Proposition de démonstration de la conjecture de Goldbach

Denise Vella-Chemla

30 juin 2018

On cherche à démontrer la conjecture de Goldbach. On définit 4 variables ainsi :

$$X_a(n) = \#\{p+q=n \textit{ tels que } p \textit{ et } q \textit{ impairs},\ 3 \leqslant p \leqslant n/2,\ p \textit{ et } q \textit{ premiers}\}$$

$$X_b(n) = \#\{p+q=n \textit{ tels que } p \textit{ et } q \textit{ impairs},\ 3 \leqslant p \leqslant n/2,\ p \textit{ composé et } q \textit{ premier}\}$$

$$X_c(n) = \#\{p+q=n \textit{ tels que } p \textit{ et } q \textit{ impairs},\ 3 \leqslant p \leqslant n/2,\ p \textit{ premier et } q \textit{ composé}\}$$

$$X_d(n) = \#\{p+q=n \textit{ tels que } p \textit{ et } q \textit{ impairs},\ 3 \leqslant p \leqslant n/2,\ p \textit{ et } q \textit{ composés}\}$$

Dans la suite de ce document, on note $E(x)$ la partie entière de x (i.e. $\lfloor x \rfloor$) et $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x. On dispose de l'égalité ci-dessous : elle découle des démonstrations par récurrence d'une note [DV] d'octobre 2014 [*].

$$X_d(n) - X_a(n) = E(n/4) - \pi(n) + \delta(n) \qquad (1)$$

$\delta(n)$ prend les valeurs 0,1 ou 2.

Simplification des propositions de la note [DV] par Alain Connes en mai 2018 : [(1) résulte du fait très général sur des sous-ensembles quelconques et les cardinalités d'intersection et réunion :

$$\#(P \cup Q) + \#(P \cap Q) = \#(P) + \#(Q) \qquad (2)$$

Ici (en négligeant les cas limites qui contribuent à $\delta(n)$), on voit que
(a) $\#(P \cap Q)$ correspond à $X_a(n)$.
(b) $\#(P \cup Q)$ correspond à $E(n/4) - X_d(n)$.
(c) $\#(P) + \#(Q)$ correspond à $\pi(n)$.
On a donc une preuve très simple de (1) comme conséquence de (2).]

Voyons maintenant une propriété concernant $X_a(n)$.

On décide de représenter les nombres composés par la couleur grise et les nombres premiers par la couleur blanche.

On représente les nombres impairs compris entre 3 et $n/2$ par les rectangles de la partie inférieure du dessin ci-dessous et les nombres impairs compris entre $n/2$ et n, complémentaires à n des nombres de la partie inférieure par les rectangles de la partie supérieure. Les rectangles symbolisent ainsi des ensembles de colonnes contigues contenant dans leur partie inférieure un nombre x et dans leur partie supérieure son complémentaire $n-x$. On positionne les colonnes contigument selon la nature des décompositions qu'elles contiennent (selon que les colonnes sont de type a, b, c ou d).

On utilise les couleurs :
- verte pour $\#(P \cap Q)$;
- rouge pour $\#(P \cup Q)$;
- bleue pour $\#(P) + \#(Q) = \pi(n)$.

[*]. Note [DV] : http://denise.vella.chemla.free.fr/nombres-et-lettres.pdf, version en anglais sur Hal https://hal.archives-ouvertes.fr/hal-01109052.

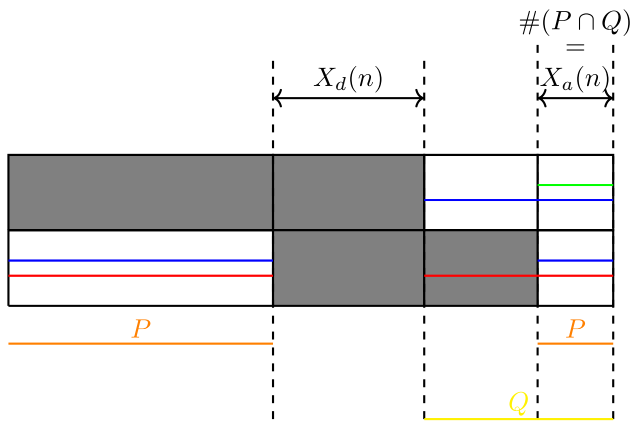

Figure 1 : ensembles de décompositions de n disposées contigument selon leur nature

Réécrivons pour rappel l'identité ensembliste (2) en $\#(P) + \#(Q) - \#(P \cup Q) = \#(P \cap Q)$.

et remplaçons les cardinaux par les variables associées, on obtient bien

$$\pi(n) - E(n/4) + X_d(n) - \delta(n) = X_a(n)$$

dont on veut avoir l'assurance qu'il est toujours strictement positif puisque $X_a(n)$ compte les décompositions de Goldbach de n (en somme de deux nombres premiers).

