Une méthode pour déterminer les décomposants de Goldbach

Denise Vella

1er Novembre 2007

Résumé

Cette note présente une méthode de détermination de décomposants de Goldbach d'un nombre pair (i.e. nombres premiers dont ce nombre pair est la somme). Elle utilise une représentation des entiers par leurs restes selon des modules premiers. Les décomposants de Goldbach sont les nombres premiers solutions de systèmes de congruence particuliers dont le théorème des restes chinois assure l'existence.

1 Introduction

La conjecture de Goldbach (1742) énonce que tout nombre pair $2x$ supérieur ou égal à 4 est la somme de deux nombres premiers p et q. Le nombre p et le nombre q sont appelés des décomposants de Goldbach de $2x$. Cette note présente un système de représentation des entiers naturels par leurs restes modulaires selon des modules premiers. Les décomposants de Goldbach d'un entier pair $2x$ sont les entiers inférieurs ou égaux à x solutions de systèmes de congruence généralisés découlant de cette représentation.

2 Théorème des restes chinois et système de numération par n-uplets de restes

L'énoncé du théorème des restes chinois[1] (qui date du troisième siècle et a été développé par le mathématicien chinois Sun Tzu) est le suivant :

Soient k nombres entiers naturels $m_1,\ m_2,\ ...,\ m_k$
premiers entre eux deux à deux
et k entiers $r_1,\ r_2,\ ...,\ r_k$,
le système de congruence
$$\begin{cases} x \equiv r_1\ (mod\ m_1) \\ x \equiv r_2\ (mod\ m_2) \\ ... \\ x \equiv r_k\ (mod\ m_k) \end{cases}$$
admet une unique solution modulo $M = m_1 m_2 ... m_k$

Du théorème des restes chinois, il résulte que chaque entier est solution

[1] On trouve le théorème des restes chinois dans le paragraphe 36 des Recherches Arithmétiques de Gauss, reformulé dans le langage des congruences que Gauss a inventé.

d'une infinité de systèmes de congruences. Par exemple, l'entier 26 est solution du système :

$$\begin{cases} x \equiv 0 \ (mod\ 2) \\ x \equiv 2 \ (mod\ 3) \end{cases}$$

mais également du système :

$$\begin{cases} x \equiv 0 \ (mod\ 2) \\ x \equiv 2 \ (mod\ 3) \\ x \equiv 1 \ (mod\ 5) \end{cases}$$

ou encore du système :

$$\begin{cases} x \equiv 0 \ (mod\ 2) \\ x \equiv 2 \ (mod\ 3) \\ x \equiv 1 \ (mod\ 5) \\ x \equiv 5 \ (mod\ 7) \\ x \equiv 4 \ (mod\ 11) \\ x \equiv 0 \ (mod\ 13) \\ x \equiv 9 \ (mod\ 17) \\ x \equiv 7 \ (mod\ 19) \\ x \equiv 3 \ (mod\ 23) \\ x \equiv 26 \ (mod\ 29) \\ x \equiv 26 \ (mod\ 31) \\ x \equiv 26 \ (mod\ 37) \end{cases}$$

On appellera ici *n-uplet* une suite de n entiers k_i. Associé à un entier x, $k_i(x)$ sera la *i-ème coordonnée* de x dans ce n-uplet. Un *n-uplet de référence* $(2, p_2, ..., p_i, ..., p_n)$ est une suite croissante de n nombres premiers commençant par deux et telle que l'intervalle entre un nombre premier de cette suite et son successeur ne contienne aucun nombre premier. Tout entier x peut être représenté à partir d'un tel n-uplet de référence : la composante k_i du n-uplet $R(x)$ de représentation de x étant le reste de la division euclidienne de x par p_i, x possède $\Pi(x)$ représentations distinctes, où $\Pi(x)$ désigne la quantité de nombres premiers inférieurs à x.
Un tel système de numération permet ainsi de représenter un grand nombre entier par des nombres entiers plus petits : il est notamment utilisé en cryptographie.
La remarque de Claude-Paul Bruter ([3]) selon laquelle "il revient à chaque utilisateur de créer son propre ensemble de nombres selon la réalité qu'il souhaite modéliser" trouve ici son illustration.
Nous étudierons dans la suite, à titre d'exemple, le cas particulier de la décomposition de Goldbach du nombre 2308. Puisque 2308 est compris entre $2 \times 3 \times 5 \times 7 = 210$ et $2 \times 3 \times 5 \times 7 \times 11 = 2310$, le théorème chinois rappelé précédemment nous conduit à choisir $(2, 3, 5, 7)$ comme n-uplet de référence. Nous donnons ici la liste des nombres inférieurs à 210 et leur représentation dans ce n-uplet.

