Annexe 1 : Rappel historique.

Conjecture de Goldbach, langage à 4 lettres, variables et invariants, avril 2014.

Conjecture de Goldbach, langage à 4 lettres, variables et invariants, mai 2014.

Conjecture de Goldbach et langage à 4 lettres, avril 2014.

Positionner les décompositions triviales de Goldbach sur la droite du plan complexe de partie réelle 1/2.

Conjecture de Goldbach, réécriture, contradiction, mars 2014.

Goldbach conjecture, 4 letters language, variables and invariants.

Goldbach's conjecture, 4 letters language, variables and invariants.

Goldbach conjecture, rewriting, contradiction.

slides.

extrait de la biographie Poincaré : philosophe et mathématicien d'Umberto Bottazzini.

Indiscernabilité, septembre 2014.

Ionesco : Mathématiques absurdes.

extraits de Mathématiques en liberté, de Pierre Cartier, Jean Dhombres, Gerhard Heinzmann et Cédric Villani.

Relations invariantes entre nombres de décompositions de Goldbach codées dans un langage à 4 lettres, octobre 2014.

Invariant relations between binary Goldbach's decompositions'numbers coded in a 4 letters language, octobre 2014.

flèche-vers-gnc : idées qui m'ont amenée aux miennes, avril 2014.

programme C++ calcul des variables.

Primalité et zéros de sommes de cosinus, juillet 2014 (somme de sommes de cos), For me, that's fun !.

résumé approche par les invariants sur variables de comptages de décompositions de telle ou telle forme.

Programme de la somme des diviseurs utilisant les sommes de cosinus, juin 2014.

champ de spin.

transparents.

transparents.

Annexe 1 : Rappel historique

Citons Charles-Ange Laisant dans la note intitulée *Sur un procédé expérimental de vérification de la conjecture de Goldbach* du Bulletin de la SMF *n*˚25 de 1897.

> *Ce fameux théorème empirique : Tout nombre pair est la somme de deux nombres premiers, dont la démonstration semble dépasser les possibilités scientifiques actuelles, a fait l'objet de nombreux travaux et de certaines contestations. Lionnet a tenté d'établir que la proposition devait probablement être inexacte. M. Georg Cantor l'a vérifiée numériquement jusqu'à 1000, en donnant pour chaque nombre pair toutes les décompositions en deux nombres premiers, et il a remarqué que le nombre de ces décompositions ne cesse de croître en moyenne, tout en présentant de grandes irrégularités.*
>
> *Voici un procédé qui permettrait de faire sans calcul la vérification expérimentale dont il s'agit, et d'avoir pour chaque nombre pair, à la seule inspection d'une figure, toutes les décompositions. Supposons que sur une bande formée de carrés accolés, représentant les nombres impairs successifs, on ait construit le crible d'Erathostène, en ombrant les nombres composés, jusqu'à une limite quelconque* $2n-1$.

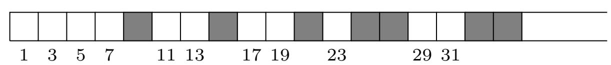


Figure 1

> *Si l'on a construit deux réglettes pareilles, et si l'on place la seconde au-dessous de la première en la retournant et en faisant correspondre la case* 1 *à* $2n^*$, *il est évident que si le théorème de Goldbach est vrai pour* $2n$, *il y aura quelque part deux cases blanches en correspondance ; et tous les couples de cases blanches donneront les diverses décompositions. On les aura même en lisant la moitié de la figure, à cause de la symétrie par rapport au milieu. Ainsi la vérification relative au nombre* 28 *donnera la figure 2 et montrera qu'on a les décompositions* $28 = 5+23 = 11+17$.

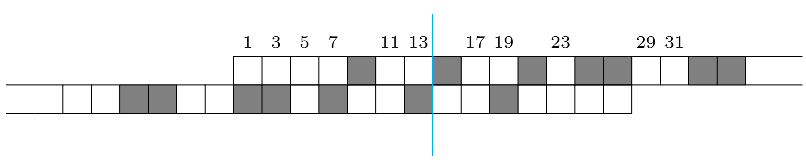


Figure 2

> *On comprend que les réglettes étant construites à l'avance, et un simple glissement permettant de passer d'un nombre à un autre, les vérifications sont très rapides.*

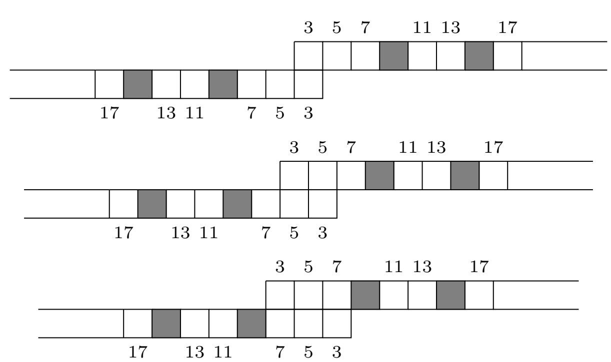


Figure 3

∗. Ici devrait être écrit $2n-1$.

Annexe 2 : Programme et son exécution des idées présentées

```
#include <iostream>
#include <stdio.h>
#include <cmath>

int prime(int atester)
{
  unsigned long diviseur=2;
  bool pastrouve=true;
  unsigned long k = 2;
  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve)
    {
    if ((k * k) > atester) return 1;
    else
      if ((atester % k) == 0) {
  return 0 ;
      }
  else k++;
    }
}

int main (int argc, char* argv[])
{
  int n, x, xa, xb, xc, xd, za, zc, ya, yc, debuthaut ;

  for (n=14 ; n <= 100 ; n=n+2)
    {
      xa=0 ; xb=0 ; xc=0 ; xd=0 ; ya=0 ; yc=0; za=0 ; zc=0 ;
      for (x = 3 ; x <= n/2 ; x=x+2)
  {
    if (prime(x)) { if (prime(n-x)) xa++ ; else xc++ ;}
    else { if (prime(n-x)) xb++ ; else xd++ ; }
  }
      for (x = 6 ; x <= (n+4)/2 ; x=x+2)
  {
    if (prime(x-3)) za++ ;
    else zc++ ;
  }
      if ((n/2) % 2 == 0) debuthaut = ((n+4)/2)+2 ; else debuthaut = ((n+4)/2)+1 ;
      for (x = debuthaut ; x <= n ; x=x+2)
  {
    if (prime(x-3)) ya++ ;
    else yc++ ;
  }
      std::cout << "\n" << n << " : \n" ;
      printf("ya = %2d yc = %2d",ya,yc) ;
      printf(" (n-2)/4 = %d\n",(n-2)/4) ;
      printf("za = %2d zc = %2d",za,zc) ;
      printf(" (n-4)/4 = %d\n",(n-4)/4) ;
      printf("xa = %2d xb = %2d xc = %2d xd = %2d\n",xa,xb,xc,xd) ;
    }
}
```

```
14  :
ya =  2 yc = 1 (n-2)/4 = 3
za =  2 zc = 0 (n-4)/4 = 2
xa =  2 xb = 0 xc = 1 xd = 0

16  :
ya =  2 yc = 1 (n-2)/4 = 3
za =  3 zc = 0 (n-4)/4 = 3
xa =  2 xb = 0 xc = 1 xd = 0

18  :
ya =  2 yc = 2 (n-2)/4 = 4
za =  3 zc = 0 (n-4)/4 = 3
xa =  2 xb = 0 xc = 1 xd = 1

20  :
ya =  3 yc = 1 (n-2)/4 = 4
za =  3 zc = 1 (n-4)/4 = 4
xa =  2 xb = 1 xc = 1 xd = 0

22  :
ya =  4 yc = 1 (n-2)/4 = 5
za =  3 zc = 1 (n-4)/4 = 4
xa =  3 xb = 1 xc = 1 xd = 0

24  :
ya =  3 yc = 2 (n-2)/4 = 5
za =  4 zc = 1 (n-4)/4 = 5
xa =  3 xb = 0 xc = 1 xd = 1

26  :
ya =  4 yc = 2 (n-2)/4 = 6
za =  4 zc = 1 (n-4)/4 = 5
xa =  3 xb = 1 xc = 2 xd = 0

28  :
ya =  3 yc = 3 (n-2)/4 = 6
za =  5 zc = 1 (n-4)/4 = 6
xa =  2 xb = 1 xc = 3 xd = 0

30  :
ya =  3 yc = 4 (n-2)/4 = 7
za =  5 zc = 1 (n-4)/4 = 6
xa =  3 xb = 0 xc = 2 xd = 2

32  :
ya =  4 yc = 3 (n-2)/4 = 7
za =  5 zc = 2 (n-4)/4 = 7
xa =  2 xb = 2 xc = 3 xd = 0

34  :
ya =  5 yc = 3 (n-2)/4 = 8
za =  5 zc = 2 (n-4)/4 = 7
xa =  4 xb = 1 xc = 2 xd = 1

36  :
ya =  4 yc = 4 (n-2)/4 = 8
za =  6 zc = 2 (n-4)/4 = 8
xa =  4 xb = 0 xc = 2 xd = 2

38  :
ya =  4 yc = 5 (n-2)/4 = 9
za =  6 zc = 2 (n-4)/4 = 8
xa =  2 xb = 2 xc = 5 xd = 0
```

```
40  :
ya = 4 yc = 5 (n-2)/4 = 9
za = 7 zc = 2 (n-4)/4 = 9
xa = 3 xb = 1 xc = 4 xd = 1

42  :
ya = 4 yc = 6 (n-2)/4 = 10
za = 7 zc = 2 (n-4)/4 = 9
xa = 4 xb = 0 xc = 3 xd = 3

44  :
ya = 5 yc = 5 (n-2)/4 = 10
za = 7 zc = 3 (n-4)/4 = 10
xa = 3 xb = 2 xc = 4 xd = 1

46  :
ya = 6 yc = 5 (n-2)/4 = 11
za = 7 zc = 3 (n-4)/4 = 10
xa = 4 xb = 2 xc = 4 xd = 1

48  :
ya = 5 yc = 6 (n-2)/4 = 11
za = 8 zc = 3 (n-4)/4 = 11
xa = 5 xb = 0 xc = 3 xd = 3

50  :
ya = 6 yc = 6 (n-2)/4 = 12
za = 8 zc = 3 (n-4)/4 = 11
xa = 4 xb = 2 xc = 4 xd = 2

52  :
ya = 6 yc = 6 (n-2)/4 = 12
za = 8 zc = 4 (n-4)/4 = 12
xa = 3 xb = 3 xc = 5 xd = 1

54  :
ya = 6 yc = 7 (n-2)/4 = 13
za = 8 zc = 4 (n-4)/4 = 12
xa = 5 xb = 1 xc = 3 xd = 4

56  :
ya = 7 yc = 6 (n-2)/4 = 13
za = 8 zc = 5 (n-4)/4 = 13
xa = 3 xb = 4 xc = 5 xd = 1

58  :
ya = 7 yc = 7 (n-2)/4 = 14
za = 8 zc = 5 (n-4)/4 = 13
xa = 4 xb = 3 xc = 5 xd = 2

60  :
ya = 6 yc = 8 (n-2)/4 = 14
za = 9 zc = 5 (n-4)/4 = 14
xa = 6 xb = 0 xc = 3 xd = 5

62  :
ya = 7 yc = 8 (n-2)/4 = 15
za = 9 zc = 5 (n-4)/4 = 14
xa = 3 xb = 4 xc = 7 xd = 1

64  :
ya = 7 yc = 8 (n-2)/4 = 15
za = 10 zc = 5 (n-4)/4 = 15
xa = 5 xb = 2 xc = 5 xd = 3
```

```
66  :
ya =  7 yc = 9 (n-2)/4 = 16
za = 10 zc = 5 (n-4)/4 = 15
xa =  6 xb = 1 xc = 4 xd = 5

68  :
ya =  7 yc = 9 (n-2)/4 = 16
za = 10 zc = 6 (n-4)/4 = 16
xa =  2 xb = 5 xc = 8 xd = 1

70  :
ya =  8 yc = 9 (n-2)/4 = 17
za = 10 zc = 6 (n-4)/4 = 16
xa =  5 xb = 3 xc = 5 xd = 4

72  :
ya =  8 yc = 9 (n-2)/4 = 17
za = 10 zc = 7 (n-4)/4 = 17
xa =  6 xb = 2 xc = 4 xd = 5

74  :
ya =  9 yc = 9 (n-2)/4 = 18
za = 10 zc = 7 (n-4)/4 = 17
xa =  5 xb = 4 xc = 6 xd = 3

76  :
ya =  9 yc = 9 (n-2)/4 = 18
za = 11 zc = 7 (n-4)/4 = 18
xa =  5 xb = 4 xc = 6 xd = 3

78  :
ya =  9 yc = 10 (n-2)/4 = 19
za = 11 zc = 7 (n-4)/4 = 18
xa =  7 xb = 2 xc = 4 xd = 6

80  :
ya =  9 yc = 10 (n-2)/4 = 19
za = 11 zc = 8 (n-4)/4 = 19
xa =  4 xb = 5 xc = 7 xd = 3

82  :
ya = 10 yc = 10 (n-2)/4 = 20
za = 11 zc = 8 (n-4)/4 = 19
xa =  5 xb = 5 xc = 7 xd = 3

84  :
ya =  9 yc = 11 (n-2)/4 = 20
za = 12 zc = 8 (n-4)/4 = 20
xa =  8 xb = 1 xc = 4 xd = 7

86  :
ya = 10 yc = 11 (n-2)/4 = 21
za = 12 zc = 8 (n-4)/4 = 20
xa =  5 xb = 5 xc = 8 xd = 3

88  :
ya =  9 yc = 12 (n-2)/4 = 21
za = 13 zc = 8 (n-4)/4 = 21
xa =  4 xb = 5 xc = 9 xd = 3

90  :
ya =  9 yc = 13 (n-2)/4 = 22
za = 13 zc = 8 (n-4)/4 = 21
xa =  9 xb = 0 xc = 4 xd = 9
```

```
92  :
ya = 10 yc = 12 (n-2)/4 = 22
za = 13 zc = 9 (n-4)/4 = 22
xa =  4 xb = 6 xc = 9 xd = 3

94  :
ya = 10 yc = 13 (n-2)/4 = 23
za = 13 zc = 9 (n-4)/4 = 22
xa =  5 xb = 5 xc = 9 xd = 4

96  :
ya =  9 yc = 14 (n-2)/4 = 23
za = 14 zc = 9 (n-4)/4 = 23
xa =  7 xb = 2 xc = 7 xd = 7

98  :
ya =  9 yc = 15 (n-2)/4 = 24
za = 14 zc = 9 (n-4)/4 = 23
xa =  3 xb = 6 xc = 11 xd = 4

100  :
ya = 10 yc = 14 (n-2)/4 = 24
za = 14 zc = 10 (n-4)/4 = 24
xa =  6 xb = 4 xc = 8 xd = 6
```

Conjecture de Goldbach, langage à 4 lettres, variables et invariants

Denise Vella-Chemla

21/04/2014

1 Introduction

La conjecture de Goldbach stipule que tout nombre pair sauf 2 est la somme de deux nombres premiers. Dans la suite, on s'intéresse aux décompositions d'un nombre pair n en somme de deux nombres impairs $p+q$ avec $3 \leqslant p \leqslant n/2$, $n/2 \leqslant q \leqslant n-3$ et $p \leqslant q$. On appelle p un *sommant de premier rang* et q un *sommant de second rang* de n.

Notations :

On désignera par :

- a : une décomposition de n de la forme $p+q$ avec p et q premiers ;
- b : une décomposition de n de la forme $p+q$ avec p composé et q premier ;
- c : une décomposition de n de la forme $p+q$ avec p premier et q composé ;
- d : une décomposition de n de la forme $p+q$ avec p et q composés.

Exemple :

40	3	5	7	9	11	13	15	17	19
	37	35	33	31	29	27	25	23	21
l_{40}	a	c	c	b	a	c	d	a	c

2 Le tableau principal

On désigne par $T = (L, C) = (\ l_{n,m}\ )$ le tableau dont les éléments $l_{n,m}$ sont l'une des lettres a, b, c, d. L'indice n appartient à l'ensemble L des nombres pairs supérieurs ou égaux à 6. L'indice m, appartenant à l'ensemble C des nombres impairs supérieurs ou égaux à 3, est un élément de la liste des sommants de n de premier rang.

Considérons la fonction g définie ainsi :

$$\begin{array}{rccl} g: & 2\mathbb{N} & \rightarrow & 2\mathbb{N}+1 \\ & x & \mapsto & 2\left\lfloor \dfrac{x-2}{4} \right\rfloor + 1 \end{array}$$

$g(6) = 3, g(8) = 3, g(10) = 5, g(12) = 5, g(14) = 7, g(16) = 7, etc.$

La fonction $g(n)$ définit le plus grand des sommants de second rang associés à n.

Comme l'on ne prend en compte que les décompositions de n de la forme $p+q$ où $p \leqslant q$, seules apparaîtront dans le tableau les lettres $l_{n,m}$ telles que $m \leqslant 2\left\lfloor \dfrac{n-2}{4} \right\rfloor + 1$ de sorte que le tableau contient les éléments suivants : $l_{6,3}, l_{8,3}, l_{10,3}, l_{10,5}, l_{12,3}, l_{12,5}, l_{14,3}, l_{14,5}, l_{14,7}, etc.$

Voici le début du tableau.

L \ C	3	5	7	9	11	13	15	17
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
...								

FIGURE 1 : mots des nombres pairs de 6 à 36

Remarques :

1) les mots situés sur les diagonales du tableau appelés *mots diagonaux* ont leurs lettres soit dans l'alphabet $A_{ab} = \{a, b\}$ soit dans l'alphabet $A_{cd} = \{c, d\}$.

2) un mot diagonal code des décompositions de même sommant de second rang.
Par exemple, sur la Figure 4, les lettres de la diagonale *aaabaa* qui commence à la lettre $l_{26,3} = a$ code les décompositions $3 + 23, 5 + 23, 7 + 23, 9 + 23, 11 + 23$ et $13 + 23$.

3) Désignons par l_n la ligne dont les éléments sont les $l_{n,m}$. La ligne l_n possède $\left\lfloor \dfrac{n-2}{4} \right\rfloor$ éléments.

4) n étant fixé, appelons $C_{n,3}$ la colonne formée des $l_{k,3}$ pour $6 \leqslant k \leqslant n$.

Dans cette colonne $C_{n,3}$, distinguons deux parties, la "partie haute" et la "partie basse" de la colonne.

Notons $H_{n,3}$ la "partie haute" de la colonne, i.e. l'ensemble des $l_{k,3}$ où $6 \leqslant k \leqslant \left\lfloor \dfrac{n+4}{2} \right\rfloor$.

Notons $B_{n,3}$ la "partie basse" de la colonne, i.e. l'ensemble des $l_{k,3}$ où $\left\lfloor \dfrac{n+4}{2} \right\rfloor < k \leqslant n$.

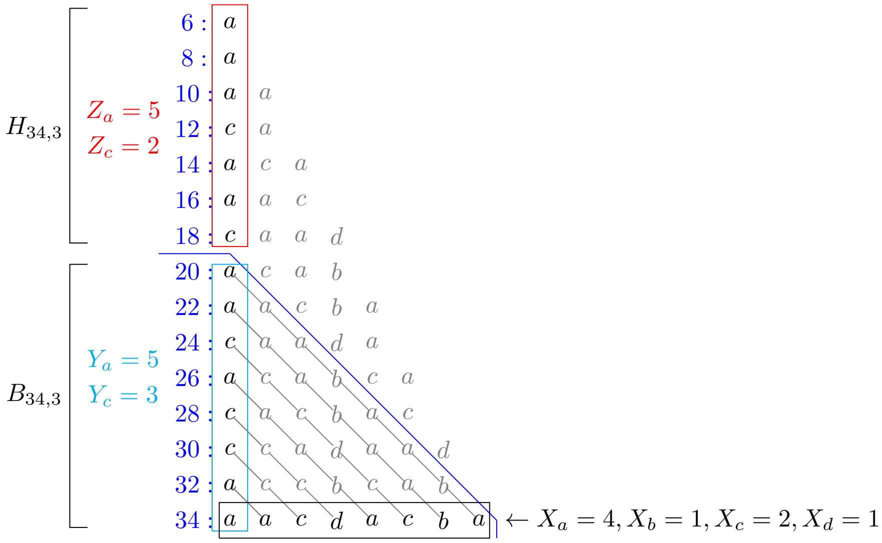


Figure 2 : $n = 34$

Pour mieux cerner les dénombrements de la section suivante, on utilisera la projection P de la ligne n sur la partie basse de la première colonne $B_{n,3}$ qui "associe" les lettres aux deux bouts d'une diagonale. Si on considère l'application $proj$ telle que $proj(a) = proj(b) = a$ et $proj(c) = proj(d) = c$ alors, puisque 3 est premier, $proj(l_{n,2k+1}) = l_{n-2k+2,3}$.

On peut comprendre l'effet de cette projection (qui préserve le sommant de second rang) en analysant les décompositions :

- si $p+q$ est codée par une lettre a ou une lettre b, cela correspond aux deux cas possibles dans lesquels q est premier, alors la décomposition $3+q$, contenant deux nombres premiers sera codée par la lettre a ;
- si $p+q$ est codée par une lettre c ou une lettre d, cela correspond aux deux cas possibles dans lesquels q est composé, alors la décomposition $3+q$, de la forme *premier* + *composé* sera codée par la lettre c.

On utilisera également dans la section suivante une projection qui transforme le sommant de premier rang en sommant de second rang que l'on combine à 3 comme sommant de premier rang ; analysons l'effet qu'une telle projection aura sur les décompositions :

- si $p+q$ est codée par une lettre a ou une lettre c, cela correspond aux deux cas possibles dans lesquels p est premier, alors la décomposition $3+p$, contenant deux nombres premiers sera codée par la lettre a ;
- si $p+q$ est codée par une lettre b ou une lettre d, cela correspond aux deux cas possibles dans lesquels p est composé, alors la décomposition $3+p$, de la forme *premier* + *composé* sera codée par la lettre c.

3 Dénombrements

1) On note dans la ligne n par :

- $X_a(n)$ le nombre de décompositions de n de la forme *premier* + *premier* ;
- $X_b(n)$ le nombre de décompositions de n de la forme *composé* + *premier* ;
- $X_c(n)$ le nombre de décompositions de n de la forme *premier* + *composé* ;
- $X_d(n)$ le nombre de décompositions de n de la forme *composé* + *composé*.

$X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor$ est le nombre d'éléments de la ligne de n.

Exemple : $n = 34$:
$X_a(34) = \#\{3+31, 5+29, 11+23, 17+17\} = 4$
$X_b(34) = \#\{15+19\} = 1.$
$X_c(34) = \#\{7+27, 13+21\} = 2$
$X_d(34) = \#\{9+25\} = 1$

2) Soit $Y_a(n)$ (resp. $Y_c(n)$) le nombre de a (resp. c) qui apparaissent dans $B_{n,3}$. On rappelle qu'il n'y a que des lettres a et c dans la première colonne car elle contient les lettres associées aux décompositions de la forme $3 + x$ et que 3 est premier.

Exemple :

- $Y_a(34) = \#\{3+17, 3+19, 3+23, 3+29, 3+31\} = 5$
- $Y_c(34) = \#\{3+21, 3+25, 3+27\} = 3$

3) Compte-tenu de la projection P qui est une bijection, des définitions des lettres a, b, c, d, $Y_a(n) = X_a(n) + X_b(n)$ et $Y_c(n) = X_c(n) + X_d(n)$. Par suite, trivialement, $Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor$.

Exemple :

$$\begin{array}{ll}
Y_a(34) & = \#\{3+17, 3+19, 3+23, 3+29, 3+31\} \\
X_a(34) & = \#\{3+31, 5+29, 11+23, 17+17\} \\
X_b(34) & = \#\{15+19\} \\
 & \\
Y_c(34) & = \#\{3+21, 3+25, 3+27\} \\
X_c(34) & = \#\{7+27, 13+21\} \\
X_d(34) & = \#\{9+25\}
\end{array}$$

4) Soit $Z_a(n)$ (resp. $Z_c(n)$) le nombre de a (resp. c) qui apparaissent dans $H_{n,3}$.

Exemple :

- $Z_a(34) = \#\{3+3, 3+5, 3+7, 3+11, 3+13\} = 5$
- $Z_c(34) = \#\{3+9, 3+15\} = 2$

$Z_a(n) + Z_c(n) = \left\lfloor \frac{n-4}{4} \right\rfloor$.

Rappel des propriétés identifiées

$$Y_a(n) = X_a(n) + X_b(n) \tag{1}$$

$$Y_c(n) = X_c(n) + X_d(n) \tag{2}$$

$$Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

$$Z_a(n) + Z_c(n) = \left\lfloor \frac{n-4}{4} \right\rfloor \tag{4}$$

Ajoutons deux nouvelles propriétés à celles-ci :

$$X_a(n) + X_c(n) = Z_a(n) + \delta_{2p} \tag{5}$$

avec δ_{2p} qui vaut 1 dans le cas où n est le double d'un nombre premier et qui vaut 0 sinon.

$$X_b(n) + X_d(n) = Z_c(n) + \delta_{spec} \tag{6}$$

avec δ_{spec} qui vaut 0 dans le cas où il existe k tel que $n = 4k$, ou bien dans le cas où n est le double d'un nombre premier, et qui vaut 1 sinon.

4 Evolution des variables

Dans cette section, étudions comment les différentes variables évoluent, de manière à en déduire que X_a (le nombre de décompositions d'un entier pair sous la forme d'une somme de deux nombres premiers) ne peut jamais être nul.

$Z_a(n) + Z_c(n) = \left\lfloor \dfrac{n-4}{4} \right\rfloor$ est une fonction croissante de n, elle augmente de 1 à chaque n double de pair.

$Z_a(n)$ augmente de 1 quand $\dfrac{n-2}{2}$ est un nombre premier et $Z_c(n)$ augmente de 1 quand $\dfrac{n-2}{2}$ est un nombre composé.

$Y_a(n)+Y_c(n) = X_a(n)+X_b(n)+X_c(n)+X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$ est une fonction croissante de n, elle augmente de 1 à chaque n double d'impair.

Voyons maintenant dans le détail comment évoluent $Y_a(n)$ et $Y_c(n)$.

Dans le cas où n est un double d'impair, on ajoute un nombre à l'intervalle $H_{n,3}$; si ce nombre $(n-3)$ est premier (resp. composé), $Y_a(n)$ (resp. $Y_c(n)$) est augmenté de 1 par rapport à $Y_a(n-2)$ (resp. $Y_c(n-2)$).

Dans le cas où n est un double de pair, 4 cas se présentent. Etudions la manière dont évolue l'ensemble de décompositions $H_{n,3}$.

- si $n-3$ et $n/2-1$ sont tous les deux premiers, on retire en bas et et on ajoute en haut de l'intervalle $H_{n,3}$ deux lettres de même sorte, alors $Y_a(n)$ et $Y_c(n)$ restent constants ;
- si $n-3$ est premier et $n/2-1$ est composé alors $Y_a(n)$ est augmenté de 1 et $Y_c(n)$ est diminué de 1 ;
- si $n-3$ est composé et $n/2-1$ est premier alors $Y_c(n)$ est augmenté de 1 et $Y_a(n)$ est diminué de 1 ;
- si $n-3$ et $n/2-1$ sont tous les deux composés, on retire en bas et et on ajoute en haut de l'intervalle $H_{n,3}$ deux lettres de même sorte, alors $Y_a(n)$ et $Y_c(n)$ restent constants.

Mais on n'arrive pas à déduire de l'intrication de toutes ces variables que $X_a(n)$ est toujours strictement positif. En annexe 1 sont fournies dans une table les valeurs des différentes variables pour n compris entre 14 et 100.

5 Essayer d'aboutir à une contradiction

Essayons cependant d'aboutir à une contradiction en partant de l'hypothèse que $X_a(n)$ est nul.

Si $X_a(n) = 0$, on a

$$X_b(n) + X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

Cela équivaut à

$$X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor - X_b(n)$$

et donc à cause de (2) à

$$Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor - X_b(n) \tag{7}$$

Là, on doit distinguer 2 cas :

- *cas 1* : Si n est un double d'impair (i.e. de la forme $4k+2$), alors

$$\left\lfloor \frac{n-2}{4} \right\rfloor = \left\lfloor \frac{n-4}{4} \right\rfloor + 1 \tag{a}$$

- *cas 2* : Si n est un double de pair (i.e. de la forme $4k$), alors

$$\left\lfloor \frac{n-2}{4} \right\rfloor = \left\lfloor \frac{n-4}{4} \right\rfloor \tag{b}$$

On remplace $\left\lfloor \frac{n-2}{4} \right\rfloor$ par ces deux valeurs dans l'égalité (7) ci-dessus ; on obtient :

- *cas 1* : $$Y_c(n) = \left\lfloor \frac{n-4}{4} \right\rfloor + 1 - X_b(n) \tag{7a}$$
- *cas 2* : $$Y_c(n) = \left\lfloor \frac{n-4}{4} \right\rfloor - X_b(n) \tag{7b}$$

D'autre part, de l'hypothèse $X_a(n) = 0$ et de $X_a(n) + X_c(n) = Z_a(n) + \delta_{2p}$ (5), il découle

$$X_c(n) = Z_a(n) + \delta_{2p} \tag{8}$$

On réécrit (2) en

$$X_c(n) = Y_c(n) - X_d(n) \tag{2'}$$

$$X_d(n) = Y_c(n) - X_c(n) \tag{2''}$$

En identifiant $X_c(n)$ dans (2') et (8), on obtient

$$Z_a(n) + \delta_{2p} = Y_c(n) - X_d(n) \tag{9}$$

que l'on réécrit

$$X_d(n) = Y_c(n) - Z_a(n) - \delta_{2p} \tag{9'}$$

En identifiant $X_d(n)$ dans (9') et (2''), on obtient

$$X_c(n) = Z_a(n) + \delta_{2p} \tag{10}$$

On est retombé sur la propriété 5, le raisonnement tourne en rond.

En annexe 2 sont fournies des représentations graphiques des bijections ensemblistes pour les cas $n = 32$, 34, 98 et 100.

Le fichier *http://denise.vella.chemla.free.fr/annexes.pdf* fournit

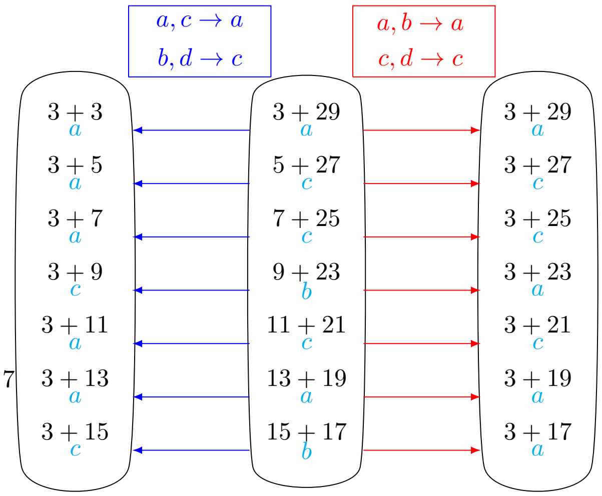
- un rappel historique d'un texte de Laisant qui présentait déjà en 1897 l'idée de "bandes" de nombres impairs à mettre en regard et à colorer pour voir les décompositions de Goldbach ;
- un programme et son exécution qui implémente les idées présentées dans la présente note.

Annexe 1 : tableau de valeurs des variables pour n compris entre 14 et 100

n	$X_a(n)$	$X_b(n)$	$X_c(n)$	$X_d(n)$	$Y_a(n)$	$Y_c(n)$	$\left\lfloor \frac{n-2}{4} \right\rfloor$	$Z_a(n)$	$Z_c(n)$	$\left\lfloor \frac{n-4}{4} \right\rfloor$
14	2	0	1	0	2	1	3	2	0	2
16	2	0	1	0	2	1	3	3	0	3
18	2	0	1	1	2	2	4	3	0	3
20	2	1	1	0	3	1	4	3	1	4
22	3	1	1	0	4	1	5	3	1	4
24	3	0	1	1	3	2	5	4	1	5
26	3	1	2	0	4	2	6	4	1	5
28	2	1	3	0	3	3	6	5	1	6
30	3	0	2	2	3	4	7	5	1	6
32	2	2	3	0	4	3	7	5	2	7
34	4	1	2	1	5	3	8	5	2	7
36	4	0	2	2	4	4	8	6	2	8
38	2	2	5	0	4	5	9	6	2	8
40	3	1	4	1	4	5	9	7	2	9
42	4	0	3	3	4	6	10	7	2	9
44	3	2	4	1	5	5	10	7	3	10
46	4	2	4	1	6	5	11	7	3	10
48	5	0	3	3	5	6	11	8	3	11
50	4	2	4	2	6	6	12	8	3	11
52	3	3	5	1	6	6	12	8	4	12
54	5	1	3	4	6	7	13	8	4	12
56	3	4	5	1	7	6	13	8	5	13
58	4	3	5	2	7	7	14	8	5	13
60	6	0	3	5	6	8	14	9	5	14
62	3	4	7	1	7	8	15	9	5	14
64	5	2	5	3	7	8	15	10	5	15
66	6	1	4	5	7	9	16	10	5	15
68	2	5	8	1	7	9	16	10	6	16
70	5	3	5	4	8	9	17	10	6	16
72	6	2	4	5	8	9	17	10	7	17
74	5	4	6	3	9	9	18	10	7	17
76	5	4	6	3	9	9	18	11	7	18
78	7	2	4	6	9	10	19	11	7	18
80	4	5	7	3	9	10	19	11	8	19
82	5	5	7	3	10	10	20	11	8	19
84	8	1	4	7	9	11	20	12	8	20
86	5	5	8	3	10	11	21	12	8	20
88	4	5	9	3	9	12	21	13	8	21
90	9	0	4	9	9	13	22	13	8	21
92	4	6	9	3	10	12	22	13	9	22
94	5	5	9	4	10	13	23	13	9	22
96	7	2	7	7	9	14	23	14	9	23
98	3	6	11	4	9	15	24	14	9	23
100	6	4	8	6	10	14	24	14	10	24

Annexe 2 : bijections ensemblistes

- Cas $n = 32$



$Z_a = X_a + X_c = 5$
$Z_c = X_b + X_d = 2$

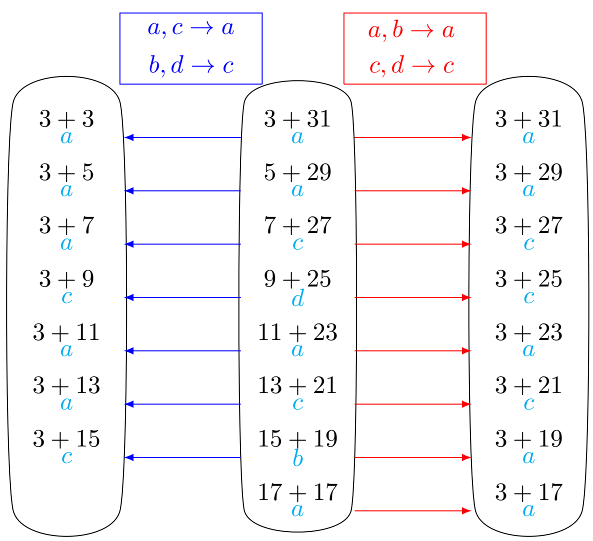
$Z_a + Z_c = \left\lfloor \frac{n-4}{4} \right\rfloor = 7$

$Y_a = X_a + X_b = 4$
$Y_c = X_c + X_d = 3$

$Y_a + Y_c = \left\lfloor \frac{n-2}{4} \right\rfloor = 7$

$X_a = 2$
$X_b = 2$
$X_c = 3$
$X_d = 0$

- Cas $n = 34$



$Z_a = X_a + X_c = 5$
$Z_c = X_b + X_d = 2$

$Z_a + Z_c = \left\lfloor \frac{n-4}{4} \right\rfloor = 7$

$Y_a = X_a + X_b = 5$
$Y_c = X_c + X_d = 3$

$Y_a + Y_c = \left\lfloor \frac{n-2}{4} \right\rfloor = 8$

$X_a = 4$
$X_b = 1$
$X_c = 2$
$X_d = 1$

- Cas $n = 98$

$Xc = 11$

$Za = 14$

$3+3 \quad 3+5 \quad 3+7 \quad 3+11$
$3+13 \quad 3+17 \quad 3+19 \quad 3+23$
$3+29 \quad 3+31 \quad 3+37$
$3+41 \quad 3+43 \quad 3+47$

$3+95 \quad 23+75$
$5+93 \quad 29+69$
$7+91 \quad 41+57$
$11+87 \quad 43+55$
$13+85 \quad 47+51$
$17+81$

$Xa = 3$

$19+79$
$31+67$
$37+61$

$Ya = 9$

$3+53 \quad 3+59 \quad 3+61$
$3+67 \quad 3+71 \quad 3+73$
$3+79 \quad 3+83 \quad 3+89$

$3+9 \quad 3+15 \quad 3+21 \quad 3+25$
$3+27 \quad 3+33 \quad 3+35 \quad 3+39$
$3+45$

$Zc = 9$

$21+77$
$33+65$
$35+63$
$49+49$

$Xd = 4$

$9+89$
$15+83$
$25+73$
$27+71$
$39+59$
$45+53$

$Xb = 6$

$3+49 \quad 3+51 \quad 3+55 \quad 3+57$
$3+63 \quad 3+65 \quad 3+69 \quad 3+75$
$3+77 \quad 3+81 \quad 3+85 \quad 3+87$
$3+91 \quad 3+93 \quad 3+95$

$Yc = 15$

- Cas $n = 100$

$Xc = 8 \qquad Xa = 6$

$Za = 14$

$3+3 \quad 3+5 \quad 3+7 \quad 3+11$
$3+13 \quad 3+17 \quad 3+19 \quad 3+23$
$3+29 \quad 3+31 \quad 3+37$
$3+41 \quad 3+43 \quad 3+47$

$5+95 \quad 37+63$
$7+93 \quad 43+57$
$13+87$
$19+81$
$23+77$
$31+69$

$3+97$
$11+89$
$17+83$
$29+71$
$41+59$
$47+53$

$Ya = 10$

$3+53 \quad 3+59 \quad 3+61$
$3+67 \quad 3+71 \quad 3+73$
$3+79 \quad 3+83 \quad 3+89 \quad 3+97$

$3+9 \quad 3+15 \quad 3+21 \quad 3+25$
$3+27 \quad 3+33 \quad 3+35 \quad 3+39$
$3+45 \quad 3+49$

$Zc = 10$

$9+91$
$15+85$
$25+75$
$35+65$
$45+55$
$49+51$

$21+79$
$27+73$
$33+67$
$39+61$

$Xb = 4$

$3+51 \quad 3+55 \quad 3+57$
$3+63 \quad 3+65 \quad 3+69 \quad 3+75$
$3+77 \quad 3+81 \quad 3+85 \quad 3+87$
$3+91 \quad 3+93 \quad 3+95$

$Yc = 14$

$Xd = 6$

Conjecture de Goldbach, langage à 4 lettres, variables et invariants

Denise Vella-Chemla

8/5/2014

1 Introduction

La conjecture de Goldbach stipule que tout nombre pair sauf 2 est la somme de deux nombres premiers. Dans la suite, on s'intéresse aux décompositions d'un nombre pair n en somme de deux nombres impairs $p+q$ avec $3 \leqslant p \leqslant n/2$, $n/2 \leqslant q \leqslant n-3$ et $p \leqslant q$. On appelle p un *sommant de premier rang* et q un *sommant de second rang* de n.

Notations :

On désignera par :
- a : une décomposition de n de la forme $p+q$ avec p et q premiers ;
- b : une décomposition de n de la forme $p+q$ avec p composé et q premier ;
- c : une décomposition de n de la forme $p+q$ avec p premier et q composé ;
- d : une décomposition de n de la forme $p+q$ avec p et q composés.

Exemple :

40	3	5	7	9	11	13	15	17	19
	37	35	33	31	29	27	25	23	21
l_{40}	a	c	c	b	a	c	d	a	c

2 Le tableau principal

On désigne par $T = (L, C) = (\ l_{n,m}\ )$ le tableau dont les éléments $l_{n,m}$ sont l'une des lettres a, b, c, d. L'indice n appartient à l'ensemble L des nombres pairs supérieurs ou égaux à 6. L'indice m, appartenant à l'ensemble C des nombres impairs supérieurs ou égaux à 3, est un élément de la liste des sommants de n de premier rang.

Considérons la fonction g définie ainsi :

$$\begin{array}{rccl} g: & 2\mathbb{N} & \to & 2\mathbb{N}+1 \\ & x & \mapsto & 2\left\lfloor \dfrac{x-2}{4} \right\rfloor + 1 \end{array}$$

$g(6) = 3, g(8) = 3, g(10) = 5, g(12) = 5, g(14) = 7, g(16) = 7, etc.$

La fonction $g(n)$ définit le plus grand des sommants de premier rang associés à n.

Comme l'on ne prend en compte que les décompositions de n de la forme $p+q$ où $p \leqslant q$, seules apparaîtront dans le tableau les lettres $l_{n,m}$ telles que $m \leqslant 2\left\lfloor \dfrac{n-2}{4} \right\rfloor + 1$ de sorte que le tableau contient les éléments suivants : $l_{6,3}, l_{8,3}, l_{10,3}, l_{10,5}, l_{12,3}, l_{12,5}, l_{14,3}, l_{14,5}, l_{14,7}, etc.$

Voici le début du tableau.

L \ C	3	5	7	9	11	13	15	17
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
...								

FIGURE 1 : mots des nombres pairs de 6 à 36

Remarques :

1) les mots situés sur les diagonales du tableau appelés *mots diagonaux* ont leurs lettres soit dans l'alphabet $A_{ab} = \{a, b\}$ soit dans l'alphabet $A_{cd} = \{c, d\}$.

2) un mot diagonal code des décompositions de même sommant de second rang.
Par exemple, sur la Figure 4, les lettres de la diagonale *aaabaa* qui commence à la lettre $l_{26,3} = a$ code les décompositions $3 + 23, 5 + 23, 7 + 23, 9 + 23, 11 + 23$ et $13 + 23$.

3) Désignons par l_n la ligne dont les éléments sont les $l_{n,m}$. La ligne l_n possède $\left\lfloor \dfrac{n-2}{4} \right\rfloor$ éléments.

4) n étant fixé, appelons $C_{n,3}$ la colonne formée des $l_{k,3}$ pour $6 \leqslant k \leqslant n$.

Dans cette colonne $C_{n,3}$, distinguons deux parties, la "partie haute" et la "partie basse" de la colonne.

Notons $H_{n,3}$ la "partie haute" de la colonne, i.e. l'ensemble des $l_{k,3}$ où $6 \leqslant k \leqslant \left\lfloor \dfrac{n+4}{2} \right\rfloor$.

Notons $B_{n,3}$ la "partie basse" de la colonne, i.e. l'ensemble des $l_{k,3}$ où $\left\lfloor \dfrac{n+4}{2} \right\rfloor < k \leqslant n$.

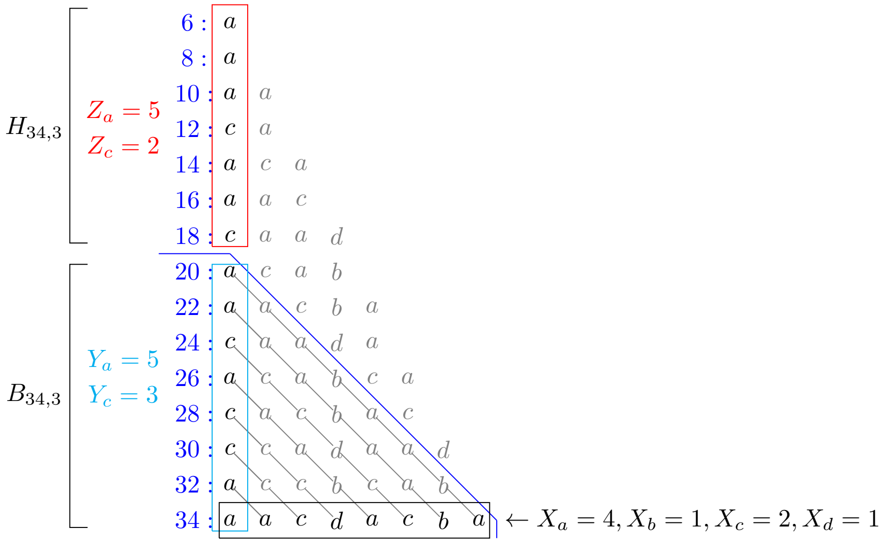


FIGURE 2 : $n = 34$

Pour mieux cerner les dénombrements de la section suivante, on utilisera la projection P de la ligne n sur la partie basse de la première colonne $B_{n,3}$ qui "associe" les lettres aux deux bouts d'une diagonale. Si on considère l'application $proj$ telle que $proj(a) = proj(b) = a$ et $proj(c) = proj(d) = c$ alors, puisque 3 est premier, $proj(l_{n,2k+1}) = l_{n-2k+2,3}$.

On peut comprendre l'effet de cette projection (qui préserve le sommant de second rang) en analysant les décompositions :

- si $p+q$ est codée par une lettre a ou une lettre b, cela correspond aux deux cas possibles dans lesquels q est premier, alors la décomposition $3+q$, contenant deux nombres premiers sera codée par la lettre a ;
- si $p+q$ est codée par une lettre c ou une lettre d, cela correspond aux deux cas possibles dans lesquels q est composé, alors la décomposition $3+q$, de la forme *premier* + *composé* sera codée par la lettre c.

On utilisera également dans la section suivante une projection qui transforme le sommant de premier rang en sommant de second rang que l'on combine à 3 comme sommant de premier rang ; analysons l'effet qu'une telle projection aura sur les décompositions :

- si $p+q$ est codée par une lettre a ou une lettre c, cela correspond aux deux cas possibles dans lesquels p est premier, alors la décomposition $3+p$, contenant deux nombres premiers sera codée par la lettre a ;
- si $p+q$ est codée par une lettre b ou une lettre d, cela correspond aux deux cas possibles dans lesquels p est composé, alors la décomposition $3+p$, de la forme *premier* + *composé* sera codée par la lettre c.

3 Dénombrements

1) On note dans la ligne n par :

- $X_a(n)$ le nombre de décompositions de n de la forme *premier* + *premier* ;
- $X_b(n)$ le nombre de décompositions de n de la forme *composé* + *premier* ;
- $X_c(n)$ le nombre de décompositions de n de la forme *premier* + *composé* ;
- $X_d(n)$ le nombre de décompositions de n de la forme *composé* + *composé*.

$X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$ est le nombre d'éléments de la ligne de n.

Exemple : $n = 34$:
$X_a(34) = \#\{3+31, 5+29, 11+23, 17+17\} = 4$
$X_b(34) = \#\{15+19\} = 1.$
$X_c(34) = \#\{7+27, 13+21\} = 2$
$X_d(34) = \#\{9+25\} = 1$

2) Soit $Y_a(n)$ (resp. $Y_c(n)$) le nombre de a (resp. c) qui apparaissent dans $B_{n,3}$. On rappelle qu'il n'y a que des lettres a et c dans la première colonne car elle contient les lettres associées aux décompositions de la forme $3 + x$ et que 3 est premier.

Exemple :

- $Y_a(34) = \#\{3+17, 3+19, 3+23, 3+29, 3+31\} = 5$
- $Y_c(34) = \#\{3+21, 3+25, 3+27\} = 3$

3) Compte-tenu de la projection P qui est une bijection, des définitions des lettres a, b, c, d, $Y_a(n) = X_a(n) + X_b(n)$ et $Y_c(n) = X_c(n) + X_d(n)$. Par suite, trivialement, $Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$.

Exemple :

$$\begin{array}{ll}
Y_a(34) & = \#\{3+17, 3+19, 3+23, 3+29, 3+31\} \\
X_a(34) & = \#\{3+31, 5+29, 11+23, 17+17\} \\
X_b(34) & = \#\{15+19\} \\
 & \\
Y_c(34) & = \#\{3+21, 3+25, 3+27\} \\
X_c(34) & = \#\{7+27, 13+21\} \\
X_d(34) & = \#\{9+25\}
\end{array}$$

4) Soit $Z_a(n)$ (resp. $Z_c(n)$) le nombre de a (resp. c) qui apparaissent dans $H_{n,3}$.

Exemple :

- $Z_a(34) = \#\{3+3, 3+5, 3+7, 3+11, 3+13\} = 5$
- $Z_c(34) = \#\{3+9, 3+15\} = 2$

$Z_a(n) + Z_c(n) = \left\lfloor \dfrac{n-4}{4} \right\rfloor$.

Rappel des propriétés identifiées

$$Y_a(n) = X_a(n) + X_b(n) \tag{1}$$

$$Y_c(n) = X_c(n) + X_d(n) \tag{2}$$

$$Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

$$Z_a(n) + Z_c(n) = \left\lfloor \frac{n-4}{4} \right\rfloor \tag{4}$$

Ajoutons quatre nouvelles propriétés à celles-ci :

$$X_a(n) + X_c(n) = Z_a(n) + \delta_{2p}(n) \tag{5}$$

avec $\delta_{2p}(n)$ qui vaut 1 dans le cas où n est le double d'un nombre premier et qui vaut 0 sinon.

$$X_b(n) + X_d(n) = Z_c(n) + \delta_{2c-imp}(n) \tag{6}$$

avec $\delta_{2c-imp}(n)$ qui vaut 1 dans le cas où n est un double d'impair composé, et qui vaut 0 sinon.

$$Z_c(n) - Y_a(n) = Y_c(n) - Z_a(n) - \delta_{4k+2}(n) \tag{7}$$

avec $\delta_{4k+2}(n)$ qui vaut 1 si n est un double d'impair et 0 sinon.

$$Z_c(n) - Y_a(n) = X_d(n) - X_a(n) - \delta_{2c-imp}(n) \tag{8}$$

4 Evolution des variables

Dans cette section, étudions comment les différentes variables évoluent.

$Z_a(n) + Z_c(n) = \left\lfloor \dfrac{n-4}{4} \right\rfloor$ est une fonction croissante de n, elle augmente de 1 à chaque n double de pair.

$Z_a(n+2) = Z_a(n)$ et $Z_c(n+2) = Z_c(n)$ sont fixes quand n est un double de pair.

$Z_a(n) = Z_a(n-2) + 1$ quand $\dfrac{n-2}{2}$ est un nombre premier (*ex* : $n = 24$ ou $n = 28$, se reporter au tableau de valeurs page 13 : on exprime cela abusivement par *"Z_a augmente"*) et $Z_c(n) = Z_c(n-2) + 1$ quand $\dfrac{n-2}{2}$ est un nombre composé impair (*ex* : $n = 42$ ou 50, abusivement, *"Z_c augmente"*).

$Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$ est une fonction croissante de n, elle augmente de 1 à chaque n double d'impair.

Voyons maintenant dans le détail comment évoluent $Y_a(n)$ et $Y_c(n)$.

Dans le cas où n est un double d'impair, on ajoute un nombre à l'intervalle $H_{n,3}$; si ce nombre $n-3$ est premier (resp. composé), $Y_a(n) = Y_a(n-2) + 1$ (abusivement *"Y_a augmente"*, *ex* : $n = 34$) (resp. $Y_c(n) = Y_c(n-2) + 1$, abusivement *"Y_c augmente"*, *ex* : $n = 38$).

Dans le cas où n est un double de pair, 4 cas se présentent. Etudions la manière dont évolue l'ensemble de décompositions $H_{n,3}$.

- si $n-3$ et $\dfrac{n-2}{2}$ sont tous les deux premiers, on retire en bas et et on ajoute en haut de l'intervalle $H_{n,3}$ deux lettres de même sorte, alors $Y_a(n) = Y_a(n-2)$ et $Y_c(n) = Y_c(n-2)$ (abusivement *"Y_a et Y_c constants"* (*ex* : $n = 40$)) ;
- si $n-3$ est premier et $\dfrac{n-2}{2}$ est composé alors $Y_a(n) = Y_a(n-2) + 1$ et $Y_c(n) = Y_c(n-2) - 1$ (abusivement, *"Y_a augmente et Y_c diminue"* (*ex* : $n = 32$)) ;
- si $n-3$ est composé et $\dfrac{n-2}{2}$ est premier alors $Y_c(n) = Y_c(n-2) + 1$ et $Y_a(n) = Y_a(n-2) - 1$ (abusivement, *"Y_a diminue et Y_c augmente"* (*ex* : $n = 48$)) ;
- si $n-3$ et $\dfrac{n-2}{2}$ sont tous les deux composés, on retire en bas et et on ajoute en haut de l'intervalle $H_{n,3}$ deux lettres de même sorte, alors $Y_a(n) = Y_a(n-2)$ et $Y_c(n) = Y_c(n-2)$ (abusivement, *"Y_a et Y_c constants"* (*ex* : $n = 52$)).

En annexe 1 sont fournies dans une table les valeurs des différentes variables pour n compris entre 14 et 100.

5 Utiliser les écarts entre variables

On va montrer ci-dessous que $X_a(n)$ ne peut jamais être nul pour $n \geqslant C$, C étant une certaine constante à définir, i.e. montrer que tout entier pair $n \geqslant C$ peut s'écrire comme une somme de deux nombres premiers, c'est-à-dire vérifie la conjecture de Goldbach.

On a vu qu'à $\delta_{4k+2}(n)$ ou $\delta_{2c-imp}(n)$ près ($\delta_{4k+2}(n)$ et/ou $\delta_{2c-imp}(n)$ étant égaux à 1 dans certains cas), on a les égalités suivantes :

$$Z_c(n) - Y_a(n) = Y_c(n) - Z_a(n) - \delta_{4k+2}(n) \qquad (7)$$

$$Z_c(n) - Y_a(n) = X_d(n) - X_a(n) - \delta_{2c-imp}(n) \qquad (8)$$

On rappelle que

- $Y_a(n)$, comptant le nombre de nombres premiers qui sont compris entre $\frac{n}{2}$ et n vaut $\pi(n) - \pi\left(\frac{n}{2}\right)$;
- $Z_a(n)$ comptant le nombre de nombres premiers inférieurs ou égaux à $\frac{n}{2}$ vaut $\pi\left(\frac{n}{2}\right)$;
- $Z_c(n)$ comptant le nombre de nombres composés impairs inférieurs ou égaux à $\frac{n}{2}$ vaut $\frac{n}{4} - \pi\left(\frac{n}{2}\right)$;
- $Y_c(n)$ comptant le nombre de nombres composés impairs qui sont compris entre $\frac{n}{2}$ et n vaut $\frac{n}{4} - \pi(n) + \pi\left(\frac{n}{2}\right)$.

L'article de Rosser et Schoenfeld [1] fournit comme formule 3.5 du corollaire 1 du théorème 2 que $\pi(x) > \frac{x}{ln\ x}$ pour tout $x \geqslant 17$, et comme formule 3.6 du même corollaire du même théorème que $\pi(x) < \frac{1,25506x}{ln\ x}$ pour tout $x > 1$.

5.1 Etude de l'inégalité $Z_c(n) > Z_a(n)$

Pour montrer que $Z_c(n) > Z_a(n)$, on peut utiliser simplement l'argument que $Z_c(n)$ augmente "bien plus souvent" que $Z_a(n)$ (à chaque $\frac{n-2}{2}$ composé impair pour $Z_c(n)$ et à chaque $\frac{n-2}{2}$ premier pour $Z_a(n)$ comme cela a été vu dans la section 4).

Pour trouver à partir de quelle valeur de n on a $Z_c(n) > Z_a(n)$, on utilise le fait que l'écart $Z_c(n) - Z_a(n)$ est égal à $\frac{n}{4} - 2\ \pi\left(\frac{n}{2}\right)$.

Par la formule (3.6), on a $2\ \pi\left(\frac{n}{2}\right) < 2\ \frac{1,25506\ n}{2\ (ln\ n + ln\ 0.5)}$ pour tout $n > 2$.

On en déduit $-2\ \pi\left(\frac{n}{2}\right) > \frac{-1,25506\ n}{ln\ n + ln\ 0.5}$ pour tout $n > 2$.