Cependant, si on a démontré que $X_a(n) = X_d(n) - E(n/4) + \pi(n) - \delta(n)$ est une relation toujours vérifiée, cette relation ne garantit pas qu'à partir d'un certain rang, $X_a(n)$ est toujours strictement positif.

On note

$$\begin{aligned} Crédit(n) &= \sum_{3 \leqslant x \leqslant n/2} (BooleanPrime(x) \wedge \neg BooleanPrime(n-x) \wedge BooleanPrime(n+2-x)) \\ Débit(n) &= \sum_{3 \leqslant x \leqslant n/2} (BooleanPrime(x) \wedge BooleanPrime(n-x) \wedge \neg BooleanPrime(n+2-x)) \end{aligned}$$

On trouve la relation de récurrence suivante pour $X_a(n)$, très comptable :

$$X_a(n+2) = X_a(n) + Crédit(n) - Débit(n) + BooleanPrime(\tfrac{n+2}{2})$$

L'ajout du booléen $BooleanPrime(\frac{n+2}{2})$ assure la positivité stricte de $X_a(n)$ pour tout double de nombre premier, qui vérifie trivialement la conjecture de Goldbach.

Hormis ces cas triviaux de vérification de la conjecture, on souhaite démontrer que $X_a(n)$ est toujours supérieur à $Débit(n)$. On sait qu'$X_a(n)$ est strictement positif jusqu'à 4.10^{18} (par calcul par ordinateur d'Oliveira e Silva en 2014).

On trouve d'abord ce qui assure la positivité de $X_a(n)$ pour les nombres $n = 6k + 2$.

Les tableaux de valeurs fournis en annexe montrent que pour quasiment tous les $n = 6k + 2$ (notamment du second tableau), on a

$$X_a(n) = Débit(n) + \epsilon(n).$$

$\epsilon(n)$ 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 $Débit(n)$) soit la valeur 0.

On voit en étudiant les définitions de $Crédit(n)$ et $Débit(n)$ que parmi les nombres premiers inférieurs à $n/2$, certains sont comptabilisés dans $Crédit(n)$ tandis que les autres sont comptabilisés dans $Débit(n)$, dans la mesure où tous les nombres premiers inférieurs à n ne peuvent être simultanément décomposants de Goldbach de n. Cet argument assure la positivité stricte de $Crédit(n)$.

Voyons pourquoi, dans le cas où n est de la forme $6k + 2$, $Débit(n) = X_a(n) - \epsilon(n)$: 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 dans les débits. On a $X_a(n) = Débit(n) + \epsilon(n)$, ce qui pourrait entraîner l'annulation de $X_a(n)$ mais l'addition de $Crédit(n)$ strictement positif permet d'éviter une telle annulation.

Dans les cas où n est de la forme $6k$ ou $6k+4$, on voit que $X_a(n)$ est toujours supérieur strictement à $Débit(n)$, ce qui garantit sa positivité stricte lorsqu'on lui soustrait $Débit(n)$. Essayons d'expliquer pourquoi cela a lieu : par sa définition, $Débit(n)$ est le cardinal d'un sous-ensemble de l'ensemble qui a pour cardinal $X_a(n)$ ($Débit(n)$ compte en effet les décompositions de Goldbach de $n = x + (n-x)$ telles que $n+2-x$ n'est pas premier) ; si $X_a(n)$ était égal à $Débit(n)$, on aurait alors, du fait de cette définition de $Débit(n)$, 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 on sait par l'étude des congruences [†] que x est un décomposant de Goldbach de n si et seulement si $x \not\equiv n \ (mod\ p)$ pour tout nombre premier p inférieur ou égal à $\sqrt{n}$. Toutes ces incongruences ne sauraient advenir simultanément, et entre x et n, et entre x et $n+2$. Cela a pour conséquence que pour les n des formes $6k$ et $6k+4$, $Débit(n) < X_a(n)$ et entraîne, par héritage de n à $n+2$, que $X_a(n)$ est strictement positif pour tout $n \geqslant 6$.

