$

On a proposé la fonction  $sumsumcos(n)$  dont les zéros sont les nombres premiers

$$sumsumcos(n) = \sum_{b=2}^{n-1} \sum_{o=1}^b \cos\left(\frac{2\pi no}{b}\right)$$

Il faudrait prouver cela, on ne sait pas le faire ; l'idée initiale provient d'une discussion sur un forum (<http://www.les-mathematiques.net/phorum/read.php?5,892412,892599>), dans laquelle on avait appris que la somme des diviseurs d'un entier était exprimable par la formule  $\sigma(n) = \sum_{k=1}^n \int_0^k \cos\left(\frac{2n\pi|x+1|}{k}\right) dx$ . Cette formule est à calculer dans l'exercice 58, page 86 du livre de J-M. de Koninck et A. Mercier *Introduction à la théorie des nombres*, Modulo Éditeur, 1994. On n'a pas pu vérifier cette référence.

On a remplacé l'intégrale par une somme et constaté par programme que la formule des doubles sommes aux bornes modifiées semble bien s'annuler pour les nombres premiers.

On souhaite calculer de telles doubles sommes en utilisant des matrices carrées  $M_n$  contenant des cosinus. Considérons la matrice  $10 \times 10$  :

$$M_{10} = \begin{pmatrix} \cos\frac{20\pi 1}{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos\frac{20\pi 1}{2} & \cos\frac{20\pi 2}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos\frac{20\pi 1}{3} & \cos\frac{20\pi 2}{3} & \cos\frac{20\pi 3}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos\frac{20\pi 1}{4} & \cos\frac{20\pi 2}{4} & \cos\frac{20\pi 3}{4} & \cos\frac{20\pi 4}{4} & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos\frac{20\pi 1}{5} & \cos\frac{20\pi 2}{5} & \cos\frac{20\pi 3}{5} & \cos\frac{20\pi 4}{5} & \cos\frac{20\pi 5}{5} & 0 & 0 & 0 & 0 & 0 \\ \cos\frac{20\pi 1}{6} & \cos\frac{20\pi 2}{6} & \cos\frac{20\pi 3}{6} & \cos\frac{20\pi 4}{6} & \cos\frac{20\pi 5}{6} & \cos\frac{20\pi 6}{6} & 0 & 0 & 0 & 0 \\ \cos\frac{20\pi 1}{7} & \cos\frac{20\pi 2}{7} & \cos\frac{20\pi 3}{7} & \cos\frac{20\pi 4}{7} & \cos\frac{20\pi 5}{7} & \cos\frac{20\pi 6}{7} & \cos\frac{20\pi 7}{7} & 0 & 0 & 0 \\ \cos\frac{20\pi 1}{8} & \cos\frac{20\pi 2}{8} & \cos\frac{20\pi 3}{8} & \cos\frac{20\pi 4}{8} & \cos\frac{20\pi 5}{8} & \cos\frac{20\pi 6}{8} & \cos\frac{20\pi 7}{8} & \cos\frac{20\pi 8}{8} & 0 & 0 \\ \cos\frac{20\pi 1}{9} & \cos\frac{20\pi 2}{9} & \cos\frac{20\pi 3}{9} & \cos\frac{20\pi 4}{9} & \cos\frac{20\pi 5}{9} & \cos\frac{20\pi 6}{9} & \cos\frac{20\pi 7}{9} & \cos\frac{20\pi 8}{9} & \cos\frac{20\pi 9}{9} & 0 \\ \cos\frac{20\pi 1}{10} & \cos\frac{20\pi 2}{10} & \cos\frac{20\pi 3}{10} & \cos\frac{20\pi 4}{10} & \cos\frac{20\pi 5}{10} & \cos\frac{20\pi 6}{10} & \cos\frac{20\pi 7}{10} & \cos\frac{20\pi 8}{10} & \cos\frac{20\pi 9}{10} & \cos\frac{20\pi 10}{10} \end{pmatrix}$$

La somme des éléments de la ligne  $d$  vaut  $d$  si  $d \mid n$  et vaut 0 sinon.

La somme de tous les éléments de la matrice vaut donc  $\sigma'(n)$ , qui est la somme des diviseurs propres de  $n$ .

Pour le calcul des éléments d'une ligne, connaissant le premier élément de la ligne, on utilise les polynômes de Tchebychev de première espèce  $T_n(\cos(\theta)) = \cos(n\theta)$  définis par les relations  $T_0(X) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ,

$$T_1(X) = \begin{pmatrix} X \\ 1 \end{pmatrix}, \begin{pmatrix} T_{n+2}(X) \\ T_{n+1}(X) \end{pmatrix} = \begin{pmatrix} 2X & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} T_{n+1}(X) \\ T_n(X) \end{pmatrix}.$$

On calcule le déterminant  $\begin{vmatrix} 2X - \lambda & -1 \\ 1 & -\lambda \end{vmatrix}$  égal à  $\lambda^2 - 2X\lambda + 1$ , les valeurs propres  $r_1 = X + i\sqrt{1 - X^2}$  et  $r_2 = X - i\sqrt{1 - X^2}$  et les vecteurs propres  $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$  et  $\begin{pmatrix} -1 \\ 1 \end{pmatrix}$ .

On a  $U_{n+1}(X) = TU_n(X) = T^n U_0(X) = P^{-1} S^n P U_0(X)$ . La matrice de passage  $P$  telle que  $T = P^{-1} S P = P^{-1} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} P$  est égale à  $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ . Sa matrice inverse est  $\frac{1}{2} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ .

Finalement,  $T_n(X) = \frac{1}{2} [(X + i\sqrt{1 - X^2})^n + (X - i\sqrt{1 - X^2})^n]$ .

Je remercie Jean Lismonde du forum *les-mathematiques.net* qui m'a fourni tous ces éléments, triviaux pour des mathématiciens.

Les éléments des matrices  $M_n$  de toutes les colonnes sauf la première sont de cette forme.

Pour obtenir la somme de cosinus qui nous intéresse, il faut prendre la matrice initiale de cosinus  $M_{10}$ , la multiplier à gauche par une matrice d'inversion

$$Inv = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

et obtenir ainsi une matrice triangulaire avec un seul cosinus sur la dernière ligne.

$$InvM_{10} = \begin{pmatrix} \cos \frac{20\pi 1}{10} & \cos \frac{20\pi 2}{10} & \cos \frac{20\pi 3}{10} & \cos \frac{20\pi 4}{10} & \cos \frac{20\pi 5}{10} & \cos \frac{20\pi 6}{10} & \cos \frac{20\pi 7}{10} & \cos \frac{20\pi 8}{10} & \cos \frac{20\pi 9}{10} & \cos \frac{20\pi 10}{10} \\ \cos \frac{20\pi 1}{9} & \cos \frac{20\pi 2}{9} & \cos \frac{20\pi 3}{9} & \cos \frac{20\pi 4}{9} & \cos \frac{20\pi 5}{9} & \cos \frac{20\pi 6}{9} & \cos \frac{20\pi 7}{9} & \cos \frac{20\pi 8}{9} & \cos \frac{20\pi 9}{9} & 0 \\ \cos \frac{20\pi 1}{8} & \cos \frac{20\pi 2}{8} & \cos \frac{20\pi 3}{8} & \cos \frac{20\pi 4}{8} & \cos \frac{20\pi 5}{8} & \cos \frac{20\pi 6}{8} & \cos \frac{20\pi 7}{8} & \cos \frac{20\pi 8}{8} & 0 & 0 \\ \cos \frac{20\pi 1}{7} & \cos \frac{20\pi 2}{7} & \cos \frac{20\pi 3}{7} & \cos \frac{20\pi 4}{7} & \cos \frac{20\pi 5}{7} & \cos \frac{20\pi 6}{7} & \cos \frac{20\pi 7}{7} & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{6} & \cos \frac{20\pi 2}{6} & \cos \frac{20\pi 3}{6} & \cos \frac{20\pi 4}{6} & \cos \frac{20\pi 5}{6} & \cos \frac{20\pi 6}{6} & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{5} & \cos \frac{20\pi 2}{5} & \cos \frac{20\pi 3}{5} & \cos \frac{20\pi 4}{5} & \cos \frac{20\pi 5}{5} & 0 & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{4} & \cos \frac{20\pi 2}{4} & \cos \frac{20\pi 3}{4} & \cos \frac{20\pi 4}{4} & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{3} & \cos \frac{20\pi 2}{3} & \cos \frac{20\pi 3}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{2} & \cos \frac{20\pi 2}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cos \frac{20\pi 1}{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Puis, il convient de la multiplier à droite par une matrice triangulaire de 1

$$Tri = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Cela permet d'obtenir sur la diagonale de la matrice résultat  $InvM_{10}Tri$  les sommes partielles ligne par ligne. La trace de la matrice résultat (la somme de ses éléments diagonaux) fournit la somme des diviseurs de  $n$ .

*Petite note concernant une matrice similaire à celle dont on doit chercher les puissances : la matrice*

$\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$  est rigolote : par multiplication, elle ajoute. On a ainsi :

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

$$\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} 4 & -3 \\ 3 & -2 \end{pmatrix}$$

$$\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} n+1 & -n \\ n & -n+1 \end{pmatrix}$$

1) Matrice de diviseurs

On est aussi émerveillé qu'Euler, lorsqu'il fournit dans l'article "Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs", une récurrence qui fournit la somme des diviseurs d'un nombre.

Mais on l'est encore plus lorsqu'on découvre que cette somme de diviseurs se calcule tout simplement par multiplication matricielle de la façon suivante : appelons  $M_n$  la matrice carrée d'entiers de taille  $n \times n$  qui contient les éléments  $M_{n,d}$  valant  $d$  si  $d \mid n$  et 0 sinon. Pour fixer les idées, fournissons  $M_{10}$ .

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 8 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 9 & 0 \\ 1 & 2 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 10 \end{pmatrix}$$

Ici,  $\sigma(10) = 18$  est la somme des éléments de la dernière ligne.

On multiplie à gauche  $M_{10}$  par une matrice diagonale de 1 "inversée" (par convention<sup>1</sup>, une matrice diagonale, par exemple la matrice *Identité*, a ses nombres sur la diagonale nord-ouest / sud-est).

$$Inv = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

On obtient la matrice suivante  $Inv.M_{10}$ , qui contient les sommes des diviseurs des nombres de 1 à 10 dans sa dernière colonne, de bas en haut.

$$\begin{pmatrix} 1 & 3 & 3 & 3 & 8 & 8 & 8 & 8 & 8 & 18 \\ 1 & 1 & 4 & 4 & 4 & 4 & 4 & 4 & 13 & 13 \\ 1 & 3 & 3 & 7 & 7 & 7 & 7 & 15 & 15 & 15 \\ 1 & 1 & 1 & 1 & 1 & 1 & 8 & 8 & 8 & 8 \\ 1 & 3 & 6 & 6 & 6 & 12 & 12 & 12 & 12 & 12 \\ 1 & 1 & 1 & 1 & 6 & 6 & 6 & 6 & 6 & 6 \\ 1 & 3 & 3 & 7 & 7 & 7 & 7 & 7 & 7 & 7 \\ 1 & 1 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 1 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Multiplions à droite le résultat du produit par une matrice d'extraction  $DerCol$  de la dernière colonne.

<sup>1</sup>qui correspond à notre lecture/écriture de gauche à droite puis de haut en bas.

$$DerCol = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

On obtient la matrice produit  $Inv.M_{10}.DerCol$  qui contient, ligne par ligne, les sommes des diviseurs des nombres de 1 à  $n$ . C'est de toute beauté !

$$\begin{pmatrix} 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 \\ 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 \\ 15 & 15 & 15 & 15 & 15 & 15 & 15 & 15 & 15 & 15 \\ 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 \\ 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 \\ 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Les sommes de diviseurs des nombres se trouvant également positionnées sur la diagonale de la matrice, un nombre premier  $p$  présentant cette particularité d'avoir sa somme de diviseurs qui vaut  $p + 1$ , les nombres premiers sont "presque" (à 1 près !) les valeurs propres de l'opérateur proposé (moyennant un "petit" retournement nord-ouest/sud-est<sup>2</sup>).

## 2) Les sommes de cosinus

On a proposé la fonction  $sumsumcos(n)$  dont il semblerait que les zéros sont les nombres premiers.

$$sumsumcos(n) = \sum_{b=2}^{n-1} \sum_{o=1}^b \cos\left(\frac{2\pi no}{b}\right)$$

Cette formule a été dérivée d'une formule pour la somme des diviseurs d'un entier

$$\sigma(n) = \sum_{k=1}^n \int_0^k \cos\left(\frac{2n\pi \lfloor x + 1 \rfloor}{k}\right) dx$$

proposée en exercice (n°58, page 86) dans le livre de J-M. de Koninck et A. Mercier *Introduction à la théorie des nombres*, Modulo Éditeur, 1994. On ne sait pas faire cet exercice, on n'a pas vérifié cette référence.

