Conjecture de Goldbach, mots booléens et loi de réciprocité quadratique

Denise Vella-Chemla

14/1/14

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 conjointement deux modélisations :

- l'une qui associe à chaque nombre pair n deux "mots booléens de primalité" m_1 et m_2 qui caractérisent la primalité des nombres impairs x (compris entre 3 et $n/2$) et $n-x$;
- l'autre qui associe à chaque nombre pair n deux "mots booléens de résiduosité quadratique" rq_1 et rq_2 qui caractérisent la résiduosité quadratique des nombres x et $n-x$ à n.

Le nombre pair n a un décomposant de Goldbach si ses mots m_1 et m_2 ont tous les deux une lettre 0 à une position commune.

2 Mots booléens de primalité

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

Deux mots booléens de primalité m_1 et m_2 sont associés à n :

- m_1 correspond aux caractères de primalité (le booléen 0 signifie qu'un nombre est premier et supérieur à $\sqrt{n}$, le booléen 1 signifie qu'il est composé ou premier inférieur à $\sqrt{n}$) des nombres impairs compris entre 3 et *milieu* inclus ;
- m_2 correspond aux 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.

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.

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).

Exemples :
Mots m_1 et m_2 de 40

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

Mots m_1 et m_2 de 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	1	1	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21

Mots m_1 et m_2 de 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	1	1	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21

3 Mots booléens de résiduosité quadratique

Deux mots booléens de résiduosité quadratique rq_1 et rq_2 sont associés à n :

- rq_1 correspond aux caractères de résiduosité quadratique à n (le booléen 1 signifie qu'un nombre est résidu quadratique de n, le booléen 0 signifie qu'il ne l'est pas) des nombres impairs compris entre 3 et *milieu* inclus ;
- rq_2 correspond aux caractères de résiduosité quadratique à n des nombres impairs compris entre $n-3$ et *milieu* inclus.

Exemples :
Mots rq_1 et rq_2 de 40 *(*9 *et* 25 *en sont résidus quadratiques)*

	37	35	33	31	29	27	25	23	21
rq_2	0	0	0	0	0	0	1	0	0
rq_1	0	0	0	1	0	0	0	0	0
	3	5	7	9	11	13	15	17	19

Mots rq_1 et rq_2 de 42 *($7, 9, 15, 21, 25, 37$ et* 39 *en sont résidus quadratiques)*

	39	37	35	33	31	29	27	25	23	21
rq_2	1	1	0	0	0	0	0	1	0	1
rq_1	0	0	1	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21

Mots rq_1 et rq_2 de 44 ($5, 9, 25, 33$ et 37 en sont résidus quadratiques)

	41	39	37	35	33	31	29	27	25	23
rq_2	0	0	1	0	1	0	0	0	1	0
rq_1	0	1	0	1	0	0	0	0	0	0
	3	5	7	9	11	13	15	17	19	21

4 Constats

Rappelons d'abord le contenu de la loi de réciprocité quadratique d'une façon imagée, qui frappe notre aire visuelle. Elle a été démontrée de multiples façons par Gauss (il l'appelait le théorème d'or pour évoquer sa richesse).

Pour les nombres premiers p, il y a exactement $\frac{p-1}{2}$ nombres inférieurs à p qui sont résidus quadratiques de p.

On les note dans les tableaux par un petit trait au-dessus. Ils "sont en face" (leur somme vaut p) lorsque p est de la forme $4k+1$ (dans l'exemple du nombre premier 13 ci-dessous) ou "ne sont pas en face" (auquel cas, il y a un résidu quadratique par colonne) lorsque p est de la forme $4k+3$ (nombre premier 19 ci-dessous).

Résidus quadratiques de 13 de la forme $4k+1$

$\overline{12}$	11	$\overline{10}$	$\overline{9}$	8	7
$\overline{1}$	2	$\overline{3}$	$\overline{4}$	5	6

Résidus quadratiques de 19 de la forme $4k+3$

18	$\overline{17}$	$\overline{16}$	15	14	13	12	$\overline{11}$	10
$\overline{1}$	2	3	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	8	$\overline{9}$

La loi de réciprocité quadratique peut s'exprimer de la façon suivante : soient p et q deux entiers premiers impairs :

- si l'un au moins est de la forme $4k+1$, alors p est résidu quadratique de q si et seulement si q l'est de p ;
- si p et q sont tous deux de la forme $4k+3$ alors p est résidu quadratique de q si et seulement si q n'est pas résidu quadratique de p [2]

Les nombres pairs $2p$ doubles de nombres premiers p de la forme $4k+1$ ont $\frac{p-1}{2}$ résidus quadratiques (26 en a 6) tandis que les doubles de $4k+3$ en ont $\frac{p+1}{2}$ (38 en a 10). Ils sont face à face pour les doubles de premiers de la forme $4k+1$ et il y en a un par colonne pour les doubles de premiers de la forme $4k+3$ (sauf dans la dernière colonne qui fournit le caractère de résiduosité quadratique à $2p$

2. article 151 page 116 des Recherches arithmétiques : "il s'ensuit que la relation de p à q est la même que celle de q à p quand p ou q est de la forme $4k+1$, et qu'elle est inverse quand p et q sont de la forme $4k+3$.