L'écart $Z_c(n) - Z_a(n)$ est donc minorable par $\frac{n\ (ln\ n + ln\ 0.5) - 5,02024n}{4\ (ln\ n + ln\ 0.5)}$. Il est strictement positif pour tout $n \geqslant 304$ (le dénominateur est positif pour $n \geqslant 2$, le numérateur est strictement positif pour tout $n > 2e^{5.02024}$).

5.2 Etude des inégalités $Z_a(n) > Y_a(n)$ et $Y_c(n) > Z_c(n)$

Pour montrer que $Z_a(n) > Y_a(n)$, on peut utiliser à nouveau l'analyse de l'évolution des variables de la section 4 : quand *"Z_a augmente"*, *"Y_a est constante ou diminue"* ; et quand *"Y_a augmente"* sans que *"Z_a n'augmente"* (lorsque $n-3$ est premier et $\frac{n-2}{2}$ est composé), Y_a n'augmente que de 1 alors que son écart à Z_a est très vite très supérieur à 1.

Pour démontrer que $Y_c(n) > Z_c(n)$, on peut utiliser à nouveau l'analyse de l'évolution des variables de la section 4 : Y_c augmente quand $n-3$ est composé tandis que Z_c augmente quand $\frac{n-2}{2}$ est composé. Z_c est croissante, parfois Y_c décroît mais peu souvent ce qui a pour conséquence qu'à partir d'une valeur plutôt petite, Z_c ne "rattrape plus" Y_c.

Pour connaître précisément à partir de quelles valeurs de n les inégalités souhaitées sont vérifiées, on utilise à nouveau la valeur des écarts et les minorations/majorations fournies dans [1].

Pour montrer que $Z_a(n) > Y_a(n)$ (resp. $Y_c(n) > Z_c(n)$), on montre que l'écart

$$Z_a(n) - Y_a(n) = Y_c(n) - Z_c(n) = 2\pi\left(\frac{n}{2}\right) - \pi(n)$$

est toujours strictement positif.

On utilise la formule 3.9 du corollaire 3 du théorème 2 de Rosser et Schoenfeld qui énonce que $\pi(x) - \pi\left(\frac{x}{2}\right) < \frac{7x}{5\ ln\ x}$ pour tout $x > 1$.

On utilise le fait que $2\pi\left(\frac{n}{2}\right) - \pi(n) = \left(\pi\left(\frac{n}{2}\right) - \pi(n)\right) + \pi\left(\frac{n}{2}\right)$

On a donc

$$\begin{aligned} 2\pi\left(\frac{n}{2}\right) - \pi(n) &> \frac{-7n}{5\ ln\ n} + \pi\left(\frac{n}{2}\right) \\ &> \frac{-7n}{5\ ln\ n} + \frac{n}{2\ (ln\ n + ln\ 0.5)} \qquad \text{(à cause de la formule 3.5 du corollaire 1 du théorème 2 de [1])} \end{aligned}$$

qui est strictement positif si

$$\frac{n(5\ ln\ n - 14\ (ln\ n + ln\ 0.5))}{10\ ln\ n(ln\ n + ln\ 0.5)} > 0$$

ce qui équivaut à

$$5\ ln\ n - 14\ (ln\ n + ln\ 0.5) > 0$$

qui est toujours vrai pour $n \geqslant 6$.

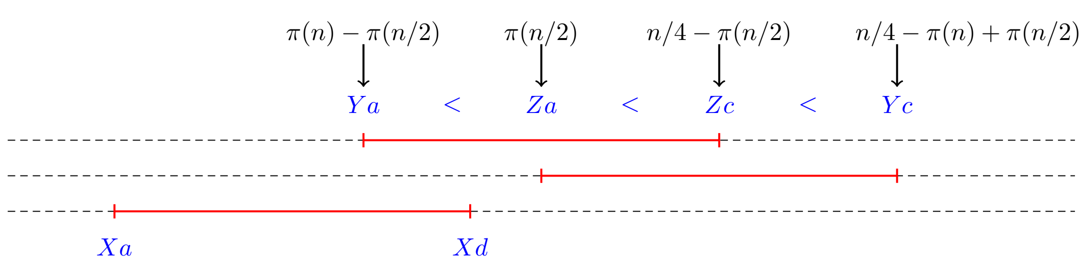
5.3 Ordre strict sur les 4 variables $Y_a(n), Y_c(n), Z_a(n)$ et $Z_c(n)$

Les variables $Y_a(n), Z_a(n), Z_c(n)$ et $Y_c(n)$ sont donc strictement ordonnées de la façon suivante :

$$Y_a(n) < Z_a(n) < Z_c(n) < Y_c(n)$$

pour tout $n \geqslant 304$.

Une représentation imagée des écarts entre variables est fournie ci-dessous, qui montre leur intrication :



Les écarts $Z_c(n) - Y_a(n)$, $Y_c(n) - Z_a(n)$ et $X_d(n) - X_a(n)$ sont strictement positifs et égaux à $\frac{n}{4} - \pi(n)$.

5.4 Etude de l'inégalité $X_a(n) > 0$

Pour être assuré que $X_a(n)$ soit toujours non nul, il faut minorer $X_d(n)$ par $\dfrac{n}{4} - \pi(n)$, i.e. la valeur de l'écart $X_d(n) - X_a(n)$.

Or $X_d(n) = Y_c(n) - X_c(n)$.

Pour minorer $X_d(n)$, il faut minorer $Y_c(n)$ et majorer $X_c(n)$.

$Y_c(n)$ est le nombre de nombres composés impairs compris entre $n/2$ et n (associés à 3).

Pour minorer $Y_c(n)$, on utilise le fait que le nombre de nombres composés impairs compris entre $n/2$ et n est égal à $\dfrac{n}{4} - \pi(n) + \pi\left(\dfrac{n}{2}\right)$.

$X_c(n)$, le nombre de décompositions de n de la forme *premier* + *composé* est majorable par le nombre total de nombres composés impairs compris entre $n/2$ et n, lui-même majorable par le nombre de nombres composés impairs compris entre n et $\dfrac{3n}{2}$.

$X_c(n)$ est donc majorable par $\dfrac{n}{4} - \left(\pi\left(\dfrac{3n}{2}\right) - \pi(n)\right)$ (le nombre de nombres impairs de l'intervalle de n à $\dfrac{3n}{2}$ est $\dfrac{n}{4}$, le nombre de nombres premiers sur cet intervalle est $\pi\left(\dfrac{3n}{2}\right) - \pi(n)$, le nombre de nombres composés impairs sur cet intervalle est la différence de ces deux nombres).

$Y_c(n) - X_c(n)$ est donc toujours supérieur à la différence de la minoration de $Y_c(n)$ et de la majoration de $X_c(n)$, ce qui donne

$$Y_c(n) - X_c(n) > \frac{n}{4} - \pi(n) + \pi\left(\frac{n}{2}\right) - \frac{n\,((ln\ n + ln\ 1.5)(ln\ n - 4 \times 1.25506) - 1.25506 \times 6 \times ln\ n)}{4\ (ln\ n + ln\ 1.5)\ ln\ n}.$$

$Y_c(n) - X_c(n) = X_d(n)$ dépasse toujours $\dfrac{n}{4} - \pi(n)$ lorsque $n > 0$ (on le constate également par programme).

En effet, $Y_c(n) - X_c(n) > \dfrac{n}{4} - \pi(n)$ lorsque

$$\pi\left(\frac{n}{2}\right) - \frac{n\,((ln\ n + ln\ 1.5)(ln\ n - 4 \times 1.25506) - 1.25506 \times 6 \times ln\ n)}{4\ (ln\ n + ln\ 1.5)\ ln\ n} > 0.$$

On remplace $\pi\left(\dfrac{n}{2}\right)$ par sa minoration fournie par la formule 3.5 du corollaire 1 du théorème 2 (qui est $\dfrac{n}{2(ln\ n + ln\ 0.5)}$), on réduit au même dénominateur, qui est toujours positif pour $n \geqslant 2$ et qu'on oublie, on cherche la condition qui assure que le numérateur est toujours strictement positif, numérateur qui est égal à :

$$n[(2(ln\ n + ln\ 1.5)ln\ n) - (ln\ n + ln\ 0.5)((ln\ n + ln\ 1.5)(ln\ n - 5.02024) - 7.53036\ ln\ n)]$$

Après calculs, on obtient que le numérateur, d'inconnue $ln\ n$, est égal au polynôme

$$-(ln\ n)^3 + 14.6755387366(ln\ n)^2 - 2.48889541216(ln\ n) - 0.26611665186$$

La plus grande racine de ce polynôme est à peu près égale à 14.502656936497 d'exponentielle 1988034.33365. La différence entre $X_d(n)$ et $X_a(n)$ est donc toujours supérieure à $\dfrac{n}{4} - \pi(n)$ pour tout $n \geqslant 1988034.33365$.

On peut ainsi conclure que pour tout $n \geqslant 1988034.33365$ (la condition nécessitée pour que $X_d(n) - X_a(n) > \dfrac{n}{4} - \pi(n)$), $X_a(n)$ (le nombre de décompositions de n comme somme de deux nombres premiers) est strictement positif.

En annexe 2 sont fournies des représentations graphiques des bijections ensemblistes pour les cas $n = 32$, 34, 98 et 100.

Le fichier $http://denise.vella.chemla.free.fr/annexes.pdf$ fournit

- un rappel historique d'un texte de Laisant qui présentait déjà en 1897 l'idée de "bandes" de nombres impairs à mettre en regard et à colorer pour voir les décompositions de Goldbach ;
- un programme et son exécution qui implémente les idées exposées dans la présente note.

6 Démonstrations

6.1 Utilitaires

Démontrons que si n est un double d'impair (i.e. de la forme $4k+2$), alors $\left\lfloor \dfrac{n-2}{4} \right\rfloor = \left\lfloor \dfrac{n-4}{4} \right\rfloor + 1$.

En effet, le membre gauche de l'égalité vaut $\left\lfloor \dfrac{(4k+2)-2}{4} \right\rfloor = \left\lfloor \dfrac{4k}{4} \right\rfloor = k$.

Le membre droit de l'égalité vaut $\left\lfloor \dfrac{(4k+2)-4}{4} \right\rfloor + 1 = \left\lfloor \dfrac{4k-2}{4} \right\rfloor + 1 = (k-1)+1 = k$.

Démontrons que si n est un double de pair (i.e. de la forme $4k$), alors $\left\lfloor \dfrac{n-2}{4} \right\rfloor = \left\lfloor \dfrac{n-4}{4} \right\rfloor$.

$\left\lfloor \dfrac{4k-2}{4} \right\rfloor = k-1$ et $\left\lfloor \dfrac{4k-4}{4} \right\rfloor = k-1$.

On peut aussi exprimer cela de la façon suivante : si n est un double d'impair, $\left\lfloor \dfrac{n-2}{4} \right\rfloor = \dfrac{n-2}{4} = \left\lfloor \dfrac{n-4}{4} \right\rfloor + 1$ tandis que si n est un double de pair, $\left\lfloor \dfrac{n-2}{4} \right\rfloor = \dfrac{n-4}{4} = \left\lfloor \dfrac{n-4}{4} \right\rfloor$.

6.2 Propriétés 5, 6 et 8

Les propriétés 5, 6 et 8 découlent directement des définitions des variables.

6.2.1 Propriété 5

La propriété 5 énonce que $X_a(n) + X_c(n) = Z_a(n) + \delta_{2p}(n)$ avec $\delta_{2p}(n)$ qui vaut 1 dans le cas où n est le double d'un nombre premier et qui vaut 0 sinon.

Par définition, $X_a(n) + X_c(n)$ compte le nombre de décompositions de n de la forme $premier + x$ avec $premier \leqslant n/2$. Dans la mesure où $Z_a(n)$ compte quant à lui le nombre de décompositions de la forme $3 + premier$ avec $premier < n/2$, l'ajout de δ_{2p} à $Z_a(n)$ permet d'assurer l'invariance de l'égalité, entre autres dans le cas où n est le double d'un nombre premier.

6.2.2 Propriété 6

La propriété 6 énonce que $X_b(n) + X_d(n) = Z_c(n) + \delta_{2c-imp}$ avec δ_{2c-imp} qui vaut 1 dans le cas où n est un double d'impair composé, et qui vaut 0 sinon.

Par définition, $X_b(n) + X_d(n)$ compte le nombre de décompositions de n de la forme $composé + x$ avec $composé \leqslant n/2$. Dans la mesure où $Z_c(n)$ compte quant à lui le nombre de décompositions de la forme $3 + composé$ avec $composé < n/2$, l'ajout de δ_{2c-imp} à $Z_c(n)$ permet d'assurer l'invariance de l'égalité, entre autres dans le cas où n est le double d'un nombre composé impair.

6.2.3 Propriété 8

La propriété 8 énonce que $Z_c(n) - Y_a(n) = X_d(n) - X_a(n) - \delta_{2c-imp}$ avec δ_{2c-imp} qui vaut 1 si n est un double de composé impair et 0 sinon.

Par définition, $Z_c(n)$ compte le nombre de nombres composés impairs inférieurs strictement à $n/2$. Il compte donc également le nombre de décompositions de n de la forme $compos\acute{e} + x$ avec $compos\acute{e} < n/2$ (appelons E cet ensemble de décompositions).

Par définition, $Y_a(n)$ compte le nombre de nombres premiers supérieurs strictement à $n/2$. Il compte donc également le nombre de décompositions de n de la forme $x + premier$ avec $premier > n/2$ (appelons F cet ensemble de décompositions).

Les décompositions de n de la forme $compos\acute{e} + premier$ sont à la fois dans E et dans F. En calculant $Z_c(n) - Y_a(n)$, on calcule donc le cardinal d'un ensemble qui s'avère être égal à $X_d(n) - X_a(n)$ par définition de ce que comptent les variables $Y_a(n), Z_c(n), X_d(n)$ et $X_a(n)$.

6.2.4 Propriété 7

Démontrons que $Z_c(n) - Y_a(n) = Y_c(n) - Z_a(n) - \delta_{4k+2}$ avec δ_{4k+2} qui vaut 1 si n est un double d'impair (il existe $k \geqslant 3$ tel que $n = 4k + 2$) et 0 sinon.

On utilise un raisonnement par récurrence :

i) On initialise les récurrences selon les 3 sortes de nombres à envisager : les doubles de pairs (de la forme $4k$, comme 16), les doubles d'impairs (donc de la forme $4k + 2$) qui sont premiers (comme 14) ou qui sont composés (comme 18).

La propriété 7 est vraie pour $n = 14$ car $Z_c(14) = 0, Y_a(14) = 2, Y_c(14) = 1, Z_a(14) = 2$ et $\delta_{4k+2}(14) = 1$ et donc $Z_c(14) - Y_a(14) = Y_c(14) - Z_a(14) - \delta_{4k+2}(14)$;
La propriété 7 est vraie pour $n = 16$ car $Z_c(16) = 0, Y_a(16) = 2, Y_c(16) = 1, Z_a(16) = 3$ et $\delta_{4k+2}(16) = 0$ et donc $Z_c(16) - Y_a(16) = Y_c(16) - Z_a(16) - \delta_{4k+2}(16)$;
La propriété 7 est vraie pour $n = 18$ car $Z_c(18) = 0, Y_a(18) = 2, Y_c(18) = 2, Z_a(18) = 3$ et $\delta_{4k+2}(18) = 1$ et donc $Z_c(18) - Y_a(18) = Y_c(18) - Z_a(18) - \delta_{4k+2}(18)$;

ii) On réécrit la propriété 7 sous la forme $Z_a(n) + Z_c(n) + \delta_{4k+2} = Y_a(n) + Y_c(n)$.
Quatre cas sont à considérer : deux cas selon lesquels n est un double d'impair (premier ou composé) et $n + 2$ est un double de pair et deux cas selon lesquels n est un double de pair et $n + 2$ est un double d'impair (premier ou composé).

iia) *n double de pair et $n + 2$ double de premier (ex : $n = 56$)* :

n	δ_{2p}	δ_{2c-imp}	δ_{4k+2}
n	0	0	0
$n+2$	1	0	1

On pose l'hypothèse que la propriété 7 est vraie pour n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \quad (H)$$

Démontrons qu'elle est vraie pour $n + 2$,

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \quad (Ccl)$$

On a $Z_a(n + 2) = Z_a(n)$ et $Z_c(n + 2) = Z_c(n)$.

Rappelons la propriété 3 concernant les Y :

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

Dans (Ccl), on peut, par l'hypothèse de récurrence et par la propriété (3), remplacer le membre gauche de l'égalité par $Z_a(n) + Z_c(n) + 1$ puis par $Y_a(n) + Y_c(n) + 1$ (par (H)) puis par $\left\lfloor \frac{n-2}{4} \right\rfloor + 1$ (par (3)) qui vaut $\left\lfloor \frac{n}{4} \right\rfloor$.

Mais dans (Ccl), on peut également remplacer le membre de droite de l'égalité par $\left\lfloor \frac{n}{4} \right\rfloor$ du fait de la propriété (3).

Il y a à nouveau pour $n+2$ égalité entre les membres gauche et droit de l'égalité, i.e. la propriété 7 est vérifiée par $n+2$. De l'hypothèse que la propriété est vraie pour n, on a démontré que la propriété est vraie pour $n+2$.

iib) *n double de pair et $n+2$ double de composé impair (ex : $n = 48$)* :

n	δ_{2p}	δ_{2c-imp}	δ_{4k+2}
n	0	0	0
$n+2$	0	1	1

On pose l'hypothèse que la propriété 7 est vraie pour n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \tag{H}$$

Démontrons qu'elle est vraie pour $n+2$,

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \tag{Ccl}$$

On a $Z_a(n+2) = Z_a(n)$ et $Z_c(n+2) = Z_c(n)$.

On a $Y_a(n+2) = Y_a(n) + 1$ et $Y_c(n+2) = Y_c(n)$.

Rappelons la propriété 3 concernant les Y :

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

Dans (Ccl), on peut, par l'hypothèse de récurrence et la propriété (3), remplacer le membre gauche de l'égalité par $Z_a(n)+Z_c(n)+1$ puis par $Y_a(n)+Y_c(n)+1$ (par (H)) puis par $\left\lfloor \frac{n-2}{4} \right\rfloor + 1$ (par (3)) qui vaut $\left\lfloor \frac{n}{4} \right\rfloor$.

Mais dans (Ccl), on peut également remplacer le membre de droite de l'égalité par $\left\lfloor \frac{n}{4} \right\rfloor$ du fait des évolutions de $Y_a(n)$ et $Y_c(n)$.

Il y a à nouveau pour $n+2$ égalité entre les membres gauche et droit de l'égalité, i.e. la propriété 7 est vérifiée par $n+2$. De l'hypothèse que la propriété est vraie pour n, on a démontré que la propriété est vraie pour $n+2$.

iic) *n double de premier et $n+2$ double de pair (ex : $n = 74$)* :

n	δ_{2p}	δ_{2c-imp}	δ_{4k+2}
n	1	0	1
$n+2$	0	0	0

On pose l'hypothèse que la propriété 7 est vraie pour n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \tag{H}$$

Démontrons qu'elle est vraie pour $n+2$,

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \qquad (Ccl)$$

On a $Z_a(n+2) = Z_a(n) + 1$ et $Z_c(n+2) = Z_c(n)$.

Rappelons la propriété 3 concernant les Y :

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \qquad (3)$$

Dans (Ccl), on peut, par l'hypothèse de récurrence et la propriété (3), remplacer le membre gauche de l'égalité par $Z_a(n)+Z_c(n)+1$ puis par $Y_a(n)+Y_c(n)$ (par (H)) puis par $\left\lfloor \frac{n-2}{4} \right\rfloor$ (par (3)) qui vaut $\left\lfloor \frac{n}{4} \right\rfloor$.

Mais dans (Ccl), on peut également remplacer le membre de droite de l'égalité par $\left\lfloor \frac{n}{4} \right\rfloor$ du fait de la propriété (3).

Il y a à nouveau pour $n+2$ égalité entre les membres gauche et droit de l'égalité, i.e. la propriété 7 est vérifiée par $n+2$. De l'hypothèse que la propriété est vraie pour n, on a démontré que la propriété est vraie pour $n+2$.

iid) n *double de composé impair et* $n+2$ *double de pair* (*ex :* $n = 70$) :

n	δ_{2p}	δ_{2c-imp}	δ_{4k+2}
n	0	1	1
$n+2$	0	0	0

On pose l'hypothèse que la propriété 7 est vraie pour n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \qquad (H)$$

Démontrons qu'elle est vraie pour

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \qquad (Ccl)$$

On a $Z_a(n+2) = Z_a(n)$ et $Z_c(n+2) = Z_c(n) + 1$.

Rappelons la propriété 3 concernant les Y :

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \qquad (3)$$

Dans (Ccl), on peut, par l'hypothèse de récurrence et la propriété (3), remplacer le membre gauche de l'égalité par $Z_a(n)+Z_c(n)+1$ puis par $Y_a(n)+Y_c(n)$ (par (H)) puis par $\left\lfloor \frac{n-2}{4} \right\rfloor$ (par (3)) qui vaut $\left\lfloor \frac{n}{4} \right\rfloor$.

Mais dans (Ccl), on peut également remplacer le membre de droite de l'égalité par $\left\lfloor \frac{n}{4} \right\rfloor$ du fait de la propriété (3).

Il y a à nouveau pour $n+2$ égalité entre les membres gauche et droit de l'égalité, i.e. la propriété 7 est vérifiée par $n+2$. De l'hypothèse que la propriété est vraie pour n, on a démontré que la propriété est vraie pour $n+2$.

Annexe 1 : tableau de valeurs des variables pour n compris entre 14 et 100

n	$X_a(n)$	$X_b(n)$	$X_c(n)$	$X_d(n)$	$Y_a(n)$	$Y_c(n)$	$\left\lfloor \frac{n-2}{4} \right\rfloor$	$Z_a(n)$	$Z_c(n)$	$\left\lfloor \frac{n-4}{4} \right\rfloor$	$\delta_{2p}(n)$	$\delta_{2c-imp}(n)$	$\delta_{4k+2}(n)$
14	2	0	1	0	2	1	3	2	0	2	1	0	1
16	2	0	1	0	2	1	3	3	0	3	0	0	0
18	2	0	1	1	2	2	4	3	0	3	0	1	1
20	2	1	1	0	3	1	4	3	1	4	0	0	0
22	3	1	1	0	4	1	5	3	1	4	1	0	1
24	3	0	1	1	3	2	5	4	1	5	0	0	0
26	3	1	2	0	4	2	6	4	1	5	1	0	1
28	2	1	3	0	3	3	6	5	1	6	0	0	0
30	3	0	2	2	3	4	7	5	1	6	0	1	1
32	2	2	3	0	4	3	7	5	2	7	0	0	0
34	4	1	2	1	5	3	8	5	2	7	1	0	1
36	4	0	2	2	4	4	8	6	2	8	0	0	0
38	2	2	5	0	4	5	9	6	2	8	1	0	1
40	3	1	4	1	4	5	9	7	2	9	0	0	0
42	4	0	3	3	4	6	10	7	2	9	0	1	1
44	3	2	4	1	5	5	10	7	3	10	0	0	0
46	4	2	4	1	6	5	11	7	3	10	1	0	1
48	5	0	3	3	5	6	11	8	3	11	0	0	0
50	4	2	4	2	6	6	12	8	3	11	0	1	1
52	3	3	5	1	6	6	12	8	4	12	0	0	0
54	5	1	3	4	6	7	13	8	4	12	0	1	1
56	3	4	5	1	7	6	13	8	5	13	0	0	0
58	4	3	5	2	7	7	14	8	5	13	1	0	1
60	6	0	3	5	6	8	14	9	5	14	0	0	0
62	3	4	7	1	7	8	15	9	5	14	1	0	1
64	5	2	5	3	7	8	15	10	5	15	0	0	0
66	6	1	4	5	7	9	16	10	5	15	0	1	1
68	2	5	8	1	7	9	16	10	6	16	0	0	0
70	5	3	5	4	8	9	17	10	6	16	0	1	1
72	6	2	4	5	8	9	17	10	7	17	0	0	0
74	5	4	6	3	9	9	18	10	7	17	1	0	1
76	5	4	6	3	9	9	18	11	7	18	0	0	0
78	7	2	4	6	9	10	19	11	7	18	0	1	1
80	4	5	7	3	9	10	19	11	8	19	0	0	0
82	5	5	7	3	10	10	20	11	8	19	1	0	1
84	8	1	4	7	9	11	20	12	8	20	0	0	0
86	5	5	8	3	10	11	21	12	8	20	1	0	1
88	4	5	9	3	9	12	21	13	8	21	0	0	0
90	9	0	4	9	9	13	22	13	8	21	0	1	1
92	4	6	9	3	10	12	22	13	9	22	0	0	0
94	5	5	9	4	10	13	23	13	9	22	1	0	1
96	7	2	7	7	9	14	23	14	9	23	0	0	0
98	3	6	11	4	9	15	24	14	9	23	0	1	1
100	6	4	8	6	10	14	24	14	10	24	0	0	0

n	$X_a(n)$	$X_b(n)$	$X_c(n)$	$X_d(n)$	$Y_a(n)$	$Y_c(n)$	$\left\lfloor \frac{n-2}{4} \right\rfloor$	$Z_a(n)$	$Z_c(n)$	$\left\lfloor \frac{n-4}{4} \right\rfloor$	δ_{2p}	δ_{2c-imp}	δ_{4k+2}
999 998	4 206	32 754	37 331	175 708	36 960	213 039	249 999	41 537	208 461	249 998	0	1	1
1 000 000	5 402	31 558	36 135	176 904	36 960	213 039	249 999	41 537	208 462	249 999	0	1	0
9 999 998	28 983	287 084	319 529	1 864 403	316 067	2 183 932	2 499 999	348 511	2 151 487	2 499 998	1	0	1
10 000 000	38 807	277 259	309 705	1 874 228	316 066	2 183 933	2 499 999	348 512	2 151 487	2 499 999	0	1	0

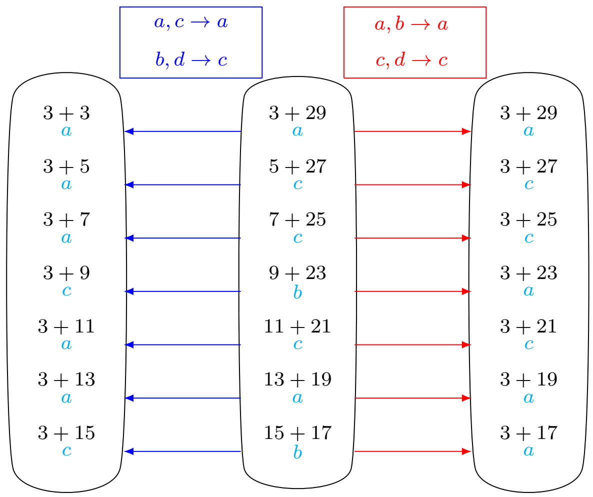
Annexe 2 : bijections ensemblistes

- Cas $n = 32$

$Z_a = X_a + X_c = 5$

$Z_c = X_b + X_d = 2$

$Z_a + Z_c = \left\lfloor \frac{n-4}{4} \right\rfloor = 7$



$Y_a = X_a + X_b = 4$

$Y_c = X_c + X_d = 3$

$Y_a + Y_c = \left\lfloor \frac{n-2}{4} \right\rfloor = 7$

$X_a = 2$

$X_b = 2$

$X_c = 3$

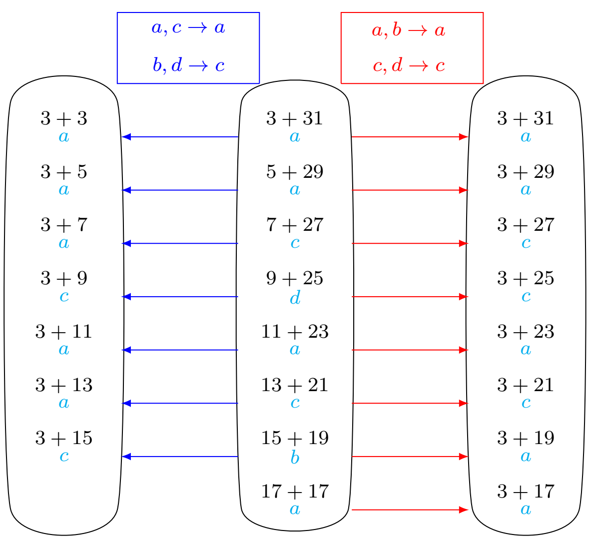
$X_d = 0$

- Cas $n = 34$

$Z_a = X_a + X_c = 5$

$Z_c = X_b + X_d = 2$

$Z_a + Z_c = \left\lfloor \frac{n-4}{4} \right\rfloor$=7



$Y_a = X_a + X_b = 5$

$Y_c = X_c + X_d = 3$

$Y_a + Y_c = \left\lfloor \frac{n-2}{4} \right\rfloor = 8$

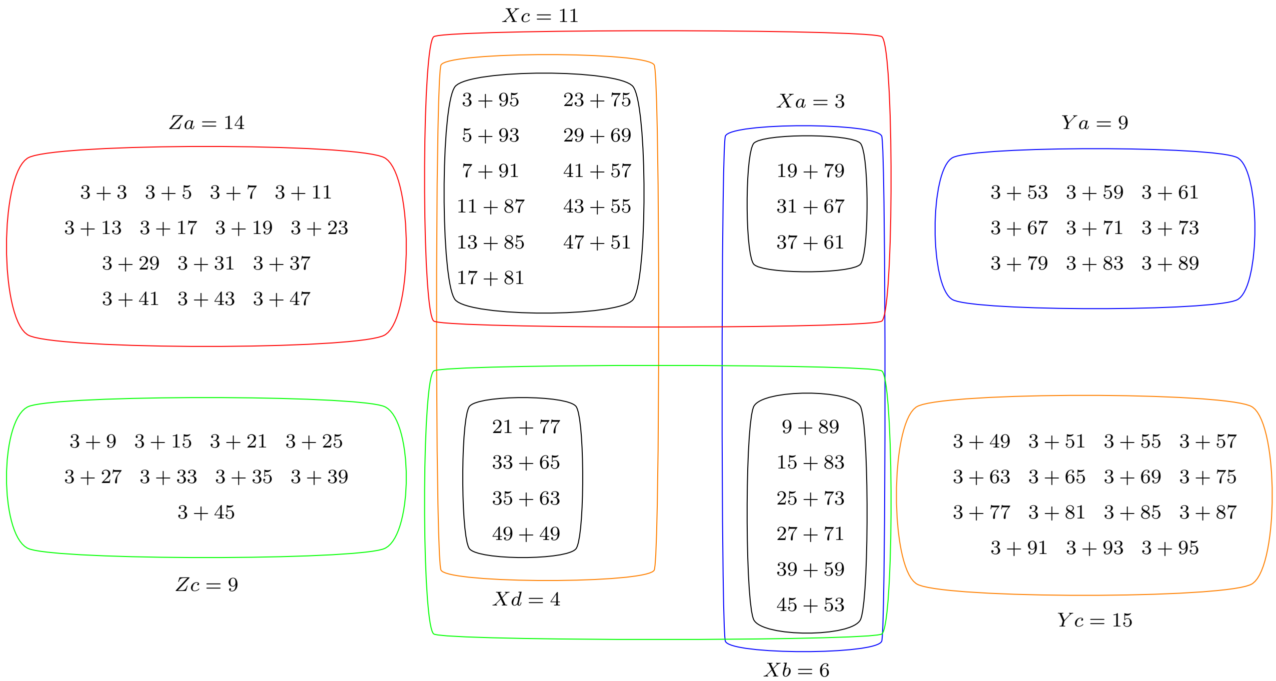
$X_a = 4$

$X_b = 1$

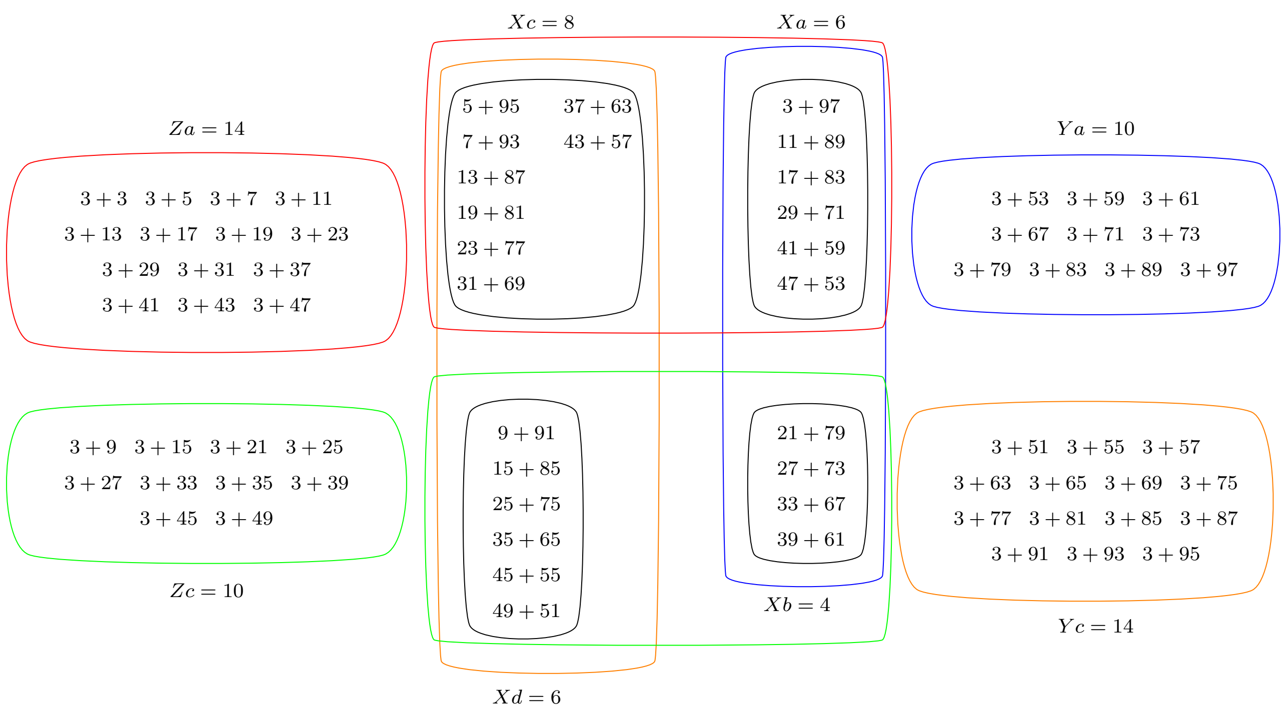
$X_c = 2$

$X_d = 1$

- **Cas** $n = 98$



- **Cas** $n = 100$



Annexe 3 : Règles de réécriture et théorie des automates

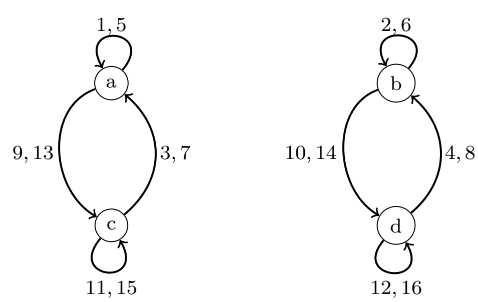
Cette annexe étudie l'évolution des variables $X_a(n), X_b(n), X_c(n), X_d(n)$ que l'on déduit de l'analyse des règles de réécriture des mots, présentées du point de vue de la théorie des automates.

Si on considère chaque ligne du tableau comme un mot sur l'alphabet $A = \{a, b, c, d\}$, le mot du nombre pair $n+2$ s'obtient de la façon suivante à partir du mot de n :

- la première lettre du mot de $n+2$ est a si $n-3$ est premier et c sinon (cette première lettre est la seule qui introduit de l'indéterminisme car elle n'appartient pas au mot de n ou ne se déduit pas des lettres de ce dernier) ;
- les lettres suivantes du mot de $n+2$ sont obtenues par réécriture du mot de n selon les règles ci-dessous :

$$
\begin{array}{lr}
aa \rightarrow a & (1) \\
ab \rightarrow b & (2) \\
ac \rightarrow a & (3) \\
ad \rightarrow b & (4) \\
ba \rightarrow a & (5) \\
bb \rightarrow b & (6) \\
bc \rightarrow a & (7) \\
bd \rightarrow b & (8) \\
ca \rightarrow c & (9) \\
cb \rightarrow d & (10) \\
cc \rightarrow c & (11) \\
cd \rightarrow d & (12) \\
da \rightarrow c & (13) \\
db \rightarrow d & (14) \\
dc \rightarrow c & (15) \\
dd \rightarrow d & (16)
\end{array}
$$

On peut représenter ces règles de réécriture par les deux automates déterministes suivants, dont les arcs sont étiquetés par les règles applicables à une lettre donnée du mot de n :



- enfin, la concaténation d'une lettre en fin de mot, dans le cas où n est un double de pair (i.e. de la forme $4k$) obéit à la règle suivante :
  - si le mot de n a a ou b comme dernière lettre, après avoir obtenu le mot de $n+2$ en appliquant les règles de réécriture, on lui concatène la lettre a ;
  - si le mot de n a c ou d comme dernière lettre, après avoir obtenu le mot de $n+2$ en appliquant les règles de réécriture, on lui concatène la lettre d.

Si on prend comme convention de noter $X_{xy}(n)$ le nombre d'occurences de la séquence de lettres xy dans le mot de n, les égalités suivantes fournissent l'évolution des nombres de lettres a, b, c ou d lors du passage du mot de n au mot de $n+2$.

$$
\begin{aligned}
X_a(n+2) &= X_a(n) - X_{ca}(n) - X_{da}(n) + X_{ac}(n) + X_{bc}(n) + \delta_{n-3\_est\_premier}(n) + \delta_a(n) \\
X_b(n+2) &= X_b(n) - X_{cb}(n) - X_{db}(n) + X_{ad}(n) + X_{bd}(n) + \delta_{n-3\_est\_premier}(n) \\
X_c(n+2) &= X_c(n) - X_{ac}(n) - X_{bc}(n) + X_{ca}(n) + X_{da}(n) + \delta_{n-3\_est\_premier}(n) \\
X_d(n+2) &= X_d(n) - X_{ad}(n) - X_{bd}(n) + X_{cb}(n) + X_{db}(n) + \delta_{n-3\_est\_premier}(n) + \delta_d(n)
\end{aligned}
$$

avec $\delta_a(n)$ qui vaut 1 si n est un double de pair (i.e. de la forme $4k$) et si la dernière lettre du mot de n est une lettre a ou b, $\delta_d(n)$ qui vaut 1 si n est un double de pair (i.e. de la forme $4k$) et si la dernière lettre du mot de n est une lettre c ou d et enfin $\delta_{n-3}(n)$ qui vaut 1 si $n-3$ est premier et 0 sinon.

Bibliographie

[1] J. Barkley Rosser, Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois Journal of Mathematics, 1962.

Conjecture de Goldbach et langage à 4 lettres

Denise Vella-Chemla

18/4/14

1 Introduction

La conjecture de Goldbach stipule que tout nombre pair sauf 2 est la somme de deux nombres premiers. Dans la suite, on s'intéresse aux décompositions d'un nombre pair n en somme de deux nombres impairs $p+q$ avec $3 \leqslant p \leqslant n/2$, $n/2 \leqslant q \leqslant n-3$ et $p \leqslant q$. On appelle p un *sommant de premier rang* et q un *sommant de second rang* de n.

Rappel historique

Citons Charles-Ange Laisant dans la note intitulée *Sur un procédé expérimental de vérification de la conjecture de Goldbach* du Bulletin de la SMF n°25 de 1897.

> *Ce fameux théorème empirique : Tout nombre pair est la somme de deux nombres premiers, dont la démonstration semble dépasser les possibilités scientifiques actuelles, a fait l'objet de nombreux travaux et de certaines contestations. Lionnet a tenté d'établir que la proposition devait probablement être inexacte. M. Georg Cantor l'a vérifiée numériquement jusqu'à 1000, en donnant pour chaque nombre pair toutes les décompositions en deux nombres premiers, et il a remarqué que le nombre de ces décompositions ne cesse de croître en moyenne, tout en présentant de grandes irrégularités.*
>
> *Voici un procédé qui permettrait de faire sans calcul la vérification expérimentale dont il s'agit, et d'avoir pour chaque nombre pair, à la seule inspection d'une figure, toutes les décompositions. Supposons que sur une bande formée de carrés accolés, représentant les nombres impairs successifs, on ait construit le crible d'Erathostène, en ombrant les nombres composés, jusqu'à une limite quelconque* $2n-1$.

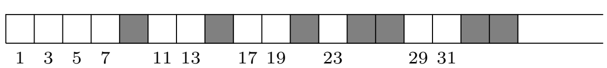


FIGURE 1

> *Si l'on a construit deux réglettes pareilles, et si l'on place la seconde au-dessous de la première en la retournant et en faisant correspondre la case 1 à* $2n$*, *il est évident que si le théorème de Goldbach est vrai pour* $2n$*, il y aura quelque part deux cases blanches en correspondance ; et tous les couples de cases blanches donneront les diverses décompositions. On les aura même en lisant la moitié de la figure, à cause de la symétrie par rapport au milieu. Ainsi la vérification relative au nombre* 28 *donnera la figure 2 et montrera qu'on a les décompositions* $28 = 5+23 = 11+17$.

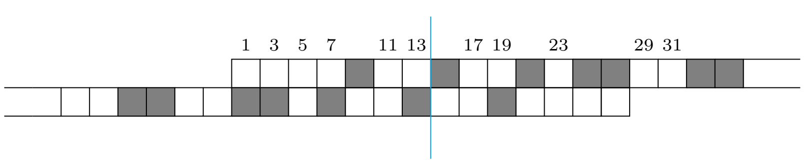


FIGURE 2

*. Ici devrait être écrit $2n-1$.

On comprend que les réglettes étant construites à l'avance, et un simple glissement permettant de passer d'un nombre à un autre, les vérifications sont très rapides.

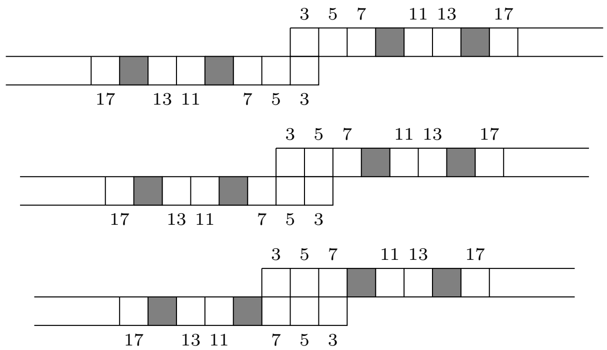


FIGURE 3

Notations :
On notera par :

- a : une décomposition de n de la forme $p+q$ avec p et q premiers ;
- b : une décomposition de n de la forme $p+q$ avec p composé et q premier ;
- c : une décomposition de n de la forme $p+q$ avec p premier et q composé ;
- d : une décomposition de n de la forme $p+q$ avec p et q composés.

Exemple :

40	3	5	7	9	11	13	15	17	19
	37	35	33	31	29	27	25	23	21
l_{40}	a	c	c	b	a	c	d	a	c

2 Le tableau principal

On désigne par $T = (L, C) = (l_{n,m})$ le tableau dont les éléments $l_{n,m}$ sont l'une des lettres a, b, c, d. L'indice n appartient à l'ensemble L des nombres pairs supérieurs ou égaux à 6. L'indice m, appartenant à l'ensemble C des nombres impairs supérieurs ou égaux à 3, est un élément de la liste des sommants de n de premier rang.

Considérons la fonction g définie ainsi :

$$g : \begin{array}{ccc} 2\mathbb{N} & \to & 2\mathbb{N}+1 \\ x & \mapsto & 2\left\lfloor \dfrac{x-2}{4} \right\rfloor + 1 \end{array}$$

$g(6) = 3, g(8) = 3, g(10) = 5, g(12) = 5, g(14) = 7, g(16) = 7, etc.$

La fonction $g(n)$ définit le plus grand des sommants de second rang associés à n.

Comme l'on ne prend en compte que les décompositions de n de la forme $p+q$ où $p \leqslant q$, seules apparaîtront dans le tableau les lettres $l_{n,m}$ telles que $m \leqslant 2\left\lfloor \dfrac{n-2}{4} \right\rfloor + 1$ de sorte que le tableau contient les éléments suivants : $l_{6,3}, l_{8,3}, l_{10,3}, l_{10,5}, l_{12,3}, l_{12,5}, l_{14,3}, l_{14,5}, l_{14,7}, etc.$

Voici le début du tableau.

C / L	3	5	7	9	11	13	15	17
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
...								

FIGURE 4 : mots des nombres pairs de 6 à 36

Remarques :

1) les mots situés sur les diagonales du tableau appelés *mots diagonaux* ont leurs lettres soit dans l'alphabet $A_{ab} = \{a, b\}$ soit dans l'alphabet $A_{cd} = \{c, d\}$.

2) un mot diagonal code des décompositions de même sommant de second rang.

Par exemple, sur la Figure 4, les lettres de la diagonale *aaabaa* qui commence à la lettre $l_{26,3} = a$ code les décompositions $3 + 23, 5 + 23, 7 + 23, 9 + 23, 11 + 23$ et $13 + 23$.

3) Désignons par l_n la ligne dont les éléments sont les $l_{n,m}$. La ligne l_n possède $\left\lfloor \dfrac{n-2}{4} \right\rfloor$ éléments.

4) n étant fixé, appelons $C_{n,3}$ la colonne formée des $l_{k,3}$ pour $6 \leqslant k \leqslant n$.

Dans cette colonne $C_{n,3}$, distinguons deux parties, la "partie haute" et la "partie basse" de la colonne.

Notons $H_{n,3}$ la "partie haute" de la colonne, i.e. l'ensemble des $l_{k,3}$ où $6 \leqslant k \leqslant \left\lfloor \dfrac{n+4}{2} \right\rfloor$.

Notons $B_{n,3}$ la "partie basse" de la colonne, i.e. l'ensemble des $l_{k,3}$ où $\left\lfloor \dfrac{n+4}{2} \right\rfloor < k \leqslant n$.

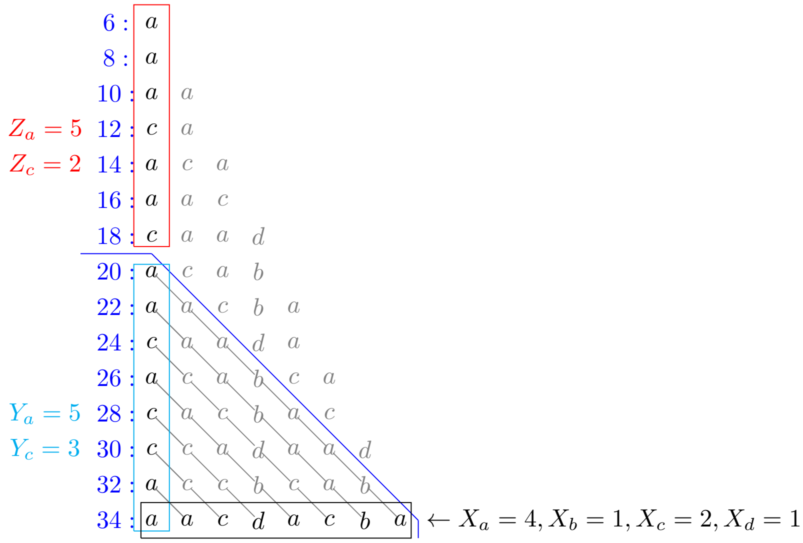


FIGURE 5 : $n = 34$

Pour mieux cerner les dénombrements de la section suivante, on utilisera la projection P de la ligne n sur la partie basse de la première colonne $B_{n,3}$ qui "associe" les lettres aux deux bouts d'une diagonale. Si on considère l'application *proj* telle que $proj(a) = proj(b) = a$ et $proj(c) = proj(d) = c$ alors, puisque 3 est premier, $proj(l_{n,2k+1}) = l_{n-2k+2,3}$.

3 Dénombrement

1) On note dans la ligne n par :

- $X_a(n)$ le nombre de décompositions de n de la forme *premier* + *premier* ;
- $X_b(n)$ le nombre de décompositions de n de la forme *composé* + *premier* ;
- $X_c(n)$ le nombre de décompositions de n de la forme *premier* + *composé* ;
- $X_d(n)$ le nombre de décompositions de n de la forme *composé* + *composé*.

$X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$ est le nombre d'éléments de la ligne de n.
Exemple : $n = 34$:
$X_a(34) = \#\{3+31, 5+29, 11+23, 17+17\} = 4$
$X_b(34) = \#\{15+19\} = 1$.
$X_c(34) = \#\{7+27, 13+21\} = 2$
$X_d(34) = \#\{9+25\} = 1$

2) Soit $Y_a(n)$ (resp. $Y_c(n)$) le nombre de a (resp. c) qui apparaissent dans $B_{n,3}$. On rappelle qu'il n'y a que des lettres a et c dans la première colonne car elle contient les lettres associées aux décompositions de la forme $3 + x$ et que 3 est premier.

Exemple :

- $Y_a(34) = \#\{3+17, 3+19, 3+23, 3+29, 3+31\} = 5$
- $Y_c(34) = \#\{3+21, 3+25, 3+27\} = 3$

3) Compte-tenu de la projection P qui est une bijection, des définitions des lettres a, b, c, d, $Y_a(n) = X_a(n) + X_b(n)$ et $Y_c(n) = X_c(n) + X_d(n)$. Par suite, trivialement, $Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$.

Exemple :

$$\begin{aligned}
Y_a(34) &= \#\{3+17, 3+19, 3+23, 3+29, 3+31\} \\
X_a(34) &= \#\{3+31, 5+29, 11+23, 17+17\} \\
X_b(34) &= \#\{15+19\} \\
\\
Y_c(34) &= \#\{3+21, 3+25, 3+27\} \\
X_c(34) &= \#\{7+27, 13+21\} \\
X_d(34) &= \#\{9+25\}
\end{aligned}$$

4) Soit $Z_a(n)$ (resp. $Z_c(n)$) le nombre de a (resp. c) qui apparaissent dans $H_{n,3}$.

Exemple :

- $Z_a(34) = \#\{3+3, 3+5, 3+7, 3+11, 3+13\} = 5$
- $Z_c(34) = \#\{3+9, 3+15\} = 2$

$Z_a(n) + Z_c(n) = \left\lfloor \dfrac{n-4}{4} \right\rfloor$.

5) On a $Z_a(n) + Z_c(n) + Y_a(n) + Y_c(n) = 2(X_a(n) + X_b(n) + X_c(n) + X_d(n)) - \delta$.

δ vaut 1 si n est un double d'impair et 0 sinon.

En effet, on peut faire correspondre à tout élément $l_{n,m}$ deux éléments : $l_{m,3}$ et $l_{n-m,3}$. Cette assertion est à δ près car dans le cas des doubles d'impairs, ce procédé associe à la décomposition $n/2 + n/2$ la décomposition $3 + n/2$ en double, comme cela se voit bien sur le schéma ensembliste suivant :

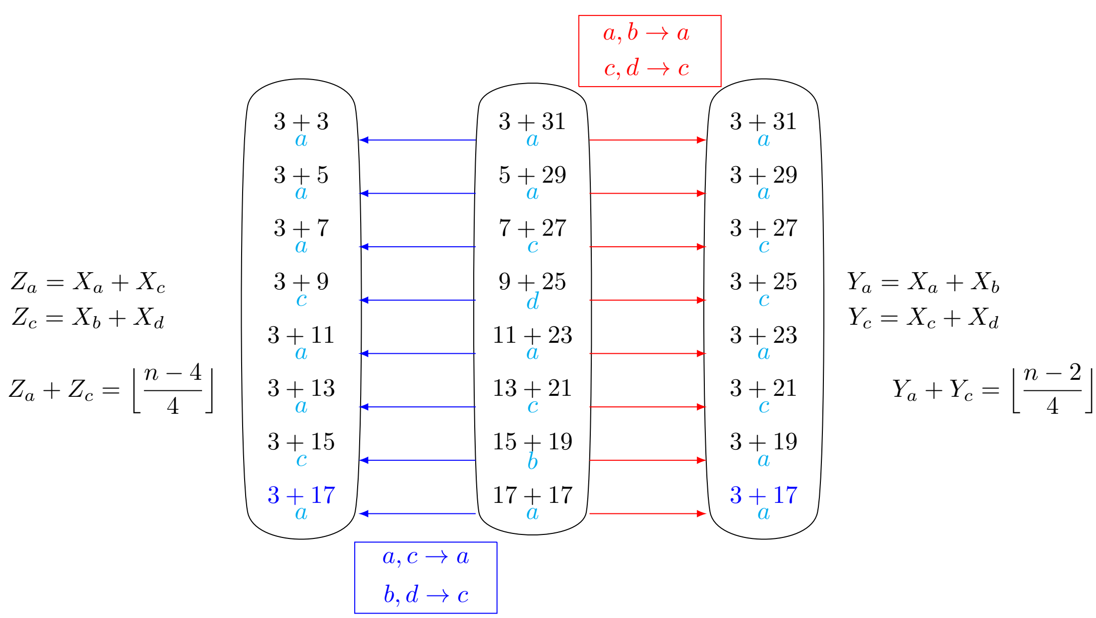


FIGURE 6 : Bijections ensemblistes

Positionner les décompositions triviales de Goldbach sur la droite du plan complexe de partie réelle $\frac{1}{2}$

Denise Vella-Chemla

11/4/14

On aimerait fournir une représentation graphique des décompositions de Goldbach dans le plan complexe qui positionnerait les décompositions dites triviales, i.e. $6 = 3 + 3, 10 = 5 + 5, 14 = 7 + 7, 22 = 11 + 11, \ldots$, sur la droite de partie réelle $\dfrac{1}{2}$.

On aimerait d'autre part trouver une fonction à variable complexe qui permettrait de distinguer les décompositions de Goldbach des nombres pairs (i.e. comme sommes de deux nombres premiers) des autres décompositions.

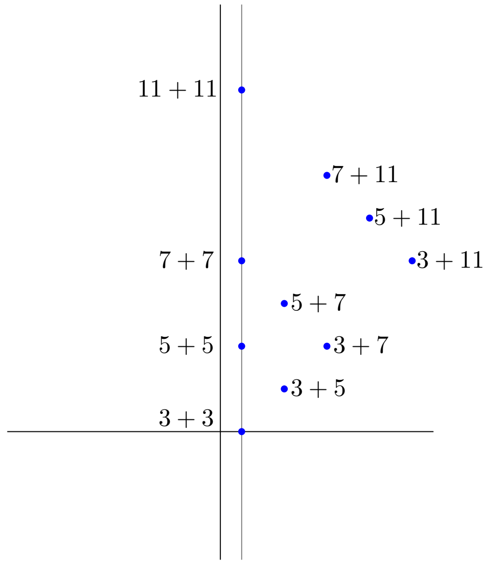
Pour cela, une décomposition $p + q$ est représentée par le point du plan complexe de coordonnées $\left(\dfrac{q-p}{2}+\dfrac{1}{2}\right)$ et $\left(\dfrac{q+p}{2}-3\right)$, correspondant au nombre complexe $\left(\dfrac{q-p}{2}+\dfrac{1}{2}\right)+\left(\dfrac{q+p}{2}-3\right)i$.

On définit une fonction $f(s)$ qui associe au nombre complexe $s = x+iy$ la valeur de $\sigma(x)+\sigma(y)$ où σ est la notation habituellement utilisée pour noter la somme des diviseurs d'un nombre. On impose que $\sigma(k) = \infty$ si k est un réel non entier.

Si la conjecture de Goldbach est vraie, la fonction f prend des valeurs minimales (égales à $n + 2$) pour les points d'un intervalle horizontal de points $x + iy$ tels que $x \in \left[\dfrac{1}{2}, \dfrac{n}{2}-\dfrac{5}{2}\right]$ et $y = \dfrac{n}{2} - 3$.