On utilise la fonction d'Euler  $\cos(x) = \frac{e^{ix} + e^{-ix}}{2}$  pour réécrire cette formule en :

$$sumsumcos(n) = \frac{1}{2} \sum_{b=2}^{n-1} \sum_{o=1}^b (e^{i\frac{2\pi no}{b}} + e^{-i\frac{2\pi no}{b}})$$

Mais on n'a pas la possibilité de pousser plus avant dans cette direction-là : les éléments de la matrice sont des réels et on manque de compétence en analyse et en théorie spectrale. Cependant, on trouve, dans plusieurs références bibliographiques, des éléments qui permettraient peut-être d'avancer sur ce chemin-là<sup>3</sup>.

<sup>2</sup>Bretagne/Provence !

<sup>3</sup>Cf [1] M. Berger and P. Gauduchon and E. Mazet, *Le spectre d'une variété Riemannienne*, p.146-147, Springer, 1971 ou bien [2] Y. De Cornulier, *Introduction au spectre du Laplacien sur une variété Riemannienne*, Exposé à l'Ecole Normale Supérieure, 2003, ou encore [3] K. R. Davidson, *C\*-Algebras by example (chapitre 6)*, Fields Institute Monographs, American Mathematical Society, 1996, ou enfin [4] H. Tal-Ezer and R. Kosloff, *Accurate and efficient scheme for propagating the time-dependent Schrödinger equation*, p.3967, J. Chem. Physics 81, 1984.

La fonction somme de cosinus proposée ci-dessus trouve les nombres premiers sur l'axe des abscisses ; c'est en quelque sorte une approche par la dimension 1, par la ligne. A propos de la conjecture de Goldbach, on a bien avancé en février 2014 lorsqu'on a "tout écrasé", i.e. lorsqu'on a représenté chaque nombre entier par un booléen qui ne conservait de toute l'information contenue dans ce nombre que son caractère de primalité (0 pour premier, 1 pour composé), oubliant ainsi toutes les autres informations qui nous semblaient pertinentes jusque-là, comme les différents restes modulaires du nombre dans les différents corps premiers.

Ici, on voudrait expérimenter un cheminement inverse : passer de la dimension 1 de l'axe des abscisses, sur lequel se trouvent les nombres premiers comme zéros d'une somme de cosinus, à la dimension juste supérieure 2, en codant les informations dont on dispose dans des matrices, passant ainsi de la séquence de nombres au tableau de nombres.

On peut par exemple définir une matrice qui contient ligne par ligne les cosinus à additionner, y compris pour les deux indices exclus pour le calcul des zéros qui correspondent aux bornes  $b = 1$  et  $b = n$ . Cette matrice  $M$  est triangulaire (haute-gauche) et contient à la position  $b, o$  l'élément  $a_{b,o} = \cos\left(\frac{2\pi n o}{b}\right)$ . En multipliant cette matrice par la matrice triangulaire haute-gauche pleine de 1, on obtient sur la diagonale les différentes sommes de cosinus à additionner et dont il faut tester l'égalité à  $1 + n$  pour savoir si  $n$  est un nombre premier (on pourrait par un artifice rajouter ce  $1 + n$  à l'une des extrémités de la diagonale par exemple). La somme des éléments diagonaux qu'il faudrait tester est la trace de la matrice. On voudrait aussi simplifier au maximum la formulation du problème, en éliminant l'appel à la fonction cosinus, en utilisant des nombres entiers.

### 3) Matrice de restes modulaires, produit de restes

On voudrait plutôt trouver une manière d'utiliser la matrice des restes modulaires ci-dessous ( $M_{i,j} = i \bmod j$ ,  $i$  variant de 1 à  $n$  et  $j$  variant de 2 à  $n - 1$ ).

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 1 & 0 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 0 & 1 & 0 & 4 & 4 & 4 & 4 & 4 & 4 \\ 1 & 2 & 1 & 0 & 5 & 5 & 5 & 5 & 5 \\ 0 & 0 & 2 & 1 & 0 & 6 & 6 & 6 & 6 \\ 1 & 1 & 3 & 2 & 1 & 0 & 7 & 7 & 7 \\ 0 & 2 & 0 & 3 & 2 & 1 & 0 & 8 & 8 \\ 1 & 0 & 1 & 4 & 3 & 2 & 1 & 0 & 9 \end{pmatrix}$$

Un nombre composé est caractérisé par le fait qu'il a au moins un reste nul dans l'une de ses divisions par un nombre supérieur ou égal à 2 et qui lui est strictement inférieur, tandis qu'un nombre premier n'a aucun tel reste nul.

On définit la fonction  $f$  suivante :

$$f(x) = x \prod_{2 \leq p < x} x \bmod p$$

Exemples :

$$f(9) = 9 \prod_{2 \leq p < 9} 9 \bmod p = 9 \times (1 \times 0 \times 1 \times 4 \times 3 \times 2 \times 1) = 0$$

$$f(13) = 13 \prod_{2 \leq p < 13} 13 \bmod p = 13 \times (1 \times 1 \times 1 \times 3 \times 1 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1) = 13 \times 63 = 819$$

$$f(15) = 15 \prod_{2 \leq p < 15} 15 \bmod p = 15 \times (1 \times 0 \times 3 \times 0 \times 3 \times 1 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1) = 0$$

$$f(25) = 25 \prod_{2 \leq p < 25} 25 \bmod p = 25 \times (1 \times 1 \times 1 \times 0 \dots) = 0$$

La fonction  $f$  associe 0 à tout nombre composé et  $\lambda p$  à tout nombre premier  $p$ .

Cela ne semble pas présenter trop d'intérêt d'en passer par un produit de restes : c'est lourd, ça oblige à utiliser le produit de Hadamard (obtention des éléments de la matrice-produit par multiplication terme à terme des éléments de 2 matrices de même taille) ; il suffirait d'être capable de tester la non-nullité de

certains éléments ciblés d'une ligne de la matrice, de l'élément de la première colonne à celui juste avant la deuxième diagonale descendante.

La "fabrication" de la matrice des restes modulaires nécessite d'être capable d'engendrer des séquences cycliques de restes. Voyons seulement sur un exemple comment se constitue une telle séquence cyclique : on veut obtenir par un produit matriciel le vecteur (ligne par exemple)

$$(1 \ 2 \ 0 \ 1 \ 2 \ 0 \ 1 \ 2 \ 0 \ 1).$$

On l'obtient par le produit  $(1 \ 2 \ 0) \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$ .

On n'arrive pas à obtenir quoi que ce soit de ce produit de restes, mais si on y arrivait, cela permettrait peut-être d'établir une dualité intéressante entre la somme des diviseurs et le produit des restes.

#### 4) Matrice de rationnels

La matrice de cosinus proposée en 2) applique la fonction cosinus à des angles réels. Obtiendrait-on des résultats intéressants en se concentrant sur les rationnels qui interviennent dans les arguments de la fonction cosinus en étudiant plutôt la matrice suivante ?

$$\begin{pmatrix} 1/2 & 2/2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/3 & 2/3 & 3/3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/4 & 2/4 & 3/4 & 4/4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/5 & 2/5 & 3/5 & 4/5 & 5/5 & 0 & 0 & 0 & 0 & 0 \\ 1/6 & 2/6 & 3/6 & 4/6 & 5/6 & 6/6 & 0 & 0 & 0 & 0 \\ 1/7 & 2/7 & 3/7 & 4/7 & 5/7 & 6/7 & 7/7 & 0 & 0 & 0 \\ 1/8 & 2/8 & 3/8 & 4/8 & 5/8 & 6/8 & 7/8 & 8/8 & 0 & 0 \\ 1/9 & 2/9 & 3/9 & 4/9 & 5/9 & 6/9 & 7/9 & 8/9 & 9/9 & 0 \end{pmatrix}$$

5) voir avec les carrés des rationnels ainsi que  $\sqrt{\frac{\lambda}{4\pi^2}}$

# Matrices, sommes de diviseurs, produits de restes

Denise Vella-Chemla

27 juillet 2015

## 1 Introduction

Dans cette note sont présentées deux méthodes qui utilisent le calcul matriciel et qui permettent de calculer aisément le résultat de deux fonctions des nombres entiers (leur somme de diviseurs ou une fonction du produit de leurs restes dans des divisions euclidiennes).

Ces méthodes fournissent deux moyens simples de distinguer les nombres premiers des nombres composés.

## 2 Matrices et sommes de diviseurs

On est aussi émerveillé qu'Euler, lorsqu'il fournit dans l'article "*Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs*", une récurrence qui fournit la somme des diviseurs d'un nombre.

Voici la table de la somme des diviseurs des entiers de 1 à 100, fournie notamment dans l'article d'Euler.

$\sigma(1) = 1$	$\sigma(21) = 32$	$\sigma(41) = 42$	$\sigma(61) = 62$	$\sigma(81) = 121$
$\sigma(2) = 3$	$\sigma(22) = 36$	$\sigma(42) = 96$	$\sigma(62) = 96$	$\sigma(82) = 126$
$\sigma(3) = 4$	$\sigma(23) = 24$	$\sigma(43) = 44$	$\sigma(63) = 104$	$\sigma(83) = 84$
$\sigma(4) = 7$	$\sigma(24) = 60$	$\sigma(44) = 84$	$\sigma(64) = 127$	$\sigma(84) = 224$
$\sigma(5) = 6$	$\sigma(25) = 31$	$\sigma(45) = 78$	$\sigma(65) = 84$	$\sigma(85) = 108$
$\sigma(6) = 12$	$\sigma(26) = 42$	$\sigma(46) = 72$	$\sigma(66) = 144$	$\sigma(86) = 132$
$\sigma(7) = 8$	$\sigma(27) = 40$	$\sigma(47) = 48$	$\sigma(67) = 68$	$\sigma(87) = 120$
$\sigma(8) = 15$	$\sigma(28) = 56$	$\sigma(48) = 124$	$\sigma(68) = 126$	$\sigma(88) = 180$
$\sigma(9) = 13$	$\sigma(29) = 30$	$\sigma(49) = 57$	$\sigma(69) = 96$	$\sigma(89) = 90$
$\sigma(10) = 18$	$\sigma(30) = 72$	$\sigma(50) = 93$	$\sigma(70) = 144$	$\sigma(90) = 234$
$\sigma(11) = 12$	$\sigma(31) = 32$	$\sigma(51) = 72$	$\sigma(71) = 72$	$\sigma(91) = 112$
$\sigma(12) = 28$	$\sigma(32) = 63$	$\sigma(52) = 98$	$\sigma(72) = 195$	$\sigma(92) = 168$
$\sigma(13) = 14$	$\sigma(33) = 48$	$\sigma(53) = 54$	$\sigma(73) = 74$	$\sigma(93) = 128$
$\sigma(14) = 24$	$\sigma(34) = 54$	$\sigma(54) = 120$	$\sigma(74) = 114$	$\sigma(94) = 144$
$\sigma(15) = 24$	$\sigma(35) = 48$	$\sigma(55) = 72$	$\sigma(75) = 124$	$\sigma(95) = 120$
$\sigma(16) = 31$	$\sigma(36) = 91$	$\sigma(56) = 120$	$\sigma(76) = 140$	$\sigma(96) = 252$
$\sigma(17) = 18$	$\sigma(37) = 38$	$\sigma(57) = 80$	$\sigma(77) = 96$	$\sigma(97) = 98$
$\sigma(18) = 39$	$\sigma(38) = 60$	$\sigma(58) = 90$	$\sigma(78) = 168$	$\sigma(98) = 171$
$\sigma(19) = 20$	$\sigma(39) = 56$	$\sigma(59) = 60$	$\sigma(79) = 80$	$\sigma(99) = 156$
$\sigma(20) = 42$	$\sigma(40) = 90$	$\sigma(60) = 168$	$\sigma(80) = 186$	$\sigma(100) = 217$

Et voilà la formule de récurrence proposée par Euler.

$$\begin{aligned} \sigma(n) = & \sigma(n-1) + \sigma(n-2) - \sigma(n-5) - \sigma(n-7) + \sigma(n-12) + \sigma(n-15) \\ & - \sigma(n-22) - \sigma(n-26) + \sigma(n-35) + \sigma(n-40) - \sigma(n-51) - \sigma(n-57) \\ & + \sigma(n-70) + \sigma(n-77) - \sigma(n-92) - \sigma(n-100) + \text{etc.} \end{aligned}$$

(on a également  $\sigma(0) = \sigma(1) = 1$  et  $\sigma(n) = 0$  si  $n < 0$ ).

Connaissant cette formule de récurrence, il est surprenant de découvrir que la somme de diviseurs se calcule simplement par multiplication matricielle de la façon suivante : appelons  $M_n$  la matrice carrée

d'entiers de taille  $n \times n$  qui contient les éléments  $M_{n,d}$  valant  $d$  si  $d \mid n$  et 0 sinon. Pour fixer les idées, fournissons  $M_{10}$ .

