Conjecture de Goldbach et disjonctions de mots cycliques

Denise Vella-Chemla

11/1/14

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 propose dans ce but une modélisation qui associe à chaque nombre pair une matrice booléenne dont les lignes sont des "mots cycliques".

Pour trouver les mots du nombre pair $n+2$ à partir de ceux du nombre pair n, on utilisera la complétion d'un mot par une lettre respectant la cyclicité du mot, à droite ou à gauche, et la troncature de la lettre finale d'un mot.

Il faudra alors caractériser l'existence d'un décomposant de Goldbach d'un nombre pair n par une condition que vérifieront ses mots.

Il faudra aussi fournir un certain "invariant" du processus de passage d'un pair au suivant, qui assurera que l'existence d'un décomposant de Goldbach pour n reste garantie pour $n+2$.

On essaiera enfin de caractériser les mots de nombres pairs particuliers :

- les doubles $2p$ de premiers p, qui vérifient trivialement la conjecture (puisque $2p = p + p$) ;
- les doubles $2.père$ de nombres pairs qui sont tels que $père - 1$ et $père + 1$ sont premiers tous les deux (les "pères de jumeaux").

2 Modélisation

A chaque nombre pair est associé une matrice dont les lignes ont leurs éléments qui sont les lettres de mots cycliques représentant la divisibilité d'entiers successifs.

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.

Appelons K le nombre de nombres premiers impairs compris entre 3 et $n/2$. Appelons *milieu* le plus grand impair inférieur ou égal à $n/2$.

On peut oublier dans un premier temps l'idée de matrice pour ne garder à l'esprit que le fait qu'à chaque nombre pair n est associé un ensemble de $2K$ mots, qu'on appellera ses mots gris et ses mots bleus.

Sont ainsi associés à n :

- K mots gris, correspondant aux caractères de divisibilité des nombres impairs compris entre 3 et *milieu* inclus, par les nombres premiers impairs compris entre 3 et $\sqrt{n}$;
- K mots bleus, correspondant aux caractères de divisibilité des nombres impairs compris entre $n-3$ et *milieu* inclus, par les nombres premiers impairs compris entre 3 et $\sqrt{n}$.

Tous les mots associés au nombre pair n sont de longueur $\left\lfloor \frac{n/2-1}{2} \right\rfloor$.

Les mots de $n+2$:

- ont le même nombre de lettres que les mots de n si n est un double d'impair ;
- ont une lettre de plus que les mots de n si n est un double de pair.

Fournissons l'exemple des nombres pairs 40 et 42. La notation $f(n,p,G)$ dénote les lettres du mot gris associé à n pour le nombre premier p. La notation $f(n,p,B)$ dénote les lettres du mot bleu associé à n pour le nombre premier p. On a noté en première et dernière lignes en cyan les nombres auxquels correspondent les booléens de divisibilité, pour se repérer un peu.

Mots de 40

	37	35	33	31	29	27	25	23	21
$f(40,5,B)$	0	1	0	0	0	0	1	0	0
$f(40,3,B)$	0	0	1	0	0	1	0	0	1
$f(40,5,G)$	0	1	0	0	0	0	1	0	0
$f(40,3,G)$	1	0	0	1	0	0	1	0	0
	3	5	7	9	11	13	15	17	19

Mots de 42

	39	37	35	33	31	29	27	25	23	21
$f(42,5,B)$	0	0	1	0	0	0	0	1	0	0
$f(42,3,B)$	1	0	0	1	0	0	1	0	0	1
$f(42,5,G)$	0	1	0	0	0	0	1	0	0	0
$f(42,3,G)$	1	0	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21

On reconnaît les séquences périodiques selon lesquelles les nombres sont barrés par l'algorithme d'Erathosthène.

3 Réécriture

Pour connaître les mots d'un nombre existent deux possibilités :

- trouver ses mots bleus à partir de ses mots gris (c'est la vision locale du processus) ;
- trouver ses mots bleus (resp. ses mots gris) à partir des mots bleus (resp. des mots gris) du nombre pair précédent, c'est la vision dynamique du processus).

3.1 Vision globale

Un mot gris du pair $n+2$ est identique pour toutes ses lettres au mot gris du pair précédent n. Si $n = 4k$, on complète ce mot à droite par une lettre en respectant la condition de cyclicité.

Un mot bleu du pair $n+2$ s'obtient toujours par complétion à gauche du mot bleu du pair précédent n. Si $n+2 = 4k$, alors on tronque ce mot en lui ôtant sa dernière lettre pour que le mot obtenu soit de la bonne longueur.

3.2 Vision locale

La première lettre 1 du mot gris $f(n, p, G)$ étant à la position i dans le mot, le mot bleu aura un 1 à la position $i + (n/2 \ mod \ p)$ et les positions des autres 1 de ce mot s'en déduiront pour que soit respectées les conditions de cyclicité.

En annexe sont fournis les mots des nombres pairs de 24 à 50.

