

Note Julyrev (Denise Vella-Chemla, 21.7.18)

On cherche à démontrer la conjecture de Goldbach qui stipule que tout nombre pair $n > 2$ est la somme de deux nombres premiers.

On note $\mathcal{P} = \{3, 5, 7, 11, 13, 17, \dots\}$ l'ensemble des nombres premiers impairs et $\overline{\mathcal{P}} = \{9, 15, 21, 25, 27, \dots\}$ l'ensemble des nombres composés impairs > 1 .

Soit $n \geq 6$ un entier pair. On appelle *décomposition de n* un couple (p, q) d'entiers impairs > 1 tels que $n = p + q$, p est un nombre premier et $p \leq q$. Une telle décomposition est dite *décomposition de Goldbach* si q est également premier. Le nombre de décompositions de Goldbach de n est noté :

$$X_{pp}(n) = \text{Card}(\{(p, q) \in \mathcal{P} \times \mathcal{P} : p + q = n, p \leq n/2\})$$

On s'intéresse ici à la manière dont ce nombre évolue lorsqu'on passe de n à $n + 2$. On note $X_{p\overline{p} \rightarrow pp}(n)$ les décompositions de $n = p + q$ qui ne sont pas des décompositions de Goldbach de n (q est composé) mais qui "deviennent" des décompositions de Goldbach de $n + 2$ ($q + 2$ est premier) et $X_{pp \rightarrow p\overline{p}}(n)$ les décompositions de Goldbach de $n = p + q$ (q est premier) qui "se perdent" pour $n + 2$ ($q + 2$ est composé).

$$\begin{aligned} X_{p\overline{p} \rightarrow pp}(n) &= \text{Card}(\{(p, q) \in \mathcal{P} \times \overline{\mathcal{P}} : p + q = n, p \leq n/2, n + 2 - p \in \mathcal{P}\}) \\ X_{pp \rightarrow p\overline{p}}(n) &= \text{Card}(\{(p, q) \in \mathcal{P} \times \mathcal{P} : p + q = n, p \leq n/2, n + 2 - p \in \overline{\mathcal{P}}\}) \end{aligned}$$

On a la relation de récurrence suivante pour $X_{pp}(n)$:

$$X_{pp}(n + 2) = X_{pp}(n) + X_{p\overline{p} \rightarrow pp}(n) - X_{pp \rightarrow p\overline{p}}(n) + \text{premier}\left(\frac{n+2}{2}\right)$$

On veut avoir l'assurance que $X_{pp}(n)$ est toujours strictement positif puisque $X_{pp}(n)$ compte les décompositions de Goldbach de n^* .

L'ajout du booléen $\text{premier}\left(\frac{n+2}{2}\right)$ assure la positivité stricte de $X_{pp}(n)$ pour tout $n = 2p$ double de p nombre premier, qui vérifie trivialement la conjecture de Goldbach.

Hormis ces cas triviaux de vérification de la conjecture, on souhaite démontrer que $X_{pp}(n)$ est toujours supérieur à $X_{pp \rightarrow p\overline{p}}(n)$, le nombre qui lui est retranché dans la relation de récurrence.

On sait que $X_{pp}(n)$ est strictement positif jusqu'à 4.10^{18} (par calcul par ordinateur d'Oliveira e Silva en 2014).

$X_{pp \rightarrow p\overline{p}}(n)$, le nombre à retrancher à $X_{pp}(n)$, est maximum lorsque n est de la forme $6k + 2$. C'est un fait que l'on découvre par programme et que l'on peut expliquer.

Les tableaux de valeurs fournis en annexe montrent que pour tout n de la forme $6k + 2$, on a

$$X_{pp}(n) = X_{pp \rightarrow p\overline{p}}(n) + \epsilon(n).$$

avec $\epsilon(n)$ qui prend soit la valeur 1 (lorsque 3 est un décomposant de n , 1 étant composé, la décomposition $3 + (n - 3)$ n'est pas comptabilisée par $X_{pp \rightarrow p\overline{p}}(n)$) soit la valeur 0.

