Infinité de l'ensemble des nombres premiers jumeaux, conjecture de Goldbach et un lemme de Gauss

Denise Vella-Chemla

30/6/2012

1 Introduction

Dans cette note, on essaie de démontrer deux conjectures portant sur les nombres premiers en utilisant une approche, que l'on pourrait qualifier de lexicale, qui utilise des mots de représentation des entiers par leurs restes modulaires selon les nombres premiers successifs.

On appelle *nombres premiers jumeaux* deux nombres premiers dont la différence est 2.

Exemples :

3 et 5 sont des nombres premiers jumeaux.
29 et 31 sont des nombres premiers jumeaux.

La conjecture des nombres premiers jumeaux stipule que l'ensemble des nombres premiers jumeaux est infini.

La conjecture de Goldbach stipule que tout nombre pair supérieur à 4 est la somme de deux nombres premiers impairs.

2 Représentation par les restes

Représentons les premiers entiers naturels par leurs restes modulo les nombres premiers successifs.

Pour passer du *"mot"* d'un nombre au mot de son successeur selon l'arithmétique de Peano, on ajoute à ce mot le mot n-uplet infini $(1, 1, 1, 1, \ldots)$ qui représente l'entier naturel 1.

mod	2	3	5	7	11	13	17	19	...
1	1	1	1	1	1	1	1	1	...
2	0	2	2	2	2	2	2	2	...
3	1	0	3	3	3	3	3	3	...
4	0	1	4	4	4	4	4	4	...
5	1	2	0	5	5	5	5	5	...
6	0	0	1	6	6	6	6	6	...
7	1	1	2	0	7	7	7	7	...
8	0	2	3	1	8	8	8	8	...
9	1	0	4	2	9	9	9	9	...
10	0	1	0	3	10	10	10	10	...
11	1	2	1	4	0	11	11	11	...
12	0	0	2	5	1	12	12	12	...
13	1	1	3	6	2	0	13	13	...
14	0	2	4	0	3	1	14	14	...
15	1	0	0	1	4	2	15	15	...

Observons quelques représentations par les restes qui sont pertinentes par rapport à la conjecture des nombres premiers jumeaux.

6, le nombre pair juste entre les deux nombres premiers jumeaux 5 et 7 a pour représentation 0 0 1 6 6 6 ....
Il a un 1 en troisième position parce que 5 a un 0 à cette position (un nombre premier est congru à 0 modulo lui-même, jamais congru à 0 modulo un nombre premier qui lui est strictement inférieur et congru à lui-même modulo tout nombre premier qui lui est strictement supérieur). 6 a un 6 en quatrième position parce que 7 a un 0 à cette position-là (le reste de 7 modulo lui-même). Les deux premières lettres du mot de représentation du nombre 6 ne sont ni des 1 ni des $p_k - 1$ pour p_k valant 2 et 3 (ni 1 ni 1 comme reste dans la division par 2, ni 1 ni 2 comme reste dans la division par 3) car si tel était le cas, l'un ou l'autre de 5 ou 7 serait composé.

18, entre 17 et 19, a pour représentation 0 0 3 4 7 5 1 18 ... : il n'a ni 1 ni $p_k - 1$ parmi ses six premières lettres, correspondant à ses restes modulo $2, 3, 5, 7, 11$ et 13. Le mot de 18 a un 1 en septième position (correspondant à son reste modulo 17 : $18 = 17 + 1$) et 18 a un reste de 18 en huitième position (correspondant à son reste modulo $19 = 18 + 1$).

Un nombre pair $p_i + 1$ juste entre deux nombres premiers jumeaux p_i et $p_i + 2$ a son écriture qui est caractérisée par le fait qu'elle ne contient ni 1 ni $p_k - 1$ pour tout module p_k strictement inférieur à p_i.

3 Définitions

Notons $\mathbb{P}$ l'ensemble des nombres premiers.

On définit la bijection p de $\mathbb{N}^*$ dans $\mathbb{P}$ qui associe à tout i, un entier naturel non-nul, $p(i) = p_i$, le i-ème plus petit nombre premier de $\mathbb{P}$.

Deux nombres premiers impairs p_j et p_k sont jumeaux si $k = j + 1$. L'entier $2n_k = p_j + 1$ sera appelé le père des jumeaux (en fait, le pair entre les jumeaux).

Une suite de k nombres premiers distincts est appelée une base modulaire d'ordre k.

La suite $B_k = (p_1 = 2, p_2 = 3, ..., p_k)$ des k premiers nombres premiers est appelée une base modulaire fondamentale d'ordre k.
Désormais, l'expression base modulaire désignera une telle base fondamentale.

Un nombre n étant donné, sa projection dans B_k est la suite des restes r_j de la divison de n par les p_j ($j \leq k$). r_j est appelé la j-ème composante de n dans B_k.

Propriété 1 : un entier naturel a tous ses restes selon les nombres premiers intervenant dans sa décomposition en facteurs premiers qui sont nuls.