$1 : (1, 1, 1, 1)$	$71 : (1, 2, 1, 1)$	$141 : (1, 0, 1, 1)$
$3 : (1, 0, 3, 3)$	$73 : (1, 1, 3, 3)$	$143 : (1, 2, 3, 3)$
$5 : (1, 2, 0, 5)$	$75 : (1, 0, 0, 5)$	$145 : (1, 1, 0, 5)$
$7 : (1, 1, 2, 0)$	$77 : (1, 2, 2, 0)$	$147 : (1, 0, 2, 0)$
$9 : (1, 0, 4, 2)$	$79 : (1, 1, 4, 2)$	$149 : (1, 2, 4, 2)$
$11 : (1, 2, 1, 4)$	$81 : (1, 0, 1, 4)$	$151 : (1, 1, 1, 4)$
$13 : (1, 1, 3, 6)$	$83 : (1, 2, 3, 6)$	$153 : (1, 0, 3, 6)$
$15 : (1, 0, 0, 1)$	$85 : (1, 1, 0, 1)$	$155 : (1, 2, 0, 1)$
$17 : (1, 2, 2, 3)$	$87 : (1, 0, 2, 3)$	$157 : (1, 1, 2, 3)$
$19 : (1, 1, 4, 5)$	$89 : (1, 2, 4, 5)$	$159 : (1, 0, 4, 5)$
$21 : (1, 0, 1, 0)$	$91 : (1, 1, 1, 0)$	$161 : (1, 2, 1, 0)$
$23 : (1, 2, 3, 2)$	$93 : (1, 0, 3, 2)$	$163 : (1, 1, 3, 2)$
$25 : (1, 1, 0, 4)$	$95 : (1, 2, 0, 4)$	$165 : (1, 0, 0, 4)$
$27 : (1, 0, 2, 6)$	$97 : (1, 1, 2, 6)$	$167 : (1, 2, 2, 6)$
$29 : (1, 2, 4, 1)$	$99 : (1, 0, 4, 1)$	$169 : (1, 1, 4, 1)$
$31 : (1, 1, 1, 3)$	$101 : (1, 2, 1, 3)$	$171 : (1, 0, 1, 3)$
$33 : (1, 0, 3, 5)$	$103 : (1, 1, 3, 5)$	$173 : (1, 2, 3, 5)$
$35 : (1, 2, 0, 0)$	$105 : (1, 0, 0, 0)$	$175 : (1, 1, 0, 0)$
$37 : (1, 1, 2, 2)$	$107 : (1, 2, 2, 2)$	$177 : (1, 0, 2, 2)$
$39 : (1, 0, 4, 4)$	$109 : (1, 1, 4, 4)$	$179 : (1, 2, 4, 4)$
$41 : (1, 2, 1, 6)$	$111 : (1, 0, 1, 6)$	$181 : (1, 1, 1, 6)$
$43 : (1, 1, 3, 1)$	$113 : (1, 2, 3, 1)$	$183 : (1, 0, 3, 1)$
$45 : (1, 0, 0, 3)$	$115 : (1, 1, 0, 3)$	$185 : (1, 2, 0, 3)$
$47 : (1, 2, 2, 5)$	$117 : (1, 0, 2, 5)$	$187 : (1, 1, 2, 5)$
$49 : (1, 1, 4, 0)$	$119 : (1, 2, 4, 0)$	$189 : (1, 0, 4, 0)$
$51 : (1, 0, 1, 2)$	$121 : (1, 1, 1, 2)$	$191 : (1, 2, 1, 2)$
$53 : (1, 2, 3, 4)$	$123 : (1, 0, 3, 4)$	$193 : (1, 1, 3, 4)$
$55 : (1, 1, 0, 6)$	$125 : (1, 2, 0, 6)$	$195 : (1, 0, 0, 6)$
$57 : (1, 0, 2, 1)$	$127 : (1, 1, 2, 1)$	$197 : (1, 2, 2, 1)$
$59 : (1, 2, 4, 3)$	$129 : (1, 0, 4, 3)$	$199 : (1, 1, 4, 3)$
$61 : (1, 1, 1, 5)$	$131 : (1, 2, 1, 5)$	$201 : (1, 0, 1, 5)$
$63 : (1, 0, 3, 0)$	$133 : (1, 1, 3, 0)$	$203 : (1, 2, 3, 0)$
$65 : (1, 2, 0, 2)$	$135 : (1, 0, 0, 2)$	$205 : (1, 1, 0, 2)$
$67 : (1, 1, 2, 4)$	$137 : (1, 2, 2, 4)$	$207 : (1, 0, 2, 4)$
$69 : (1, 0, 4, 6)$	$139 : (1, 1, 4, 6)$	$209 : (1, 2, 4, 6)$

$210 : (0, 0, 0, 0)$
$211 : (1, 1, 1, 1)$
...

3 Les décomposants de Goldbach sont non congrus à $2x$ selon tout module

On peut formuler ainsi la conjecture de Goldbach : "tout nombre inférieur à x et dont les restes de divisions euclidiennes par les nombres premiers inférieurs à x sont différents un à un des restes de $2x$ par ces mêmes divisions a son complémentaire à $2x$ qui est premier". En d'autres termes :

$\forall\ 2x$
$\forall\ p_1$ *premier impair inférieur ou égal à* x
$\forall\ q$ *premier impair inférieur ou égal à* x,
$2x \not\equiv p_1\ (mod\ q) \iff p_2 = 2x - p_1$ *premier impair supérieur ou égal à* x
(p_1 *et* p_2 *sont des décomposants de Goldbach de* $2x$).

En effet,

$$\begin{array}{ll} & 2x \not\equiv p_1 \ (mod\ q) \\ \iff & 2x - p_1 \not\equiv 0 \ (mod\ q) \\ \iff & 2x - p_1 \ est\ un\ nombre\ premier \\ & \quad car\ il\ n'est\ divisible\ par\ aucun\ autre\ nombre\ premier\ q \end{array}$$

Les décomposants de Goldbach d'un nombre pair $2x$, devant être premiers, sont a fortiori premiers à $2x$ (i.e. de plus grand diviseur commun à $2x$ égal à 1).
On notera qu'un nombre premier inférieur à x étant donné, son complémentaire à $2x$ n'est pas obligatoirement un nombre premier. D'autre part, un nombre inférieur à x et non congru à $2x$ selon tout module n'est pas nécessairement premier.
L'énoncé présenté ci-dessus est vrai. Cependant, il pourrait être vrai par vacuité, c'est à dire vrai alors qu'il n'existerait aucun p_1 le vérifiant. Démontrer la conjecture de Goldbach consisterait à démontrer que cet énoncé ne peut jamais être vrai par vacuité[2].

