# Conjecture de Goldbach : un monoïde, deux booléens, quatre lettres, seize règles, un invariant et des changements de parité

Denise Vella-Chemla

16/3/14

## 1 Transposition

On considère un alphabet fini de 4 lettres $A = \{a, b, c, d\}$.
On appelle mot une suite finie d'éléments de $A$.
L'ensemble des mots sur $A$ est muni par la concaténation d'une structure de monoïde.
Ainsi défini, cet ensemble, noté $A^*$, est le monoïde libre.
On appelle longueur d'un mot le nombre de lettres qui le composent. les lettres d'un mot $m$ sont notées $m_1, m_2, \ldots, m_l$ dans leur ordre d'occurrence dans le mot si $l$ est la longueur de $m$. La lettre $a$ code la matrice $\binom{0}{0}$, et respectivement $b$ $\binom{0}{1}$, $c$ $\binom{1}{0}$ et enfin $d$ $\binom{1}{1}$ *.

Dans la suite, on utilise l'opération définie sur les matrices :

$$\binom{x_1}{x_2}.\binom{y_1}{y_2} = \binom{x_1}{y_2}$$

L'opération de multiplication des matrices fournit 16 règles de réécriture de couples de lettres (règles dénotées par la lettre $r$ ci-après), qui semblent pertinentes pour l'étude de la conjecture de Goldbach :

| | | | |
|---|---|---|---|
| 1) $aa \to a$ | 5) $ba \to a$ | 9) $ca \to c$ | 13) $da \to c$ |
| 2) $ab \to b$ | 6) $bb \to b$ | 10) $cb \to d$ | 14) $db \to d$ |
| 3) $ac \to a$ | 7) $bc \to a$ | 11) $cc \to c$ | 15) $dc \to c$ |
| 4) $ad \to b$ | 8) $bd \to b$ | 12) $cd \to d$ | 16) $dd \to d$ |

∗. Pour disposer d'un moyen de distinguer les 4 lettres à toutes fins utiles, on considère l'application $f$ qui à la matrice $M = \binom{x}{y}$ associe l'entier $f(M) = x - \frac{1}{2}y$.
Cette application $f$ envoie $\binom{0}{0}$ sur $0$, $\binom{0}{1}$ sur $1$, $\binom{1}{0}$ sur $-\frac{1}{2}$ et $\binom{1}{1}$ sur $\frac{1}{2}$.
On peut également considérer la fonction $g$ telle que $g(M) = 2y - x$ qui associe aux matrices une classe d'équivalence de $\mathbb{Z}/4\mathbb{Z}$ en envoyant $\binom{0}{0}$ sur $0$, $\binom{0}{1}$ sur $2$, $\binom{1}{0}$ sur $-1 = 3$ et $\binom{1}{1}$ sur $1$.

Si le mot associé au nombre pair $n$ est noté $m_n = m_1 m_2 \dots m_l$, le mot associé au nombre pair $n+2$ est $m_{n+2} = m'_1 m'_2 \dots m'_{l'}$ avec $l' = l$ si $n$ est un double d'impair et $l' = l+1$ sinon ; dans le cas où $n$ est un double d'impair, les règles de concaténation d'une lettre en fin de mot de la forme $m'_{l'} = r'(m_l)$ pour les nombres $n$ doubles de pairs sont $r'(a) = r'(b) = a$ et $r'(c) = r'(d) = d$.

D'autre part, l'application des règles de réécriture s'écrit :

$$\forall i \in \mathbb{N}, 2 \leqslant i \leqslant l, m'_i = r(m_{i-1} m_i).$$

Enfin, la "règle de la première lettre" (qui est la seule règle indéterministe à appliquer) est : $m'_1 = a$ si $n-1$ est un nombre premier et $m'_1 = c$ sinon.

On rappelle qu'on cherche un invariant qui garantirait qu'*"on ne perd jamais la lettre a"* au fur et à mesure du déroulement de l'algorithme.

On analyse localement les règles de réécriture :
- les règles 1, 2, 4 font "perdre un $a$" (la règle 4 fait en outre perdre un $d$) tandis que la règle 3 fait perdre un $c$ ;
- les règles 5, 6, 7 font "perdre un $b$" (la règle 7 fait en outre perdre un $c$) tandis que la règle 8 fait perdre un $d$ ;
- les règles 10, 11, 12 font "perdre un $c$" (la règle 10 fait en outre perdre un $b$) tandis que la règle 9 fait perdre un $a$ ;
- enfin, les règles 13, 15, 16 font "perdre un $d$" (la règle 13 fait en outre perdre un $a$) tandis que la règle 14 fait perdre un $b$ ;
- d'autre part, la règle 4 fait gagner un $b$, la règle 7 fait gagner un $a$, la règle 10 fait gagner un $d$ et la règle 13 fait gagner un $c$.

