Tamis (Denise Vella-Chemla, 12.6.2016)

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

$$x \ mod \ y = x - \left\lfloor \frac{x}{y} \right\rfloor y$$

Les relations invariantes qui caractérisent la division euclidienne sur les entiers positifs sont $x = qy + k$ avec $k = x \ mod \ y$ et $qy \leqslant x < (q+1)y$.

Observons la table de restes qui fournit pour les entiers x de 2 à 20 leur reste dans les divisions euclidiennes par les entiers de 2 à x (en dernière colonne est calculée la somme des restes par ligne).

mod	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Σ
2	0																			$\rightarrow 0$
3	1	0																		$\rightarrow 1$
4	0	1	0																	$\rightarrow 1$
5	1	2	1	0																$\rightarrow 4$
6	0	0	2	1	0															$\rightarrow 3$
7	1	1	3	2	1	0														$\rightarrow 8$
8	0	2	0	3	2	1	0													$\rightarrow 8$
9	1	0	1	4	3	2	1	0												$\rightarrow 12$
10	0	1	2	0	4	3	2	1	0											$\rightarrow 13$
11	1	2	3	1	5	4	3	2	1	0										$\rightarrow 22$
12	0	0	0	2	0	5	4	3	2	1	0									$\rightarrow 17$
13	1	1	1	3	1	6	5	4	3	2	1	0								$\rightarrow 28$
14	0	2	2	4	2	0	6	5	4	3	2	1	0							$\rightarrow 31$
15	1	0	3	0	3	1	7	6	5	4	3	2	1	0						$\rightarrow 36$
16	0	1	0	1	4	2	0	7	6	5	4	3	2	1	0					$\rightarrow 36$
17	1	2	1	2	5	3	1	8	7	6	5	4	3	2	1	0				$\rightarrow 51$
18	0	0	2	3	0	4	2	0	8	7	6	5	4	3	2	1	0			$\rightarrow 47$
19	1	1	3	4	1	5	3	1	9	8	7	6	5	4	3	2	1	0		$\rightarrow 64$
20	0	2	0	0	2	6	4	2	0	9	8	7	6	5	4	3	2	1	0	$\rightarrow 61$

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

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

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

La fonction $sr(x)$ prend les valeurs suivantes (on note en troisième ligne le différentiel $sr(x) - sr(x-1)$) :

x	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$sr(x)$	0	1	1	4	3	8	8	12	13	22	17	28	31	36	36	51	47	64	61
$sr(x) - sr(x-1)$		1	0	3	−1	5	0	4	1	9	−5	11	3	5	0	15	−4	17	−3

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 a donc :

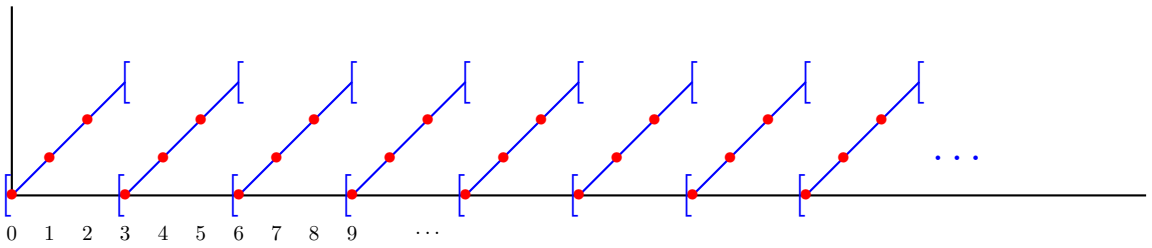
$$p \ premier \iff sr(p) - sr(p-1) = p - 2.$$

En utilisant la somme des diviseurs $\sigma(x)$ dont on fournit les premières valeurs, on obtient une définition par récurrence de la somme des restes :

$$\begin{cases} sr(2) = 0 \\ sr(x+1) = sr(x) - \sigma(x+1) + 2x + 1 \end{cases}$$

x	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$sr(x)$	0	1	1	4	3	8	8	12	13	22	17	28	31	36	36	51	47	64	61
$\sigma(x)$	3	4	7	6	12	8	15	13	18	12	28	14	24	24	31	18	39	20	42

On peut voir les restes comme autant de points discrets de fonctions continues par morceaux 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 périodique (y désignant le module) est définie par :

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

Cependant, la fonction *mod* n'étant pas polynomiale, on cherche plutôt une fonction qui, étant donnés deux entiers x et y, fournit le reste de la division euclidienne de x par y (noté $x \ mod \ y = k$), mais sans utiliser la fonction partie entière.

Prenons un exemple : $13 \ mod \ 5 = 3$ car 13 est compris entre $10 = 2 \times 5$ et $15 = 3 \times 5$ et $13 - 10 = 3$. Si on prend deux produits kx et $(k+1)x$ avec $k \geqslant 3$ et qu'on leur ôte 13, ces différences seront de même signe (positif). Si on prend deux produits kx et $(k+1)x$ avec $k < 2$ et qu'on leur ôte 13, les différences seront de même signe (négatif). Le seul cas où les différences kx et $(k+1)x$ sont de signe opposé est le cas où $k = 3 = 13 \ div \ 5$ (div désignant ici la division entière).

On remplace la définition habituelle de la division euclidienne par :

$$\forall x \in \mathbb{N}, \forall y \in \mathbb{N}\backslash\{0\}, x \ mod \ y = k$$

si et seulement si

$$\exists q \in \mathbb{N}, \exists k \in \mathbb{N}\backslash\{0\} \ tels \ que \begin{cases} x - qy = k \ et \\ (x-qy)(x-(q+1)y) \leqslant 0 \iff x^2 - (2q+1)xy + q(q+1)y^2 \leqslant 0 \end{cases}$$

On réécrit cette équation d'inconnue q sous la forme habituelle selon les puissances décroissantes de q (x et y sont connues) :

$$y^2q^2 + y(y-2x)q + x(x-y) \leqslant 0$$

Cette équation polynomiale du second degré définit une parabole. y^2 étant positif, la fonction décroît puis croît. Le sommet de la parabole est de coordonnées $\left(\frac{2x-y}{2y}; -\left(\frac{1}{2}y\right)^2\right)$.