En conséquence,

Propriété 2 : en particulier, un nombre premier a comme seul reste nul son reste modulo lui-même.

Propriété 3 : dans B_{j-1}, les k-èmes ($k < j$) composantes de $2n_j$ (père des jumeaux p_j et p_{j+1}) sont différentes de 1 et de $p_k - 1$.

Preuve :

Supposons que l'une des k-èmes ($k < j$) composantes de $2n_j$ soit égale à 1.

Alors $2n_j = \prod_1^{j-1} p_r^{\alpha_r} = c(k)p_k^{\alpha_k} + 1$ de sorte que $2n_j - 1 = p_j = c(k)p_k^{\alpha_k}$: par suite, quel que soit k, la k-ème composante de p_j dans B_{j-1} est nulle, ce qui est en contradiction avec la propriété 2 pour le nombre premier p_j.

De façon similaire, supposons que l'une des k-èmes ($k < j$) composantes de $2n_j$ soit égale à $p_k - 1$, alors $2n_j = \prod_1^{j-1} p_r^{\alpha_r} = c(k)p_k^{\alpha_k} - 1$ de sorte que $2n_j + 1 = p_{j+1} = c(k)p_k^{\alpha_k}$: par suite, quel que soit k, la k-ème composante de p_{j+1} dans B_{j-1} est nulle, ce qui est en contradiction avec la propriété 2 pour le nombre premier p_{j+1}.

Propriété 4 : dans B_{j-1}, les k-èmes ($k < j$) composantes de n_j (la moitié du père $2n_j$ de 2 jumeaux p_j et p_{j+1}) sont différentes de $\frac{p_k-1}{2}$ et de $\frac{p_k+1}{2}$.
Cela découle du fait que :

$$\begin{array}{ll} & 2n_j \not\equiv p_k - 1 \ (mod\ p_k) \\ \iff & n_j \not\equiv \frac{p_k-1}{2} \ (mod\ p_k) \end{array}$$

et d'autre part :

$$\begin{array}{ll} & 2n_j \not\equiv 1 \ (mod\ p_k) \\ \iff & 2n_j \not\equiv p_k + 1 \ (mod\ p_k) \\ \iff & n_j \not\equiv \frac{p_k+1}{2} \ (mod\ p_k) \end{array}$$

4 A la recherche d'un père de jumeaux

On appelle *primorielle* d'un nombre premier p_i le produit de tous les nombres premiers inférieurs ou égaux à p_i.

$$\#p_i = \prod_{\substack{2 \leq p_k \leq p_i, \\ p_k\ premier}}^{p_i} p_k$$

On souhaite démontrer qu'il y a toujours entre deux primorielles consécutives un père de jumeaux.

Si l'on considère tous les nombres pairs entre deux primorielles consécutives $\#p_i$ et $\#p_{i+1}$ (par exemple, tous les pairs compris entre $30 = 2.3.5$ et $210 = 2.3.5.7$), ces nombres sont les doubles de nombres consécutifs compris quant à eux entre deux moitiés de primorielles (en l'occurrence 15 et 105) et il faudrait être capable de démontrer que parmi eux, l'un forcément est la moitié d'un père de jumeaux.

4.1 Exemple

Dans le tableau suivant, on consigne dans la première ligne les restes de 51 selon tous les modules inférieurs à 105 (modules en tête des colonnes), ainsi que dans les deuxième et troisième lignes les restes interdits $\frac{p_k-1}{2}$ et $\frac{p_k+1}{2}$.

p_k	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	...	105
$51\ mod\ p_k$	1	0	1	2	7	12	0	13	5	22	20	14	10	8	4	51	...	51
$\frac{p_k-1}{2}$		1	2	3	5	6	8	9	11	14	15	18	20	21	23	...	...	...
$\frac{p_k+1}{2}$		2	3	4	6	7	9	10	12	15	16	19	21	22	24	...	...	...

51 vérifie les conditions requises pour que son double soit un père de jumeaux (i.e. un nombre pair juste entre deux nombres premiers). Effectivement, $102 = 2 \times 51$ est entre les deux nombres premiers 101 et 103.

5 L'article 127 des recherches arithmétiques de Gauss

Dans l'article 127 des Recherches arithmétiques, Gauss fournit un lemme qu'il démontre :

> LEMME : *Dans la progression* $1, 2, 3, 4, \ldots, n$, *il ne peut y avoir plus de termes divisibles par un nombre quelconque* h, *que dans la progression* $a, a+1, a+2, \ldots, a+n-1$, *qui a le même nombre de termes.*

En effet, on voit sans peine que si n est divisible par h, il y a dans chaque progression $\frac{n}{h}$ termes divisibles par h ; sinon soit $n = he + f$, f étant $< h$; il y aura dans la première série e termes, et dans la seconde e ou $e+1$ termes divisibles par h.