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 8 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 9 & 0 \\ 1 & 2 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 10 \end{pmatrix}$$

Ici,  $\sigma(10) = 18$  est la somme des éléments de la dernière ligne de  $M_{10}$ .

On multiplie à gauche  $M_{10}$  par une matrice diagonale de 1 "inversée" (par convention<sup>1</sup>, une matrice diagonale, par exemple la matrice *Identité*, a ses nombres sur la diagonale nord-ouest / sud-est).

$$Inv = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

On obtient la matrice produit suivante  $S1 = Inv.M_{10}$ , qui contient les sommes des diviseurs des nombres de 1 à 10 dans sa dernière colonne, de bas en haut.

$$S1 = \begin{pmatrix} 1 & 3 & 3 & 3 & 8 & 8 & 8 & 8 & 8 & 18 \\ 1 & 1 & 4 & 4 & 4 & 4 & 4 & 4 & 13 & 13 \\ 1 & 3 & 3 & 7 & 7 & 7 & 7 & 15 & 15 & 15 \\ 1 & 1 & 1 & 1 & 1 & 1 & 8 & 8 & 8 & 8 \\ 1 & 3 & 6 & 6 & 6 & 12 & 12 & 12 & 12 & 12 \\ 1 & 1 & 1 & 1 & 6 & 6 & 6 & 6 & 6 & 6 \\ 1 & 3 & 3 & 7 & 7 & 7 & 7 & 7 & 7 & 7 \\ 1 & 1 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 1 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Multiplions à droite la matrice  $S1$  par une matrice d'extraction  $DerCol$  de la dernière colonne.

$$DerCol = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

On obtient la matrice produit  $S2 = S1.DerCol$  qui contient, ligne par ligne et de bas en haut, les sommes des diviseurs des nombres de 1 à  $n$ . C'est de toute beauté !

<sup>1</sup>qui correspond à notre lecture/écriture de gauche à droite puis de haut en bas.

$$S2 = \begin{pmatrix} 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 \\ 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 \\ 15 & 15 & 15 & 15 & 15 & 15 & 15 & 15 & 15 & 15 \\ 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 \\ 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 \\ 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Les sommes de diviseurs des nombres se trouvant également positionnées sur la diagonale de la matrice, un nombre premier  $p$  présentant cette particularité d'avoir sa somme de diviseurs qui vaut  $p + 1$ , les nombres premiers sont "presque" (à 1 près) les valeurs propres de l'opérateur produit proposé, moyennant un retournement nord-ouest/sud-est de la matrice résultat. Un tel retournement s'effectue de la façon suivante :  $S = (S2.Inv)^T.Inv$

$$S = \begin{pmatrix} 1 & 3 & 4 & 7 & 6 & 12 & 8 & 15 & 13 & 18 \\ 1 & 3 & 4 & 7 & 6 & 12 & 8 & 15 & 13 & 18 \\ 1 & 3 & 4 & 7 & 6 & 12 & 8 & 15 & 13 & 18 \\ 1 & 3 & 4 & 7 & 6 & 12 & 8 & 15 & 13 & 18 \\ 1 & 3 & 4 & 7 & 6 & 12 & 8 & 15 & 13 & 18 \\ 1 & 3 & 4 & 7 & 6 & 12 & 8 & 15 & 13 & 18 \\ 1 & 3 & 4 & 7 & 6 & 12 & 8 & 15 & 13 & 18 \\ 1 & 3 & 4 & 7 & 6 & 12 & 8 & 15 & 13 & 18 \\ 1 & 3 & 4 & 7 & 6 & 12 & 8 & 15 & 13 & 18 \\ 1 & 3 & 4 & 7 & 6 & 12 & 8 & 15 & 13 & 18 \end{pmatrix}$$

### 3 Matrices et produits de restes modulaires

On voudrait également trouver une manière d'utiliser la matrice des restes modulaires ci-dessous ( $M_{i,j} = i \bmod j$ ,  $i$  variant de 1 à  $n$  et  $j$  variant de 2 à  $n - 1$ ).

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 1 & 0 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 0 & 1 & 0 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 1 & 2 & 1 & 0 & 5 & 5 & 5 & 5 & 5 & 5 \\ 0 & 0 & 2 & 1 & 0 & 6 & 6 & 6 & 6 & 6 \\ 1 & 1 & 3 & 2 & 1 & 0 & 7 & 7 & 7 & 7 \\ 0 & 2 & 0 & 3 & 2 & 1 & 0 & 8 & 8 & 8 \\ 1 & 0 & 1 & 4 & 3 & 2 & 1 & 0 & 9 & 9 \\ 0 & 1 & 2 & 0 & 4 & 3 & 2 & 1 & 0 & 10 \end{pmatrix}$$

Un nombre composé est caractérisé par le fait qu'il a au moins un reste nul dans l'une de ses divisions par un nombre supérieur ou égal à 2 et qui lui est strictement inférieur, tandis qu'un nombre premier n'a aucun tel reste nul.

On définit la fonction  $f$  suivante :

$$f(x) = x \prod_{2 \leq p < x} x \bmod p$$

Exemples :

$$f(9) = 9 \prod_{2 \leq p < 9} 9 \bmod p = 9 \times (1 \times 0 \times 1 \times 4 \times 3 \times 2 \times 1) = 0$$

$$f(13) = 13 \prod_{2 \leq p < 13} 13 \bmod p = 13 \times (1 \times 1 \times 1 \times 3 \times 1 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1) = 13 \times 63 = 819$$

$$f(15) = 15 \prod_{2 \leq p < 15} 15 \bmod p = 15 \times (1 \times 0 \times 3 \times 0 \times 3 \times 1 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1) = 0$$

$$f(25) = 25 \prod_{2 \leq p < 25} 25 \bmod p = 25 \times (1 \times 1 \times 1 \times 0 \dots) = 0$$

La fonction  $f$  associe 0 à tout nombre composé et  $\lambda p$  à tout nombre premier  $p$ .

Cette approche est difficile à mener à son terme : pour calculer le produit de plusieurs éléments d'une même ligne, il semble nécessaire d'utiliser le produit matriciel de Hadamard (obtention des éléments d'une matrice-produit par multiplication terme à terme des éléments de 2 matrices de même taille). Ce produit n'est pas le produit utilisé habituellement en calcul matriciel. L'objectif essentiel est d'être capable de tester la non-nullité de certains éléments ciblés d'une ligne de la matrice, de l'élément de la première colonne à celui juste avant la deuxième diagonale descendante. Cette méthode n'est pas assez développée.

La "fabrication" de la matrice des restes modulaires nécessite d'être capable d'engendrer des séquences cycliques de restes. Voyons seulement sur un exemple comment se constitue une telle séquence cyclique : on veut obtenir par un produit matriciel le vecteur (ligne par exemple)

$$(1 \ 2 \ 0 \ 1 \ 2 \ 0 \ 1 \ 2 \ 0 \ 1).$$

On l'obtient par le produit  $(1 \ 2 \ 0) \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$ .

Les deux approches suggérées permettraient peut-être d'établir un lien entre la somme des diviseurs et le produit des restes d'un entier.

## Bibliographie

[1] L. Euler, *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs*, Opera posthuma, Arithmetica, Exhib. Berol. 1747 Junii 22, Conf. Comment. arithm. Prooem. pag. XVIII. N. 57 et Suppl. Prooem. N. 1.

# Matrices et divisibilité

Denise Vella-Chemla

29 juillet 2015

## 1 Introduction

Dans cette note sont présentées deux méthodes qui utilisent le calcul matriciel pour calculer la somme des diviseurs des entiers et caractériser les nombres premiers.

## 2 Matrices et sommes de diviseurs

On est aussi émerveillé qu'Euler, lorsqu'il fournit dans l'article "*Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs*", une formule par récurrence qui calcule la somme des diviseurs d'un nombre.

Voici la table de la somme des diviseurs des entiers de 1 à 100, présentée en section 4 de la note d'Euler.

$\sigma(1) = 1$	$\sigma(21) = 32$	$\sigma(41) = 42$	$\sigma(61) = 62$	$\sigma(81) = 121$
$\sigma(2) = 3$	$\sigma(22) = 36$	$\sigma(42) = 96$	$\sigma(62) = 96$	$\sigma(82) = 126$
$\sigma(3) = 4$	$\sigma(23) = 24$	$\sigma(43) = 44$	$\sigma(63) = 104$	$\sigma(83) = 84$
$\sigma(4) = 7$	$\sigma(24) = 60$	$\sigma(44) = 84$	$\sigma(64) = 127$	$\sigma(84) = 224$
$\sigma(5) = 6$	$\sigma(25) = 31$	$\sigma(45) = 78$	$\sigma(65) = 84$	$\sigma(85) = 108$
$\sigma(6) = 12$	$\sigma(26) = 42$	$\sigma(46) = 72$	$\sigma(66) = 144$	$\sigma(86) = 132$
$\sigma(7) = 8$	$\sigma(27) = 40$	$\sigma(47) = 48$	$\sigma(67) = 68$	$\sigma(87) = 120$
$\sigma(8) = 15$	$\sigma(28) = 56$	$\sigma(48) = 124$	$\sigma(68) = 126$	$\sigma(88) = 180$
$\sigma(9) = 13$	$\sigma(29) = 30$	$\sigma(49) = 57$	$\sigma(69) = 96$	$\sigma(89) = 90$
$\sigma(10) = 18$	$\sigma(30) = 72$	$\sigma(50) = 93$	$\sigma(70) = 144$	$\sigma(90) = 234$
$\sigma(11) = 12$	$\sigma(31) = 32$	$\sigma(51) = 72$	$\sigma(71) = 72$	$\sigma(91) = 112$
$\sigma(12) = 28$	$\sigma(32) = 63$	$\sigma(52) = 98$	$\sigma(72) = 195$	$\sigma(92) = 168$
$\sigma(13) = 14$	$\sigma(33) = 48$	$\sigma(53) = 54$	$\sigma(73) = 74$	$\sigma(93) = 128$
$\sigma(14) = 24$	$\sigma(34) = 54$	$\sigma(54) = 120$	$\sigma(74) = 114$	$\sigma(94) = 144$
$\sigma(15) = 24$	$\sigma(35) = 48$	$\sigma(55) = 72$	$\sigma(75) = 124$	$\sigma(95) = 120$
$\sigma(16) = 31$	$\sigma(36) = 91$	$\sigma(56) = 120$	$\sigma(76) = 140$	$\sigma(96) = 252$
$\sigma(17) = 18$	$\sigma(37) = 38$	$\sigma(57) = 80$	$\sigma(77) = 96$	$\sigma(97) = 98$
$\sigma(18) = 39$	$\sigma(38) = 60$	$\sigma(58) = 90$	$\sigma(78) = 168$	$\sigma(98) = 171$
$\sigma(19) = 20$	$\sigma(39) = 56$	$\sigma(59) = 60$	$\sigma(79) = 80$	$\sigma(99) = 156$
$\sigma(20) = 42$	$\sigma(40) = 90$	$\sigma(60) = 168$	$\sigma(80) = 186$	$\sigma(100) = 217$

Et voilà la formule de récurrence qu'il a trouvée.

$$\left\{ \begin{array}{l} \sigma(n) = \sigma(n-1) + \sigma(n-2) - \sigma(n-5) - \sigma(n-7) + \sigma(n-12) + \sigma(n-15) \\ \quad - \sigma(n-22) - \sigma(n-26) + \sigma(n-35) + \sigma(n-40) - \sigma(n-51) - \sigma(n-57) \\ \quad + \sigma(n-70) + \sigma(n-77) - \sigma(n-92) - \sigma(n-100) + \text{etc.} \\ \sigma(0) = \sigma(1) = 1 \text{ et } \sigma(n) = 0 \text{ si } n < 0. \end{array} \right.$$

Pour  $p$  un nombre premier,  $\sigma(p) = p + 1$ .

On propose de calculer la somme des diviseurs par multiplication matricielle.

Appelons  $M = (m_{nd})$  la matrice carrée d'entiers de taille  $n \times n$  qui contient les éléments  $m_{nd} = d$  si  $d \mid n$  et  $m_{nd} = 0$  sinon.

Voici  $M$  pour  $n = 10$ .

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & \boxed{3} & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 8 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 9 & 0 \\ 1 & 2 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 10 \end{pmatrix}$$

Le nombre 3 encadré correspond à  $3 \mid 6$ .

$\sigma(10) = 18$  est la somme des éléments de la dernière ligne de  $M$ .

Multiplions  $M$  par la matrice  $U$  "pleine de 1".

$$U = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$S = MU = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 \\ 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\ 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 \\ 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 \\ 15 & 15 & 15 & 15 & 15 & 15 & 15 & 15 & 15 & 15 \\ 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 \\ 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 & 18 \end{pmatrix}$$

La matrice  $S$  présente l'intérêt d'avoir sur sa diagonale pour un entier  $i$  donné la somme de ses diviseurs  $S_{i,i} = \sigma(i)$ .

