Conjecture de Goldbach et anagrammes de mots de restes

Denise Vella-Chemla

4/1/14

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 dont les éléments sont les lettres de "mots de restes".

Pour trouver les mots du nombre pair $n+2$ à partir de ceux du nombre pair n, on utilisera des règles de réécriture.

Il faudra alors caractériser l'existence d'un décomposant de Goldbach d'un nombre pair n par certaines conditions que vérifieront les mots de n.

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 $2.p\grave{e}re$ de nombres pairs qui sont tels que $p\grave{e}re - 1$ et $p\grave{e}re + 1$ sont premiers tous les deux (les "pères de jumeaux").

2 Modélisation

A chaque nombre pair est associé une matrice dont les éléments ligne par ligne sont les lettres de mots.

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

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.

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 restes des divisions euclidiennes 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 restes des divisions euclidiennes des nombres impairs compris entre *milieu* et $n-3$ inclus par les nombres premiers impairs compris entre 3 et $\sqrt{n}$.

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

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.

Pour faciliter la lecture, on pourra intercaler des parenthèses autour d'ensemble de lettres mais ces parenthèses ne doivent pas être considérées comme des lettres.

Fournissons l'exemple des nombres pairs 40 et 42. La notation $f(n,p,G)$ dénote les lettres du mot gris associé à n : les divisions euclidiennes ont pour diviseur p. La notation $f(n,p,B)$ dénote les lettres du mot bleu associé à n : les divisions euclidiennes ont pour diviseur p. On a noté en première et dernière lignes en cyan les nombres auxquels correspondent les restes, pour se repérer un peu.

Mots de 40

	37	35	33	31	29	27	25	23	21
$f(40,5,B)$	2	0	3	1	4	2	0	3	1
$f(40,3,B)$	1	2	0	1	2	0	1	2	0
$f(40,5,G)$	3	0	2	4	1	3	0	2	4
$f(40,3,G)$	0	2	1	0	2	1	0	2	1
	3	5	7	9	11	13	15	17	19

Mots de 42

	39	37	35	33	31	29	27	25	23	21
$f(42,5,B)$	4	2	0	3	1	4	2	0	3	1
$f(42,3,B)$	0	1	2	0	1	2	0	1	2	0
$f(42,5,G)$	3	0	2	4	1	3	0	2	4	1
$f(42,3,G)$	0	2	1	0	2	1	0	2	1	0
	3	5	7	9	11	13	15	17	19	21

On reconnaît les séquences périodiques de restes modulaires chères à Gauss.

Comme il est trop fastidieux d'écrire des suites périodiques de lettres, on utilisera une notation indicée pour exprimer qu'un mot est une suite réitérée d'une même séquence de lettres et contenant un certain nombre de lettres.

Par exemple, $(120)_7$ sera le mot 1201201 qui s'obtient par répétition de la séquence des lettres 1, 2 et 0 et qui contient 7 lettres.

3 Réécriture, anagrammes

Pour passer d'un mot de n (par exemple, $f(n,p,G)$ (resp. $f(n,p,B)$) au mot de $n+2$ correspondant (i.e. $f(n+2,p,G)$ (resp. $f(n+2,p,B)$), on utilise deux règles de réécriture :

- permuter cycliquement les lettres d'un mot,
- concaténer une lettre à un mot.

Exprimons récursivement comment s'obtiennent les mots de $n+2$ à partir des mots de n.

En annexe sont fournis les mots des nombres pairs de 24 à 100.

4 Invariant

Il faut exprimer par un invariant cette perception que l'on a eue en regardant les grilles de divisibilité de "formes" qui restent fixes (en l'occurence les 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" sans lettre nulle dans chaque matrice de lettres.

5 Nombres premiers, nombres pères de jumeaux

Mots de 26 (double de 13 premier)

	23	21	19	17	15	13
$f(26,5,B)$	3	1	4	2	0	3
$f(26,3,B)$	2	0	1	2	0	1
$f(26,5,G)$	3	0	2	4	1	3
$f(26,3,G)$	0	2	1	0	2	1
	3	5	7	9	11	13

Mots de 34 (double de 17 premier)

	31	29	27	25	23	21	19	17
$f(34,5,B)$	1	4	2	0	3	1	4	2
$f(34,3,B)$	1	2	0	1	2	0	1	2
$f(34,5,G)$	3	0	2	4	1	3	0	2
$f(34,3,G)$	0	2	1	0	2	1	0	2
	3	5	7	9	11	13	15	17

On voit que les mots gris et bleus doivent bien sûr se terminer par la même lettre (puisqu'ils concernent les restes du même nombre p).