Il suit de là, comme corollaire, que $\frac{a(a+1)(a+2)(a+3)\ldots(a+n-1)}{1\ 2\ 3\ \ n}$ est toujours un nombre entier : proposition connue par la théorie des nombres figurés, mais qui, si je ne me trompe, n'a encore été démontrée directement par personne*.

Enfin on aurait pu présenter plus généralement ce lemme comme il suit :

> *Dans la progression* $a, a+1, a+2, \ldots, a+n-1$, *il y a au moins autant de termes congrus suivant le module* h *à un nombre donné quelconque, qu'il y a de termes divisibles par* h *dans la progression* $1, 2, 3, \ldots, n$.

6 Utilisation du lemme de Gauss dans la recherche d'un père de jumeaux

Ce que nous dit le lemme de Gauss, c'est que la quantité de nombres compris entre deux valeurs a et b et qui ne sont congrus ni à $\frac{p_k-1}{2}$ ni à $\frac{p_k+1}{2}$ selon tout module p_k inférieur à un nombre donné c est au moins égale à la quantité de nombres compris entre 1 et $b-a+1$ qui ne sont congrus ni à $\frac{p_k-1}{2}$ ni à $\frac{p_k+1}{2}$ selon tout module p_k inférieur à c.

Le tableau suivant présente quelques résultats pour les premières primorielles.

L'expression *"Nb satisf."* est utilisé pour représenter la quantité de nombres qui ne sont ni congrus à $\frac{p_k-1}{2}$ ni à $\frac{p_k+1}{2}$ pour tout p_k inférieur à $\frac{\#p_{i+1}}{2}$.

*En annexe 3 est fournie une démonstration de ce corollaire.

$\frac{\#p_i}{2}$	$\frac{\#p_{i+1}}{2}$	$Diff$	$Nb\ satisf.\ de\ 1\ à\ Diff$	$Nb\ satisf.\ de\ \frac{\#p_i}{2}\ à\ \frac{\#p_{i+1}}{2}$
3	15	12	1	2
15	105	90	3	6
105	1 155	1 050	23	28
1 155	15 015	13 860	169	196

Le fait de se ramener ainsi à des ensembles de nombres consécutifs à partir de 1 devrait permettre de montrer qu'au fur et à mesure de l'augmentation des primorielles, on est assuré de toujours trouver un nombre entre 2 moitiés de primorielles qui ne soit jamais congru à $\frac{p_k-1}{2}$ ou à $\frac{p_k+1}{2}$ pour tout p_k inférieur à une moitié de primorielle donnée $\frac{\#p_{i+1}}{2}$. Le double de ce nombre n'est quant à lui ni congru à 1 ni congru à $p_k - 1$ selon tout module p_k inférieur à $\frac{\#p_{i+1}}{2}$, ce qui assure qu'il est un père de jumeaux. Pour être assuré de toujours trouver une moitié de père de jumeaux entre 2 moitiés de primorielles, on minore la quantité de nombres non-congrus à $\frac{p_k-1}{2}$ ou à $\frac{p_k+1}{2}$ pour tout p_k inférieur à la moitié de primorielle $\frac{\#p_{i+1}}{2}$ par une quantité de nombres à calculer sur l'intervalle de nombres $[1, \Delta]$, où $\Delta = \frac{\#p_{i+1}-\#p_i}{2}$.

En effet, la quantité de nombres compris entre 1 et $\frac{\#p_{i+1}-\#p_i}{2}$ et qui sont non-congrus à $\frac{p_k-1}{2}$ selon tout module premier p_k inférieur à $\frac{\#p_{i+1}}{2}$ est minorable par la quantité de nombres premiers compris entre 1 et $\frac{\#p_{i+1}-\#p_i}{2}$ selon le lemme de Gauss, la congruence à 0 advenant avec autant d'occurrence que la congruence à $\frac{p_k-1}{2}$ $(mod\ p_k)$. On doit noter également que si $x \equiv \frac{p_k-1}{2}\ (mod\ p_k)$ alors $x+1 \equiv \frac{p_k+1}{2}\ (mod\ p_k)$ (i.e. les nombres congrus à $\frac{p_k+1}{2}$ sont les successeurs au sens de Peano des nombres congrus à $\frac{p_k-1}{2}$). En annexe 2, on présente un exemple d'application de l'algorithme d'élimination des nombres congrus à $\frac{p_k-1}{2}$ ou à$\frac{p_k+1}{2}$ selon un module premier p_k inférieur à $\frac{\#p_{i+1}}{2}$ dans le cas où $\#p_{i+1} = 30 = 2 \times 3 \times 5$.

Le nombre de moitiés de père de jumeaux augmente strictement lorsqu'on passe de l'intervalle $[1, \frac{\#p_{i+1}-\#p_i}{2}]$ à l'intervalle $[1, \frac{\#p_{i+2}-\#p_{i+1}}{2}]$; cela devrait permettre d'assurer qu'un père de jumeaux existe toujours entre deux primorielles consécutives.