La fonction $f'(x) = f(x) - x - 2$ admet donc des "zéros" correspondant aux points $x + ix$ qui sont sur la droite de partie réelle $\dfrac{1}{2}$ [*].

[*]. Le seul zéro trivial de f' correspond à la décomposition $6 = 3 + 3$.



On pourrait inversement utiliser la fonction $g(x)$ qui associe au nombre complexe $x+iy$ la valeur de $\varphi(x)\times\varphi(y)$ où φ est la notation habituellement utilisée pour noter le nombre $\varphi(k)$ de nombres k' inférieurs à k et premiers à k (tels que $(k,k')=1$). On étend $\varphi(k)$ aux k qui sont des réels non entiers en imposant que pour eux, $\varphi(k)=0$.

Si la conjecture de Goldbach est vraie, la fonction g prend des valeurs maximales (égales à $(x-1)(n-x-1)$) pour les points $x+iy$ d'un intervalle horizontal tels que $x \in \left[\frac{1}{2}, \frac{n}{2}-\frac{5}{2}\right]$ et $y = \frac{n}{2} - 3$.

Les "pics triviaux" de la fonction g, correspondant aux points $x+ix$, sont sur la droite de partie réelle $\frac{1}{2}$.

Conjecture de Goldbach, réécriture, contradiction

Denise Vella-Chemla

30/3/14

1 16 règles de réécriture

On rappelle qu'on a choisi 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 a également pris comme conventions que ($3 \leqslant p \leqslant n/2$) :

– la lettre a symbolise une décomposition de n de la forme $p+q$ avec p et q premiers ;
– la lettre b symbolise une décomposition de n de la forme $p+q$ avec p composé et q premier ;
– la lettre c symbolise une décomposition de n de la forme $p+q$ avec p premier et q composé ;
– la lettre d symbolise une décomposition de n de la forme $p+q$ avec p et q composés.

La lettre a code la matrice $\begin{pmatrix}0\\0\end{pmatrix}$, et respectivement b $\begin{pmatrix}0\\1\end{pmatrix}$, c $\begin{pmatrix}1\\0\end{pmatrix}$ et enfin d $\begin{pmatrix}1\\1\end{pmatrix}$

Exemple : Ci-dessous le mot $m_{abcd}(40)$.

40	37	35	33	31	29	27	25	23	21
	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0
	3	5	7	9	11	13	15	17	19
$m_{abcd}(40)$	a	c	c	b	a	c	d	a	c

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

$$\begin{pmatrix}x_1\\x_2\end{pmatrix}.\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{pmatrix}x_1\\y_2\end{pmatrix}$$

L'opération ci-dessus fournit 16 règles de réécriture de couples de lettres, 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) $dd \to d$

2 Rappels de théorie des langages

Un alphabet est un ensemble fini de symboles.

Les alphabets utilisés ci-après sont : $A = \{a, b, c, d\}$, $A_{ab} = \{a, b\}$, $A_{cd} = \{c, d\}$, $A_{ac} = \{a, c\}$ et $A_{bd} = \{b, d\}$.

Un mot sur l'alphabet X est une séquence finie et ordonnée, éventuellement vide, d'éléments de l'alphabet. C'est une concaténation de lettres. On note X^* l'ensemble des mots sur l'alphabet X.

Un mot est préfixe d'un autre s'il contient, sur toute sa longueur, les mêmes lettres aux mêmes positions (Soient un alphabet X et $w, u \in X^*$. u est préfixe de w si et seulement si $\exists v \in X^*$ tel que $w = u.v$).

3 Observer les mots

Observons les mots associés aux nombres pairs compris entre 6 et 36.

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

FIGURE 1 : mots des nombres pairs de 6 à 36

4 Propriétés des mots

Les mots diagonaux (diagonales) ont leurs lettres soit dans l'alphabet A_{ab} soit dans l'alphabet A_{cd}.

Toute diagonale est préfixe de la diagonale suivante définie sur le même alphabet.

Une diagonale code en effet des décompositions de même second sommant et de premier sommant un nombre impair de la liste des impairs successifs à partir de 3.

Par exemple, la diagonale *aaaba*, qui commence au a première lettre du mot de 26 sur la figure 1 code les décompositions $3+23, 5+23, 7+23; 9+23, 11+23$ et $13+23$.

Ainsi, les diagonales sur l'alphabet A_{ab} “codent” les décompositions dont le second sommant est premier ; les lettres de telles diagonales codent soit par des a correspondant aux nombres premiers, soit par des b correspondant aux nombres composés la séquence des caractères de primalité des entiers impairs, à partir de 3.

Les diagonales sur l'alphabet A_{cd} “codent” quant à elles des décompositions dont le second sommant est composé ; les lettres de telles diagonales codent soit par des c correspondant aux nombres premiers, soit par des d correspondant aux nombres composés la séquence des caractères de primalité des entiers impairs, à partir de 3.

Les mots verticaux ont leurs lettres soit dans l'alphabet A_{ac} soit dans l'alphabet A_{bd}. Un mot vertical code des décompositions successives en somme de deux impairs de même premier sommant. Tout mot vertical est contenu dans un mot vertical qui se trouve à sa gauche et qui est défini sur le même alphabet.

5 Quelques régularités

On observe quelques régularités facilement explicables, qui lient entre eux les nombres de lettres de chaque sorte apparaissant dans un mot et dans une portion de la colonne des premières lettres. La figure 2 ci-dessous présente schématiquement les noms des variables qui seront utiles au raisonnement :

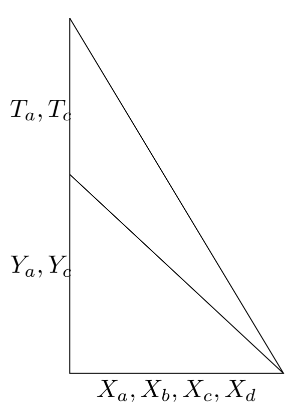


FIGURE 2 : variables liées

Le triangle global contient les mots associés aux nombres pairs de 6 à n.

X_a, X_b, X_c et X_d comptent le nombre de a, b, c ou d du mot associé à n.

T_a et T_c comptent le nombre de lettres a ou c qui sont premières lettres des mots associés aux nombres pairs compris entre 6 et $2\left\lceil \dfrac{n+2}{4} \right\rceil$.

T_a correspond ainsi aux décompositions de la forme $n' = 3 + p_i$, p_i premier, $n' \leqslant 2\left\lceil \dfrac{n+2}{4} \right\rceil$. Par exemple, pour $n = 34$, $T_a = \#\{3{+}3, 3{+}5, 3{+}7, 3{+}11, 3{+}13\}$.

T_c correspond aux décompositions de la forme $n' = 3 + c_i$, c_i composé pour $n' \leqslant 2\left\lceil \dfrac{n+2}{4} \right\rceil$. Par exemple, pour $n = 34$, $T_c = \#\{3 + 9, 3 + 15\}$.

Y_a et Y_c comptent le nombre de lettres a ou c qui sont premières lettres de mots associés aux nombres pairs compris entre $2\left\lceil \dfrac{n+2}{4} \right\rceil + 2$ et n.

La bijection triviale sur le deuxième sommant des décompositions permet d'expliquer aisément pourquoi $Y_a = X_a + X_b$ ou bien pourquoi $Y_c = X_c + X_d$. La simple présentation des ensembles en extension suffit à s'en convaincre.

$$
\begin{aligned}
Y_a &= \#\{3 + 17, 3 + 19, 3 + 23, 3 + 29, 3 + 31\}\\
X_a &= \#\{3 + 31, 5 + 29, 11 + 23, 17 + 17\}\\
X_b &= \#\{15 + 19\}\\
\\
Y_c &= \#\{3 + 21, 3 + 25, 3 + 27\}\\
X_c &= \#\{7 + 27, 13 + 21\}\\
X_d &= \#\{9 + 25\}
\end{aligned}
$$

Ci-après deux figures permettant de "fixer les idées" pour les nombres pairs $n = 32$ ou $n = 34$.

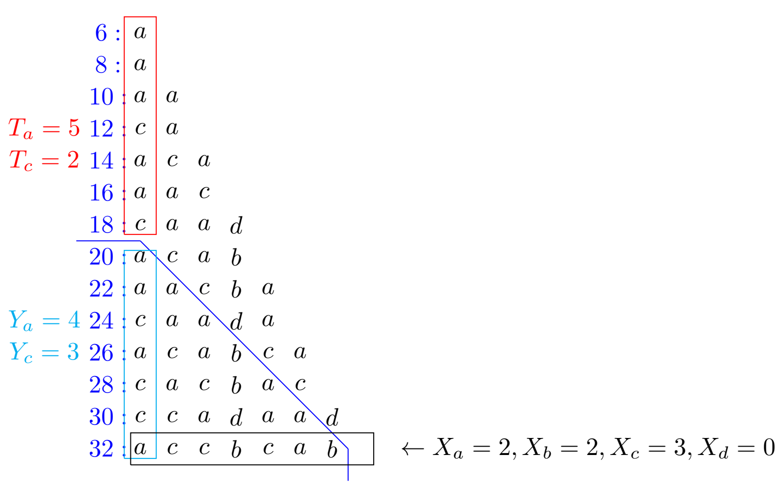


FIGURE 3 : premier exemple : $n = 32$

	6 :	a								
	8 :	a								
	10 :	a	a							
$T_a = 5$	12 :	c	a							
$T_c = 2$	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			
$Y_a = 5$	28 :	c	a	c	b	a	c			
$Y_c = 3$	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	$\leftarrow X_a = 4, X_b = 1, X_c = 2, X_d = 1$

Figure 4 : second exemple : $n = 34$

Les contraintes suivantes sont toujours vérifiées :

$$\begin{aligned} &Y_a = X_a + X_b \\ &Y_c = X_c + X_d \\ &T_a + T_c + Y_a + Y_c + \epsilon = 2(X_a + X_b + X_c + X_d) \end{aligned}$$

$\epsilon = 1$ si n est un double d'impair, $\epsilon = 0$ sinon.

On a vu que les contraintes ci-dessus peuvent être aisément comprises si l'on revient aux nombres de décompositions qu'elles représentent et si l'on utilise des bijections “à la Cantor”.

Les lettres des différents mots sont ainsi très *intriquées* et ces intrications ont pour conséquence que tout mot contient un a. On va prouver cela en menant un raisonnement par l'absurde dans la section 7.

6 Visualisation des bijections de Cantor

Ci-dessous, on visualise les bijections de Cantor pour les cas $n = 32$ et $n = 34$.

La bijection f qui permet de passer de la ligne 2 du tableau à la ligne 1 est telle que $f(a) = f(c) = a$ et $f(b) = f(d) = c$.

La bijection g qui permet de passer de la ligne 2 du tableau à la ligne 3 est telle que $g(a) = g(b) = a$ et $g(c) = g(d) = c$.

C'est la duplication de la décomposition $3 + n/2$ dans le cas des doubles d'impairs qui nécessite l'introduction de la variable ϵ qui vaut alors 1 et 0 sinon.

– Bijections pour $n = 32$

	3	3	3	3	3	3	3
1	a	a	a	c	a	a	c
	3	5	7	9	11	13	15
	3	5	7	9	11	13	15
2	a	c	c	b	c	a	b
	29	27	25	23	21	19	17
	29	27	25	23	21	19	17
3	a	c	c	a	c	a	a
	3	3	3	3	3	3	3

– Bijections pour $n = 34$

	3	3	3	3	3	3	3	3
1	a	a	a	c	a	a	c	a
	3	5	7	9	11	13	15	17
	3	5	7	9	11	13	15	17
2	a	a	c	d	a	c	b	a
	31	29	27	25	23	21	19	17
	31	29	27	25	23	21	19	17
3	a	a	c	c	a	c	a	a
	3	3	3	3	3	3	3	3

7 Rechercher une contradiction

Imaginons que le mot m_n est associé à un nombre n qui contredit la conjecture de Goldbach, i.e. m_n ne contient aucune lettre a, la lettre a symbolisant on le rappelle la somme de deux nombres premiers.

m_n ne contenant aucune lettre a, on a $X_a = 0$. Mais puisque $Y_a = X_a + X_b$, on a alors $Y_a = X_b$. En identifiant Y_a à X_b et Y_c à $X_c + X_d$ dans la dernière contrainte toujours respectée fournie au paragraphe précédent, on obtient la suite d'égalités suivante :

$$\begin{aligned}
T_a + T_c + Y_a + Y_c + \epsilon &= 2(X_a + X_b + X_c + X_d) \\
T_a + T_c + X_b + X_c + X_d + \epsilon &= 2X_a + 2X_b + 2X_c + 2X_d \\
T_a + T_c + \epsilon &= X_b + X_c + X_d \\
T_a + T_c + \epsilon &= X_b + Y_c
\end{aligned}$$

Il s'agit maintenant de se souvenir de ce que représentent ces différentes variables :

– $T_a + T_c = \left\lfloor \dfrac{n-4}{4} \right\rfloor$;

– X_b compte le nombre de décompositions de n sous la forme d'une somme de deux nombres impairs $p + q$ avec $p \leqslant n/2$ composé et q premier ;

– Y_c compte le nombre de nombres composés impairs compris entre $n/2$ et $n - 3$.

Le nombre X_b de décompositions de n sous la forme d'une somme de deux nombres impairs $p + q$ avec $p \leqslant n/2$ composé et q premier étant forcément inférieur au nombre de nombres premiers compris entre $n/2$ et $n-3$, on a $X_b < Y_a$ (on a utilisé ici une sorte de "principe des tiroirs" inversé : si on met 0 ou 1 objet dans k tiroirs, on ne peut avoir plus d'objets que de tiroirs, i.e. plus de k objets). Mais le nombre de nombres premiers contenus dans un intervalle $[2k+3, 4k+1]$ est toujours inférieur au nombre de nombres composés impairs contenus dans cet intervalle pour $k > 25$. Dans ces cas, $Y_a < Y_c$ et $X_b + Y_c < Y_a + Y_c < 2Y_c$.

Or $\left\lfloor \dfrac{n-4}{4} \right\rfloor$ est pour tout entier supérieur à un certain entier assez petit (tel que 100) supérieur à $2Y_c$. Cela assure qu'on a jamais l'égalité $T_a + T_c + \epsilon = X_b + Y_c$ qui découlerait de l'absence de lettre a dans un mot.

On a ainsi abouti à une contradiction qui serait conséquence de l'absence de a dans un mot. Cela entraîne l'impossibilité qu'un nombre pair contredise la conjecture de Goldbach. Les règles de réécriture intriquent totalement les lettres des mots de telle manière que les nombres de lettres de chaque sorte doivent respecter impérativement certaines contraintes. On se situe dans une théorie lexicale des nombres, selon laquelle les nombres sont des mots. Cette théorie exploite le fait que l'ordre des lettres dans les mots de Goldbach est primordial.

Goldbach conjecture, 4 letters language, variables and invariants

Denise Vella-Chemla

21/04/2014

1 Introduction

Goldbach conjecture states that each even integer except 2 is the sum of two prime numbers. In the following, one is interested in decompositions of an even number n as a sum of two odd integers $p+q$ with $3 \leqslant p \leqslant n/2$, $n/2 \leqslant q \leqslant n-3$ and $p \leqslant q$. We call p a *n's first range sommant* and q a *n's second range sommant.*

Notations :

We will note by :

- a : an n decomposition of the form $p+q$ with p and q primes ;
- b : an n decomposition of the form $p+q$ with p compound and q prime ;
- c : an n decomposition of the form $p+q$ with p prime and q compound ;
- d : an n decomposition of the form $p+q$ with p and q compound numbers.

Example :

40	3	5	7	9	11	13	15	17	19
	37	35	33	31	29	27	25	23	21
l_{40}	a	c	c	b	a	c	d	a	c

2 Main array

We designate by $T = (L, C) = (\ l_{n,m}\ )$ the array containing $l_{n,m}$ elements that are one of a, b, c, d letters. n belongs to the set of even integers greater than or equal to 6. m, belonging to the set of odd integers greater than or equal to 3, is an element of list of n first range sommants.

Let us consider g function defined by :

$$\begin{array}{rccl} g: & 2\mathbb{N} & \rightarrow & 2\mathbb{N}+1 \\ & x & \mapsto & 2\left\lfloor \dfrac{x-2}{4} \right\rfloor + 1 \end{array}$$

$g(6) = 3, g(8) = 3, g(10) = 5, g(12) = 5, g(14) = 7, g(16) = 7, etc.$

$g(n)$ function defines the greatest of n second range sommants.

As we only consider n decompositions of the form $p+q$ where $p \leqslant q$, in T will only appear letters $l_{n,m}$ such that $m \leqslant 2\left\lfloor \dfrac{n-2}{4} \right\rfloor + 1$ in such a way that the T array first letters are : $l_{6,3}, l_{8,3}, l_{10,3}, l_{10,5}, l_{12,3}, l_{12,5}, l_{14,3}, l_{14,5}, l_{14,7}, etc.$

Here are first lines of array T.

L \ C	3	5	7	9	11	13	15	17
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
...								

FIGURE 1 : words of even numbers between 6 and 36

Remarks :

1) words on array's diagonals called *diagonal words* have their letters either in $A_{ab} = \{a, b\}$ alphabet or in $A_{cd} = \{c, d\}$ alphabet.

2) a diagonal word codes decompositions that have the same second range sommant.
For instance, on Figure 4, diagonal letters *aaabaa* that begin at letter $l_{26,3} = a$ code decompositions $3 + 23, 5 + 23, 7 + 23, 9 + 23, 11 + 23$ and $13 + 23$.

3) let us designate by l_n the line whose elements are $l_{n,m}$. Line l_n contains $\left\lfloor \dfrac{n-2}{4} \right\rfloor$ elements.

4) n begin fixed, let us call $C_{n,3}$ the column formed by $l_{k,3}$ for $6 \leqslant k \leqslant n$.

In this column $C_{n,3}$, let us distinguish two parts, the "top part" and the "bottom part" of the column.

Let us call $H_{n,3}$ column's "top part", i.e. set of $l_{k,3}$ where $6 \leqslant k \leqslant \left\lfloor \dfrac{n+4}{2} \right\rfloor$.

Let us call $B_{n,3}$ column's "bottom part", i.e. set of $l_{k,3}$ where $\left\lfloor \dfrac{n+4}{2} \right\rfloor < k \leqslant n$.

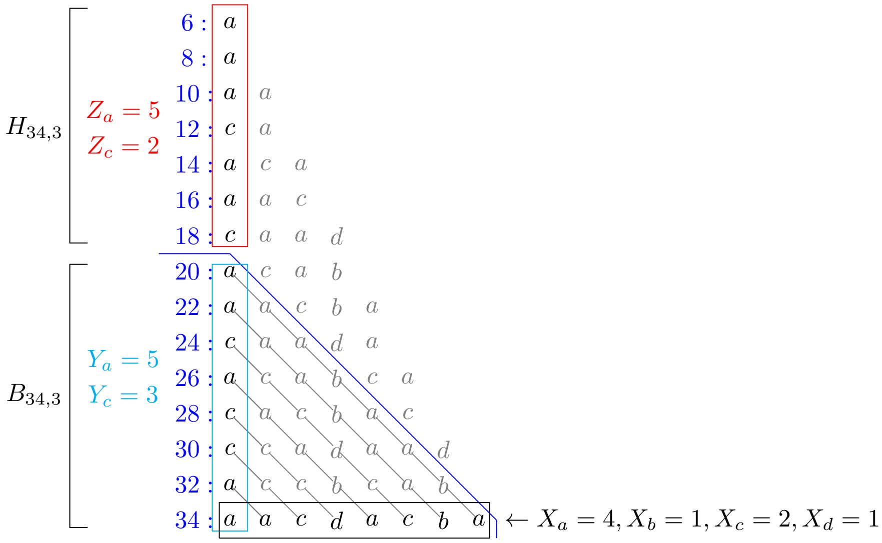


FIGURE 2 : $n = 34$

To better understand computations in next section, we will use projection P of line n on bottom part of first column $B_{n,3}$ that "associates" letters at both extremities of a diagonal. If we consider application $proj$ such that $proj(a) = proj(b) = a$ and $proj(c) = proj(d) = c$ then, since 3 is prime, $proj(l_{n,2k+1}) = l_{n-2k+2,3}$.

We can also understand the effect of this projection (that preserves second range sommant) by analyzing decompositions :

- if $p + q$ is coded by an a or a b letter, it corresponds to two possible cases in which q is prime, and so $3 + q$ decomposition, containing two prime numbers will be coded by an a letter ;
- if $p + q$ is coded by a c or a d letter, it corresponds to two possible cases in which q is compound, and so $3 + q$ decomposition, of the form $prime + compound$ will be coded by a c letter.

We will also use in next section a projection that transforms first range sommant in a second range sommant that is combined with 3 as a first range sommant ; let us analyze the effect of such a projection will have on decompositions :

- if $p + q$ is coded by an a or a c letter, it corresponds to two possible cases in which p is prime, and so $3 + p$ decomposition, containing two prime numbers will be coded by a a letter ;
- if $p + q$ is coded by a b or a d letter, it corresponds to two possible cases in which p is compound, and so $3 + p$ decomposition, of the form $prime + compound$ will be coded by a c letter.

3 Computations

1) We note in line n by :

- $X_a(n)$ the number of n decompositions of the form $prime + prime$;
- $X_b(n)$ the number of n decompositions of the form $compound + prime$;
- $X_c(n)$ the number of n decompositions of the form $prime + compound$;
- $X_d(n)$ the number of n decompositions of the form $compound + compound$.

$X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$ is the number of elements of line n.

Example : $n = 34$:
$X_a(34) = \#\{3+31, 5+29, 11+23, 17+17\} = 4$
$X_b(34) = \#\{15+19\} = 1.$
$X_c(34) = \#\{7+27, 13+21\} = 2$
$X_d(34) = \#\{9+25\} = 1$

2) Let $Y_a(n)$ (resp. $Y_c(n)$) being the number of a letters (resp. c) that appear in $B_{n,3}$. We recall that there are only a and c letters in first column because it contains letters associated with decompositions of the form $3+x$ and because 3 is prime.

Example :

- $Y_a(34) = \#\{3+17, 3+19, 3+23, 3+29, 3+31\} = 5$
- $Y_c(34) = \#\{3+21, 3+25, 3+27\} = 3$

3) Because of P projection that is a bijection, and because of a, b, c, d letters definitions, $Y_a(n) = X_a(n) + X_b(n)$ and $Y_c(n) = X_c(n) + X_d(n)$. Thus, trivially, $Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$.

Example :

$$\begin{aligned}
Y_a(34) &= \#\{3+17, 3+19, 3+23, 3+29, 3+31\} \\
X_a(34) &= \#\{3+31, 5+29, 11+23, 17+17\} \\
X_b(34) &= \#\{15+19\} \\
\\
Y_c(34) &= \#\{3+21, 3+25, 3+27\} \\
X_c(34) &= \#\{7+27, 13+21\} \\
X_d(34) &= \#\{9+25\}
\end{aligned}$$

4) Let $Z_a(n)$ (resp. $Z_c(n)$) being the number of a letters (resp. c) that appear in $H_{n,3}$.

Example :

- $Z_a(34) = \#\{3+3, 3+5, 3+7, 3+11, 3+13\} = 5$
- $Z_c(34) = \#\{3+9, 3+15\} = 2$

$Z_a(n) + Z_c(n) = \left\lfloor \dfrac{n-4}{4} \right\rfloor$.

Reminding identified properties

$$Y_a(n) = X_a(n) + X_b(n) \tag{1}$$

$$Y_c(n) = X_c(n) + X_d(n) \tag{2}$$

$$Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

$$Z_a(n) + Z_c(n) = \left\lfloor \frac{n-4}{4} \right\rfloor \tag{4}$$

Let us add two new properties to those ones :

$$X_a(n) + X_c(n) = Z_a(n) + \delta_{2p} \tag{5}$$

with δ_{2p} equal to 1 in the case that n is the double of a prime number and equal to 0 either.

$$X_b(n) + X_d(n) = Z_c(n) + \delta_{spec} \tag{6}$$

with δ_{spec} equal to 0 in the case that there exists k such that $n = 4k$, or in the case that n is the double of a prime number, and equal to 1 either.

4 Variables evolution

In this section, let us study how different variables change, in the aim to deduce that X_a (the number of an even number decompositions that are sums of two primes) can't never be null.

$Z_a(n)+Z_c(n) = \left\lfloor \dfrac{n-4}{4} \right\rfloor$ is an increasing function of n, it is increased by 1 at each n that is an even double.

$Z_a(n)$ is increased by 1 when $\dfrac{n-2}{2}$ is prime and $Z_c(n)$ is increased by 1 each time when $\dfrac{n-2}{2}$ is compound.

$Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$ is an increasing function of n, it is increased by 1 each time when n is an odd number double.

Let us see now in detail how $Y_a(n)$ and $Y_c(n)$ change.

Dans le cas où n est un double d'impair, on ajoute un nombre à l'intervalle $H_{n,3}$; si ce nombre $(n-3)$ est premier (resp. composé), $Y_a(n)$ (resp. $Y_c(n)$) est augmenté de 1 par rapport à $Y_a(n-2)$ (resp. $Y_c(n-2)$).

If n is an even number double, there are 4 possible cases. Let us study how top decompositions belonging to $C_{n,3}$'s top part (i.e. $H_{n,3}$) evoluate.

- if $n-3$ and $n/2-1$ are both primes, we remove at bottom and add at top of $H_{n,3}$ two letters that are of the same type, thus $Y_a(n)$ and $Y_c(n)$ remain constant ;
- if $n-3$ is prime and $n/2-1$ is compound then $Y_a(n)$ is increased by 1 and $Y_c(n)$ is decreased by 1 ;
- if $n-3$ is compound and $n/2-1$ is prime then $Y_c(n)$ is increased by 1 and $Y_a(n)$ is decreased by 1 ;
- if $n-3$ and $n/2-1$ are both compound, we remove at bottom and add at top of $H_{n,3}$ two letters that are of the same type thus $Y_a(n)$ and $Y_c(n)$ remain constants.

But we don't succeed in deducing from all those variables entanglement that $X_a(n)$ is always strictly positive. In annex 1 are provided in an array values of different variables for n between 14 and 100.

5 Leading to a contradiction

However, let us try to reach a contradiction from the hypothesis that $X_a(n) = 0$.

If $X_a(n) = 0$, we have

$$X_b(n) + X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

This is equivalent to

$$X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor - X_b(n)$$

and thus, because of (2), to

$$Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor - X_b(n) \tag{7}$$

Here, 2 cases have to be distinguished :

– *case 1* : If n is the double of an odd number (i.e. of the form $4k+2$), then

$$\left\lfloor \frac{n-2}{4} \right\rfloor = \left\lfloor \frac{n-4}{4} \right\rfloor + 1 \tag{a}$$

– *case 2* : If n is the double of an even number (i.e. of the form $4k$), then

$$\left\lfloor \frac{n-2}{4} \right\rfloor = \left\lfloor \frac{n-4}{4} \right\rfloor \tag{b}$$

We replace $\left\lfloor \frac{n-2}{4} \right\rfloor$ by those two values in equality (7) above ; we obtain :

– *case 1* : $$Y_c(n) = \left\lfloor \frac{n-4}{4} \right\rfloor + 1 - X_b(n) \tag{7a}$$

– *case 2* : $$Y_c(n) = \left\lfloor \frac{n-4}{4} \right\rfloor - X_b(n) \tag{7b}$$

On the other part, from the hypothesis $X_a(n) = 0$ and from $X_a(n) + X_c(n) = Z_a(n) + \delta_{2p}$ (5), it results that

$$X_c(n) = Z_a(n) + \delta_{2p} \tag{8}$$

We rewrite (2) in

$$X_c(n) = Y_c(n) - X_d(n) \tag{2'}$$

By identifying $X_c(n)$ in both (2') and (8), we obtain

$$Z_a(n) + \delta_{2p} = Y_c(n) - X_d(n) \tag{9'}$$

from which results

$$Y_c(n) = Z_a(n) + \delta_{2p} + X_d(n) \tag{2'}$$

that we rewrite

$$X_d(n) = Y_c(n) - Z_a(n) - \delta_{2p} \tag{9''}$$

From two equations (9') and (2) system :

$$\begin{cases} X_d(n) & = & Y_c(n) - Z_a(n) - \delta_{2p} \\ Y_c(n) & = & X_c(n) + X_d(n) \end{cases}$$

results

$$X_c(n) = Z_a(n) + \delta_{2p} - Y_c(n) \tag{10}$$

Contradiction results from the fact that $Y_c(n)$ is always greater than $Z_c(n)$ (since $n \geqslant 24$), itself always greater than $Z_a(n)$, n being greater than a rather small value of n (since $n \geqslant 240$). Equation (10) that we reached under $X_a(n) = 0$ hypothesis would provide a negative value for $X_c(n)$, that is clearly impossible, $X_c(n)$ counting, let us remind it, n decompositions of the form *prime* + *compound*.

In annex 2 are provided graphic representations of sets bijections for cases $n = 32$, 34, 98 and 100.

The file *http : //denise.vella.chemla.free.fr/annexes.pdf* provides

– an historical recall of a Laisant's note that presented yet in 1897 the idea of "strips" of odd numbers to be put in regard and to be colorated to *see* Goldbach decompositions ;
– a program and its execution that implements ideas presented here.

Annex 1 : variables values array for n between 14 and 100

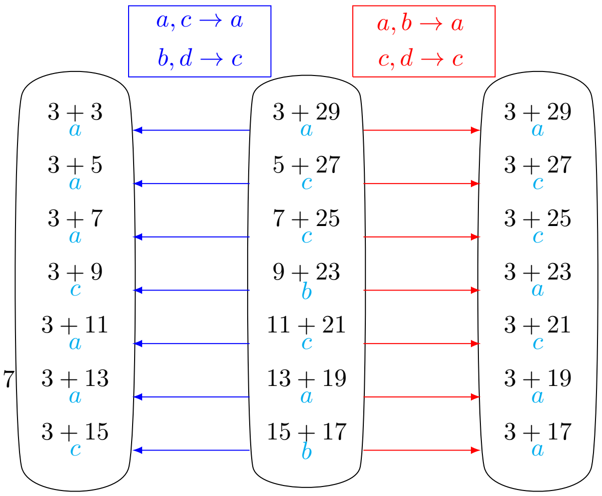
n	$X_a(n)$	$X_b(n)$	$X_c(n)$	$X_d(n)$	$Y_a(n)$	$Y_c(n)$	$\left\lfloor \frac{n-2}{4} \right\rfloor$	$Z_a(n)$	$Z_c(n)$	$\left\lfloor \frac{n-4}{4} \right\rfloor$
14	2	0	1	0	2	1	3	2	0	2
16	2	0	1	0	2	1	3	3	0	3
18	2	0	1	1	2	2	4	3	0	3
20	2	1	1	0	3	1	4	3	1	4
22	3	1	1	0	4	1	5	3	1	4
24	3	0	1	1	3	2	5	4	1	5
26	3	1	2	0	4	2	6	4	1	5
28	2	1	3	0	3	3	6	5	1	6
30	3	0	2	2	3	4	7	5	1	6
32	2	2	3	0	4	3	7	5	2	7
34	4	1	2	1	5	3	8	5	2	7
36	4	0	2	2	4	4	8	6	2	8
38	2	2	5	0	4	5	9	6	2	8
40	3	1	4	1	4	5	9	7	2	9
42	4	0	3	3	4	6	10	7	2	9
44	3	2	4	1	5	5	10	7	3	10
46	4	2	4	1	6	5	11	7	3	10
48	5	0	3	3	5	6	11	8	3	11
50	4	2	4	2	6	6	12	8	3	11
52	3	3	5	1	6	6	12	8	4	12
54	5	1	3	4	6	7	13	8	4	12
56	3	4	5	1	7	6	13	8	5	13
58	4	3	5	2	7	7	14	8	5	13
60	6	0	3	5	6	8	14	9	5	14
62	3	4	7	1	7	8	15	9	5	14
64	5	2	5	3	7	8	15	10	5	15
66	6	1	4	5	7	9	16	10	5	15
68	2	5	8	1	7	9	16	10	6	16
70	5	3	5	4	8	9	17	10	6	16
72	6	2	4	5	8	9	17	10	7	17
74	5	4	6	3	9	9	18	10	7	17
76	5	4	6	3	9	9	18	11	7	18
78	7	2	4	6	9	10	19	11	7	18
80	4	5	7	3	9	10	19	11	8	19
82	5	5	7	3	10	10	20	11	8	19
84	8	1	4	7	9	11	20	12	8	20
86	5	5	8	3	10	11	21	12	8	20
88	4	5	9	3	9	12	21	13	8	21
90	9	0	4	9	9	13	22	13	8	21
92	4	6	9	3	10	12	22	13	9	22
94	5	5	9	4	10	13	23	13	9	22
96	7	2	7	7	9	14	23	14	9	23
98	3	6	11	4	9	15	24	14	9	23
100	6	4	8	6	10	14	24	14	10	24

Annex 2 : sets bijections

- case $n = 32$

$Z_a = X_a + X_c = 5$
$Z_c = X_b + X_d = 2$

$Z_a + Z_c = \left\lfloor \frac{n-4}{4} \right\rfloor = 7$



$Y_a = X_a + X_b = 4$
$Y_c = X_c + X_d = 3$

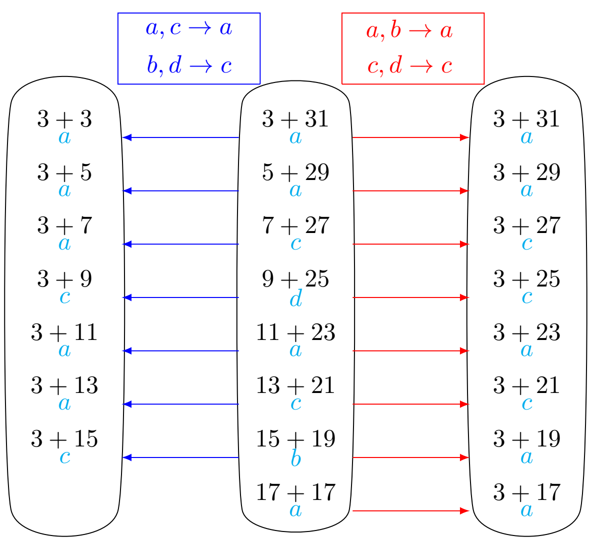
$Y_a + Y_c = \left\lfloor \frac{n-2}{4} \right\rfloor = 7$

$X_a = 2$
$X_b = 2$
$X_c = 3$
$X_d = 0$

- case $n = 34$

$Z_a = X_a + X_c = 5$
$Z_c = X_b + X_d = 2$

$Z_a + Z_c = \left\lfloor \frac{n-4}{4} \right\rfloor = 7$



$Y_a = X_a + X_b = 5$
$Y_c = X_c + X_d = 3$

$Y_a + Y_c = \left\lfloor \frac{n-2}{4} \right\rfloor = 8$

$X_a = 4$
$X_b = 1$
$X_c = 2$
$X_d = 1$

- case $n = 98$

$Xc = 11$

$Za = 14$

$3+3 \quad 3+5 \quad 3+7 \quad 3+11$
$3+13 \quad 3+17 \quad 3+19 \quad 3+23$
$3+29 \quad 3+31 \quad 3+37$
$3+41 \quad 3+43 \quad 3+47$

$3+95 \quad 23+75$
$5+93 \quad 29+69$
$7+91 \quad 41+57$
$11+87 \quad 43+55$
$13+85 \quad 47+51$
$17+81$

$Xa = 3$

$19+79$
$31+67$
$37+61$

$Ya = 9$

$3+53 \quad 3+59 \quad 3+61$
$3+67 \quad 3+71 \quad 3+73$
$3+79 \quad 3+83 \quad 3+89$

$3+9 \quad 3+15 \quad 3+21 \quad 3+25$
$3+27 \quad 3+33 \quad 3+35 \quad 3+39$
$3+45$

$Zc = 9$

$21+77$
$33+65$
$35+63$
$49+49$

$Xd = 4$

$9+89$
$15+83$
$25+73$
$27+71$
$39+59$
$45+53$

$Xb = 6$

$3+49 \quad 3+51 \quad 3+55 \quad 3+57$
$3+63 \quad 3+65 \quad 3+69 \quad 3+75$
$3+77 \quad 3+81 \quad 3+85 \quad 3+87$
$3+91 \quad 3+93 \quad 3+95$

$Yc = 15$

- case $n = 100$

$Xc = 8$ $\quad Xa = 6$

$Za = 14$

$3+3 \quad 3+5 \quad 3+7 \quad 3+11$
$3+13 \quad 3+17 \quad 3+19 \quad 3+23$
$3+29 \quad 3+31 \quad 3+37$
$3+41 \quad 3+43 \quad 3+47$

$5+95 \quad 37+63$
$7+93 \quad 43+57$
$13+87$
$19+81$
$23+77$
$31+69$

$3+97$
$11+89$
$17+83$
$29+71$
$41+59$
$47+53$

$Ya = 10$

$3+53 \quad 3+59 \quad 3+61$
$3+67 \quad 3+71 \quad 3+73$
$3+79 \quad 3+83 \quad 3+89 \quad 3+97$

$3+9 \quad 3+15 \quad 3+21 \quad 3+25$
$3+27 \quad 3+33 \quad 3+35 \quad 3+39$
$3+45 \quad 3+49$

$Zc = 10$

$9+91$
$15+85$
$25+75$
$35+65$
$45+55$
$49+51$

$21+79$
$27+73$
$33+67$
$39+61$

$Xb = 4$

$3+51 \quad 3+55 \quad 3+57$
$3+63 \quad 3+65 \quad 3+69 \quad 3+75$
$3+77 \quad 3+81 \quad 3+85 \quad 3+87$
$3+91 \quad 3+93 \quad 3+95$

$Yc = 14$

$Xd = 6$

Goldbach's conjecture, 4 letters language, variables and invariants

Denise Vella-Chemla

10/5/2014

1 Introduction

Goldbach's conjecture states that each even integer except 2 is the sum of two prime numbers. In the following, one is interested in decompositions of an even number n as a sum of two odd integers $p+q$ with $3 \leqslant p \leqslant n/2$, $n/2 \leqslant q \leqslant n-3$ and $p \leqslant q$. We call p a *n's first range sommant* and q a *n's second range sommant.*

Notations :

We will designate by :

- a : an n decomposition of the form $p+q$ with p and q primes ;
- b : an n decomposition of the form $p+q$ with p compound and q prime ;
- c : an n decomposition of the form $p+q$ with p prime and q compound ;
- d : an n decomposition of the form $p+q$ with p and q compound numbers.

Example :

40	3	5	7	9	11	13	15	17	19
	37	35	33	31	29	27	25	23	21
l_{40}	a	c	c	b	a	c	d	a	c

2 Main array

We designate by $T = (L, C) = (\ l_{n,m}\ )$ the array containing $l_{n,m}$ elements that are one of a, b, c, d letters. n belongs to the set of even integers greater than or equal to 6. m, belonging to the set of odd integers greater than or equal to 3, is an element of list of n first range sommants.

Let us consider g function defined by :

$$\begin{array}{rccl} g: & 2\mathbb{N} & \to & 2\mathbb{N}+1 \\ & x & \mapsto & 2\left\lfloor \dfrac{x-2}{4} \right\rfloor + 1 \end{array}$$

$g(6) = 3, g(8) = 3, g(10) = 5, g(12) = 5, g(14) = 7, g(16) = 7, etc.$

$g(n)$ function defines the greatest of n first range sommants.

As we only consider n decompositions of the form $p+q$ where $p \leqslant q$, in T will only appear letters $l_{n,m}$ such that $m \leqslant 2\left\lfloor \dfrac{n-2}{4} \right\rfloor + 1$ in such a way that T array first letters are : $l_{6,3}, l_{8,3}, l_{10,3}, l_{10,5}, l_{12,3}, l_{12,5}, l_{14,3}, l_{14,5}, l_{14,7}, etc.$

Here are first lines of array T.

L \ C	3	5	7	9	11	13	15	17
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
...								

FIGURE 1 : words of even numbers between 6 and 36

Remarks :

1) words on array's diagonals called *diagonal words* have their letters either in $A_{ab} = \{a, b\}$ alphabet or in $A_{cd} = \{c, d\}$ alphabet.

2) a diagonal word codes decompositions that have the same second range sommant.
For instance, on Figure 4, letters *aaabaa* of the diagonal that begins at letter $l_{26,3} = a$ code decompositions $3 + 23, 5 + 23, 7 + 23, 9 + 23, 11 + 23$ and $13 + 23$.

3) let us designate by l_n the line whose elements are $l_{n,m}$. Line l_n contains $\left\lfloor \dfrac{n-2}{4} \right\rfloor$ elements.

4) n being fixed, let us call $C_{n,3}$ the column formed by $l_{k,3}$ for $6 \leqslant k \leqslant n$.

In this column $C_{n,3}$, let us distinguish two parts, the "top part" and the "bottom part" of the column.

Let us call $H_{n,3}$ column's "top part", i.e. set of $l_{k,3}$ where $6 \leqslant k \leqslant \left\lfloor \dfrac{n+4}{2} \right\rfloor$.

Let us call $B_{n,3}$ column's "bottom part", i.e. set of $l_{k,3}$ where $\left\lfloor \dfrac{n+4}{2} \right\rfloor < k \leqslant n$.

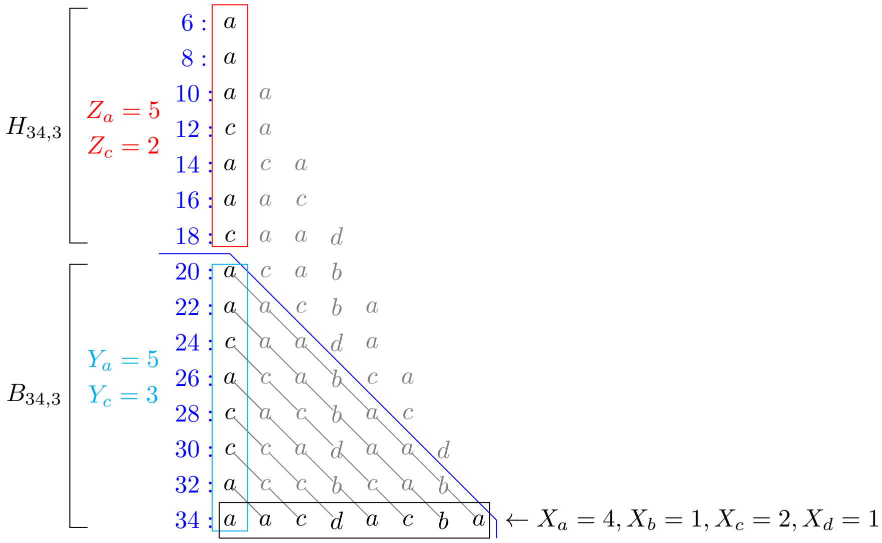


FIGURE 2 : $n = 34$

To better understand countings in next section, we will use projection P of line n on bottom part of first column $B_{n,3}$ that "associates" letters at both extremities of a diagonal. If we consider application *proj* such that $proj(a) = proj(b) = a$ and $proj(c) = proj(d) = c$ then, since 3 is prime, $proj(l_{n,2k+1}) = l_{n-2k+2,3}$.

We can also understand the effect of this projection (that preserves second range sommant) by analyzing decompositions :

- if $p+q$ is coded by an a or a b letter, it corresponds to two possible cases in which q is prime, and so $3+q$ decomposition, containing two prime numbers, will be coded by an a letter ;
- if $p+q$ is coded by a c or a d letter, it corresponds to two possible cases in which q is compound, and so $3+q$ decomposition, of the form $prime + compound$ will be coded by a c letter.

We will also use in next section a projection that transforms first range sommant in a second range sommant that is combined with 3 as a first range sommant ; let us analyze the effect that such a projection will have on decompositions :

- if $p+q$ is coded by an a or a c letter, it corresponds to two possible cases in which p is prime, and so $3+p$ decomposition, containing two prime numbers, will be coded by an a letter ;
- if $p+q$ is coded by a b or a d letter, it corresponds to two possible cases in which p is compound, and so $3+p$ decomposition, of the form $prime + compound$ will be coded by a c letter.

3 Computations

1) We note in line n by :

- $X_a(n)$ the number of n decompositions of the form $prime + prime$;
- $X_b(n)$ the number of n decompositions of the form $compound + prime$;
- $X_c(n)$ the number of n decompositions of the form $prime + compound$;
- $X_d(n)$ the number of n decompositions of the form $compound + compound$.

$X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor$ is the number of elements of line n.

Example $n = 34$:
$X_a(34) = \#\{3+31, 5+29, 11+23, 17+17\} = 4$
$X_b(34) = \#\{15+19\} = 1.$
$X_c(34) = \#\{7+27, 13+21\} = 2$
$X_d(34) = \#\{9+25\} = 1$

2) Let $Y_a(n)$ (resp. $Y_c(n)$) being the number of a letters (resp. c) that appear in $B_{n,3}$. We recall that there are only a and c letters in first column because it contains letters associated with decompositions of the form $3+x$ and because 3 is prime.

Example :

- $Y_a(34) = \#\{3+17, 3+19, 3+23, 3+29, 3+31\} = 5$
- $Y_c(34) = \#\{3+21, 3+25, 3+27\} = 3$

3) Because of P projection that is a bijection, and because of a, b, c, d letters definitions, $Y_a(n) = X_a(n) + X_b(n)$ and $Y_c(n) = X_c(n) + X_d(n)$. Thus, trivially, $Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$.

Example :

$$\begin{aligned}
Y_a(34) &= \#\{3+17, 3+19, 3+23, 3+29, 3+31\} \\
X_a(34) &= \#\{3+31, 5+29, 11+23, 17+17\} \\
X_b(34) &= \#\{15+19\} \\
\\
Y_c(34) &= \#\{3+21, 3+25, 3+27\} \\
X_c(34) &= \#\{7+27, 13+21\} \\
X_d(34) &= \#\{9+25\}
\end{aligned}$$

4) Let $Z_a(n)$ (resp. $Z_c(n)$) being the number of a letters (resp. c) that appear in $H_{n,3}$.

Example :

- $Z_a(34) = \#\{3+3, 3+5, 3+7, 3+11, 3+13\} = 5$
- $Z_c(34) = \#\{3+9, 3+15\} = 2$

$Z_a(n) + Z_c(n) = \left\lfloor \dfrac{n-4}{4} \right\rfloor$.

Reminding identified properties

$$Y_a(n) = X_a(n) + X_b(n) \tag{1}$$

$$Y_c(n) = X_c(n) + X_d(n) \tag{2}$$

$$Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

$$Z_a(n) + Z_c(n) = \left\lfloor \frac{n-4}{4} \right\rfloor \tag{4}$$

Let us add four new properties to those ones :

$$X_a(n) + X_c(n) = Z_a(n) + \delta_{2p}(n) \tag{5}$$

with $\delta_{2p}(n)$ equal to 1 when n is the double of a prime number and equal to 0 otherwise.

$$X_b(n) + X_d(n) = Z_c(n) + \delta_{c-imp}(n) \tag{6}$$

with $\delta_{2c-imp}(n)$ equal to 1 when n is the double of a compound odd number and equal to 0 otherwise (when there exists k such that $n = 4k$ (doubles of even numbers) or when n is the double of a prime number).

$$Z_c(n) - Y_a(n) = Y_c(n) - Z_a(n) - \delta_{4k+2}(n) \tag{7}$$

with $\delta_{4k+2}(n)$ equal to 1 when n is the double of an odd number and 0 otherwise.

$$Z_c(n) - Y_a(n) = X_d(n) - X_a(n) - \delta_{2c-imp}(n) \tag{8}$$

4 Variables evolution

In this section, let us study how different variables change.

$Z_a(n)+Z_c(n) = \left\lfloor \dfrac{n-4}{4} \right\rfloor$ is an increasing function of n, it is increased by 1 at each n that is an even double.

$Z_a(n+2) = Z_a(n)$ and $Z_c(n+2) = Z_c(n)$ are constant when n is an even double.

$Z_a(n) = Z_a(n-2) + 1$ when $\dfrac{n-2}{2}$ is prime (*ex* : $n = 24$ or $n = 28$, look to values array page 13 : we will express this abusively by *"Z_a is increasing"*) and $Z_c(n) = Z_c(n-2) + 1$ when $\dfrac{n-2}{2}$ is an odd compound number (*ex* : $n = 42$ or 50, abusively, *"Z_c is increasing"*).

$Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$ is an increasing function of n, it is increased by 1 at each n that is an odd double.

Let us see now in details how $Y_a(n)$ and $Y_c(n)$ evoluate.

In case if n is an odd double, a number more is put in $H_{n,3}$; if this number $n-3$ is prime (resp. compound), $Y_a(n) = Y_a(n-2) + 1$ (abusively *"Y_a is increasing"*, *ex* : $n = 34$) (resp. $Y_c(n) = Y_c(n-2) + 1$, abusively *"Y_c is increasing"*, *ex* : $n = 38$).

In case if n is an even double, 4 cases are to be studied. Let us study the way decompositions set $H_{n,3}$ evoluates.

- if $n-3$ and $\dfrac{n-2}{2}$ are both primes, there is a decomposition that is taken out in the bottom and another decomposition that is put in in the top of $H_{n,3}$ and those two decompositions have two letters of the same type, so $Y_a(n) = Y_a(n-2)$ and $Y_c(n) = Y_c(n-2)$ (abusively *"Y_a and Y_c constants"* (*ex* : $n = 40$) ;
- if $n-3$ is prime and $\dfrac{n-2}{2}$ is compound then $Y_a(n) = Y_a(n-2) + 1$ and $Y_c(n) = Y_c(n-2) - 1$ (abusively, *"Y_a is increasing and Y_c is decreasing"* (*ex* : $n = 32$) ;
- if $n-3$ is compound and $\dfrac{n-2}{2}$ is prime then $Y_c(n) = Y_c(n-2) + 1$ and $Y_a(n) = Y_a(n-2) - 1$ (abusively, *"Y_a is decreasing and Y_c is increasing"*) (*ex* : $n = 48$) ;
- if $n-3$ and $\dfrac{n-2}{2}$ are both compound, there is a decomposition that is taken out in the bottom and another decomposition that is put in in the top of $H_{n,3}$ and those two decompositions have two letters of the same type, so $Y_a(n) = Y_a(n-2)$ and $Y_c(n) = Y_c(n-2)$ (abusively, *"Y_a and Y_c constants"* (*ex* : $n = 52$).

In annex 1 is provided an array containing different variables values for n between 14 and 100.

5 Use gaps between variables

We are going to show in the following that $X_a(n)$ can never be equal to 0 for $n \geqslant C$, C being a constant to be defined, i.e. to show that each even integer $n \geqslant C$ can be written as a sum of two primes, or in other words verifies Goldbach's conjecture.

We saw that at $\delta_{4k+2}(n)$ and $\delta_{2c-imp}(n)$ near ($\delta_{4k+2}(n)$ and/or $\delta_{2c-imp}(n)$ being equal to 1 in certain cases), we have following equalities :

$$Z_c(n) - Y_a(n) = Y_c(n) - Z_a(n) - \delta_{4k+2}(n) \qquad (7)$$

$$Z_c(n) - Y_a(n) = X_d(n) - X_a(n) - \delta_{2c-imp}(n) \qquad (8)$$

We remind that

- $Y_a(n)$, counting number of primes that are between $\frac{n}{2}$ and n is equal to $\pi(n) - \pi\left(\frac{n}{2}\right)$;
- $Z_a(n)$ counting number of primes lesser than or equal to $\frac{n}{2}$ is equal to $\pi\left(\frac{n}{2}\right)$;
- $Z_c(n)$ counting number of odd compound numbers lesser than or equal to $\frac{n}{2}$ is equal to $\frac{n}{4} - \pi\left(\frac{n}{2}\right)$;
- $Y_c(n)$ counting number of odd compound numbers that are between $\frac{n}{2}$ and n is equal to $\frac{n}{4} - \pi(n) + \pi\left(\frac{n}{2}\right)$.

Rosser and Schoenfeld [1] note provides formula 3.5 of corollary 1 of theorem 2 that $\pi(x) > \frac{x}{ln\ x}$ for every $x \geqslant 17$, and as formula 3.6 of the same corollary of the same theorem that $\pi(x) < \frac{1,25506x}{ln\ x}$ for every $x > 1$.

5.1 $Z_c(n) > Z_a(n)$ inequality study

To show that $Z_c(n) > Z_a(n)$, one can simply use the fact that $Z_c(n)$ is increasing "many more times" than $Z_a(n)$ (each time $\frac{n-2}{2}$ is an odd compound number for $Z_c(n)$ and each time $\frac{n-2}{2}$ is a prime number for $Z_a(n)$ as it was shown in section 4).

To find from which value of n, $Z_c(n) > Z_a(n)$, one uses the fact that $Z_c(n) - Z_a(n)$ gap is equal to $\frac{n}{4} - 2\,\pi\left(\frac{n}{2}\right)$.

From formula 3.6 of corollary 1 of theorem 2 of [1], we have $2\,\pi\left(\frac{n}{2}\right) < 2\,\frac{1,25506\,n}{2\,(ln\ n + ln\ 0.5)}$ for every $n > 2$.

We deduce from this $-2\,\pi\left(\frac{n}{2}\right) > \frac{-1,25506\,n}{ln\ n + ln\ 0.5}$ for every $n > 2$.

$Z_c(n) - Z_a(n)$ gap is so minorable by $\frac{n\,(ln\ n + ln\ 0.5) - 5,02024n}{4\,(ln\ n + ln\ 0.5)}$. It is strictly greater than 0 for every $n \geqslant 304$ (denominator is greater or equal to 0 for every $n \geqslant 2$, numerator is strictly greater than 0 for every $n > 2e^{5.02024}$).

5.2 $Z_a(n) > Y_a(n)$ and $Y_c(n) > Z_c(n)$ inequalities study

To show that $Z_a(n) > Y_a(n)$, one can use once more the analysis of variables evolution provided in section 4 : when *"Z_a is increasing"*, *"Y_a is constant or is decreasing"*; and when *"Y_a is increasing"* without *"Z_a is also increasing"* (when $n-3$ is prime and $\frac{n-2}{2}$ is compound), Y_a is increased only by 1 although its gap to Z_a is very quickly very greater than 1.

To show that $Y_c(n) > Z_c(n)$, one can use once more the analysis of variables evolution provided in section 4 : Y_c is increasing when $n-3$ is compound while Z_c is increasing when $\frac{n-2}{2}$ is compound. Z_c is an increasing function, there are times when Y_c is decreasing but not so often, and this has as consequence that over a rather small value, Z_c never catches Y_c again.

To know precisely from which values of n wished inequalities are verified, we use once more gaps values and minorations/majorations provided in [1].

To show that $Z_a(n) > Y_a(n)$ (resp. $Y_c(n) > Z_c(n)$), we show that the gap

$$Z_a(n) - Y_a(n) = Y_c(n) - Z_c(n) = 2\pi\left(\frac{n}{2}\right) - \pi(n)$$

is always strictly greater than 0.

We use formula 3.9 of corollary 1 of theorem 2 of Rosser and Schoenfeld that states that $\pi(x) - \pi\left(\frac{x}{2}\right) < \frac{7x}{5\ ln\ x}$ for every $x > 1$.

We use the fact that $2\pi\left(\frac{n}{2}\right) - \pi(n) = \left(\pi\left(\frac{n}{2}\right) - \pi(n)\right) + \pi\left(\frac{n}{2}\right)$

So we have

$$\begin{aligned} 2\pi\left(\frac{n}{2}\right) - \pi(n) &> \frac{-7n}{5\ ln\ n} + \pi\left(\frac{n}{2}\right) \\ &> \frac{-7n}{5\ ln\ n} + \frac{n}{2\ (ln\ n + ln\ 0.5)} \qquad \text{(because of formula 3.5 of corollary 1 of theorem 2 in [1])} \end{aligned}$$

that is strictly greater than 0

$$\frac{n(5\ ln\ n - 14\ (ln\ n + ln\ 0.5))}{10\ ln\ n(ln\ n + ln\ 0.5)} > 0$$

that is equivalent to

$$5\ ln\ n - 14\ (ln\ n + ln\ 0.5) > 0$$

that is always true when $n \geqslant 6$.