### 3 Matrice booléenne de divisibilité

Dans cette seconde approche, on utilise une matrice de divisibilité, pour les nombres entiers supérieurs strictement à 1. Elle fait apparaître les diviseurs d'un entier  $n$  dits non-triviaux, i.e. différents de 1 et de  $n$ .

Appelons  $M' = (m'_{nd})$  la matrice carrée d'entiers de taille  $n \times n$  qui contient les éléments  $m'_{nd} = 1$  si  $d \mid n$  et  $d \neq n$  et  $m'_{nd} = 0$  sinon.

Voici  $M'$ , de taille  $9 \times 9$ , fournissant les diviseurs non-triviaux des entiers de 2 à 10.

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

Le nombre 1 encadré correspond à  $3 \mid 6$ .

Un nombre premier n'a aucun diviseur non-trivial, sa ligne ne contient que des 0, un nombre composé en a au moins 1, sa ligne contient un 1 au moins.

Définissons deux matrices utiles :  $Z$  le vecteur colonne nul et  $N$  la matrice carrée contenant les nombres entiers successifs, sauf 1, sur sa diagonale.

$$Z = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$N = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 10 \end{pmatrix}$$

On définit le produit booléen de 2 matrices, qui projette dans un vecteur colonne le  $\vee$  booléen de tous les éléments d'une ligne :

Soient  $A = (a_{ij})$  une matrice  $n \times p$  et  $B = (b_{ij})$  une matrice  $p \times q$ . Alors le produit booléen (noté  $\vee$ )  $C = A \vee B$  est une matrice  $n \times q$  dont les coefficients  $c_{ij}$  sont définis par :

$$c_{ij} = \sum_{k=1}^p a_{ik} \vee b_{kj}$$

Le produit booléen de  $M'$  par un vecteur colonne nul  $Z$  permet d'obtenir un vecteur colonne  $P$  contenant des 0 aux positions des nombres premiers.

$$P = M' \vee Z = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \vee \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

Ce vecteur colonne  $P$ , dont on prend la négation  $\neg P$ , multiplié selon la multiplication matricielle habituelle par la matrice carrée  $N$  permet d'obtenir la matrice  $S'$  suivante dont l'élément diagonal  $S'_{i,i} = i$  si  $i$  est premier et  $S'_{i,i} = 0$  sinon.

$$S' = N\neg P = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 10 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

## Bibliographie

[1] L. Euler, *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs*, Bibliothèque impartiale 3, 1751, S. 10-31. In : Opera omnia (1) 2, Leipzig, Berlin 1915, S. 241-253 (E 175).

1) Introduction

Dans cette note, on joue avec des spectres de matrices. On cherche à caractériser l'ensemble des nombres premiers, la clef se cache peut-être dans un opérateur subtil.

2) Définition

Extrait de [1] : Soit  $A$  une matrice carrée d'ordre  $n$  à valeurs réelles ou complexes ; on dit que  $\lambda \in \mathbb{C}$  est une *valeur propre* de  $A$  s'il existe un vecteur non nul  $x \in \mathbb{C}^n$  tel que  $Ax = \lambda x$ . Le vecteur  $x$  est le vecteur propre associé à la valeur propre  $\lambda$  et l'ensemble des valeurs propres de  $A$  est appelé *spectre* de  $A$ . On le note  $\sigma(A)$ .

Extrait de [2] : les valeurs propres d'une matrice  $A \in \mathbb{C}^{n \times n}$  sont les  $n$  racines de son *polynôme caractéristique*  $p(z) = \det(zI - A)$ . L'ensemble de racines est appelé le spectre.

Si  $\sigma(A) = \{\lambda_1, \dots, \lambda_n\}$ ,  $\det(A) = \lambda_1 \lambda_2 \dots \lambda_n$ .

3) Exemples jouets

Une récurrence simple calcule la somme des diviseurs :

$$\sigma(n) = \frac{12}{n^2(n-1)} \sum_{k=1}^{n-1} (-5k^2 + 5kn - n^2) \sigma(k) \sigma(n-k)$$

Un programme récursif la calcule trivialement, il suffit d'initialiser  $\sigma(1) = 1$  et la somme des diviseurs est effectivement trouvée pour les entiers successifs sans que ne soit jamais testé aucun reste de division. Les nombres premiers  $p$  sont aisément caractérisés par le fait que pour eux,  $\sigma(p) = p + 1$ .

Similairement, on cherche ici à être surpris par les opérateurs matriciels, en testant certains calculs de spectre, un peu au hasard, et en espérant le coup de chance, qui ferait apparaître les nombres premiers par exemple. On utilise le logiciel *Scilab* qui fournit un spectre de matrice à la demande.

3a) Matrices-gnomons

Si  $A_1 = \begin{pmatrix} 1 \end{pmatrix}$ ,  
 $\text{Spec}(A_1) = \{1\}$ .

Si  $A_2 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$ ,  
 $\text{Spec}(A_2) = \{-0.5615528, 3.5615528\}$ .

Si  $A_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \\ 3 & 3 & 3 \end{pmatrix}$ ,  
 $\text{Spec}(A_3) = \{-1.1776168, -0.3389217, 7.5165385\}$ .

Si  $A_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 2 & 3 & 4 \\ 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 \end{pmatrix}$ ,  
 $\text{Spec}(A_4) = \{-2.0531158, -0.5146428, -0.2943265, 12.862085\}$ .

Si  $A_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 3 & 4 & 5 \\ 3 & 3 & 3 & 4 & 5 \\ 4 & 4 & 4 & 4 & 5 \\ 5 & 5 & 5 & 5 & 5 \end{pmatrix}$ ,  
 $\text{Spec}(A_5) = \{-3.185096, -0.7498856, -0.3857228, -0.2769322, 19.597637\}$ .

$$\text{Si } A_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 2 & 3 & 4 & 5 & 6 \\ 3 & 3 & 3 & 4 & 5 & 6 \\ 4 & 4 & 4 & 4 & 5 & 6 \\ 5 & 5 & 5 & 5 & 5 & 6 \\ 6 & 6 & 6 & 6 & 6 & 6 \end{pmatrix},$$

$$\text{Spec}(A_6) = \{-4.5728999, -1.040565, -0.5065657, -0.3347785, -0.2681985, 27.723008\}.$$

On a compris le principe, on n'écrit plus les matrices.

$$\text{Spec}(A_7) = \{-6.2163067, -1.3855235, -0.6529671, -0.4115027, -0.3086653, -0.2631553, 37.238121\}.$$

$$\text{Spec}(A_8) = \{-8.1152237, -1.7843181, -0.8236182, -0.5037270, -0.3628137, -0.2932653, -0.2599676, 48.142933\}.$$

$$\text{Spec}(A_9) = \{-10.269606, -2.2367501, -1.0179672, -0.6101633, -0.4277919, -0.3339874, -0.2833391, -0.2578199, 60.437425\}.$$

$$\text{Spec}(A_{10}) = \{-12.679428, -2.7427181, -1.2357461, -0.7302233, -0.502402-0.3829322, -0.3152953, -0.2765327, -0.2563021, 74.12158\}.$$

$$\text{Spec}(A_{11}) = \{-15.344678, -3.3021658, -1.4768107, -0.8636042, -0.5860603, -0.4390148, -0.3538327, -0.3023903, -0.2716470, -0.2551890, 89.195392\}.$$

$$\text{Spec}(A_{12}) = \{-18.265345, -3.9150598, -1.7410776, -1.0101359, -0.6784516, -0.5016770, -0.3979809, -0.3337051, -0.2930613, -0.2680135, -0.2543478, 105.65885\}.$$

On a l'impression que la dernière valeur du spectre est un nombre premier quand  $n$  est premier mais pour  $n = 13$ , patatras, 123 est composé.

$$\text{Spec}(A_{13}) = \{-21.441423, -4.5813793, -2.0284957, -1.1697163, -0.7793923, -0.5706049, -0.4472171, -0.3696142, -0.3191154, -0.2860751, -0.2652338, -0.2536965, 123.51196\}.$$

### 3b) Matrices de suites arithmétiques

Dans cette section et les deux sections suivantes sont effectués quelques calculs de spectre. Les contenus des matrices se déduisent des titres des sections.

$$\text{Si } B_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 7 & 9 \\ 1 & 4 & 7 & 10 & 13 \\ 1 & 5 & 9 & 13 & 17 \end{pmatrix},$$

$$\text{Spec}(B_5) = \{-2.222 \cdot 10^{-15}, -1.415 \cdot 10^{-16}, 1.791 \cdot 10^{-16}, 1.4921894, 33.507811\} \text{ (les nombres minuscules sont sûrement des zéros).}$$

$$\text{Si } B_6 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 7 & 9 & 11 \\ 1 & 4 & 7 & 10 & 13 & 16 \\ 1 & 5 & 9 & 13 & 17 & 21 \\ 1 & 6 & 11 & 16 & 21 & 26 \end{pmatrix},$$

$$\text{Spec}(B_6) = \{-1.288 \cdot 10^{-15}, -8.990 \cdot 10^{-17}, 8.547 \cdot 10^{-16}, 1.266 \cdot 10^{-14}, 1.7728352, 59.227165\}.$$

Abandon.

On peut également tester une matrice symétrique,  $5 \times 5$ .

$$\text{Si } B'_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 6 & 8 & 10 \\ 3 & 6 & 9 & 12 & 15 \\ 4 & 8 & 12 & 16 & 20 \\ 5 & 10 & 15 & 20 & 25 \end{pmatrix},$$

$$\text{Spec}(B'_5) = \{0, 0, 0, 3.553 \cdot 10^{-15}, 55\}.$$

Il se trouve que  $55 = 5 \times 11$ , on continue.

$$\text{Spec}(B'_6) = \{-2.560 \cdot 10^{-15}, 0, 0, 0, 2.560 \cdot 10^{-15}, 91\}.$$

Il se trouve que  $91 = 7 \times 13$ , on continue.

$$\text{Spec}(B'_6) = \{-8.000 \cdot 10^{-15}, -2.434 \cdot 10^{-16}, -1.525 \cdot 10^{-64}, 4.911 \cdot 10^{-32}, 1.279 \cdot 10^{-15}, 6.298; 10^{-15}, 140\}.$$

Il se trouve que  $140 = 2^2 \times 5 \times 7$ , abandon.

### 3c) Matrices de suites de puissances

$$\text{Si } C_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 9 & 16 & 25 \\ 1 & 8 & 27 & 64 & 125 \\ 1 & 16 & 81 & 256 & 625 \end{pmatrix},$$

$$\text{Spec}(C_5) = \{680.92666, 17.658486, 1.9730603, 0.4123561, 0.0294392\}.$$

Même si 17 est premier, les nombres grossissent trop vite, abandon.

En cherchant la symétrie, on retrouve les puissances de 2.

$$\text{Si } C'_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 \\ 1 & 4 & 16 & 64 & 256 \\ 1 & 8 & 64 & 512 & 4096 \\ 1 & 16 & 256 & 4096 & 65536 \end{pmatrix},$$

$$\text{Spec}(C'_5) = \{0.1357339, 1.1891004, 7.2373579, 264.40988, 65794.028\}.$$

Notre énervement face à la notion de puissance perdure, les puissances, même de 2 comme dans la légende de l'échiquier de Sissa, grossissent trop vite.

### 3d) Matrices-compagnons les plus élémentaires

On lit que la détermination des zéros d'un polynôme de degré  $\leq n$  à coefficients réels

$$p_n(x) = \sum_{k=0}^n a_k x^k = a_0 + a_1 x + \dots + a_n x^n, \text{ avec } a_n \neq 0 \text{ et } a_k \in \mathbb{R} \text{ et } k = 0, \dots, n$$

est équivalente à la détermination du spectre de la matrice de Frobenius  $D \in \mathbb{R}^{n \times n}$  associée à  $p_n$  appelée matrice compagnon (contenant des ratios de coefficients du polynôme dans la première ligne, des 1 dans la diagonale immédiatement en-dessous de la diagonale principale et des 0 partout ailleurs).

$$D = \begin{pmatrix} -(a_{n-1}/a_n) & -(a_{n-2}/a_n) & \dots & -(a_0/a_n) \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

On calcule deux spectres, au hasard :

$$\text{Si } D_5 = \begin{pmatrix} -1/6 & -1/5 & -1/4 & -1/3 & -1/2 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\text{Spec}(D_5) = \{0.6010558 + 0.6605334i, 0.6010558 - 0.6605334i, \\ -0.7196965, \\ -0.3245409 + 0.6894803i, -0.3245409 - 0.6894803i\}.$$

$$\text{Si } D_6 = \begin{pmatrix} -1/5 & -1/4 & -1/3 & -1/2 & -1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\text{Spec}(D_6) = \{0.7436122 + 0.7498717i, 0.7436122 - 0.7498717i, \\ -0.9501551, \\ -0.3685346 + 0.8988140i, -0.3685346 - 0.8988140i\}.$$

$$\text{Enfin, si } D'_5 = \begin{pmatrix} -5/6 & -4/6 & -3/6 & -2/6 & -1/6 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\text{Spec}(D'_5) = \{0.6500656 + 0.6715345i, 0.6500656 - 0.6715345i \\ -0.8150367 \\ -0.3258806 + 0.7720611i, -0.3258806 - 0.7720611i\}.$$

$$\text{Enfin, si } D''_5 = \begin{pmatrix} -5/5 & -4/5 & -3/5 & -2/5 & -1/5 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\text{Spec}(D''_5) = \{0.2749880 + 0.6837609i, 0.2749880 - 0.6837609i \\ -0.7195054 \\ -0.4152353 + 0.5825408i, -0.4152353 - 0.5825408i\}.$$

On voit apparaître dans ces deux derniers exemples des nombres complexes et une certaine symétrie entre les différentes valeurs propres. Il faudra tester d'autres possibilités avec des nombres plus grands sur la première ligne car les nombres trouvés sont trop petits.