4 Remarques préliminaires au traitement de cas

Définissons d'abord la relation binaire *Congru_à* [3] entre deux n-uplets dans un même n-uplet de référence de la façon suivante :

$$(x_1, x_2, ..., x_n)\ Congru\_à\ (y_1, y_2, ...y_n)\ dans\ (p_1, p_2, ..., p_n)$$
$$\iff$$
$$\begin{cases} x_1 \equiv y_1 \ (mod\ p_1) \vee \\ x_2 \equiv y_2 \ (mod\ p_2) \vee \\ ... \vee \\ x_n \equiv y_n \ (mod\ p_n) \end{cases}$$

Cette relation est réflexive, symétrique mais elle n'est pas transitive. La relation "inverse" de cette relation, que l'on pourrait appeler *Non_congru_à*[4], est quant à elle non réflexive, symétrique et non transitive.

Définissons également une relation unaire *Contient_un_zéro* qui à un n-uplet $(x_1, x_2, ..., x_n)$ dans un n-uplet de référence $(p_1, p_2, ..., p_n)$ associe le booléen vrai si et seulement si l'une des coordonnées du n-uplet est nulle.

$$Contient\_un\_zéro((x_1, x_2, ..., x_n))\ est\ vrai$$
$$\iff$$
$$x_1 \equiv 0 \ (mod\ p_1) \vee x_2 \equiv 0 \ (mod\ p_2) \vee ... \vee x_n \equiv 0 \ (mod\ p_n)$$

Nous allons nous intéresser ici à des triplets de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, que nous noterons sans parenthèses ni virgules pour en alléger l'écriture. Trouvons d'abord pour chaque triplet quels sont les triplets qui lui sont

[2] Le corollaire de ce qui vient d'être présenté est que les facteurs premiers de $2x - p$ sont les nombres premiers du n-uplet de référence dans lequel est représenté p selon lesquels p et $2x$ sont congrus.
[3] i.e. sous-entendu *Congru à* selon un module
[4] i.e. sous-entendu *Non_congru_à* selon tout module

non congrus selon toutes les coordonnées.
Sont non congrus à 000 les triplets 111, 112, 121, 113, 122, 114, 123, 124.
Sont non congrus à 001 les triplets 120, 112, 113, 122, 114, 123, 110, 124.
Sont non congrus à 002 les triplets 111, 120, 121, 113, 114, 123, 110, 124.
Sont non congrus à 003 les triplets 111, 120, 112, 121, 122, 114, 110, 124.
Sont non congrus à 004 les triplets 111, 120, 112, 121, 113, 122, 123, 110.
Sont non congrus à 010 les triplets 103, 104, 121, 122, 101, 123, 102, 124.
Sont non congrus à 011 les triplets 103, 120, 104, 100, 122, 123, 102, 124.
Sont non congrus à 012 les triplets 103, 120, 104, 121, 100, 101, 123, 124.
Sont non congrus à 013 les triplets 120, 104, 121, 100, 122, 101, 102, 124.
Sont non congrus à 014 les triplets 103, 121, 100, 122, 101, 102, 123, 120.
Sont non congrus à 020 les triplets 111, 103, 112, 104, 113, 114, 101, 102.
Sont non congrus à 021 les triplets 103, 112, 104, 113, 100, 114, 110, 102.
Sont non congrus à 022 les triplets 111, 103, 104, 113, 100, 114, 101, 110.
Sont non congrus à 023 les triplets 111, 112, 104, 100, 114, 101, 110, 102.
Sont non congrus à 024 les triplets 111, 103, 112, 113, 100, 101, 110, 102.
On voit qu'à chaque triplet correspondent 8 triplets qui lui sont non congrus selon toutes les coordonnées. En effet, la fonction $\varphi(x)$, appelée fonction indicatrice d'Euler, qui compte les nombres inférieurs à x et premiers à x, prend la valeur 8 pour $30 = 2 \times 3 \times 5$ ($\varphi(30) = 8$).
Cherchons d'autre part quels sont les triplets qui n'ont aucune coordonnée nulle. Ce sont les triplets 111, 112, 113, 114, 121, 122, 123 et 124. Eux aussi sont au nombre de 8.

Effectuons encore quelques comptages : considérons l'ensemble des nombres premiers à 98. Ils sont au nombre de 42 ($\varphi(98) = 42$). Ils vont par deux car si p appartient à cet ensemble, $2x - p$ appartient aussi à cet ensemble.
98 a pour représentation $(0, 2, 3)$ selon $(2, 3, 5)$. Fournissons dans un tableau en première colonne la valeur entière de chacun des nombres en question (c'est à dire les nombres inférieurs à 98 et premiers à 98) ; en deuxième colonne, fournissons leur représentation dans $(2, 3, 5)$. En troisième colonne, on note le fait que la représentation en question vérifie une propriété que l'on appellera $c1$ qui consiste à être congru à la représentation de 98 selon une coordonnée, et en quatrième colonne, on note le fait qu'elle vérifie une propriété que l'on appellera $c2$, c'est à dire qu'elle ne contient aucune coordonnée nulle. On dira qu'un nombre a la propriété c dans un n-uplet de référence R si sa représentation vérifie les deux propriétés $c1$ et $c2$.

