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.

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

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

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[1], 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.

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

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 !

[1]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 ($M_{i,j} = i \ mod \ j$, 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 :

$$f(x) = x \prod_{2 \leqslant p < x} x \ mod \ p$$

Exemples :

$$f(9) = 9 \prod_{2 \leqslant p < 9} 9 \ mod \ p = 9 \times (1 \times 0 \times 1 \times 4 \times 3 \times 2 \times 1) = 0$$
$$f(13) = 13 \prod_{2 \leqslant p < 13} 13 \ mod \ p = 13 \times (1 \times 1 \times 1 \times 3 \times 1 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1) = 13 \times 63 = 819$$
$$f(15) = 15 \prod_{2 \leqslant p < 15} 15 \ mod \ p = 15 \times (1 \times 0 \times 3 \times 0 \times 3 \times 1 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1) = 0$$
$$f(25) = 25 \prod_{2 \leqslant p < 25} 25 \ mod \ p = 25 \times (1 \times 1 \times 1 \times 0 \ldots) = 0$$

La fonction f associe 0 à tout nombre composé et λp 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)

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

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

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.