De façon un peu plus générale, les règles 1, 2, 3, 4, 9, 10, 11, 12 laissent la somme $N_b + N_d$ constante tandis que les règles 5, 6, 7, 8, 13, 14, 15 et 16 laissent la somme $N_a + N_c$ constante (si on note $N_\alpha$ le nombre de lettres $\alpha$ du mot sur lequel sont appliquées simultanément toutes les règles de réécriture possibles).

Si on considère une sorte de "permutation de lettres à la Galois", on constate qu'à un renommage de $a$ en $d$ et inversement près, ainsi qu'à un renommage de $b$ en $c$ et inversement près, il y a une parfaite symétrie entre les règles 1 et 16, 2 et 15, 3 et 14, 4 et 13, etc. i.e. entre les règles $i$ et $17-i$.

On trouve un invariant de la façon suivante : il faut considérer les mots associés aux nombres pairs privés de leur première lettre [†] présentant le fait que les mots utilisés ici "codent" les décompositions d'un nombre pair en somme de deux impairs dont le plus petit sommant est compris entre 3 et $n/2$ inclus). Il s'agit alors de coder le nombre de lettres $a, b, c$ et $d$ par des nombres notés $N_a, N_b, N_c$ et $N_d$. Puis on calcule les nombres $N_a + N_d$ d'une part et $N_b + N_c$ d'autre part et on étudie le changement de parité des sommes en question lors du passage d'un nombre pair au nombre pair suivant. A cause de la manière dont les règles de réécriture affectent l'une ou l'autre de ces sommes, lors du passage d'un double de pair à un double d'impair, seule l'une des deux parités change, tandis que lors du passage d'un double d'impair à un double de pair, soit les parités des

†. cf une note précédente à l'adresse http ://denise.vella.chemla.free.fr/ecrreecc.pdf.

deux sommes en question changent, soit aucune d'entre elles. En annexe 2, sont fournis les nombres de lettres, les valeurs des sommes $N_a + N_d$ et $N_b + N_c$, on a noté les changements de parité en utilisant la couleur rouge.

Le problème est qu'on ne sait pas combien de règles de chacune des deux sortes sont applicables sur un mot donné, qui permettrait de déduire que tout mot contient forcément une lettre $a$ (les lettres $a$ correspondent aux décompositions de Goldbach).

On constate cependant que la fonction $N_a + N_c$ est une fonction en espalier qui augmente simplement de 1 à chaque fois que $n$ est le double d'un nombre premier.

## 2 Un espace double

On se place avec cette modélisation dans une sorte d'*espace double* qui rappelle les tirettes que présentait Laisant dans la note *"Sur un procédé de vérification expérimentale du théorème de Goldbach"* du Bulletin de la SMF [‡].

La droite des entiers est doublée et "mise en face" d'elle-même à une certaine position translatée de $n/2$ de manière à ce que $x$ se trouve associé à $n - x$.

## 3 Des causes différentes produisent les mêmes effets

On pourrait s'interroger sur l'intérêt de présenter une n-ième modélisation du problème binaire de Goldbach.

La modélisation proposée ici peut être intéressante car elle ne considère plus les nombres selon leurs propriétés, comme la divisibilité par exemple, ou bien encore les distances qui les séparent, mais selon leur position relative les uns par rapport aux autres dans un certain repère variant selon le nombre pair dont on cherche une décomposition de Goldbach [§].

Ainsi, dans l'annexe 1, les deux sous-mots bleus *acd* que l'on trouve dans les mots des nombres pairs 34 et 70 correspondent aux décompositions $5+29, 7+27, 9+25$ pour 34 et $17 + 53, 19 + 51, 21 + 49$ pour 70 et n'ont en quelque sorte "rien à voir". Mais par réécriture, ces décompositions se "comporteront" de la même façon au fur et à mesure du déroulement de l'algorithme.

De la même façon, si on utilise une modélisation par points dont les coordonnées sont des restes modulaires dans les corps finis $\mathbb{Z}/p\mathbb{Z}$, on avait trouvé un bel

‡. cf Charles-Ange Laisant, *"Sur un procédé de vérification expérimentale du théorème de Goldbach"*, Bulletin de la Société Mathématique de France, n° 25, p. 108, 1/12/1897.

