Réécrire

Denise Vella-Chemla (7.12.2019) aidée par Leila Schneps pour la section 1

1. Caractérisation des décomposants de Goldbach d'un nombre pair

Soit n un nombre pair supérieur à 4 et p_k un nombre premier compris entre 3 et $\sqrt{n}$.

Notons $F(p_k, n) = \{m \in \mathbb{N} : m \text{ impair}, \sqrt{n} \leq m \leq n/2, m \neq 0\ [p_k], m \neq n\ [p_k]\}$

Appelons $D(n) = \cap F(p_k, n)$ l'intersection des ensembles $F(p_k, n)$ pour tous les premiers p_k compris entre 3 et $\sqrt{n}$.

Démontrons que $D(n)$ ne contient que des nombres premiers.

Lemme 1 : Soit m un entier positif impair. Si m n'est divisible par aucun nombre premier compris entre 3 et $\sqrt{m}$, alors m est premier.

Démonstration : Supposons que m ne soit pas premier. Alors il existe un nombre premier $p < m$ qui divise m. Mais on sait que p n'est pas compris entre 3 et $\sqrt{m}$, donc $p > \sqrt{m}$. On pose $k = m/p$. On a donc $kp = m$. Si $k \geq \sqrt{m}$, alors puisqu'on a aussi $p > \sqrt{m}$, on obtient $kp > m$, ce qui est impossible. On doit donc avoir $k < \sqrt{m}$. Mais comme tout entier, l'entier k est divisible par un nombre premier $q \leq k$. Comme q divise k et k divise m, on a que q divise aussi m, et comme $k \leq \sqrt{m}$, on a que $q \leq \sqrt{m}$, ce qui contredit notre hypothèse de départ que m n'est divisible par aucun premier $\leq \sqrt{m}$. QED.

Appliquons ce résultat à $D(n)$ pour obtenir que $D(n)$ ne contient que des nombres premiers.

Lemme 2 : $D(n)$ ne contient que des nombres premiers [*].

Démonstration : Soit $m \in D(n)$. Alors m est impair et $m \leq n/2$. On sait par le lemme 1 que si m n'est divisible par aucun premier compris entre 3 et $\sqrt{m}$, alors m est premier. Mais par la définition de $D(n)$, on sait déjà que m n'est divisible par aucun premier compris entre 3 et $\sqrt{n}$, et puisque $m < n$, on a $\sqrt{m} < \sqrt{n}$ et donc a fortiori m n'est divisible par aucun premier compris entre 3 et $\sqrt{m}$, donc par le lemme 1, m est bien premier. QED.

Lemme 3 : Si m appartient à $D(n)$, alors $n - m$ est premier.

Démonstration : On commence par montrer qu'aucun nombre premier p compris entre 3 et $\sqrt{n}$ ne divise $n - m$. En effet, si $n - m$ est divisible par p, alors m est congru à n modulo p, ce qui contredit le fait que m appartient à $D(n)$. Ensuite, on note que puisque $n - m < n$, on a $\sqrt{n - m} < \sqrt{n}$ et donc a fortiori, $n - m$ n'est divisible par aucun premier $\leq \sqrt{n - m}$, donc par le lemme 1, $n - m$ est bien un nombre premier.

Si $D(n)$ est non vide, alors n vérifie la conjecture de Goldbach.

2. Existence d'un décomposant de Goldbach pour tout nombre pair

On a vu que $D(n)$ ne contient que des nombres premiers qui sont décomposants de Goldbach de n. Il faut maintenant démontrer que $D(n)$ est non vide pour que n vérifie la conjecture de Goldbach.

