Conjecture de Goldbach, mots booléens et invariant

Denise Vella-Chemla

29/1/14

1 Introduction

On souhaite trouver une démonstration de la conjecture de Goldbach, qui stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers [1].

On se propose dans ce but d'utiliser une modélisation qui associe à chaque nombre pair n un "mot booléen de primalité" m qui code la primalité des nombres impairs x (compris entre 3 et et $n-3$).

On identifiera le processus permettant de passer du mot booléen d'un nombre pair n au mot booléen du nombre pair suivant $n+2$.

On caractérisera l'existence d'un décomposant de Goldbach d'un nombre pair par une condition que vérifie son mot booléen.

On essaiera de trouver une contrainte invariante respectée par les mots booléens des nombres pairs successifs qui assurera que l'existence d'un décomposant de Goldbach est toujours conservée.

2 Mot booléen d'un nombre pair

On choisit de représenter le fait qu'un entier est premier par le booléen 0 et le fait qu'il est composé par le booléen 1.

On appelle $sym(m)$ la fonction qui associe à un mot m son symétrique, i.e. le mot contenant les lettres de m depuis la dernière jusqu'à la première.

Appelons *milieu* le plus grand nombre entier impair inférieur ou égal à $n/2$.

1. Dans l'égalité $n = p + q$ avec n pair supérieur à 2, p et q premiers, on appellera p et q décomposants de Goldbach de n ou sommants.

A chaque nombre pair n sont associés deux mots booléens m_1 et m_2 définis de la façon suivante :

- les lettres de m_1 sont les caractères de primalité des nombres impairs compris entre 3 et *milieu* inclus ;
- les lettres de m_2 sont les caractères de primalité des nombres impairs compris entre $n-3$ et *milieu* inclus.

Les mots m_1 et m_2 associés au nombre pair n sont de longueur $\left\lfloor \frac{n/2-1}{2} \right\rfloor$. La longueur des mots augmente donc de 1 à chaque double d'impair, i.e. une fois sur deux.

Le mot booléen m du nombre pair n est la concaténation des deux mots suivants :

- m_1 ;
- $sym(m_2)$, le symétrique de m_2.

Note : on a pris pour habitude de fournir le mot m_2 en première ligne et le mot m_1 en deuxième ligne (3 en bas à gauche, $n-3$ en haut à gauche). On constate que pour les doubles d'impairs, la lettre codant le caractère de primalité de l'entier *milieu* est doublée.

Exemples : Ci-dessous les mots m_1, m_2 et m des nombres 40, 42 et 44.

40	37	35	33	31	29	27	25	23	21									
m_2	0	1	1	0	0	1	1	0	1									
m_1	0	0	0	1	0	0	1	0	0									
	3	5	7	9	11	13	15	17	19									
m	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0

42	39	37	35	33	31	29	27	25	23	21									
m_2	1	0	1	1	0	0	1	1	0	1									
m_1	0	0	0	1	0	0	1	0	0	1									
	3	5	7	9	11	13	15	17	19	21									
m	0	0	0	1	0	0	1	0	0	1	1	0	1	1	0	0	1	1	0	1

44	41	39	37	35	33	31	29	27	25	23										
m_2	0	1	0	1	1	0	0	1	1	0										
m_1	0	0	0	1	0	0	1	0	0	1										
	3	5	7	9	11	13	15	17	19	21										
m	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0

3 Identifier ce que fait le processus

Reprenons les mots des nombres pairs 24 à 34.