### 3e) Ellipsoïde de révolution

Une ellipse rend invariante l'aire délimitée par un triangle dont les sommets sont le point décrivant l'orbite elliptique et les deux points focaux. On aimerait trouver un opérateur en lien avec une telle surface elliptique ou même avec un volume ellipsoïdal et calculer son spectre, pour voir.

### Bibliographie

[1] A. Quarteroni, R. Sacco, F. Saleri, *Méthodes numériques (algorithmes, analyse et applications)*, Springer, 2007.

[2] G. H. Golub, C. F. Van Loan, *Matrix computations (4th edition)*, Johns Hopkins University editors, 2013.

[3] Site Images des mathématiques : article "De l'autre côté du miroir" : "*Spectre*"  
<http://images.math.cnrs.fr/Spectre.html>

# Matrices et indicateur d'Euler

Denise Vella-Chemla

1er août 2015

## 1 Introduction

Dans une note toute récente, on a montré comment calculer la somme des diviseurs des nombres successifs en effectuant un simple calcul matriciel. Selon une méthode similaire, on calcule l'indicateur d'Euler en utilisant une matrice contenant des pgcd.

## 2 Matrices et indicateur d'Euler

L'indicateur d'Euler fournit pour un nombre donné  $x$  le nombre  $\varphi(x)$  de nombres qui lui sont inférieurs et qui sont premiers à lui.

Voici la table des indicateurs d'Euler des entiers de 1 à 100.

$\varphi(1) = 1$	$\varphi(21) = 12$	$\varphi(41) = 40$	$\varphi(61) = 60$	$\varphi(81) = 54$
$\varphi(2) = 1$	$\varphi(22) = 10$	$\varphi(42) = 12$	$\varphi(62) = 30$	$\varphi(82) = 40$
$\varphi(3) = 2$	$\varphi(23) = 22$	$\varphi(43) = 42$	$\varphi(63) = 36$	$\varphi(83) = 82$
$\varphi(4) = 2$	$\varphi(24) = 8$	$\varphi(44) = 20$	$\varphi(64) = 32$	$\varphi(84) = 24$
$\varphi(5) = 4$	$\varphi(25) = 20$	$\varphi(45) = 24$	$\varphi(65) = 48$	$\varphi(85) = 64$
$\varphi(6) = 2$	$\varphi(26) = 12$	$\varphi(46) = 22$	$\varphi(66) = 20$	$\varphi(86) = 42$
$\varphi(7) = 6$	$\varphi(27) = 18$	$\varphi(47) = 46$	$\varphi(67) = 66$	$\varphi(87) = 56$
$\varphi(8) = 4$	$\varphi(28) = 12$	$\varphi(48) = 16$	$\varphi(68) = 32$	$\varphi(88) = 40$
$\varphi(9) = 6$	$\varphi(29) = 28$	$\varphi(49) = 42$	$\varphi(69) = 44$	$\varphi(89) = 88$
$\varphi(10) = 4$	$\varphi(30) = 8$	$\varphi(50) = 20$	$\varphi(70) = 24$	$\varphi(90) = 24$
$\varphi(11) = 10$	$\varphi(31) = 30$	$\varphi(51) = 32$	$\varphi(71) = 70$	$\varphi(91) = 72$
$\varphi(12) = 4$	$\varphi(32) = 16$	$\varphi(52) = 24$	$\varphi(72) = 24$	$\varphi(92) = 44$
$\varphi(13) = 12$	$\varphi(33) = 20$	$\varphi(53) = 52$	$\varphi(73) = 72$	$\varphi(93) = 60$
$\varphi(14) = 6$	$\varphi(34) = 16$	$\varphi(54) = 18$	$\varphi(74) = 36$	$\varphi(94) = 46$
$\varphi(15) = 8$	$\varphi(35) = 24$	$\varphi(55) = 40$	$\varphi(75) = 40$	$\varphi(95) = 72$
$\varphi(16) = 8$	$\varphi(36) = 12$	$\varphi(56) = 24$	$\varphi(76) = 36$	$\varphi(96) = 32$
$\varphi(17) = 16$	$\varphi(37) = 36$	$\varphi(57) = 36$	$\varphi(77) = 60$	$\varphi(97) = 96$
$\varphi(18) = 6$	$\varphi(38) = 18$	$\varphi(58) = 28$	$\varphi(78) = 24$	$\varphi(98) = 42$
$\varphi(19) = 18$	$\varphi(39) = 24$	$\varphi(59) = 58$	$\varphi(79) = 78$	$\varphi(99) = 60$
$\varphi(20) = 8$	$\varphi(40) = 16$	$\varphi(60) = 16$	$\varphi(80) = 32$	$\varphi(100) = 40$

Pour  $p$  un nombre premier,  $\varphi(p) = p - 1$ .

On propose de calculer l'indicateur d'Euler par multiplication matricielle.

Appelons  $M = (m_{nd})$  la matrice carrée de booléens de taille  $n \times n$  qui contient les éléments  $m_{nd} = (\text{pgcd}(d, n + 1) = 1)$  si  $d \leq n$  et  $m_{nd} = 0$  sinon.

Voici  $M$  pour  $n = 6$ .

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

Le 1 encadré est le booléen correspondant à  $\text{pgcd}(4, 3) = 1$ . En annexe est fournie la matrice pour  $n = 23$  de façon à ce que soit notée les périodicités booléennes “rigolotes” (une manière de dire qu’on ne risque pas d’y trouver une quelconque périodicité) dans les colonnes correspondant aux nombres 6 et 10.

Multiplions  $M$  par la matrice  $U$  “pleine de 1”.

$$U = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$S = MU = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 \\ 4 & 4 & 4 & 4 & 4 & 4 \\ 2 & 2 & 2 & 2 & 2 & 2 \\ 6 & 6 & 6 & 6 & 6 & 6 \end{pmatrix}$$

La matrice  $S$  présente l’intérêt d’avoir sur sa diagonale pour un entier  $i$  son indicateur d’Euler  $S_{i,i} = \varphi(i + 1)$ .

## Annexe

Noter les périodicités des colonnes  $n = 6$  et  $n = 10$  marquées d’une croix.



# Distance suprême

Denise Vella-Chemla

24/8/2015

## 1 Restes de divisions euclidiennes

Dans la suite, on note  $p \bmod k$  le reste de la division euclidienne de  $p$  par  $k$ .

$$p \bmod k = p - \left\lfloor \frac{p}{k} \right\rfloor k$$

Observons la table de restes qui fournit pour les entiers de 2 à 20 leur reste dans les divisions euclidiennes par les entiers de 2 à 20.

<i>mod</i>	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	0	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3	1	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
4	0	1	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
5	1	2	1	0	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
6	0	0	2	1	0	6	6	6	6	6	6	6	6	6	6	6	6	6	6
7	1	1	3	2	1	0	7	7	7	7	7	7	7	7	7	7	7	7	7
8	0	2	0	3	2	1	0	8	8	8	8	8	8	8	8	8	8	8	8
9	1	0	1	4	3	2	1	0	9	9	9	9	9	9	9	9	9	9	9
10	0	1	2	0	4	3	2	1	0	10	10	10	10	10	10	10	10	10	10
11	1	2	3	1	5	4	3	2	1	0	11	11	11	11	11	11	11	11	11
12	0	0	0	2	0	5	4	3	2	1	0	12	12	12	12	12	12	12	12
13	1	1	1	3	1	6	5	4	3	2	1	0	13	13	13	13	13	13	13
14	0	2	2	4	2	0	6	5	4	3	2	1	0	14	14	14	14	14	14
15	1	0	3	0	3	1	7	6	5	4	3	2	1	0	15	15	15	15	15
16	0	1	0	1	4	2	0	7	6	5	4	3	2	1	0	16	16	16	16
17	1	2	1	2	5	3	1	8	7	6	5	4	3	2	1	0	17	17	17
18	0	0	2	3	0	4	2	0	8	7	6	5	4	3	2	1	0	18	18
19	1	1	3	4	1	5	3	1	9	8	7	6	5	4	3	2	1	0	19
20	0	2	0	0	2	6	4	2	0	9	8	7	6	5	4	3	2	1	0

On définit pour les entiers supérieurs ou égaux à 2 la fonction  $sr(x)$  ( $sr$  pour somme des restes) par :

$$sr(x) = \sum_{2 \leq k < x} x \bmod k$$

La fonction  $sr$  prend les valeurs suivantes :

$$\begin{aligned}
 sr(2) &= 0 \\
 sr(3) &= 1 \\
 sr(4) &= 1 \\
 sr(5) &= 4 \\
 sr(6) &= 3 \\
 sr(7) &= 8 \\
 sr(8) &= 8 \\
 sr(9) &= 12 \\
 sr(10) &= 13 \\
 sr(11) &= 22 \\
 sr(12) &= 17 \\
 sr(13) &= 28 \\
 sr(14) &= 31 \\
 sr(15) &= 36 \\
 sr(16) &= 36 \\
 sr(17) &= 51 \\
 sr(18) &= 47 \\
 sr(19) &= 64 \\
 sr(20) &= 61
 \end{aligned}$$

Chaque colonne de la table des restes, trivialement, contient une suite cyclique de nombres “retombant” régulièrement à zéro.

Un nombre premier n’étant divisible par aucun nombre qui lui soit strictement inférieur, à part 1, on comprend aisément que tous les restes d’un nombre premier  $p$  sont des incréments stricts des restes du nombre  $p - 1$ . On définit la distance :

$$\begin{aligned}
 d(p, q) &= sr(p) - sr(q) \\
 &= \sum_{k \leq \min(p, q)} (p \bmod k) - \sum_{k \leq \min(p, q)} (q \bmod k) \\
 &= \sum_{k \leq \min(p, q)} (p \bmod k) - (q \bmod k)
 \end{aligned}$$

Les distances  $d(p, p - 1)$  pour  $p$  variant de 3 à 20 valent :

$$\begin{aligned}
 d(3, 2) &= 1 \\
 d(4, 3) &= 0 \\
 d(5, 4) &= 3 \\
 d(6, 5) &= -1 \\
 d(7, 6) &= 5 \\
 d(8, 7) &= 0 \\
 d(9, 8) &= 4 \\
 d(10, 9) &= 1 \\
 d(11, 10) &= 9 \\
 d(12, 11) &= -5 \\
 d(13, 12) &= 11 \\
 d(14, 13) &= 3 \\
 d(15, 14) &= 5 \\
 d(16, 15) &= 0 \\
 d(17, 16) &= 15 \\
 d(18, 17) &= -4 \\
 d(19, 18) &= 17 \\
 d(20, 19) &= -3
 \end{aligned}$$

Le reste d’une division euclidienne étant nécessairement inférieur strictement au diviseur, la différence entre les sommes de restes d’un nombre  $p$  et de son prédécesseur  $p - 1$  pourrait dans les cas extrêmes

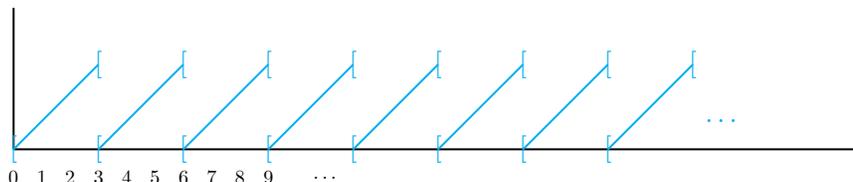
varier entre  $-\frac{(p-2)(p-1)}{2}$  et  $+\frac{(p-2)(p-1)}{2}$ , ces valeurs n'étant en fait jamais atteintes.

Les nombres premiers  $p$  maximisent la distance  $d(p, p-1)$ . En effet, la somme des restes des divisions euclidiennes d'un nombre premier par les nombres qui lui sont strictement inférieurs est toujours le plus éloignée qu'il est possible de la somme des restes des divisions euclidiennes de son prédécesseur et vaut  $p-2$  (nombres bleus de la liste des distances ci-dessus).