1	$(1,1,1)$	$\times$	$\circ$	97	$(1,1,2)$	$\times$	$\circ$
3	$(1,0,3)$			95	$(1,2,0)$		
5	$(1,2,0)$			93	$(1,0,3)$		
9	$(1,0,4)$	$\times$		89	$(1,2,4)$		$\circ$
11	$(1,2,1)$		$\circ$	87	$(1,0,2)$	$\times$	
13	$(1,1,3)$		$\circ$	85	$(1,1,0)$	$\times$	
15	$(1,0,0)$	$\times$		83	$(1,2,3)$		$\circ$
17	$(1,2,2)$		$\circ$	81	$(1,0,1)$	$\times$	
19	$(1,1,4)$	$\times$	$\circ$	79	$(1,1,4)$	$\times$	$\circ$
23	$(1,2,3)$		$\circ$	75	$(1,0,0)$	$\times$	
25	$(1,1,0)$	$\times$		73	$(1,1,3)$		$\circ$
27	$(1,0,2)$	$\times$		71	$(1,2,1)$		$\circ$
29	$(1,2,4)$		$\circ$	69	$(1,0,4)$	$\times$	
31	$(1,1,1)$	$\times$	$\circ$	67	$(1,1,2)$	$\times$	$\circ$
33	$(1,0,3)$			65	$(1,2,0)$		
37	$(1,1,2)$	$\times$	$\circ$	61	$(1,1,1)$	$\times$	$\circ$
39	$(1,0,4)$	$\times$		59	$(1,2,4)$		$\circ$
41	$(1,2,1)$		$\circ$	57	$(1,0,2)$	$\times$	
43	$(1,1,3)$		$\circ$	55	$(1,1,0)$	$\times$	
45	$(1,0,0)$	$\times$		53	$(1,2,3)$		$\circ$
47	$(1,2,2)$		$\circ$	51	$(1,0,1)$	$\times$	

On constate que les troisième et quatrième colonnes sont symétriques l'une de l'autre autour du nombre 49 (moitié de 98) en ce sens que si p est non congru à $2x$ selon toute coordonnée, alors la représentation de $2x-p$ ne contient aucun zéro. Les nombres p vérifiant la propriété $c(p)$ sont les décomposants de Goldbach de 98. Trouver ce qui garantit l'existence d'un nombre dont la troisième et la quatrième colonne sont marquées consiste à prouver la conjecture de Goldbach.

5 Traitement de cas

Au paragraphe précédent, on a traité le cas du nombre pair 98 en considérant les nombres premiers à 98. Traitons maintenant ce cas en ne considérant que l'espace des représentations par les n-uplets. 98 a pour racine carrée 9.89... Il est compris entre $2\times3\times5$ et $2\times3\times5\times7$. On rappelle que sa représentation est le triplet $(0,2,3)$ selon le triplet de référence $(2,3,5)$. Considérons les nombres p qui vérifient la propriété $c(p)$.
Puisque 98 a pour coordonnée 2 (mod 3), on ne va conserver que les nombres ayant pour coordonnée 1 (mod 3). Puisque 98 a pour coordonnée 3 (mod 5), on ne va conserver que les nombres ayant pour coordonnée 1, 2 *ou* 4 (mod 5). On a omis de dire que trivialement les solutions doivent être impaires (première coordonnée (mod 2) égale à 1).
Ces nombres sont solutions du système de congruence généralisé par disjonction suivant :

$$\begin{cases} p \equiv 1\ (mod\ 2) \\ p \equiv 1\ (mod\ 3) \\ p \equiv 1 \vee 2 \vee 4\ (mod\ 5) \end{cases}$$

Ils ont pour représentation selon le triplet de référence $(2,3,5)$ les triplets $(1,1,1)$, $(1,1,2)$ et $(1,1,4)$.
Le premier système de la disjonction correspondant au triplet $(1,1,1)$ a pour solutions les nombres : 31, 61, ... en vertu du théorème des restes chinois.

Le deuxième système de la disjonction correspondant au triplet $(1, 1, 2)$ a pour solutions les nombres : 7, 37, 67... en vertu du théorème des restes chinois.
Le troisième système de la disjonction correspondant au triplet $(1, 1, 4)$ a pour solutions les nombres : 19, 49, 79, ... en vertu du théorème des restes chinois.
Il s'agit maintenant d"'étendre" les solutions trouvées en vérifiant qu'elles restent solutions lorsqu'on ajoute la condition de non congruence à 0 (mod 7). 7 étant congru à 0 (mod 7) et 98 l'étant également, 7 n'est donc pas un décomposant de Goldbach de 98. 19, 31 et 37 ne sont pas éliminés par l'extension au module 7 et sont donc décomposants de Goldbach de 98.

Supposons qu'au lieu de devoir examiner le triplet de représentation associé à 98, on ait eu à examiner un triplet quelconque. Il est possible de calculer le nombre de triplets qui vérifient la propriété c.
Dans le cas où le triplet serait 010, ne subsisteraient que 121, 122, 123 et 124. Pour le triplet 023, ne subsisteraient que 111, 112 et 113. On voit que le nombre de triplets appartenant à l'intersection des deux ensembles a un cardinal fonction du triplet en question. Si une coordonnée du triplet est nulle, il subsiste $p_i - 1$ possibilités pour cette coordonnée dans les triplets que l'on recherche (p_i étant le nombre premier du triplet de référence selon lequel est calculée la coordonnée) tandis que si cette coordonnée est non nulle, il subsiste $p_i - 2$ possibilités (p_i premier impair) pour cette coordonnée dans les triplets que l'on recherche[5].

Un problème persiste, dû au fait que les comptages présentés ci-dessus ne peuvent s'effectuer précisément que lorsque l'on se place sur un ensemble de nombres "complet", par exemple sur l'ensemble des nombres de 0 à 210 ($= 2 \times 3 \times 5$), ou bien ceux de 0 à 30030 ($= 2 \times 3 \times 5 \times 7 \times 11 \times 13$). Dans des ensembles de nombres "incomplets", on ne pourra effectuer ces comptages précisément.
Par analogie avec le terme factorielle, appelons *primorielle* n le produit des n nombres d'un n-uplet de référence. Le nombre pair $2x$ étant donné, la primorielle $n(x)$ est choisie de sorte que $n(x) < 2x < (n+1)(x)$. $2x$ admet une représentation $R(2x)$ dans le n-uplet de référence ainsi défini.