7 Approche similaire pour la recherche d'un décomposant de Goldbach d'un nombre pair donné

7.1 Reformulation de la conjecture de Goldbach

Notons $\mathbb{P}^*$ l'ensemble des nombres premiers impairs et $\mathbb{P}^*(y) = \{x \in \mathbb{P}^* / x \leq y\}$.
La conjecture de Goldbach est équivalente à l'énoncé suivant :

$$\forall\, n \in 2\mathbb{N}\backslash\{0,2,4\},\ \exists\, p \in \mathbb{P}^*(n/2),\ \forall\, m \in \mathbb{P}^*(\sqrt{n}), \qquad p \not\equiv n\ (mod\ m)$$

En effet,

$$\begin{array}{c}\forall\, n \in 2\mathbb{N}\backslash\{0,2,4\},\ \exists\, p \in \mathbb{P}^*(n/2),\ \forall\, m \in \mathbb{P}^*(\sqrt{n}),\\ p \not\equiv n\ (mod\ m) \Leftrightarrow n-p \not\equiv 0\ (mod\ m) \Leftrightarrow n-p\ premier\end{array}$$

Il y a autant de nombres congrus à n $(mod\ p_k)$ sur l'intervalle $[1, n/2]$ que de nombres divisibles par p_k sur cet intervalle.

7.2 Étude d'un exemple

L'exemple présenté est la recherche de décomposants de Goldbach de $n = 38$. 38 étant le double d'un nombre premier vérifie trivialement la conjecture mais cet exemple nous permettra de comprendre que les doubles de nombres composés ne peuvent qu'avoir davantage de décomposants de Goldbach que les

doubles de nombres premiers.

Première étape : élimination des "petits" nombres premiers qui sont inférieurs à $\sqrt{n}$ (qui pourraient parfois être des décomposants de Goldbach de n mais on souhaite montrer qu'il existe toujours des décomposants de Goldbach de n non-compris ceux-là) et des nombres composés dont un diviseur est un nombre premier inférieur à $\sqrt{n}$ (on élimine tout nombre qui a un reste égal à 0 selon l'un des modules inférieurs à $\sqrt{n}$).

mod	3	5	
1	1	1	
3	⓪	3	*
5	2	⓪	*
7	1	2	
9	⓪	4	*
11	2	1	
13	1	3	
15	⓪	⓪	*
17	2	2	
19	1	4	
38	2	3	

Deuxième étape : élimination des nombres congrus à n selon un module premier inférieur à $\sqrt{n}$.

mod	3	5	
1	1	1	
3	0	③	*
5	②	0	*
7	1	2	
9	0	4	
11	②	1	*
13	1	③	*
15	0	0	
17	②	2	*
19	1	4	
38	2	3	

Le nombre 3, divisible par 3 d'une part, et partageant son reste dans la division par 5 avec 38 d'autre part, est éliminé lors des deux étapes. Le nombre 5, divisible par 5 d'une part, et partageant son reste dans la division par 3 avec 38 d'autre part, est également éliminé lors des deux étapes.

En annexe 4 est fournie la quantité de nombres de l'intervalle $[1, x]$ congrus à $2x$ $(mod\ p_k)$ et qui dépend des restes de x et $2x$ dans la division par p_k.

7.3 Minoration du nombre de décomposants de Goldbach

Il semblerait alors qu'on puisse minorer le nombre de décomposants de Goldbach d'un nombre pair donné en appliquant la fonction π de comptage des nombres premiers à $\pi(\frac{n+2}{4})$, la première application de la fonction π étant destinée à éliminer de l'intervalle $[1, n/2]$ les nombres composés (ainsi que les petits premiers) et la deuxième application de la fonction π servant quant à elle à éliminer les nombres congrus à n parmi les nombres restants.

Le tableau suivant fournit les valeurs de n, $\pi(\frac{n+2}{4})$, $\pi(\pi(\frac{n+2}{4}))$ et $NbDG(n)$ (le nombre de décompositions de Goldbach de n) pour des nombres pairs n qui sont des doubles de nombres premiers.

n	$n/2$ (*qui est premier*)	$\frac{n+2}{4}$	$\pi(\frac{n+2}{4})$	$\pi(\pi(\frac{n+2}{4}))$	$NbDG(n)$
202	101	51	15	6	9
2 018	1 009	505	96	24	28
20 014	10 007	5 004	670	121	174
200 006	100 003	50 002	5 133	685	1 071
2 000 006	1 000 003	500 002	41 538	4 343	7 336
20 000 038	10 000 019	5 000 010	348 513	29 859	53 269

En ce qui concerne les doubles de nombres composés, le pair n ayant plusieurs restes nuls, la quantité de nombres éliminés par la deuxième étape est bien moindre. L'écart entre le nombre obtenu et le nombre de décomposants de Goldbach est encore plus grand que pour les doubles de premiers. Le double d'un composé a plus de décomposants de Goldbach qu'un double de premier qui le divise.