Pour un nombre premier  $p$ ,  $d(p, p-1)$  est une distance suprême (maximale) et vaut :

$$\text{Sup}(\sum_{k \leq p-1} (p \bmod k) - \sum_{k \leq p-1} ((p-1) \bmod k) = p-2$$

On peut voir les restes comme autant de points discrets de fonctions continues en dents de scie, qui sont du fait de l'ouverture/fermeture des intervalles, non dérivables pour les multiples, et qu'il s'agit de sommer. Par exemple, le graphe de la fonction en dents de scie fournissant les restes des divisions par 3 est :



Cette fonction (dépendant de  $p$ ) est définie par :

$$\begin{aligned} f(x, p) &= x \bmod p \text{ si } 0 \leq x < p \\ f(x, p) &= f(x+p) \text{ si } x < 0 \\ f(x, p) &= f(x-p) \text{ si } x \geq p. \end{aligned}$$

On trouve sur la toile que la somme des restes euclidiens d'un nombre peut s'obtenir en soustrayant un cumul de sommes de diviseurs au carré de ce nombre.

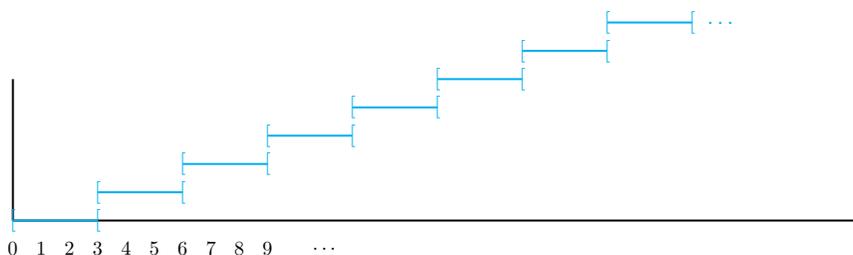
$$sr(x) = x^2 - \sum_{k=1}^x \sigma(k)$$

avec  $\sigma(k)$  égale à la somme des diviseurs de  $k$ .

On peut également voir cette somme de restes comme comptant des oscillations autour de fonctions en escalier dans l'égalité ci-dessous :

$$sr(x) = x^2 - \sum_{k=1}^x \left\lfloor \frac{x}{k} \right\rfloor k$$

Par exemple, le graphe de la fonction en escalier  $g(x, p) = \left\lfloor \frac{x}{p} \right\rfloor$  pour  $p = 3$  est :



On rappelle la définition par récurrence de la somme des diviseurs.

$$\sigma(x) = \frac{12}{n^2(n-1)} \sum_{k=1}^{n-1} (-5k^2 + 5kn - n^2) \sigma(k) \sigma(n-k)$$

Enfin, on trouve sur la toile un lien entre la somme des diviseurs et certaines valeurs de  $\zeta$ .

$$\zeta(s)\zeta(s-1) = \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s}$$

## 2 Symétries liant certains restes quadratiques

Observons la table de restes quadratiques qui fournit pour les carrés des entiers de 2 à 20 leur reste dans les divisions euclidiennes par les entiers de 2 à 20.

<i>mod</i>	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
4	0	1	0	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
9	1	0	1	4	3	2	1	0	9	9	9	9	9	9	9	9	9	9	9
16	0	1	0	1	4	2	0	7	6	5	4	3	2	1	0	16	16	16	16
25	1	1	1	0	1	4	1	7	5	3	1	12	11	10	9	8	7	6	5
36	0	0	0	1	0	1	4	0	6	3	0	10	8	6	4	2	0	17	16
49	1	1	1	4	1	0	1	4	9	5	1	10	7	4	1	15	13	11	9
64	0	1	0	4	4	1	0	1	4	9	4	12	8	4	0	13	10	7	4
81	1	0	1	1	3	4	1	0	1	4	9	3	11	6	1	13	9	5	1
100	0	1	0	0	4	2	4	1	0	1	4	9	2	10	4	15	10	5	0
121	1	1	1	1	1	2	1	4	1	0	1	4	9	1	9	2	13	7	1
144	0	0	0	4	0	4	0	0	4	1	0	1	4	9	0	8	0	11	4
169	1	1	1	4	1	1	1	7	9	4	1	0	1	4	9	16	7	17	9
196	0	1	0	1	4	0	4	7	6	9	4	1	0	1	4	9	16	6	16
225	1	0	1	0	3	1	1	0	5	5	9	4	1	0	1	4	9	16	5
256	0	1	0	1	4	4	0	4	6	3	4	9	4	1	0	1	4	9	16
289	1	1	1	4	1	2	1	1	9	3	1	3	9	4	1	0	1	4	9
324	0	0	0	4	0	2	4	0	4	5	0	12	2	9	4	1	0	1	4
361	1	1	1	1	1	4	1	1	1	9	1	10	11	1	9	4	1	0	1
400	0	1	0	0	4	1	0	4	0	4	4	10	8	10	0	9	4	1	0

On peut observer une ligne de restes “à rebours” depuis la fin de la ligne ; par exemple, la suite des restes du carré 25, qui écrite de droite à gauche, contient les résidus quadratiques

$$5, 6, 7, 8, 9, 10, 11, 12, 1, 3, 5, 7, 1, 4, 1, 0, 1, 1, 1$$

Les restes commencent par augmenter de 1 en 1, puis, lorsque “0 est traversé”, ils croissent de 2 en 2, puis lorsque 0 est à nouveau traversé, ils croissent de 3 en 3, et ainsi de suite, avec une croissance de plus en plus grande à chaque fois qu’on passe d’un reste à l’autre en “traversant 0”.

On a coloré (dans des croix dites “de pharmacie”<sup>1</sup>) les cases contenant des restes quadratiques vérifiant les égalités suivantes, qui présentent une sorte de symétrie verticale-horizontale. Comme attendu, leur taille est fonction de la racine du diviseur tête de colonne.

$$x^2 \bmod (x + a) = x^2 \bmod (x - a) = (x + a)^2 \bmod x = (x - a)^2 \bmod x$$

Toutes ces idées ne nous permettent cependant pas d’avoir une appréhension plus précise de l’ensemble des nombres premiers.

<sup>1</sup>dont les cellules centrales sont voisines au sens du “voisinage de Von Neumann”.

# Etrangeté de certaines opérations matricielles

Denise Vella-Chemla

9/9/2015

Le plus difficile est d'oublier les points, pour se concentrer sur les opérateurs : ça ne nous est pas naturel.

Le jeu dans cette note consiste à “inventer” des matrices numériques présentant certaines symétries de structure et à programmer certains calculs sur ces matrices, l'objectif étant d'attraper par ce biais certains nombres premiers dans nos filets.

On a commencé à effectuer de tels tout petits calculs en juillet 2015, sans succès, mais certains choix structurels pour les matrices ne nous satisfaisaient pas : on privilégiait les coins haut-gauche des matrices. Ici l'idée va être de “faire partir les nombres en étoile à partir du centre des matrices”, de façon à ce que celles-ci soient “le plus symétrique possible”.

Pour les calculs, on utilise le calculateur de matrices fourni par l'université de Nice (?), sur le site Wims, à l'adresse :

[http://wims.unice.fr/wims/fr\\_ool\\_linear\\_matrix.html](http://wims.unice.fr/wims/fr_ool_linear_matrix.html)

Pour l'instant, on ne fait que présenter quelques résultats qui sont intrigants. Il faudra programmer les calculs sur des matrices jusqu'à la taille  $101 \times 101$  pour voir si les éléments qui semblent se dégager se confirment, alors on pourra essayer d'en trouver les causes.

Les matrices de taille croissante qu'on va tester sont les suivantes :

$$M_2 = \begin{pmatrix} 2 & 1 & 2 \\ 0 & 1 & 0 \\ 2 & 1 & 2 \end{pmatrix}, M_3 = \begin{pmatrix} 3 & 0 & 1 & 0 & 3 \\ 0 & 2 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 3 & 2 & 1 & 2 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, M_4 = \begin{pmatrix} 4 & 0 & 2 & 1 & 2 & 0 & 4 \\ 0 & 3 & 0 & 1 & 0 & 3 & 0 \\ 0 & 0 & 2 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 4 & 3 & 2 & 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 2 & 0 & 0 \end{pmatrix},$$

$$M_5 = \begin{pmatrix} 5 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 5 \\ 0 & 4 & 0 & 2 & 1 & 2 & 0 & 4 & 0 \\ 0 & 0 & 3 & 0 & 1 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 5 & 4 & 3 & 2 & 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 1 & 0 & 3 & 0 & 0 \end{pmatrix} \text{ et } M_6 = \begin{pmatrix} 6 & 0 & 0 & 3 & 2 & 1 & 2 & 3 & 0 & 0 & 6 \\ 0 & 5 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 4 & 0 & 2 & 1 & 2 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 1 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 6 & 5 & 4 & 3 & 2 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 1 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 2 & 1 & 2 & 0 & 4 & 0 & 0 \end{pmatrix}.$$

On élève simplement ces matrices au carré, on obtient les matrices suivantes, dont on constate que leur colonne centrale ne contient que des nombres premiers, sauf 1.

$$(M_2)^2 = \begin{pmatrix} 8 & 5 & 8 \\ 0 & 1 & 0 \\ 8 & 5 & 8 \end{pmatrix}, (M_3)^2 = \begin{pmatrix} 9 & 0 & 7 & 0 & 9 \\ 6 & 8 & 5 & 8 & 6 \\ 0 & 0 & 1 & 0 & 0 \\ 15 & 8 & 11 & 8 & 15 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, (M_4)^2 = \begin{pmatrix} 24 & 6 & 24 & 13 & 24 & 6 & 24 \\ 0 & 9 & 0 & 7 & 0 & 9 & 0 \\ 8 & 6 & 8 & 5 & 8 & 6 & 8 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 24 & 15 & 24 & 19 & 24 & 15 & 24 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 8 & 6 & 8 & 5 & 8 & 6 & 8 \end{pmatrix},$$

$$(M_5)^2 = \begin{pmatrix} 25 & 0 & 15 & 0 & 11 & 0 & 15 & 0 & 25 \\ 10 & 24 & 6 & 24 & 13 & 24 & 6 & 24 & 10 \\ 0 & 0 & 9 & 0 & 7 & 0 & 9 & 0 & 0 \\ 10 & 8 & 6 & 8 & 5 & 8 & 6 & 8 & 10 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 35 & 24 & 30 & 24 & 29 & 24 & 30 & 24 & 35 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 10 & 8 & 6 & 8 & 5 & 8 & 6 & 8 & 10 \\ 0 & 0 & 9 & 0 & 7 & 0 & 9 & 0 & 0 \end{pmatrix},$$

$$(M_6)^2 = \begin{pmatrix} 48 & 10 & 32 & 33 & 32 & 23 & 32 & 33 & 32 & 10 & 48 \\ 0 & 25 & 0 & 15 & 0 & 11 & 0 & 15 & 0 & 25 & 0 \\ 12 & 10 & 24 & 6 & 24 & 13 & 24 & 6 & 24 & 10 & 12 \\ 0 & 0 & 0 & 9 & 0 & 7 & 0 & 9 & 0 & 0 & 0 \\ 12 & 10 & 8 & 6 & 8 & 5 & 8 & 6 & 8 & 10 & 12 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 48 & 35 & 48 & 48 & 48 & 41 & 48 & 48 & 48 & 35 & 48 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 12 & 10 & 8 & 6 & 8 & 5 & 8 & 6 & 8 & 10 & 12 \\ 0 & 0 & 0 & 9 & 0 & 7 & 0 & 9 & 0 & 0 & 0 \\ 12 & 10 & 24 & 6 & 24 & 13 & 24 & 6 & 24 & 10 & 12 \end{pmatrix}$$

Il y a un élément perturbant : la ligne verticale de 1 est le signe qu'on privilégie une direction et on souhaiterait symétriser encore davantage en ayant une ligne horizontale de 1 "correspondant" à la ligne verticale de 1 en question. Le problème est qu'une telle ligne horizontale rompt toutes les belles symétries verticales de la forme "un 1 tous les 1 élément dans la colonne des 1", "un 2 tous les 2 éléments dans la colonne des 2 et des 0 entre", "un 3 tous les 3 éléments dans la colonne des 3 et des 0 entre", ..., "un  $p$  tous les  $p$  éléments dans la colonne des  $p$  et des 0 entre".