On va associer à $R(2x)$ l'ensemble des n-uplets vérifiant la propriété c. En effet, d'une part, le fait d'être non congru à $R(2x)$ selon toute coordonnée est une nécessité pour les décomposants de Goldbach de $2x$ (le complémentaire à $2x$ d'un nombre qui serait congru à $2x$ selon une coordonnée serait nécessairement composé). Le fait de n'avoir aucune coordonnée nulle garantit que l'on ne récupèrera pas des nombres composés ayant pour facteurs les nombres premiers du n-uplet de référence.
Un problème peut persister lorsque le plus grand nombre premier de $n(x)$ est inférieur au plus grand nombre premier inférieur à $\sqrt{2x}$. On verra sur des exemples qu'il faut s'assurer qu'il subsiste toujours un nombre premier qui va "conserver sa propriété c" en étendant ainsi l'ensemble des modules à considérer. C'est ce que fait la deuxième étape de l'algorithme, qui étend les représentations selon un n-uplet de référence contenant tous les nombres premiers inférieurs à la racine de $2x$.

[5]De ce fait, on peut vérifier que le nombre de décomposants de Goldbach des nombres pairs qui ont un nombre de facteurs premiers élevé (comme les multiples de 30, ou de 210 ou de 2310,...) subit des pics d'augmentation ponctuels.

Résumons l'algorithme :
Première étape : trouver les nombres compris entre 3 et $2x$ qui :
a) sont non congrus à $2x$ selon toute coordonnée dans le n-uplet de référence $(2, 3, ..., n(x))$;
b) ont une représentation ne contenant aucune coordonnée nulle.

Deuxième étape : extension éventuelle (au cas où $n(x) < \sqrt{2x}$)
Ne conserver de l'ensemble de nombres obtenus par la première étape que ceux qui "conservent leur propriété c" dans le n-uplet de référence $((n+1)(x), ..., plus\ grand\ nombre\ premier\ inférieur\ à \sqrt{2x})$.

Remarque : on aura noté que l'étape $I.a$ permet d'obtenir trois sortes de nombres :

- les nombres dont la représentation est un n-uplet vérifiant la propriété c, seuls nombres dont on va tester la représentation dans la deuxième étape ;
- les nombres dont la représentation contient un seul zéro et qui sont de deux sortes, soit de petits nombres premiers (qui peuvent d'ailleurs fournir des décompositions de Goldbach de $2x$), soit des puissances de ces petits nombres premiers qui sont donc des nombres composés et ne peuvent par conséquent fournir de décompositions de Goldbach de $2x$;
- les nombres composés dont la représentation contient au moins deux zéros (i.e. qui ont au moins deux facteurs premiers).

Soit $pair$ un nombre pair qui a pour représentation $(0, pair_2, pair_3, ...)$. Trouver les décomposants de Goldbach de $pair$ consiste à trouver les n-uplets $(1, x_2, x_3..., x_{n-1}, x_n)$ égaux à $(1, 1, 1, ..., 1, 1) + k(1, 1, 1, ..., 1, 1)$ et appartenant au produit cartésien $\mathbb{Z}/2\mathbb{Z} - \{0\} \times \mathbb{Z}/3\mathbb{Z} - \{0, pair_2\} \times \mathbb{Z}/5\mathbb{Z} - \{0, pair_3\} \times .....$ (c'est à dire le produit cartésien des corps premiers duquel on a enlevé les n-uplets vérifiant la propriété c.

Quelles sont les données numériques qui pourraient nous conforter dans l'idée qu'on n'a pas à craindre la non congruence aux nombres premiers plus grands quand on a la non congruence aux nombres premiers plus petits ?
On a vu qu'étant donné un nombre pair $2x$, il y a au minimum

$$\prod_{p_i\ premier\ impair} (p_i - 2)$$

n-uplets vérifiant la propriété c (où p_i est le plus grand nombre premier de la plus grande primorielle inférieure à $2x$).
Ce produit prendra les valeurs successives 1, $3 = 1 \times 3$, $15 = 1 \times 3 \times 5$, $135 = 1 \times 3 \times 5 \times 9$, etc... Ces nombres pourront être "éliminés" par des nombres premiers plus grands. Cependant, le nombre de nombres premiers plus grands qui pourraient éliminer des solutions croît bien plus lentement que le nombre de solutions potentielles [6].

Etudions un deuxième cas qui illustrera davantage le souci posé par ce que l'on pourrait appeler l' "extension" des solutions aux nombres

[6] la première quantité croît comme le produit des $p_i - 2$ (p_i premier impair) alors que la seconde croît comme le nombre de nombres premiers compris entre les nombres premiers successifs et les racines des primorielles successives : elle vaudra 11 quand la première vaudra 15 puis vaudra 35 quand la première vaudra 135, puis vaudra 121 quand la première vaudra 1485, etc.

premiers plus grands. Le nombre pair à étudier est 2308 (de racine 48.04) : il est compris entre $2\times3\times5\times7$ et $2\times3\times5\times7\times11$; sa représentation selon le quadruplet de référence $(2,3,5,7)$ est $(0,1,3,5)$. Les quadruplets (que l'on écrit à nouveau sans parenthèse ni virgule) qui vérifient la propriété c sont

1214, 1223, 1241, 1216, 1243, 1211, 1213, 1222, 1224, 1212, 1221, 1246, 1242, 1226, 1244.