n	$\pi(n/4)$	$\pi(\pi(n/4))$	$\pi(n/2)$	$\pi(\pi(n/2))$	$NbDG(n)$
10^2	9	4	15	6	6
10^3	53	16	95	24	28
10^4	367	73	669	121	127
10^5	2 762	402	5 133	685	810
10^6	22 044	2 470	41 538	4 343	5 402
10^7	183 072	16 589	348 513	29 859	38 807
10^8	1 565 927	118 784	3 001 134	216 890	291 400

Cependant, comme on ne sait pas comment "agréger" les probabilités selon les différents modules les unes aux autres, comme présenté en annexe 4, on s'orientera plutôt vers une méthode de démonstration connue sous le nom de descente infinie de Fermat.

8 Essayer de démontrer la conjecture de Goldbach par une descente infinie de Fermat

On cherche à démontrer l'impossibilité de l'existence d'un entier pair qui ne vérifie pas la conjecture de Goldbach.

$(\exists x \in 2\mathbb{N},\ x \geq 20,\ x\ ne\ v\acute{e}rifie\ pas\ la\ conjecture\ de\ Goldbach) \Rightarrow\ false$

mais $\exists x \in 2\mathbb{N},\ x \geq 20,\ x\ ne\ v\acute{e}rifie\ pas\ la\ conjecture\ de\ Goldbach$

$\Leftrightarrow \exists x \in 2\mathbb{N},\ x \geq 20,\ \forall p \in \mathbb{P}^*(x/2),\ x - p\ compos\acute{e}$

$\Leftrightarrow \exists x \in 2\mathbb{N},\ x \geq 20,\ \forall p \in \mathbb{P}^*(x/2),\ \exists m \in \mathbb{P}^*(\sqrt{x}),\ x - p \equiv 0\ (mod\ m)$

$\Leftrightarrow \exists x \in 2\mathbb{N},\ x \geq 20,\ \forall p \in \mathbb{P}^*(x/2),\ \exists m \in \mathbb{P}^*(\sqrt{x}),\ x \equiv p\ (mod\ m)$

$$\Leftrightarrow \exists x \in 2\mathbb{N},\ x \geq 20,\ \forall p \in \mathbb{P}^*(x/2),\ \exists m \in \mathbb{P}^*(\sqrt{x}),\ \mathcal{S} \begin{cases} x \equiv p_1\ (mod\ m_{j_1}) \\ x \equiv p_2\ (mod\ m_{j_2}) \\ \dots \\ x \equiv p_k\ (mod\ m_{j_k}) \end{cases}$$

Note : les modules m_{j_i} sont des modules premiers impairs qui peuvent être égaux.

8.1 Mode de raisonnement de ce type de démonstration

Si un nombre ne vérifiait pas la conjecture de Goldbach, il y en aurait un plus petit qui ne la vérifierait pas non plus et ainsi de proche en proche, jusqu'à atteindre des nombres si petits qu'on sait qu'ils vérifient la conjecture.

Il n'existe pas de suite infinie strictement décroissante d'entiers naturels.

Il s'agit de raisonner par l'absurde :
- on suppose que x est le plus petit entier tel que $P(x)$.
- on montre qu'alors $P(x')$ avec $x' < x$.
- on a abouti à une contradiction.

Si $P(n)$ est vérifiée pour un entier naturel n donné, il existe une partie non vide de $\mathbb{N}$ contenant un élément qui vérifie la propriété P. Cette partie admet un plus petit élément. En l'occurrence, la propriété P consiste à ne pas vérifier la conjecture de Goldbach.

8.2 Aboutir à une contradiction

Rappel : on cherche à aboutir à une contradiction à partir de l'hypothèse :

$$\exists x \in 2\mathbb{N},\ x \geq 20,\ \textit{tel que}\ \forall\, p_1, \ldots, p_k \in \mathbb{P}^*(x/2),\ \exists m_{j_1}, \ldots, m_{j_k} \in \mathbb{P}^*(\sqrt{x}).$$
$$\mathcal{S} \begin{cases} x \equiv p_1 \ (mod\ m_{j_1}) \\ x \equiv p_2 \ (mod\ m_{j_2}) \\ \qquad \ldots \\ x \equiv p_k \ (mod\ m_{j_k}) \end{cases}$$

x n'est congru à aucun nombre premier selon tout module qui divise x.

x est congru à un certain nombre (éventuellement nul) de nombres premiers selon le module 3, à un certain nombre (éventuellement nul) de nombres premiers selon le module 5, etc.

Il faut démontrer qu'il existe forcément deux modules selon lesquels x est congru à un entier naturel différent.

On appelle congruence canonique une congruence de la forme $x \equiv a\ (mod\ m)$ avec $a < m$ (par exemple, $x \equiv 3\ (mod\ 5)$ est une congruence canonique alors que $x \equiv 8\ (mod\ 5)$ n'en est pas une).