24	m_2	1	0	0	1	0											
	m_1	0	0	0	1	0											
	m	0	0	0	1	0	|	0	1	0	0	1					
26	m_2	0	1	0	0	1	0										
	m_1	0	0	0	1	0	0										
	m	0	0	0	1	0	0	|	0	1	0	0	1	0			
28	m_2	1	0	1	0	0	1										
	m_1	0	0	0	1	0	0										
	m	0	0	0	1	0	0	|	1	0	0	1	0	1			
30	m_2	1	1	0	1	0	0	1									
	m_1	0	0	0	1	0	0	1									
	m	0	0	0	1	0	0	1	|	1	0	0	1	0	1	1	
32	m_2	0	1	1	0	1	0	0									
	m_1	0	0	0	1	0	0	1									
	m	0	0	0	1	0	0	1	|	0	0	1	0	1	1	0	
34	m_2	0	0	1	1	0	1	0	0								
	m_1	0	0	0	1	0	0	1	0								
	m	0	0	0	1	0	0	1	0	|	0	0	1	0	1	1	0	0

On voit que si au nombre pair n est associé un mot booléen de longueur $2i$, le processus qui permet d'obtenir le mot booléen associé au nombre pair $n+2$ effectue plusieurs actions différentes :

- 1) *travail sur la lettre à la position* $i+1$: dans le cas où n est un double d'impair, le mot de $n+2$ est obtenu en enlevant du mot de n la lettre à la position $i+1$; dans le cas où n est un double de pair, le mot de $n+2$ est obtenu en dupliquant cette lettre à la position $i+1$;
- 2) *concaténation en fin du mot :* dans tous les cas, est concaténée à la fin du mot booléen ainsi obtenu la lettre qui caractérise la primalité du nombre entier $2n-3$ pour obtenir le mot de $n+2$.

4 Caractériser une décomposition de Goldbach

Il faut maintenant être capable de caractériser par une condition sur le mot m la présence à une même position dans les mots m_1 et m_2 d'une lettre 0.

Cette caractérisation est simple :

- un double d'impair n se décompose en somme de deux nombres premiers $p = 2i+1$ et $q = 2j-1$ si et seulement si le mot m de n contient une lettre 0 à la position i et une lettre 0 à la position j ;
- un double de pair n se décompose en somme de deux nombres premiers $p = 2i+1$ et $q = 2j+1$ si et seulement si le mot m de n contient une

lettre 0 à la position i et une lettre 0 à la position j.

On note que la somme des positions i et j des deux 0 dans le mot m est toujours un nombre impair.

5 Invariant

Supposons que le mot n admet une décomposition de Goldbach. Essayons de comprendre pourquoi une décomposition va également exister pour $n+2$.

L'invariant est à rechercher dans la liste des positions des 0 successifs dans le mot m.

Si lors de l'étape de concaténation, on concatène la lettre 0 pour obtenir le mot de $n+2$, l'existence d'une décomposition de Goldbach est garantie par le fait que $n+2$ se décompose en $3+(n-1)$.

Dans le cas contraire, si lors de l'étape de concaténation, on concatène un 1 pour obtenir le mot de $n+2$, alors 4 cas sont à considérer, selon que la longueur de la chaîne est conservée ou bien incrémentée de 2 :

- la chaîne conserve sa longueur et on enlève la lettre 0 à la position $i+1$; les mots m_1 et m_2 de $n+2$ ont les formes suivantes :

m_2	1	1	$-$	$-$	$\ldots$	$-$	0	$\ldots$	$-$
m_1	0	0	0	1	$\ldots$	0	$-$	$\ldots$	0

  La lettre 0 en fin de m_1 est justifiée par le fait que si la longueur des mots est conservée, n est forcément un double d'impair premier. On ne voit pas encore ce qui garantit qu'ils contiennent une lettre 0 à une position commune ;

- la chaîne conserve sa longueur et on enlève la lettre 1 à la position $i+1$; les mots m_1 et m_2 de $n+2$ ont les formes suivantes :

m_2	1	$-$	$-$	$-$	$\ldots$	$-$	0	$\ldots$	$-$
m_1	0	0	0	1	$\ldots$	0	$-$	$\ldots$	1

  La lettre 1 en fin de m_1 est justifiée par le fait que si la longueur des mots est conservée, n est forcément un double d'impair composé. On ne voit pas encore ce qui garantit qu'ils contiennent une lettre 0 à une position commune ;

- la chaîne voit sa longueur incrémentée de 2 et la lettre 0 en position $i+1$ est dupliquée ; alors $n+2$ est le double d'un nombre premier p et admet une décomposition de Goldbach triviale $p+p$.