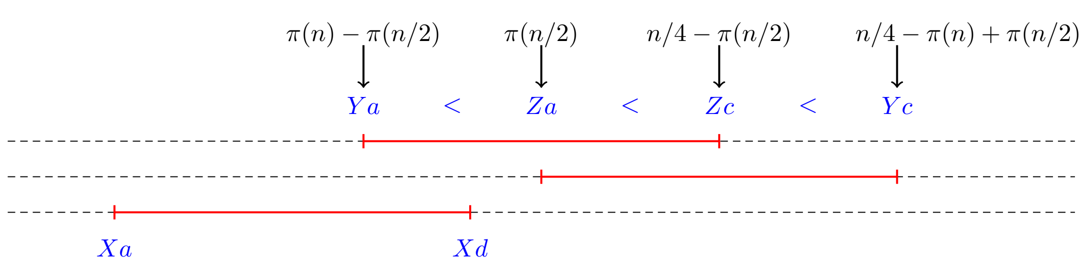
5.3 Strict order on $Y_a(n), Y_c(n), Z_a(n)$ and $Z_c(n)$ variables

$Y_a(n), Z_a(n), Z_c(n)$ and $Y_c(n)$ variables are so strictly ordered in the following way :

$$Y_a(n) < Z_a(n) < Z_c(n) < Y_c(n)$$

for every $n \geqslant 304$.

A graphical representation of gaps between variables can be found above, that shows their entanglement :



$Z_c(n) - Y_a(n)$, $Y_c(n) - Z_a(n)$ and $X_d(n) - X_a(n)$ gaps are strictly greater than 0 and equal to $\frac{n}{4} - \pi(n)$.

5.4 $X_a(n) > 0$ inequality study

To be ensured that $X_a(n)$ is never equal to 0, one has to minorate $X_d(n)$ by $\frac{n}{4} - \pi(n)$, i.e. the value of $X_d(n) - X_a(n)$ gap.

But $X_d(n) = Y_c(n) - X_c(n)$.

To minorate $X_d(n)$, one has to minorate $Y_c(n)$ and to majorate $X_c(n)$.

$Y_c(n)$ is the number of odd compound numbers that are between $n/2$ and n (associated to 3).

To minorate $Y_c(n)$, we use the fact that the number of odd compound numbers that are between $n/2$ and n is equal to $\frac{n}{4} - \pi(n) + \pi\left(\frac{n}{2}\right)$.

$X_c(n)$, which is the number of n's decompositions of the form *prime*+*compound* is majorable by the total number of odd compound numbers that are between $n/2$ and n, that is itself majorable by the number of odd compound numbers that are between n and $\frac{3n}{2}$.

$X_c(n)$ is so majorable by $\frac{n}{4} - \left(\pi\left(\frac{3n}{2}\right) - \pi(n)\right)$ (the number of odd compound numbers from the interval from n to $\frac{3n}{2}$ is $\frac{n}{4}$, the number of prime numbers in this interval is $\pi\left(\frac{3n}{2}\right) - \pi(n)$, the number of odd compound numbers in this interval is the difference of those two numbers).

$Y_c(n) - X_c(n)$ is thus always greater than the difference between $Y_c(n)$'s minoration and $X_c(n)$'s majoration, that will give

$$Y_c(n) - X_c(n) > \frac{n}{4} - \pi(n) + \pi\left(\frac{n}{2}\right) - \frac{n\,((ln\ n + ln\ 1.5)(ln\ n - 4 \times 1.25506) - 1.25506 \times 6 \times ln\ n)}{4\ (ln\ n + ln\ 1.5)\ ln\ n}.$$

$Y_c(n) - X_c(n) = X_d(n)$ is always greater than $\frac{n}{4} - \pi(n)$ when $n > 0$ (we also make this constatation by computing all this by program).

Indeed, $Y_c(n) - X_c(n) > \frac{n}{4} - \pi(n)$ when

$$\pi\left(\frac{n}{2}\right) - \frac{n\,((ln\ n + ln\ 1.5)(ln\ n - 4 \times 1.25506) - 1.25506 \times 6 \times ln\ n)}{4\ (ln\ n + ln\ 1.5)\ ln\ n} > 0.$$

We replace $\pi\left(\frac{n}{2}\right)$ by its minoration provided by formula 3.5 of corollary 1 of theorem 2 in [1] (that is $\frac{n}{2(ln\ n + ln\ 0.5)}$), we reduce to same denominator, that is always greater than 0 when $n \geqslant 2$ and that we forget, we are looking for condition that ensures that numerator is always strictly greater than 0, numerator that is equal to :

$$n[(2(ln\ n + ln\ 1.5)ln\ n) - (ln\ n + ln\ 0.5)((ln\ n + ln\ 1.5)(ln\ n - 5.02024) - 7.53036\ ln\ n)]$$

After several computations, we obtain that numerator, with unknown $ln\ n$, is equal to polynom

$$-(ln\ n)^3 + 14.6755387366(ln\ n)^2 - 2.48889541216(ln\ n) - 0.26611665186$$

The biggest root of this polynom is nearly equal to 14.502656936497 from which exponential is equal to 1988034.33365. Difference between $X_d(n)$ and $X_a(n)$ is thus always greater than $\frac{n}{4} - \pi(n)$ for every

$n \geqslant 1988034.33365$.

We can thus conclude that for every $n \geqslant 1988034.33365$ (necessary condition to have $X_d(n) - X_a(n) > \frac{n}{4} - \pi(n)$), $X_a(n)$ (number of n's decompositions as a sum of two primes) is strictly greater than 0.

In annex 2 are provided graphic representations of sets bijections for cases $n = 32$, 34, 98 and 100.

The file *http://denise.vella.chemla.free.fr/annexes.pdf* contains
- an historical recall of a Laisant's note in which he presented yet in 1897 the idea of "strips" of odd numbers to be put in regard and to be colorated to *see* Goldbach decompositions ;
- a program and its execution that implement ideas presented here.

6 Demonstrations

6.1 Utilitaries

Let us demonstrate that if n is an odd number double (i.e. of the form $4k+2$), then $\left\lfloor \frac{n-2}{4} \right\rfloor = \left\lfloor \frac{n-4}{4} \right\rfloor + 1$.
Indeed, the left part of the equality is equal to $\left\lfloor \frac{(4k+2)-2}{4} \right\rfloor = \left\lfloor \frac{4k}{4} \right\rfloor = k$.
The right part of the equality is equal to $\left\lfloor \frac{(4k+2)-4}{4} \right\rfloor + 1 = \left\lfloor \frac{4k-2}{4} \right\rfloor + 1 = (k-1)+1 = k$.

Let us demonstrate that if n is an even number double (i.e. of the $4k$), then $\left\lfloor \frac{n-2}{4} \right\rfloor = \left\lfloor \frac{n-4}{4} \right\rfloor$.
$\left\lfloor \frac{4k-2}{4} \right\rfloor = k-1$ and $\left\lfloor \frac{4k-4}{4} \right\rfloor = k-1$.

We can also express this by the following way : if n is an odd number double, $\left\lfloor \frac{n-2}{4} \right\rfloor = \frac{n-2}{4} = \left\lfloor \frac{n-4}{4} \right\rfloor + 1$ although if n is an even number double, $\left\lfloor \frac{n-2}{4} \right\rfloor = \frac{n-4}{4} = \left\lfloor \frac{n-4}{4} \right\rfloor$.

6.2 5, 6 and 8 properties

5, 6 and 8 properties follows directly from variables definitions.

6.2.1 Property 5

Property 5 states that $X_a(n) + X_c(n) = Z_a(n) + \delta_{2p}(n)$ with $\delta_{2p}(n)$ that is equal to 1 in the case if n is a prime number double and that is equal to 0 otherwise.

By definition, $X_a(n)+X_c(n)$ counts number of n's decompositions of the form $prime+x$ with $prime \leqslant n/2$. But by the fact that $Z_a(n)$ counts on its side number of decompositions of the form $3 + prime$ with $prime < n/2$, adding δ_{2p} to $Z_a(n)$ permits to ensure the equality's invariance in all cases and in particular when n is a prime number double.

6.2.2 Property 6

Property 6 states that $X_b(n) + X_d(n) = Z_c(n) + \delta_{2c-imp}$ with δ_{2c-imp} that is equal to 1 in the case if n is a compound odd number, and is equal to 0 otherwise.

By definition, $X_b(n) + X_d(n)$ counts the number of decompositions of the form $compound + x$ with $compound \leqslant n/2$. But by the fact that $Z_c(n)$ counts on its side number of decompositions of the form $3 + compound$ with $compound < n/2$, adding δ_{2c-imp} to $Z_c(n)$ permits to ensure the equality's invariance in all cases and in particular when n is an odd compound double.

6.2.3 Property 8

Property 8 states that $Z_c(n) - Y_a(n) = X_d(n) - X_a(n) - \delta_{2c-imp}$ with δ_{2c-imp} that is equal to 1 if n is an odd compound double and is equal to 0 otherwise.

By definition, $Z_c(n)$ counts the number of odd compound numbers strictly lesser than $n/2$. It counts also the number of n's decompositions of the form $compound + x$ with $compound < n/2$ (let us call E this decompositions set).

By definition, $Y_a(n)$ counts the number of prime numbers strictly greater than $n/2$. It counts also the number of n's decompositions of the form $x + prime$ with $prime > n/2$ (let us call F this decompositions set).

n's decompositions of the form $compound + prime$ are at the same time in E and in F. By computing $Z_c(n) - Y_a(n)$, we are computing the cardinality of a set that is equal to $X_d(n) - X_a(n)$ by definition of what $Y_a(n), Z_c(n), X_d(n)$ and $X_a(n)$ variables count.

6.2.4 Property 7

Let us demonstrate that $Z_c(n) - Y_a(n) = Y_c(n) - Z_a(n) - \delta_{4k+2}$ with δ_{4k+2} that is equal to 1 if n is an odd double (there exists some $k \geqslant 3$ such that $n = 4k + 2$) and is equal to 0 otherwise.

One uses a recurrence reasoning :

i) One initialises recurrences according to the 3 sorts of numbers to be envisaged : even doubles (of the form $4k$, like 16), odd doubles (of the form $4k + 2$) that are prime (like 14) or that are compound (like 18).

Property 7 is true for $n = 14$ because $Z_c(14) = 0, Y_a(14) = 2, Y_c(14) = 1, Z_a(14) = 2$ and $\delta_{4k+2}(14) = 1$ and thus $Z_c(14) - Y_a(14) = Y_c(14) - Z_a(14) - \delta_{4k+2}(14)$;
Property 7 is true for $n = 16$ because $Z_c(16) = 0, Y_a(16) = 2, Y_c(16) = 1, Z_a(16) = 3$ and $\delta_{4k+2}(16) = 0$ and thus $Z_c(16) - Y_a(16) = Y_c(16) - Z_a(16) - \delta_{4k+2}(16)$;
Property 7 is true for $n = 18$ because $Z_c(18) = 0, Y_a(18) = 2, Y_c(18) = 2, Z_a(18) = 3$ and $\delta_{4k+2}(18) = 1$ and thus $Z_c(18) - Y_a(18) = Y_c(18) - Z_a(18) - \delta_{4k+2}(18)$;

ii) We rewrite property in the following form $Z_a(n) + Z_c(n) + \delta_{4k+2} = Y_a(n) + Y_c(n)$.
Four cases must be considered : two cases in which n is an odd double (prime or compound) and $n + 2$ is an even double and two cases in which n is an even double and $n + 2$ is an the double of an odd number (that is prime or compound).

iia) *n even double and $n + 2$ prime double (ex : $n = 56$)* :

n	δ_{2p}	δ_{2c-imp}	δ_{4k+2}
n	0	0	0
$n+2$	1	0	1

One states the hypothesis that property 7 is verified by n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \qquad (H)$$

Let us demonstrate the property is true for $n + 2$,

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \qquad (Ccl)$$

One has $Z_a(n + 2) = Z_a(n)$ and $Z_c(n + 2) = Z_c(n)$.

Recall property 3 concerning $Y_a(n)$ and $Y_c(n)$:

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

In (Ccl), we can, by recurrence hypothesis and by proprerty (3), replace the left part of the equality by $Z_a(n) + Z_c(n) + 1$ and than by $Y_a(n) + Y_c(n) + 1$ (because (H)) and then by $\left\lfloor \frac{n-2}{4} \right\rfloor + 1$ (because (3)) that is equal to $\left\lfloor \frac{n}{4} \right\rfloor$.

But in (Ccl), we can also replace the right part of the equality by $\left\lfloor \frac{n}{4} \right\rfloor$ because of property (3).

There is also, for $n+2$, equality between left and right parts of the equality, i.e. property 7 is verified by $n+2$. From the hypothesis that property is verified by n, we demonstrated that property is true for $n+2$.

iib) *n even double and $n+2$ odd compound double* (*ex :* $n = 48$) :

n	δ_{2p}	δ_{2c-imp}	δ_{4k+2}
n	0	0	0
$n+2$	0	1	1

One states the hypothesis that property 7 is verified by n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \tag{H}$$

Let us demonstrate the property is verified by $n+2$,

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \tag{Ccl}$$

One has $Z_a(n+2) = Z_a(n)$ and $Z_c(n+2) = Z_c(n)$.

And one has also $Y_a(n+2) = Y_a(n) + 1$ and $Y_c(n+2) = Y_c(n)$.

Let us recall property 3 concerning $Y_a(n)$ and $Y_c(n)$:

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

In (Ccl), we can, by recurrence hypothesis and property (3), replace the left part of the equality by $Z_a(n) + Z_c(n) + 1$ and the by $Y_a(n) + Y_c(n) + 1$ (by (H)) and then by $\left\lfloor \frac{n-2}{4} \right\rfloor + 1$ (by (3)) that is equal to $\left\lfloor \frac{n}{4} \right\rfloor$.

But in (Ccl), we can also replace the right part of the equality by $\left\lfloor \frac{n}{4} \right\rfloor$ because of evolutions of $Y_a(n)$ and $Y_c(n)$.

There is also, for $n+2$, equality between left and right parts of the equality, i.e. property 7 is verified by $n+2$. From the hypothesis that property is verified by n, we demonstrated that property is verified by $n+2$.

iic) *n prime double and $n+2$ even double* (*ex :* $n = 74$) :

n	δ_{2p}	δ_{2c-imp}	δ_{4k+2}
n	1	0	1
$n+2$	0	0	0

One states the hypothesis that property 7 is verified by n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \tag{H}$$

Let us demonstrate that property is verified by $n+2$,

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \qquad (Ccl)$$

One has $Z_a(n+2) = Z_a(n) + 1$ and $Z_c(n+2) = Z_c(n)$.

Let us recall property 3 concerning $Y_a(n)$ and $Y_c(n)$:

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \qquad (3)$$

In (Ccl), we can, by recurrence hypothesis and property (3), replace the left part of the equality by $Z_a(n) + Z_c(n) + 1$ and then by $Y_a(n) + Y_c(n)$ (because (H)) and then by $\left\lfloor \frac{n-2}{4} \right\rfloor$ (by (3)) that is equal to $\left\lfloor \frac{n}{4} \right\rfloor$.

But in (Ccl), one can also replace the right part of the equality by $\left\lfloor \frac{n}{4} \right\rfloor$ because of property (3).

There is once more, for $n+2$, equality between left and right part of the equality, i.e. property 7 is verified by $n+2$. From the hypothesis that property is true for n, we demonstrated that property is verified by $n+2$.

iid) *n odd compound double and $n+2$ even double* (*ex :* $n = 70$) :

n	δ_{2p}	δ_{2c-imp}	δ_{4k+2}
n	0	1	1
$n+2$	0	0	0

We state the hypothesis that property 7 is true for n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \qquad (H)$$

Let us demonstrate that it is true for

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \qquad (Ccl)$$

One has $Z_a(n+2) = Z_a(n)$ and $Z_c(n+2) = Z_c(n) + 1$.

Let us recall property 3 concerning $Y_a(n)$ and $Y_c(n)$:

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \qquad (3)$$

In (Ccl), we can, by recurrence hypothesis and property (3), replace the left part of the equality by $Z_a(n) + Z_c(n) + 1$ and then by $Y_a(n) + Y_c(n)$ (by (H)) and then by $\left\lfloor \frac{n-2}{4} \right\rfloor$ (by (3)) that is equal to $\left\lfloor \frac{n}{4} \right\rfloor$.

But in (Ccl), one can also replace the right part of the equality by $\left\lfloor \frac{n}{4} \right\rfloor$ because of property (3).

There is once more, for $n+2$, equality between left and right parts of the equality, i.e. property 7 is verified by $n+2$. From the hypothesis that property is verified by n, we demonstrated property is verified by $n+2$.

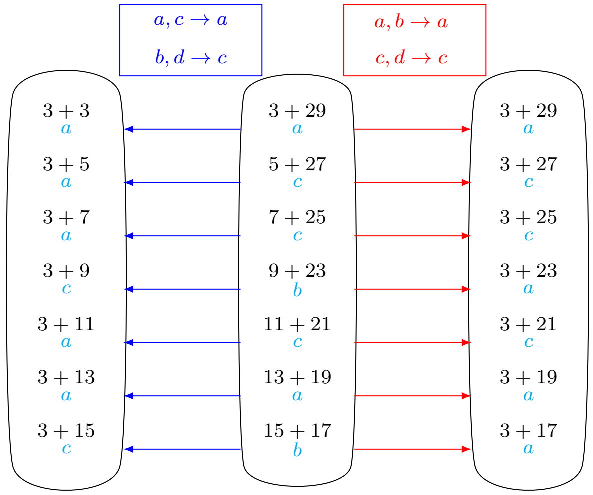
Annex 1 : variables values array for n between 14 and 100

n	$X_a(n)$	$X_b(n)$	$X_c(n)$	$X_d(n)$	$Y_a(n)$	$Y_c(n)$	$\left\lfloor \frac{n-2}{4} \right\rfloor$	$Z_a(n)$	$Z_c(n)$	$\left\lfloor \frac{n-4}{4} \right\rfloor$	$\delta_{2p}(n)$	$\delta_{2c-imp}(n)$	$\delta_{4k+2}(n)$
14	2	0	1	0	2	1	3	2	0	2	1	0	1
16	2	0	1	0	2	1	3	3	0	3	0	0	0
18	2	0	1	1	2	2	4	3	0	3	0	1	1
20	2	1	1	0	3	1	4	3	1	4	0	0	0
22	3	1	1	0	4	1	5	3	1	4	1	0	1
24	3	0	1	1	3	2	5	4	1	5	0	0	0
26	3	1	2	0	4	2	6	4	1	5	1	0	1
28	2	1	3	0	3	3	6	5	1	6	0	0	0
30	3	0	2	2	3	4	7	5	1	6	0	1	1
32	2	2	3	0	4	3	7	5	2	7	0	0	0
34	4	1	2	1	5	3	8	5	2	7	1	0	1
36	4	0	2	2	4	4	8	6	2	8	0	0	0
38	2	2	5	0	4	5	9	6	2	8	1	0	1
40	3	1	4	1	4	5	9	7	2	9	0	0	0
42	4	0	3	3	4	6	10	7	2	9	0	1	1
44	3	2	4	1	5	5	10	7	3	10	0	0	0
46	4	2	4	1	6	5	11	7	3	10	1	0	1
48	5	0	3	3	5	6	11	8	3	11	0	0	0
50	4	2	4	2	6	6	12	8	3	11	0	1	1
52	3	3	5	1	6	6	12	8	4	12	0	0	0
54	5	1	3	4	6	7	13	8	4	12	0	1	1
56	3	4	5	1	7	6	13	8	5	13	0	0	0
58	4	3	5	2	7	7	14	8	5	13	1	0	1
60	6	0	3	5	6	8	14	9	5	14	0	0	0
62	3	4	7	1	7	8	15	9	5	14	1	0	1
64	5	2	5	3	7	8	15	10	5	15	0	0	0
66	6	1	4	5	7	9	16	10	5	15	0	1	1
68	2	5	8	1	7	9	16	10	6	16	0	0	0
70	5	3	5	4	8	9	17	10	6	16	0	1	1
72	6	2	4	5	8	9	17	10	7	17	0	0	0
74	5	4	6	3	9	9	18	10	7	17	1	0	1
76	5	4	6	3	9	9	18	11	7	18	0	0	0
78	7	2	4	6	9	10	19	11	7	18	0	1	1
80	4	5	7	3	9	10	19	11	8	19	0	0	0
82	5	5	7	3	10	10	20	11	8	19	1	0	1
84	8	1	4	7	9	11	20	12	8	20	0	0	0
86	5	5	8	3	10	11	21	12	8	20	1	0	1
88	4	5	9	3	9	12	21	13	8	21	0	0	0
90	9	0	4	9	9	13	22	13	8	21	0	1	1
92	4	6	9	3	10	12	22	13	9	22	0	0	0
94	5	5	9	4	10	13	23	13	9	22	1	0	1
96	7	2	7	7	9	14	23	14	9	23	0	0	0
98	3	6	11	4	9	15	24	14	9	23	0	1	1
100	6	4	8	6	10	14	24	14	10	24	0	0	0

n	$X_a(n)$	$X_b(n)$	$X_c(n)$	$X_d(n)$	$Y_a(n)$	$Y_c(n)$	$\left\lfloor \frac{n-2}{4} \right\rfloor$	$Z_a(n)$	$Z_c(n)$	$\left\lfloor \frac{n-4}{4} \right\rfloor$	δ_{2p}	δ_{2c-imp}	δ_{4k+2}
999 998	4 206	32 754	37 331	175 708	36 960	213 039	249 999	41 537	208 461	249 998	0	1	1
1 000 000	5 402	31 558	36 135	176 904	36 960	213 039	249 999	41 537	208 462	249 999	0	1	0
9 999 998	28 983	287 084	319 529	1 864 403	316 067	2 183 932	2 499 999	348 511	2 151 487	2 499 998	1	0	1
10 000 000	38 807	277 259	309 705	1 874 228	316 066	2 183 933	2 499 999	348 512	2 151 487	2 499 999	0	1	0

Annex 2 : sets bijections

- Case $n = 32$



$Z_a = X_a + X_c = 5$

$Z_c = X_b + X_d = 2$

$$Z_a + Z_c = \left\lfloor \frac{n-4}{4} \right\rfloor = 7$$

$Y_a = X_a + X_b = 4$

$Y_c = X_c + X_d = 3$

$$Y_a + Y_c = \left\lfloor \frac{n-2}{4} \right\rfloor = 7$$

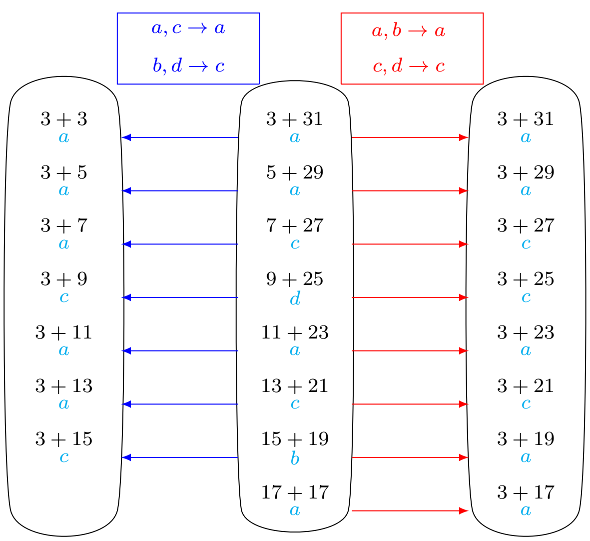
$X_a = 2$

$X_b = 2$

$X_c = 3$

$X_d = 0$

- Case $n = 34$



$Z_a = X_a + X_c = 5$

$Z_c = X_b + X_d = 2$

$$Z_a + Z_c = \left\lfloor \frac{n-4}{4} \right\rfloor = 7$$

$Y_a = X_a + X_b = 5$

$Y_c = X_c + X_d = 3$

$$Y_a + Y_c = \left\lfloor \frac{n-2}{4} \right\rfloor = 8$$

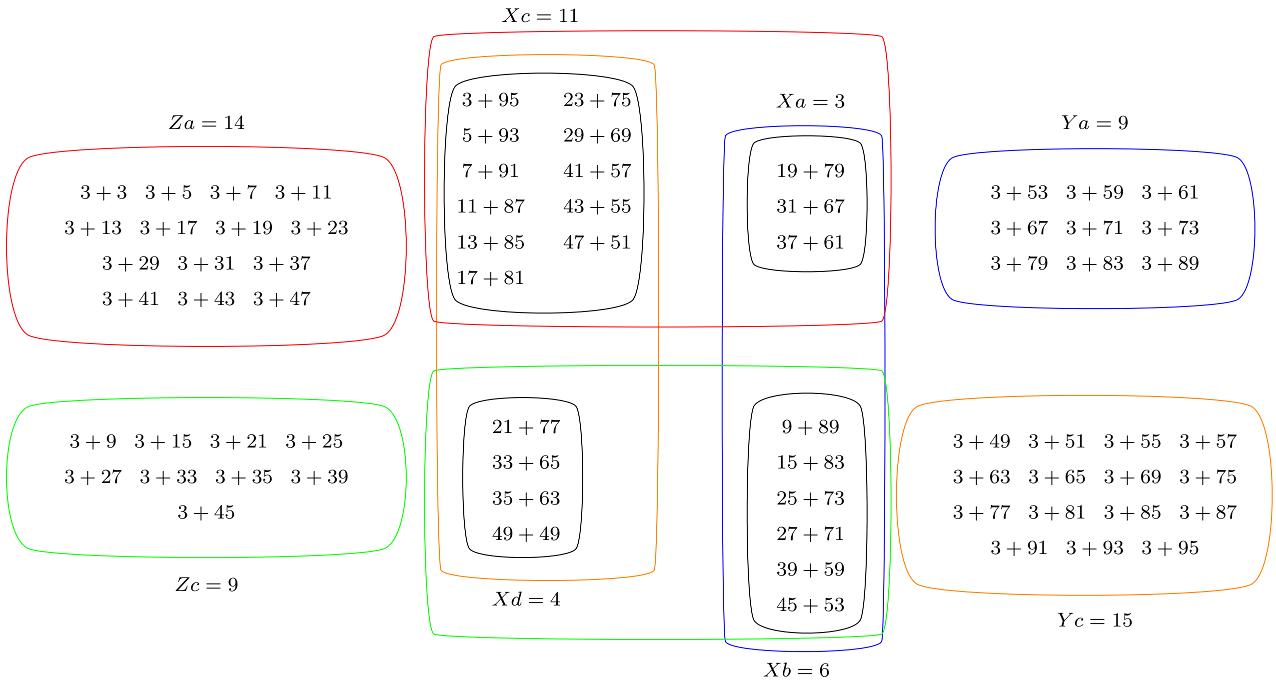
$X_a = 4$

$X_b = 1$

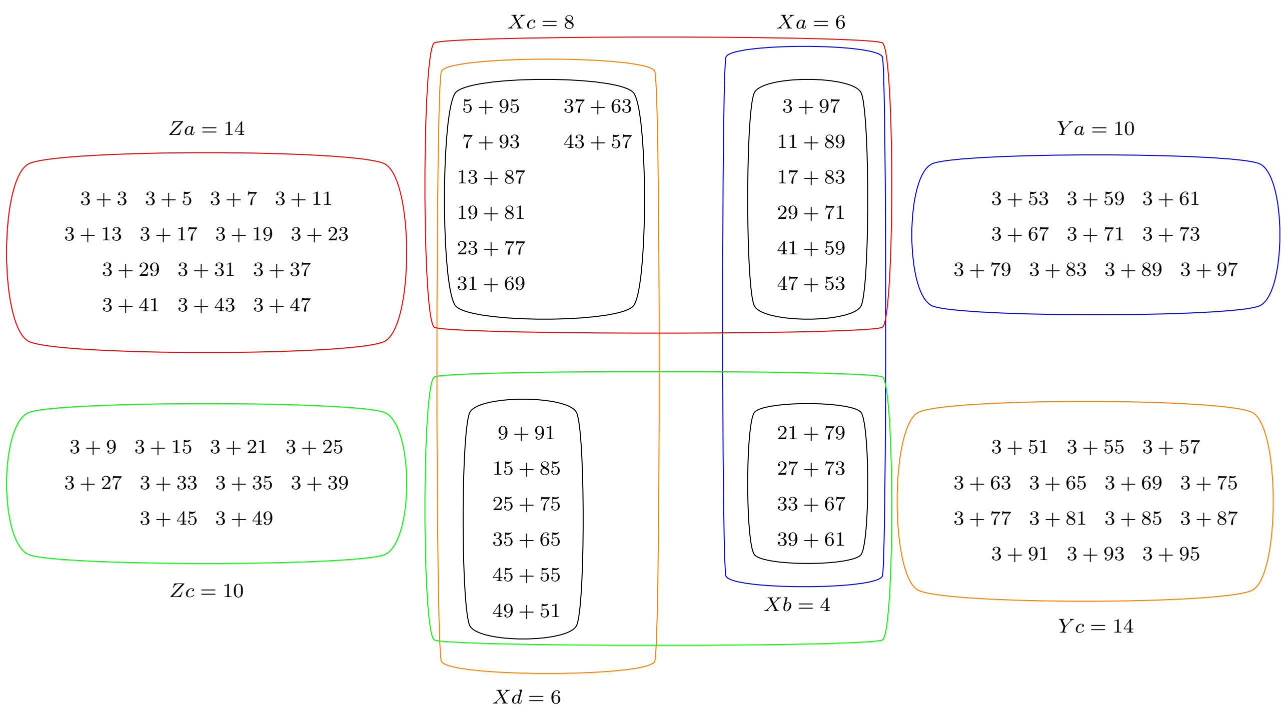
$X_c = 2$

$X_d = 1$

- **Case** $n = 98$



- **Case** $n = 100$



Annex 3 : rewriting rules and automata theory

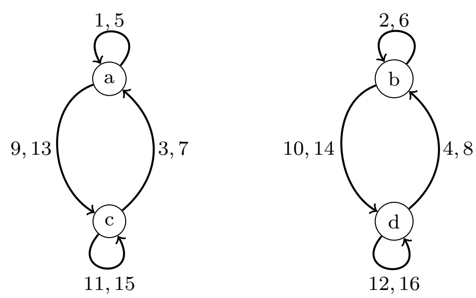
This annex studies variables $X_a(n), X_b(n), X_c(n), X_d(n)$ evolution that we deduce from analyzing words rewriting rules, presented from automata theory point of view.

If we consider each line of the global array as a word on alphabet $A = \{a, b, c, d\}$, $n+2$ even number's word is obtained by the following way from even number n's word :

- first letter of $n+2$'s word is a if $n-3$ is prime and c otherwise (this first letter is the only one that introduces indeterminism because it doesn't belong to n's word and it can't be deduced from n's word letters ;
- following letters of $n+2$'s word are obtained by applying parallely following rewriting rules to n's word :

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

  We can represent those rewriting rules by the two above deterministic automata, from which edges are labelled by applicable rules to one given letter of n's word :



- finally, one letter concatenation at the end of the word, in case if n is an even double (i.e. of the form $4k$) obeys to following rule :
  - if n's word has an a or b letter as last letter, after having obtained $n+2$'s word by applying rewriting rules, we concatenate a letter a to it (at last position) ;
  - if n's word has a c or d letter as last letter, after having obtained $n+2$'s word by applying rewriting rules, we concatenate a letter d to it (at last position).

If we take as convention to notate $X_{xy}(n)$ occurences number of xy letters sequences in n's word, the following equalities provide a, b, c or d letters numbers evolution when passing from n's word to $n+2$'s word.

$$X_a(n+2) = X_a(n) - X_{ca}(n) - X_{da}(n) + X_{ac}(n) + X_{bc}(n) + \delta_{n-3\_is\_prime}(n) + \delta_a(n)$$
$$X_b(n+2) = X_b(n) - X_{cb}(n) - X_{db}(n) + X_{ad}(n) + X_{bd}(n) + \delta_{n-3\_is\_prime}(n)$$
$$X_c(n+2) = X_c(n) - X_{ac}(n) - X_{bc}(n) + X_{ca}(n) + X_{da}(n) + \delta_{n-3\_is\_prime}(n)$$
$$X_d(n+2) = X_d(n) - X_{ad}(n) - X_{bd}(n) + X_{cb}(n) + X_{db}(n) + \delta_{n-3\_is\_prime}(n) + \delta_d(n)$$

with $\delta_a(n)$ that is equal to 1 if n is an even number (i.e. of the form $4k$) and if n's word last letter is an a or b letter, $\delta_d(n)$ that is equal to 1 if n is an even number (i.e. of the form $4k$) and if n's word last letter is a c or d letter and finally with $\delta_{n-3}(n)$ that is equal to 1 if $n-3$ is prime and equal to 0 otherwise.

Bibliographie

[1] J. Barkley Rosser, Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois Journal of Mathematics, 1962.

Goldbach conjecture, rewriting, contradiction

Denise Vella-Chemla

March 30, 2014

1 16 rewriting rules

We remind that we choosed to represent that an integer is prime by boolean 0 and the fact that it is compound by boolean 1.

We also decided to use the following conventions$(3 \leqslant p \leqslant n/2)$:

- a letter symbolizes an n decomposition of the form $p+q$ with p and q primes ;
- b letter symbolizes an n decomposition of the form $p+q$ with p compound and q prime ;
- c letter symbolizes an n decomposition of the form $p+q$ with p prime and q compound ;
- d letter symbolizes an n decomposition of the form $p+q$ with p and q compound.

a letter codes $\begin{pmatrix}0\\0\end{pmatrix}$ matrix, and respectively b $\begin{pmatrix}0\\1\end{pmatrix}$, c $\begin{pmatrix}1\\0\end{pmatrix}$ and finally d $\begin{pmatrix}1\\1\end{pmatrix}$

Example : Hereafter the word $m_{abcd}(40)$.

40	37	35	33	31	29	27	25	23	21
	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0
	3	5	7	9	11	13	15	17	19
$m_{abcd}(40)$	a	c	c	b	a	c	d	a	c

In the following, we use the operation on matrices defined as :

$$\begin{pmatrix}x_1\\x_2\end{pmatrix}.\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{pmatrix}x_1\\y_2\end{pmatrix}$$

Our operation provides 16 rewriting rules of couples of letters, that seem relevant to study Goldbach conjecture :

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) $dd \to d$

2 Reminders from language theory

An alphabet is a finite set of symbols.

Alphabets used in the following are : $A = \{a, b, c, d\}$, $A_{ab} = \{a, b\}$, $A_{cd} = \{c, d\}$, $A_{ac} = \{a, c\}$ and $A_{bd} = \{b, d\}$.

A word on X alphabet is a finite and ordered sequence, eventually empty, of alphabet elements. It's a letters concatenation. We note X^* the set of words over X alphabet.

A word is called a prefix of another one if it contains, on all its length, the same letters as it at same positions (X being an alphabet and $w, u \in X^*$. u is a prefix of w if and only if $\exists v \in X^*$ such that $w = u.v$).

3 Observing words

Let us observe words associated with even numbers between 6 and 80.

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

FIGURE 1 : words associated to even numbers between 6 and 36

We see that words in diagonals contain either a and b letters exclusively, or c and d letters exclusively.

4 Words properties

Diagonal words (diagonals) have their letters either in A_{ab} alphabet or in A_{cd} alphabet.

Every diagonal is a prefix of the following one that is defined on the same alphabet.

Indeed, a diagonal code decompositions that have the same second sommant and that have a first sommant that is an odd number from the list of successive odd numbers beginning at 3.

For instance, diagonal *aaabaa* beginning with first letter of 26's word on figure 1 code the following decompositions : 3+23, 5+23, 7+23, 9+23, 11+23 and 13+23.

Thus, diagonals on A_{ab} alphabet "code" decompositions that have a same second sommant which is prime ; their letters code either by a letters corresponding to prime numbers, or by b letters corresponding to compound ones the primality characters of odd numbers (the first sommants), beginning at 3.

Diagonals on A_{cd} alphabet "code" on their side decompositions that have a same second sommant which is compound ; their letters code either by c letters corresponding to prime numbers, or by d letters corresponding to compound ones the primality characters of odd numbers (the first sommants), beginning at 3.

Vertical words have their letters either in A_{ac} alphabet or in A_{bd} alphabet. A vertical word code decompositions that have same first sommant. Every vertical word is contained in a vertical word that is "on its left side" and that is defined on the same alphabet.

5 Some regularities

We observe some regularities easily explanables, that link together letters numbers of each kind that appear in an even number word or in a certain portion of first column of letters. Figure 2 above presents schematically variable names that will be useful to conduct reasoning :

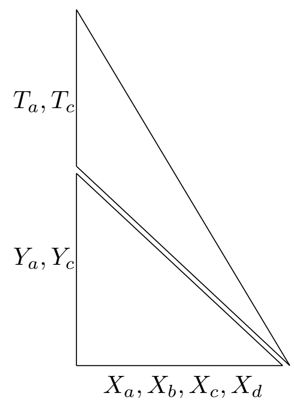


FIGURE 2 : linked variables

Global triangle contains words associated to even numbers from 6 to n.

X_a, X_b, X_c et X_d count a, b, c or d letters numbers in n word.

T_a and T_c count numbers of a or c letters that are first letters of words associated with even numbers between 6 and $2\left\lceil\frac{n+2}{4}\right\rceil$.

T_a thus corresponds to decompositions of the form $n' = 3 + p_i$, p_i prime, $n' \leqslant 2\left\lceil\frac{n+2}{4}\right\rceil$. For instance, if $n = 34$, $T_a = \#\{3+3, 3+5, 3+7, 3+11, 3+13\}$.

T_a thus corresponds to decompositions of the form $n' = p_i + p_i$, p_i prime for $n' < n$. For instance, if $n = 34$, $T_a = \#\{3+3, 5+5, 7+7, 11+11, 13+13\}$.

T_c corresponds to decompositions of the form $n' = 3 + c_i$, c_i compound $n' \leqslant 2\left\lceil\frac{n+2}{4}\right\rceil$. For instance, if $n = 34$, $T_c = \#\{9+9, 15+15\}$.

Y_a and Y_c count numbers of a or c letters that are first letters of words associated to even numbers between $2\left\lceil\frac{n+2}{4}\right\rceil + 2$ and n.

The trivial one-to-one mapping on the decompositions second term permits to explain easily why $Y_a = X_a + X_b$ or $Y_c = X_c + X_d$. The simple reading of sets defined in extension suffices to convince oneself.

$$
\begin{aligned}
Y_a &= \#\{3+17, 3+19, 3+23, 3+29, 3+31\} \\
X_a &= \#\{3+31, 5+29, 11+23, 17+17\} \\
X_b &= \#\{15+19\} \\
\\
Y_c &= \#\{3+21, 3+25, 3+27\} \\
X_c &= \#\{7+27, 13+21\} \\
X_d &= \#\{9+25\}
\end{aligned}
$$

Hereafter two figures to “fix ideas” for even numbers $n = 32$ or $n = 34$.

	6 :	a							
	8 :	a							
	10 :	a	a						
$T_a = 5$	12 :	c	a						
$T_c = 2$	14 :	a	c	a					
	16 :	a	a	c					
	18 :	c	a	a	d				
	20 :	a	c	a	b				
	22 :	a	a	c	b	a			
$Y_a = 4$	24 :	c	a	a	d	a			
$Y_c = 3$	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	$\leftarrow X_a = 2, X_b = 2, X_c = 3, X_d = 0$

FIGURE 3 : premier exemple : $n = 32$

	6 :	a								
	8 :	a								
	10 :	a	a							
$T_a = 5$	12 :	c	a							
$T_c = 2$	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			
$Y_a = 5$	28 :	c	a	c	b	a	c			
$Y_c = 3$	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	$\leftarrow X_a = 4, X_b = 1, X_c = 2, X_d = 1$

FIGURE 4 : second example : $n = 34$

Following constraints are always satisfied :

$$Y_a = X_a + X_b$$
$$Y_c = X_c + X_d$$
$$T_a + T_c + Y_a + Y_c + \epsilon = 2(X_a + X_b + X_c + X_d)$$

$\epsilon = 1$ if n is an odd double, $\epsilon = 0$ otherwise.

We saw that constraints above can be easily understood if we come back to numbers of decompositions they represent and if we use “Cantor-like” one-to-one mappings.

Different words letters are thus very *intricated* and those intrications have as consequence that every word contains at least one a letter.

We are going to prove this using a *reductio ad absurdum* reasoning in section 7.

6 Cantor one-to-one mappings visualization

We provide above Cantor one-to-one mappings for cases $n = 32$ and $n = 34$.

One-to-one mapping f that permits to pass from line 2 to line 1 is such that $f(a) = f(c) = a$ et $f(b) = f(d) = c$.

One-to-one mapping g that permits to pass from line 2 to line 3 is such that $g(a) = g(b) = a$ et $g(c) = g(d) = c$.

It’s the double decomposition $3 + n/2$ in the case where n is an odd’s double that necessitates introduction of the variable ϵ that is equal to 1 in that case and equal to 0 otherwise.

– One-to-one mappings if $n = 32$

	3	3	3	3	3	3	3
1	a	a	a	c	a	a	c
	3	5	7	9	11	13	15
	3	5	7	9	11	13	15
2	a	c	c	b	c	a	b
	29	27	25	23	21	19	17
	29	27	25	23	21	19	17
3	a	c	c	a	c	a	a
	3	3	3	3	3	3	3

– One-to-one mappings if $n = 34$

	3	3	3	3	3	3	3	3
1	a	a	a	c	a	a	c	a
	3	5	7	9	11	13	15	17
	3	5	7	9	11	13	15	17
2	a	a	c	d	a	c	b	a
	31	29	27	25	23	21	19	17
	31	29	27	25	23	21	19	17
3	a	a	c	c	a	c	a	a
	3	3	3	3	3	3	3	3

7 Looking for a contradiction

Let us imagine that a word m_n is associated to an even number n that contradicts Goldbach conjecture, i.e. m_n doesn't contain any a letter (we remind that a letter symbolizes sum of two primes).

m_n containing no a, we have $X_a = 0$. But since $Y_a = X_a + X_b$, we deduce $Y_a = X_b$. Identifying Y_a to X_b and Y_c to $X_c + X_d$ in the last constraint always satisfied provided in the paragraph above, one obtains the following equalities :

$$\begin{array}{l} T_a + T_c + Y_a + Y_c + \epsilon = 2(X_a + X_b + X_c + X_d) \\ T_a + T_c + X_b + X_c + X_d + \epsilon = 2X_a + 2X_b + 2X_c + 2X_d \\ T_a + T_c + \epsilon = X_b + X_c + X_d \\ T_a + T_c + \epsilon = X_b + Y_c \end{array}$$

We must now remember what those variables represent :

- $T_a + T_c = (n-4)/4$;
- X_b counts the number of n decompositions of the form of a sum of two odd numbers $p+q$ with $p \leqslant n/2$ compound and q prime ;
- Y_c counts the number of compound odd numbers between $n/2$ and $n-3$.

Number X_b of n decompositions of the form of a sum of two odd numbers $p+q$ with $p \leqslant n/2$ compound and q prime being necessarily lesser than the number of primes between $n/2$ and $n-3$, we have $X_b < Y_a$ (we used here a sort of inverted "pigeonhole principle" : if one puts 0 or 1 object in k holes, there can't be more objects than holes, i.e. more than k objects). But the number of prime numbers contained in an interval $[2k+3, 4k+1]$ is always lesser than the number of compound odd numbers contained in this interval for $k > 25$. In those cases, $Y_a < Y_c$ and $X_b + Y_c < Y_a + Y_c < 2Y_c$.

But, for all integers greater than a certain small integer (such that 100), $(n-4)/4$ is greater than $2Y_c$. This ensures we never have $T_a + T_c + \epsilon = X_b + Y_c$ that should result from the absence of an a letter in a word.

We reached a contradiction that would be a consequence of the absence of an a letter in a word. This brings the impossibility that an even number contradict Goldbach conjecture. Rewriting rules intricate totally words letters in such a manner that their numbers must mandatory respect certain constraints. This work can be localized in a lexical theory of numbers, according to which numbers are words. This theory relies on the fact that letters order in words is primordial.

Goldbach conjecture (June 7, 1742)

- 271 years old.
- **Statement** : Every even number (n) greater than 2 is the sum of two primes.
- $\Longleftrightarrow$ Every integer greater than 1 is the average of two primes ($\frac{1}{2}p_1 + \frac{1}{2}p_2$).
- $$\begin{aligned} 98 &= 19 + 79 \\ &= 31 + 67 \\ &= 37 + 61 \end{aligned}$$

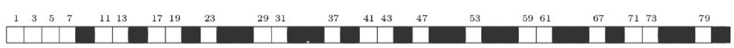
Laisant's strip

- **Charles-Ange Laisant** : Sur un procédé expérimental de vérification de la conjecture de Goldbach, Bulletin de la SMF, 25, 1897.

- *"This famous empirical theorem : every even number is the sum of two primes, whose demonstration seems to overpass actual possibilities, has generated a certain amount of works and contestations. Lionnet tried to establish the proposition should probably be false. M. Georg Cantor verified it numerically until 1000, giving for each even number all decompositions in two primes, and he noticed that this decompositions number is always growing in average, even if it presents big irregularities."*

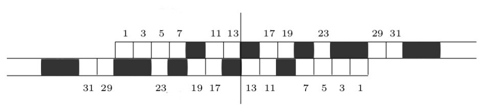
Laisant's strips

- *"Let us show a process that would permit to make without computing the experimental verification we mentioned, and to have, for each even number, only inspecting a figure, all the decompositions. Let us suppose that on a strip constituted by pasted squares, representing odd successive numbers, we had constructed the Erathosthene's sieve, shading compound numbers, until any limit* $2n$*."*



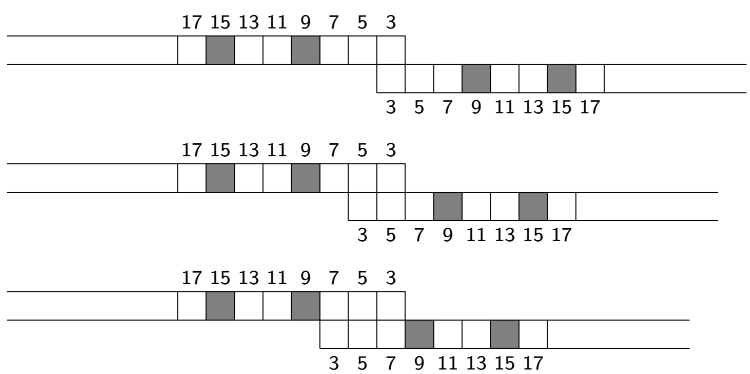
Laisant's strips

- *"If we constructed two similar strips, and if we put the second one behind the first one returning it and making correspond* 1 *cell with* $2n$ *cell, it is evident that if Goldbach theorem was true for* $2n$*, there would be somewhere two white cells corresponding to each other ; and all the couples of white cells will give diverse decompositions. We will even have them reading only the half of the figure, because of the symmetry around the middle. In this way, verification concerning* 28 *even number will give figure above and will show that we have* $28 = 5 + 23 = 11 + 17$*."*



Laisant's strips

- *"We understand that, strips being constructed in advance, a single shift permits to pass from one number to another, verifications are very rapid."*



Boolean algebra

- We represent primality by booleans.
- 0 signifies *is prime*, while 1 signifies *is compound*.
- $23 \to 0$
- $25 \to 1$
-

3	5	7	9	11	13	15	17	19	21	23	25	27	29	...
0	0	0	1	0	0	1	0	0	1	0	1	1	0	...

A space copy : 2 booleans matrices

- We represent n decompositions in sums of two odd numbers by 2 booleans matrices (the boolean in the bottom corresponding to the smaller number).
- $28 = \underset{p}{5} + \underset{p}{23} \rightarrow \begin{pmatrix} 0 \\ 0 \end{pmatrix} = a$
- $28 = \underset{c}{9} + \underset{p}{19} \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} = b$
- $28 = \underset{p}{3} + \underset{c}{25} \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} = c$
- $40 = \underset{c}{15} + \underset{c}{25} \rightarrow \begin{pmatrix} 1 \\ 1 \end{pmatrix} = d$

40, 42 and 44 words

40									
	37	35	33	31	29	27	25	23	21
	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0
	3	5	7	9	11	13	15	17	19
	a	*c*	*c*	*b*	*a*	*c*	*d*	*a*	*c*

42										
	39	37	35	33	31	29	27	25	23	21
	1	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21
	c	*a*	*c*	*d*	*a*	*a*	*d*	*c*	*a*	*d*

44										
	41	39	37	35	33	31	29	27	25	23
	0	1	0	1	1	0	0	1	1	0
	0	0	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21
	a	*c*	*a*	*d*	*c*	*a*	*b*	*c*	*c*	*b*

Operations on matrices

- General rule :

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ y_2 \end{pmatrix}$$

- Example :

$$\underbrace{\begin{pmatrix} 1 \\ 0 \end{pmatrix}}_{c} \cdot \underbrace{\begin{pmatrix} 0 \\ 1 \end{pmatrix}}_{b} = \underbrace{\begin{pmatrix} 1 \\ 1 \end{pmatrix}}_{d}$$

- Particular rules :

$aa \to a$	$ba \to a$	$ca \to c$	$da \to c$
$ab \to b$	$bb \to b$	$cb \to d$	$db \to d$
$ac \to a$	$bc \to a$	$cc \to c$	$dc \to c$
$ad \to b$	$bd \to b$	$cd \to d$	$dd \to d$

Let us observe words : 16 rewriting rules.

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

Language theory reminders

- An alphabet is a finite set of symbols.
- Alphabets used in the following are :
$A = \{a, b, c, d\}, A_{ab} = \{a, b\}, A_{cd} = \{c, d\}, A_{ac} = \{a, c\}$ and $A_{bd} = \{b, d\}$.
- A word on X alphabet is a finite and ordered sequence, eventually empty, of alphabet elements. It's a letters concatenation. We note X^* set of words on X alphabet.
- A word is a prefix of another one if it contains, on all its length, the same letters at the same positions (X being an alphabet and $w, u \in X^*$. u is a prefix of w if and only if $\exists v \in X^*$ such that $w = u.v$)

Let us observe diagonal words.

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

Diagonal words properties

- Diagonal words (diagonals) have their letters either in A_{ab} alphabet or in A_{cd} alphabet.
- Each diagonal is a prefix of the following diagonal using same alphabet.
- Indeed, a diagonal codes decompositions that have the same second term and that have as first term an odd number from sequence of odd numbers beginning with 3.
- For instance, diagonal *aaaba*, that begins with an *a* letter, first letter of 26's word on figure 1 codes following decompositions : $3+23, 5+23, 7+23; 9+23, 11+23$ and $13+23$.

Diagonal word properties

- Thus, diagonals on A_{ab} alphabet "code" decompositions that have a second term that is prime ; letters of such diagonals code either by a letters corresponding to prime numbers, or by b letters corresponding to compound numbers, the sequence of primality characters of odd numbers, beginning by 3.

- On the other side, diagonals on A_{cd} alphabet "code" decompositions that have a second term that is compound ; letters of such diagonals code either by c letters corresponding to prime numbers, or by d letters corresponding to compound numbers, the sequence of primality characters of odd numbers, beginning by 3.

Let us observe vertical words.

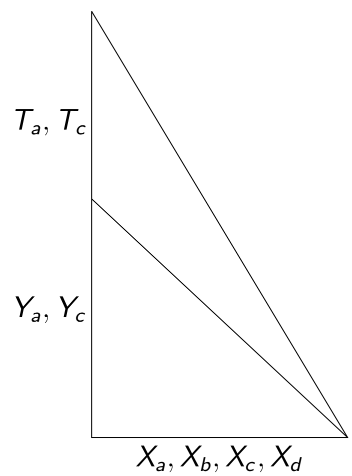
6 :	a							
8 :	a							
10 :	a	a						
12 :	c	a						
14 :	a	c	a					
16 :	a	a	c					
18 :	c	a	a	d				
20 :	a	c	a	b				
22 :	a	a	c	b	a			
24 :	c	a	a	d	a			
26 :	a	c	a	b	c	a		
28 :	c	a	c	b	a	c		
30 :	c	c	a	d	a	a	d	
32 :	a	c	c	b	c	a	b	
34 :	a	a	c	d	a	c	b	a

(and vertical "slices")

Vertical words properties

- Vertical words have their letters either in A_{ac} alphabet or in A_{bd} alphabet.
- A vertical word codes successive decompositions that have the same first term.
- Every vertical word is contained in a vertical word that is on its left side and that is defined on the same alphabet.

n doesn't verify Goldbach conjecture.



n doesn't verify Goldbach conjecture.

	6 :	a							
	8 :	a							
	10 :	a	a						
$T_a = 5$	12 :	c	a						
$T_c = 2$	14 :	a	c	a					
	16 :	a	a	c					
	18 :	c	a	a	d				
	20 :	a	c	a	b				
	22 :	a	a	c	b	a			
$Y_a = 4$	24 :	c	a	a	d	a			
$Y_c = 3$	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	$\leftarrow X_a = 2, X_b = 2, X_c = 3, X_d = 0$

n doesn't verify Goldbach conjecture.

	6 :	a								
	8 :	a								
	10 :	a	a							
$T_a = 5$	12 :	c	a							
$T_c = 2$	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			
$Y_a = 5$	28 :	c	a	c	b	a	c			
$Y_c = 3$	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	$\leftarrow X_a = 4, X_b = 1, X_c = 2, X_d = 1$

Cantor-like one-to-one mappings

- T_a counts decompositions of the form $n' = 3 + p_i$, p_i prime, $n' \leqslant 2\left\lceil \frac{n+2}{4} \right\rceil$.
- For instance, if $n = 34$, $T_a = \#\{3+3, 3+5, 3+7, 3+11, 3+13\}$.
- T_c, on its side, counts decompositions of the form $n' = 3 + c_i$, c_i compound $n' \leqslant 2\left\lceil \frac{n+2}{4} \right\rceil$.
- For instance, if $n = 34$, $T_c = \#\{3+9, 3+15\}$.

Cantor-like one-to-one mappings

- The trivial one-to-one mapping on decompositions second term permits to easily explain why $Y_a = X_a + X_b$ or $Y_c = X_c + X_d$. The simple presentation of sets in extension suffices to convince oneself.

- $$\begin{aligned} Y_a &= \#\{3+17, 3+19, 3+23, 3+29, 3+31\} \\ X_a &= \#\{3+31, 5+29, 11+23, 17+17\} \\ X_b &= \#\{15+19\} \\ \\ Y_c &= \#\{3+21, 3+25, 3+27\} \\ X_c &= \#\{7+27, 13+21\} \\ X_d &= \#\{9+25\} \end{aligned}$$

Cantor-like one-to-one mappings

- One-to-one mapping f that permits to pass from line 2 to line 1 of the table above is such that $f(a) = f(c) = a$ and $f(b) = f(d) = c$.

- One-to-one mapping g that permits to pass from line 2 to line 3 is such that $g(a) = g(b) = a$ and $g(c) = g(d) = c$.

- It's the $3 + n/2$ decomposition duplication in cases of odd numbers doubles that necessitates the introduction of ϵ variable that equals 1 in those cases and 0 in others.

Cantor-like one-to-one mappings

1	3 *a* 3	3 *a* 5	3 *a* 7	3 *c* 9	3 *a* 11	3 *a* 13	3 *c* 15
2	3 *a* 29	5 *c* 27	7 *c* 25	9 *b* 23	11 *c* 21	13 *a* 19	15 *b* 17
3	29 *a* 3	27 *c* 3	25 *c* 3	23 *a* 3	21 *c* 3	19 *a* 3	17 *a* 3

1	3 *a* 3	3 *a* 5	3 *a* 7	3 *c* 9	3 *a* 11	3 *a* 13	3 *c* 15	3 *a* 17
2	3 *a* 31	5 *a* 29	7 *c* 27	9 *d* 25	11 *a* 23	13 *c* 21	15 *b* 19	17 *a* 17
3	31 *a* 3	29 *a* 3	27 *c* 3	25 *c* 3	23 *a* 3	21 *c* 3	19 *a* 3	17 *a* 3

n doesn't verify Goldbach conjecture.