Il faut d'abord avoir à l'esprit que si l'on considère les 5 nombres premiers 3, 5, 7, 11 et 19, ces 5 nombres ne peuvent jamais être simultanément décomposants de Goldbach d'un nombre pair n car ils couvrent à eux cinq tous les restes possibles modulo 5 (ils ont 3, 0, 2, 1 et 4 pour reste dans une division par 5). En effet, on sait par l'étude des congruences[†] que x est un décomposant de Goldbach de n si et seulement si $x \not\equiv n \pmod{p}$ pour tout nombre premier p inférieur ou égal à \sqrt{n} . Si les 5 nombres premiers ci-dessus étaient simultanément décomposants de Goldbach de n , n n'aurait aucun reste modulaire possible selon le module 5. On voit en étudiant les définitions de $X_{p\overline{p} \rightarrow pp}(n)$ et $X_{pp \rightarrow p\overline{p}}(n)$ que parmi les nombres premiers inférieurs à $n/2$ (et notamment parmi les 5 nombres premiers ci-dessus, choisis du fait de leur couverture totale des restes modulaires dans $\mathbb{Z}/5\mathbb{Z}$, ou plus généralement dans la mesure où tous les nombres premiers inférieurs à n ne peuvent être simultanément décomposants de Goldbach de n), certains sont comptabilisés

*. On note qu'il est inutile de comptabiliser les nombres de décompositions qui ne sont ni décompositions de Goldbach de n , ni décompositions de Goldbach de $n + 2$ (auxquelles aurait été associée la variable $X_{p\overline{p} \rightarrow pp}(n)$) ou encore les nombres de décompositions qui sont à la fois des décompositions de Goldbach de n et de $n + 2$ (auxquelles aurait été associée la variable $X_{pp \rightarrow pp}(n)$) car ces nombres de décompositions ne font pas varier $X_{pp}(n)$ lors du passage de n à $n + 2$.

†. voir par exemple une note écrite en octobre 2007, *Changer l'ordre sur les entiers pour comprendre le partage des décomposants de Goldbach* téléchargeable sur le site <http://denisevellachemla.eu/reordonner.pdf>.

par $X_{pp \rightarrow p\bar{p}}(n)$ et ceux qui ne sont pas petits sommants d'une décomposition de Goldbach de n doivent également être comptabilisés, on se dit qu'ils le sont par la variable $X_{p\bar{p} \rightarrow pp}(n)$ (ils ne disparaissent pas dans la nature). Cet argument semble assurer la positivité stricte de $X_{p\bar{p} \rightarrow pp}(n)$ même si c'est un argument bizarre car on pense "tous les non-décomposants de Goldbach de n pourraient rester des non-décomposants de Goldbach de $n + 2$ " mais comme on a fait ce choix de ne pas comptabiliser les non-décomposants de Goldbach et qui le restent, dans la mesure où ils ne font pas varier $X_{pp}(n)$, il semblerait que la nécessité d'avoir les deux sortes de décompositions pour n ait pour conséquence qu'un non-décomposant de Goldbach au moins de n devient un décomposant de Goldbach de $n + 2$. On n'est pas bien convaincue, on dirait que ça ne va pas.

Voyons pourquoi, dans le cas où n est de la forme $6k + 2$, $X_{pp \rightarrow p\bar{p}}(n) = X_{pp}(n) - \epsilon(n)$: dans un tel cas, les nombres premiers de la forme $6k' - 1$ ne peuvent être décomposants de Goldbach de n car alors $n - x = (6k + 2) - (6k' - 1) = 6(k - k') + 3$ est divisible par 3. Les nombres premiers x qui peuvent être des décomposants de Goldbach de n sont alors de la forme $6k' + 1$; ce fait a pour conséquence que $n + 2 - x = (6k + 4) - (6k' + 1) = 6(k - k') + 3$ est divisible par 3 et est donc comptabilisé par $X_{pp \rightarrow p\bar{p}}(n)$. On a $X_{pp}(n) = X_{pp \rightarrow p\bar{p}}(n) + \epsilon(n)$, ce qui pourrait entraîner l'annulation de $X_{pp}(n)$ mais l'addition de $X_{p\bar{p} \rightarrow pp}(n)$ dont on a expliqué au paragraphe précédent la nécessaire positivité stricte permet d'éviter une telle annulation.

Les cas correspondant aux nombres n de la forme $6k + 2$ sont ceux pour lesquels tous les décomposants de Goldbach de n ne pouvant être des décomposants de Goldbach de $n + 2$, l'intégralité de leur nombre doit être soustrait de $X_{pp}(n)$. Comme on a alors $X_{pp}(n+2) = X_{pp}(n) - X_{pp}(n) + X_{p\bar{p} \rightarrow pp}(n)$, c'est alors seulement l'argument de la positivité stricte de $X_{p\bar{p} \rightarrow pp}(n)$ qui permet d'éviter l'annulation pour $X_{pp}(n + 2)$.