Ci-dessous sont fournies 2 matrices ressemblant aux matrices ci-dessus mais contenant une ligne horizontale de 1 intercalée près de l'origine (près de l'élément central de la matrice) et leur carré.

$$M'_2 = \begin{pmatrix} 4 & 0 & 2 & 1 & 2 & 0 & 4 \\ 0 & 3 & 0 & 1 & 0 & 3 & 0 \\ 0 & 0 & 2 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 4 & 3 & 2 & 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 & 2 & 0 & 0 \end{pmatrix}, (M'_2)^2 = \begin{pmatrix} 24 & 6 & 24 & 13 & 24 & 6 & 24 \\ 3 & 12 & 3 & 7 & 3 & 12 & 3 \\ 8 & 6 & 8 & 5 & 8 & 6 & 8 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 27 & 18 & 27 & 19 & 27 & 18 & 27 \\ 9 & 7 & 9 & 7 & 9 & 7 & 9 \\ 8 & 6 & 8 & 5 & 8 & 6 & 8 \end{pmatrix}$$

$$M''_2 = \begin{pmatrix} 4 & 0 & 2 & 1 & 2 & 0 & 4 \\ 0 & 3 & 0 & 1 & 0 & 3 & 0 \\ 0 & 0 & 2 & 1 & 2 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 4 & 3 & 2 & 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 2 & 0 & 0 \end{pmatrix}, (M''_2)^2 = \begin{pmatrix} 25 & 7 & 25 & 13 & 25 & 7 & 25 \\ 1 & 10 & 1 & 7 & 1 & 10 & 1 \\ 9 & 7 & 9 & 5 & 9 & 7 & 9 \\ 9 & 7 & 9 & 7 & 9 & 7 & 9 \\ 25 & 16 & 25 & 19 & 25 & 16 & 25 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 9 & 7 & 9 & 5 & 9 & 7 & 9 \end{pmatrix}$$

On constate le lendemain qu'on peut rendre les matrices initiales proposées plus symétriques encore en décalant vers le haut leur ligne "sans zéro".

On effectuera les tests par programmes de carrés de matrices de la forme de  $D_6$  ci-dessous

$$D_6 = \begin{pmatrix} 0 & 5 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 4 & 0 & 2 & 1 & 2 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 1 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 6 & 5 & 4 & 3 & 2 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 1 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 2 & 1 & 2 & 0 & 4 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 5 & 0 \end{pmatrix}$$

dont le carré est

$$(D_6)^2 = \begin{pmatrix} 6 & 5 & 44 & 3 & 22 & 11 & 22 & 3 & 44 & 5 & 6 \\ 6 & 5 & 4 & 27 & 2 & 13 & 2 & 27 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 14 & 7 & 14 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 5 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 65 & 44 & 27 & 34 & 41 & 34 & 27 & 44 & 65 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 5 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 14 & 7 & 14 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 27 & 2 & 13 & 2 & 27 & 4 & 5 & 6 \\ 6 & 5 & 44 & 3 & 22 & 11 & 22 & 3 & 44 & 5 & 6 \end{pmatrix}$$

Malheureusement, il suffit d'élever  $D_7$  au carré pour trouver un composé dans la colonne médiane.

$$(D_7)^2 = \begin{pmatrix} 7 & 6 & 65 & 4 & 3 & 14 & 23 & 14 & 3 & 4 & 65 & 6 & 7 \\ 7 & 6 & 5 & 44 & 3 & 22 & 11 & 22 & 3 & 44 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 27 & 2 & 13 & 2 & 27 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 14 & 7 & 14 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 5 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 90 & 65 & 44 & 69 & 62 & 55 & 62 & 69 & 44 & 65 & 90 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 5 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 14 & 7 & 14 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 27 & 2 & 13 & 2 & 27 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 44 & 3 & 22 & 11 & 22 & 3 & 44 & 5 & 6 & 7 \\ 7 & 6 & 65 & 4 & 3 & 14 & 23 & 14 & 3 & 4 & 65 & 6 & 7 \end{pmatrix}$$

Fournissons tout de même  $(D_8)^2$ ,  $(D_9)^2$  et  $(D_{10})^2$  parce qu'on trouvait l'idée jol...



Le plus difficile est d'oublier les points, pour se concentrer sur les opérateurs : ça ne nous est pas naturel.

Pour comprendre ce qui se tramait pour que la conjecture de Goldbach soit vraie, on a mis tête-bêche deux lignes des booléens de primalité (en bleu dans les exemples) associés aux entiers successifs exactement de la façon dont cela était présenté dans un texte de Laisant "Sur un procédé de vérification expérimental de la conjecture de Goldbach" (on rappelle qu'on a choisi comme convention que 0 code "premier" tandis que 1 code "composé"). Le nombre entier que l'on souhaite décomposer en somme de deux nombres détermine le positionnement des deux lignes de booléens l'une par rapport à l'autre.

Par exemple, on montre dans les tableaux ci-dessous le positionnement des séquences booléennes tête-bêche correspondant aux décompositions de 16, 18 et 20.

<i>décompositions de 16</i>					
...	13	11	9	...	
...	0	0	1	...	
...	0	0	0	...	
...	3	5	7	...	
<i>décompositions de 18</i>					
...	15	13	11	9	...
...	1	0	0	1	...
...	0	0	0	1	...
...	3	5	7	9	...
<i>décompositions de 20</i>					
...	17	15	13	11	...
...	0	1	0	0	...
...	0	0	0	1	...
...	3	5	7	9	...

Le passage d'un entier pair à l'entier pair suivant consiste, on l'a vu, à "faire glisser" la séquence de booléens du haut d'un cran vers la droite et c'est ceci qu'on a choisi de symboliser par 16 règles de réécriture qu'on réécrit ci-dessous :

$aa \rightarrow a$	$ba \rightarrow a$	$ca \rightarrow c$	$da \rightarrow c$
$ab \rightarrow b$	$bb \rightarrow b$	$cb \rightarrow d$	$db \rightarrow d$
$ac \rightarrow a$	$bc \rightarrow a$	$cc \rightarrow c$	$dc \rightarrow c$
$ad \rightarrow b$	$bd \rightarrow b$	$cd \rightarrow d$	$dd \rightarrow d$

Ces règles sont en fait autant d'instances différentes d'une seule et même règle qui associe à deux doublons de booléens un troisième doublon dont les coordonnées sont la première coordonnée du premier doublon et la seconde coordonnée du second doublon. On peut coder ces règles en utilisant des matrices  $2 \times 2$  de la façon suivante :

- On code le premier doublon par une matrice  $M1 = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$  ;
- On code le second doublon par une matrice  $M2 = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$  ;
- On concatène (intègre) ces deux matrices verticalement dans une matrice :  $\begin{pmatrix} M1 \\ M2 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & b \\ c & 0 \\ 0 & d \end{pmatrix}$  ;
- On multiplie ce résultat à gauche par la matrice  $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$  ;

- On obtient la matrice  $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \\ c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$  qui contient la première coordonnée du premier doublon et la seconde du second.

Ci-dessous le poème de Boileau, qui illustre ce sentiment que l'on a de revenir sans cesse en arrière, en tournant toujours en rond autour des mêmes idées.

Toile de Pénélope

*Avant donc que d'écrire, apprenez à penser.*

*Ce que l'on conçoit bien s'énonce clairement,  
Et les mots pour le dire arrivent aisément.*

*Hâtez-vous lentement, et sans perdre courage,  
Vingt fois sur le métier remettez votre ouvrage,  
Polissez-le sans cesse, et le repolissez,  
Ajoutez quelquefois, et souvent effacez.*

Boileau, L'Art poétique

Dans la note *maillage.pdf*, on a rappelé les règles de réécriture qu'on a utilisées pour une modélisation des décompositions de Goldbach. Ces règles sont en fait autant d'instances différentes d'une seule et même règle qui associe à deux doublons de booléens un troisième doublon dont les coordonnées sont la première coordonnée du premier doublon et la seconde coordonnée du second doublon. On peut coder ces règles en utilisant des matrices  $2 \times 2$  de la façon suivante :

- On code le premier doublon par une matrice  $M1 = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$  ;
- On code le second doublon par une matrice  $M2 = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$  ;

On est ennuyé parce que le choix effectué dans notre note précédente fait intervenir des matrices rectangulaires plutôt que carrées et que l'ensemble des matrices manque "d'homogénéité".

On fixe les éléments de vocabulaire ci-dessous :

- On appelle matrice "génitrice-gauche" une matrice de taille 4 de la forme suivante  $\begin{pmatrix} M1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ .
- On appelle matrice "génitrice-droite" une matrice de taille 4 de la forme suivante  $\begin{pmatrix} 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ .

Il faudra trouver un opérateur (noté  $\circ$  par exemple) qui à partir d'une matrice génitrice-gauche et d'une matrice génitrice-droite permet d'obtenir une matrice fille de la forme

$$\begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & d \end{pmatrix}.$$

On a aussi besoin de 2 autres opérateurs :

- l'un qui fait passer une sous-matrice de la position de génitrice-gauche à la position de génitrice-droite, de la façon suivante :  $\begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & a & 0 \\ 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$  ;
- l'autre qui fait passer une sous-matrice de la position de fille à la position de génitrice-gauche de la façon suivante :  $\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & b \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ .

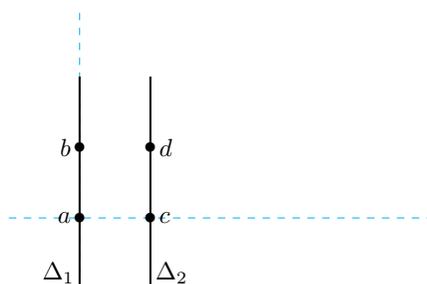
Modéliser (DV, 31/10/2015)

On explique ici où on est arrêté, bloqué : on ne trouve pas comment utiliser une fonction qu'on a définie, fonction qui agit sur un champ de lettres, pour obtenir des informations sur l'ensemble des nombres premiers.

Notre fonction  $f$  est définie par :

$$\begin{aligned} f : E \times E &\longrightarrow E \\ (u, v) &\longmapsto p_x(u) + p_y(v) \\ \left( \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \right) &\longmapsto \begin{pmatrix} x_1 \\ y_2 \end{pmatrix} \end{aligned}$$

On peut "voir" la fonction  $f$  de la façon suivante. On note  $a \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ ,  $b \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ ,  $c \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  et  $d \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ , les 4 points du plan. On appelle  $\Delta_1$  la droite contenant les points  $a$  et  $b$  et  $\Delta_2$  la droite contenant les points  $c$  et  $d$ .



$f$  est la projection orthogonale qui associe à un bipoint (vecteur) le point projeté orthogonal de son point extrémité sur la droite  $d$  à laquelle appartient son point origine ( $d = \Delta_1$  ou  $d = \Delta_2$ ). Les images par cette projection des bipoints sont :

$$\begin{array}{c|c|c|c} aa \rightarrow a & ba \rightarrow a & ca \rightarrow c & da \rightarrow c \\ ab \rightarrow b & bb \rightarrow b & cb \rightarrow d & db \rightarrow d \\ ac \rightarrow a & bc \rightarrow a & cc \rightarrow c & dc \rightarrow c \\ ad \rightarrow b & bd \rightarrow b & cd \rightarrow d & dd \rightarrow d \end{array}$$

On étend cette fonction à une suite de lettres, en l'appliquant d'un coup à tous les doublons de lettres de cette suite. Par exemple,

$$f(\dots aacdacha \dots) = \dots aadcada \dots$$

On imagine cette opération appliquée à l'infini, sur un champ de lettres infini ; chaque lettre  $l_{i,j}$  du champ se déduit par les règles de réécriture vues ci-dessus des lettres  $l_{i-1,j-1}$  et  $l_{i-1,j}$  (d'une manière similaire à la manière dont les coefficients du binôme sont calculés dans le triangle de Pascal). Ci-dessous est fourni un extrait de ce champ qui représente les décompositions des nombres pairs de 6 à 34 en sommes de 2 entiers impairs depuis la somme 3+3 en haut à gauche du nombre pair 6 à la somme 17+19 en bas à droite du nombre pair 34. La huitième ligne par exemple fournit les lettres associées aux sommes décomposant l'entier pair 20 et qui sont 3+17 =  $a$ , 5+15 =  $c$ , 7+13 =  $a$ , 9+11 =  $b$ , 11+9 =  $c$ , 13+7 =  $a$ , 15+5 =  $b$  et 17+3 =  $a$ .

```

⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮
... a c c b a a d a ...
... a a c d a a b c ...
... a a a d c a b a ...
... c a a b c c b a ...
... a c a b a c d a ...
... a a c b a a d c ...
... c a a d a a b c ...
... a c a b c a b a ...
... a a c b a c b a ...
... c a a d a a d a ...
... a c a b c a b c ...
... c a c b a c b a ...
... c c a d a a d a ...
... a c c b c a b c ...
... a a c d a c b a ...
⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮

```

Illustrons sur un exemple la règle générale de réécriture qui permet de trouver la lettre  $l_{i,j}$  à partir des lettres  $l_{i-1,j-1}$  et  $l_{i-1,j}$  :

la lettre	représente la décomposition	exemple
$l_{i-1,j-1}$	$n = x_1 + y_1$	$30 = 3 + 27$
$l_{i-1,j}$	$n = x_2 + y_2 = (x_1 + 2) + (y_1 - 2)$	$30 = 5 + 25$
$l_{i,j}$	$n + 2 = x_2 + y_1 = (x_1 + 2) + y_1$	$32 = 5 + 27$

Lorsqu'on compte les lettres dans certains mots extraits du champ de lettres, par exemple des lettres  $a$ , on compte des assertions logiques du type

$$(n = x + y) \wedge (x \leq y) \wedge (x \text{ premier}) \wedge (y \text{ premier})$$

Remarque : les décompositions de Goldbach binaire (i.e. en somme de 2 premiers) sont les  $a$  qui se trouvent parmi les lettres colorées en bleu du champ de lettres.