Le plus petit entier naturel vérifiant une congruence canonique de la forme $x \equiv a\ (mod\ m)$ est a.

Deux congruences $x \equiv a\ (mod\ m)$ et $x \equiv b\ (mod\ n)$ ont un même plus petit entier naturel les vérifiant si et seulement si $a = b$.

Exemples

$x \equiv 2\ (mod\ 3)$ $\rightarrow 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38$
$x \equiv 3\ (mod\ 5)$ $\rightarrow 3, 8, 13, 18, 23, 28, 33, 38, 43, 48$

$x \equiv 8\ (mod\ 15)$

Alors que :

$x \equiv 2\ (mod\ 3)$ $\rightarrow 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38$
$x \equiv 2\ (mod\ 5)$ $\rightarrow 2, 7, 12, 17, 22, 27, 32, 37, 42, 47$

$x \equiv 2\ (mod\ 15)$

8.3 Utilitaire : solutions minimales de systèmes de congruences

$$\mathcal{S}\begin{cases} x \equiv 0\ (mod\ 2) \\ x \equiv 1\ (mod\ 3) \\ x \equiv 4\ (mod\ 5) \\ x \equiv 5\ (mod\ 7) \\ x \equiv 6\ (mod\ 11) \\ x \equiv 3\ (mod\ 13) \end{cases}$$

sol.min.	2	3	5	7	11	13		*sol.min.*	2	3	5	7	11	13
21544	0	1	4	5	6	3		1524	0	×	4	5	6	3
754	0	1	4	5	6	×		754	0	×	4	5	6	×
2434	0	1	4	5	×	3		614	0	×	4	5	×	3
124	0	1	4	5	×	×		54	0	×	4	5	×	×
94	0	1	4	×	6	3		94	0	×	4	×	6	3
94	0	1	4	×	6	×		94	0	×	4	×	6	×
94	0	1	4	×	×	3		94	0	×	4	×	×	3
4	0	1	4	×	×	×		4	0	×	4	×	×	×
3526	0	1	×	5	6	3		1524	0	×	×	5	6	3
292	0	1	×	5	6	×		138	0	×	×	5	6	×
250	0	1	×	5	×	3		68	0	×	×	5	×	3
40	0	1	×	5	×	×		12	0	×	×	5	×	×
94	0	1	×	×	6	3		94	0	×	×	×	6	3
28	0	1	×	×	6	×		6	0	×	×	×	6	×
16	0	1	×	×	×	3		16	0	×	×	×	×	3
4	0	1	×	×	×	×		×	0	×	×	×	×	×

On passe de la solution n du système contenant toutes les congruences à une solution n' d'un système inclus en soustrayant un multiple le plus grand possible d'un produit de nombres premiers.

Par exemple, $21544 - 3526 = 18018 = 2.3^2.7.11.13$.

Il faudrait être capable de démontrer que, par une telle soustraction d'un multiple de primorielle, si un nombre ne vérifiait pas Goldbach, un nombre plus petit ne la vérifierait pas non plus.

8.4 Idée générale de la démonstration

	m_1	m_2	$\dots$	m_i	$\dots$	m_k	
p_1	$\boxed{r_1}$						
p_2		$\boxed{r_2}$					
$\vdots$							
p_i				$\boxed{r_i}$			
$\vdots$							
p_k						$\boxed{r_k}$	
$\vdots$							
$x - \prod m_i$	$\boxed{r_1}$	$\boxed{r_2}$	$\dots$	$\boxed{r_i}$			*ne vérifie pas CG*
$\vdots$							
x	$\boxed{r_1}$	$\boxed{r_2}$	$\dots$	$\boxed{r_i}$	$\dots$	$\boxed{r_k}$	*ne vérifie pas CG*

x est le nombre pair dont on considère au début de la démonstration qu'il est le plus entier naturel ne vérifiant pas la conjecture de Goldbach.

Les $p_1, p_2, \dots, p_k$ sont les nombres premiers impairs inférieurs à la moitié de x.

S'en déduisent les modules $m_1, m_2, \ldots, m_k$ selon lesquels x est congru aux différents p_i ; même si plusieurs colonnes peuvent avoir le même entête, on les a distinguées pour faciliter l'écriture du tableau de restes.

$x - \prod m_i$ est l'entier naturel strictement plus petit que x dont il faut s'assurer qu'il ne vérifie pas non-plus la conjecture de Goldbach de façon à "descendre" une marche de Fermat.

$x - \prod m_i$ a les mêmes restes que x selon chacun des m_i intervenant dans le produit.

