Proposition for a Goldbach's conjecture demonstration

Denise Vella-Chemla

June 30, 2018

One tries to demonstrate Goldbach's conjecture. One defines 4 variables :

$$X_a(n) = \#\{p+q=n \textit{ such that } p \textit{ and } q \textit{ odd},\ 3 \leqslant p \leqslant n/2,\ p \textit{ and } q \textit{ primes}\}$$

$$X_b(n) = \#\{p+q=n \textit{ such that } p \textit{ and } q \textit{ odd},\ 3 \leqslant p \leqslant n/2,\ p \textit{ compound and } q \textit{ prime}\}$$

$$X_c(n) = \#\{p+q=n \textit{ such that } p \textit{ and } q \textit{ odd},\ 3 \leqslant p \leqslant n/2,\ p \textit{ prime and } q \textit{ compound}\}$$

$$X_d(n) = \#\{p+q=n \textit{ such that } p \textit{ and } q \textit{ odd},\ 3 \leqslant p \leqslant n/2,\ p \textit{ and } q \textit{ compound}\}$$

In the following, one notes $E(x)$ the integer part of x (i.e. $\lfloor x \rfloor$) and $\pi(x)$ the number of prime numbers lesser than or equal to x. We have the equality above : it follows from recurrence demonstrations that can be found in [DV] a note written in octobre 2014 [*].

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

$\delta(n)$ takes values 0,1 or 2.

Simplification of note [DV] propositions provided by Alain Connes in may 2018 : [(1) results from the very general fact on any subsets and intersection and union cardinalities :

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

Here neglecting limit cases that contribute to $\delta(n)$), one sees that
(a) $\#(P \cap Q)$ corresponds to $X_a(n)$.
(b) $\#(P \cup Q)$ corresponds to $E(n/4) - X_d(n)$.
(c) $\#(P) + \#(Q)$ corresponds to $\pi(n)$.
Then we have a very simple proof of (1) as a consequence of (2).]

Let us see now a property concerning $X_a(n)$.

We decide to represent compound numbers by gray color and prime numbers by white color.

We represent odd numbers between 3 and $n/2$ by rectangles in the bottom of the drawing above and odd numbers between $n/2$ and n, complementary to n of numbers from the bottom of the drawing by rectangles in the top of the drawing. Rectangles represent contiguous columns associated to decompositions as two odds'sum, and containing x in their bottom part and $n-x$ their complementary in their top part. Columns are contiguously positioned according to the nature of decompositions they contain (according to their type a, b, c or d).

We use those colors :
- green for $\#(P \cap Q)$;
- red for $\#(P \cup Q)$;
- blue for $\#(P) + \#(Q) = \pi(n)$.

*. Note [DV] : http://denise.vella.chemla.free.fr/numbers-and-letters.pdf, also on Hal https://hal.archives-ouvertes.fr/hal-01109052.

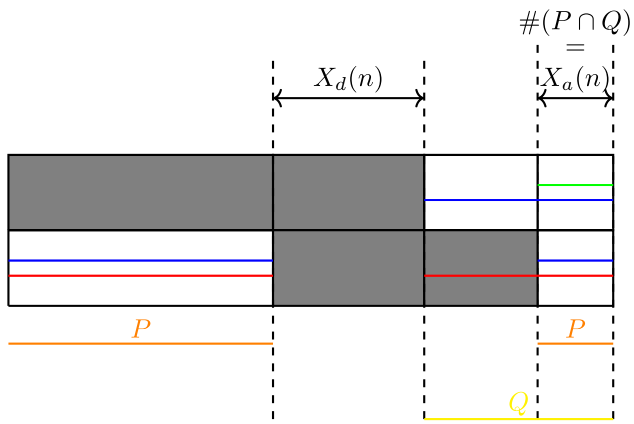

FIGURE 1 : n'decompositions contiguously positionned according to their nature

Let us remind the set identity (2) : $\#(P) + \#(Q) - \#(P \cup Q) = \#(P \cap Q)$.

and let's replace cardinals by associated variables, we obtain

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

and we wish to have the insurance that $X_a(n)$ is always strictly positive since it counts Goldbach's n's decompositions (as sum of two primes).

Although, if we demonstrated that $X_a(n) = X_d(n) - E(n/4) + \pi(n) - \delta(n)$ is a relation always verified, this relation doesn't guarantee that above a certain integer range, $X_a(n)$ is always strictly positive.

