Conjecture de Goldbach, mots booléens, parité, imparité, invariant

Denise Vella-Chemla

2/2/14

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 :

- *travail sur la lettre à la position* $i+1$ (on a coloré cette lettre en bleu dans le tableau ci-dessus) : 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 $i+1$;
- *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 $n+2$. *Remarque :* la concaténation est une opération non-commutative. Par exemple, $1(110) = 1110$ alors que $(110)1 = 1101$.

4 Caractériser l'existence d'une décomposition de Goldbach dans le mot d'un nombre pair

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.

Rappelons quelques éléments de logique booléenne.

La conjonction logique est définie par :

$$1 \wedge 0 = 0 \wedge 1 = 0 \wedge 0 = 0 \text{ et } 1 \wedge 1 = 1.$$

La négation logique est définie par :

$$\neg 0 = 1 \text{ et } \neg 1 = 0.$$

Si l'on appelle $l(m, i)$ la lettre à la position i dans le mot m, alors l'existence d'une décomposition de Goldbach est équivalente à la condition :

$$\Big[\sum_{1 \leqslant i \leqslant \lfloor \frac{n/2-1}{2} \rfloor, i+j=\lfloor \frac{n}{2} \rfloor} \neg l(m,i) \wedge \neg l(m,j) \Big] = 1$$

5 Invariant

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

Les lettres 0 et 1 ne se trouvent pas réparties "n'importe comment" dans les mots m_1 et m_2, au fur et à mesure du déroulement du processus : une condition est toujours vérifiée par les lettres et qui correspond au fait qu'un multiple quelconque d'un nombre non nul est composé. On appelle une telle condition toujours vérifiée un invariant de l'algorithme.

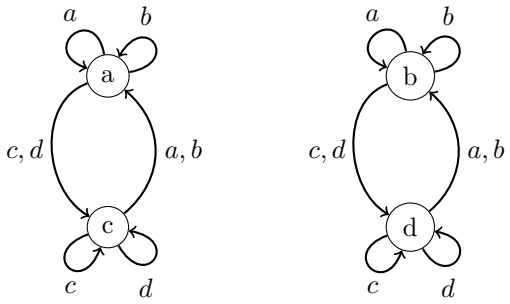
$$\forall\, 0 < i \leqslant n/2,\ \forall k \leqslant n/3, l(m, i + k(2i + 1)) = 1.$$

D'autre part, la condition dont il faut démontrer l'invariance est l'existence de deux lettres 0 à la même position dans les mots m_1 et m_2. On cherche à démontrer cette propriété d'invariance par récurrence (i.e. si n admet une décomposition de Goldbach alors $n + 2$ en admet une aussi). Pour cela, il faut peut-être analyser la manière dont les doublons de lettres à la même position dans les mots m_1 et m_2 de n se combinent lorsqu'ils sont contigus pour engendrer les doublons de lettres à la même position dans les mots m_1 et m_2 de $n+2$.

La table suivante fournit la manière dont les doublons se combinent :

	a $\binom{0}{0}$	b $\binom{0}{1}$	c $\binom{1}{0}$	d $\binom{1}{1}$
a $\binom{0}{0}$	a $\binom{0}{0}$	b $\binom{0}{1}$	a $\binom{0}{0}$	b $\binom{0}{1}$
b $\binom{0}{1}$	a $\binom{0}{0}$	b $\binom{0}{1}$	a $\binom{0}{0}$	b $\binom{0}{1}$
c $\binom{1}{0}$	c $\binom{1}{0}$	d $\binom{1}{1}$	c $\binom{1}{0}$	d $\binom{1}{1}$
d $\binom{1}{1}$	c $\binom{1}{0}$	d $\binom{1}{1}$	c $\binom{1}{0}$	d $\binom{1}{1}$

On peut représenter ces combinaisons d'états par les deux petits automates suivants :



On peut enfin représenter cette même connaissance par les règles de réécriture :

$$
\begin{aligned}
aa &\to a\\
ab &\to b\\
ac &\to a\\
ad &\to b\\
ba &\to a\\
bb &\to b\\
bc &\to a\\
bd &\to b\\
ca &\to c\\
cb &\to d\\
cc &\to c\\
cd &\to d\\
da &\to c\\
db &\to d\\
dc &\to c\\
dd &\to d
\end{aligned}
$$

Les mots associés aux nombres pairs de 24 à 38 sont (lecture colonne par colonne des mots m_2 et m_1 utilisés plus haut :

6 :	a						
8 :	a						
10 :	a	a					
12 :	c	a					
14 :	a	c	a				
16 :	a	a	c				
18 :	c	a	a	d			
20 :	a	c	a	b			
22 :	a	a	c	b	a		
24 :	c	a	a	d	a		
26 :	a	c	a	b	c	a	
28 :	c	a	c	b	a	c	
30 :	c	c	a	d	a	a	d

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