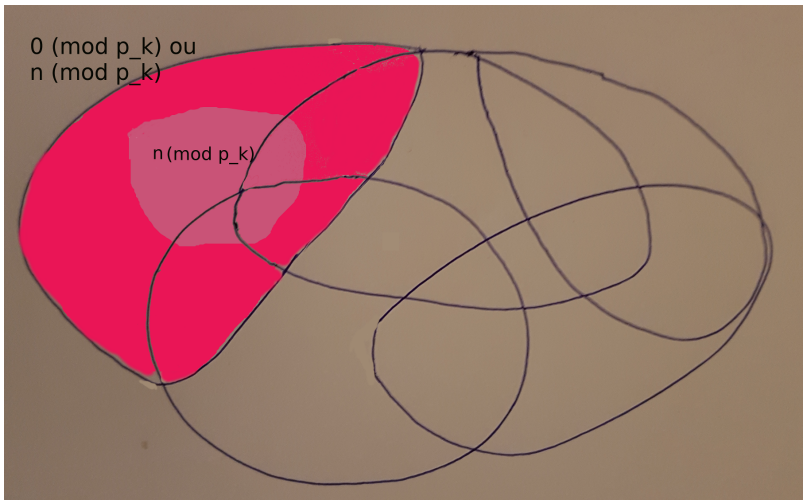
Essayons de comprendre pourquoi $D(n) = \cap F(p_k, n)$ ne peut être vide. On reprend l'écriture initiale qu'on avait choisie, sous forme logique : dire que l'intersection des ensembles de la forme $\{\neg 0_{p_k} \wedge \neg n_{p_k}\}$

∗. si $D(n)$ est vide, le lemme est vrai par vacuité.

est vide [†], ce que l'on note $\bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \varnothing = \bot$ (le symbole $\bot$ est le symbole logique pour *False*), est équivalent à dire que le complémentaire de cet ensemble est le "plein" (dénoté par $\top$, ou *Vrai*), i.e. couvre l'ensemble de tous les nombres impairs compris entre 3 et $n/2$.

$$\complement \bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \bigvee_{p_k}\{0_{p_k} \vee n_{p_k}\} = \top$$

Pour fixer (autant que faire se peut) les idées, on représente cette union d'ensembles de nombres "congrus à 0 ou à n selon un nombre premier p_k compris entre 3 et $\sqrt{n}$" qui contient TOUS les nombres impairs compris entre 3 et $n/2$ par un ensemble de patatoïdes comme sur le dessin suivant ;



Chaque ensemble délimité contient un ensemble de nombres impairs compris entre 3 et $n/2$ et congrus à 0 ou bien congrus à n selon un nombre premier p_k (p_k compris entre 3 et $\sqrt{n}$). On a coloré l'un d'eux en fuschia et à l'intérieur de lui on a "isolé" en utilisant la couleur rose clair les nombres qui sont congrus à n parmi ceux qui sont congrus à 0 ou à n modulo p_k.

Etudions le cas d'un nombre pair n qui est le double d'un nombre composé et considérons les nombres premiers (notons les p_{m_k}) compris entre $\sqrt{n}$ et $n/2$.

Alors on a que tout p_{m_k} ne peut pas être un élément des parties des ensembles contenant les nombres "congrus à 0" selon un p_k compris entre 3 et $\sqrt{n}$ puisque p_{m_k} est un nombre premier. Chaque nombre premier p_{m_k} est donc forcément dans les parties des ensembles contenant les nombres "congrus à n selon un p_k" (partie rose clair et non fuschia pour la fixation d'idées).

Essayons maintenant de démontrer pourquoi il est impossible qu'il existe pour chaque p_{m_k} compris entre $\sqrt{n}$ et $n/2$ un nombre premier p_k compris entre 3 et $\sqrt{n}$ tel que p_{m_k} et n ont même reste dans une division entière par p_k.

Voyons l'exemple du nombre pair 100 [‡].

†. $\neg$ est le symbole logique du "*non*", $\wedge$ est le symbole logique du "*et*", $\vee$ est le symbole logique du "*ou*", 0_{p_k} est l'expression choisie pour exprimer "*x est congru à 0 modulo p_k, i.e. $x \equiv 0$ (mod p_k) de Gauss*" (on omet le x pour alléger l'écriture) et n_{p_k} est l'expression choisie pour exprimer "*x est congru à n modulo p_k*".

‡. puisqu'on est 100 (sans) démonstration !

	3	5	7
11	2	1	4
13	1	3	6
17	2	2	3
19	1	4	5
23	2	3	2
29	2	4	1
31	1	1	3
37	1	2	2
41	2	1	6
43	1	3	1
47	2	2	5
100	1	0	2

On a noté en rouge les restes partagés par $n = 100$ et par les nombres premiers compris entre $\sqrt{n} = \sqrt{100} = 10$ et $n/2 = 100/2 = 50$ selon les modules 3, 5, 7 inférieurs à $\sqrt{n} = \sqrt{100} = 10$. Les lignes dans lesquels aucun reste n'est partagé avec 100 fournissent les décomposants de Goldbach de 100.