- Following constraints are always satisfied :

$$\begin{array}{l} Y_a = X_a + X_b \\ Y_c = X_c + X_d \\ T_a + T_c + Y_a + Y_c + \epsilon = 2(X_a + X_b + X_c + X_d) \end{array}$$

- $\epsilon = 1$ si n est un double d'impair, $\epsilon = 0$ sinon.
- m_n contains no a, we have $X_a = 0$.
- But since $Y_a = X_a + X_b$, we also have $Y_a = X_b$.

n doesn't verify Goldbach conjecture.

- Identifying Y_a with X_b and Y_c with $X_c + X_d$ in last constraint, one obtains the following equalities :

$$\begin{aligned} T_a + T_c + Y_a + Y_c + \epsilon &= 2(X_a + X_b + X_c + X_d) \\ T_a + T_c + X_b + X_c + X_d + \epsilon &= 2X_a + 2X_b + 2X_c + 2X_d \\ T_a + T_c + \epsilon &= X_b + X_c + X_d \\ T_a + T_c + \epsilon &= X_b + Y_c \end{aligned}$$

- We must now remind the variables meaning :
  - $T_a + T_c = \left\lfloor \frac{n-4}{4} \right\rfloor$;
  - X_b counts the number of n decompositions as a sum of two odd numbers $p+q$ with $p \leqslant n/2$ compound and q prime.
  - Y_c counts the number of odd compound numbers between $n/2$ and $n-3$.

n doesn't verify Goldbach conjecture.

- The number X_b of n decompositions de n as a sum of two odd numbers $p+q$ with $p \leqslant n/2$ compound and q prime being necessarily lesser than the number of primes between $n/2$ and $n-3$, we have $X_b < Y_a$ (we used here a sort of inverted pigeonhole principle : if we put 0 or 1 object in k holes, there can be more objects than holes, i.e. more than k objects). But the number of prime numbers contained in an interval is always lesser than the number of odd compound numbers contained in the same interval (since $n > 100$). Thus $Y_a < Y_c$. Thus $X_b + Y_c < Y_a + Y_c < 2Y_c$.
- $\left\lfloor \dfrac{n-4}{4} \right\rfloor$ is greater than $2Y_c$ for all integer greater than a certain one that is small (such as 100). This ensures that we never have $T_a + T_c + \epsilon = X_b + Y_c$ which would result from the absence of a letter in a word.

Conclusion

- We used a 4 letters language to represent n decompositions as two odd numbers sums.
- Rewriting rules preserve "letters slices" width.
- We use a lexical theory of numbers, according to which numbers are words.
- We have always to well observe letters order in words.

Goldbach's conjecture (7, june 1742)

- 271 years old
- **Postulate** : Every even number (n) greater than 2 is the sum of two primes $(n = p + q)$.
- p and q are odd ; $3 \leqslant p \leqslant n/2$ and $n/2 \leqslant q \leqslant n - 3$
- $$\begin{aligned} 98 &= 19 + 79 \\ &= 31 + 67 \\ &= 37 + 61 \end{aligned}$$

Booleans

- One represents primality by booleans.
- 0 significates *is prime*, 1 significates *is compound*.
- $23 \rightarrow 0$
- $25 \rightarrow 1$
-

3	5	7	9	11	13	15	17	19	21	23	25	27	29	...
0	0	0	1	0	0	1	0	0	1	0	1	1	0	...

The space's copy : 4 letters for 4 possibilities

- One represents n's decompositions in sums of two odd numbers by letters.
- $28 = \underset{p}{5} + \underset{p}{23} = \textit{prime} + \textit{prime} = a$
- $28 = \underset{c}{9} + \underset{p}{19} = \textit{compound} + \textit{prime} = b$
- $28 = \underset{p}{3} + \underset{c}{25} = \textit{prime} + \textit{compound} = c$
- $40 = \underset{c}{15} + \underset{c}{25} = \textit{compound} + \textit{compound} = d$

40 and 42 words

40	37	35	33	31	29	27	25	23	21
	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0
	3	5	7	9	11	13	15	17	19
	a	*c*	*c*	*b*	*a*	*c*	*d*	*a*	*c*

42	39	37	35	33	31	29	27	25	23	21
	1	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21
	c	*a*	*c*	*d*	*a*	*a*	*d*	*c*	*a*	*d*

Let us observe diagonal words

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

Diagonal words properties

- Diagonal words have their letters either in A_{ab} alphabet or in A_{cd} alphabet.
- Indeed, a diagonal codes decompositions that have the same second sommant and that have as first sommant an odd number from list of successive odd numbers beginning at 3.
- For instance, *aaaba* diagonal, that begins at th *a* first letter of 26's word codes les decompositions $3 + 23, 5 + 23, 7 + 23, 9 + 23, 11 + 23$ and $13 + 23$.

Projection P

$H_{34,3}$ $\quad Z_a = 5$, $Z_c = 2$

6 : a
8 : a
10 : a a
12 : c a
14 : a c a
16 : a a c
18 : c a a d

$B_{34,3}$ $\quad Y_a = 5$, $Y_c = 3$

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 $\leftarrow X_a = 4, X_b = 1$
$X_c = 2, X_d = 1$

Example

- Entanglement $Y_a(n), X_a(n), X_b(n)$

$$\begin{aligned}
Y_a(34) &= \#\{3+17, 3+19, 3+23, 3+29, 3+31\}\\
\\
X_a(34) &= \#\{3+31, 5+29, 11+23, 17+17\}\\
X_b(34) &= \#\{15+19\}
\end{aligned}$$

- Entanglement $Y_c(n), X_c(n), X_d(n)$

$$\begin{aligned}
Y_c(34) &= \#\{3+21, 3+25, 3+27\}\\
\\
X_c(34) &= \#\{7+27, 13+21\}\\
X_d(34) &= \#\{9+25\}
\end{aligned}$$

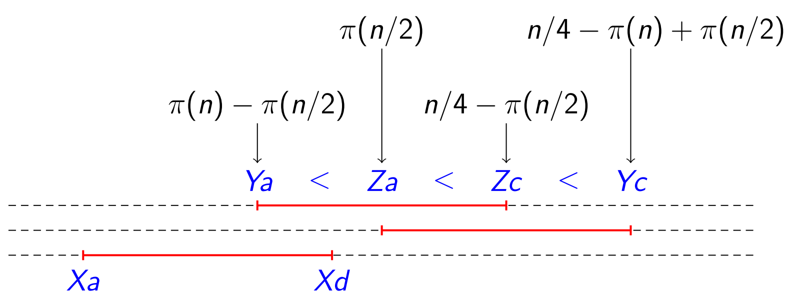
Variables entanglement properties

- $$Y_a(n) = X_a(n) + X_b(n) \quad (1)$$
- $$Y_c(n) = X_c(n) + X_d(n) \quad (2)$$
- $$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \quad (3)$$
- $$X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \quad (4)$$
- $$Z_a(n) + Z_c(n) = \left\lfloor \frac{n-4}{4} \right\rfloor \quad (5)$$

Variables entanglement properties

- $$X_a(n) + X_c(n) = Z_a(n) + \delta_{2p}(n) \qquad (6)$$
  with $\delta_{2p}(n)$ that is equal to 1 if n is a prime double and that is equal to 0 otherwise.
- $$X_b(n) + X_d(n) = Z_c(n) + \delta_{2c-imp}(n) \qquad (7)$$
  with $\delta_{2c-imp}(n)$ that is equal to 1 if n is an odd compound number and that is equal to 0 otherwise.
- $$Z_c(n) - Y_a(n) = Y_c(n) - Z_a(n) - \delta_{4k+2}(n) \qquad (8)$$
  with $\delta_{4k+2}(n)$ that is equal to 1 if n is an odd double and that is equal to 0 otherwise.
- $$Z_c(n) - Y_a(n) = X_d(n) - X_a(n) - \delta_{2c-imp}(n) \qquad (9)$$

Gaps entanglements properties



n	X_a	X_b	X_c	X_d	Y_a	Y_c	A	Z_a	Z_c	B	$\delta_{2p}(n)$	$\delta_{2cimp}(n)$	$\delta_{4k+2}(n)$
14	2	0	1	0	2	1	3	2	0	2	1	0	1
16	2	0	1	0	2	1	3	3	0	3	0	0	0
18	2	0	1	1	2	2	4	3	0	3	0	1	1
20	2	1	1	0	3	1	4	3	1	4	0	0	0
22	3	1	1	0	4	1	5	3	1	4	1	0	1
24	3	0	1	1	3	2	5	4	1	5	0	0	0
26	3	1	2	0	4	2	6	4	1	5	1	0	1
28	2	1	3	0	3	3	6	5	1	6	0	0	0
30	3	0	2	2	3	4	7	5	1	6	0	1	1
32	2	2	3	0	4	3	7	5	2	7	0	0	0
34	4	1	2	1	5	3	8	5	2	7	1	0	1
36	4	0	2	2	4	4	8	6	2	8	0	0	0
38	2	2	5	0	4	5	9	6	2	8	1	0	1
40	3	1	4	1	4	5	9	7	2	9	0	0	0
42	4	0	3	3	4	6	10	7	2	9	0	1	1
44	3	2	4	1	5	5	10	7	3	10	0	0	0
46	4	2	4	1	6	5	11	7	3	10	1	0	1
48	5	0	3	3	5	6	11	8	3	11	0	0	0
50	4	2	4	2	6	6	12	8	3	11	0	1	1
52	3	3	5	1	6	6	12	8	4	12	0	0	0
54	5	1	3	4	6	7	13	8	4	12	0	1	1
56	3	4	5	1	7	6	13	8	5	13	0	0	0
58	4	3	5	2	7	7	14	8	5	13	1	0	1
60	6	0	3	5	6	8	14	9	5	14	0	0	0
62	3	4	7	1	7	8	15	9	5	14	1	0	1
64	5	2	5	3	7	8	15	10	5	15	0	0	0
66	6	1	4	5	7	9	16	10	5	15	0	1	1
68	2	5	8	1	7	9	16	10	6	16	0	0	0
70	5	3	5	4	8	9	17	10	6	16	0	1	1
72	6	2	4	5	8	9	17	10	7	17	0	0	0
74	5	4	6	3	9	9	18	10	7	17	1	0	1
76	5	4	6	3	9	9	18	11	7	18	0	0	0
78	7	2	4	6	9	10	19	11	7	18	0	1	1
80	4	5	7	3	9	10	19	11	8	19	0	0	0

Variables and gaps entanglement (invariants)

n	$X_a(n)$	$X_b(n)$	$X_c(n)$	$X_d(n)$
999 998	4 206	32 754	37 331	175 708
1 000 000	5 402	31 558	36 135	176 904
9 999 998	28 983	287 084	319 529	1 864 403
10 000 000	38 807	277 259	309 705	1 874 228

n	$Y_a(n)$	$Y_c(n)$	$\left\lfloor \frac{n-2}{4} \right\rfloor$	$Z_a(n)$	$Z_c(n)$	$\left\lfloor \frac{n-4}{4} \right\rfloor$	$\delta_{2p}(n)$	$\delta_{2ci}(n)$	$\delta_{4k+2}(n)$
999 998	36 960	213 039	249 999	41 537	208 461	249 998	0	1	1
1 000 000	36 960	213 039	249 999	41 537	208 462	249 999	0	1	0
9 999 998	316 067	2 183 932	2 499 999	348 511	2 151 487	2 499 998	1	0	1
10 000 000	316 066	2 183 933	2 499 999	348 512	2 151 487	2 499 999	0	1	0

Bijections

- $n = 32$

$a, c \to a$ $b, d \to c$		$a, b \to a$ $c, d \to c$
$3+3$ a	$3+29$ a	$3+29$ a
$3+5$ a	$5+27$ c	$3+27$ c
$3+7$ a	$7+25$ c	$3+25$ c
$3+9$ c	$9+23$ b	$3+23$ a
$3+11$ a	$11+21$ c	$3+21$ c
$3+13$ a	$13+19$ a	$3+19$ a
$3+15$ c	$15+17$ b	$3+17$ a

$Z_a = X_a + X_c = 5$

$Z_c = X_b + X_d = 2$

$$Z_a + Z_c = \left\lfloor \frac{n-4}{4} \right\rfloor = 7$$

$Y_a = X_a + X_b = 4$

$Y_c = X_c + X_d = 3$

$$Y_a + Y_c = \left\lfloor \frac{n-2}{4} \right\rfloor = 7$$

$X_a = 2$

$X_b = 2$

$X_c = 3$

$X_d = 0$

Bijections

- $n = 34$

$a, c \to a$
$b, d \to c$

$a, b \to a$
$c, d \to c$

$3+3$ a	$3+31$ a	$3+31$ a
$3+5$ a	$5+29$ a	$3+29$ a
$3+7$ a	$7+27$ c	$3+27$ c
$3+9$ c	$9+25$ d	$3+25$ c
$3+11$ a	$11+23$ a	$3+23$ a
$3+13$ a	$13+21$ c	$3+21$ c
$3+15$ c	$15+19$ b	$3+19$ a
	$17+17$ a	$3+17$ a

$Z_a = X_a + X_c = 5$
$Z_c = X_b + X_d = 2$

$$Z_a + Z_c = \left\lfloor \frac{n-4}{4} \right\rfloor = 7$$

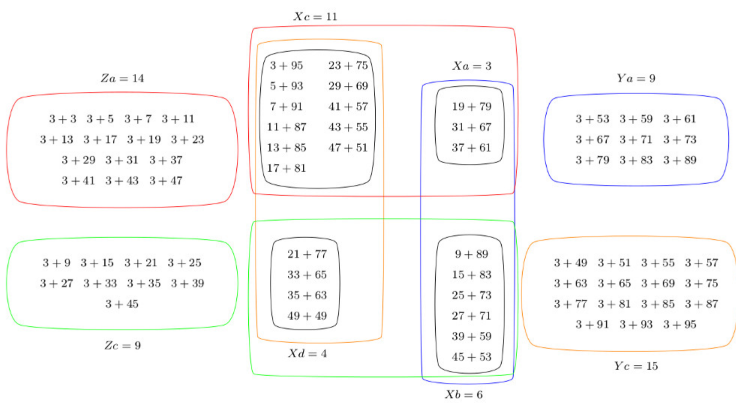
$Y_a = X_a + X_b = 5$
$Y_c = X_c + X_d = 3$

$$Y_a + Y_c = \left\lfloor \frac{n-2}{4} \right\rfloor = 8$$

$X_a = 4$
$X_b = 1$
$X_c = 2$
$X_d = 1$

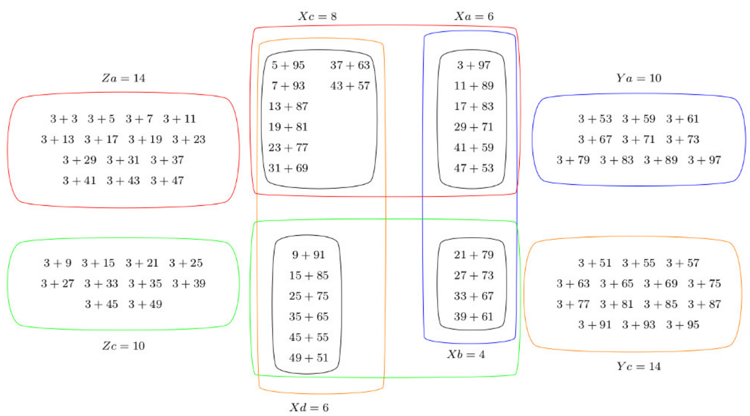
Bijections : double counting visualization

- $n = 98$



Bijections : double counting visualization

- $n = 100$



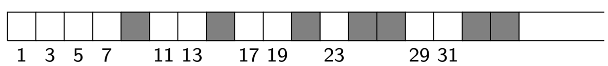
Laisant's strips

- **Charles-Ange Laisant** : Sur un procédé expérimental de vérification de la conjecture de Goldbach, Bulletin de la SMF, 25, 1897.

- *"This famous empirical theorem : every even number is the sum of two primes, whose demonstration seems to overpass actual possibilities, has generated a certain amount of works and contestations. Lionnet tried to establish the proposition should probably be false. M. Georg Cantor verified it numerically until 1000, giving for each even number all decompositions in two primes, and he noticed that this decompositions number is always growing in average, even if it presents big irregularities."*

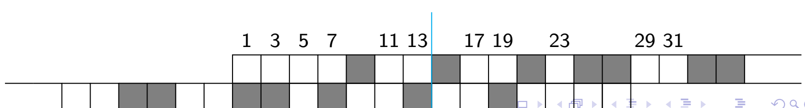
Laisant's strips

- *"Let us show a process that would permit to make without computing the experimental verification we mentioned, and to have, for each even number, only inspecting a figure, all the decompositions. Let us suppose that on a strip constituted by pasted squares, representing odd successive numbers, we had constructed the Erathosthene's sieve, shading compound numbers, until any limit $2n$."*



Laisant's strips

- *"If we constructed two similar strips, and if we put the second one behind the first one returning it and making correspond* 1 *cell with* $2n$ *cell, it is evident that if Goldbach theorem was true for* $2n$*, there would be somewhere two white cells corresponding to each other ; and all the couples of white cells will give diverse decompositions. We will even have them reading only the half of the figure, because of the symmetry around the middle. In this way, verification concerning* 28 *even number will give figure above and will show that we have* $28 = 5 + 23 = 11 + 17$*."*
- *"We understand that, strips being constructed in advance, a single shift permits to pass from one number to another, verifications are very rapid."*



Summary

- $X_a : p + p$
- $X_b : c + p$
- $X_c : p + c$
- $X_d : c + c$
- $Z_a : 3 + p,$ $(p < n/2)$
- $Z_c : 3 + c,$ $(c < n/2)$
- $Y_a : 3 + p,$ $(p \geqslant n/2)$
- $Y_c : 3 + c,$ $(c \geqslant n/2)$
- $\{3+p_k\}$ $Y_a = X_a + X_b$ $\{p+p_i\} \cup \{c+p_j\}$ $(p_i, p_j, p_k \geqslant n/2)$
- $\{3+c_k\}$ $Y_c = X_c + X_d$ $\{p+c_i\} \cup \{c+c_j\}$ $(c_i, c_j, c_k \geqslant n/2)$
- $\{3+p_k\}$ $Z_a = X_a + X_c$ $\{p_i+p\} \cup \{p_j+c\}$ $(p_i, p_j, p_k < n/2)$
- $\{3+c_k\}$ $Z_c = X_b + X_d$ $\{c_i+p\} \cup \{c_j+c\}$ $(c_i, c_j, c_k < n/2)$

Summary

- $Y_a + Y_c = X_a + X_b + X_c + X_d = \left\lfloor \dfrac{n-2}{4} \right\rfloor$

- $Z_a + Z_c = \left\lfloor \dfrac{n-4}{4} \right\rfloor$

- $\left\lfloor \dfrac{n-4}{4} \right\rfloor = Z_a + Z_c \simeq Y_a + Y_c = \left\lfloor \dfrac{n-2}{4} \right\rfloor$

- $Z_c - Y_a \simeq X_d - X_a$
  by definition because $Z_c - Y_a$ corresponds to
  $\{c + p\} \cup \{c + c\} \setminus \{c + p\} \cup \{p + p\}$

Conclusion

- We used a 4 letters language to represent n decompositions as two odd numbers sums.
- We use a lexical theory of numbers, according to which numbers are words.
- We have always to well observe letters order in words.

Ci-dessous Un extrait de la biographie "Poincaré : philosophe et mathématicien" d'Umberto Bottazzini aux éditions Belin Pour la Science.

Au sujet du raisonnement par récurrence : le terrain le plus naturel et le plus favorable pour cette étude est l'arithmétique élémentaire, c'est à dire les opérations mettant en jeu des nombres entiers. Quand nous analysons des opérations telles que l'addition et la multiplication, nous nous rendons compte qu'un type de raisonnement se "retrouve à chaque pas", c'est la démonstration "par récurrence" : "on établit d'abord un théorème pour n égal à 1 ; on montre ensuite que, s'il est vrai de $n-1$, il est vrai de n, et on en conclut qu'il est vrai pour tous les nombres entiers." C'est là le "raisonnement mathématique par excellence", déclare Poincaré. Sa particularité est "qu'il contient, sous une forme condensée, une infinité de syllogismes", et qu'il permet de passer du particulier au général, du fini à l'infini, concept qui apparaît dès les premiers pas de l'arithmétique élémentaire et sans lequel "il n'y aurait pas de science parce qu'il n'y aurait rien de général", mais uniquement des énoncés particuliers. D'où nous vient ce "raisonnement pas récurrence", s'interroge Poincaré ? Certainement pas de l'expérience. Celle-ci peut nous suggérer que la règle est vraie pour les dix ou les cent premiers nombres, mais elle est désarmée face à l'infinité de tous les nombres naturels. Le principe de contradiction (on dirait aujourd'hui le raisonnement par l'absurde) est aussi impuissant : il nous permet d'obtenir certaines vérités, mais non d'en enfermer une infinité en une seule formule. "Cette règle (le raisonnement par récurrence), inaccessible à la démonstration analytique et à l'expérience, est le véritable type du jugement synthétique a priori, conclut Poincaré". L"'irrésistible évidence" avec laquelle ce "principe" s'impose n'est autre que "l'affirmation de la puissance de l'esprit qui se sait capable de concevoir la répétition indéfinie d'un même acte dès que cet acte est une fois possible"...

Deux citations d'Euler, dans "Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs" :

"Cette règle, que je vais expliquer, est à mon avis d'autant plus importante qu'elle appartient à ce genre dont nous pouvons nous assurer de la vérité, sans en donner une démonstration parfaite." Et plus loin, "Ces choses remarquées, il ne sera pas difficile de faire l'application de cette formule à chaque nombre proposé et de se convaincre de sa vérité, par autant d'exemples qu'on voudra développer. Et comme je dois avouer que je ne suis pas en état d'en donner une démonstration rigoureuse, j'en ferai voir sa justesse par un assez grand nombre d'exemples.".

Hardy écrit quant à lui dans son autobiographie Apologie d'un mathématicien :

"Je pense que la réalité mathématique existe en dehors de nous, que notre fonction est de la découvrir ou de l'observer et que les théorèmes que nous démontrons et que nous décrivons avec grandiloquence comme nos créations sont simplement les notes de nos observations."

Indiscernabilité (DV 27/9/2014)

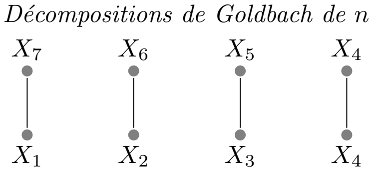
Certains ont dit que ce qui est le plus important à retenir de la Théorie de Galois, c'est l'indiscernabilité des variables d'une équation. On cherche les différents moyens de les échanger, on raisonne sur ces moyens, et l'on en déduit l'existence de solutions ou pas, quelles que soient ces solutions.

C'est souvent profitable de "transposer" (comme on le fait en musique) certaines idées d'un domaine à l'autre ; cela peut permettre de les fixer davantage, de mieux les percevoir, comme une mise au point photographique.

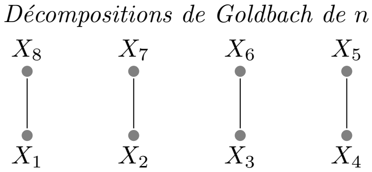
La communication via la toile illustre bien l'idée d'indiscernabilité : j'ai un interlocuteur, comment puis-je être sûre qu'il est bien qui il prétend être, ou bien qui il veut que je croie qu'il soit. Après tout, il a peut-être donné ses pseudo et mot de passe à quelqu'un d'autre, et quand nécessaire, l'autre prend le relais de la communication, un peu comme ces personnes qui "se couvrent" les unes les autres, inventant de faux alibi, pour préserver le secret de leur double (voire multiple) vie. La toile serait ainsi un immense bal masqué : on ne sait pas qui est qui et une bonne intrigue de roman pourrait être la mise en regard de la théorie de Galois et de l'usurpation d'identité ou de l'ubiquité.

Cette incertitude peut être angoissante, ou excitante, ça dépend de la force du caractère de celui ou celle qui reçoit le message, qui maintient le contact.

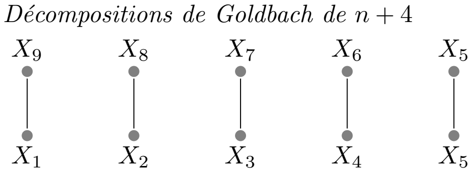
Décompositions de Goldbach de n



Décompositions de Goldbach de $n+2$



Décompositions de Goldbach de $n+4$



EUGÈNE IONESCO

Mathématiques absurdes

Dans La leçon, *Ionesco met en scène une leçon d'arithmétique des plus surprenantes.*

LE PROFESSEUR
Bon. Arithmétisons donc un peu.

L'ÉLÈVE
Oui, très volontiers, monsieur.

LE PROFESSEUR
Cela ne vous ennuierait pas de me dire…

L'ÉLÈVE
Du tout, monsieur, allez-y.

LE PROFESSEUR
Combien font un et un ?

L'ÉLÈVE
Un et un font deux.

LE PROFESSEUR, *émerveillé par le savoir de l'Élève.*
Oh, mais c'est très bien. Vous me paraissez très avancée dans vos études. Vous aurez facilement votre doctorat total, mademoiselle.

L'ÉLÈVE
Je suis bien contente. D'autant plus que c'est vous qui le dites.

LE PROFESSEUR
Poussons plus loin : combien font deux et un ?

L'ÉLÈVE
Trois.

LE PROFESSEUR
Trois et un ?

L'ÉLÈVE
Quatre.

LE PROFESSEUR
Quatre et un ?

L'ÉLÈVE
Cinq.

LE PROFESSEUR
Cinq et un ?

L'ÉLÈVE
Six.

LE PROFESSEUR
Six et un ?

L'ÉLÈVE
Sept.

LE PROFESSEUR
Sept et un ?

L'ÉLÈVE
Huit.

LE PROFESSEUR
Sept et un ?

L'ÉLÈVE

Huit… *bis.*

LE PROFESSEUR

Très bonne réponse. Sept et un ?

L'ÉLÈVE

Huit *ter.*

LE PROFESSEUR

Parfait. Excellent. Sept et un ?

L'ÉLÈVE

Huit *quater.* Et parfois neuf.

LE PROFESSEUR

Magnifique ! Vous êtes magnifique ! Vous êtes exquise. Je vous félicite chaleureusement, mademoiselle. Ce n'est pas la peine de continuer. Pour l'addition, vous êtes magistrale. Voyons la soustraction. Dites-moi, seulement, si vous n'êtes pas épuisée, combien font quatre moins trois ?

L'ÉLÈVE

Quatre moins trois ?… Quatre moins trois ?

LE PROFESSEUR

Oui. Je veux dire : retirez trois de quatre

[…]

L'ÉLÈVE

On peut soustraire deux unités de trois unités, mais peut-on soustraire deux deux de trois trois ? et deux chiffres de quatre nombres ? et trois nombres d'une unité ?

LE PROFESSEUR

Non, mademoiselle.

L'ÉLÈVE

Pourquoi, monsieur ?

LE PROFESSEUR

Parce que, mademoiselle.

L'ÉLÈVE

Parce que quoi, monsieur ? Puisque les uns sont bien les autres ?

LE PROFESSEUR

Il en est ainsi, mademoiselle. Ça ne s'explique pas. Ça se comprend par un raisonnement mathématique intérieur. On l'a ou on ne l'a pas.

L'ÉLÈVE

Tant pis !

LE PROFESSEUR

Écoutez-moi, mademoiselle, si vous n'arrivez pas à comprendre profondément ces principes, ces archétypes arithmétiques, vous n'arriverez jamais à faire correctement un travail de polytechnicien. Encore moins ne pourra-t-on vous charger d'un cours à l'École polytechnique… ni à la maternelle supérieure. Je reconnais que ce n'est pas facile, c'est très, très abstrait… évidemment… mais comment pourriez-vous arriver, avant d'avoir bien approfondi les éléments premiers, à calculer mentalement combien font, et ceci est la moindre des choses pour un ingénieur moyen — combien font, par exemple, trois milliards sept cent cinquante-cinq millions neuf cent quatre-vingt-dix-huit mille deux cent cinquante et un, multiplié par cinq milliards cent soixante-deux millions trois cent trois mille cinq cent huit ?

L'ÉLÈVE, *très vite.*

Ça fait dix-neuf quintillions trois cent quatre-vingt-dix quadrillions deux trillions huit cent quarante-quatre milliards deux cent dix-neuf millions cent soixante-quatre mille cinq cent huit…

LE PROFESSEUR, *étonné.*

Non. Je ne pense pas. Ça doit faire dix-neuf quintillions trois cent quatre-vingt-dix quadrillions deux trillions huit cent quarante-quatre milliards deux cent dix-neuf millions cent soixante-quatre mille cinq cent neuf.

L'ÉLÈVE

… Non… cinq cent huit…

LE PROFESSEUR, *de plus en plus étonné, calcule mentalement.*

Oui… Vous avez raison… le produit est bien… *(Il bredouille inintelligiblement.)*… quintillions, quadrillions, trillions, milliards, millions… *(Distinctement.)*… cent soixante-quatre mille cinq cent huit… *(Stupéfait.)* Mais comment le savez-vous, si vous ne connaissez pas les principes du raisonnement arithmétique ?

L'ÉLÈVE

C'est simple. Ne pouvant me fier à mon raisonnement, j'ai appris par cœur tous les résultats possibles de toutes les multiplications possibles.

LE PROFESSEUR

C'est assez fort… Pourtant, vous me permettrez de vous avouer que cela ne me satisfait pas, mademoiselle,

et je ne vous féliciterai pas : en mathématiques et en arithmétique tout spécialement, ce qui compte — car en arithmétique il faut toujours compter — ce qui compte, c'est surtout de comprendre… C'est par un raisonnement mathématique, inductif et déductif à la fois, que vous auriez dû trouver ce résultat — ainsi que tout autre résultat. Les mathématiques sont les ennemies acharnées de la mémoire, excellente par ailleurs, mais néfaste, arithmétiquement parlant !… Je ne suis donc pas content… ça ne va donc pas, mais pas du tout…

L'ÉLÈVE, *désolée.*

Non, monsieur.

LE PROFESSEUR

Laissons cela pour le moment. Passons à un autre genre d'exercice…

L'ÉLÈVE

Oui, monsieur.

La Leçon

Ci-dessous, quelques extraits de Mathématiques en liberté, de Pierre Cartier, Jean Dhombres, Gerhard Heinzmann et Cédric Villani (DV, 11/4/2014)

(p.26 Pierre Cartier) En exagérant un peu, on pourrait presque définir les mathématiques de cette tradition grecque comme une science dans laquelle on peut se débarrasser du maître. Je veux dire que l'objet des mathématiques, c'est de pouvoir faire seul. La fameuse expression de Cantor : "l'essence des mathématiques, c'est la liberté" est tout à fait pertinente en ce sens que faire des mathématiques, c'est se les approprier, sans pour autant déposséder qui que ce soit.

(p.28 Cédric Villani) C'est l'une des caractéristiques des mathématiques, le fait de se donner une base très resserrée au départ, en ayant en même temps pour ambition de décrire une grande variété de phénomènes.

(p.37 Dominique Lambert) On croit Galilée quand il note que "le grand livre de la nature est écrit en caractères mathématiques" parce que son approche est efficace.

(p.39 Dominique Lambert) Or que font les mathématiciens sinon définir des ensembles d'objets sur lesquels on réalise des opérations où l'on recherche des invariants ?

(p.41 Cédric Villani) La complexité qui nous entoure est complètement affolante si on essaie de se la représenter. [...]
Pour y parvenir, on va simplifier toutes les lignes, tous les chemins, que l'on va remplacer par une droite, une sorte de représentation extrêmement simple ; pour des formes un peu plus complexes, on a le triangle... Et petit à petit, on s'approche de la complexité du monde qui nous entoure, en essayant de se reposer sur un ensemble d'axiomes simples, de règles simples, de règles logiques qui nous permettent de nous y retrouver un peu, de mettre un peu d'ordre dans un monde qui est complètement brutal tant il est indéchiffrable.[...]
On fait une théorie, on observe si ça décrit bien, on change son point de vue et ainsi de suite.

(p.45 Jean Dhombres) Galilée a éliminé tout le "bruit" autour du phénomène. Les mathématiques jouent avec le réel, par la volonté à la fois de pouvoir décrire au plus simple et de pouvoir agir, à la façon d'une expérimentation.

(p.48 Gerhard Heinzmann) Le mathématicien est un homme qui crée un langage qu'il comprend.

(p.62 Jean Dhombres) Fourier ne voulut pas effacer l'étape de calcul, car c'eut été [...] empêcher de comprendre ce que Karl Popper appelle la "logique de la découverte".

(p.69 Henri Poincaré) Ce que nous demandons au mathématicien, c'est de nous aider à voir.

Weil

(p.107 Pierre Cartier) André Weyl a aussi prôné l'idée de considérer Gauss ou Euler comme nos contemporains, comme nos collègues de l'autre côté du couloir. Autrement dit, il faut fréquenter les classiques.

(p.121 Pierre Cartier) Ma force, c'était ma conviction que les mathématiques modernes, en particulier l'algèbre, fourniraient des outils nouveaux.

(p.146 Cédric Villani) A mon niveau, le travail de synthèse de ce qu'ont fait les autres influence beaucoup ma production personnelle.

Relations invariantes
entre nombres de décompositions de Goldbach
codées dans un langage à 4 lettres

Denise Vella-Chemla

Octobre 2014

1 Introduction

La conjecture de Goldbach binaire stipule que tout nombre pair sauf 2 est la somme de deux nombres premiers. Cette note présente un ensemble de relations invariantes découvertes entre certains nombres de décompositions de Goldbach codées dans un langage à 4 lettres. On essaiera d'utiliser ces relations invariantes pour aboutir à une démonstration par récurrence de la conjecture. On s'intéresse aux décompositions d'un nombre pair n en somme de deux nombres impairs $p+q$ avec $3 \leqslant p \leqslant n/2$, $n/2 \leqslant q \leqslant n-3$ et $p \leqslant q$. On appelle p un *sommant de premier rang* et q un *sommant de second rang* de n.

Notations : On désignera par :

- a : une décomposition de n de la forme $p+q$ avec p et q premiers ;
- b : une décomposition de n de la forme $p+q$ avec p composé et q premier ;
- c : une décomposition de n de la forme $p+q$ avec p premier et q composé ;
- d : une décomposition de n de la forme $p+q$ avec p et q composés.

Exemple :

40	3	5	7	9	11	13	15	17	19
	37	35	33	31	29	27	25	23	21
l_{40}	a	c	c	b	a	c	d	a	c

2 Le tableau principal

On désigne par $T = (L, C) = (\ l_{n,m}\ )$ le tableau dont les éléments $l_{n,m}$ sont l'une des lettres a, b, c, d. L'indice n appartient à l'ensemble L des nombres pairs supérieurs ou égaux à 6. L'indice m, appartenant à l'ensemble C des nombres impairs supérieurs ou égaux à 3, est un élément de la liste des sommants de n de premier rang.

Considérons la fonction g définie ainsi :

$$\begin{array}{rccl} g: & 2\mathbb{N} & \rightarrow & 2\mathbb{N}+1 \\ & x & \mapsto & 2\left\lfloor \dfrac{x-2}{4} \right\rfloor + 1 \end{array}$$

$g(6) = 3, g(8) = 3, g(10) = 5, g(12) = 5, g(14) = 7, g(16) = 7, etc.$

La fonction $g(n)$ définit le plus grand des sommants de premier rang associés à n.

Comme l'on ne prend en compte que les décompositions de n de la forme $p+q$ où $p \leqslant q$, seules apparaîtront dans le tableau les lettres $l_{n,m}$ telles que $m \leqslant 2\left\lfloor \dfrac{n-2}{4} \right\rfloor + 1$ de sorte que le tableau contient les éléments suivants : $l_{6,3}, l_{8,3}, l_{10,3}, l_{10,5}, l_{12,3}, l_{12,5}, l_{14,3}, l_{14,5}, l_{14,7}, etc.$

Voici le début du tableau.

L \ C	3	5	7	9	11	13	15	17
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
...								

FIGURE 1 : mots des nombres pairs de 6 à 36

Remarques :

1) les mots situés sur les diagonales du tableau appelés *mots diagonaux* ont leurs lettres soit dans l'alphabet $A_{ab} = \{a, b\}$ soit dans l'alphabet $A_{cd} = \{c, d\}$.

2) un mot diagonal code des décompositions de même sommant de second rang.
Par exemple, sur la Figure 4, les lettres de la diagonale *aaabaa* qui commence à la lettre $l_{26,3} = a$ code les décompositions $3 + 23, 5 + 23, 7 + 23, 9 + 23, 11 + 23$ et $13 + 23$.

3) Désignons par l_n la ligne dont les éléments sont les $l_{n,m}$. La ligne l_n possède $\left\lfloor \dfrac{n-2}{4} \right\rfloor$ éléments.

4) n étant fixé, appelons $C_{n,3}$ la colonne formée des $l_{k,3}$ pour $6 \leqslant k \leqslant n$.

Dans cette colonne $C_{n,3}$, distinguons deux parties, la "partie haute" et la "partie basse" de la colonne.

Notons $H_{n,3}$ la "partie haute" de la colonne, i.e. l'ensemble des $l_{k,3}$ où $6 \leqslant k \leqslant \left\lfloor \dfrac{n+4}{2} \right\rfloor$.

Notons $B_{n,3}$ la "partie basse" de la colonne, i.e. l'ensemble des $l_{k,3}$ où $\left\lfloor \dfrac{n+4}{2} \right\rfloor < k \leqslant n$.

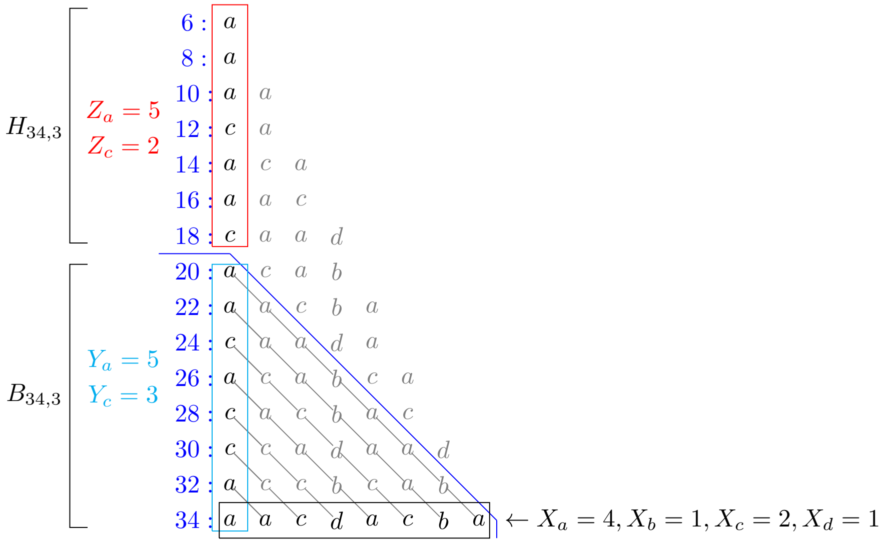


FIGURE 2 : $n = 34$

Pour mieux cerner les dénombrements de la section suivante, on utilisera la projection P de la ligne n sur la partie basse de la première colonne $B_{n,3}$ qui "associe" les lettres aux deux bouts d'une diagonale (elle associe à la lettre qui code la décomposition $p+q$ la lettre qui code la décomposition $3+q$). Si on considère l'application $proj$ telle que $proj(a) = proj(b) = a$ et $proj(c) = proj(d) = c$ alors, puisque 3 est premier, $proj(l_{n,2k+1}) = l_{n-2k+2,3}$. On peut comprendre l'effet de cette projection (qui préserve le sommant de second rang) en analysant les décompositions :

- si $p+q$ est codée par une lettre a ou une lettre b, cela correspond aux deux cas possibles dans lesquels q est premier, alors la décomposition $3+q$, contenant deux nombres premiers sera codée par la lettre a ;
- si $p+q$ est codée par une lettre c ou une lettre d, cela correspond aux deux cas possibles dans lesquels q est composé, alors la décomposition $3+q$, de la forme *premier* + *composé* sera codée par la lettre c.

On utilisera également dans la section suivante une projection P' de la ligne n sur la partie haute de la première colonne $H_{n,3}$ qui associe à la lettre qui code la décomposition $p+q$ la lettre qui code la décomposition $3+p$ (noter que le *sommant de premier rang* devient *sommant de second rang*) ; analysons l'effet qu'une telle projection aura sur les décompositions :

- si $p+q$ est codée par une lettre a ou une lettre c, cela correspond aux deux cas possibles dans lesquels p est premier, alors la décomposition $3+p$, contenant deux nombres premiers sera codée par la lettre a ;
- si $p+q$ est codée par une lettre b ou une lettre d, cela correspond aux deux cas possibles dans lesquels p est composé, alors la décomposition $3+p$, de la forme *premier* + *composé* sera codée par la lettre c.

3 Dénombrements

1) On note :

- $X_a(n)$ le nombre de décompositions de n de la forme *premier* + *premier* ;
- $X_b(n)$ le nombre de décompositions de n de la forme *composé* + *premier* ;
- $X_c(n)$ le nombre de décompositions de n de la forme *premier* + *composé* ;
- $X_d(n)$ le nombre de décompositions de n de la forme *composé* + *composé*.

Les variables $X_a(n), X_b(n), X_c(n), X_d(n)$ dénombrent donc des assertions logiques.

$X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$ est le nombre d'éléments de la ligne de n.

Exemple : $n = 34$:
$X_a(34) = \#\{3+31, 5+29, 11+23, 17+17\} = 4$
$X_b(34) = \#\{15+19\} = 1.$
$X_c(34) = \#\{7+27, 13+21\} = 2$
$X_d(34) = \#\{9+25\} = 1$

2) Soit $Y_a(n)$ (resp. $Y_c(n)$) le nombre de a (resp. c) qui apparaissent dans $B_{n,3}$. On rappelle qu'il n'y a que des lettres a et c dans la première colonne car elle contient les lettres associées aux décompositions de la forme $3 + x$ et que 3 est premier.

Exemple :

- $Y_a(34) = \#\{3+17, 3+19, 3+23, 3+29, 3+31\} = 5$
- $Y_c(34) = \#\{3+21, 3+25, 3+27\} = 3$

3) Compte-tenu de la projection P qui est une bijection, des définitions des lettres a, b, c, d, $Y_a(n) = X_a(n) + X_b(n)$ et $Y_c(n) = X_c(n) + X_d(n)$. Par suite, trivialement, $Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$.

Exemple :

$$
\begin{aligned}
Y_a(34) &= \#\{3+17, 3+19, 3+23, 3+29, 3+31\} \\
X_a(34) &= \#\{3+31, 5+29, 11+23, 17+17\} \\
X_b(34) &= \#\{15+19\} \\
\\
Y_c(34) &= \#\{3+21, 3+25, 3+27\} \\
X_c(34) &= \#\{7+27, 13+21\} \\
X_d(34) &= \#\{9+25\}
\end{aligned}
$$

4) Soit $Z_a(n)$ (resp. $Z_c(n)$) le nombre de a (resp. c) qui apparaissent dans $H_{n,3}$.

Exemple :

- $Z_a(34) = \#\{3+3, 3+5, 3+7, 3+11, 3+13\} = 5$
- $Z_c(34) = \#\{3+9, 3+15\} = 2$

$Z_a(n) + Z_c(n) = \left\lfloor \dfrac{n-4}{4} \right\rfloor$.

Rappel des propriétés identifiées

$$Y_a(n) = X_a(n) + X_b(n) \tag{1}$$

$$Y_c(n) = X_c(n) + X_d(n) \tag{2}$$

$$Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

$$Z_a(n) + Z_c(n) = \left\lfloor \frac{n-4}{4} \right\rfloor \tag{4}$$

Ajoutons quatre nouvelles propriétés à celles-ci :

$$X_a(n) + X_c(n) = Z_a(n) + \delta_{2p}(n) \tag{5}$$

avec $\delta_{2p}(n)$ qui vaut 1 dans le cas où n est le double d'un nombre premier et qui vaut 0 sinon.

$$X_b(n) + X_d(n) = Z_c(n) + \delta_{2c-imp}(n) \tag{6}$$

avec $\delta_{2c-imp}(n)$ qui vaut 1 dans le cas où n est un double d'impair composé, et qui vaut 0 sinon.

$$Z_c(n) - Y_a(n) = X_d(n) - X_a(n) - \delta_{2c-imp}(n) \tag{7}$$

$$Z_c(n) - Y_a(n) = Y_c(n) - Z_a(n) - \delta_{4k+2}(n) \tag{8}$$

avec $\delta_{4k+2}(n)$ qui vaut 1 si n est un double d'impair et 0 sinon.

Les propriétés 1, 2 et 3 découlent simplement de la définition de la projection P.

Les propriétés 5 et 6 découlent simplement de la définition de la projection P'.

On note une certaine redondance entre les 3 booléens introduits ici que sont $\delta_{2p}(n), \delta_{2c-imp}(n)$ et $\delta_{4k+2}(n)$. L'assertion logique triviale $(\delta_{2p}(n) \vee \delta_{2c-imp}(n)) \rightarrow \delta_{4k+2}(n)$ est vérifiée.

4 Démonstrations

4.1 Utilitaires

Démontrons que si n est un double d'impair (i.e. de la forme $4k+2$), alors $\left\lfloor \frac{n-2}{4} \right\rfloor = \left\lfloor \frac{n-4}{4} \right\rfloor + 1$.
En effet, le membre gauche de l'égalité vaut $\left\lfloor \frac{(4k+2)-2}{4} \right\rfloor = \left\lfloor \frac{4k}{4} \right\rfloor = k$.
Le membre droit de l'égalité vaut $\left\lfloor \frac{(4k+2)-4}{4} \right\rfloor + 1 = \left\lfloor \frac{4k-2}{4} \right\rfloor + 1 = (k-1)+1 = k$.

Démontrons que si n est un double de pair (i.e. de la forme $4k$), alors $\left\lfloor \frac{n-2}{4} \right\rfloor = \left\lfloor \frac{n-4}{4} \right\rfloor$.
$\left\lfloor \frac{4k-2}{4} \right\rfloor = k-1$ et $\left\lfloor \frac{4k-4}{4} \right\rfloor = k-1$.

On peut aussi exprimer cela de la façon suivante : si n est un double d'impair, $\left\lfloor \frac{n-2}{4} \right\rfloor = \frac{n-2}{4} = \left\lfloor \frac{n-4}{4} \right\rfloor + 1$ tandis que si n est un double de pair, $\left\lfloor \frac{n-2}{4} \right\rfloor = \frac{n-4}{4} = \left\lfloor \frac{n-4}{4} \right\rfloor$.

4.2 Propriétés 7 et 8

4.2.1 Propriété 7

La propriété 7 énonce que $Z_c(n) - Y_a(n) = X_d(n) - X_a(n) - \delta_{2c-imp}(n)$ avec $\delta_{2c-imp}(n)$ qui vaut 1 si n est un double de composé impair et 0 sinon.

Par définition, $Z_c(n)$ compte le nombre de décompositions de la forme $\alpha = 3 + \textit{compos}é$ avec $\textit{compos}é$ strictement inférieur à $n/2$ (appelons E cet ensemble de décompositions). $Z_c(n)$ compte donc également le nombre de décompositions de n de la forme $\beta = \textit{compos}é + y$ par bijection du sommant de second rang de la décomposition α sur le sommant de premier rang de la décomposition β. Or le nombre de décompositions de la forme $\textit{compos}é + y$ est égal à $X_b(n) + X_d(n)$ par définition de ces variables.

Par définition, $Y_a(n)$ compte le nombre de décompositions de la forme $\gamma = 3 + \textit{premier}$ avec $\textit{premier}$ strictement supérieur à $n/2$ (appelons F cet ensemble de décompositions). $Y_a(n)$ compte donc également le nombre de décompositions de n de la forme $\eta = x + \textit{premier}$ par bijection du sommant de second rang de la décomposition γ sur le sommant de second rang de la décomposition η. Or le nombre de décompositions de la forme $x + premier$ est égal à $X_b(n) + X_a(n)$ par définition de ces variables.

Les décompositions de n de la forme *composé* + *premier* sont à la fois dans E et dans F. En calculant $Z_c(n) - Y_a(n)$, on obtient également la valeur de $X_d(n) - X_a(n)$ par définition de ce que comptent les variables $Y_a(n), Z_c(n), X_d(n)$ et $X_a(n)$.

4.2.2 Propriété 8

Démontrons que $Z_c(n) - Y_a(n) = Y_c(n) - Z_a(n) - \delta_{4k+2}(n)$ avec $\delta_{4k+2}(n)$ qui vaut 1 si n est un double d'impair (il existe $k \geqslant 3$ tel que $n = 4k + 2$) et 0 sinon.

On utilise un raisonnement par récurrence :

i) On initialise les récurrences selon les 3 sortes de nombres à envisager : les doubles de pairs (de la forme $4k$, comme 16), les doubles d'impairs (donc de la forme $4k + 2$) qui sont premiers (comme 14) ou qui sont composés (comme 18).

La propriété 8 est vraie pour $n = 14, 16$ et 18. Fournissons dans un tableau les valeurs des variables pour ces 3 nombres :

n	$Z_c(n)$	$Y_a(n)$	$Y_c(n)$	$Z_a(n)$	δ_{4k+2}
14	0	2	1	2	1
16	0	2	1	3	0
18	0	2	2	3	1

ii) On réécrit la propriété 8 sous la forme $Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n)$.
Quatre cas sont à considérer : deux cas selon lesquels n est un double d'impair (premier ou composé) et $n + 2$ est un double de pair et deux cas selon lesquels n est un double de pair et $n + 2$ est un double d'impair (premier ou composé).

iia) *n double de pair et $n + 2$ double de premier* :

n	δ_{2p}	δ_{2c-imp}	δ_{4k+2}
n	0	0	0
$n+2$	1	0	1

On pose l'hypothèse que la propriété 8 est vraie pour n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \qquad (H)$$

Démontrons qu'elle est vraie pour $n + 2$,

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \qquad (Ccl)$$

On a $Z_a(n + 2) = Z_a(n)$ et $Z_c(n + 2) = Z_c(n)$.

Rappelons la propriété 3 concernant les Y:

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \qquad (3)$$

Dans (Ccl), on peut, par l'hypothèse de récurrence et par la propriété (3), remplacer le membre gauche de l'égalité par $Z_a(n) + Z_c(n) + 1$ puis par $Y_a(n) + Y_c(n) + 1$ (par (H)) puis par $\left\lfloor \frac{n-2}{4} \right\rfloor + 1$ (par (3)) qui vaut $\left\lfloor \dfrac{n}{4} \right\rfloor$.

Mais dans (Ccl), on peut également remplacer le membre de droite de l'égalité par $\left\lfloor \dfrac{n}{4} \right\rfloor$ du fait de la propriété (3).

Il y a à nouveau pour $n+2$ égalité entre les membres gauche et droit de l'égalité, i.e. la propriété 8 est vérifiée par $n+2$. De l'hypothèse que la propriété est vraie pour n, on a démontré que la propriété est vraie pour $n+2$.

iib) *n double de pair et $n+2$ double de composé impair* :

n	δ_{2p}	δ_{2c-imp}	δ_{4k+2}
n	0	0	0
$n+2$	0	1	1

On pose l'hypothèse que la propriété 8 est vraie pour n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \qquad (H)$$

Démontrons qu'elle est vraie pour $n+2$,

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \qquad (Ccl)$$

On a $Z_a(n+2) = Z_a(n)$ et $Z_c(n+2) = Z_c(n)$.

On a $Y_a(n+2) = Y_a(n) + 1$ et $Y_c(n+2) = Y_c(n)$.

Rappelons la propriété 3 concernant les Y:

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \qquad (3)$$

Dans (Ccl), on peut, par l'hypothèse de récurrence et la propriété (3), remplacer le membre gauche de l'égalité par $Z_a(n) + Z_c(n) + 1$ puis par $Y_a(n) + Y_c(n) + 1$ (par (H)) puis par $\left\lfloor \dfrac{n-2}{4} \right\rfloor + 1$ (par (3)) qui vaut $\left\lfloor \dfrac{n}{4} \right\rfloor$.

Mais dans (Ccl), on peut également remplacer le membre de droite de l'égalité par $\left\lfloor \dfrac{n}{4} \right\rfloor$ du fait des évolutions de $Y_a(n)$ et $Y_c(n)$.

Il y a à nouveau pour $n+2$ égalité entre les membres gauche et droit de l'égalité, i.e. la propriété 8 est vérifiée par $n+2$. De l'hypothèse que la propriété est vraie pour n, on a démontré que la propriété est vraie pour $n+2$.

iic) *n double de premier et $n+2$ double de pair* :

n	δ_{2p}	δ_{2c-imp}	δ_{4k+2}
n	1	0	1
$n+2$	0	0	0

On pose l'hypothèse que la propriété 8 est vraie pour n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \qquad (H)$$

Démontrons qu'elle est vraie pour $n+2$,

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \qquad (Ccl)$$

On a $Z_a(n+2) = Z_a(n) + 1$ et $Z_c(n+2) = Z_c(n)$.

Rappelons la propriété 3 concernant les Y :

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

Dans (Ccl), on peut, par l'hypothèse de récurrence et la propriété (3), remplacer le membre gauche de l'égalité par $Z_a(n) + Z_c(n) + 1$ puis par $Y_a(n) + Y_c(n)$ (par (H)) puis par $\left\lfloor \frac{n-2}{4} \right\rfloor$ (par (3)) qui vaut $\left\lfloor \frac{n}{4} \right\rfloor$.

Mais dans (Ccl), on peut également remplacer le membre de droite de l'égalité par $\left\lfloor \frac{n}{4} \right\rfloor$ du fait de la propriété (3).

Il y a à nouveau pour $n+2$ égalité entre les membres gauche et droit de l'égalité, i.e. la propriété 8 est vérifiée par $n+2$. De l'hypothèse que la propriété est vraie pour n, on a démontré que la propriété est vraie pour $n+2$.

iid) *n double de composé impair et $n+2$ double de pair* :

n	δ_{2p}	δ_{2c-imp}	δ_{4k+2}
n	0	1	1
$n+2$	0	0	0

On pose l'hypothèse que la propriété 8 est vraie pour n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \tag{H}$$

Démontrons qu'elle est vraie pour $n+2$,

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \tag{Ccl}$$

On a $Z_a(n+2) = Z_a(n)$ et $Z_c(n+2) = Z_c(n) + 1$.

Rappelons la propriété 3 concernant les Y :

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

Dans (Ccl), on peut, par l'hypothèse de récurrence et la propriété (3), remplacer le membre gauche de l'égalité par $Z_a(n) + Z_c(n) + 1$ puis par $Y_a(n) + Y_c(n)$ (par (H)) puis par $\left\lfloor \frac{n-2}{4} \right\rfloor$ (par (3)) qui vaut $\left\lfloor \frac{n}{4} \right\rfloor$.

Mais dans (Ccl), on peut également remplacer le membre de droite de l'égalité par $\left\lfloor \frac{n}{4} \right\rfloor$ du fait de la propriété (3).

Il y a à nouveau pour $n+2$ égalité entre les membres gauche et droit de l'égalité, i.e. la propriété 8 est vérifiée par $n+2$. De l'hypothèse que la propriété est vraie pour n, on a démontré que la propriété est vraie pour $n+2$.

5 Evolution des variables

5.1 Dénombrements des décompositions de la forme $3+p$ (dites "basses")

1) $Z_a(n+2) = Z_a(n)$ et $Z_c(n+2) = Z_c(n)$ quand n est un double de pair. En effet, $Z_a(n)$ (resp. $Z_c(n)$) compte le nombre de nombres premiers (resp. composés impairs) strictement inférieurs à $\frac{n}{2}$ et il y a autant de nombres premiers (resp. composés impairs) inférieurs à un nombre pair qu'inférieurs à son successeur immédiat.