Ils sont bien au nombre de 15, produit des $p_i - 2$ (p_i premier impair).

Fournissons une table de congruence qui va nous permettre de voir s'ils conservent la propriété c, selon les modules de 11 à 47, 47 étant le plus grand nombre premier inférieur à la racine carrée de 2308.

	11	13	17	19	23	29	31	37	41	43	47
$71=(1,2,1,1)$	5	6	3	14	2	13	11	34	30	28	24
$191=(1,2,1,2)$	4	9	4	1	7	17	5	6	27	19	3
$101=(1,2,1,3)$	2	10	16	6	9	14	8	27	19	15	7
$11=(1,2,1,4)$	0	11	11	11	11	11	11	11	11	11	11
$41=(1,2,1,6)$	8	2	7	3	18	12	10	4	0	41	41
$197=(1,2,2,1)$	10	2	10	7	13	23	11	12	33	25	9
$107=(1,2,2,2)$	8	3	5	12	15	20	14	33	25	21	13
$17=(1,2,2,3)$	6	4	0	17	17	17	17	17	17	17	17
$137=(1,2,2,4)$	5	7	1	4	22	21	13	26	14	8	43
$167=(1,2,2,6)$	2	11	14	15	6	22	12	19	3	38	26
$29=(1,2,4,1)$	7	3	12	10	6	0	29	29	29	29	29
$149=(1,2,4,2)$	6	6	13	16	11	4	25	1	26	20	8
$59=(1,2,4,3)$	4	7	8	2	13	1	28	22	18	16	12
$179=(1,2,4,4)$	3	10	9	8	18	5	24	31	15	7	38
$209=(1,2,4,6)$	0	1	5	0	2	6	23	24	4	37	21
$2308=(0,1,3,5)$	9	7	13	9	8	17	14	14	12	29	5

Tous les nombres premiers n'ayant pas été éliminés par cette table, certains, comme 11, 41, 71, 101, 167, 197, 179 permettent d'obtenir des décompositions de Goldbach de 2308.

Le théorème des restes chinois garantit l'existence de solutions mais il ne garantit pas, d'une part que ces solutions sont inférieures à une borne fixée, en l'occurrence ici, il s'agit pour nous d'être assuré que les solutions des systèmes de congruence sont inférieures à x quand on cherche les décomposants de Goldbach de $2x$. Le théorème ne garantit rien non plus quant à la primarité des solutions d'un système de congruence. On voit bien par contre ci-dessus que ces solutions des systèmes de congruences sont éléments de suites arithmétiques (i.e. $31+30k$, $7+30k'$, $19+30k''$ sont les suites arithmétiques correspondant au traitement du nombre pair 98 au paragraphe précédent). Le théorème de Dirichlet et le théorème de Linnik assurent de trouver des nombres premiers dans de telles suites arithmétiques inférieurs à certaine limite mais le problème de la borne supérieure est le bât qui blesse pour l'instant car la limite fournie par le théorème de Linnik est bien trop élevée pour garantir ce qui nous intéresse. On trouve dans [4] des éléments au sujet de deux théorèmes issus de la théorie analytique des nombres qui pourraient peut-être être utilisés ici : le théorème de Siegel-Walfisz et le théorème de Brun-Titchmarsh qui fournissent des renseignements sur la fonction de comptage des nombres

premiers p inférieurs ou égaux à un nombre donné x et congrus à un certain nombre modulo un certain autre (i.e. tels que $p \equiv a\ (mod\ q)$).

6 Descente infinie de Fermat

En matière de démonstrations "simples", on peut suivre la recommandation de Poincaré qui qualifiait la démonstration par récurrence de démonstration par excellence. Mais le mode de raisonnement par récurrence nécessite de prouver $P(n) \Rightarrow P(Succ(n))$[7]. Or les représentations choisies ici sont telles que $R(x+1)$ diffère par toutes ses coordonnées de $R(x)$. Puisqu'on a vu que les décomposants de Goldbach de $2x$ sont les nombres premiers p inférieurs ou égaux à x tels que $non[R(p)\ Congru\_à\ R(2x)]$, on imagine davantage relier entre elles les décompositions de Goldbach de nombres dont les représentations partagent des coordonnées plutôt que relier entre elles les décompositions de nombres dont les représentations ne partagent aucune coordonnée. Le raisonnement appelé "descente infinie de Fermat" permettrait-il d'atteindre la conjecture de Goldbach ?

Ce mode de raisonnement repose sur le fait qu'il n'existe pas de suite infinie strictement décroissante d'entiers positifs. L'ensemble $\mathbb{N}$ des entiers naturels et toutes ses parties propres non vides possèdent une propriété remarquable : ils admettent un plus petit élément.
Imaginons que nous voulions démontrer qu'une certaine propriété $P(n)$ est impossible (n est un entier naturel). On raisonne par l'absurde en supposant $P(n)$ vraie pour un certain entier n (la partie E de $\mathbb{N}$ où $P(n)$ est vraie est donc non vide). Si nous sommes capables de montrer que P est alors vraie pour un entier strictement inférieur à n, nous aboutirons à une contradiction. En effet, si a désigne le plus petit élément de E, on a simultanément $P(a)$ vraie et $P(b)$ vraie avec $b < a$. L'entier b appartient donc à E et est strictement plus petit que le plus petit élément de E. D'où la contradiction.