Exprimons les partages de restes par des égalités (égalités classiques de la forme $n = aq + p$ représentant des divisions euclidiennes) portant sur le nombre 100 et sur les nombres premiers entêtes de lignes : on a

$$\begin{array}{ll}
100 = ... & + 11 \\
100 = 29 \times 3 & + 13 \\
100 = ... & + 17 \\
100 = 27 \times 3 & + 19 \\
100 = 11 \times 7 & + 23 \\
100 = ... & + 29 \\
100 = 23 \times 3 & + 31 \\
100 = 21 \times 3 & + 37 \\
100 = ... & + 41 \\
100 = 19 \times 3 & + 43 \\
100 = ... & + 47
\end{array}$$

On a utilisé des points de suspension (...) pour exprimer qu'on n'a pas trouvé de produits de deux entiers, l'un compris entre 3 et $\sqrt{n}$, l'autre compris entre $n/2$ et $n - \sqrt{n}$, pour certaines lignes, les lignes des décomposants de Goldbach de 100 justement.

Il faudrait réussir à montrer que le système suivant d'équations correspondant à des divisions euclidiennes (en nombre $\pi(n/2) - \pi(\sqrt{n})$, avec la notation habituelle $\pi(x)$ est le nombre de nombres premiers inférieurs ou égaux à x) ne peut être vérifié par des a_k tous strictement supérieurs à 1.

$$\left\{\begin{array}{ll}
n = a_1 \times q_1 & + p_1 \\
n = a_2 \times q_2 & + p_2 \\
... & \\
n = a_k \times q_k & + p_k
\end{array}\right.$$

Les p_k sont compris entre $\sqrt{n}$ et $n/2$. Les q_k sont compris entre 3 et $\sqrt{n}$, il est nécessaire qu'il y ait des redondances, i.e. des égalités de la forme $q_i = q_j$ avec $i \neq j$, dans la mesure où les q_k sont bien moins nombreux que les p_k.

On arrive à établir une contradiction pour l'instant seulement si tous les nombres premiers compris entre 3 et $\sqrt{n}$ apparaissent chacun au moins une fois dans les équations du système : pour cela, on isole les p_k du côté droit des équations, on obtient :

$$\left\{\begin{array}{ll}
n - a_1 \times q_1 & = p_1 \\
n - a_2 \times q_2 & = p_2 \\
... & \\
n - a_k \times q_k & = p_k
\end{array}\right.$$

On multiplie alors toutes les équations entre elles, ce qui permet d'obtenir une égalité entre le produit de tous les nombres premiers compris entre $\sqrt{n}$ et $n/2$ et le produit de facteurs $(n - a_1 \times q_1)(n - a_2 \times$

$q_2)\dots(n - a_k \times q_k)$. Le développement de ce produit de facteurs est une somme de termes dans lesquels on peut toujours mettre n en facteur et d'un dernier terme produit de tous les $a_k p_k$. Le produit de toutes les équations donne :

$$\prod_k (n - a_k q_k) = \prod_k p_k$$

$$\iff \quad nT \pm \prod a_k q_k = \prod_k p_k$$

Note : On a noté $\pm$ dans la partie gauche de la seconde égalité car on ne sait pas si le dernier terme est ajouté ou soustrait (cela dépend du nombre d'équations du système mais cela n'intervient pas dans l'étude des différentes divisibilités). Si tous les nombres premiers compris entre 3 et $\sqrt{n}$ sont représentés "dans" l'une des équations, un diviseur de n figure au moins parmi eux. Il divise tous les termes contenant un facteur n, il divise également $\prod a_k q_k$ puisqu'il est l'un des q_k mais il ne divise pas le produit $\prod_k p_k$ de droite dans la mesure où ce produit est un produit de nombres premiers. On aboutit ainsi à une contradiction dans ce cas.

Subsiste un problème si l'un des nombres premiers compris entre 3 et $\sqrt{n}$ n'apparaît dans aucune équation du système.