We note

$$Credit(n) = \sum_{3 \leqslant x \leqslant n/2} (BooleanPrime(x) \wedge \neg BooleanPrime(n-x) \wedge BooleanPrime(n+2-x))$$
$$Debit(n) = \sum_{3 \leqslant x \leqslant n/2} (BooleanPrime(x) \wedge BooleanPrime(n-x) \wedge \neg BooleanPrime(n+2-x))$$

We find the following recurrence relation for $X_a(n)$, very accounting :

$$X_a(n+2) = X_a(n) + Credit(n) - Debit(n) + BooleanPrime(\tfrac{n+2}{2})$$

Adding the boolean $BooleanPrime(\frac{n+2}{2})$ ensure $X_a(n)$'s positivity for all $2p$ with p prime, $2p$ verifying trivially Goldbach's conjecture.

Except those trivial cases of Goldbach's conjecture verification, we wish to demonstrate that $X_a(n)$ is always greater than $Debit(n)$. We know that $X_a(n)$ is always strictly positive below 4.10^{18} (by computer calculations from Oliveira e Silva in 2014).

First we explain what ensure $X_a(n)$ positivity for numbers $n = 6k + 2$.

Variables values arrays in annex show that for nearly all $n = 6k + 2$ (notably in the second array), we have

$$X_a(n) = Debit(n) + \epsilon(n).$$

$\epsilon(n)$ has either value 1 (when 3 is a Goldbach's decomponent of n, 1 being compound, $3 + (n - 3)$ decomposition is not counted by $Debit(n)$) or value 0.

We see studying $Credit(n)$ and $Debit(n)$ definitions that among prime numbers lesser than $n/2$, ones are counted by $Credit(n)$ while the others are counted by $Debit(n)$, because all prime numbers lesser than n can't be simultaneously Goldbach's decomponents of n. This argument ensure the strict positivity of $Credit(n)$.

Let us see now why, in the case in which n is of the form $6k + 2$, $Debit(n) = X_a(n) - \epsilon(n)$: in such a case, prime numbers of the form $6k' - 1$ can't be Goldbach's decomponent of n because if it were the case, $n - x = (6k + 2) - (6k' - 1) = 6(k - k') + 3$ would be divisible by 3. Prime numbers x that can be Goldbach's decomponents of n are thus of the form $6k' + 1$; this fact has as consequance that

$n+2-x = (6k+4)-(6k'+1) = 6(k-k')+3$ is divisible by 3 and is thus countable as a debit. We have $X_a(n) = Debit(n) + \epsilon(n)$, that could implies $X_a(n)$'s vanishing but the $Credit(n)$ addition, $Credit(n)$ being strictly positive permits to avoid such a vanishing.

In the case where n is of the form $6k$ or $6k+4$, one sees that $X_a(n)$ is always strictly greater than $Debit(n)$, what guarantees its strict positivity when one substracts $Debit(n)$ to it. Let us try to explain why this is the case : by its definition, $Debit(n)$ is the cardinality of a subset of the set of cardinal $X_a(n)$ (indeed, $Debit(n)$ counts Goldbach's decompositions of $n = x+(n-x)$ such that $n+2-x$ is not prime) ; if $X_a(n)$ were equal to $Debit(n)$, we would have, from the definition of $Debit(n)$, for all Goldbach's decomposition of n, at the same time $n-x$ prime and $n+2-x$ prime, implying that $x+(n+2-x)$ would be a Goldbach's decomposition of $n+2$ (i.e. that all Goldbach's decompositions $p1+p2$ of n would be inherited as Goldbach's decompositions $p1+(p2+2)$ by $n+2$). But we know by congruences study † that x is a Goldbach's decomponent of n if and only if $x \not\equiv n \ (mod\ p)$ for every p lesser than $\sqrt{n}$. All those incongruences couldn't be verified all at the same time, on one side by x and n, and on the other side by x and $n+2$. This has as consequence that for even numbers n of the forms $6k$ and $6k+4$, $Debit(n) < X_a(n)$ and it implies, by inheritance from n to $n+2$, that $X_a(n)$ is strictly positive for all $n \geqslant 6$.

†. see for instance a october 2007 note, *Changer l'ordre sur les entiers pour comprendre le partage des décomposants de Goldbach* that can be downloaded at http://denisevellachemla.eu.

Annex 1a : variables values array for even numbers between 6 and 100

n	$X_a(n)$	$Credit$	$Debit$	$BooleanPrime(\frac{n+2}{2})$
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	

Annex 1b : variables values array for even numbers between 99 900 and 100 000

n	$X_a(n)$	$Credit$	$Debit$	$BooleanPrime(\frac{n+2}{2})$
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	

Annex 2 : rewriting rules that permit to find a letter of $n+2$'s word knowing two letters from n's word

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

Annex 3 : parts of words associated to even numbers between 6 and 100 (are only provided the letters concerning decompositions of n as sums of the form $p+x$ with p a prime between 3 and $n/2$

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*