Distance suprême

Denise Vella-Chemla

24/8/2015

1 Restes de divisions euclidiennes

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

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

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.

mod	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 :

$$sr(x) = \sum_{2 \leqslant k < x} x \ mod \ k$$

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 :

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

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 précédesseur $p-1$ pourrait dans les cas extrêmes

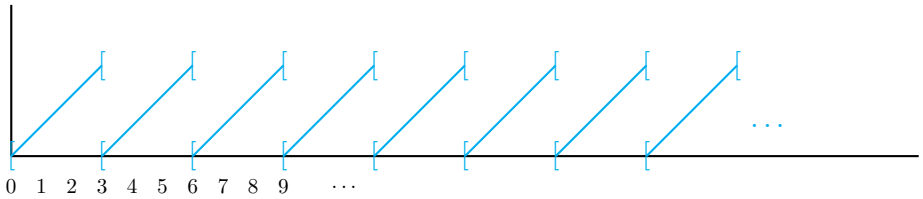
varier entre $-\frac{(p-2)(p-1)}{2}$ et $+\frac{(p-2)(p-1)}{2}$, ces valeurs n'étant en fait jamais atteintes.

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 :

$$Sup(\sum_{k \leqslant p-1} (p \ mod \ k) - \sum_{k \leqslant p-1} ((p-1) \ mod \ k) = p-2$$

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 :

$$\begin{array}{ll} f(x,p) & = x \ mod \ p \text{ si } 0 \leqslant \text{x} < \text{p} \\ f(x,p) & = f(x+p) \text{ si x} < 0 \\ f(x,p) & = f(x-p) \text{ si x} \geqslant \text{p.} \end{array}$$

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.

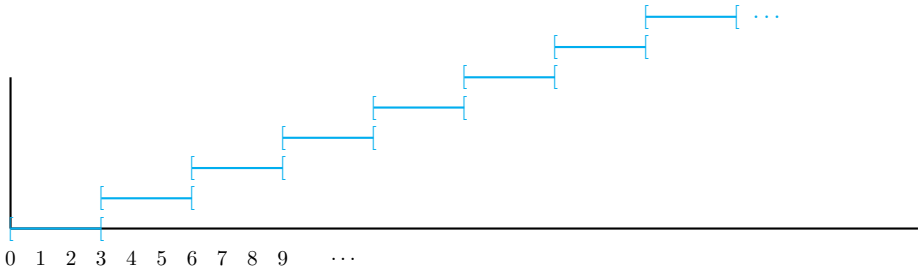
$$sr(x) = x^2 - \sum_{k=1}^{x} \sigma(k)$$

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 ζ.

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

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.

mod	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”[1]) 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.

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

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

[1] dont les cellules centrales sont voisines au sens du “voisinage de Von Neumann”.