Annexe 1 : un exemple d'application de l'algorithme de recherche d'une moitié de père de jumeaux

Pour mémoire, on note en bas du tableau les restes interdits pour le module en tête de colonne. On entoure dans chaque colonne les restes interdits.
Le premier tableau étudie les nombres de l'intervalle $[3, 15]$ tandis que le deuxième étudie les nombres de l'intervalle $[1, 12]$; cela nous permet de constater que le nombre de solutions est plus élevé sur l'intervalle dont les bornes sont plus grandes :

p_k	3	5	7	11	13	
3	0	③	③	3	3	*
4	①	4	④	4	4	*
5	②	0	5	⑤	5	*
6	0	1	6	⑥	⑥	*
7	①	②	0	7	⑦	*
8	②	③	1	8	8	*
9	0	4	2	9	9	
10	①	0	③	10	10	*
11	②	1	④	0	11	*
12	0	②	5	1	12	*
13	①	③	6	2	0	*
14	②	4	0	3	1	*
15	0	0	1	4	2	
reste interdit $(\frac{p_k-1}{2})$	1	2	3	5	6	
reste interdit $(\frac{p_k+1}{2})$	2	3	4	6	7	

Les lignes concernant les nombres de l'intervalle $[3, 12]$ sont communes aux deux tableaux. Le fait qu'il y ait plus de nombres qui respectent les contraintes imposées sur l'intervalle $[13, 15]$ que sur l'intervalle $[1, 2]$ puisqu'il contient un nombre de plus garantit que l'on trouvera systématiquement des moitiés de pères de jumeaux sur nos intervalles successifs.

p_k	3	5	7	11	13	
1	①	1	1	1	1	*
2	②	②	2	2	2	*
3	0	③	③	3	3	*
4	①	4	④	4	4	*
5	②	0	5	⑤	5	*
6	0	1	6	⑥	⑥	*
7	①	②	0	7	⑦	*
8	②	③	1	8	8	*
9	0	4	2	9	9	
10	①	0	③	10	10	*
11	②	1	④	0	11	*
12	0	②	5	1	12	*
reste interdit $(\frac{p_k-1}{2})$	1	2	3	5	6	
reste interdit $(\frac{p_k+1}{2})$	2	3	4	6	7	

Annexe 2 : programmation de la recherche des moitiés de pères de jumeaux sur quelques intervalles

Les nombres suivants, compris entre 3 et 15, ne sont jamais congrus ni à $\frac{p_k-1}{2}$ ni à $\frac{p_k+1}{2}$ selon tout module p_k inférieur à 15, ce qui assure que leur double est un père de jumeaux compris entre les primorielles $6 = 2 \times 3$ et $30 = 2 \times 3 \times 5$: **9, 15**.

Les nombres suivants, compris entre 15 et 105, ne sont jamais congrus ni à $\frac{p_k-1}{2}$ ni à $\frac{p_k+1}{2}$ selon tout module p_k inférieur à 105, ce qui assure que leur double est un père de jumeaux compris entre les primorielles $30 = 2 \times 3 \times 5$ et $210 = 2 \times 3 \times 5 \times 7$: **54, 69, 75, 90, 96, 99**.

Les nombres suivants, compris entre 105 et 1155, ne sont jamais congrus ni à $\frac{p_k-1}{2}$ ni à $\frac{p_k+1}{2}$ selon tout module p_k inférieur à 1155, ce qui assure que leur double est un père de jumeaux compris entre les primorielles $210 = 2 \times 3 \times 5 \times 7$ et $2310 = 2 \times 3 \times 5 \times 7 \times 11$: **615, 639, 645, 651, 660, 714, 726, 741, 744, 804, 810, 834, 849, 861, 894, 936, 939, 966, 975, 999, 1014, 1041, 1044, 1056, 1065, 1071, 1119, 1134, 1155**.

Annexe 3 : démonstration du corollaire du lemme de Gauss : le produit de n nombres consécutifs est divisible par $n!$

Cette démonstration peut être trouvée sur le site de Gérard Villemin à l'adresse `http://villemin.gerard.free.fr/Wwwgvmm/Compter/Facttron.htm`.

Soit le produit de n nombres consécutifs commençant par un nombre quelconque $a + 1$:

$$(a + 1)(a + 2) \dots (a + n)$$

.

Multiplions le par $\frac{a!}{a!}$ en développant la factorielle au numérateur : $\frac{1.2 \dots a(a + 1)(a + 2) \dots (a + n)}{a!}$.

On reconnaît $(a + n)!$ au numérateur.

En multipliant le résultat par $\frac{n!}{n!}$, on reconnaît l'expression du coefficient du binôme ($C^n_{a+n} = \frac{(a+n)!}{a!n!}$) et l'expression devient $n!C^n_{a+n}$.

De la formule obtenue $(a + 1)(a + 2) \dots (a + n) = n!C^n_{a+n}$, on tire que $C^n_{a+n} = \frac{(a + 1)(a + 2) \dots (a + n)}{n!}$.

Les coefficients du binôme (ou éléments du triangle de Pascal) étant des nombres entiers, on en déduit que $(a + 1)(a + 2) \dots (a + n)$ est divisible par $n!$.

Le numérateur dans l'article de Gauss est "décalé" d'un rang à gauche : le premier élément de l'intervalle aux grandes bornes est a au lieu de $a + 1$.