2) $Z_a(n+2) = Z_a(n) + 1$ et $Z_c(n+2) = Z_c(n)$ quand n est un double de nombre premier ;

3) $Z_a(n+2) = Z_a(n)$ et $Z_c(n+2) = Z_c(n) + 1$ quand n est un double de nombre composé impair.

5.2 Dénombrements des décompositions de la forme $3 + q$ (dites “hautes”)

Dans le cas où $n + 2$ est un double d'impair, on ne fait qu'ajouter un nombre à l'intervalle $H_{n+2,3}$; si ce nombre $n - 1$ est premier (resp. composé), $Y_a(n + 2) = Y_a(n) + 1$ (resp. $Y_c(n + 2) = Y_c(n) + 1$).

Dans le cas où $n + 2$ est un double de pair, on ajoute un nombre à l'extrémité haute de l'intervalle et on enlève un nombre à l'extrémité basse de l'intervalle. De ce fait, 4 cas se présentent. Etudions la manière dont évolue l'ensemble de décompositions $H_{n+2,3}$.

- si $n - 1$ et $\dfrac{n}{2}$ sont tous les deux premiers, on retire en bas et on ajoute en haut de l'intervalle $H_{n+2,3}$ deux lettres de même sorte, alors $Y_a(n + 2) = Y_a(n)$;
- si $n - 1$ est premier et $\dfrac{n}{2}$ est composé alors $Y_a(n + 2) = Y_a(n) + 1$;
- si $n - 1$ est composé et $\dfrac{n}{2}$ est premier alors $Y_a(n + 2) = Y_a(n) - 1$;
- si $n - 1$ et $\dfrac{n}{2}$ sont tous les deux composés, on retire en bas et on ajoute en haut de l'intervalle $H_{n+2,3}$ deux lettres de même sorte, alors $Y_a(n + 2) = Y_a(n)$.

6 Utiliser les écarts entre variables

On va montrer que $X_a(n)$ ne peut jamais être nul pour $n \geqslant C$, i.e. que tout entier pair $n \geqslant C$ peut s'écrire comme une somme de deux nombres premiers, c'est-à-dire vérifie la conjecture de Goldbach.

Précisons davantage à quoi sont égales les variables $Z_a(n), Z_c(n), Y_a(n)$ et $Y_c(n)$.

- $Z_a(n)$ compte à 2 près le nombre de nombres premiers inférieurs ou égaux à $\dfrac{n}{2}$;

$$Z_a(n) = \pi\left(\frac{n}{2}\right) + \delta_{Z_a}(n) \tag{9}$$

  avec $\delta_{Z_a}(n)$ égal à -2 si n est le double d'un nombre premier et égal à -1 sinon ;

- $Z_c(n)$ compte à 1 près le nombre de nombres composés impairs inférieurs ou égaux à $\dfrac{n}{2}$;

$$Z_c(n) = \left\lfloor\frac{n}{4}\right\rfloor - \pi\left(\frac{n}{2}\right) + \delta_{Z_c}(n) \tag{10}$$

  avec $\delta_{Z_c}(n)$ égal à 1 si n est le double d'un nombre premier et égal à 0 sinon ;

- $Y_a(n)$ compte à 1 près le nombre de nombres premiers qui sont compris entre $\dfrac{n}{2}$ et n ;

$$Y_a(n) = \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \tag{11}$$

  avec $\delta_{Y_a}(n)$ égal à $-1, 0$ ou 1 ($\delta_{Y_a}(n)$ est égal à 0 quand $n - 1$ et $n/2$ sont tous les deux premiers ou bien tous les deux composés, $\delta_{Y_a}(n)$ est égal à -1 quand $n - 1$ est premier tandis que $n/2$ est composé, et enfin, $\delta_{Y_a}(n)$ est égal à 1 quand $n - 1$ est composé tandis que $n/2$ est premier) ;

- $Y_c(n)$ compte à 1 près le nombre de nombres composés impairs qui sont compris entre $\dfrac{n}{2}$ et n ;

$$Y_c(n) = \left\lfloor\frac{n}{4}\right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \tag{12}$$

  avec $\delta_{Y_c}(n)$ égal à $-1, 0$ ou 1. Les valeurs de $\delta_{Y_c}(n)$ seront fournies de façon détaillée dans la section démontrant la propriété 12.

6.1 Démonstrations des propriétés 9, 10, 11 et 12

6.1.1 Propriété 9 : relation invariante portant sur $Z_a(n)$

i) Initialisation : (9) est vraie pour $n = 14, 16$, 18 et 20.

En effet, on a :

n	$Z_a(n)$	$\pi\left(\frac{n}{2}\right)$	$\delta_{Z_a}(n)$
14	2	4	-2
16	3	4	-1
18	3	4	-1
20	3	4	-1
22	3	5	-2

ii) Démontrons par récurrence que si (9) est vraie pour n, elle est vraie pour $n+2$.

On pose l'hypothèse que la propriété 9 est vraie pour n,

$$Z_a(n) = \pi\left(\frac{n}{2}\right) + \delta_{Z_a}(n) \qquad (H)$$

Démontrons qu'elle est vraie pour $n+2$,

$$Z_a(n+2) = \pi\left(\frac{n+2}{2}\right) + \delta_{Z_a}(n+2) \qquad (Ccl)$$

Distinguons 4 cas comme dans le paragraphe 4.2.2.

iia) n double de pair, $n+2$ double de premier.

Dans ce cas, $Z_a(n+2) = Z_a(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right) + 1$ et $\delta_{Z_a}(n) = -1$.

Auquel cas,

$$\begin{aligned} Z_a(n+2) &= Z_a(n) \\ &= \pi\left(\frac{n}{2}\right) + \delta_{Z_a}(n) \\ &= \pi\left(\frac{n+2}{2}\right) - 1 + \delta_{Z_a}(n) \\ &= \pi\left(\frac{n+2}{2}\right) - 1 - 1 \\ &= \pi\left(\frac{n+2}{2}\right) + \delta_{Z_a}(n+2) \end{aligned}$$

avec $\delta_{Z_a}(n+2) = -2$ comme attendu puisque $n+2$ est un double de nombre premier.

iib) n double de pair, $n+2$ double de composé impair.

Dans ce cas, $Z_a(n+2) = Z_a(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$ et $\delta_{Z_a}(n) = -1$.

Auquel cas,

$$\begin{aligned} Z_a(n+2) &= Z_a(n) \\ &= \pi\left(\frac{n}{2}\right) + \delta_{Z_a}(n) \\ &= \pi\left(\frac{n+2}{2}\right) - 1 \\ &= \pi\left(\frac{n+2}{2}\right) + \delta_{Z_a}(n+2) \end{aligned}$$

avec $\delta_{Z_a}(n+2) = -1$ comme attendu puisque $n+2$ est un double de composé impair.

iic) n double de premier, $n+2$ double de pair.

Dans ce cas, $Z_a(n+2) = Z_a(n) + 1$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$ et $\delta_{Z_a}(n) = -2$.

Auquel cas,

$$\begin{aligned} Z_a(n+2) &= Z_a(n)+1 \\ &= \pi\left(\frac{n}{2}\right)+\delta_{Z_a}(n)+1 \\ &= \pi\left(\frac{n+2}{2}\right)-2+1 \\ &= \pi\left(\frac{n+2}{2}\right)-1 \\ &= \pi\left(\frac{n+2}{2}\right)+\delta_{Z_a}(n+2) \end{aligned}$$

avec $\delta_{Z_a}(n+2)=-1$ comme attendu puisque $n+2$ est un double de pair.

iid) n double de composé impair, $n+2$ double de pair.

Dans ce cas, $Z_a(n+2)=Z_a(n)$, $\pi\left(\dfrac{n+2}{2}\right)=\pi\left(\dfrac{n}{2}\right)$ et $\delta_{Z_a}(n)=-1$.

Auquel cas,

$$\begin{aligned} Z_a(n+2) &= Z_a(n) \\ &= \pi\left(\frac{n}{2}\right)+\delta_{Z_a}(n) \\ &= \pi\left(\frac{n+2}{2}\right)-1 \\ &= \pi\left(\frac{n+2}{2}\right)+\delta_{Z_a}(n+2) \end{aligned}$$

avec $\delta_{Z_a}(n+2)=-1$ comme attendu puisque $n+2$ est un double de pair.

6.1.2 Propriété 10 : relation invariante portant sur $Z_c(n)$

i) Initialisation : (10) est vraie pour $n=14,16,18$ et 20.

On a :

n	$Z_c(n)$	$\left\lfloor \frac{n}{4} \right\rfloor$	$\pi\left(\frac{n}{2}\right)$	$\delta_{Z_c}(n)$
14	0	3	4	1
16	0	4	4	0
18	0	4	4	0
20	1	5	4	0
22	1	5	5	1

et on vérifie donc que (10) est vraie pour ces 4 nombres.

ii) Démontrons par récurrence que si (10) est vraie pour n, elle est vraie pour $n+2$.

On pose l'hypothèse que la propriété 10 est vraie pour n,

$$Z_c(n)=\left\lfloor \frac{n}{4} \right\rfloor-\pi\left(\frac{n}{2}\right)+\delta_{Z_c}(n) \tag{H}$$

Démontrons qu'elle est vraie pour $n+2$,

$$Z_c(n+2)=\left\lfloor \frac{n+2}{4} \right\rfloor-\pi\left(\frac{n+2}{2}\right)+\delta_{Z_c}(n+2) \tag{Ccl}$$

Reprenons les 4 cas.

iia) n double de pair, $n+2$ double de premier.

Dans ce cas, $Z_c(n+2)=Z_c(n)$, $\left\lfloor \dfrac{n+2}{4} \right\rfloor=\left\lfloor \dfrac{n}{4} \right\rfloor$, $\pi\left(\dfrac{n+2}{2}\right)=\pi\left(\dfrac{n}{2}\right)+1$ et $\delta_{Z_c}(n)=0$.

Auquel cas,

$$\begin{aligned}
Z_c(n+2) &= Z_c(n) \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi\left(\frac{n}{2}\right) + \delta_{Z_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + 1 + \delta_{Z_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + 1 + 0 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + \delta_{Z_c}(n+2)
\end{aligned}$$

avec $\delta_{Z_c}(n+2) = 1$ comme attendu puisque $n+2$ est un double de nombre premier.

iib) n double de pair, $n+2$ double de composé impair.

Dans ce cas, $Z_c(n+2) = Z_c(n)$, $\left\lfloor \frac{n+2}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$ et $\delta_{Z_c}(n) = 0$.

Auquel cas,

$$\begin{aligned}
Z_c(n+2) &= Z_c(n) \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi\left(\frac{n}{2}\right) + \delta_{Z_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + \delta_{Z_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + 0 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + \delta_{Z_c}(n+2)
\end{aligned}$$

avec $\delta_{Z_c}(n+2) = 0$ comme attendu puisque $n+2$ est un double de nombre composé impair.

iic) n double de premier, $n+2$ double de pair.

Dans ce cas, $Z_c(n+2) = Z_c(n)$, $\left\lfloor \frac{n+2}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor + 1$, $\pi\left(\frac{n+2}{4}\right) = \pi\left(\frac{n}{2}\right)$ et $\delta_{Z_c}(n) = 1$.

Auquel cas,

$$\begin{aligned}
Z_c(n+2) &= Z_c(n) \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi\left(\frac{n}{2}\right) + \delta_{Z_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{4}\right) - 1 + \delta_{Z_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) - 1 + 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + \delta_{Z_c}(n+2)
\end{aligned}$$

avec $\delta_{Z_c}(n+2) = 0$ comme attendu puisque $n+2$ est un double de pair.

iid) n double de composé impair, $n+2$ double de pair.

Dans ce cas, $Z_c(n+2) = Z_c(n) + 1$, $\left\lfloor \frac{n+2}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor + 1$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$ et $\delta_{Z_c}(n) = 0$.

Auquel cas,

$$\begin{aligned}
Z_c(n+2) &= Z_c(n) \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi\left(\frac{n}{2}\right) + \delta_{Z_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - 1 - \pi\left(\frac{n+2}{2}\right) + 1 + \delta_{Z_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) - 1 + 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + \delta_{Z_c}(n+2)
\end{aligned}$$

avec $\delta_{Z_c}(n+2) = 0$ comme attendu puisque $n+2$ est un double de pair.

6.1.3 Propriété 11 : relation invariante portant sur $Y_a(n)$

Il s'agit de démontrer pourquoi la relation invariante portant sur $Y_a(n)$ et qui est :

$$Y_a(n) = \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n)$$

est toujours vérifiée. Pour cela, il convient de distinguer 16 cas, selon le caractère de primalité des quatre nombres $\frac{n}{2}$, $\frac{n+2}{2}$, $n-1$ et $n+1$, ces caractères de primalité ayant une influence sur les évolutions de $Y_a(n)$, de $\pi(n)$, de $\pi\left(\frac{n}{2}\right)$ et de $\delta_{Y_a}(n)$.

i) initialisation des récurrences : pour 5 cas sur 16, on est dans des cas de contradictions (on les a nommés $C1$ à $C5$ en bas de tableau, la contradiction provient pour $C1$ à $C4$ du fait qu'on ne peut avoir $n/2$ et $(n+2)/2$ qui sont premiers tous les deux puisque ce sont des entiers consécutifs) ; $C5$ est contradictoire car si $n-1$ et $n+1$ sont des nombres premiers jumeaux, leur "père" n est divisible par 3 et la moitié du père en question qui est $n/2$ ne peut être un nombre premier lui-aussi, ce qui est représenté par les 3 croix en première, troisième et quatrième colonnes). Pour les 11 cas restant, il convient d'initialiser les récurrences. Dans le tableau ci-dessous, on fournit les valeurs qui permettent d'aisément vérifier que pour des petits entiers, la propriété 11 est bien systématiquement vérifiée.

n	$n/2$ *est premier*	$(n+2)/2$ *est premier*	$n-1$ *est premier*	$n+1$ *est premier*	$Y_a(n)$	$\pi(n)$	$\pi(n/2)$	$\delta_{Y_a}(n)$
14	×	–	×	–	2	6	4	0
16	–	–	–	×	2	6	4	0
18	–	–	×	×	2	7	4	−1
20	–	×	×	–	3	8	4	−1
22	×	–	–	×	4	8	5	1
26	×	–	–	–	4	9	6	1
36	–	×	–	×	4	11	7	0
48	–	–	×	–	5	15	9	−1
50	–	–	–	–	6	15	9	0
56	–	×	–	–	7	16	9	0
60	–	×	×	×	6	17	10	−1
$C1$	×	×	×	×	–	–	–	–
$C2$	×	×	×	–	–	–	–	–
$C3$	×	×	–	×	–	–	–	–
$C4$	×	×	–	–	–	–	–	–
$C5$	×	–	×	×	–	–	–	–

ii) passage de n à $n+2$: Démontrons par récurrence que si (11) est vraie pour n, elle est vraie pour $n+2$.

On pose l'hypothèse que la propriété 11 est vraie pour n,

$$Y_a(n) = \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \qquad (H)$$

Démontrons qu'elle est vraie pour $n+2$,

$$Y_a(n+2) = \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \qquad (Ccl)$$

Etudions les 11 cas.

iia) $n+1$ composé, $(n+2)/2$ composé, $n/2$ premier, $n-1$ premier

Dans ce cas, $\pi(n+2) = \pi(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$, $\delta_{Y_a}(n) = 0$ et $Y_a(n+2) = Y_a(n)$.

Auquel cas,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

puisque $\delta_{Y_a}(n+2) = 0$ dans ce cas. Cela entraîne que (Ccl) est vérifiée.

iib) $n+1$ premier, $(n+2)/2$ composé, $n/2$ composé, $n-1$ composé

Dans ce cas, $\pi(n+2) = \pi(n) + 1$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$, $\delta_{Y_a}(n) = 0$ et $Y_a(n+2) = Y_a(n)$.

Auquel cas,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \\ &= \pi(n+2) - 1 - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

puisque $\delta_{Y_a}(n+2) = -1$ dans ce cas. Cela entraîne que (Ccl) est vérifiée.

iic) $n+1$ composé, $(n+2)/2$ composé, $n/2$ premier, $n-1$ composé

Dans ce cas, $\pi(n+2) = \pi(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$, $\delta_{Y_a}(n) = 1$ et $Y_a(n+2) = Y_a(n) - 1$.

Auquel cas,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) - 1 \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) - 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + 1 - 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

puisque $\delta_{Y_a}(n+2) = 0$ dans ce cas. Cela entraîne que (Ccl) est vérifiée.

iid) $n+1$ premier, $(n+2)/2$ premier, $n/2$ composé, $n-1$ premier

Dans ce cas, $\pi(n+2) = \pi(n) + 1$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right) + 1$, $\delta_{Y_a}(n) = -1$ et $Y_a(n+2) = Y_a(n) + 1$.

Auquel cas,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) + 1 \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) + 1 \\ &= \pi(n+2) - 1 - \pi\left(\frac{n+2}{2}\right) + 1 - 1 + 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

puisque $\delta_{Y_a}(n+2) = 0$ dans ce cas. Cela entraîne que (Ccl) est vérifiée.

iie) $n+1$ composé, $(n+2)/2$ premier, $n/2$ composé, $n-1$ premier

Dans ce cas, $\pi(n+2) = \pi(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right) + 1$, $\delta_{Y_a}(n) = -1$ et $Y_a(n+2) = Y_a(n) + 1$.

Auquel cas,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) + 1 \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) + 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + 1 - 1 + 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

puisque $\delta_{Y_a}(n+2) = 1$ dans ce cas. Cela entraîne que (Ccl) est vérifiée.

iif) $n+1$ premier, $(n+2)/2$ premier, $n/2$ composé, $n-1$ composé

Dans ce cas, $\pi(n+2) = \pi(n) + 1$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right) + 1$, $\delta_{Y_a}(n) = 0$ et $Y_a(n+2) = Y_a(n)$.

Auquel cas,

$$\begin{aligned}
Y_a(n+2) &= Y_a(n) \\
&= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \\
&= \pi(n+2) - 1 - \pi\left(\frac{n+2}{2}\right) + 1 \\
&= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2)
\end{aligned}$$

puisque $\delta_{Y_a}(n+2) = 0$ dans ce cas. Cela entraîne que (Ccl) est vérifiée.

iig) $n+1$ composé, $(n+2)/2$ premier, $n/2$ composé, $n-1$ composé

Dans ce cas, $\pi(n+2) = \pi(n)$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right) + 1$, $\delta_{Y_a}(n) = 0$ et $Y_a(n+2) = Y_a(n)$.

Auquel cas,

$$\begin{aligned}
Y_a(n+2) &= Y_a(n) \\
&= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \\
&= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + 1 + 0 \\
&= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2)
\end{aligned}$$

puisque $\delta_{Y_a}(n+2) = 1$ dans ce cas. Cela entraîne que (Ccl) est vérifiée.

iih) $n+1$ premier, $(n+2)/2$ composé, $n/2$ composé, $n-1$ premier

Dans ce cas, $\pi(n+2) = \pi(n) + 1$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right)$, $\delta_{Y_a}(n) = -1$ et $Y_a(n+2) = Y_a(n) + 1$.

Auquel cas,

$$\begin{aligned}
Y_a(n+2) &= Y_a(n) + 1 \\
&= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) + 1 \\
&= \pi(n+2) - 1 - \pi\left(\frac{n+2}{2}\right) - 1 + 1 \\
&= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2)
\end{aligned}$$

puisque $\delta_{Y_a}(n+2) = -1$ dans ce cas. Cela entraîne que (Ccl) est vérifiée.

iii) $n+1$ composé, $(n+2)/2$ composé, $n/2$ composé, $n-1$ premier

Dans ce cas, $\pi(n+2) = \pi(n)$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right)$, $\delta_{Y_a}(n) = -1$ et $Y_a(n+2) = Y_a(n) + 1$.

Auquel cas,

$$\begin{aligned}
Y_a(n+2) &= Y_a(n) + 1 \\
&= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) + 1 \\
&= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) - 1 + 1 \\
&= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2)
\end{aligned}$$

puisque $\delta_{Y_a}(n+2) = 0$ dans ce cas. Cela entraîne que (Ccl) est vérifiée.

iij) $n+1$ premier, $(n+2)/2$ composé, $n/2$ premier, $n-1$ composé

Dans ce cas, $\pi(n+2) = \pi(n) + 1$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right)$, $\delta_{Y_a}(n) = 1$ et $Y_a(n+2) = Y_a(n) - 1$.

Auquel cas,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) - 1 \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) - 1 \\ &= \pi(n+2) - 1 - \pi\left(\frac{n+2}{2}\right) + 1 - 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

puisque $\delta_{Y_a}(n+2) = -1$ dans ce cas. Cela entraîne que (Ccl) est vérifiée.

iik) $n+1$ composé, $(n+2)/2$ composé, $n/2$ composé, $n-1$ composé

Dans ce cas, $\pi(n+2) = \pi(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$, $\delta_{Y_a}(n) = 0$ et $Y_a(n+2) = Y_a(n)$.

Auquel cas,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

puisque $\delta_{Y_a}(n+2) = 0$ dans ce cas. Cela entraîne que (Ccl) est vérifiée.

6.1.4 Propriété 12 : relation invariante portant sur $Y_c(n)$

Il s'agit de démontrer pourquoi la relation invariante portant sur $Y_c(n)$ et qui est :

$$Y_c(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n)$$

est toujours vérifiée.

i) initialisation des récurrences :

n	$n/2$ *est premier*	$(n+2)/2$ *est premier*	$n-1$ *est premier*	$n+1$ *est premier*	$Y_c(n)$	$\left\lfloor \frac{n}{4} \right\rfloor$	$\pi(n)$	$\pi(n/2)$	$\delta_{Y_c}(n)$
14	x	–	x	–	1	3	6	4	0
16	–	–	–	x	1	4	6	4	−1
18	–	–	x	x	2	4	7	4	1
20	–	x	x	–	1	5	8	4	0
22	x	–	–	x	1	5	8	5	−1
26	x	–	–	–	2	6	9	6	−1
36	–	x	–	x	4	9	11	7	−1
48	–	–	x	–	6	12	15	9	0
50	–	–	–	–	6	12	15	9	0
56	–	x	–	–	6	14	16	9	−1
60	–	x	x	x	8	15	17	10	0

On vérifie aisément que pour les petits entiers, la propriété 12 est bien systématiquement vérifiée.

ii) passage de n à $n+2$: Démontrons par récurrence que si (12) est vraie pour n, elle est vraie pour $n+2$.

On pose l'hypothèse que la propriété 12 est vraie pour n,

$$Y_c(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \qquad (H)$$

Démontrons qu'elle est vraie pour $n+2$,

$$Y_c(n+2) = \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2) \qquad (Ccl)$$

On retrouve ici les 11 cas identifiés pour la propriété 11 ; parfois, on a deux sous-cas, lorsque $n/2$ est composé, selon que n est un double de pair auquel cas $\left\lfloor \dfrac{n+2}{4} \right\rfloor = \left\lfloor \dfrac{n}{4} \right\rfloor$ ou que n est un double d'impair auquel cas $\left\lfloor \dfrac{n+2}{4} \right\rfloor = \left\lfloor \dfrac{n}{4} \right\rfloor + 1$.

Dans le tableau ci-dessous sont fournies les valeurs de $\delta_{Y_c}(n)$ selon les valeurs des booléens pertinents à considérer (en première colonne, on indique un numéro de ligne l_i utile dans la suite ; un exemple de petit nombre est fourni en avant-dernière colonne, pour fixer les idées ; la lettre correspondant au type de récurrence intervenant (cf après le tableau) est fournie en dernière colonne) :

	$n-1$ *est premier*	$n+1$ *est premier*	$n/2$ *est premier*	$(n+2)/2$ *est premier*	$\delta_{4k+2}(n)$	$\delta_{Y_c}(n)$	*ex*	*cas*
l_1	×	−	×	−	×	0	14	a
l_2	×	−	−	×	−	0	20	e
l_3	×	−	−	−	×	0	54	i
l_4	×	−	−	−	−	1	48	i
l_5	−	×	×	−	×	−1	22	b
l_6	−	×	−	×	−	−1	36	f
l_7	−	×	−	−	×	0	66	j
l_8	−	×	−	−	−	−1	16	j
l_9	−	−	×	−	×	−1	26	c
l_{10}	−	−	−	×	−	−1	56	g
l_{11}	−	−	−	−	×	0	50	k
l_{12}	−	−	−	−	−	−1	64	k
l_{13}	×	×	−	×	−	0	60	d
l_{14}	×	×	−	−	×	1	18	h
l_{15}	×	×	−	−	−	0	108	h

iia) $n+1$ composé, $(n+2)/2$ composé, $n/2$ premier, $n-1$ premier

Dans ce cas, $\pi(n+2) = \pi(n)$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right)$, $\delta_{Y_c}(n) = 0$ et $Y_c(n+2) = Y_c(n)$.

Auquel cas,

$$\begin{aligned} Y_c(n+2) &= Y_c(n) \\ &= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - 1 - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + 0 \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2) \end{aligned}$$

puisque $\delta_{Y_c}(n+2) = -1$ dans ce cas ($n+2$ correspond alors à l'un des cas des lignes l_6, l_8, l_{10} ou l_{12} car n étant un double d'impair, $n+2$ ne peut en être un). Cela entraîne que (Ccl) est vérifiée.

iib) $n+1$ premier, $(n+2)/2$ composé, $n/2$ premier, $n-1$ composé

Dans ce cas, $\pi(n+2) = \pi(n) + 1$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right)$, $\delta_{Y_c}(n) = -1$ et $Y_c(n+2) = Y_c(n) + 1$.

Auquel cas,

$$\begin{aligned} Y_c(n+2) &= Y_c(n) + 1 \\ &= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) + 1 \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - 1 - \pi(n+2) + 1 + \pi\left(\frac{n+2}{2}\right) - 1 + 1 \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2) \end{aligned}$$

puisque $\delta_{Y_c}(n+2) = 0$ dans ce cas ($n+2$ correspond alors à l'un des cas des lignes l_2, l_{13} ou l_{15} car n étant un double d'impair, $n+2$ ne peut en être un). Cela entraîne que (Ccl) est vérifiée.

iic) $n+1$ composé, $(n+2)/2$ composé, $n/2$ premier, $n-1$ composé

Dans ce cas, $\pi(n+2)=\pi(n)$, $\pi\left(\dfrac{n+2}{2}\right)=\pi\left(\dfrac{n}{2}\right)$, $\delta_{Y_c}(n)=-1$ et $Y_c(n+2)=Y_c(n)+1$.

Auquel cas,

$$\begin{aligned}
Y_c(n+2) \quad &= Y_c(n)+1 \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) + 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - 1 - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) - 1 + 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

puisque $\delta_{Y_c}(n+2)=-1$ dans ce cas ($n+2$ correspond alors à l'un des cas des lignes l_6, l_8, l_{10} ou l_{12} car n étant un double d'impair, $n+2$ ne peut en être un). Cela entraîne que (Ccl) est vérifiée.

iid) $n+1$ premier, $(n+2)/2$ premier, $n/2$ composé, $n-1$ premier

Dans ce cas, $\pi(n+2)=\pi(n)+1$, $\pi\left(\dfrac{n+2}{2}\right)=\pi\left(\dfrac{n}{2}\right)+1$, $\delta_{Y_c}(n)=0$ et $Y_c(n+2)=Y_c(n)$.

n est obligatoirement un double de pair.

Auquel cas,

$$\begin{aligned}
Y_c(n+2) \quad &= Y_c(n) \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + 1 + \pi\left(\frac{n+2}{2}\right) - 1 + 0 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

puisque $\delta_{Y_c}(n+2)=0$ dans ce cas ($n+2$ correspond alors au cas de la ligne l_1). Cela entraîne que (Ccl) est vérifiée.

iie) $n+1$ composé, $(n+2)/2$ premier, $n/2$ composé, $n-1$ premier

Dans ce cas, $\pi(n+2)=\pi(n)$, $\pi\left(\dfrac{n+2}{2}\right)=\pi\left(\dfrac{n}{2}\right)+1$, $\delta_{Y_c}(n)=0$ et $Y_c(n+2)=Y_c(n)$.

n est obligatoirement un double de pair.

Auquel cas,

$$\begin{aligned}
Y_c(n+2) \quad &= Y_c(n) \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) - 1 + 0 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

puisque $\delta_{Y_c}(n+2)=-1$ dans ce cas ($n+2$ correspond alors à l'un des cas des lignes l_5 ou l_9). Cela entraîne que (Ccl) est vérifiée.

iif) $n+1$ premier, $(n+2)/2$ premier, $n/2$ composé, $n-1$ composé

Dans ce cas, $\pi(n+2)=\pi(n)+1$, $\pi\left(\dfrac{n+2}{2}\right)=\pi\left(\dfrac{n}{2}\right)+1$, $\delta_{Y_c}(n)=-1$ et $Y_c(n+2)=Y_c(n)+1$.

n est obligatoirment un double de pair.

Auquel cas,

$$\begin{aligned}
Y_c(n+2) \quad &= Y_c(n)+1 \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) + 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + 1 + \pi\left(\frac{n+2}{2}\right) - 1 - 1 + 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

puisque $\delta_{Y_c}(n+2) = 0$ dans ce cas ($n+2$ correspond alors au cas de la ligne l_1). Cela entraîne que (Ccl) est vérifiée.

iig) $n+1$ composé, $(n+2)/2$ premier, $n/2$ composé, $n-1$ composé

Dans ce cas, $\pi(n+2) = \pi(n)$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right) + 1$, $\delta_{Y_c}(n) = -1$ et $Y_c(n+2) = Y_c(n) + 1$.

n est obligatoirement un double de pair.

Auquel cas,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n) + 1 \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) + 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) - 1 - 1 + 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

puisque $\delta_{Y_c}(n+2) = -1$ dans ce cas ($n+2$ correspond alors à l'un des cas des lignes l_5 ou l_9). Cela entraîne que (Ccl) est vérifiée.

iih) $n+1$ premier, $(n+2)/2$ composé, $n/2$ composé, $n-1$ premier

Dans ce cas, $\pi(n+2) = \pi(n) + 1$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right)$.

iih1) n double de pair, $\delta_{Y_c}(n) = 0$ et $Y_c(n+2) = Y_c(n)$.

Auquel cas,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n) \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + 1 + \pi\left(\frac{n+2}{2}\right) + 0 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

puisque $\delta_{Y_c}(n+2) = 1$ dans ce cas ($n+2$ correspond alors aux cas des lignes l_3 ou l_{14}). Cela entraîne que (Ccl) est vérifiée.

iih2) n double d'impair, $\delta_{Y_c}(n) = 1$ et $Y_c(n+2) = Y_c(n) - 1$.

Auquel cas,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n) - 1 \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) - 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - 1 - \pi(n+2) + 1 + \pi\left(\frac{n+2}{2}\right) + 1 - 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

puisque $\delta_{Y_c}(n+2) = 0$ dans ce cas ($n+2$ correspond alors aux cas des lignes l_2, l_4, l_{13} ou l_{15}). Cela entraîne que (Ccl) est vérifiée.

iii) $n+1$ composé, $(n+2)/2$ composé, $n/2$ composé, $n-1$ premier

Dans ce cas, $\pi(n+2) = \pi(n)$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right)$.

iii1) n double de pair, $\delta_{Y_c}(n) = 0$ et $Y_c(n+2) = Y_c(n)$.

Auquel cas,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n) \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + 0 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

puisque $\delta_{Y_c}(n+2) = 0$ dans ce cas ($n+2$ correspond alors aux cas des lignes l_7 ou l_{11}). Cela entraîne que (Ccl) est vérifiée.

iii2) n double d'impair, $\delta_{Y_c}(n) = 1$ et $Y_c(n+2) = Y_c(n) - 1$.

Auquel cas,

$$\begin{aligned} Y_c(n+2) \quad &= Y_c(n) - 1 \\ &= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) - 1 \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - 1 - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + 1 - 1 \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2) \end{aligned}$$

puisque $\delta_{Y_c}(n+2) = -1$ dans ce cas ($n+2$ correspond alors aux cas des lignes l_6, l_8, l_{10} ou l_{12}). Cela entraîne que (Ccl) est vérifiée.

iij) $n+1$ premier, $(n+2)/2$ composé, $n/2$ composé, $n-1$ composé

Dans ce cas, $\pi(n+2) = \pi(n) + 1$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right)$.

iij1) n double de pair, $\delta_{Y_c}(n) = -1$ et $Y_c(n+2) = Y_c(n) + 1$.

Auquel cas,

$$\begin{aligned} Y_c(n+2) \quad &= Y_c(n) + 1 \\ &= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) + 1 \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + 1 + \pi\left(\frac{n+2}{2}\right) - 1 + 1 \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2) \end{aligned}$$

puisque $\delta_{Y_c}(n+2) = 1$ dans ce cas ($n+2$ correspond alors aux cas des lignes l_3 ou l_{14}). Cela entraîne que (Ccl) est vérifiée.

iij2) n double d'impair, $\delta_{Y_c}(n) = 0$ et $Y_c(n+2) = Y_c(n)$.

Auquel cas,

$$\begin{aligned} Y_c(n+2) \quad &= Y_c(n) \\ &= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - 1 - \pi(n+2) + 1 + \pi\left(\frac{n+2}{2}\right) + 0 \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2) \end{aligned}$$

puisque $\delta_{Y_c}(n+2) = 0$ dans ce cas ($n+2$ correspond alors aux cas des lignes l_2, l_4, l_{13} ou l_{15}). Cela entraîne que (Ccl) est vérifiée.

iik) $n+1$ composé, $(n+2)/2$ composé, $n/2$ composé, $n-1$ composé

Dans ce cas, $\pi(n+2) = \pi(n)$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right)$.

iik1) n double de pair, $\delta_{Y_c}(n) = -1$ et $Y_c(n+2) = Y_c(n) + 1$.

Auquel cas,

$$\begin{aligned} Y_c(n+2) \quad &= Y_c(n) + 1 \\ &= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) + 1 \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) - 1 + 1 \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2) \end{aligned}$$

puisque $\delta_{Y_c}(n+2) = 0$ dans ce cas ($n+2$ correspond alors aux cas des lignes l_7 ou l_{11}). Cela entraîne que (Ccl) est vérifiée.

iik2) n double d'impair, $\delta_{Y_c}(n) = 0$ et $Y_c(n+2) = Y_c(n)$

Auquel cas,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n) \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - 1 - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + 0 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

puisque $\delta_{Y_c}(n+2) = -1$ dans ce cas ($n+2$ correspond alors aux cas des lignes l_6, l_8, l_{10} ou l_{12}). Cela entraîne que (Ccl) est vérifiée.

6.2 Relations d'ordre entre variables

6.2.1 Etude des inégalités $Z_c(n) > Z_a(n), Z_a(n) > Y_a(n)$ et $Y_c(n) > Z_c(n)$

Des propriétés 9 et 10, on déduit que $Z_c(n) - Z_a(n) = \left\lfloor \frac{n}{4} \right\rfloor - 2\,\pi\left(\frac{n}{2}\right) + \delta_{Z_c - Z_a}(n)$ avec $\delta_{Z_c - Z_a}(n)$ égal à $1, 2$ ou 3.

$Z_c(n) - Z_a(n)$ semble globalement croissante avec de petites oscillations. On constate que $Z_c(n) > Z_a(n)$ pour $n \geqslant 240$. A partir de ce nombre, l'inégalité stricte sera toujours vérifiée car $\left\lfloor \frac{n}{4} \right\rfloor$ augmente plus souvent que $2\,\pi\left(\frac{n}{2}\right)$.

Des propriétés 9 et 11, on déduit que $Z_a(n) - Y_a(n) = 2\,\pi\left(\frac{n}{2}\right) - \pi(n) + \delta_{Z_a - Y_a}(n)$ avec $\delta_{Z_a - Y_a}(n)$ égal à $-3, -2, -1$ ou 0.

$Z_a(n) - Y_a(n)$ semble globalement croissante avec de petites oscillations. On constate que $Z_a(n) > Y_a(n)$ pour $n \geqslant 36$.

Des propriétés 10 et 12, on déduit que $Y_c(n) - Z_c(n) = 2\,\pi\left(\frac{n}{2}\right) - \pi(n) + \delta_{Y_c - Z_c}(n)$ avec $\delta_{Y_c - Z_c}(n)$ égal à $-2, -1, 0$ ou 1.

$Y_c(n) - Z_c(n)$ est une fonction croissante de n. On constate que $Y_c(n) > Z_c(n)$ pour $n \geqslant 24$.

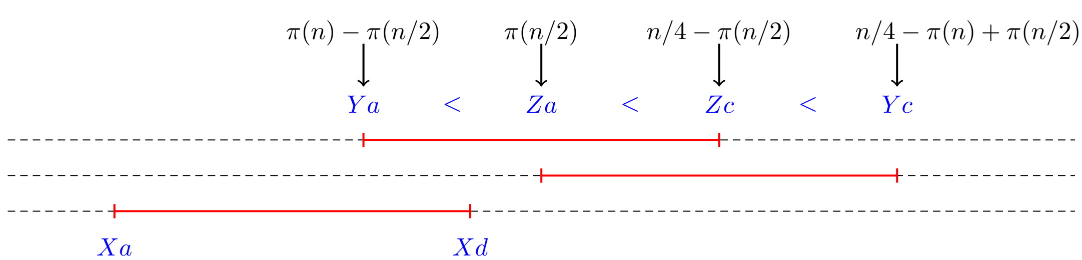
6.2.2 Ordre strict sur les 4 variables $Y_a(n), Y_c(n), Z_a(n)$ et $Z_c(n)$

Les variables $Y_a(n), Z_a(n), Z_c(n)$ et $Y_c(n)$ sont strictement ordonnées de la façon suivante :

$$Y_a(n) < Z_a(n) < Z_c(n) < Y_c(n)$$

pour tout $n \geqslant 240$.

Une représentation imagée des écarts entre variables est fournie ci-dessous, qui montre leur intrication :



6.3 D'autres propriétés

Des propriétés 9, 10, 11 et 12, on déduit :

- $Z_c(n) - Y_a(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \delta_{Z_c - Y_a}(n)$ avec $\delta_{Z_c - Y_a}(n)$ égal à $-1, 0, 1$ ou 2 ;
- $Y_c(n) - Z_a(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \delta_{Y_c - Z_a}(n)$ avec $\delta_{Y_c - Z_a}(n)$ égal à $0, 1, 2$ ou 3 ;
- $X_d(n) - X_a(n) = Z_c(n) - Y_a(n) + \delta_{2c-imp}(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \delta_{X_d - X_a}(n)$ avec $\delta_{X_d - X_a}(n)$ égal à $-1, 0, 1$ ou 2.

On constate également par programme et il faudrait le démontrer rigoureusement que :

- $X_c(n) - X_b(n) = 2\pi \left(\frac{n}{2}\right) - \pi(n) + \delta_{X_c - X_b}(n)$ avec $\delta_{X_c - X_b}(n)$ égal à $-2, -1, 0$ ou 1.

De même, on déduit des égalités dont on dispose que :

- $X_a(n) + X_b(n) = \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{X_c - X_b}(n)$ avec $\delta_{X_a + X_b}(n)$ minuscule.

La fonction $\left\lfloor \frac{n}{4} \right\rfloor - \pi(n)$ qui apparaît dans les membres droits des trois premières égalités ci-dessus est globalement croissante avec de petites oscillations. Elle s'annule pour $n = 122$.

Dans la mesure où $\left\lfloor \frac{n+2}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor + 1$ quand n est un double de pair (i.e. pour un nombre pair sur deux) tandis que $\pi(n+2) = \pi(n) + 1$ quand $n+1$ est premier (beaucoup moins souvent que pour un nombre pair sur deux), pour tout n supérieur à une valeur petite (i.e. $n > 122$), on aura systématiquement $\left\lfloor \frac{n}{4} \right\rfloor - \pi(n) > 0$.

6.4 Etude de l'inégalité $X_a(n) > 0$

Pour être assuré que $X_a(n)$ soit toujours non nul, il faudrait montrer qu'à partir d'une certaine valeur de n, l'inégalité

$$X_d(n) > \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + 2$$

est toujours vérifiée.

En effet, cette inégalité, combinée avec l'invariant $X_d(n) - X_a(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \delta_{X_d - X_a}(n)$, aurait pour conséquence qu'$X_a(n)$ serait toujours strictement positif.

On constate que

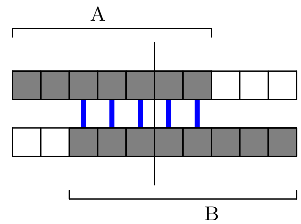
$$X_d(n) > \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + 2$$

à partir de $n \geqslant 30$.

Intuitivement, on comprend le phénomène à l'oeuvre : le nombre de nombres composés devient si grand par rapport au nombre de nombres premiers que chaque nombre composé a “beaucoup plus de chances” de se trouver complémentaire à n d'un nombre composé plutôt que d'un nombre premier. C'est ainsi qu'on constate qu'$X_d(n)$ devient vite plus grand que la somme $X_b(n) + X_c(n)$, chacun des deux termes de la somme étant quant à lui supérieur à $X_a(n)$.

6.5 Exercice subsidiaire

Posons comme exercice que l'on doive apparier bijectivement les nombres de deux ensembles ; dans le premier ensemble contenant k nombres, A sont composés et $k - A$ sont premiers tandis que dans le deuxième ensemble, contenant également k nombres, B nombres sont composés et $k - B$ sont premiers. Si $A \leqslant k/2$ et $B \leqslant k/2$, la bijection peut ne pas apparier forcément deux nombres composés. Mais dès que $A > k/2$ et $B > k/2$, un certain nombre d'appariements sont contraints d'associer un nombre composé du premier ensemble et un nombre composé du deuxième ensemble. On peut même aisément comprendre grâce au schéma ci-dessous que le nombre d'appariements associant bijectivement deux nombres composés est au moins égal à $A + B - k$.



6.6 $X_a(n)$ contrainte à être strictement positive

Parmi les nombres impairs compris entre 3 et $n/2$, très vite, plus de la moitié sont composés. De même, parmi les nombres impairs compris entre $n/2$ et $n - 3$, très vite, plus de la moitié sont composés.

Ainsi, il y a assez vite à la fois plus de la moitié des nombres qui peuvent être sommant de premier rang d'une décomposition de n qui sont composés et plus de la moitié des nombres qui peuvent être sommant de second rang d'une décomposition de n qui sont composés (i.e. $Y_c(n) > \left\lfloor \dfrac{n-2}{8} \right\rfloor$ et $Z_c(n) > \left\lfloor \dfrac{n-2}{8} \right\rfloor$) dès que $n \geqslant 244$. En effet, pour $n \geqslant 244$, $\left\lfloor \dfrac{n}{4} \right\rfloor - \pi(n) + \pi\left(\dfrac{n}{2}\right) > \left\lfloor \dfrac{n-2}{8} \right\rfloor$ et $\left\lfloor \dfrac{n}{4} \right\rfloor - \pi\left(\dfrac{n}{2}\right) > \left\lfloor \dfrac{n-2}{8} \right\rfloor$. $X_d(n)$ comptant les décompositions de la forme *composé* + *composé* est alors systématiquement supérieur à $Y_c(n) + Z_c(n) - \left\lfloor \dfrac{n-4}{4} \right\rfloor$ (cf exercice subsidiaire de la section précédente) et le restera définitivement, ce qui assure qu'$X_a(n)$ sera alors toujours strictement positif, ce qui prouve la conjecture de Goldbach binaire.

Invariant relations
between binary Goldbach's decompositions'numbers
coded in a 4 letters language

Denise Vella-Chemla

October 2014

1 Introduction

Goldbach's conjecture states that each even integer except 2 is the sum of two prime numbers. This note presents a set of invariant relations uncovered between some Goldbach's decompositions'numbers, the decompositions being coded in a 4 letters language. We will try to use those invariant relations to attempt to obtain a recurrence demonstration of Goldbach's binary conjecture. In the following, one is interested in decompositions of an even number n as a sum of two odd integers $p+q$ with $3 \leqslant p \leqslant n/2$, $n/2 \leqslant q \leqslant n-3$ and $p \leqslant q$. We call p a *n's first range sommant* and q a *n's second range sommant*.

Notations :

We will designate by :

- a : an n's decomposition of the form $p+q$ with p and q primes ;
- b : an n's decomposition of the form $p+q$ with p compound and q prime ;
- c : an n's decomposition of the form $p+q$ with p prime and q compound ;
- d : an n's decomposition of the form $p+q$ with p and q compound numbers.

Example :

40	3	5	7	9	11	13	15	17	19
	37	35	33	31	29	27	25	23	21
l_{40}	a	c	c	b	a	c	d	a	c

2 The main array

We designate by $T = (L, C) = (\ l_{n,m}\ )$ the array containing $l_{n,m}$ elements that are one of a, b, c, d letters. n belongs to the set of even integers greater than or equal to 6. m, belonging to the set of odd integers greater than or equal to 3, is an element of list of n first range sommants.

Let us consider g function defined by :

$$\begin{array}{rccl} g: & 2\mathbb{N} & \to & 2\mathbb{N}+1 \\ & x & \mapsto & 2\left\lfloor \dfrac{x-2}{4} \right\rfloor + 1 \end{array}$$

$g(6) = 3, g(8) = 3, g(10) = 5, g(12) = 5, g(14) = 7, g(16) = 7, etc.$

$g(n)$ function defines the greatest of n first range sommants.

As we only consider n decompositions of the form $p+q$ where $p \leqslant q$, in T will only appear letters $l_{n,m}$ such that $m \leqslant 2\left\lfloor \frac{n-2}{4} \right\rfloor + 1$ in such a way that T array first letters are : $l_{6,3}, l_{8,3}, l_{10,3}, l_{10,5}, l_{12,3}, l_{12,5}, l_{14,3}, l_{14,5}, l_{14,7}, etc.$

Here are first lines of array T.

C / L	3	5	7	9	11	13	15	17
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
...								

FIGURE 1 : words of even numbers between 6 and 36

Remarks :

1) words on array's diagonals called *diagonal words* have their letters either in $A_{ab} = \{a, b\}$ alphabet or in $A_{cd} = \{c, d\}$ alphabet.

2) a diagonal word codes decompositions that have the same second range sommant.
For instance, on Figure 4, letters *aaabaa* of the diagonal that begins at letter $l_{26,3} = a$ code decompositions $3 + 23, 5 + 23, 7 + 23, 9 + 23, 11 + 23$ and $13 + 23$.

3) let us designate by l_n the line whose elements are $l_{n,m}$. Line l_n contains $\left\lfloor \frac{n-2}{4} \right\rfloor$ elements.

4) n being fixed, let us call $C_{n,3}$ the column formed by $l_{k,3}$ for $6 \leqslant k \leqslant n$.

In this column $C_{n,3}$, let us distinguish two parts, the "top part" and the "bottom part" of the column.

Let us call $H_{n,3}$ column's "top part", i.e. set of $l_{k,3}$ where $6 \leqslant k \leqslant \left\lfloor \frac{n+4}{2} \right\rfloor$.

Let us call $B_{n,3}$ column's "bottom part", i.e. set of $l_{k,3}$ where $\left\lfloor \frac{n+4}{2} \right\rfloor < k \leqslant n$.

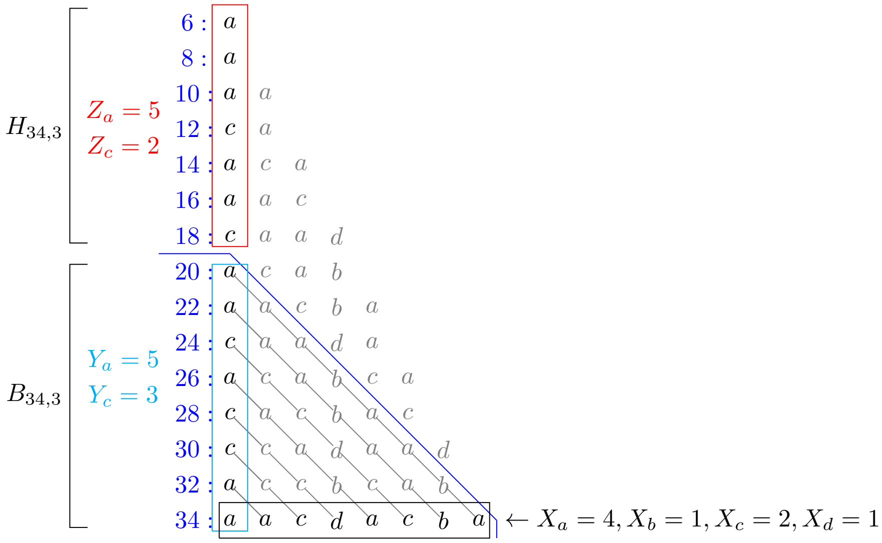


FIGURE 2 : $n = 34$

To better understand countings in next section, we will use projection P of line n on bottom part of first column $B_{n,3}$ that "associates" letters at both extremities of a diagonal (it associates to the letter that codes $p+q$ decomposition the letter that codes $3+q$ decomposition). If we consider application *proj* such that $proj(a) = proj(b) = a$ and $proj(c) = proj(d) = c$ then, since 3 is prime, $proj(l_{n,2k+1}) = l_{n-2k+2,3}$.

We can also understand the effect of this projection (that preserves second range sommant) by analyzing decompositions :

- if $p+q$ is coded by an a or a b letter, it corresponds to two possible cases in which q is prime, and so $3+q$ decomposition, containing two prime numbers, will be coded by an a letter ;
- if $p+q$ is coded by a c or a d letter, it corresponds to two possible cases in which q is compound, and so $3+q$ decomposition, of the form $prime + compound$ will be coded by a c letter.

We will also use in next section projection P' of line n on top part of the first column $H_{n,3}$ that associates to the letter that codes $p+q$ decomposition the letter that codes $3+p$ decomposition (let us note that *first range sommant* becomes *second range sommant*) ; let us analyze how such a projection will affect decompositions :

- if $p+q$ is coded by an a or c letter, it corresponds to the two possible cases in which p is prime, then $3+p$ decomposition, containing two prime numbers will be coded by an a letter ;
- if $p+q$ is coded by a b or d letter, it corresponds to the two possibl cases in which p is compound, then $3+p$ decomposition, of the form $prime + compound$ will be coded by a c letter.

3 Computations

1) We note :

- $X_a(n)$ the number of n's decompositions of the form $prime + prime$;
- $X_b(n)$ the number of n's decompositions of the form $compound + prime$;
- $X_c(n)$ the number of n's decompositions of the form $prime + compound$;
- $X_d(n)$ the number of n's decompositions of the form $compound + compound$.

$X_a(n), X_b(n), X_c(n), X_d(n)$ variables are counting logical assertions numbers.

$X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$ is the number of elements of line n.

Example : $n = 34$:
$X_a(34) = \#\{3+31, 5+29, 11+23, 17+17\} = 4$
$X_b(34) = \#\{15+19\} = 1.$
$X_c(34) = \#\{7+27, 13+21\} = 2$
$X_d(34) = \#\{9+25\} = 1$

2) Let $Y_a(n)$ (resp. $Y_c(n)$) being the number of a letters (resp. c) that appear in $B_{n,3}$. We recall that there are only a and c letters in first column because it contains letters associated with decompositions of the form $3+x$ and because 3 is prime.

Example :

- $Y_a(34) = \#\{3+17, 3+19, 3+23, 3+29, 3+31\} = 5$
- $Y_c(34) = \#\{3+21, 3+25, 3+27\} = 3$

3) Because of P projection that is a bijection, and because of a, b, c, d letters definitions, $Y_a(n) = X_a(n) + X_b(n)$ and $Y_c(n) = X_c(n) + X_d(n)$. Thus, trivially, $Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \dfrac{n-2}{4} \right\rfloor$.

Example :

$$\begin{array}{ll}
Y_a(34) & = \#\{3+17, 3+19, 3+23, 3+29, 3+31\} \\
X_a(34) & = \#\{3+31, 5+29, 11+23, 17+17\} \\
X_b(34) & = \#\{15+19\} \\
 & \\
Y_c(34) & = \#\{3+21, 3+25, 3+27\} \\
X_c(34) & = \#\{7+27, 13+21\} \\
X_d(34) & = \#\{9+25\}
\end{array}$$

4) Let $Z_a(n)$ (resp. $Z_c(n)$) being the number of a letters (resp. c) that appear in $H_{n,3}$.

Example :

- $Z_a(34) = \#\{3+3, 3+5, 3+7, 3+11, 3+13\} = 5$
- $Z_c(34) = \#\{3+9, 3+15\} = 2$

$Z_a(n) + Z_c(n) = \left\lfloor \dfrac{n-4}{4} \right\rfloor$.

Reminding identified properties

$$Y_a(n) = X_a(n) + X_b(n) \tag{1}$$

$$Y_c(n) = X_c(n) + X_d(n) \tag{2}$$

$$Y_a(n) + Y_c(n) = X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

$$Z_a(n) + Z_c(n) = \left\lfloor \frac{n-4}{4} \right\rfloor \tag{4}$$

Let us add four new properties to those ones :

$$X_a(n) + X_c(n) = Z_a(n) + \delta_{2p}(n) \tag{5}$$

with $\delta_{2p}(n)$ equal to 1 when n is the double of a prime number and equal to 0 otherwise.

$$X_b(n) + X_d(n) = Z_c(n) + \delta_{c-imp}(n) \tag{6}$$

with $\delta_{2odd-compound}(n)$ equal to 1 when n is the double of a compound odd number and equal to 0 otherwise (when there exists k such that $n = 4k$ (doubles of even numbers) or when n is the double of a prime number).

$$Z_c(n) - Y_a(n) = Y_c(n) - Z_a(n) - \delta_{4k+2}(n) \tag{7}$$

with $\delta_{4k+2}(n)$ equal to 1 when n is the double of an odd number and 0 otherwise.

$$Z_c(n) - Y_a(n) = X_d(n) - X_a(n) - \delta_{2odd-compound}(n) \tag{8}$$

Properties 1, 2 and 3 come simply from projection P's definition.

Properties 5 and 6 come simply from projection P''s definition.

One can notice a certain redundancy between the 3 booleans that are introduced here $\delta_{2p}(n)$, $\delta_{2odd-compound}(n)$ and $\delta_{4k+2}(n)$. Trivial logical assertion $(\delta_{2p}(n) \vee \delta_{2odd-compound}(n)) \rightarrow \delta_{4k+2}(n)$ is always verified.

4 Demonstrations

4.1 Utilitaries

Let us demonstrate that if n is an odd number double (i.e. of the form $4k+2$), then $\left\lfloor \frac{n-2}{4} \right\rfloor = \left\lfloor \frac{n-4}{4} \right\rfloor + 1$.
Indeed, the left part of the equality is equal to $\left\lfloor \frac{(4k+2)-2}{4} \right\rfloor = \left\lfloor \frac{4k}{4} \right\rfloor = k$.
The right part of the equality is equal to $\left\lfloor \frac{(4k+2)-4}{4} \right\rfloor + 1 = \left\lfloor \frac{4k-2}{4} \right\rfloor + 1 = (k-1) + 1 = k$.

Let us demonstrate that if n is an even number double (i.e. of the $4k$), then $\left\lfloor \frac{n-2}{4} \right\rfloor = \left\lfloor \frac{n-4}{4} \right\rfloor$.
$\left\lfloor \frac{4k-2}{4} \right\rfloor = k-1$ and $\left\lfloor \frac{4k-4}{4} \right\rfloor = k-1$.

4.2 Properties 7 and 8

4.2.1 Property 7

Property 7 enonciates that $Z_c(n) - Y_a(n) = X_d(n) - X_a(n) - \delta_{2odd-compound}(n)$ with $\delta_{2odd-compound}(n)$ that equals 1 if n is the double of an odd compound integer and equals 0 otherwise.

By definition, $Z_c(n)$ counts the number of decompositions of the form $\alpha = 3 + compound$ with *compound* strictly lesser than $n/2$ (let us call E this decompositions'set). So $Z_c(n)$ counts also the number of n's decompositions of the form $\beta = compound + y$ by bijection of second range sommant of α decomposition on first range sommant of β decomposition. But the number of decompositions of the form $compound + y$ is equal to $X_b(n) + X_d(n)$ by definition of those variables.