†. 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.

Annexe 1a : tableau de valeurs des variables pour les pairs compris entre 6 et 100

n	$X_a(n)$	$Crédit$	$Débit$	$BooleanPrime(\frac{n+2}{2})$
6	1	0	0	
8	1	0	0	1
10	2	0	1	
12	1	1	1	1
14	2	1	1	
16	2	1	1	
18	2	1	1	
20	2	1	1	1
22	3	1	1	
24	3	1	2	1
26	3	2	3	
28	2	2	1	
30	3	1	2	
32	2	2	1	1
34	4	2	2	
36	4	0	3	1
38	2	3	2	
40	3	3	2	
42	4	2	3	
44	3	2	2	1
46	4	3	2	
48	5	2	3	
50	4	3	4	
52	3	3	1	
54	5	2	4	
56	3	3	3	1
58	4	4	2	
60	6	1	5	1
62	3	4	2	
64	5	4	3	
66	6	1	5	
68	2	5	2	
70	5	4	3	
72	6	2	4	1
74	5	4	4	
76	5	5	3	
78	7	1	4	
80	4	4	4	1
82	5	5	2	
84	8	3	7	1
86	5	4	5	
88	4	7	2	
90	9	2	7	
92	4	4	4	1
94	5	6	4	
96	7	2	6	
98	3	6	3	
100	6	6	4	

Annexe 1b : tableau de valeurs des variables pour les pairs compris entre 99 900 et 100 000

n	$X_a(n)$	$Crédit$	$Débit$	$BooleanPrime(\frac{n+2}{2})$
99900	1655	475	1436	
99902	694	731	694	
99904	731	1053	577	
99906	1207	506	1091	
99908	622	824	622	
99910	824	1097	633	
99912	1288	484	1176	1
99914	597	617	597	
99916	617	1435	452	
99918	1600	541	1352	
99920	789	601	789	
99922	601	1212	464	
99924	1349	510	1223	
99926	636	586	636	
99928	586	1424	420	
99930	1590	538	1383	
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	

Annexe 2 : les règles de réécriture qui permettent de passer d'un doublon de lettres du mot de n à la lettre sous la lettre de droite du mot de $n+2$

$aa \to a$	$ba \to a$	$ca \to c$	$da \to c$
$ab \to b$	$bb \to b$	$cb \to d$	$db \to d$
$ac \to a$	$bc \to a$	$cc \to c$	$dc \to c$
$ad \to b$	$bd \to b$	$cd \to d$	$dd \to d$

Annexe 3 : extraits des mots associés aux nombres pairs de 6 à 100 (ne sont fournies que les lettres associées aux décompositions de petit sommant premier).

a							
a							
aa							
ca							
aca							
aac							
caa							
aca							
aac	a						
caa	a						
aca	ca						
cac	ac						
cca	aa						
acc	ca						
aac	ac	a					
caa	ca	a					
cca	cc	ca					
acc	ac	ac					
cac	aa	ca					
aca	ca	cc					
aac	cc	ac	a				
caa	ac	aa	c				
aca	ca	ca	c				
cac	ac	cc	a				
cca	aa	ac	a				
acc	ca	ca	c				
cac	ac	ac	c	a			
cca	ca	aa	a	a			
acc	cc	ca	c	ca			
aac	ac	ac	a	cc			
caa	ca	ca	a	ac			
cca	cc	cc	c	ca			
acc	ac	ac	a	ac			
cac	aa	ca	c	aa			
aca	ca	cc	c	ca	a		
aac	cc	ac	a	ac	c		
caa	ac	aa	c	ca	a		
cca	ca	ca	c	cc	a		
acc	ac	cc	a	ac	c	a	
cac	aa	ac	a	ca	a	a	
aca	ca	ca	c	cc	c	ca	
cac	cc	ac	c	ac	c	ac	
cca	ac	aa	a	aa	a	ca	
acc	ca	ca	c	ca	c	cc	
cac	ac	cc	a	cc	c	ac	a
cca	ca	ac	a	ac	a	ca	c
ccc	cc	ca	c	ca	a	cc	c
acc	ac	ac	c	ac	c	ac	a