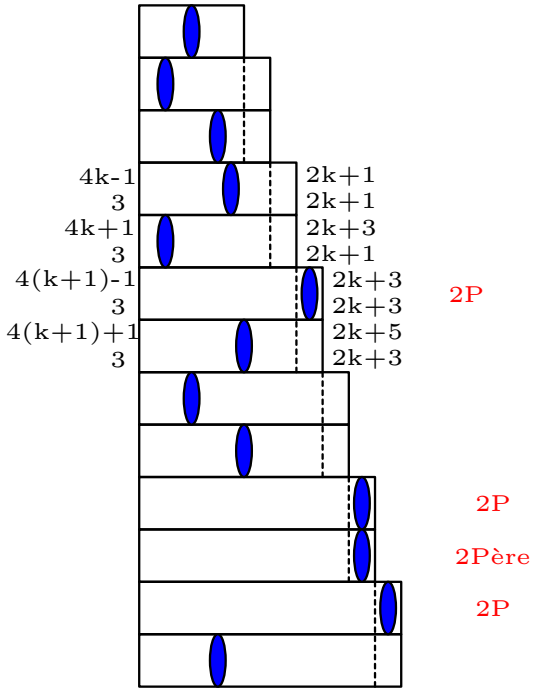
de p, et dans rq_1, et dans rq_2).

Les nombres pairs de la forme p^2+1 ont leurs résidus quadratiques ou non-résidus quadratiques complémentaires à n "face à face", ce quelle que soit leur forme.

Un nombre premier p est résidu quadratique de son double (il se trouve être congru à son propre carré) car $p^2 = \left(\frac{p-1}{2}\right)(2p) + p$.

5 Objectif

Peut-être qu'en mélangeant intelligemment le contenu de ces deux sortes de tableaux, de ces deux types de connaissances que sont, d'une part, le fait que dans le premier cas, on passe des mots m_1 et m_2 d'un nombre pair aux mots m_1 et m_2 du nombre pair suivant uniquement en concaténant à m_1 une lettre à droite et en concaténant à m_2 une lettre à gauche voire en lui en retirant une à droite un coup sur deux, cumulé à d'autre part, tout ce qui est connu des mathématiciens en terme de conséquences de la loi de réciprocité quadratique, pourrait-on parvenir à obtenir une démonstration du fait que les mots m_1 et m_2 ont toujours une lettre 0 à une position commune, ce qui démontrerait la conjecture de Goldbach.
Fournissons ci-dessous une représentation graphique du processus. Les ellipses bleues représentent une décomposition de Goldbach qui irait se déplaçant de pair en pair. Lorsque l'ellipse est en dernière colonne, n est un double de nombre premier. Lorsque 3 dernières colonnes vides se succèdent pour 3 pairs consécutifs, les nombres en question sont deux doubles de nombres premiers encadrant un double de "père de jumeaux".



Annexe 1 : résidus quadratiques des nombres pairs de 24 à 50

24 : 1 9

26 : 1 3 9 13 17 23 25

28 : 1 9 21 25

30 : 1 9 15 19 21 25

32 : 1 9 17 25

34 : 1 9 13 15 17 19 21 25 33

36 : 1 9 13 25

38 : 1 5 7 9 11 17 19 23 25 35

40 : 1 9 25

42 : 1 7 9 15 21 25 37 39

44 : 1 5 9 25 33 37

46 : 1 3 9 13 23 25 27 29 31 35 39 41

48 : 1 9 25 33

50 : 1 9 11 19 21 25 29 31 39 41 49

Annexe 2 : Mots m_1, m_2, rq_1, rq_2 pour les nombres pairs de 24 à 50

24	m_2	1	0	0	1	0			
	m_1	1	0	0	1	0			
	rq_2	0	0	0	0	0			
	rq_1	0	0	0	1	0			
26	m_2	0	1	0	0	1	0		
	m_1	1	1	0	1	0	0		
	rq_2	1	0	0	1	0	1		
	rq_1	1	0	0	1	0	1		
28	m_2	1	0	1	0	0	1		
	m_1	1	1	0	1	0	0		
	rq_2	1	0	1	0	0	0		
	rq_1	0	0	0	1	0	0		
30	m_2	1	1	0	1	0	0	1	
	m_1	1	1	0	1	0	0	1	
	rq_2	0	1	0	1	1	0	1	
	rq_1	0	0	0	1	0	0	1	
32	m_2	0	1	1	0	1	0	0	
	m_1	1	1	0	1	0	0	1	
	rq_2	0	0	1	0	0	0	1	
	rq_1	0	0	0	1	0	0	0	
34	m_2	0	0	1	1	0	1	0	0
	m_1	1	1	0	1	0	0	1	0
	rq_2	0	0	0	1	0	1	1	1
	rq_1	0	0	0	1	0	1	1	1
36	m_2	1	0	0	1	1	0	1	0
	m_1	1	1	0	1	0	0	1	0
	rq_2	0	0	0	0	1	0	0	0
	rq_1	0	0	0	1	0	1	0	0
38	m_2	1	1	0	0	1	1	0	1	0
	m_1	1	1	0	1	0	0	1	0	0
	rq_2	1	0	0	0	0	1	1	0	1
	rq_1	0	1	1	1	1	0	0	1	1
40	m_2	0	1	1	0	0	1	1	0	1
	m_1	1	1	0	1	0	0	1	0	0
	rq_2	0	0	0	0	0	0	1	0	0
	rq_1	0	0	0	1	0	0	0	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	
	rq_2	1	1	0	0	0	0	0	1	0	1	
	rq_1	0	0	1	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	
	rq_2	0	0	1	0	1	0	0	0	1	0	
	rq_1	0	1	0	1	0	0	0	0	0	0	
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
	rq_2	0	1	1	0	1	0	1	1	1	1	1
	rq_1	1	0	0	1	0	1	0	0	0	0	1
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
	rq_2	0	0	0	0	0	0	1	0	0	0	1
	rq_1	0	0	0	1	0	0	0	0	0	0	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
	rq_2	0	0	0	1	1	0	0	0	1	1	0	1
	rq_1	0	0	0	1	1	0	0	0	1	1	0	1