§. En cela, c'est une approche topologique au sens décrit par la professeur Eva Bayer-Fluckiger dans la conférence à l'adresse $http://www.canal-u.tv/video/universite_de_tous_les_savoirs/theorie_des_noeuds.1023$ au sujet de la théorie des noeuds.

exemple dans le Davis et Hersh de nombres partageant des décomposants de Goldbach en partageant peu de coordonnées modulaires : ils se "comportaient" eux-aussi de la même façon avec chacun des décomposants de Goldbach partagé (ils n'avaient aucune coordonnée commune avec lui) en n'ayant "rien à voir" l'un avec l'autre (selon un ensemble de relations qu'on pourrait résumer par $a \neq c$ et $b \neq c$ et cependant $a \neq b$).

On peut noter l'analogie suivante entre la conjecture de Goldbach et la conjecture des nombres premiers jumeaux si l'on utilise la modélisation par points de coordonnées les restes : un décomposant de Goldbach $p$ d'un nombre pair $n$ ne partage aucune de ses coordonnées ni avec le point origine (de coordonnées toutes nulles) puisqu'il est premier, ni avec $n$ (puisque son complémentaire est premier). Un décomposant de Goldbach de $n$ dépend de $n$, ce qui semble normal. Un "père de jumeau" (i.e. le double d'un nombre pair, "coincé" entre deux nombres premiers) de façon similaire n'a aucune coordonnée égale à 1 ou bien à $p-1$ dans le corps $\mathbb{Z}/p\mathbb{Z}$. On pourrait dire en quelque sorte que la conjecture de Goldbach est un problème relatif quand la conjecture des nombres premiers jumeaux est un problème absolu mais il s'agit dans les deux cas d'éliminer deux coordonnées (voire une lorsqu'elles sont confondues) dans chaque corps premier $\mathbb{Z}/p\mathbb{Z}$.

## Annexe 1 : mots du langage à 4 lettres associés aux nombres pairs de 6 à 100

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 : $c\ c\ a\ d\ a\ a\ d$
32 : $a\ c\ c\ b\ c\ a\ b$
34 : $a\ a\ c\ d\ a\ c\ b\ a$
36 : $c\ a\ a\ d\ c\ a\ d\ a$
38 : $c\ c\ a\ b\ c\ c\ b\ c\ a$
40 : $a\ c\ c\ b\ a\ c\ d\ a\ c$
42 : $c\ a\ c\ d\ a\ a\ d\ c\ a\ d$
44 : $a\ c\ a\ d\ c\ a\ b\ c\ c\ b$
46 : $a\ a\ c\ b\ c\ c\ b\ a\ c\ d\ a$
48 : $c\ a\ a\ d\ a\ c\ d\ a\ a\ d\ c$
50 : $a\ c\ a\ b\ c\ a\ d\ c\ a\ b\ c\ d$
52 : $c\ a\ c\ b\ a\ c\ b\ c\ c\ b\ a\ d$
54 : $c\ c\ a\ d\ a\ a\ d\ a\ c\ d\ a\ b\ d$
56 : $a\ c\ c\ b\ c\ a\ b\ c\ a\ d\ c\ b\ b$
58 : $c\ a\ c\ d\ a\ c\ b\ a\ c\ b\ c\ d\ b\ a$
60 : $c\ c\ a\ d\ c\ a\ d\ a\ a\ d\ a\ d\ d\ a$
62 : $a\ c\ c\ b\ c\ c\ b\ c\ a\ b\ c\ b\ d\ c\ a$
64 : $a\ a\ c\ d\ a\ c\ d\ a\ c\ b\ a\ d\ b\ c\ c$
66 : $c\ a\ a\ d\ c\ a\ d\ c\ a\ d\ a\ b\ d\ a\ c\ d$
68 : $c\ c\ a\ b\ c\ c\ b\ c\ c\ b\ c\ b\ b\ c\ a\ d$
70 : $a\ c\ c\ b\ a\ c\ d\ a\ c\ d\ a\ d\ b\ a\ c\ b\ d$
72 : $c\ a\ c\ d\ a\ a\ d\ c\ a\ d\ c\ b\ d\ a\ a\ d\ b$
74 : $a\ c\ a\ d\ c\ a\ b\ c\ c\ b\ c\ d\ b\ c\ a\ b\ d\ a$
76 : $a\ a\ c\ b\ c\ c\ b\ a\ c\ d\ a\ d\ d\ a\ c\ b\ b\ c$
78 : $c\ a\ a\ d\ a\ c\ d\ a\ a\ d\ c\ b\ d\ c\ a\ d\ b\ a\ d$
80 : $c\ c\ a\ b\ c\ a\ d\ c\ a\ b\ c\ d\ b\ c\ c\ b\ d\ a\ b$
82 : $a\ c\ c\ b\ a\ c\ b\ c\ c\ b\ a\ d\ d\ a\ c\ d\ b\ c\ b\ a$
84 : $c\ a\ c\ d\ a\ a\ d\ a\ c\ d\ a\ b\ d\ c\ a\ d\ d\ a\ d\ a$
86 : $a\ c\ a\ d\ c\ a\ b\ c\ a\ d\ c\ b\ b\ c\ c\ b\ d\ c\ b\ c\ a$
88 : $c\ a\ c\ b\ c\ c\ b\ a\ c\ b\ c\ d\ b\ a\ c\ d\ b\ c\ d\ a\ c$
90 : $c\ c\ a\ d\ a\ c\ d\ a\ a\ d\ a\ d\ d\ a\ a\ d\ d\ a\ d\ c\ a\ d$
92 : $a\ c\ c\ b\ c\ a\ d\ c\ a\ b\ c\ b\ d\ c\ a\ b\ d\ c\ b\ c\ c\ b$
94 : $c\ a\ c\ d\ a\ c\ b\ c\ c\ b\ a\ d\ b\ c\ c\ b\ b\ c\ d\ a\ c\ d\ a$
96 : $c\ c\ a\ d\ c\ a\ d\ a\ c\ d\ a\ b\ d\ a\ c\ d\ b\ a\ d\ c\ a\ d\ c$
98 : $c\ c\ c\ b\ c\ c\ b\ c\ a\ d\ c\ b\ b\ c\ a\ d\ d\ a\ b\ c\ c\ b\ c\ d$
100 : $a\ c\ c\ d\ a\ c\ d\ a\ c\ b\ c\ d\ b\ a\ c\ b\ d\ c\ b\ a\ c\ d\ a\ d$