On a vu précédemment qu'un décomposant de Goldbach d'un nombre pair $2x$ est un nombre premier inférieur à x qui ne partage avec $2x$ aucune classe de congruence[8]. S'il existait un nombre pair $2ng$ contredisant la conjecture de Goldbach, ce nombre pair "partagerait" chacune de ses classes d'équivalence selon des modules premiers inférieurs à sa racine avec des nombres premiers inférieurs à sa moitié (i.e. chaque élément du n-uplet représentant $2x$ serait commun avec l'élément correspondant du n-uplet de représentation d'un nombre premier inférieur à x). Mais alors, en prenant un nombre plus petit que $2ng$ et qui partage de nombreuses coordonnées avec $2ng$ (par exemple un nombre dont la représentation est un préfixe propre de la représentation de $2ng$), on construirait un nombre plus petit que $2ng$ et qui contredirait également la conjecture de Goldbach car lui aussi, par "inclusion" en quelque sorte, "partagerait" chacune de

[7] où Succ est défini par l'axiomatique de Peano.
[8] Cf en annexe 1 l'exemple du nombre pair 43532 très explicite à ce sujet.

ses classes d'équivalence selon des modules inférieurs à sa racine.

$$
\begin{array}{ll}
 & \exists\, 2x \,/\, 2x \textit{ ne vérifie pas la conjecture de Goldbach} \\
\Longleftrightarrow & \forall\, p \textit{ premier impair inférieur ou égal à } \sqrt{2x} \\
 & \exists\, q \textit{ premier impair inférieur ou égal à } x, \\
 & \quad R(2x) \textit{ Congru\_à } R(p) \textit{ dans } n(x) \\
\Rightarrow & \exists\, 2y < 2x \,/\, R(2y) \textit{ préfixe propre de } R(2x) \textit{ et} \\
 & \forall\, p \textit{ premier impair inférieur ou égal à } \sqrt{2x} \\
 & \quad (\textit{et donc inférieur ou égal à } \sqrt{2y}) \\
 & \exists\, q \textit{ premier impair inférieur ou égal à } x, \\
 & \quad R(2y) \textit{ Congru\_à } R(p) \textit{ dans } n(x) \\
\Rightarrow & \exists\, 2y < 2x \,/\, 2y \textit{ ne vérifie pas la conjecture de Goldbach.}
\end{array}
$$

Or, cela est impossible. Donc, la conjecture de Goldbach doit être vraie.

7 Conclusion

La conjecture de Goldbach fait partie, avec l'hypothèse de Riemann et la conjecture des nombres premiers jumeaux, du huitième problème de la liste des 23 problèmes de Hilbert. La méthode présentée ici nous fait voir les décomposants de Goldbach d'un nombre pair sous un jour nouveau, comme solutions de systèmes de congruence particuliers. Le théorème des restes chinois ne nous permet cependant pas d'assurer qu'il existe des nombres premiers parmi de telles solutions.

Je remercie le professeur Claude-Paul Bruter, qui m'a encouragée et orientée tout au long de ce travail.

Bibliographie

(1) C.F. Gauss, *Recherches arithmétiques*, Ed. Jacques Gabay, 1801.
(2) C.P. Bruter, *La construction des nombres*, Ed. Ellipses, 2000.
(3) C.P. Bruter, *Du nouveau du côté des nombres*, Quadrature, n°66, Octobre-Décembre 2007, p-8-14.
(4) O. Bordellès, *Thèmes d'arithmétique*, Ed. Ellipses, 2006. (5) P.J. Davis, R.Hersh, *l'Univers mathématique*, Ed. Gauthier-Villars, 1985
(6) N. Charraud, *Infini et Inconscient, essai sur Georg Cantor*, Ed. Anthropos, 1994.
(7) D. Guedj, *Villa des hommes*, Ed. Robert Laffont, 2007
(8) D. Nordon, M.Mendès-France (illustrations), *Les mathématiques pures n'existent pas !*, Ed. Actes Sud, 1985.
(9) D. Nordon, *Les obstinations d'un mathématicien*, Ed. Belin Pour La Science, 2003.
(10) A. Doxiadis, *Oncle Pétros et la conjecture de Goldbach*, Ed. Points, 2002.
(11) L. Euler, *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs*, Commentatio 175 indicis Enestroemiani, Bibliothèque impartiale 3, 1751, p.10-31.
(12) P. Damphousse, *Découvrir l'arithmétique*, Ed. Ellipses, 2000.
(13) A. Astruc, *Evariste Galois*, Ed. Grandes biographies, 1999.
(14) M. Du Sautoy, *La symphonie des nombres premiers*, Ed. Eloïse d'Ormesson, 2005.
(15) J.P. Belna, *Cantor*, Ed. Les belles lettres, 2000.
(16) P. Hoffman, *Erdös, l'homme qui n'aimait que les nombres*, Ed. Belin,

2000.
(17) J. Hadamard, *Essai sur la psychologie de l'invention dans le domaine mathématique*, suivi de H. Poincaré, *L'invention mathématique*, Ed. Jacques Gabay, 2000.
(18) J.J.Gray, *Le défi de Hilbert*, Ed. Dunod, 2003.
(19) Collectif, Ebbinghaus et autres auteurs, *Les Nombres*, Ed. Vuibert, 1999.
(20) C. Laisant, *Sur un procédé expérimental de vérification de la conjecture de Goldbach*, Bulletin de la SMF n°25 de 1897.
(21) G. Tenenbaum, M. Mendès-France, *Les nombres premiers*, Collection Que sais-je ?, PUF, 2000

Annexe 1 : Etude d'un cas : le nombre pair 43532 de premier décomposant de Goldbach égal à 211

Etudions le cas du nombre pair 43532 de racine 208 et quelques en calculant ses restes selon les nombres premiers inférieurs ou égaux à 199, le plus grand nombre premier inférieur à sa racine.