By definition, $Y_a(n)$ counts the number of decompositions of the form $\gamma = 3 + prime$ with *prime* strictly greater than $n/2$ (let us call F this decompositions'set). So $Y_a(n)$ counts also the number of n's decompositions of the form $\eta = x + prime$ by bijection of second range sommant of γ decomposition on second range sommant of η decomposition. But the number of decompositions of the form $x + prime$ is equal to $X_b(n) + X_a(n)$ by definition of those variables.

n's decompositions of the form $compound + prime$ are at the same time in E and in F. By computing $Z_c(n) - Y_a(n)$, we also obtain the value of $X_d(n) - X_a(n)$ by definition of what variables $Y_a(n)$, $Z_c(n)$, $X_d(n)$ et $X_a(n)$ count.

4.2.2 Property 8

Let us demonstrate that $Z_c(n) - Y_a(n) = Y_c(n) - Z_a(n) - \delta_{4k+2}(n)$ with $\delta_{4k+2}(n)$ that equals 1 if n is the double of an odd number ($\exists k \geqslant 3, n = 4k+2$) and 0 otherwise.

We use a recurrence reasoning :

i) We initialize recurrences according to the 3 types of numbers that must be studied : even doubles de pairs ($4k$), odd doubles ($4k+2$) with the odd being prime or compound.

Proprety 8 is true for $n = 14, 16$ and 18. Let us provide variables values in an array for those 3 even numbers :

n	$Z_c(n)$	$Y_a(n)$	$Y_c(n)$	$Z_a(n)$	δ_{4k+2}
14	0	2	1	2	1
16	0	2	1	3	0
18	0	2	2	3	1

ii) Property 8 is equivalent to $Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n)$.
Four cases must be considered : two cases wherein n is an odd's double (prime or compound) and $n+2$ is an even's double and two cases wherein n is an even's double and $n+2$ is an odd's double (prime or compound).

iia) *n even's double and $n+2$ prime's double* :

n	δ_{2p}	$\delta_{2odd-compound}$	δ_{4k+2}
n	0	0	0
$n+2$	1	0	1

We make the hypothesis that property 8 is true for n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \quad (H)$$

Let us demonstrate that it is true for $n+2$,

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \quad (Ccl)$$

We have $Z_a(n+2) = Z_a(n)$ and $Z_c(n+2) = Z_c(n)$.

Let us remain property 3 concerning Ys:

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \quad (3)$$

In (Ccl), we can, par by our recurrence hypothesis and by property (3), replace the left member of the equality by $Z_a(n) + Z_c(n) + 1$ and then by $Y_a(n) + Y_c(n) + 1$ (by (H)) and then by $\left\lfloor \frac{n-2}{4} \right\rfloor + 1$ (by (3)) that is equal to $\left\lfloor \frac{n}{4} \right\rfloor$.

But in (Ccl), we can also replace the right member of the equality by $\left\lfloor \frac{n}{4} \right\rfloor$ because of property (3).

We have for $n+2$ an equality between left and right sides, i.e. property 8 is verified by $n+2$. From the hypothesis that property is true for n, we have inferred property is true for $n+2$.

iib) *n even's double and $n+2$ odd compound's double* :

n	δ_{2p}	$\delta_{2odd-compound}$	δ_{4k+2}
n	0	0	0
$n+2$	0	1	1

Let us make the hypothesis that property 8 is true for n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \tag{H}$$

Let us demonstrate it is true for $n+2$,

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \tag{Ccl}$$

We have $Z_a(n+2) = Z_a(n)$ and $Z_c(n+2) = Z_c(n)$.

We have $Y_a(n+2) = Y_a(n) + 1$ and $Y_c(n+2) = Y_c(n)$.

Let us recall property 3 concerning Ys :

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

In (Ccl), one can, by recurrence hypothesis and by property 3, replace equality's left member by $Z_a(n) + Z_c(n) + 1$, then by $Y_a(n) + Y_c(n) + 1$ (because of (H)), and then by $\left\lfloor \frac{n-2}{4} \right\rfloor + 1$ (because of (3)) that is equal to $\left\lfloor \frac{n}{4} \right\rfloor$.

But in (Ccl), one can also replace equality's right member by $\left\lfloor \frac{n}{4} \right\rfloor$ because of $Y_a(n)$'s and $Y_c(n)$'s evolutions.

There is also for $n+2$ equality between left and right members of the equation, i.e. property 8 is verified by $n+2$. From the hypothesis that property is true for n, we deduced property is true for $n+2$.

iic) n *prime's double and* $n+2$ *even's double* :

n	δ_{2p}	$\delta_{2odd-compound}$	δ_{4k+2}
n	1	0	1
$n+2$	0	0	0

Let us make the hypothesis that property 8 is true for n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \tag{H}$$

Let us demonstrate it is true for $n+2$,

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \tag{Ccl}$$

We have $Z_a(n+2) = Z_a(n) + 1$ et $Z_c(n+2) = Z_c(n)$.

Let us recall property 3 concerning Ys :

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

In (Ccl), one can, by recurrence hypothesis and by property 3, replace equality's left member by $Z_a(n) + Z_c(n)+1$ then by $Y_a(n)+Y_c(n)$ (because of (H)), and then by $\left\lfloor \frac{n-2}{4} \right\rfloor$ (because of (3)) that is equal to $\left\lfloor \frac{n}{4} \right\rfloor$.

But in (Ccl), one can also replace equality's right member by $\left\lfloor \frac{n}{4} \right\rfloor$ because of property (3).

There is also for $n+2$ equality between left and right members of the equation, i.e. property 8 is verified by $n+2$. From the hypothesis that property is true for n, we deduced property is true for $n+2$.

iid) *n odd compound's double and $n+2$ even double* :

n	δ_{2p}	$\delta_{2odd-compound}$	δ_{4k+2}
n	0	1	1
$n+2$	0	0	0

Let us make the hypothesis that property 8 is true for n,

$$Z_a(n) + Z_c(n) + \delta_{4k+2}(n) = Y_a(n) + Y_c(n) \qquad (H)$$

Let us demonstrate it is true for $n+2$,

$$Z_a(n+2) + Z_c(n+2) + \delta_{4k+2}(n+2) = Y_a(n+2) + Y_c(n+2) \qquad (Ccl)$$

We have $Z_a(n+2) = Z_a(n)$ et $Z_c(n+2) = Z_c(n) + 1$.

Let us recall property 3 concerning Ys :

$$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \qquad (3)$$

In (Ccl), one can, by recurrence hypothesis and by property 3, replace equality's left member by $Z_a(n) + Z_c(n) + 1$ puis par $Y_a(n) + Y_c(n)$ (because of (H)) then by $\left\lfloor \frac{n-2}{4} \right\rfloor$ (because of (3)) that is equal to $\left\lfloor \frac{n}{4} \right\rfloor$.

But in (Ccl), one can also replace equality's right member by $\left\lfloor \frac{n}{4} \right\rfloor$ because of property (3).

There is also for $n+2$ equality between left and right members of the equation, i.e. property 8 is verified by $n+2$. From the hypothesis that property is true for n, we deduced property is true for $n+2$.

5 Variables evolution

5.1 Counting decompositions of the forme $3+p$ (called "bottom-ones")

1) $Z_a(n+2) = Z_a(n)$ and $Z_c(n+2) = Z_c(n)$ when n is an even double. Indeed, $Z_a(n)$ (resp. $Z_c(n)$) counts number of primes (resp. odd compound numbers) strictly lesser than $\frac{n}{2}$ and there are as many as primes (resp. odd compound numbers) lesser than an even number than there are primes (resp. odd compound numbers) lesser than its immediate successor.

2) $Z_a(n+2) = Z_a(n) + 1$ and $Z_c(n+2) = Z_c(n)$ when n is a prime double ;

3) $Z_a(n+2) = Z_a(n)$ and $Z_c(n+2) = Z_c(n) + 1$ when n is an odd compound number's double.

5.2 Counting decompositions of the form $3+q$ (called "top-ones")

In the case in which $n+2$ is an odd's double, we only add a number to $H_{n+2,3}$ interval ; if this number $n-1$ is prime (resp. compound), $Y_a(n+2) = Y_a(n) + 1$ (resp. $Y_c(n+2) = Y_c(n) + 1$).

In the case in which $n+2$ is an even's double, we only add a number to the top extremity of the interval and we take off a number at the bottom extremity of the interval. From this fact, 4 cases have to be studied. Let us study how the decompositions'set $H_{n+2,3}$ evoluate.

- if $n-1$ and $\frac{n}{2}$ are both primes, we take off at the bottom and we put on at the top of the interval $H_{n+2,3}$ two letters of same kind, so $Y_a(n+2) = Y_a(n)$;
- if $n-1$ is prime and $\frac{n}{2}$ is compound then $Y_a(n+2) = Y_a(n) + 1$;

- if $n-1$ is compound and $\frac{n}{2}$ is prime then $Y_a(n+2) = Y_a(n) - 1$;
- if $n-1$ and $\frac{n}{2}$ are both compound, we take off at the bottom and we put on at the top of the interval $H_{n+2,3}$ two letters of same kind, then $Y_a(n+2) = Y_a(n)$.

6 Using variables'gaps

We are going to show that $X_a(n)$ can never be equal to 0 for $n \geqslant C$, i.e. that every even number $n \geqslant C$ can be written as a sum of two primes, i.e. verifies binary Goldbach's conjecture.

Let us present in more details what variables $Z_a(n), Z_c(n), Y_a(n)$ et $Y_c(n)$ represent.

- $Z_a(n)$ counts with a maximum error of 2 the number of prime numbers that are lesser than or equal to $\frac{n}{2}$;

$$Z_a(n) = \pi\left(\frac{n}{2}\right) + \delta_{Z_a}(n) \tag{9}$$

  with $\delta_{Z_a}(n)$ equal to -2 if n is a prime's double and equal to -1 otherwise ;

- $Z_c(n)$ counts with a maximum error of 1 the number of odd compound numbers that are lesser than or equal to $\frac{n}{2}$;

$$Z_c(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi\left(\frac{n}{2}\right) + \delta_{Z_c}(n) \tag{10}$$

  with $\delta_{Z_c}(n)$ equal to 1 if n is a prime's double and equal to 0 otherwise ;

- $Y_a(n)$ count with a maximum error of 1 the number of prime numbers that are between $\frac{n}{2}$ and n ;

$$Y_a(n) = \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \tag{11}$$

  with $\delta_{Y_a}(n)$ equal to $-1, 0$ or 1 ($\delta_{Y_a}(n)$ is equal to 0 when $n-1$ and $n/2$ are both primes or both compound, $\delta_{Y_a}(n)$ is equal to -1 when $n-1$ is prime while $n/2$ is compound, and at last, $\delta_{Y_a}(n)$ is equal to 1 when $n-1$ is compound while $n/2$ is prime) ;

- $Y_c(n)$ counts with a maximum error of 1 the number of odd compound numbers that are between $\frac{n}{2}$ and n ;

$$Y_c(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \tag{12}$$

  with $\delta_{Y_c}(n)$ equal to $-1, 0$ or 1. $\delta_{Y_c}(n)$'s values will be provided in a detailled way in section demonstrating property 12.

6.1 Demonstrations of properties 9, 10, 11 and 12

6.1.1 Property 9 : invariant relation concerning $Z_a(n)$

i) Initialisation : (9) is true for $n = 14, 16, 18$ and 20.

Indeed, we have :

n	$Z_a(n)$	$\pi\left(\frac{n}{2}\right)$	$\delta_{Z_a}(n)$
14	2	4	-2
16	3	4	-1
18	3	4	-1
20	3	4	-1
22	3	5	-2

ii) Let us demonstrate by recurrence that if (9) is true for n, it is also true for $n+2$.

Let us make the hypothesis that property 9 is true for n,

$$Z_a(n) = \pi\left(\frac{n}{2}\right) + \delta_{Z_a}(n) \qquad (H)$$

Let us demonstrate it is true for $n+2$,

$$Z_a(n+2) = \pi\left(\frac{n+2}{2}\right) + \delta_{Z_a}(n+2) \qquad (Ccl)$$

Let us distinguish 4 cases, as in paragraph 4.2.2.

iia) n even's double, $n+2$ prime's double.

In that case, $Z_a(n+2) = Z_a(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right) + 1$ and $\delta_{Z_a}(n) = -1$.

So we have,

$$\begin{aligned} Z_a(n+2) &= Z_a(n) \\ &= \pi\left(\frac{n}{2}\right) + \delta_{Z_a}(n) \\ &= \pi\left(\frac{n+2}{2}\right) - 1 + \delta_{Z_a}(n) \\ &= \pi\left(\frac{n+2}{2}\right) - 1 - 1 \\ &= \pi\left(\frac{n+2}{2}\right) + \delta_{Z_a}(n+2) \end{aligned}$$

with $\delta_{Z_a}(n+2) = -2$ as expected since in that case, $n+2$ is a prime's double.

iib) n even's double, $n+2$ odd compound's double.

In that case, $Z_a(n+2) = Z_a(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$ and $\delta_{Z_a}(n) = -1$.

So we have,

$$\begin{aligned} Z_a(n+2) &= Z_a(n) \\ &= \pi\left(\frac{n}{2}\right) + \delta_{Z_a}(n) \\ &= \pi\left(\frac{n+2}{2}\right) - 1 \\ &= \pi\left(\frac{n+2}{2}\right) + \delta_{Z_a}(n+2) \end{aligned}$$

with $\delta_{Z_a}(n+2) = -1$ as expected since in that case, $n+2$ is an odd compound's double.

iic) n prime's double, $n+2$ even's double.

In that case, $Z_a(n+2) = Z_a(n) + 1$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$ and $\delta_{Z_a}(n) = -2$.

So we have,

$$\begin{aligned} Z_a(n+2) &= Z_a(n) + 1 \\ &= \pi\left(\frac{n}{2}\right) + \delta_{Z_a}(n) + 1 \\ &= \pi\left(\frac{n+2}{2}\right) - 2 + 1 \\ &= \pi\left(\frac{n+2}{2}\right) - 1 \\ &= \pi\left(\frac{n+2}{2}\right) + \delta_{Z_a}(n+2) \end{aligned}$$

with $\delta_{Z_a}(n+2) = -1$ as expected since in that case, $n+2$ is an even's double.

iid) n odd compound's double, $n+2$ even's double.

In that case, $Z_a(n+2) = Z_a(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$ and $\delta_{Z_a}(n) = -1$.

So we have,

$$\begin{aligned} Z_a(n+2) &= Z_a(n) \\ &= \pi\left(\frac{n}{2}\right) + \delta_{Z_a}(n) \\ &= \pi\left(\frac{n+2}{2}\right) - 1 \\ &= \pi\left(\frac{n+2}{2}\right) + \delta_{Z_a}(n+2) \end{aligned}$$

with $\delta_{Z_a}(n+2) = -1$ as expected since in that case, $n+2$ is an even's double.

6.1.2 Property 10 : invariant relation concerning $Z_c(n)$

i) Initialisation : (10) is true for $n = 14, 16, 18$ and 20.

We have :

n	$Z_c(n)$	$\left\lfloor \frac{n}{4} \right\rfloor$	$\pi\left(\frac{n}{2}\right)$	$\delta_{Z_c}(n)$
14	0	3	4	1
16	0	4	4	0
18	0	4	4	0
20	1	5	4	0
22	1	5	5	1

and we verify that (10) is true for those 4 numbers.

ii) Let us demonstrate by recurrence that if (10) is true for n, it is also true for $n+2$.

Let us make the hypothesis that property 10 is true for n,

$$Z_c(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi\left(\frac{n}{2}\right) + \delta_{Z_c}(n) \qquad (H)$$

Let us demonstrate it is also true for $n+2$,

$$Z_c(n+2) = \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + \delta_{Z_c}(n+2) \qquad (Ccl)$$

Let us study our 4 cases again.

iia) n even's double, $n+2$ prime's double.

Dans ce cas, $Z_c(n+2) = Z_c(n)$, $\left\lfloor \frac{n+2}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right) + 1$ et $\delta_{Z_c}(n) = 0$.

In that case,

$$\begin{aligned} Z_c(n+2) &= Z_c(n) \\ &= \left\lfloor \frac{n}{4} \right\rfloor - \pi\left(\frac{n}{2}\right) + \delta_{Z_c}(n) \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + 1 + \delta_{Z_c}(n) \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + 1 + 0 \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + \delta_{Z_c}(n+2) \end{aligned}$$

with $\delta_{Z_c}(n+2) = 1$ as expected since in that case $n+2$ is a prime's double.

iib) n even's double, $n+2$ odd compound's double.

In that case, $Z_c(n+2) = Z_c(n)$, $\left\lfloor \frac{n+2}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$ et $\delta_{Z_c}(n) = 0$.

So we have,

$$\begin{aligned}
Z_c(n+2) &= Z_c(n)\\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi\left(\frac{n}{2}\right) + \delta_{Z_c}(n)\\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + \delta_{Z_c}(n)\\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + 0\\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + \delta_{Z_c}(n+2)
\end{aligned}$$

with $\delta_{Z_c}(n+2) = 0$ as expected in that case since $n+2$ is an odd compound's double.

iic) n prime's double, $n+2$ even's double.

In that case, $Z_c(n+2) = Z_c(n)$, $\left\lfloor \frac{n+2}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor + 1$, $\pi\left(\frac{n+2}{4}\right) = \pi\left(\frac{n}{2}\right)$ et $\delta_{Z_c}(n) = 1$.

So we have,

$$\begin{aligned}
Z_c(n+2) &= Z_c(n)\\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi\left(\frac{n}{2}\right) + \delta_{Z_c}(n)\\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{4}\right) - 1 + \delta_{Z_c}(n)\\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) - 1 + 1\\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + \delta_{Z_c}(n+2)
\end{aligned}$$

with $\delta_{Z_c}(n+2) = 0$ as expected since in that case $n+2$ is an even's double.

iid) n odd compound's double, $n+2$ even's double.

In that case, $Z_c(n+2) = Z_c(n) + 1$, $\left\lfloor \frac{n+2}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor + 1$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$ and $\delta_{Z_c}(n) = 0$.

So we have,

$$\begin{aligned}
Z_c(n+2) &= Z_c(n)\\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi\left(\frac{n}{2}\right) + \delta_{Z_c}(n)\\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - 1 - \pi\left(\frac{n+2}{2}\right) + 1 + \delta_{Z_c}(n)\\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) - 1 + 1\\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi\left(\frac{n+2}{2}\right) + \delta_{Z_c}(n+2)
\end{aligned}$$

with $\delta_{Z_c}(n+2) = 0$ as expected since in that case $n+2$ is an even's double.

6.1.3 Property 11 : invariant relation concerning $Y_a(n)$

The objective is to demonstrate why the invariant relation concerning $Y_a(n)$ and that is :

$$Y_a(n) = \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n)$$

is always verified. In this aim, 16 cases are to be distinguished, according to primality characters of 4 numbers : $\frac{n}{2}$, $\frac{n+2}{2}$, $n-1$ and $n+1$, those primality characters having an influence on $Y_a(n)$, $\pi(n)$, $\pi\left(\frac{n}{2}\right)$ and $\delta_{Y_a}(n)$ evolutions.

i) recurrences initialisations : for 5 cases among the 16 to be envisagd, there is a contradiction (we called them $C1$ to $C5$ in bottom of the array below, contradiction coming for cases $C1$ to $C4$ from the fact that one can't have simmultaneously $n/2$ and $(n+2)/2$ that are both prime since they are consecutive integers) ; $C5$ is a contradiction because if $n-1$ and $n+1$ ar twin primes, their "father" (the even number between them) can be divided by 3 and so the half of this father, that is $n/2$, can't be a prime number too ; this is represented by crosses in first, third and fourth columns). For the remaining 11 cases, we must initialize recurrences. In the array below, we provide values that permit easily to verify that for small integers, property 11 is systematically verified.

n	$n/2$ *is prime*	$(n+2)/2$ *is prime*	$n-1$ *is prime*	$n+1$ *is prime*	$Y_a(n)$	$\pi(n)$	$\pi(n/2)$	$\delta_{Y_a}(n)$
14	×	−	×	−	2	6	4	0
16	−	−	−	×	2	6	4	0
18	−	−	×	×	2	7	4	−1
20	−	×	×	−	3	8	4	−1
22	×	−	−	×	4	8	5	1
26	×	−	−	−	4	9	6	1
36	−	×	−	×	4	11	7	0
48	−	−	×	−	5	15	9	−1
50	−	−	−	−	6	15	9	0
56	−	×	−	−	7	16	9	0
60	−	×	×	×	6	17	10	−1
$C1$	×	×	×	×	−	−	−	−
$C2$	×	×	×	−	−	−	−	−
$C3$	×	×	−	×	−	−	−	−
$C4$	×	×	−	−	−	−	−	−
$C5$	×	−	×	×	−	−	−	−

ii) Let us demonstrate by recurrence that if (11) is true for n, it is true for $n+2$ too.

Let us make the hypothesis that property 11 is true for n,

$$Y_a(n) = \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \qquad (H)$$

Let us demonstrate it is true for $n+2$,

$$Y_a(n+2) = \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \qquad (Ccl)$$

Let us study the 11 cases listed in last section.

iia) $n+1$ compound, $(n+2)/2$ compound, $n/2$ prime, $n-1$ prime

In that case, $\pi(n+2) = \pi(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$, $\delta_{Y_a}(n) = 0$ and $Y_a(n+2) = Y_a(n)$.

So we have,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

since $\delta_{Y_a}(n+2) = 0$ in that case. It implies that (Ccl) is verified.

iib) $n+1$ prime, $(n+2)/2$ compound, $n/2$ compound, $n-1$ compound

In that case, $\pi(n+2) = \pi(n) + 1$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$, $\delta_{Y_a}(n) = 0$ and $Y_a(n+2) = Y_a(n)$.

So we have,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \\ &= \pi(n+2) - 1 - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

since $\delta_{Y_a}(n+2) = -1$ in that case. This implies that (Ccl) is verified.

iic) $n+1$ compound, $(n+2)/2$ compound, $n/2$ prime, $n-1$ compound

In that case, $\pi(n+2) = \pi(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$, $\delta_{Y_a}(n) = 1$ and $Y_a(n+2) = Y_a(n) - 1$.

So we have,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) - 1 \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) - 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + 1 - 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

since $\delta_{Y_a}(n+2) = 0$ in that case. This implies that (Ccl) is verified.

iid) $n+1$ prime, $(n+2)/2$ prime, $n/2$ compound, $n-1$ prime

In that case, $\pi(n+2) = \pi(n) + 1$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right) + 1$, $\delta_{Y_a}(n) = -1$ and $Y_a(n+2) = Y_a(n) + 1$.

So we have,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) + 1 \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) + 1 \\ &= \pi(n+2) - 1 - \pi\left(\frac{n+2}{2}\right) + 1 - 1 + 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

since $\delta_{Y_a}(n+2) = 0$ in that case. This implies that (Ccl) is verified.

iie) $n+1$ compound, $(n+2)/2$ prime, $n/2$ compound, $n-1$ prime

In that case, $\pi(n+2) = \pi(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right) + 1$, $\delta_{Y_a}(n) = -1$ and $Y_a(n+2) = Y_a(n) + 1$.

So we have,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) + 1 \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) + 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + 1 - 1 + 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

since $\delta_{Y_a}(n+2) = 1$ in that case. This implies that (Ccl) is verified.

iif) $n+1$ prime, $(n+2)/2$ prime, $n/2$ compound, $n-1$ compound

In that case, $\pi(n+2) = \pi(n) + 1$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right) + 1$, $\delta_{Y_a}(n) = 0$ and $Y_a(n+2) = Y_a(n)$.

So we have,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \\ &= \pi(n+2) - 1 - \pi\left(\frac{n+2}{2}\right) + 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

since $\delta_{Y_a}(n+2) = 0$ in that case. This implies that (Ccl) is verified.

iig) $n+1$ compound, $(n+2)/2$ prime, $n/2$ compound, $n-1$ compound

In that case, $\pi(n+2) = \pi(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right) + 1$, $\delta_{Y_a}(n) = 0$ and $Y_a(n+2) = Y_a(n)$.

So we have,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + 1 + 0 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

since $\delta_{Y_a}(n+2) = 1$ in that case. This implies that (Ccl) is verified.

iih) $n+1$ prime, $(n+2)/2$ compound, $n/2$ compound, $n-1$ prime

In that case, $\pi(n+2) = \pi(n)+1$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$, $\delta_{Y_a}(n) = -1$ and $Y_a(n+2) = Y_a(n)+1$.

So we have,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) + 1 \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) + 1 \\ &= \pi(n+2) - 1 - \pi\left(\frac{n+2}{2}\right) - 1 + 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

since $\delta_{Y_a}(n+2) = -1$ in that case. This implies that (Ccl) is verified.

iii) $n+1$ compound, $(n+2)/2$ compound, $n/2$ compound, $n-1$ prime

In that case, $\pi(n+2) = \pi(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$, $\delta_{Y_a}(n) = -1$ and $Y_a(n+2) = Y_a(n)+1$.

So we have,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) + 1 \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) + 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) - 1 + 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

since $\delta_{Y_a}(n+2) = 0$ in that case. It implies that (Ccl) is verified.

iij) $n+1$ prime, $(n+2)/2$ compound, $n/2$ prime, $n-1$ compound

In that case, $\pi(n+2) = \pi(n)+1$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$, $\delta_{Y_a}(n) = 1$ and $Y_a(n+2) = Y_a(n)-1$.

So we have,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) - 1 \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) - 1 \\ &= \pi(n+2) - 1 - \pi\left(\frac{n+2}{2}\right) + 1 - 1 \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

since $\delta_{Y_a}(n+2) = -1$ in that case. This implies that (Ccl) is verified.

iik) $n+1$ compound, $(n+2)/2$ compound, $n/2$ compound, $n-1$ compound

In that case, $\pi(n+2) = \pi(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$, $\delta_{Y_a}(n) = 0$ and $Y_a(n+2) = Y_a(n)$.

So we have,

$$\begin{aligned} Y_a(n+2) &= Y_a(n) \\ &= \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \\ &= \pi(n+2) - \pi\left(\frac{n+2}{2}\right) + \delta_{Y_a}(n+2) \end{aligned}$$

since $\delta_{Y_a}(n+2) = 0$ in that case. This implies that (Ccl) is verified.

6.1.4 Property 12 : invariant relation concerning $Y_c(n)$

The objective is to demonstrate why the invariant relation concerning $Y_c(n)$ and that is :

$$Y_c(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n)$$

is always verified.

i) recurrences'initializations :

n	$n/2$ *is prime*	$(n+2)/2$ *is prime*	$n-1$ *is prime*	$n+1$ *is prime*	$Y_c(n)$	$\left\lfloor \frac{n}{4} \right\rfloor$	$\pi(n)$	$\pi(n/2)$	$\delta_{Y_c}(n)$
14	×	–	×	–	1	3	6	4	0
16	–	–	–	×	1	4	6	4	−1
18	–	–	×	×	2	4	7	4	1
20	–	×	×	–	1	5	8	4	0
22	×	–	–	×	1	5	8	5	−1
26	×	–	–	–	2	6	9	6	−1
36	–	×	–	×	4	9	11	7	−1
48	–	–	×	–	6	12	15	9	0
50	–	–	–	–	6	12	15	9	0
56	–	×	–	–	6	14	16	9	−1
60	–	×	×	×	8	15	17	10	0

It is easy to verify that for small integers, property 12 is well systematically verified.

ii) Let us demonstrate by recurrence that if (12) is true for n, it is true for $n+2$.

Let us make the hypothesis that property 12 is true for n,

$$Y_c(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \qquad (H)$$

Let us demonstrate it is true for $n+2$,

$$Y_c(n+2) = \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2) \qquad (Ccl)$$

We find here another time the 11 cases identified for demonstrating property 11 ; sometimes, there are two subcases, when $n/2$ is compound, according to the fact that n is an even's double in which case $\left\lfloor \frac{n+2}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor$ or that n is an odd's double $\left\lfloor \frac{n+2}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor + 1$.

In the array below are provided $\delta_{Y_c}(n)$'s values according to the booleans that must be considered (in first column, we indicate a number of line l_i that will be useful in the following ; an example of a small integer is provided in penultimate column, to fix ideas ; the letter corresponding to the recurrence type intervening (cf after the array) is provided in last column :

	$n-1$ *is prime*	$n+1$ *is prime*	$n/2$ *is prime*	$(n+2)/2$ *is prime*	$\delta_{4k+2}(n)$	$\delta_{Y_c}(n)$	*ex*	*case*
l_1	×	–	×	–	×	0	14	a
l_2	×	–	–	×	–	0	20	e
l_3	×	–	–	–	×	0	54	i
l_4	×	–	–	–	–	1	48	i
l_5	–	×	×	–	×	-1	22	b
l_6	–	×	–	×	–	-1	36	f
l_7	–	×	–	–	×	0	66	j
l_8	–	×	–	–	–	-1	16	j
l_9	–	–	×	–	×	-1	26	c
l_{10}	–	–	–	×	–	-1	56	g
l_{11}	–	–	–	–	×	0	50	k
l_{12}	–	–	–	–	–	-1	64	k
l_{13}	×	×	–	×	–	0	60	d
l_{14}	×	×	–	–	×	1	18	h
l_{15}	×	×	–	–	–	0	108	h

iia) $n+1$ compound, $(n+2)/2$ compound, $n/2$ prime, $n-1$ prime

In that case, $\pi(n+2)=\pi(n)$, $\pi\left(\dfrac{n+2}{2}\right)=\pi\left(\dfrac{n}{2}\right)$, $\delta_{Y_c}(n)=0$ and $Y_c(n+2)=Y_c(n)$.

So we have,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n)\\
&= \left\lfloor\frac{n}{4}\right\rfloor-\pi(n)+\pi\left(\frac{n}{2}\right)+\delta_{Y_c}(n)\\
&= \left\lfloor\frac{n+2}{4}\right\rfloor-1-\pi(n+2)+\pi\left(\frac{n+2}{2}\right)+0\\
&= \left\lfloor\frac{n+2}{4}\right\rfloor-\pi(n+2)+\pi\left(\frac{n+2}{2}\right)+\delta_{Y_c}(n+2)
\end{aligned}$$

since $\delta_{Y_c}(n+2)=-1$ in that case ($n+2$ corresponds than to one of the cases of lines l_6, l_8, l_{10} or l_{12} because n being an odd's double, $n+2$ can't be one). This implies that (Ccl) is verified.

iib) $n+1$ prime, $(n+2)/2$ compound, $n/2$ prime, $n-1$ compound

In that case, $\pi(n+2)=\pi(n)+1$, $\pi\left(\dfrac{n+2}{2}\right)=\pi\left(\dfrac{n}{2}\right)$, $\delta_{Y_c}(n)=-1$ and $Y_c(n+2)=Y_c(n)+1$.

So we have,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n)+1\\
&= \left\lfloor\frac{n}{4}\right\rfloor-\pi(n)+\pi\left(\frac{n}{2}\right)+\delta_{Y_c}(n)+1\\
&= \left\lfloor\frac{n+2}{4}\right\rfloor-1-\pi(n+2)+1+\pi\left(\frac{n+2}{2}\right)-1+1\\
&= \left\lfloor\frac{n+2}{4}\right\rfloor-\pi(n+2)+\pi\left(\frac{n+2}{2}\right)+\delta_{Y_c}(n+2)
\end{aligned}$$

since $\delta_{Y_c}(n+2)=0$ in that case ($n+2$ corresponds then to one of the cases of lines l_2, l_{13} or l_{15} because n being an odd's double, $n+2$ can't be one). This implies that (Ccl) is verified.

iic) $n+1$ compound, $(n+2)/2$ compound, $n/2$ prime, $n-1$ compound

In that case, $\pi(n+2)=\pi(n)$, $\pi\left(\dfrac{n+2}{2}\right)=\pi\left(\dfrac{n}{2}\right)$, $\delta_{Y_c}(n)=-1$ and $Y_c(n+2)=Y_c(n)+1$.

So we have,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n)+1\\
&= \left\lfloor\frac{n}{4}\right\rfloor-\pi(n)+\pi\left(\frac{n}{2}\right)+\delta_{Y_c}(n)+1\\
&= \left\lfloor\frac{n+2}{4}\right\rfloor-1-\pi(n+2)+\pi\left(\frac{n+2}{2}\right)-1+1\\
&= \left\lfloor\frac{n+2}{4}\right\rfloor-\pi(n+2)+\pi\left(\frac{n+2}{2}\right)+\delta_{Y_c}(n+2)
\end{aligned}$$

since $\delta_{Y_c}(n+2) = -1$ in that case ($n+2$ corresponds then to one of the cases of lines l_6, l_8, l_{10} or l_{12} because n being an odd's double, $n+2$ can't be one). This implies that (Ccl) is verified.

iid) $n+1$ prime, $(n+2)/2$ prime, $n/2$ compound, $n-1$ prime

In that case, $\pi(n+2) = \pi(n)+1$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right)+1$, $\delta_{Y_c}(n) = 0$ and $Y_c(n+2) = Y_c(n)$.

n is mandatory an even's double.

So we have,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n) \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + 1 + \pi\left(\frac{n+2}{2}\right) - 1 + 0 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

since $\delta_{Y_c}(n+2) = 0$ in that case ($n+2$ corresponds then to the case of line l_1). This implies that (Ccl) is verified.

iie) $n+1$ compound, $(n+2)/2$ prime, $n/2$ compound, $n-1$ prime

In that case, $\pi(n+2) = \pi(n)$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right)+1$, $\delta_{Y_c}(n) = 0$ and $Y_c(n+2) = Y_c(n)$.

n is mandatory an even's double.

So we have,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n) \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) - 1 + 0 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

since $\delta_{Y_c}(n+2) = -1$ in that case ($n+2$ corresponds then to one of the cases of lines l_5 or l_9). This implies that (Ccl) is verified.

iif) $n+1$ prime, $(n+2)/2$ prime, $n/2$ compound, $n-1$ compound

In that case, $\pi(n+2) = \pi(n)+1$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right)+1$, $\delta_{Y_c}(n) = -1$ and $Y_c(n+2) = Y_c(n)+1$.

n is mandatory an even's double.

So we have,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n) + 1 \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) + 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + 1 + \pi\left(\frac{n+2}{2}\right) - 1 - 1 + 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

since $\delta_{Y_c}(n+2) = 0$ in that case ($n+2$ corresponds then to the case of line l_1). This implies that (Ccl) is verified.

iig) $n+1$ compound, $(n+2)/2$ prime, $n/2$ compound, $n-1$ compound

In that case, $\pi(n+2) = \pi(n)$, $\pi\left(\dfrac{n+2}{2}\right) = \pi\left(\dfrac{n}{2}\right)+1$, $\delta_{Y_c}(n) = -1$ and $Y_c(n+2) = Y_c(n)+1$.

n is mandatory an even's double.

So we have,

$$\begin{aligned}Y_c(n+2) &= Y_c(n)+1\\ &= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) + 1\\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) - 1 - 1 + 1\\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)\end{aligned}$$

since $\delta_{Y_c}(n+2) = -1$ in that case ($n+2$ corresponds then to one of the cases of lines l_5 or l_9). This implies that (Ccl) is verified.

iih) $n+1$ prime, $(n+2)/2$ compound, $n/2$ compound, $n-1$ prime

In that case, $\pi(n+2) = \pi(n)+1$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$.

iih1) n even's double, $\delta_{Y_c}(n) = 0$ and $Y_c(n+2) = Y_c(n)$.

So we have,

$$\begin{aligned}Y_c(n+2) &= Y_c(n)\\ &= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n)\\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + 1 + \pi\left(\frac{n+2}{2}\right) + 0\\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)\end{aligned}$$

since $\delta_{Y_c}(n+2) = 1$ in that case ($n+2$ corresponds then to one of the cases of lines l_3 or l_{14}). This implies that (Ccl) is verified.

iih2) n odd's double, $\delta_{Y_c}(n) = 1$ and $Y_c(n+2) = Y_c(n) - 1$.

So we have,

$$\begin{aligned}Y_c(n+2) &= Y_c(n)-1\\ &= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) - 1\\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - 1 - \pi(n+2) + 1 + \pi\left(\frac{n+2}{2}\right) + 1 - 1\\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)\end{aligned}$$

since $\delta_{Y_c}(n+2) = 0$ in that case ($n+2$ corresponds then to one of the cases of lines l_2, l_4, l_{13} or l_{15}). This implies that (Ccl) is verified.

iii) $n+1$ compound, $(n+2)/2$ compound, $n/2$ compound, $n-1$ prime

In that case, $\pi(n+2) = \pi(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$.

iii1) n even's double, $\delta_{Y_c}(n) = 0$ and $Y_c(n+2) = Y_c(n)$.

So we have,

$$\begin{aligned}Y_c(n+2) &= Y_c(n)\\ &= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n)\\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + 0\\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)\end{aligned}$$

since $\delta_{Y_c}(n+2) = 0$ in that case ($n+2$ corresponds then to one of the cases of lines l_7 or l_{11}). This implies that (Ccl) is verified.

iii2) n odd's double, $\delta_{Y_c}(n) = 1$ and $Y_c(n+2) = Y_c(n) - 1$.

So we have,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n) - 1 \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) - 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - 1 - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + 1 - 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

since $\delta_{Y_c}(n+2) = -1$ in that case ($n+2$ corresponds then to one of the cases of lines l_6, l_8, l_{10} or l_{12}). This implies that (Ccl) is verified.

iij) $n+1$ prime, $(n+2)/2$ compound, $n/2$ compound, $n-1$ compound

In that case, $\pi(n+2) = \pi(n) + 1$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$.

iij1) n even's double, $\delta_{Y_c}(n) = -1$ and $Y_c(n+2) = Y_c(n) + 1$.

So we have,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n) + 1 \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) + 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + 1 + \pi\left(\frac{n+2}{2}\right) - 1 + 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

since $\delta_{Y_c}(n+2) = 1$ in that case ($n+2$ corresponds then to one of the cases of lines l_3 or l_{14}). This implies that (Ccl) is verified.

iij2) n odd's double, $\delta_{Y_c}(n) = 0$ and $Y_c(n+2) = Y_c(n)$.

So we have,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n) \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - 1 - \pi(n+2) + 1 + \pi\left(\frac{n+2}{2}\right) + 0 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

since $\delta_{Y_c}(n+2) = 0$ in that case ($n+2$ corresponds then to one of the cases of lines l_2, l_4, l_{13} or l_{15}). This implies that (Ccl) is verified.

iik) $n+1$ compound, $(n+2)/2$ compound, $n/2$ compound, $n-1$ compound

In that case, $\pi(n+2) = \pi(n)$, $\pi\left(\frac{n+2}{2}\right) = \pi\left(\frac{n}{2}\right)$.

iik1) n even's double, $\delta_{Y_c}(n) = -1$ and $Y_c(n+2) = Y_c(n) + 1$.

So we have,

$$\begin{aligned}
Y_c(n+2) &= Y_c(n) + 1 \\
&= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) + 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) - 1 + 1 \\
&= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2)
\end{aligned}$$

since $\delta_{Y_c}(n+2) = 0$ in that case ($n+2$ corresponds then to one of the cases of lines l_7 or l_{11}). This implies that (Ccl) is verified.

iik2) n odd compound's double, $\delta_{Y_c}(n) = 0$ and $Y_c(n+2) = Y_c(n)$

So we have,

$$\begin{aligned} Y_c(n+2) &= Y_c(n) \\ &= \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - 1 - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + 0 \\ &= \left\lfloor \frac{n+2}{4} \right\rfloor - \pi(n+2) + \pi\left(\frac{n+2}{2}\right) + \delta_{Y_c}(n+2) \end{aligned}$$

since $\delta_{Y_c}(n+2) = -1$ in that case ($n+2$ corresponds to cases in lines l_6, l_8, l_{10} or l_{12}). This implies that (Ccl) is verified.

6.2 Order relations between variables

6.2.1 Study of inequalities $Z_c(n) > Z_a(n), Z_a(n) > Y_a(n)$ and $Y_c(n) > Z_c(n)$

From properties 9 and 10, we deduce that $Z_c(n) - Z_a(n) = \left\lfloor \frac{n}{4} \right\rfloor - 2\,\pi\left(\frac{n}{2}\right) + \delta_{Z_c - Z_a}(n)$ with $\delta_{Z_c - Z_a}(n)$ equal to $1, 2$ or 3.

$Z_c(n) - Z_a(n)$ seems globally increasing with little variations. One observes that $Z_c(n) > Z_a(n)$ for $n \geqslant 240$. For greater values, strict inequality will be always verified because $\left\lfloor \frac{n}{4} \right\rfloor$ is increased much more often than $2\,\pi\left(\frac{n}{2}\right)$.

From properties 9 and 11, we deduce that $Z_a(n) - Y_a(n) = 2\,\pi\left(\frac{n}{2}\right) - \pi(n) + \delta_{Z_a - Y_a}(n)$ with $\delta_{Z_a - Y_a}(n)$ equal to $-3, -2, -1$ or 0.

$Z_a(n) - Y_a(n)$ seems globally increasing with little variations. One observes that $Z_a(n) > Y_a(n)$ for $n \geqslant 36$.

From properties 10 and 12, we deduce that $Y_c(n) - Z_c(n) = 2\,\pi\left(\frac{n}{2}\right) - \pi(n) + \delta_{Y_c - Z_c}(n)$ with $\delta_{Y_c - Z_c}(n)$ equal to $-2, -1, 0$ or 1.

$Y_c(n) - Z_c(n)$ is an increasing function of n. One observes that $Y_c(n) > Z_c(n)$ for $n \geqslant 24$.

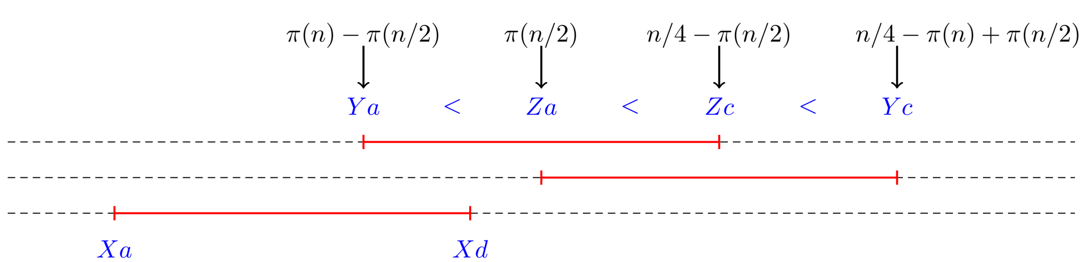
6.2.2 Strict order between 4 variables $Y_a(n), Y_c(n), Z_a(n)$ and $Z_c(n)$

Variables $Y_a(n), Z_a(n), Z_c(n)$ et $Y_c(n)$ are strictly ordered in the following way :

$$Y_a(n) < Z_a(n) < Z_c(n) < Y_c(n)$$

for all $n \geqslant 240$.

A picture showing variables'gaps is provided below, that illustrates their intrication :



From properties 9, 10, 11 and 12, we deduce :

- $Z_c(n) - Y_a(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \delta_{Z_c - Y_a}(n)$ with $\delta_{Z_c-Y_a}(n)$ equal to $-1, 0, 1$ or 2 ;
- $Y_c(n) - Z_a(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \delta_{Y_c - Z_a}(n)$ with $\delta_{Y_c-Z_a}(n)$ equal to $0, 1, 2$ or 3 ;
- $X_d(n) - X_a(n) = Z_c(n) - Y_a(n) + \delta_{2odd-compound}(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \delta_{X_d-X_a}(n)$ with $\delta_{X_d-X_a}(n)$ equal to $-1, 0, 1$ or 2.

One can also observe by program that :

- $X_c(n) - X_b(n) = 2\pi\left(\frac{n}{2}\right) - \pi(n) + \delta_{X_c-X_b}(n)$ with $\delta_{X_c-X_b}(n)$ equal to $-2, -1, 0$ or 1.

Also, one can deduce from equalities yet provided that :

- $X_a(n) + X_b(n) = \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{X_c-X_b}(n)$ with $\delta_{X_a+X_b}(n)$ very small.

The function $\left\lfloor \frac{n}{4} \right\rfloor - \pi(n)$ that appear in right members of three first equalities above is globally increasing with little variations. It's equal to 0 for $n = 122$.

Since $\left\lfloor \frac{n+2}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor + 1$ when n is an even's double (i.e. for one even number each two) while $\pi(n+2) = \pi(n) + 1$ when $n+1$ is prime (far less often than for one even number each two), for all n greater than a small value (i.e. $n > 122$), we will always have $\left\lfloor \frac{n}{4} \right\rfloor - \pi(n) > 0$.

6.3 Study of inequality $X_a(n) > 0$

To be sure that $X_a(n)$ would never be equal to 0, we should have to show that since a certain value of n, the inequality

$$X_d(n) > \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + 2$$

is always verified.

Indeed, this inequality, combined with the invariant $X_d(n) - X_a(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \delta_{X_d-X_a}(n)$, would have as consequence that $X_a(n)$ would be always strictly positive.

We observe that it seems that

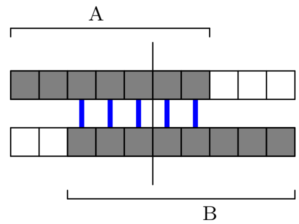
$$X_d(n) > \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + 2$$

for $n \geqslant 30$.

Intuitively, one understands what process is at work : the number of compound numbers becomes so big comparatively to the number of prime numbers that each compound number has "many more chances" to be the complementary to n of another compound number rather than a prime one. It is thus one can observe $X_d(n)$ becomes quickly greater than the sum $X_b(n) + X_c(n)$, in which each term is greater than $X_a(n)$.

6.4 Subsidiary exercize

Let us propose as an exercize that we must match (with a bijection) numbers of two sets ; in the first set containing k numbers, A are compound and $k - A$ are prime while in the second set, containing also k numbers, B numbers are compound while $k - B$ are prime. If $A \leqslant k/2$ and $B \leqslant k/2$, the matching can put in bijection two numbers that are not mandatory compound. But as soon as $A > k/2$ and $B > k/2$, some matching must necessarily put in bijection a compound number from the first set with a compound number of the second set. We can easily understand thanks to the drawing below that the number of matchings associating bijectively two compound numbers is necessarily greater than $A + B - k$.



6.5 $X_a(n)$ constrained to be strictly positive

Among odd numbers that are between 3 and $n/2$, very quickly, more than a half are compound. On the same manner, among odd numbers that are between $n/2$ and $n-3$, very quickly, more than a half are compound.

By this way, there are rather quickly both more than a half of numbers that can be an n's decomposition first range sommant that are compound and more than a half of numbers that can be an n's decomposition second range sommant that are compound too (i.e. $Y_c(n) > \left\lfloor \frac{n-2}{8} \right\rfloor$ and $Z_c(n) > \left\lfloor \frac{n-2}{8} \right\rfloor$) as soon as $n \geqslant 244$. Indeed, for $n \geqslant 244$, $\left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) > \left\lfloor \frac{n-2}{8} \right\rfloor$ and $\left\lfloor \frac{n}{4} \right\rfloor - \pi\left(\frac{n}{2}\right) > \left\lfloor \frac{n-2}{8} \right\rfloor$. $X_d(n)$ counting n's decompositions of the form *compound+compound* is then systematically greater than $Y_c(n) + Z_c(n) - \left\lfloor \frac{n-4}{4} \right\rfloor$ (cf subsidiary exercize of precedent section) and will remain greater than it definitively, which ensures that $X_a(n)$ will be always strictly positive, which proves binary Goldbach's conjecture.

Ci-dessous les idées qui m'ont amenée aux miennes (DV, 25/4/2014)

- la manière dont Gauss met les nombres tête-bêche : pour trouver la formule de la somme des n premiers entiers, ou bien pour voir comment "tombent en face" ou "pas en face" les résidus quadratiques d'un nombre premier suivant qu'il est de la forme $4k+1$ ou $4k+3$. La lecture intensive des sections 1, 2, 3 et 4 des Recherches arithmétiques ;

- la notion d'invariant informatique qui intervient dans le modèle de preuves de programmes de Hoare ;

- toutes les conférences d'Alain Connes, notamment son insistance sur la notion de permutations de lettres, qu'il présente dans ses conférences sur la théorie de l'ambiguité de Galois ;

- les notions de permutations qui interviennent dans le jeu du taquin, auquel j'ai souvent joué ;

- la recherche intensive d'anagrammes depuis mai 2013 ;

- le fait qu'Alain Connes ait dit en conférence que les algèbres non-commutatives si complexes qu'ils étudiaient pouvaient trouver leur illustration dans la très simple structure de monoïde, cumulé au fait que la concaténation des mots est non-commutative ; ces notions m'étaient familières pour avoir suivi plusieurs cours de théorie des langages lors de mes études universitaires ;

- le fait que la structure *chaîne de caractères* (string) soit une structure de données essentielle en informatique et que la concaténation des mots, ainsi que toute autre opération sur les chaînes (reconnaissance de sous-chaînes, comptage de lettres, etc) soit un concept sous-jacent à toute l'idée de programmation informatique ;

- le fait que la notion d'*échange* (*swap*) soit une action essentielle en informatique (elle est enseignée en tout début de formation, lorsque est présenté le piège de l'échange brutal de deux variables, sans en passer par une troisième pour échanger, et qui fait perdre un contenu) ; elle est réutilisée intensivement en algorithmique, dans les algorithmes de tris par exemple ;

- la notion de machine de Turing avec son ruban de booléens plutôt qu'un ruban de lettres, dont la tête de lecture lit les éléments et agit en fonction de leur valeur et de sa liste d'instructions qui est exactement ce qui intervient ici dans la notion de règles de réécriture sous-jacentes à la composition des mots, ces idées ayant été ravivées lors de la conférence récente de Bernard Chazelle et par la lecture de la biographie de Turing d'Andrew Hodges ;

- ma redécouverte du petit livre de Trathenbrot et ses invariants qui interviennent dans le problème des mots ;

- l'impossibilité de lire des articles de géométrie non-commutative ou de mathématiques en général qui m'a fait prendre la décision de revenir à mes fondamentaux à Noël 2013 : la programmation, les instructions, les variables, les booléens, les invariants de Hoare ;

- la rencontre d'Yves Meyer qui donnait une conférence à des lycéens au sujet de la preuve d'Helfgott de la conjecture ternaire de Goldbach ; cela m'a amenée à lire et visionner des articles sur la théorie des ondelettes utilisée dans la compression d'images ; mais par une curieuse coïncidence, peu de temps avant que je ne le rencontre, des articles sont sortis sur une nouvelle méthode révolutionnaire de compression d'images, qui utilise le fait que l'information est condensée dans certains pixels (i.e. on peut retrouver toute l'information en ne conservant que les pixels en question, et en déduisant de celle-ci toutes les autres). Cela m'a confortée dans l'idée, que j'avais déjà d'ailleurs à cause de la programmation de la fonction somme des diviseurs d'Euler, que des booléens codant seulement l'information premier-composé devaient pouvoir suffire à mener le raisonnement (sans en passer comme je l'avais toujours fait jusque-là, par les restes dans les différents corps premiers) ;

- la lecture d'articles sur les groupes de tresses avec là-encore, permutations de variables et invariants ;

- le fait d'avoir lu que les pavages de Penrose peuvent être étudiés en utilisant des chaînes de booléens telles que $x_n = 1 \implies x_{n+1} = 0$, ce qui est exactement ce qui se produit dans le cas de la divisibilité d'entiers successifs par un certain nombre ;

- le fait d'avoir, par formation initiale, une manière de penser calculatoire : Richard Karp, éminent informaticien américain, présente dans la dernière partie de sa conférence à la fondation Simons, ce qui distingue les mathématiciens des informaticiens : ils diffèrent dans leur manière d'aborder les problèmes ; selon Karp, un informaticien regarde les processus, les changements, la dynamique : il cherche ce qui change tandis qu'un mathématicien regarde les objets décrits par un ensemble fixe d'axiomes et peut prouver l'existence de solutions d'une manière non forcément constructive. La notion importante, selon lui, pour les informaticiens, est celle de calcul effectif et de processus dynamiques ; Karp ne parle pas de mathématiciens qui se préoccupent de la notion de temps ;

- la lecture de livres de vulgarisation de mécanique quantique : les équations de Bell, qui lient entre elles des variables ; et l'intrication de q-bits dans le cadre de la communication codée d'Alice et Bob ;

- l'écoute des conférences d'Alain Aspect et Serge Haroche, qui expliquent l'intrication des photons, dans le cadre de l'expérience des fentes de Young entre autres ;

- l'article de Rosser et Schoenfeld qui fournit des minorations et majorations pour $\pi(x)$ ou $\pi(2x)-\pi(x)$, mais sans lui, on sait que les nombres premiers vont se raréfiant tandis que les nombres composés sont de plus en plus nombreux par le Théorème des Nombres Premiers conjecturé par Gauss et prouvé par Hadamard et De La Vallée-Poussin ;

- le fait d'avoir reçu, de 1968 à 1975, une éducation élémentaire aux mathématiques par la méthode dite des "mathématiques modernes" : ensembles, bijections, tableaux à double entrée, numération et comptage dans différentes bases ;

- le fait d'avoir eu, toute petite, deux jeux extra : la maison aux clefs géométriques, et le puzzle de Notre-Dame de Paris.

```
#include <iostream>
#include <stdio.h>
#include <cmath>

int prime(int atester)
{
  unsigned long diviseur=2;
  bool pastrouve=true;
  unsigned long k = 2;
  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve)
    {
    if ((k * k) > atester) return 1;
    else
      if ((atester % k) == 0) {
      return 0 ;
      }
      else k++;
    }
}

int main (int argc, char* argv[])
{
  int n, x, xa, xb, xc, xd, xaprim, xbprim, xcprim, xdprim ;
  int pix, pi2x, compteprem, debuthaut, za, zc, ya, yc ;

  for (n=14 ; n <= 10000 ; n=n+2)
      {
      xa=0 ; xb=0 ; xc=0 ; xd=0 ; ya=0 ; yc=0; za=0 ; zc=0 ;
      for (x = 6 ; x <= (n+4)/2 ; x=x+2)
        {
          if (prime(x-3)) za++ ;
          else zc++ ;
        }
      if ((n/2) % 2 == 0) debuthaut = ((n+4)/2)+2 ;
      else debuthaut = ((n+4)/2)+1 ;
      for (x = debuthaut ; x <= n ; x=x+2)
        {
          if (prime(x-3)) ya++ ;
          else yc++ ;
        }
      for (x = 3 ; x <= n/2 ; x=x+2)
        {
          if (prime(x)) { if (prime(n-x)) xa++ ; else xc++ ;}
          else { if (prime(n-x)) xb++ ; else xd++ ; }
        }
      pix=0 ; pi2x = 0 ;
      for (compteprem=2 ; compteprem <= n ; compteprem++)
        {
          if (prime(compteprem)) {
            if (compteprem <= n/2) pix++ ;
            pi2x++ ;
          }
        }
      std::cout << "\n\n" << n << "  : \n" ;
      //std::cout << "(n-2)/8 " << (n-2)/8 ;
      std::cout << "n/4 " << n/4 << "  ";
      std::cout << " pi(n) " << pi2x << "  " ;
      std::cout << " pi(n/2) " << pix << "\n";
      printf("Xa %2d ",xa) ;
```

```
        printf("Xb %2d ",xb) ;
        printf("Xc %2d ",xc) ;
        printf("Xd %2d ",xd) ;
        std::cout << "\n" ;
        printf("Ya %2d ",ya) ;
        printf("Yc %2d ",yc) ;
        std::cout << "\n" ;
        printf("Za %2d ",za) ;
        printf("Zc %2d ",zc) ;
        //if (yc > (n-2)/8) std::cout << "Yc a dépassé la moitié du haut !\n" ;
        //else std::cout << "Yc plus petit que la moitié du haut !\n" ;
        //if (zc > (n-2)/8) std::cout << "Zc a dépassé la moitié du bas !\n" ;
        //else std::cout << "Zc plus petit que la moitié du bas !\n" ;
        //if ((yc>0) &&
        //    (zc>0) &&
        //    (xd > yc+zc-(n-4)/4) &&
        //    (yc > (n-2)/8) &&
        //    (zc > (n-2)/8))
        //  std::cout << "Xd est devenu assez grand pour tirer Xa !\n" ;
        //else
        //  std::cout << "Xd n'est pas encore assez grand pour tirer Xa !\n" ;
        }
}
```

Primalité et zéros de sommes de cosinus

Denise Vella-Chemla

10/7/14

L'article d'Euler *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs* est magique. On reste subjugué par la manière dont le mathématicien a trouvé la formule récurrente de la somme des diviseurs.