## Annexe 2 : Invariant de parités pour les nombres pairs compris entre 12 et 50

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 : | $a$ | $c$ | $a$ | | | | | | | | $1a0b1c0d$ | 11 |
| 16 : | $a$ | $a$ | $c$ | | | | | | | | $1a0b1c0d$ | 11 |
| 18 : | $c$ | $a$ | $a$ | $d$ | | | | | | | $2a0b0c1d$ | 30 |
| 20 : | $a$ | $c$ | $a$ | $b$ | | | | | | | $1a1b1c0d$ | 12 |
| 22 : | $a$ | $a$ | $c$ | $b$ | $a$ | | | | | | $2a1b1c0d$ | 22 |
| 24 : | $c$ | $a$ | $a$ | $d$ | $a$ | | | | | | $3a0b0c1d$ | 40 |
| 26 : | $a$ | $c$ | $a$ | $b$ | $c$ | $a$ | | | | | $2a1b2c0d$ | 23 |
| 28 : | $c$ | $a$ | $c$ | $b$ | $a$ | $c$ | | | | | $2a1b2c0d$ | 23 |
| 30 : | $c$ | $c$ | $a$ | $d$ | $a$ | $a$ | $d$ | | | | $3a0b1c2d$ | 51 |
| 32 : | $a$ | $c$ | $c$ | $b$ | $c$ | $a$ | $b$ | | | | $1a2b3c0d$ | 15 |
| 34 : | $a$ | $a$ | $c$ | $d$ | $a$ | $c$ | $b$ | $a$ | | | $3a1b2c1d$ | 43 |
| 36 : | $c$ | $a$ | $a$ | $d$ | $c$ | $a$ | $d$ | $a$ | | | $4a0b1c2d$ | 61 |
| 38 : | $c$ | $c$ | $a$ | $b$ | $c$ | $c$ | $b$ | $c$ | $a$ | | $2a2b4c0d$ | 26 |
| 40 : | $a$ | $c$ | $c$ | $b$ | $a$ | $c$ | $d$ | $a$ | $c$ | | $2a1b4c1d$ | 35 |
| 42 : | $c$ | $a$ | $c$ | $d$ | $a$ | $a$ | $d$ | $c$ | $a$ | $d$ | $4a0b2c3d$ | 72 |
| 44 : | $a$ | $c$ | $a$ | $d$ | $c$ | $a$ | $b$ | $c$ | $c$ | $b$ | $2a2b4c1d$ | 36 |
| 46 : | $a$ | $a$ | $c$ | $b$ | $c$ | $c$ | $b$ | $a$ | $c$ | $d$ | $3a2b4c1d$ | 46 |
| 48 : | $c$ | $a$ | $a$ | $d$ | $a$ | $c$ | $d$ | $a$ | $a$ | $d$ | $5a0b2c3d$ | 82 |