Ci-dessous, on a noté en rouge les lettres  $a$  en fin de mots bleus qui représentent les nombres premiers au sens où elles codent les décompositions de Goldbach triviales de la forme  $2p = p + p$ . Ces lettres sont bien sûr alignées car elles sont en fin de mots et que la longueur des mots bleus augmente régulièrement.

```

⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮
... a c c b a a d a ...
... a a c d a a b c ...
... a a a d c a b a ...
... c a a b c c b a ...
... a c a b a c d a ...
... a a c b a a d c ...
... c a a d a a b c ...
... a c a b c a b a ...
... a a c b a c b a ...
... c a a d a a d a ...
... a c a b c a b c ...
... c a c b a c b a ...
... c c a d a a d a ...
... a c c b c a b c ...
... a a c d a c b a ...
⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮ ⋮

```

On cherche à coder les lettres  $a, b, c, d$  par des matrices  $2 \times 2$ . On a trouvé par programme certaines possibilités de matrices dont les éléments sont tous entiers mais aucune de ces possibilités ne permet de

distinguer  $a$  de  $c$  et  $b$  de  $d$ . Il est vrai que la lecture des 16 règles de réécriture montre cette similarité des rôles des lettres  $a$  et  $c$  d'une part et  $b$  et  $d$  d'autre part.

Une solution possible qui vérifie les règles  $aa = a, ab = b, etc$  est :

$$a = c = \begin{pmatrix} -1 & -2 \\ 1 & 2 \end{pmatrix}$$

$$b = d = \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix}$$

On a trouvé, qui se sont avérées intéressantes pour notre dessein, des règles de réécriture de doublons de lettres appartenant à des mots qu'on a associés à des nombres et que voici :

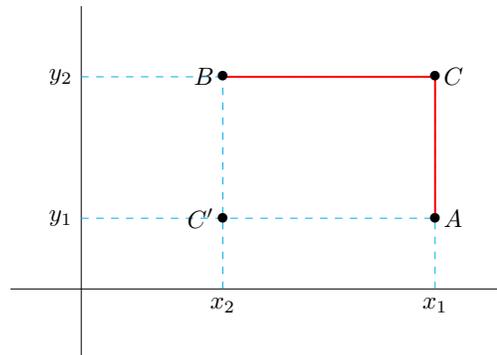
$$\begin{array}{c|c|c|c}
 aa \rightarrow a & ba \rightarrow a & ca \rightarrow c & da \rightarrow c \\
 ab \rightarrow b & bb \rightarrow b & cb \rightarrow d & db \rightarrow d \\
 ac \rightarrow a & bc \rightarrow a & cc \rightarrow c & dc \rightarrow c \\
 ad \rightarrow b & bd \rightarrow b & cd \rightarrow d & dd \rightarrow d
 \end{array}$$

Ces règles de réécriture sont autant d'instances d'une seule règle toute simple qui associe à deux points  $A$  et  $B$  du plan un troisième point qui partage l'une de ses coordonnées avec chacun d'entre eux ; il existe deux tels points, comme présenté sur le schéma ci-dessous, on privilégie une coordonnée par rapport à l'autre lorsqu'on s'intéresse à  $C$  plutôt qu'à  $C'$ .

$$f : \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ y_2 \end{pmatrix}$$

L'opérateur qui permettrait d'associer  $C'$  plutôt que  $C$  à  $A$  et  $B$  est

$$f : \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \mapsto \begin{pmatrix} x_2 \\ y_1 \end{pmatrix}$$



Si on note par exemple  $+$  le premier opérateur (qui associe  $C$  au couple  $(A, B)$ ) et  $\times$  le second opérateur (qui associe  $C'$  au même couple), il faudrait être capable d'étudier la manière dont ces 2 opérateurs se combinent. Je ne sais pas ce qu'il faut étudier concernant ces deux opérateurs.

On associe à chaque nombre entier la suite de nombres indexée par l'infinité des nombres premiers successifs et qui contient les restes obtenus dans les divisions euclidiennes de ce nombre par les nombres premiers en question. Par exemple, au nombre 6 est associée la séquence  $s_6 = 0, 0, 1, 6, 6, 6, \dots$  et au nombre 30 est associée la séquence  $s_{30} = 0, 0, 0, 2, 8, 4, 13, 11, 7, 1, 30, 30, 30, \dots$

Par commodité, on notera à côté de chaque reste le diviseur permettant de l'obtenir. Ainsi, la séquence associée à 30 ci-dessus sera plutôt écrite :  $s_6 = 0 (2), 0 (3), 1 (5), 6 (7), 6 (11), 6 (13), 6 (17), \dots$

On rappelle que deux nombres premiers jumeaux ont pour différence 2. Par exemple, 3 et 5 sont des nombres premiers jumeaux, 41 et 43 en sont également. Appelons "père de jumeaux" un nombre pair compris entre 2 nombres premiers jumeaux. 4, compris entre 3 et 5, est un père de jumeaux ; 42, compris entre 41 et 43, en est un autre. Tout père de jumeau (sauf 4) est un multiple de 6. En effet, les pairs de la forme  $6k + 2$  (resp.  $6k + 4$ ) ne peuvent être pères de jumeaux car le nombre qui les suit (resp. précède), étant un  $6k + 3$ , est divisible par 3 et ne peut donc être premier.

Considérons  $n_k$  un père de jumeau ; si on appelle  $p_k$  le plus grand nombre premier strictement inférieur à  $n_k - 1$ , la séquence d'entiers  $s_{n_k}$  associée à  $n_k$  est toujours de la forme suivante

$$s_{n_k} = 0 (2), 0 (3), x_1 (5), x_2 (7), \dots, x_k (p_k), 1 (n_k - 1), n_k (n_k + 1), n_k (p_j > n_k + 1), \dots$$

avec  $x_i \neq 1$  et  $x_i \neq p_i - 1$  pour tout  $p_i$  tel que  $5 \leq p_i < n_k - 1$  (on appellera ces deux conditions "contraintes pour pouvoir être un père de jumeau").

En effet, un nombre (en particulier un père de jumeau) a pour reste 1 quand on le divise par le nombre qui le précède. D'autre part, un nombre a pour reste lui-même dans toute division par un nombre qui lui est strictement supérieur.

Posons maintenant l'hypothèse qu'on a dénombré tous les pères de jumeaux sous prétexte qu'il en existerait un nombre fini. Notons les séquences de restes modulaires selon les nombres premiers successifs associées à chacun d'eux dans un tableau.  $p_{der}$  est le plus grand des aînés de couples de jumeaux recensés.

	2	3	5	7	...	$p_{i-1}$	$p_i = n_i - 1$	$p_{i+1} = n_i + 1$	$p_{j>i+1}$	...	$p_{der}$
$n_1$	0	0	$x_1$	$\alpha_2$	...	$\alpha_{i-1}$	1	$n_1$	$n_1$	...	$n_1$
$n_2$	0	0	$\beta_1$	$x_2$	...	$\beta_{i-1}$	...	...	$n_2$	...	$n_2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$n_{i-1}$	0	0	...	...	...	$x_{i-1}$	...	...	...	...	$n_{i-1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$n_{der}$	...	...	...	...	...	...	...	...	...	1	$n_{der}$

Considérons alors les nombres dont la séquence de restes associée commence par les  $y_k (p_k)$ , cette séquence étant fabriquée de la façon suivante à partir des séquences du tableau :

- si  $x_k = 0$  alors  $y_k = 2$  ;
- si  $x_k = p_k - 2$  alors  $y_k = 0$  ;
- si  $x_k \neq 0$  et  $x_k \neq p_k - 2$  alors  $y_k = x_k + 1$ .

Ces nombres sont solutions du système de congruences

$$[X_k \equiv 0 \pmod{6}] \wedge [X_k \equiv y_k \pmod{p_k}, \forall p_k \text{ tel que } 5 \leq p_k \leq p_{der}].$$

Le théorème des restes chinois assure qu'il existe une infinité de nombres satisfaisant le système de congruences ainsi modifié. Ces nombres parcourent toutes les possibilités combinatoires de valeurs des différents restes possibles selon les différents modules possibles à égales proportions.

Considérons le plus petit de ces nombres qui soit supérieur à  $p_{der}$  et qui vérifie les contraintes que nous avons appelées plus haut "contraintes pour pouvoir être un père de jumeaux" (non-congruence à 1 ou  $p_k - 1$  selon tout module premier  $p_k$ ). Ce nombre est un père de jumeaux (on l'a choisi pour ça).

Or il n'appartient pas à l'ensemble fini des pères de jumeaux déjà recensés dans le tableau<sup>1</sup>. Pourtant, son écriture fait de lui un père de jumeau. Cela est en contradiction avec le fait qu'on avait recensé dans le tableau *tous* les pères de jumeaux. L'ensemble des pères de jumeaux est donc infini.

---

<sup>1</sup>On a "perturbé la diagonale" pour l'obtenir, selon la méthode de Cantor.

Il s'agit de démontrer que l'ensemble des nombres premiers jumeaux est infini. On rappelle que deux nombres premiers jumeaux ont pour différence 2. Par exemple, 3 et 5 sont des nombres premiers jumeaux, 41 et 43 en sont également.

On définit deux fonctions  $pp(x)$  ( $pp$  pour *prec\_premier*) et  $sp(x)$  ( $sp$  pour *succ\_premier*) qui associent à un nombre pair  $x$  deux booléens de primalité selon que  $x-1$  et  $x+1$  sont premiers ou non. Par convention, le booléen 0 signifie *premier* et le booléen 1 signifie *composé*.

Par exemple,  $pp(8) = 0$  car  $8-1 = 7$  est premier tandis que  $sp(8) = 1$  car  $8+1 = 9$  est composé.

Les valeurs des fonctions  $pp(x)$  et  $sp(x)$  sont notées dans le tableau ci-dessous pour  $x$  compris entre 2 et 24.

$x$	2	4	6	8	10	12	14	16	18	20	22	24
$pp(x)$	1	0	0	0	1	0	0	1	0	0	1	0
$sp(x)$	0	0	0	1	0	0	1	0	0	1	0	1

On note de façon évidente que la séquence des valeurs de la fonction  $sp(x)$  est simplement un "décalage" d'un cran de la séquence des valeurs de la fonction  $pp(x)$ . En effet,  $\forall x, sp(x) = pp(x+2)$ .

**Notations :** On désigne par la lettre :

- $a$  : un entier pair tel que  $pp(x) = 0$  et  $sp(x) = 0$  ;
- $b$  : un entier pair tel que  $pp(x) = 0$  et  $sp(x) = 1$  ;
- $c$  : un entier pair tel que  $pp(x) = 1$  et  $sp(x) = 0$  ;
- $d$  : un entier pair tel que  $pp(x) = 1$  et  $sp(x) = 1$ .

Cette convention de notation permet d'ajouter une ligne au tableau en associant à chaque nombre pair  $x$  la lettre  $l(x)$  lui correspondant selon les valeurs que prennent pour lui les fonctions  $pp(x)$  et  $sp(x)$ .

$x$	2	4	6	8	10	12	14	16	18	20	22	24
$pp(x)$	1	0	0	0	1	0	0	1	0	0	1	0
$sp(x)$	0	0	0	1	0	0	1	0	0	1	0	1
$l(x)$	$c$	$a$	$a$	$b$	$c$	$a$	$b$	$c$	$a$	$b$	$c$	$b$

Supposons qu'à partir d'un certain rang, il n'y ait plus de couple de nombres premiers jumeaux (i.e. que le nombre de nombres premiers jumeaux est fini). Alors la séquence de lettres à partir d'un certain rang ne contiendrait plus aucune lettre  $a$ . A cause de la condition de décalage, les lettres de la séquence devraient alors se succéder selon les règles suivantes :

- après une lettre  $b$  ou une lettre  $d$  ne pourraient venir qu'une lettre  $c$  ou une lettre  $d$  ;
- après une lettre  $c$  ne pourrait venir qu'une lettre  $b$  ;

On représente ces contraintes sur la séquence de lettres par un automate. Une flèche entre une lettre  $x$  et une lettre  $y$  de l'automate exprime la condition " $x$  peut être suivie par  $y$  dans la séquence globale des lettres". On n'arrive cependant pas à aboutir à une contradiction en partant de l'hypothèse que la séquence globale de lettres ne contient plus de lettre  $a$  à partir d'un certain rang.