4 Invariant

Il faudrait exprimer par un invariant cette perception que l'on a eue en regardant les grilles de divisibilité de "formes" qui restent fixes (dans le cas des formes grises) ou sont translatées à droite (dans le cas des formes bleues) d'un nombre pair au suivant. Cette "invariance de forme" devrait assurer l'existence d'un "mot-colonne" à lettres toutes nulles dans chaque matrice de lettres (cela équivaut à la nullité de la disjonction booléenne des éléments de la colonne).

On n'arrive pas pour l'instant à trouver un tel invariant.

Il faudrait maîtriser la manière dont certaines colonnes de la matrice de n se trouvent comme "permutées" pour devenir d'autres colonnes de la matrice de $n+2$ et pour ça, connaître précisément la combinatoire des permutations de lettres dans les mots booléens.

5 Nombres premiers, nombres pères de jumeaux

Mots de 26 (double de 13 premier)

	23	21	19	17	15	13
$f(26,5,B)$	0	0	0	0	1	0
$f(26,3,B)$	0	1	0	0	1	0
$f(26,5,G)$	0	1	0	0	0	0
$f(26,3,G)$	1	0	0	1	0	0
	3	5	7	9	11	13

Mots de 34 (double de 17 premier)

	31	29	27	25	23	21	19	17
$f(34,5,B)$	0	0	0	1	0	0	0	0
$f(34,3,B)$	0	0	1	0	0	1	0	0
$f(34,5,G)$	0	1	0	0	0	0	1	0
$f(34,3,G)$	1	0	0	1	0	0	1	0
	3	5	7	9	11	13	15	17

On voit que les mots gris et bleus doivent bien sûr se terminer par 0 (puisqu'ils concernent la divisibilité du nombre premier p, qui est par définition non divisible par tous les nombres premiers de 3 à $\sqrt{p}$).

Oublions maintenant les nombres-mémoires cyan et regroupons les mots gris et bleu concernant la divisibilité par 3 et les mots gris et bleu concernant la divisibilité par 5.

$f(34,5,B)$	0	0	0	1	0	0	0	0
$f(34,5,G)$	0	1	0	0	0	0	1	0
$f(34,3,B)$	0	0	1	0	0	1	0	0
$f(34,3,G)$	1	0	0	1	0	0	1	0

Que constatons-nous, après avoir colorié certaines lettres des grilles ? Qu'il y a exactement 3 lettres 0 à l'extrémité droite des mots bleus et gris concernant la divisibilité par 3 et qu'il y a exactement 5 lettres 0 à l'extrémité droite des mots bleus et gris concernant la divisibilité par 5.

En utilisant la vision locale, et si on compte tous les zéros à l'extrémité droite de la grille, on peut regarder la grille du double d'un nombre premier $n = 2p$ comme un goban (un plateau de jeu de go) et voir les lettres 1 comme délimitant une zone de 0 à l'extrémité droite de la grille. Le nombre de zéros appartenant à la zone ainsi délimitée semble toujours égal à la somme de nombres premiers p_k inférieurs à $\sqrt{n}$, i.e. selon chaque p_k, il reste à droite des dernières letres 1 des lignes p_k lettres 0 en tout. Cela est attendu, le nombre de zéros en question comptant exactement le nombre de p_k nombres successifs non-divisibles par p_k, il vaut p_k pour tous les doubles d'impairs lorsque p_k ne divise pas n. Donc, si le nombre de zéros "entourés" par la ligne de 1 est égal à $\sum_{p_k \ premier \ impair \leqslant \sqrt{n}} p_k$, n est un double de premier tandis que si le nombre de zéros est inférieur strictement au nombre en question, n est le double d'un nombre composé impair.

Le comptage des zéros de la zone à l'extrémité droite du goban pour les doubles

de pairs a toujours pour valeur $\sum_{p_k\ premier\ impair \leqslant \sqrt{n}}(p_k - 1)$. Si de plus, la dernière colonne ne contient que des zéros, n est le double d'un père de jumeaux.

Revenons alors aux nombres de la forme $p^2 + 1$ qui sont ceux pour lesquels il faut ajouter deux mots à l'ensemble de mots par rapport à l'ensemble des mots de leur pair précédent et observons la "petite zone du goban" pour les deux lignes de la divisibilité par le nombre premier p. Sans surprise, on constate que la zone contient "exactement le nombre de zéros qu'il faut", c'est à dire p.

6 Petit détour

Il s'agit ici d'essayer de comprendre à quelle condition une permutation cyclique "garde un zéro" dans le mot résultant de la disjonction booléenne de 2 mots.

On fournit la table de la disjonction booléenne, pour des mots cycliques de longueur impaires (en l'occurrence des mots de longueur 3 ou 5) ne contenant qu'une seule lettre 1). On constate que tout mot obtenu par une telle opération de disjonction contient toujours une lettre 0 au moins.