- la chaîne voit sa longueur incrémentée de 2 et la lettre 1 en position $i+1$ est dupliquée ; alors $n+2$ est le double d'un nombre composé, ce qui justifie les lettres 1 en fin des mots m_1 et m_2 ; les mots m_1 et m_2 de $n+2$ ont les formes suivantes :

m_2	1	$-$	$-$	$-$	$\ldots$	$-$	0	$\ldots$	1
m_1	0	0	0	1	$\ldots$	0	$-$	$\ldots$	1

On ne voit pas encore ce qui garantit qu'ils contiennent une lettre 0 à une position commune ;

Annexe : Mots m_1, m_2 des nombres pairs de 24 à 50

24	m_2	1	0	0	1	0										
	m_1	1	0	0	1	0										
26	m_2	0	1	0	0	1	0									
	m_1	1	1	0	1	0	0									
28	m_2	1	0	1	0	0	1									
	m_1	1	1	0	1	0	0									
30	m_2	1	1	0	1	0	0	1								
	m_1	1	1	0	1	0	0	1								
32	m_2	0	1	1	0	1	0	0								
	m_1	1	1	0	1	0	0	1								
34	m_2	0	0	1	1	0	1	0	0							
	m_1	1	1	0	1	0	0	1	0							
36	m_2	1	0	0	1	1	0	1	0							
	m_1	1	1	0	1	0	0	1	0							
38	m_2	1	1	0	0	1	1	0	1	0						
	m_1	1	1	0	1	0	0	1	0	0						
40	m_2	0	1	1	0	0	1	1	0	1						
	m_1	1	1	0	1	0	0	1	0	0						
42	m_2	1	0	1	1	0	0	1	1	0	1					
	m_1	1	1	0	1	0	0	1	0	0	1					
44	m_2	0	1	0	1	1	0	0	1	1	0					
	m_1	1	1	0	1	0	0	1	0	0	1					
46	m_2	0	0	1	0	1	1	0	0	1	1	0				
	m_1	1	1	0	1	0	0	1	0	0	1	0				
48	m_2	1	0	0	1	0	1	1	0	0	1	1				
	m_1	1	1	0	1	0	0	1	0	0	1	0				
50	m_2	0	1	0	0	1	0	1	1	0	0	1	1			
	m_1	1	1	1	1	0	0	1	0	0	1	0	1			
52	m_2	1	0	1	0	0	1	0	1	1	0	0	1			
	m_1	0	0	0	1	0	0	1	0	0	1	0	1			
54	m_2	1	1	0	1	0	0	1	0	1	1	0	0	1		
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1		
56	m_2	0	1	1	0	1	0	0	1	0	1	1	0	0		
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1		
58	m_2	1	0	1	1	0	1	0	0	1	0	1	1	0	0	
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	
60	m_2	1	1	0	1	1	0	1	0	0	1	0	1	1	0	
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	
62	m_2	0	1	1	0	1	1	0	1	0	0	1	0	1	1	0
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0
64	m_2	0	0	1	1	0	1	1	0	1	0	0	1	0	1	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0
66	m_2	1	0	0	1	1	0	1	1	0	1	0	0	1	0	1	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1
68	m_2	1	1	0	0	1	1	0	1	1	0	1	0	0	1	0	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1

70	m_2	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1	0	1							
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1							
72	m_2	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1	0							
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1							
74	m_2	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1	0						
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0						
76	m_2	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1						
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0						
78	m_2	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1					
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1					
80	m_2	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0					
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1					
82	m_2	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0				
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0				
84	m_2	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0				
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0				
86	m_2	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0			
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0			
88	m_2	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1			
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0			
90	m_2	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1		
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1		
92	m_2	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0		
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1		
94	m_2	1	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	0	
96	m_2	1	1	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	0	
98	m_2	1	1	1	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	0	1
100	m_2	0	1	1	1	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	0	1