Infinitude de l'ensemble des nombres premiers jumeaux

Denise Chemla

23 mai 2012

On appelle nombres premiers jumeaux deux nombres premiers qui diffèrent de 2.

3 et 5 sont des nombres premiers jumeaux. 17 et 19 en sont également.

Dans la suite, on dénommera nombres premiers jumeaux *cadets* les nombres premiers qui ont un jumeau qui leur est strictement supérieur (pour les exemples cités, ce sont 3 et 17 qui sont des nombres premiers jumeaux *cadets*).

Pour prouver que l'ensemble des nombres premiers jumeaux cadets est infini, on va utiliser un argument similaire à celui appelé "diagonale de Cantor".

Supposons que l'ensemble des nombres premiers jumeaux cadets est fini. Notons le $\mathcal{C}adets = \{c_1, \ldots, c_n\}$. A chacun des éléments de cet ensemble $\mathcal{C}adets = \{c_1, \ldots, c_n\}$, on associe par une bijection l'ensemble de ses restes modulo les nombres premiers compris entre 2 et $c_n + 2$. Puis on invente un ensemble de restes selon les modules premiers compris entre 2 et $c_n + 2$ différent de tous les ensembles de restes déjà recensés. Cet ensemble de restes correspond à un nombre qui n'a pas été recensé alors qu'il aurait dû l'être dans l'ensemble fini des jumeaux cadets $\mathcal{C}adets$ initial. On a ainsi prouvé que l'ensemble des nombres premiers jumeaux cadets n'est pas fini et a fortiori, qu'il en est de même de l'ensemble des nombres premiers jumeaux.

Le nombre premier jumeau cadet 101 est codé par l'ensemble de restes suivant selon les modules compris entre 2 et 103 :

$\{1, 2, 1, 3, 2, 10, 16, 6, 9, 14, 8, 27, 19, 15, 7, 48, 42, 40, 34, 30, 28, 22, 18, 12, 4, 0, 101\}$

On notera que tous les nombres premiers jumeaux cadets sauf 3 sont congrus à 1 (mod 2) et à 2 (mod 3) (3 quant à lui est congru à 0 (mod 3)) ; d'une part, ils sont impairs ; d'autre part, ils doivent être congrus à 2 (mod 3) (sauf 3) car dans le cas contraire, soit, étant congrus à 0 (mod 3), ils ne seraient pas premiers, soit, étant congru à 1 (mod 3), leur *aîné* ne serait pas premier étant quant à lui congru à 0 (mod 3) puisque $1+2 \equiv 0$ (mod 3) et dans ces deux cas, ils ne pourraient pas être éléments de l'ensemble des nombres premiers jumeaux cadets.

Pour inventer un nouveau nombre premier jumeau cadet dont l'ensemble des restes n'appartient pas à l'ensemble fini des ensembles de restes déjà recensés, on procède en "perturbant" une diagonale qui assure la "nouveauté" du nombre premier jumeau cadet fabriqué.

Le tableau suivant contient les restes associés aux nombres premiers jumeaux cadets, en nombre fini, qui appartiennent à $\mathcal{C}adets$.

Nous devons maintenant inventer un nouvel ensemble de restes, non encore recensé, par la méthode de la diagonale de Cantor, en modifiant les restes modulaires qui se trouvent sur une diagonale du tableau.

	2	3	5	7	11	...	c_n+2
$c_1 = 3$	1	0	$\boxed{\mathrm{r}_{c_1,5}}$				
$c_2 = 5$	1	2		$\boxed{\mathrm{r}_{c_2,7}}$			
$c_3 = 11$	1	2			$\boxed{\mathrm{r}_{c_3,11}}$		
						...	
c_n	1	2					$\boxed{\mathrm{r}_{c_n,c_n+2}}$

Le plus petit nombre premier jumeau cadet 3 est congru à 0 ($mod\ 3$), les autres restes nuls se trouvent sur la deuxième diagonale descendante du tableau qui contient des restes modulaires de la forme $r_{i,i}$. La diagonale utilisée pour appliquer l'argument de Cantor est la troisième diagonale descendante, dont on a encadré les éléments dans le tableau.

Pour "perturber la diagonale", on change chacun des restes modulaires qui lui appartient par un autre reste modulaire selon le module considéré, le nouveau reste choisi devant respecter deux contraintes seulement : ne pas être nul et ne pas être égal à $p-2$ quand on traite le module premier p (pour assurer que l'aîné de ce nombre premier est bien un nombre premier également).

On a inventé un ensemble de restes qui n'était pas déjà une ligne du tableau. Si notre ensemble d'ensembles de restes avait été complet, il aurait dû contenir cette nouvelle ligne or il ne la contient pas. Cela est contradictoire avec notre hypothèse de finitude de l'ensemble des nombres premiers jumeaux. L'idée du codage entraîne la contradiction [1]. On s'est appuyé pour pouvoir construire le "nouvel ensemble de restes" sur l'*Axiome du choix* qui a pour conséquence qu'on peut toujours choisir dans des ensembles d'entiers naturels contenant chacun 5 nombres ou plus un nombre dans chaque ensemble, en respectant la contrainte que, dans chacun des ensembles, l'élément choisi soit non nul et différent d'une valeur donnée.

[1] Cet ensemble de restes est le codage d'un nombre premier jumeau cadet qui n'appartient pas à l'ensemble des jumeaux cadets que l'on a supposé fini. La constitution même de ce nouvel ensemble de restes nous garantit que c'est un nombre premier jumeau cadet qui est inférieur à $(c_n+2)^2$ que le théorème des restes chinois nous permet de calculer : aucun de ses restes selon les modules premiers compris entre 2 et c_n+2 n'est nul et dans la mesure où aucun de ses restes selon un module premier p n'est égal à $p-2$ (on s'est assuré de cela en construisant le nouvel ensemble de restes par perturbation de la bonne diagonale du tableau), ce nombre augmenté de 2 est premier également puisqu'il n'a aucun reste nul selon les nombres premiers considérés.