On peut trouver sur un forum de mathématiques à l'adresse $http://www.les-mathematiques.net/phorum/read.php?5,892412,892599$ une autre formule :

$$\sigma(n) = \sum_{k=1}^{n} \sum_{l=1}^{k} cos\left(\frac{2\pi nl}{k}\right)$$

Les cosinus se comportent ici comme des booléens qui comptent pour chaque diviseur sa valeur comme une somme de 1, de façon analogue à la fonction *Succ* de l'arithmétique de Peano.

Du coup, on en déduit une manière rigolote de trouver les nombres premiers : ce sont les zéros de la fonction *sumsumcos* ci-dessous :

$$sumsumcos(n) = \sum_{k=2}^{n-1} \sum_{l=1}^{k} cos\left(\frac{2\pi nl}{k}\right)$$

For me, that's F_{un} !

La conjecture de Goldbach stipule que tout nombre pair sauf 2 est la somme de deux nombres premiers. Dans la suite, on s'intéresse aux décompositions d'un nombre pair n en somme de deux nombres impairs $p+q$ avec $3 \leqslant p \leqslant n/2$ et $n/2 \leqslant q \leqslant n-3$.

On note :

- $X_a(n)$ le nombre de décompositions de n de la forme *premier* + *premier* ;
- $X_b(n)$ le nombre de décompositions de n de la forme *composé* + *premier* ;
- $X_c(n)$ le nombre de décompositions de n de la forme *premier* + *composé* ;
- $X_d(n)$ le nombre de décompositions de n de la forme *composé* + *composé*.

Exemples :

- $n = 32$:
  $X_a(32) = \#\{3+29, 13+19\} = 2$.
  $X_b(32) = \#\{9+23, 15+17\} = 2$.
  $X_c(32) = \#\{5+27, 7+25, 11+21\} = 3$.
  $X_d(32) = \#\varnothing = 0$.
- $n = 34$:
  $X_a(34) = \#\{3+31, 5+29, 11+23, 17+17\} = 4$.
  $X_b(34) = \#\{15+19\} = 1$.
  $X_c(34) = \#\{7+27, 13+21\} = 2$
  $X_d(34) = \#\{9+25\} = 1$.

D'autre part, on note $T_a(n)$ le nombre de décompositions de la forme 3+*premier* avec $3 \leqslant p \leqslant 2\left\lfloor \frac{n}{4} \right\rfloor - 1$.

Exemples : $T_a(32) = T_a(34) = \#\{3+3, 3+5, 3+7, 3+11, 3+13\} = 5$.

On note $T_c(n)$ le nombre de décompositions de la forme 3 + *composé* avec $3 \leqslant c \leqslant 2\left\lfloor \frac{n}{4} \right\rfloor - 1$.

Exemples : $T_c(32) = T_c(34) = \#\{3+9, 3+15\} = 2$.

On note $Y_a(n)$ le nombre de décompositions de la forme 3 + *premier* avec $2\left\lfloor \frac{n}{4} \right\rfloor - 1 < p \leqslant n-3$.

Exemples :

- $Y_a(32) = \#\{3+17, 3+19, 3+23, 3+29\} = 4$;
- $Y_a(34) = \#\{3+17, 3+19, 3+23, 3+29, 3+31\} = 5$.

On note Y_c le nombre de décompositions de la forme 3 + *composé* avec $2\left\lfloor \frac{n}{4} \right\rfloor - 1 < c \leqslant n-3$.

Exemples : $Y_c(32) = Y_c(34) = \#\{3+21, 3+25, 3+27\} = 3$.

Pour tout entier pair n, les contraintes suivantes sont vérifiées :

$$(1) Y_a = X_a + X_b$$
$$(2) Y_c = X_c + X_d$$
$$(3) T_a + T_c + Y_a + Y_c + \epsilon = 2(X_a + X_b + X_c + X_d)$$

ϵ vaut 1 si n est un double d'impair et 0 sinon.

L'égalité $(1) Y_a = X_a + X_b$ découle du fait que l'on a une bijection sur le second sommant des décompositions comptées par Y_a d'une part et comptées par X_a et X_b d'autre part.

Identiquement, $(2) Y_c = X_c + X_d$ découle du fait que l'on a une bijection sur le second sommant des décompositions comptées par Y_c d'une part et comptées par X_c et X_d d'autre part.

$(3) T_a + T_c + Y_a + Y_c + \epsilon = 2(X_a + X_b + X_c + X_d)$ correspond à la manipulation suivante : on prend les décompositions de n et on obtient à partir d'elle deux décompositions pour chacune, en remplaçant soit le premier, soit le second sommant par 3.

Prenons comme hypothèse qu'un nombre n n'admet aucune décomposition de Goldbach. Puisque $X_a(n)$ compte les décompositions de n sous la forme d'une somme de deux nombres premiers, poser cette hypothèse s'écrit $X_a(n) = 0$.

On a alors $T_a + T_c + \epsilon = X_b + Y_c$.

On a $T_a + T_c = \left\lfloor \dfrac{n-4}{4} \right\rfloor$.

On a $X_b < Y_a$: il y a forcément moins de décompositions de n de la forme $compos\acute{e} + premier$ (comptés par X_b) que de nombres premiers compris entre $n/2$ et $n-3$ (comptés par Y_a) (on utilise ici une sorte de "principe des tiroirs inversé" : si l'on met 0 ou 1 objet dans k tiroirs, on ne peut avoir plus d'objets que de tiroirs, i.e. plus de k objets).

On a, pour $k > 25$, moins de premiers que de composés impairs dans l'intervalle $[2k+3, 4k+1]$. Ceci s'écrit avec nos variables $\forall k > 25, Y_a(k) < Y_c(k)$. Pour notre nombre n très grand, censé ne pas vérifier la conjecture de Goldbach, on déduit $Y_a < Y_c$ et $X_b + Y_c < Y_a + Y_c < 2Y_c$.

Or $\left\lfloor \dfrac{n-4}{4} \right\rfloor$ est pour tout entier supérieur à un certain entier assez petit (tel que 100) supérieur à $2Y_c$. Cela assure qu'on a jamais l'égalité $T_a + T_c + \epsilon = X_b + Y_c$ qui découlerait de l'absence de décompositions de Goldbach d'un certain nombre pair.

Il est donc impossible qu'un nombre pair contredise la conjecture de Goldbach. On a utilisé pour le démontrer un simple *"langage à 4 lettres"*.

Résumé

$$Y_a(n) = X_a(n) + X_b(n) \tag{1}$$

$$Y_c(n) = X_c(n) + X_d(n) \tag{2}$$

$$X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3}$$

$$Y_a(n){+}Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \tag{3'}$$

$$Z_a(n) + Z_c(n) = \left\lfloor \frac{n-4}{4} \right\rfloor \tag{4}$$

$$X_a(n) + X_c(n) = Z_a(n) + \delta_{2p}(n) \tag{5}$$

avec $\delta_{2p}(n)$ qui vaut 1 dans le cas où n est le double d'un nombre premier et qui vaut 0 sinon.

$$X_b(n) + X_d(n) = Z_c(n) + \delta_{2c-imp}(n) \tag{6}$$

avec $\delta_{2c-imp}(n)$ qui vaut 1 dans le cas où n est un double d'impair composé, et qui vaut 0 sinon.

$$Z_c(n) - Y_a(n) = X_d(n) - X_a(n) - \delta_{2c-imp}(n) \tag{7}$$

$$Z_c(n) - Y_a(n) = Y_c(n) - Z_a(n) - \delta_{4k+2}(n) \tag{8}$$

avec $\delta_{4k+2}(n)$ qui vaut 1 si n est un double d'impair et 0 sinon.

$$Z_a(n) = \pi\left(\frac{n}{2}\right) + \delta_{Z_a}(n) \tag{9}$$

avec $\delta_{Z_a}(n)$ égal à -2 si n est le double d'un nombre premier et égal à -1 sinon ;

$$Z_c(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi\left(\frac{n}{2}\right) + \delta_{Z_c}(n) \tag{10}$$

avec $\delta_{Z_c}(n)$ égal à 1 si n est le double d'un nombre premier et égal à 0 sinon ;

$$Y_a(n) = \pi(n) - \pi\left(\frac{n}{2}\right) + \delta_{Y_a}(n) \tag{11}$$

avec $\delta_{Y_a}(n)$ égal à $-1, 0$ ou 1 ($\delta_{Y_a}(n)$ est égal à 0 quand $n-1$ et $n/2$ sont tous les deux premiers ou bien tous les deux composés, $\delta_{Y_a}(n)$ est égal à -1 quand $n-1$ est premier tandis que $n/2$ est composé, et enfin, $\delta_{Y_a}(n)$ est égal à 1 quand $n-1$ est composé tandis que $n/2$ est premier) ;

$$Y_c(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \pi\left(\frac{n}{2}\right) + \delta_{Y_c}(n) \tag{12}$$

avec $\delta_{Y_c}(n)$ égal à $-1, 0$ ou 1.

Des propriétés 9 et 10, on déduit que $Z_c(n) - Z_a(n) = \left\lfloor \frac{n}{4} \right\rfloor - 2\,\pi\left(\frac{n}{2}\right) + \delta_{Z_c - Z_a}(n)$ avec $\delta_{Z_c - Z_a}(n)$ égal à $1, 2$ ou 3.
$Z_c(n) - Z_a(n)$ semble globalement croissante avec de petites oscillations. On constate que $Z_c(n) > Z_a(n)$ pour $n \geqslant 240$. A partir de ce nombre, l'inégalité stricte sera toujours vérifiée car $\left\lfloor \frac{n}{4} \right\rfloor$ augmente plus

souvent que $2\,\pi\left(\frac{n}{2}\right)$.

Des propriétés 9 et 11, on déduit que $Z_a(n) - Y_a(n) = 2\,\pi\left(\frac{n}{2}\right) - \pi(n) + \delta_{Z_a - Y_a}(n)$ avec $\delta_{Z_a - Y_a}(n)$ égal à $-3, -2, -1$ ou 0.
$Z_a(n) - Y_a(n)$ semble globalement croissante avec de petites oscillations. On constate que $Z_a(n) > Y_a(n)$ pour $n \geqslant 36$.

Des propriétés 10 et 12, on déduit que $Y_c(n) - Z_c(n) = 2\,\pi\left(\frac{n}{2}\right) - \pi(n) + \delta_{Y_c - Z_c}(n)$ avec $\delta_{Y_c - Z_c}(n)$ égal à $-2, -1, 0$ ou 1.
$Y_c(n) - Z_c(n)$ est une fonction croissante de n. On constate que $Y_c(n) > Z_c(n)$ pour $n \geqslant 24$.

Des propriétés 9, 10, 11 et 12, on déduit :

- $Z_c(n) - Y_a(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \delta_{Z_c - Y_a}(n)$ avec $\delta_{Z_c - Y_a}(n)$ égal à $-1, 0, 1$ ou 2 ;
- $Y_c(n) - Z_a(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \delta_{Y_c - Z_a}(n)$ avec $\delta_{Y_c - Z_a}(n)$ égal à $0, 1, 2$ ou 3 ;
- $X_d(n) - X_a(n) = Z_c(n) - Y_a(n) + \delta_{2c-imp}(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \delta_{X_d - X_a}(n)$ avec $\delta_{X_d - X_a}(n)$ égal à $-1, 0, 1$ ou 2.

La fonction $\left\lfloor \frac{n}{4} \right\rfloor - \pi(n)$ qui apparaît dans tous les membres droits des égalités ci-dessus est globalement croissante avec de petites oscillations. Elle s'annule pour $n = 122$.

Dans la mesure où $\left\lfloor \frac{n+2}{4} \right\rfloor = \left\lfloor \frac{n}{4} \right\rfloor + 1$ quand n est un double de pair (i.e. pour un nombre pair sur deux) tandis que $\pi(n+2) = \pi(n) + 1$ quand $n+1$ est premier (beaucoup moins souvent que pour un nombre pair sur deux), pour tout n supérieur à une valeur petite (i.e. $n > 122$), on aura systématiquement $\left\lfloor \frac{n}{4} \right\rfloor - \pi(n) > 0$.

Etude de l'inégalité $X_a(n) > 0$

Pour être assuré que $X_a(n)$ soit toujours non nul, il faudrait montrer qu'à partir d'une certaine valeur de n, l'inégalité

$$X_d(n) > \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + 2$$

est toujours vérifiée.

En effet, cette inégalité, combinée avec l'invariant $X_d(n) - X_a(n) = \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + \delta_{X_d - X_a}(n)$, aurait pour conséquenc qu'$X_a(n)$ serait toujours strictement positif.

On constate que

$$X_d(n) > \left\lfloor \frac{n}{4} \right\rfloor - \pi(n) + 2$$

à partir de $n \geqslant 30$. L'ensemble des propriétés invariantes découvertes précédemment doit avoir ce nouvel invariant comme conséquence. Mais pour pouvoir mettre en oeuvre une telle déduction, peut-être faudrait-il trouver de façon similaire des invariants sur l'évolution des variables $X_a(n), X_b(n), X_c(n)$ et $X_d(n)$.

Programme de la somme des diviseurs utilisant les sommes de cosinus

Denise Vella-Chemla

19/6/14

L'article d'Euler *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs* est magique. On reste subjugué par la manière dont le mathématicien a trouvé la formule récurrente de la somme des diviseurs. On peut trouver sur un forum de mathématiques à l'adresse $http : //www.les-mathematiques.net/phorum/read.php?5, 892412, 892599$ une autre formule :

$$\sigma(n) = \sum_{k=1}^{n} \sum_{l=1}^{k} cos\left(\frac{2\pi nl}{k}\right)$$

```
#include <iostream>
#include <math.h>
# define M_PI        3.14159265358979323846

int main (int argc, char* argv[]) {
  int n, k, x ;
  float res ;

  for (n = 1 ; n <= 100 ; n++) {
      std::cout << n << " a pour somme des diviseurs " ;
      res = 0.0 ;
      for (k = 1 ; k <= n ; k++)
         for (l = 1 ; l <= k ; l++)
           res = res+cos((2.0*(float)n*M_PI*(float)l)/(float)k) ;
      std::cout << res << "\n" ;
  }
}
```

On peut voir les nombres premiers comme des minima locaux de la fonction somme des diviseurs.

Puisque la somme des diviseurs d'un nombre premier p vaut $p+1$, les nombres premiers annulent $\sigma(p) - p - 1$. On ne sait pas évaluer si la formule ci-dessus présente une utilité pour connaître davantage l'ensemble des nombres premiers mais sa découverte rend contente.

On fournit ici une représentation de ce que l'on pourrait appeler l"'espace de Goldbach" qui représente les décompositions des nombres en sommes de deux entiers selon la convention choisie ($premier+premier = a$, $composé + premier = b$, $premier + composé = c$ et $composé + composé = d$).

a	d	d	d	b	d	a	d	c	d	b	d	b	d	c	d	b	d	a	d	a	b	d	b
d	c	d	b	d	b	d	c	d	a	d	b	d	d	d	a	d	b	d	a	b	c	b	d
d	d	a	d	b	d	d	d	a	d	a	d	d	d	b	d	a	d	b	b	c	b	c	b
d	b	d	a	d	d	d	b	d	a	d	c	d	b	d	b	d	a	b	d	b	c	b	a
a	d	b	d	c	d	b	d	b	d	c	d	a	d	b	d	b	b	c	b	d	b	a	d
d	a	d	d	d	a	d	b	d	d	d	a	d	a	d	b	b	d	b	c	b	b	d	a
a	d	c	d	b	d	a	d	d	d	b	d	a	d	a	b	d	b	d	b	a	d	b	d
d	c	d	a	d	b	d	c	d	b	d	b	d	a	b	c	b	d	b	b	d	a	d	b
d	d	a	d	a	d	d	d	a	d	b	d	b	b	c	b	c	b	b	d	b	d	a	d
d	b	d	a	d	c	d	b	d	a	d	b	b	d	b	c	b	a	d	b	d	b	d	c
a	d	b	d	c	d	a	d	b	d	a	b	d	b	d	b	a	d	a	d	b	d	d	d
d	a	d	d	d	a	d	a	d	b	b	c	b	d	b	b	d	a	d	a	d	d	d	b
a	d	c	d	b	d	a	d	a	b	d	b	c	b	b	d	b	d	a	d	c	d	b	d
d	c	d	a	d	b	d	a	b	c	b	d	b	a	d	b	d	b	d	c	d	a	d	b
d	d	a	d	a	d	b	b	c	b	c	b	b	d	a	d	b	d	d	d	a	d	a	d
d	b	d	a	d	a	b	d	b	c	b	a	d	b	d	a	d	d	d	b	d	a	d	c
a	d	b	d	a	b	c	b	d	b	a	d	a	d	b	d	c	d	b	d	b	d	c	d
d	a	d	b	b	c	b	c	b	b	d	a	d	a	d	d	d	a	d	b	d	d	d	a
a	d	a	b	d	b	c	b	a	d	b	d	a	d	c	d	b	d	a	d	d	d	b	d
d	a	b	c	b	d	b	a	d	a	d	b	d	c	d	a	d	b	d	c	d	b	d	b
a	b	c	b	c	b	b	d	a	d	a	d	d	d	a	d	a	d	d	d	a	d	b	d
a	c	b	c	b	a	d	b	d	a	d	c	d	b	d	a	d	c	d	b	d	a	d	d
d	a	c	b	a	d	a	d	b	d	c	d	a	d	b	d	c	d	a	d	b	d	c	d
a	d	a	a	d	a	d	a	d	d	d	a	d	a	d	d	d	a	d	a	d	d	d	a

Les a colorées en rouge correspondent aux décompositions de Goldbach $19 + 19$ et $7 + 31$ de 38.

Si on remplace les lettres par des flèches selon la convention ($0 + 0 = \bullet$, $1 + 1 = \rightarrow$, $0 + 1 = \nearrow$, $1 + 0 = \searrow$), on obtient :

•	→	→	→	↘	→	•	→	↗	→	↘	→	↘	→	↗	→	↘	→	•	→	•	↘	→	↘
→	↗	→	↘	→	↘	→	↗	→	•	→	↘	→	→	→	•	→	↘	→	•	↘	↗	↘	→
→	→	•	→	↘	→	→	→	•	→	•	→	→	→	↘	→	•	→	↘	↘	↗	↘	↗	↘
→	↘	→	•	→	→	→	↘	→	•	→	↗	→	↘	→	↘	→	•	↘	→	↘	↗	↘	•
•	→	↘	→	↗	→	↘	→	↘	→	↗	→	•	→	↘	→	↘	↘	↗	↘	→	↘	•	→
→	•	→	→	→	•	→	↘	→	→	→	•	→	•	→	↘	↘	→	↘	↗	↘	↘	→	•
•	→	↗	→	↘	→	•	→	→	→	↘	→	•	→	•	↘	→	↘	→	↘	•	→	↘	→
→	↗	→	•	→	↘	→	↗	→	↘	→	↘	→	•	↘	↗	↘	→	↘	↘	→	•	→	↘
→	→	•	→	•	→	→	→	•	→	↘	→	↘	↘	↗	↘	↗	↘	↘	→	↘	→	•	→
→	↘	→	•	→	↗	→	↘	→	•	→	↘	↘	→	↘	↗	↘	•	→	↘	→	↘	→	↗
•	→	↘	→	↗	→	•	→	↘	→	•	↘	→	↘	→	↘	•	→	•	→	↘	→	→	→
→	•	→	→	→	•	→	•	→	↘	↘	↗	↘	→	↘	↘	→	•	→	•	→	→	→	↘
•	→	↗	→	↘	→	•	→	•	↘	→	↘	↗	↘	↘	→	↘	→	•	→	↗	→	↘	→
→	↗	→	•	→	↘	→	•	↘	↗	↘	→	↘	•	→	↘	→	↘	→	↗	→	•	→	↘
→	→	•	→	•	→	↘	↘	↗	↘	↗	↘	↘	→	•	→	↘	→	→	→	•	→	•	→
→	↘	→	•	→	•	↘	→	↘	↗	↘	•	→	↘	→	•	→	→	→	↘	→	•	→	↗
•	→	↘	→	•	↘	↗	↘	→	↘	•	→	•	→	↘	→	↗	→	↘	→	↘	→	↗	→
→	•	→	↘	↘	↗	↘	↗	↘	↘	→	•	→	•	→	→	→	•	→	↘	→	→	→	•
•	→	•	↘	→	↘	↗	↘	•	→	↘	→	•	→	↗	→	↘	→	•	→	→	→	↘	→
→	•	↘	↗	↘	→	↘	•	→	•	→	↘	→	↗	→	•	→	↘	→	↗	→	↘	→	↘
•	↘	↗	↘	↗	↘	↘	→	•	→	•	→	→	→	•	→	•	→	→	→	•	→	↘	→
•	↗	↘	↗	↘	•	→	↘	→	•	→	↗	→	↘	→	•	→	↗	→	↘	→	•	→	→
→	•	↗	↘	•	→	•	→	↘	→	↗	→	•	→	↘	→	↗	→	•	→	↘	→	↗	→
•	→	•	•	→	•	→	•	→	→	→	•	→	•	→	→	→	•	→	•	→	→	→	•

Conjecture de Goldbach (7 juin 1742)

- 271 ans
- **Énoncé** : Tout nombre pair (n) supérieur à 2 est la somme de deux nombres premiers.
- $\iff$ Tout entier supérieur à 1 est la moyenne de deux nombres premiers ($\frac{1}{2}p_1 + \frac{1}{2}p_2$).
- $$\begin{aligned} 98 &= 19 + 79 \\ &= 31 + 67 \\ &= 37 + 61 \end{aligned}$$

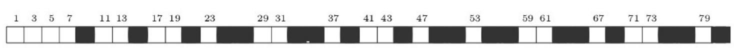
Les tirettes de Laisant

- **Charles-Ange Laisant** : Sur un procédé expérimental de vérification de la conjecture de Goldbach, Bulletin de la SMF, 25, 1897.

- *"Ce fameux théorème empirique : Tout nombre pair est la somme de deux nombres premiers, dont la démonstration semble dépasser les possibilités scientifiques actuelles, a fait l'objet de nombreux travaux et de certaines contestations. Lionnet a tenté d'établir que la proposition devait probablement être inexacte. M. Georg Cantor l'a vérifiée numériquement jusqu'à 1000, en donnant pour chaque nombre pair toutes les décompositions en deux nombres premiers, et il a remarqué que le nombre de ces décompositions ne cesse de croître en moyenne, tout en présentant de grandes irrégularités."*

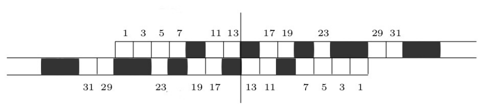
Les tirettes de Laisant

- *"Voici un procédé qui permettrait de faire sans calculs la vérification expérimentale dont il s'agit, et d'avoir pour chaque nombre pair, à la seule inspection d'une figure, toutes les décompositions. Supposons que sur une bande formée de carrés accolés, représentant les nombres impairs successifs, on ait construit le crible d'Erathostène, en ombrant les nombres composés, jusqu'à une limite quelconque* 2*n.*"



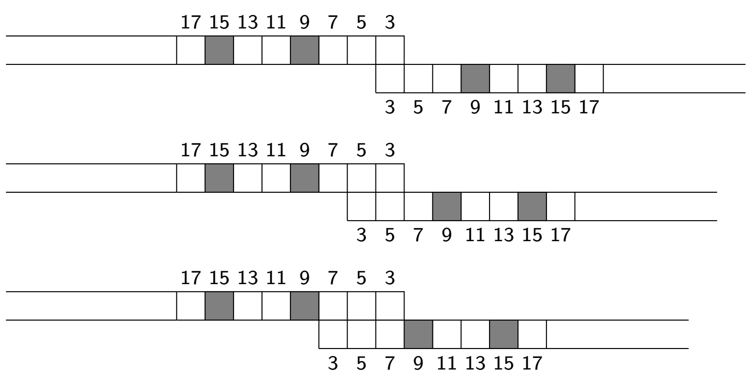
Les tirettes de Laisant

- *"Si l'on a construit deux réglettes pareilles, et si l'on place la seconde au-dessous de la première en la retournant et en faisant correspondre la case* 1 *à* $2n$*, il est évident que si le théorème de Goldbach est vrai pour* $2n$*, il y aura quelque part deux cases blanches en correspondance ; et tous les couples de cases blanches donneront les diverses décompositions. On les aura même en lisant la moitié de la figure, à cause de la symétrie par rapport au milieu. Ainsi la vérification relative au nombre* 28 *donnera la figure 2 et montrera qu'on a les décompositions* $28 = 5 + 23 = 11 + 17$*."*



Les tirettes de Laisant

- *"On comprend que les réglettes étant construites à l'avance, et un simple glissement permettant de passer d'un nombre à un autre, les vérifications sont très rapides."*



Booléens

- On représente la primalité par des booléens.
- 0 signifie *est premier*, 1 signifie *est composé*.
- $23 \rightarrow 0$
- $25 \rightarrow 1$
-

3	5	7	9	11	13	15	17	19	21	23	25	27	29	...
0	0	0	1	0	0	1	0	0	1	0	1	1	0	...

Copie de l'espace : matrices à 2 booléens

- On représente les décompositions de n en sommes de deux nombres impairs par des matrices à 2 booléens (le booléen du nombre le plus petit en bas).
- $28 = \underset{p}{5} + \underset{p}{23} \rightarrow \begin{pmatrix} 0 \\ 0 \end{pmatrix} = a$
- $28 = \underset{c}{9} + \underset{p}{19} \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} = b$
- $28 = \underset{p}{3} + \underset{c}{25} \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} = c$
- $40 = \underset{c}{15} + \underset{c}{25} \rightarrow \begin{pmatrix} 1 \\ 1 \end{pmatrix} = d$

Mots de 40, 42 et 44

	37	35	33	31	29	27	25	23	21
40	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0
	3	5	7	9	11	13	15	17	19
	a	*c*	*c*	*b*	*a*	*c*	*d*	*a*	*c*

	39	37	35	33	31	29	27	25	23	21
42	1	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21
	c	*a*	*c*	*d*	*a*	*a*	*d*	*c*	*a*	*d*

	41	39	37	35	33	31	29	27	25	23
44	0	1	0	1	1	0	0	1	1	0
	0	0	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21
	a	*c*	*a*	*d*	*c*	*a*	*b*	*c*	*c*	*b*

Opérations sur les matrices

- Règle générale :

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ y_2 \end{pmatrix}$$

- Exemple :

$$\underbrace{\begin{pmatrix} 1 \\ 0 \end{pmatrix}}_{c} \cdot \underbrace{\begin{pmatrix} 0 \\ 1 \end{pmatrix}}_{b} = \underbrace{\begin{pmatrix} 1 \\ 1 \end{pmatrix}}_{d}$$

- Règles particulières :

$aa \to a$	$ba \to a$	$ca \to c$	$da \to c$
$ab \to b$	$bb \to b$	$cb \to d$	$db \to d$
$ac \to a$	$bc \to a$	$cc \to c$	$dc \to c$
$ad \to b$	$bd \to b$	$cd \to d$	$dd \to d$

Observer les mots : 16 règles de réécriture

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

Rappels de théorie des langages

- Un alphabet est un ensemble fini de symboles.
- Les alphabets utilisés ci-après sont :
$A = \{a, b, c, d\}, A_{ab} = \{a, b\}, A_{cd} = \{c, d\}, A_{ac} = \{a, c\}$ et $A_{bd} = \{b, d\}$.
- Un mot sur l'alphabet X est une séquence finie et ordonnée, éventuellement vide, d'éléments de l'alphabet. C'est une concaténation de lettres. On note X^* l'ensemble des mots sur l'alphabet X.
- Un mot est préfixe d'un autre s'il contient, sur toute sa longueur, les mêmes lettres aux mêmes positions (Soient un alphabet X et $w, u \in X^*$. u est préfixe de w si et seulement si $\exists v \in X^*$ tel que $w = u.v$).

Observer les mots diagonaux

6 : a
8 : a
10 : $a \quad a$
12 : $c \quad a$
14 : $a \quad c \quad a$
16 : $a \quad a \quad c$
18 : $c \quad a \quad a \quad d$
20 : $a \quad c \quad a \quad b$
22 : $a \quad a \quad c \quad b \quad a$
24 : $c \quad a \quad a \quad d \quad a$
26 : $a \quad c \quad a \quad b \quad c \quad a$
28 : $c \quad a \quad c \quad b \quad a \quad c$
30 : $c \quad c \quad a \quad d \quad a \quad a \quad d$
32 : $a \quad c \quad c \quad b \quad c \quad a \quad b$
34 : $a \quad a \quad c \quad d \quad a \quad c \quad b \quad a$

Propriétés des mots diagonaux

- Les mots diagonaux (diagonales) ont leurs lettres soit dans l'alphabet A_{ab} soit dans l'alphabet A_{cd}.
- Toute diagonale est préfixe de la diagonale suivante définie sur le même alphabet.
- Une diagonale code en effet des décompositions de même second sommant et de premier sommant un nombre impair de la liste des impairs successifs à partir de 3.
- Par exemple, la diagonale *aaaba*, qui commence au *a* première lettre du mot de 26 sur la figure 1 code les décompositions $3 + 23, 5 + 23, 7 + 23; 9 + 23, 11 + 23$ et $13 + 23$.

Propriétés des mots diagonaux

- Ainsi, les diagonales sur l'alphabet A_{ab} "codent" les décompositions dont le second sommant est premier ; les lettres de telles diagonales codent soit par des a correspondant aux nombres premiers, soit par des b correspondant aux nombres composés la séquence des caractères de primalité des entiers impairs, à partir de 3.

- Les diagonales sur l'alphabet A_{cd} "codent" quant à elles des décompositions dont le second sommant est composé ; les lettres de telles diagonales codent soit par des c correspondant aux nombres premiers, soit par des d correspondant aux nombres composés la séquence des caractères de primalité des entiers impairs, à partir de 3.

Observer les mots verticaux

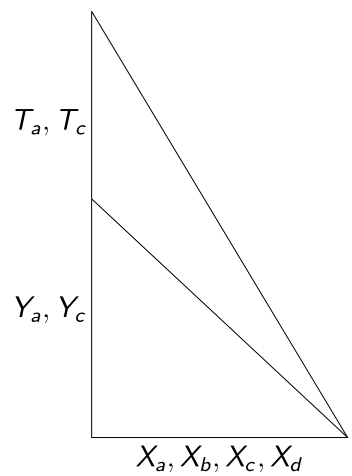
6 :	a							
8 :	a							
10 :	a	a						
12 :	c	a						
14 :	a	c	a					
16 :	a	a	c					
18 :	c	a	a	d				
20 :	a	c	a	b				
22 :	a	a	c	b	a			
24 :	c	a	a	d	a			
26 :	a	c	a	b	c	a		
28 :	c	a	c	b	a	c		
30 :	c	c	a	d	a	a	d	
32 :	a	c	c	b	c	a	b	
34 :	a	a	c	d	a	c	b	a

(et les "tranches" verticales)

Propriétés des mots verticaux

- Les mots verticaux ont leurs lettres soit dans l'alphabet A_{ac} soit dans l'alphabet A_{bd}.
- Un mot vertical code des décompositions successives en somme de deux impairs de même premier sommant.
- Tout mot vertical est contenu dans un mot vertical qui se trouve à sa gauche et qui est défini sur le même alphabet.

n ne vérifie pas la conjecture de Goldbach.



- Les variables sont liées.

n ne vérifie pas la conjecture de Goldbach.

	6 :	a							
	8 :	a							
	10 :	a	a						
$T_a = 5$	12 :	c	a						
$T_c = 2$	14 :	a	c	a					
	16 :	a	a	c					
	18 :	c	a	a	d				
	20 :	a	c	a	b				
	22 :	a	a	c	b	a			
$Y_a = 4$	24 :	c	a	a	d	a			
$Y_c = 3$	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	$\leftarrow X_a = 2, X_b = 2, X_c = 3, X_d = 0$

n ne vérifie pas la conjecture de Goldbach.

	6 :	a							
	8 :	a							
	10 :	a	a						
$T_a = 5$	12 :	c	a						
$T_c = 2$	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		
$Y_a = 5$	28 :	c	a	c	b	a	c		
$Y_c = 3$	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

$\leftarrow X_a = 4, X_b = 1, X_c = 2, X_d = 1$

Bijections à la Cantor

- T_a compte les décompositions de la forme $n' = 3 + p_i$, p_i premier, $n' \leqslant 2\left\lceil \dfrac{n+2}{4} \right\rceil$.
- Par exemple, pour $n = 34$, $T_a = \#\{3+3, 3+5, 3+7, 3+11, 3+13\}$.
- T_c, quant à elle, compte les décompositions de la forme $n' = 3 + c_i$, c_i composé $n' \leqslant 2\left\lceil \dfrac{n+2}{4} \right\rceil$.
- Par exemple, pour $n = 34$, $T_c = \#\{3+9, 3+15\}$.

Bijections à la Cantor

- Cette bijection triviale sur le deuxième sommant permet d'expliquer aisément pourquoi $Y_a = X_a + X_b$ ou bien pourquoi $Y_c = X_c + X_d$. La simple présentation des ensembles en extension suffit à s'en convaincre.

- $$Y_a = \#\{3+17, 3+19, 3+23, 3+29, 3+31\}$$
  $$X_a = \#\{3+31, 5+29, 11+23, 17+17\}$$
  $$X_b = \#\{15+19\}$$

  $$Y_c = \#\{3+21, 3+25, 3+27\}$$
  $$X_c = \#\{7+27, 13+21\}$$
  $$X_d = \#\{9+25\}$$

Bijections à la Cantor

- La bijection f qui permet de passer de la ligne 2 du tableau la ligne 1 est telle que $f(a) = f(c) = a$ et $f(b) = f(d) = c$.

- La bijection g qui permet de passer de la ligne 2 du tableau la ligne 3 est telle que $g(a) = g(b) = a$ et $g(c) = g(d) = c$.

- C'est la duplication de la dcomposition $3 + n/2$ dans le cas des doubles d'impairs qui ncessite l'introduction de la variable ϵ qui vaut alors 1 et 0 sinon.

Bijections à la Cantor

	3	3	3	3	3	3	3
1	*a*	*a*	*a*	*c*	*a*	*a*	*c*
	3	5	7	9	11	13	15
	3	5	7	9	11	13	15
2	*a*	*c*	*c*	*b*	*c*	*a*	*b*
	29	27	25	23	21	19	17
	29	27	25	23	21	19	17
3	*a*	*c*	*c*	*a*	*c*	*a*	*a*
	3	3	3	3	3	3	3

	3	3	3	3	3	3	3	3
1	*a*	*a*	*a*	*c*	*a*	*a*	*c*	*a*
	3	5	7	9	11	13	15	17
	3	5	7	9	11	13	15	17
2	*a*	*a*	*c*	*d*	*a*	*c*	*b*	*a*
	31	29	27	25	23	21	19	17
	31	29	27	25	23	21	19	17
3	*a*	*a*	*c*	*c*	*a*	*c*	*a*	*a*
	3	3	3	3	3	3	3	3

n ne vérifie pas la conjecture de Goldbach.

- Les contraintes suivantes sont toujours vérifiées :

$$\begin{array}{l} Y_a = X_a + X_b \\ Y_c = X_c + X_d \\ T_a + T_c + Y_a + Y_c + \epsilon = 2(X_a + X_b + X_c + X_d) \end{array}$$

- $\epsilon = 1$ si n est un double d'impair, $\epsilon = 0$ sinon.
- m_n ne contenant aucune lettre a, on a $X_a = 0$.
- Mais puisque $Y_a = X_a + X_b$, on a alors $Y_a = X_b$.

n ne vérifie pas la conjecture de Goldbach.

- En identifiant Y_a à X_b et Y_c à $X_c + X_d$ dans la dernière contrainte toujours respectée, on obtient la suite d'égalités suivante :

$$\begin{aligned} T_a + T_c + Y_a + Y_c + \epsilon &= 2(X_a + X_b + X_c + X_d) \\ T_a + T_c + X_b + X_c + X_d + \epsilon &= 2X_a + 2X_b + 2X_c + 2X_d \\ T_a + T_c + \epsilon &= X_b + X_c + X_d \\ T_a + T_c + \epsilon &= X_b + Y_c \end{aligned}$$

- Rappel du sens des variables :
  - $T_a + T_c = \left\lfloor \dfrac{n-4}{4} \right\rfloor$;
  - X_b compte le nombre de décompositions de n sous la forme d'une somme de deux nombres impairs $p + q$ avec $p \leqslant n/2$ composé et q premier ;
  - Y_c compte le nombre de nombres composés impairs compris entre $n/2$ et $n - 3$.

n ne vérifie pas la conjecture de Goldbach.

- Le nombre X_b de décompositions de n sous la forme d'une somme de deux nombres impairs $p + q$ avec $p \leqslant n/2$ composé et q premier étant forcément inférieur au nombre de nombres premiers compris entre $n/2$ et $n - 3$, on a $X_b < Y_a$ (on a utilisé ici une sorte de "principe des tiroirs" inversé : si on met 0 ou 1 objet dans k tiroirs, on ne peut avoir plus d'objets que de tiroirs, i.e. plus de k objets). Mais le nombre de nombres premiers contenus dans un intervalle est toujours inférieur au nombre de nombres composés contenus dans cet intervalle (pour $n > 100$). Donc $Y_a < Y_c$. Donc $X_b + Y_c < Y_a + Y_c < 2Y_c$.

- $\left\lfloor \dfrac{n-4}{4} \right\rfloor$ est pour tout entier supérieur à un certain entier assez petit (comme 100) supérieur à $2Y_c$. Cela assure qu'on a jamais l'égalité $T_a + T_c + \epsilon = X_b + Y_c$ qui découlerait de l'absence de lettre a dans un mot.

Conclusion

- On a utilisé un langage à 4 lettres pour représenter les décompositions de n comme somme de deux impairs.
- Les règles de réécriture préservent la largeur des "tranches de lettres".
- On se situe dans une théorie lexicale des nombres, selon laquelle les nombres sont des mots.
- Il faut toujours bien observer l'ordre des lettres dans les mots.

Conjecture de Goldbach (7 juin 1742)

- 271 ans
- **Énoncé** : Tout nombre pair (n) supérieur à 2 est la somme de deux nombres premiers ($n = p + q$).
- p et q impairs ; $3 \leqslant p \leqslant n/2$ et $n/2 \leqslant q \leqslant n - 3$
- $$\begin{aligned} 98 &= 19 + 79 \\ &= 31 + 67 \\ &= 37 + 61 \end{aligned}$$

Booléens

- On représente la primalité par des booléens.
- 0 signifie *est premier*, 1 signifie *est composé*.
- $23 \rightarrow 0$
- $25 \rightarrow 1$
-

3	5	7	9	11	13	15	17	19	21	23	25	27	29	...
0	0	0	1	0	0	1	0	0	1	0	1	1	0	...

Copie de l'espace : 4 lettres pour 4 possibilités

- On représente les décompositions de n en sommes de deux nombres impairs par des lettres.
- $28 = \underset{p}{5} + \underset{p}{23} = \textit{premier} + \textit{premier} = a$
- $28 = \underset{c}{9} + \underset{p}{19} = \textit{composé} + \textit{premier} = b$
- $28 = \underset{p}{3} + \underset{c}{25} = \textit{premier} + \textit{composé} = c$
- $40 = \underset{c}{15} + \underset{c}{25} = \textit{composé} + \textit{composé} = d$

Mots de 40 et 42

40	37	35	33	31	29	27	25	23	21
	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0
	3	5	7	9	11	13	15	17	19
	a	*c*	*c*	*b*	*a*	*c*	*d*	*a*	*c*

42	39	37	35	33	31	29	27	25	23	21
	1	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21
	c	*a*	*c*	*d*	*a*	*a*	*d*	*c*	*a*	*d*

Observer les mots diagonaux

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

Propriétés des mots diagonaux

- Les mots diagonaux (diagonales) ont leurs lettres soit dans l'alphabet A_{ab} soit dans l'alphabet A_{cd}.
- Une diagonale code en effet des décompositions de même second sommant et de premier sommant un nombre impair de la liste des impairs successifs à partir de 3.
- Par exemple, la diagonale *aaaba*, qui commence au *a* première lettre du mot de 26 code les décompositions $3 + 23, 5 + 23, 7 + 23, 9 + 23, 11 + 23$ et $13 + 23$.

Projection P

$H_{34,3}$: $Z_a = 5$, $Z_c = 2$

6 : a

8 : a

10 : a a

12 : c a

14 : a c a

16 : a a c

18 : c a a d

$B_{34,3}$: $Y_a = 5$, $Y_c = 3$

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 $\leftarrow X_a = 4, X_b = 1$

$X_c = 2, X_d = 1$

Exemple

- Intrication $Y_a(n), X_a(n), X_b(n)$

$$\begin{aligned} Y_a(34) &= \#\{3+17, 3+19, 3+23, 3+29, 3+31\} \\ \\ X_a(34) &= \#\{3+31, 5+29, 11+23, 17+17\} \\ X_b(34) &= \#\{15+19\} \end{aligned}$$

- Intrication $Y_c(n), X_c(n), X_d(n)$

$$\begin{aligned} Y_c(34) &= \#\{3+21, 3+25, 3+27\} \\ \\ X_c(34) &= \#\{7+27, 13+21\} \\ X_d(34) &= \#\{9+25\} \end{aligned}$$

Propriétés d'intrication des variables

- $$Y_a(n) = X_a(n) + X_b(n) \quad (1)$$
- $$Y_c(n) = X_c(n) + X_d(n) \quad (2)$$
- $$Y_a(n) + Y_c(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \quad (3)$$
- $$X_a(n) + X_b(n) + X_c(n) + X_d(n) = \left\lfloor \frac{n-2}{4} \right\rfloor \quad (4)$$
- $$Z_a(n) + Z_c(n) = \left\lfloor \frac{n-4}{4} \right\rfloor \quad (5)$$

Propriétés d'intrication des variables

- $$X_a(n) + X_c(n) = Z_a(n) + \delta_{2p}(n) \qquad (6)$$

  avec $\delta_{2p}(n)$ qui vaut 1 si n est le double d'un nombre premier et 0 sinon.

- $$X_b(n) + X_d(n) = Z_c(n) + \delta_{2c-imp}(n) \qquad (7)$$

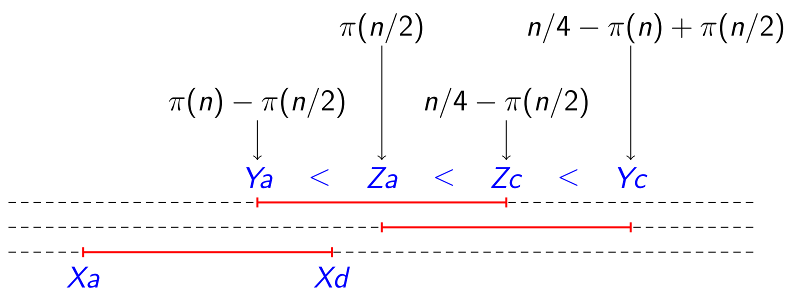
  avec $\delta_{2c-imp}(n)$ qui vaut 1 si n est un double d'impair composé et 0 sinon.

- $$Z_c(n) - Y_a(n) = Y_c(n) - Z_a(n) - \delta_{4k+2}(n) \qquad (8)$$

  avec $\delta_{4k+2}(n)$ qui vaut 1 si n est un double d'impair et 0 sinon.

- $$Z_c(n) - Y_a(n) = X_d(n) - X_a(n) - \delta_{2c-imp}(n) \qquad (9)$$

Propriétés d'intrication des écarts



n	X_a	X_b	X_c	X_d	Y_a	Y_c	A	Z_a	Z_c	B	$\delta_{2p}(n)$	$\delta_{2cimp}(n)$	$\delta_{4k+2}(n)$
14	2	0	1	0	2	1	3	2	0	2	1	0	1
16	2	0	1	0	2	1	3	3	0	3	0	0	0
18	2	0	1	1	2	2	4	3	0	3	0	1	1
20	2	1	1	0	3	1	4	3	1	4	0	0	0
22	3	1	1	0	4	1	5	3	1	4	1	0	1
24	3	0	1	1	3	2	5	4	1	5	0	0	0
26	3	1	2	0	4	2	6	4	1	5	1	0	1
28	2	1	3	0	3	3	6	5	1	6	0	0	0
30	3	0	2	2	3	4	7	5	1	6	0	1	1
32	2	2	3	0	4	3	7	5	2	7	0	0	0
34	4	1	2	1	5	3	8	5	2	7	1	0	1
36	4	0	2	2	4	4	8	6	2	8	0	0	0
38	2	2	5	0	4	5	9	6	2	8	1	0	1
40	3	1	4	1	4	5	9	7	2	9	0	0	0
42	4	0	3	3	4	6	10	7	2	9	0	1	1
44	3	2	4	1	5	5	10	7	3	10	0	0	0
46	4	2	4	1	6	5	11	7	3	10	1	0	1
48	5	0	3	3	5	6	11	8	3	11	0	0	0
50	4	2	4	2	6	6	12	8	3	11	0	1	1
52	3	3	5	1	6	6	12	8	4	12	0	0	0
54	5	1	3	4	6	7	13	8	4	12	0	1	1
56	3	4	5	1	7	6	13	8	5	13	0	0	0
58	4	3	5	2	7	7	14	8	5	13	1	0	1
60	6	0	3	5	6	8	14	9	5	14	0	0	0
62	3	4	7	1	7	8	15	9	5	14	1	0	1
64	5	2	5	3	7	8	15	10	5	15	0	0	0
66	6	1	4	5	7	9	16	10	5	15	0	1	1
68	2	5	8	1	7	9	16	10	6	16	0	0	0
70	5	3	5	4	8	9	17	10	6	16	0	1	1
72	6	2	4	5	8	9	17	10	7	17	0	0	0
74	5	4	6	3	9	9	18	10	7	17	1	0	1
76	5	4	6	3	9	9	18	11	7	18	0	0	0
78	7	2	4	6	9	10	19	11	7	18	0	1	1
80	4	5	7	3	9	10	19	11	8	19	0	0	0

Intrications des variables et des écarts (invariants)

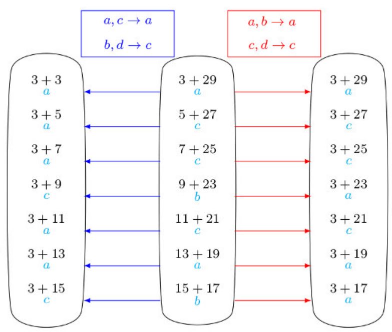
n	$X_a(n)$	$X_b(n)$	$X_c(n)$	$X_d(n)$
999 998	4 206	32 754	37 331	175 708
1 000 000	5 402	31 558	36 135	176 904
9 999 998	28 983	287 084	319 529	1 864 403
10 000 000	38 807	277 259	309 705	1 874 228

n	$Y_a(n)$	$Y_c(n)$	$\left\lfloor \frac{n-2}{4} \right\rfloor$	$Z_a(n)$	$Z_c(n)$	$\left\lfloor \frac{n-4}{4} \right\rfloor$	$\delta_{2p}(n)$	$\delta_{2ci}(n)$	$\delta_{4k+2}(n)$
999 998	36 960	213 039	249 999	41 537	208 461	249 998	0	1	1
1 000 000	36 960	213 039	249 999	41 537	208 462	249 999	0	1	0
9 999 998	316 067	2 183 932	2 499 999	348 511	2 151 487	2 499 998	1	0	1
10 000 000	316 066	2 183 933	2 499 999	348 512	2 151 487	2 499 999	0	1	0

Bijections

- $n = 32$

$$Z_a = X_a + X_c = 5$$
$$Z_c = X_b + X_d = 2$$
$$Z_a + Z_c = \left\lfloor \frac{n-4}{4} \right\rfloor = 7$$



$$Y_a = X_a + X_b = 4$$
$$Y_c = X_c + X_d = 3$$
$$Y_a + Y_c = \left\lfloor \frac{n-2}{4} \right\rfloor = 7$$

$$X_a = 2$$
$$X_b = 2$$
$$X_c = 3$$
$$X_d = 0$$

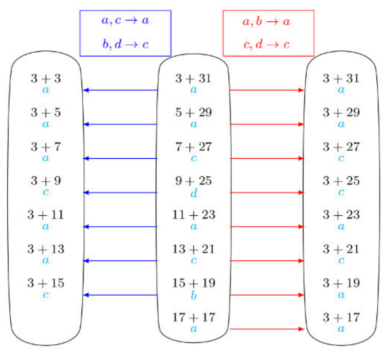
Bijections

- $n = 34$

$Z_a = X_a + X_c = 5$

$Z_c = X_b + X_d = 2$

$Z_a + Z_c = \left\lfloor \frac{n-4}{4} \right\rfloor = 7$



$Y_a = X_a + X_b = 5$

$Y_c = X_c + X_d = 3$

$Y_a + Y_c = \left\lfloor \frac{n-2}{4} \right\rfloor = 8$

$X_a = 4$

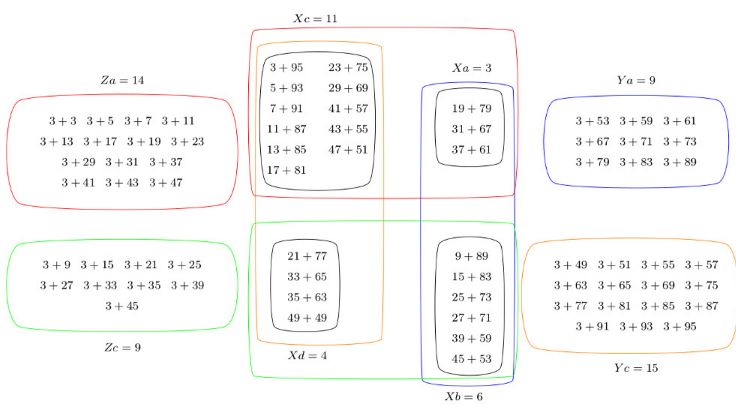
$X_b = 1$

$X_c = 2$

$X_d = 1$

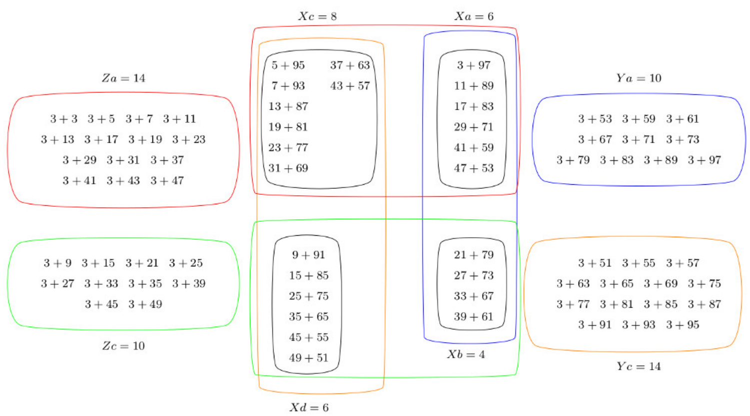
Bijections : visualisation du double comptage

- $n = 98$



Bijections : visualisation du double comptage

- $n = 100$



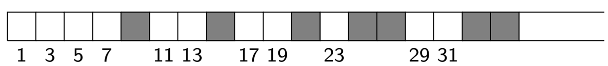
Les tirettes de Laisant

- **Charles-Ange Laisant** : Sur un procédé expérimental de vérification de la conjecture de Goldbach, Bulletin de la SMF, 25, 1897.

- *"Ce fameux théorème empirique : Tout nombre pair est la somme de deux nombres premiers, dont la démonstration semble dépasser les possibilités scientifiques actuelles, a fait l'objet de nombreux travaux et de certaines contestations. Lionnet a tenté d'établir que la proposition devait probablement être inexacte. M. Georg Cantor l'a vérifiée numériquement jusqu'à 1000, en donnant pour chaque nombre pair toutes les décompositions en deux nombres premiers, et il a remarqué que le nombre de ces décompositions ne cesse de croître en moyenne, tout en présentant de grandes irrégularités."*

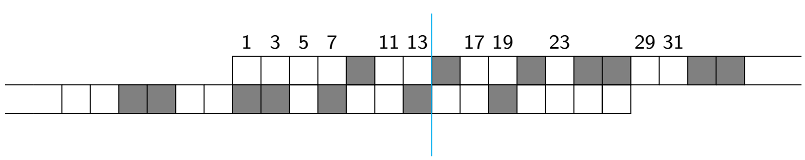
Les tirettes de Laisant

- *"Voici un procédé qui permettrait de faire sans calculs la vérification expérimentale dont il s'agit, et d'avoir pour chaque nombre pair, à la seule inspection d'une figure, toutes les décompositions. Supposons que sur une bande formée de carrés accolés, représentant les nombres impairs successifs, on ait construit le crible d'Erathostène, en ombrant les nombres composés, jusqu'à une limite quelconque* $2n$*."*



Les tirettes de Laisant

- *"Si l'on a construit deux réglettes pareilles, et si l'on place la seconde au-dessous de la première en la retournant et en faisant correspondre la case* 1 *à* $2n$*, il est évident que si le théorème de Goldbach est vrai pour* $2n$*, il y aura quelque part deux cases blanches en correspondance ; et tous les couples de cases blanches donneront les diverses décompositions. On les aura même en lisant la moitié de la figure, à cause de la symétrie par rapport au milieu. Ainsi la vérification relative au nombre* 28 *donnera la figure 2 et montrera qu'on a les décompositions* $28 = 5 + 23 = 11 + 17$*."*



Résumé

- $X_a : p + p$
- $X_b : c + p$
- $X_c : p + c$
- $X_d : c + c$
- $Z_a : 3 + p, \quad (p < n/2)$
- $Z_c : 3 + c, \quad (c < n/2)$
- $Y_a : 3 + p, \quad (p \geqslant n/2)$
- $Y_c : 3 + c, \quad (c \geqslant n/2)$
- $\{3+p_k\} \quad Y_a = X_a + X_b \quad \{p+p_i\} \cup \{c+p_j\} \quad (p_i, p_j, p_k \geqslant n/2)$
- $\{3+c_k\} \quad Y_c = X_c + X_d \quad \{p+c_i\} \cup \{c+c_j\} \quad (c_i, c_j, c_k \geqslant n/2)$
- $\{3+p_k\} \quad Z_a = X_a + X_c \quad \{p_i+p\} \cup \{p_j+c\} \quad (p_i, p_j, p_k < n/2)$
- $\{3+c_k\} \quad Z_c = X_b + X_d \quad \{c_i+p\} \cup \{c_j+c\} \quad (c_i, c_j, c_k < n/2)$

Résumé

- $Y_a + Y_c = X_a + X_b + X_c + X_d = \left\lfloor \frac{n-2}{4} \right\rfloor$

- $Z_a + Z_c = \left\lfloor \frac{n-4}{4} \right\rfloor$

- $\left\lfloor \frac{n-4}{4} \right\rfloor = Z_a + Z_c \simeq Y_a + Y_c = \left\lfloor \frac{n-2}{4} \right\rfloor$

- $Z_c - Y_a \simeq X_d - X_a$
  par définition car $Z_c - Y_a$ correspond à
  $\{c+p\} \cup \{c+c\} \backslash \{c+p\} \cup \{p+p\}$

Conclusion

- On a utilisé un langage à 4 lettres pour représenter les décompositions de n comme somme de deux impairs.
- On se situe dans une théorie lexicale des nombres, selon laquelle les nombres sont des mots.
- Il faut toujours bien observer l'ordre des lettres dans les mots.