Dans les cas où n est de la forme $6k$ ou $6k + 4$, on voit que $X_{pp}(n)$ est toujours strictement à $X_{pp \rightarrow p\bar{p}}(n)$, ce qui garantit sa positivité stricte lorsqu'on lui soustrait $X_{pp \rightarrow p\bar{p}}(n)$. Pourquoi cela a-t-il lieu ? Par sa définition, $X_{pp \rightarrow p\bar{p}}(n)$ est le cardinal d'un sous-ensemble de l'ensemble qui a pour cardinal $X_{pp}(n)$ ($X_{pp \rightarrow p\bar{p}}(n)$ compte en effet les décompositions de Goldbach de $n = x + (n - x)$ telles que $n + 2 - x$ n'est pas premier) ; si $X_{pp}(n)$ était égal à $X_{pp \rightarrow p\bar{p}}(n)$, on aurait alors, du fait de cette définition de $X_{pp \rightarrow p\bar{p}}(n)$, pour toute décomposition de Goldbach de n , à la fois $n - x$ premier et $n + 2 - x$ premier, entraînant que $x + (n + 2 - x)$ serait une décomposition de Goldbach de $n + 2$ (c'est-à-dire que tous les décomposants de Goldbach de n se transfèreraient à $n + 2$). Mais toutes ces incongruences ne sauraient advenir simultanément, et entre x et n , et entre x et $n + 2$ ([et pourquoi pas ?](#)). Cela a pour conséquence que pour les n des formes $6k$ et $6k + 4$, $X_{pp \rightarrow p\bar{p}}(n) < X_{pp}(n)$ et entraîne, par héritage de n à $n + 2$, que $X_{pp}(n)$ est strictement positif pour tout $n \geq 6$.

Annexe : exemples de décompositions et valeurs des variables

n									$X_{pp}(n)$	$X_{p\bar{p} \rightarrow pp}(n)$	$X_{pp \rightarrow p\bar{p}}(n)$	$2p$
6	3 + 3								1	0	0	
8	3 + 5								1	0	0	1
10	3 + 7	5 + 5							2	0	1	
12		5 + 7							1	1	1	1
14	3 + 11		7 + 7						2	1	1	
16	3 + 13	5 + 11							2	1	1	
18		5 + 13	7 + 11						2	1	1	
20	3 + 17		7 + 13						2	1	1	1
22	3 + 19	5 + 17		11 + 11					3	1	1	
24		5 + 19	7 + 17	11 + 13					3	1	2	1
26	3 + 23		7 + 19		13 + 13				3	2	3	
28		5 + 23		11 + 17					2	2	1	
30			7 + 23	11 + 19	13 + 17				3	1	2	
32	3 + 29				13 + 19				2	2	1	1
34	3 + 31	5 + 29		11 + 23		17 + 17			4	2	2	
36		5 + 31	7 + 29		13 + 23	17 + 19			4	0	3	1
38			7 + 31			19 + 19			2	3	2	
40	3 + 37			11 + 29		17 + 23			3	3	2	
42		5 + 37		11 + 31	13 + 29		19 + 23		4	2	3	
44	3 + 41		7 + 37		13 + 31				3	2	2	1
46	3 + 43	5 + 41				17 + 29	23 + 23		4	3	2	
48		5 + 43	7 + 41	11 + 37		17 + 31	19 + 29		5	2	3	
50	3 + 47		7 + 43		13 + 37		19 + 31		4	3	4	
52		5 + 47		11 + 41			23 + 29		3	3	1	
54			7 + 47	11 + 43	13 + 41	17 + 37	23 + 31		5	2	4	
56	3 + 53				13 + 43		19 + 37		3	3	3	1
58		5 + 53		11 + 47		17 + 41		29 + 29	4	4	2	
60			7 + 53		13 + 47	17 + 43	19 + 41	23 + 37	29 + 31	6	5	1

n	$X_{pp}(n)$	$X_{p\bar{p} \rightarrow pp}(n)$	$X_{pp \rightarrow p\bar{p}}(n)$	$2p$
99932	745	630	745	
99934	630	1107	508	
99936	1229	467	1109	
99938	587	859	587	
99940	859	1015	675	
99942	1199	541	1064	
99944	676	835	676	
99946	835	1010	665	
99948	1180	630	1000	
99950	810	613	810	
99952	613	1089	508	
99954	1194	494	1083	
99956	605	660	605	
99958	660	1802	399	
99960	2063	374	1819	
99962	618	606	618	
99964	606	1113	497	
99966	1222	565	1079	
99968	708	900	708	
99970	900	1009	719	
99972	1190	587	1041	
99974	736	601	736	
99976	601	1140	477	
99978	1264	620	1083	
99980	801	607	801	1
99982	608	1092	484	
99984	1216	475	1089	1
99986	603	736	603	
99988	736	1596	477	
99990	1855	425	1642	
99992	638	650	637	
99994	651	1163	511	
99996	1303	478	1177	1
99998	605	810	605	
100000	810	1213	600	