Annexe 4 : étude de cardinaux d'ensembles de nombres congrus à certaines valeurs

Dans les tableaux suivants, on compte les nombres compris entre 1 et x qui sont congrus à 0 ($mod\ p_k$) et congrus à $2x$ ($mod\ p_k$).

mod	3	5	7	
1	①	1	1	*
2	2	2	2	
3	⓪	3	3	*
4	①	④	4	*
5	2	⓪	5	*
6	⓪	1	⑥	*
7	①	2	⓪	*
8	2	3	1	
9	⓪	④	2	*
10	①	⓪	3	*
11	2	1	4	
12	⓪	2	5	*
13	①	3	⑥	*
14	2	④	⓪	*
15	⓪	⓪	1	*
16	①	1	2	*
17	2	2	3	
34	1	4	6	

mod	3	5	7	
1	1	①	①	*
2	2	2	2	
3	⓪	3	3	*
4	1	4	4	
5	2	⓪	5	*
6	⓪	①	6	*
7	1	2	⓪	*
8	2	3	①	*
9	⓪	4	2	*
10	1	⓪	3	*
11	2	①	4	*
12	⓪	2	5	*
13	1	3	6	
14	2	4	⓪	*
15	⓪	⓪	①	*
16	1	①	2	*
17	2	2	3	
18	⓪	3	4	*
36	0	1	1	

mod	3	5	7	
1	1	1	1	
2	②	2	2	*
3	⓪	③	③	*
4	1	4	4	
5	②	⓪	5	*
6	⓪	1	6	*
7	1	2	⓪	*
8	②	③	1	*
9	⓪	4	2	*
10	1	⓪	③	*
11	②	1	4	*
12	⓪	2	5	*
13	1	③	6	*
14	②	4	⓪	*
15	⓪	⓪	1	*
16	1	1	2	
17	②	2	③	*
18	⓪	③	4	*
19	1	4	5	
38	2	3	3	

On note $x \bmod p$ le reste de la division de x par p.

De 1 à x, il y a $\left\lfloor \frac{x}{p} \right\rfloor$ nombres congrus à 0 $(mod\ p)$.

Et si $2x \not\equiv 0\ (mod\ p)$, de 1 à x,

- il y a $\left\lfloor \frac{x}{p} \right\rfloor$ nombres congrus à $2x\ (mod\ p) \Leftrightarrow x \bmod p < \frac{p-1}{2}$;
- il y a $\left\lfloor \frac{x}{p} \right\rfloor + 1$ nombres congrus à $2x\ (mod\ p) \Leftrightarrow x \bmod p > \frac{p-1}{2}$.

On rappelle que la formule de Da Silva et Sylvester pour dénombrer la quantité de nombres qui ne sont pas divisibles par les nombres $p_1, p_2, \ldots, p_k$ premiers entre eux est :

$$n - \sum_{1 \le i \le m} \left\lfloor \frac{n}{p_i} \right\rfloor + \sum_{1 \le i < j \le m} \left\lfloor \frac{n}{p_i p_j} \right\rfloor + \ldots + (-1)^m \left\lfloor \frac{n}{p_1 p_2 \ldots p_m} \right\rfloor$$

Pour compter les décomposants de Goldbach des doubles de premiers (en omettant d'ailleurs tous les décomposants éventuels qui seraient des "petits" premiers, i.e. des nombres premiers inférieurs à la racine du nombre pair considéré), on doit utiliser une formule similaire si ce n'est qu'il faut intégrer le fait que la quantité de nombres congrus à $2n\ (mod\ p_k)$ et appartenant à l'intervalle $[1, n]$ vaut $\left\lfloor \frac{n}{p_k} \right\rfloor$ si $n \bmod p_k < \frac{p_k-1}{2}$ tandis qu'elle vaut $\left\lfloor \frac{n}{p_k} \right\rfloor + 1$ si $n \bmod p_k > \frac{p_k-1}{2}$.

Plaçons-nous toujours dans le pire des cas : la formule de Da Silva et Sylvester devient alors :

$$n - \sum_{1 \le i \le m} \left(\left\lfloor \frac{n}{p_i} \right\rfloor + 1 \right) + \sum_{1 \le i < j \le m} \left(\left\lfloor \frac{n}{p_i p_j} \right\rfloor + 1 \right) + \ldots + (-1)^m \left(\left\lfloor \frac{n}{p_1 p_2 \ldots p_m} \right\rfloor + 1 \right)$$

Si l'on sort les +1 des signes $\sum$, on compte le nombre de nombres premiers, le nombre de leurs produits 2 à 2, 3 à 3, etc, et donc on ajoute et soustrait alternativement les coefficients du binôme, ce qui donne

systématiquement un résultat global de -1. Mais les nombres ont rarement tous leurs restes selon les différents modules p_k qui sont simultanément $> \frac{p_k-1}{2}$ par exemple et il devient compliqué de trouver comment agréger les différentes probabilités.