$43532 \equiv 2 \ (mod\ 3)$
$43532 \equiv 2 \ (mod\ 5)$
$43532 \equiv 6 \ (mod\ 7)$
$43532 \equiv 5 \ (mod\ 11)$
$43532 \equiv 8 \ (mod\ 13)$
$43532 \equiv 12 \ (mod\ 17)$
$43532 \equiv 3 \ (mod\ 19)$
$43532 \equiv 16 \ (mod\ 23)$
$43532 \equiv 3 \ (mod\ 29)$
$43532 \equiv 8 \ (mod\ 31)$
$43532 \equiv 20 \ (mod\ 37)$
$43532 \equiv 31 \ (mod\ 41)$
$43532 \equiv 16 \ (mod\ 43)$
$43532 \equiv 10 \ (mod\ 47)$
$43532 \equiv 19 \ (mod\ 53)$
$43532 \equiv 49 \ (mod\ 59)$
$43532 \equiv 39 \ (mod\ 61)$
$43532 \equiv 49 \ (mod\ 67)$
$43532 \equiv 9 \ (mod\ 71)$
$43532 \equiv 24 \ (mod\ 73)$
$43532 \equiv 3 \ (mod\ 79)$
$43532 \equiv 40 \ (mod\ 83)$
$43532 \equiv 11 \ (mod\ 89)$
$43532 \equiv 76 \ (mod\ 97)$
$43532 \equiv 1 \ (mod\ 101)$
$43532 \equiv 66 \ (mod\ 103)$
$43532 \equiv 90 \ (mod\ 107)$
$43532 \equiv 41 \ (mod\ 109)$
$43532 \equiv 27 \ (mod\ 113)$
$43532 \equiv 98 \ (mod\ 127)$
$43532 \equiv 40 \ (mod\ 131)$
$43532 \equiv 103 \ (mod\ 137)$
$43532 \equiv 25 \ (mod\ 139)$
$43532 \equiv 24 \ (mod\ 149)$
$43532 \equiv 44 \ (mod\ 151)$
$43532 \equiv 43 \ (mod\ 157)$
$43532 \equiv 11 \ (mod\ 163)$
$43532 \equiv 112 \ (mod\ 167)$
$43532 \equiv 109 \ (mod\ 173)$
$43532 \equiv 35 \ (mod\ 179)$
$43532 \equiv 92 \ (mod\ 181)$
$43532 \equiv 175 \ (mod\ 191)$
$43532 \equiv 107 \ (mod\ 193)$
$43532 \equiv 192 \ (mod\ 197)$
$43532 \equiv 150 \ (mod\ 199)$

Les décomposants de Goldbach de 43532 sont donc les nombres x premiers et inférieurs à 21766 solutions du système de congruence suivant :

$$\begin{cases} x \equiv r_1 \ (mod\ 2) \\ x \equiv r_2 \ (mod\ 3) \\ x \equiv r_3 \ (mod\ 5) \\ x \equiv r_4 \ (mod\ 7) \\ x \equiv r_5 \ (mod\ 11) \\ ... \\ x \equiv r_4 6 \ (mod\ 199) \end{cases} \quad avec \begin{cases} r_1 \in \mathbb{Z}/2\mathbb{Z} - \{0\} \\ r_2 \in \mathbb{Z}/3\mathbb{Z} - \{0,2\} \\ r_3 \in \mathbb{Z}/5\mathbb{Z} - \{0,2\} \\ r_4 \in \mathbb{Z}/7\mathbb{Z} - \{0,6\} \\ r_5 \in \mathbb{Z}/11\mathbb{Z} - \{0,5\} \\ ... \\ r_4 6 \in \mathbb{Z}/199\mathbb{Z} - \{0,150\} \end{cases}$$

La congruence à 2 (mod 3) élimine les nombres premiers $5, 11, 17, 23, 29, 47, 53, 59, 71, 83, 89, 101, 131, 137, 149, 167, 173, 179, 191$ et 197.
La congruence à 2 (mod 5) élimine les nombres premiers $7, 37, 67, 97, 127$ et 157.
La congruence à 6 (mod 7) élimine les nombres premiers $13, 139$ et 181.
La congruence à 8 (mod 13) élimine les nombres premiers $73, 151$ et 193.
La congruence à 12 (mod 17) élimine le nombre premier 199.
La congruence à 3 (mod 19) élimine les nombres premiers 3 et 79.
La congruence à 3 (mod 29) élimine le nombre premier 61.
La congruence à 8 (mod 31) élimine le nombre premier 163.
La congruence à 31 (mod 41) élimine les nombres premiers 31 et 113.
La congruence à 19 (mod 53) élimine le nombre premier 19.
La congruence à 103 (mod 137) élimine le nombre premier 103.
La congruence à 43 (mod 157) élimine le nombre premier 43.
La congruence à 109 (mod 173) élimine le nombre premier 109.

Le nombre premier le plus petit à ne pas être éliminé par toutes ces congruences est donc 211 dont la représentation par un n-uplet de 46 coordonnées est $(1, 1, 1, 1, 2, 3, 7, 2, 4, 8, 25, 26, 6, 39, 23{,}52, 34, 28, 10, 69, 65, 53, 45, 33, 17, 9, 5, 104, 102, 98, 84, 80, 74, 72, 62, 60, 54, 48, 44, 38, 32, 30, 20, 18, 14, 12)$.

La méthode présentée ici tire parti des représentations modulaires des entiers pour estimer plus rapidement si un nombre peut être décomposant de Goldbach d'un nombre pair, sans avoir à tester "précisément" sa primarité. Elle est en ceci avantageuse par rapport à une procédure qui, cherchant les décomposants de Goldbach de $2x$, consisterait à calculer pour chaque premier p inférieur à x si $2x - p$ est premier.