$\vee$	100	010	001
100	100	110	101
010	110	010	011
001	101	011	001

Mots cycliques de longueur 3 *contenant une seule lettre* 1

$\vee$	10000	01000	00100	00010	00001
10000	10000	11000	10100	10010	10001
01000	11000	01000	01100	01010	01001
00100	10100	01100	00100	00110	00101
00010	10010	01010	00110	00010	00011
00001	10001	01001	00101	00011	00001

Mots cycliques de longueur 5 *contenant une seule lettre* 1

On n'est pas étonné de constater le caractère commutatif de la disjonction booléenne, en voyant que des cases symétriques par rapport à la première diagonale de la table.

On est un peu plus étonné de constater des symétries-miroir entre différentes cases, mais elles s'expliquent vite. Ainsi $10000 \vee 00010 = 10010$ tandis que $01000 \vee 00001 = 01001$, c'est à dire que si on appelle *miroir* la fonction qui associe à un mot booléen son symétrique selon une symétrie-miroir (la première lettre du premier est la dernière lettre du second, la deuxième lettre du premier est l'avant-dernière lettre du second, etc), on a $x \vee y = z$ et $miroir(x) \vee miroir(y) = miroir(z)$.

Annexe : mots des pairs de 24 à 50

24	$3B$	1	0	0	1	0				
	$3G$	1	0	0	1	0				
			×	×		×				
26	$5B$	0	0	0	0	1	0			
	$5G$	0	1	0	0	0	0			
	$3B$	0	1	0	0	1	0			
	$3G$	1	0	0	1	0	0			
				×			×			
28	$5B$	1	0	0	0	0	1			
	$5G$	0	1	0	0	0	0			
	$3B$	0	0	1	0	0	1			
	$3G$	1	0	0	1	0	0			
						×				
30	$5B$	0	1	0	0	0	0	1		
	$5G$	0	1	0	0	0	0	1		
	$3B$	1	0	0	1	0	0	1		
	$3G$	1	0	0	1	0	0	1		
				×		×	×			
32	$5B$	0	0	1	0	0	0	0		
	$5G$	0	1	0	0	0	0	1		
	$3B$	0	1	0	0	1	0	0		
	$3G$	1	0	0	1	0	0	1		
							×			
34	$5B$	0	0	0	1	0	0	0	0	
	$5G$	0	1	0	0	0	0	1	0	
	$3B$	0	0	1	0	0	1	0	0	
	$3G$	1	0	0	1	0	0	1	0	
						×			×	
36	$5B$	0	0	0	0	1	0	0	0	
	$5G$	0	1	0	0	0	0	1	0	
	$3B$	1	0	0	1	0	0	1	0	
	$3G$	1	0	0	1	0	0	1	0	
				×			×		×	
38	$5B$	1	0	0	0	0	1	0	0	0
	$5G$	0	1	0	0	0	0	1	0	0
	$3B$	0	1	0	0	1	0	0	1	0
	$3G$	1	0	0	1	0	0	1	0	0
				×						×
40	$5B$	0	1	0	0	0	0	1	0	0
	$5G$	0	1	0	0	0	0	1	0	0
	$3B$	0	0	1	0	0	1	0	0	1
	$3G$	1	0	0	1	0	0	1	0	0
						×			×	

42	$5B$	0	0	1	0	0	0	0	1	0	0		
	$5G$	0	1	0	0	0	0	1	0	0	0		
	$3B$	1	0	0	1	0	0	1	0	0	1		
	$3G$	1	0	0	1	0	0	1	0	0	1		
						×	×			×			
44	$5B$	0	0	0	1	0	0	0	0	1	0		
	$5G$	0	1	0	0	0	0	1	0	0	0		
	$3B$	0	1	0	0	1	0	0	1	0	0		
	$3G$	1	0	0	1	0	0	1	0	0	1		
				×			×						
46	$5B$	0	0	0	0	1	0	0	0	0	1	0	
	$5G$	0	1	0	0	0	0	1	0	0	0	0	
	$3B$	0	0	1	0	0	1	0	0	1	0	0	
	$3G$	1	0	0	1	0	0	1	0	0	1	0	
									×			×	
48	$5B$	1	0	0	0	0	1	0	0	0	0	1	
	$5G$	0	1	0	0	0	0	1	0	0	0	0	
	$3B$	1	0	0	1	0	0	1	0	0	1	0	
	$3G$	1	0	0	1	0	0	1	0	0	1	0	
				×		×			×	×			
50	$7B$	0	0	0	0	0	0	1	0	0	0	0	0
	$7G$	0	0	1	0	0	0	0	0	0	1	0	0
	$5B$	0	1	0	0	0	0	1	0	0	0	0	1
	$5G$	0	1	0	0	0	0	1	0	0	0	0	1
	$3B$	0	1	0	0	1	0	0	1	0	0	1	0
	$3G$	1	0	0	1	0	0	1	0	0	1	0	0
							×			×			