On constate également que le mot bleu s'obtient en effectuant une symétrie-miroir du mot gris, puis un certain nombre de shifts. Shift correspond à l'élévation à la puissance. Il faut trouver quelle est la condition sur les puissances qui a pour conséquence que les dernières lettres des mots sont identiques.

Annexe : mots des pairs de 24 à 100

On ne fournira les mots détaillés que pour les pairs jusqu'à 34.

Deux mots pour 24 (selon le seul module 3)

$$f(24,3,G) = (021)_5 = 02102$$
$$f(24,3,B) = (012)_5 = 01201$$

Quatre mots pour les pairs de 26 à 48 (selon les modules 3 et 5)

Précisons toutes les lettres des mots pour les pairs de 26 à 34 puis généralisons.

$$\begin{aligned}
f(26,3,G) &= (021)_6 &&= 021021\\
f(26,5,G) &= (30241)_6 &&= 302413\\
f(26,3,B) &= (201)_6 &&= 201201\\
f(26,5,B) &= (31420)_6 &&= 314203
\end{aligned}$$

$$\begin{aligned}
f(28,3,G) &= (021)_6 &&= 021021\\
f(28,5,G) &= (30241)_6 &&= 302413\\
f(28,3,B) &= (120)_6 &&= 12012\\
f(28,5,B) &= (03142)_6 &&= 031420
\end{aligned}$$

$$\begin{aligned}
f(30,3,G) &= (021)_7 &&= 0210210\\
f(30,5,G) &= (30241)_7 &&= 3024130\\
f(30,3,B) &= (012)_7 &&= 0120120\\
f(30,5,B) &= (20314)_7 &&= 2031420
\end{aligned}$$

$$\begin{aligned}
f(32,3,G) &= (021)_7 &&= 0210210\\
f(32,5,G) &= (30241)_7 &&= 3024130\\
f(32,3,B) &= (201)_7 &&= 2012012\\
f(32,5,B) &= (42031)_7 &&= 4203142
\end{aligned}$$

$$\begin{aligned}
f(34,3,G) &= (021)_8 &&= 02102102\\
f(34,5,G) &= (30241)_8 &&= 30241302\\
f(34,3,B) &= (120)_8 &&= 1201201\\
f(34,5,B) &= (14203)_8 &&= 14203142
\end{aligned}$$

Rappel : $NbCol = \left\lfloor \frac{n/2-1}{2} \right\rfloor$

$f(n, 3, G) = (021)_{NbCol}$

$f(n, 5, G) = (30241)_{NbCol}$

$f(n, 3, B) = (012)_{NbCol}$ pour n de la forme *6k*
$f(n, 3, B) = (201)_{NbCol}$ pour n de la forme *6k+2*
$f(n, 3, B) = (120)_{NbCol}$ pour n de la forme *6k+4*

$f(n, 5, B) = (20314)_{NbCol}$ pour n de la forme *10k*
$f(n, 5, B) = (42031)_{NbCol}$ pour n de la forme *10k+2*
$f(n, 5, B) = (14203)_{NbCol}$ pour n de la forme *10k+4*
$f(n, 5, B) = (31420)_{NbCol}$ pour n de la forme *10k+6*
$f(n, 5, B) = (03142)_{NbCol}$ pour n de la forme *10k+8*

Six mots pour les pairs de 50 à 100 (selon les modules 3, 5 et 7)

Les définitions sont reprises à l'identique par rapport aux précédentes pour les modules 3 et 5. Pour le module 7, on a :

$f(n, 7, G) = (5316420)_{NbCol}$
$f(n, 7, B) = (4205316)_{NbCol}$ pour n de la forme *14k*
$f(n, 7, B) = (6420531)_{NbCol}$ pour n de la forme *14k+2*
$f(n, 7, B) = (1642053)_{NbCol}$ pour n de la forme *14k+4*
$f(n, 7, B) = (3164205)_{NbCol}$ pour n de la forme *14k+6*
$f(n, 7, B) = (5316420)_{NbCol}$ pour n de la forme *14k+8*
$f(n, 7, B) = (0531642)_{NbCol}$ pour n de la forme *14k+10*
$f(n, 7, B) = (2053164)_{NbCol}$ pour n de la forme *14k+12*