Réécrire (Denise Vella-Chemla, 6.12.2019)

On cherche à démontrer la conjecture de Goldbach.

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

Fixons un nombre pair n supérieur à 4, double d'un nombre composé (car les doubles de nombres premiers vérifient trivialement la conjecture). Pour tout nombre premier p_k entre 3 et $\sqrt{n}$, notons $F(p_k, n)$ l'ensemble des entiers m qui sont * :

i) impairs,

ii) compris entre $\sqrt{n}$ et $n/2$,

iii) non congrus à 0 modulo p_k (i.e. non divisibles par p_k),

iv) non congrus à n modulo p_k (i.e. le reste après division de m par p_k n'est pas égal au reste après division de n par p_k).

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

Démontrons que si $D(n)$ est non vide, il 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 maintenant à $D(n)$ pour obtenir que $D(n)$ ne contient que des nombres premiers.

Lemme 2 : Si $D(n)$ est non vide, il 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 $D(n)$ est non vide et m appartient à $D(n)$, alors $n - m$ est premier.

Démonstration : On commence par montrer qu'aucun nombre premier p_k compris entre 3 et $\sqrt{n}$ ne divise $n - m$. En effet, si $n - m$ est divisible par p_k, alors m est congru à n modulo p_k, 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.

∗. Cette section a été rédigée formellement par Leila Schneps : du fait de travaux récents que j'ai effectués de secrétariat bibliographique, j'ai pris contact avec elle, car elle gère sur son site académique la page du "Grothendieck circle" ; en échange de ce service, je lui ai demandé de regarder mon texte http://denisevellachemla.eu/fibres-inter.pdf, ce qu'elle a fait, et elle m'a envoyé par mail la formalisation de cette section *Caractérisation des décomposants de Goldbach d'un nombre pair.*

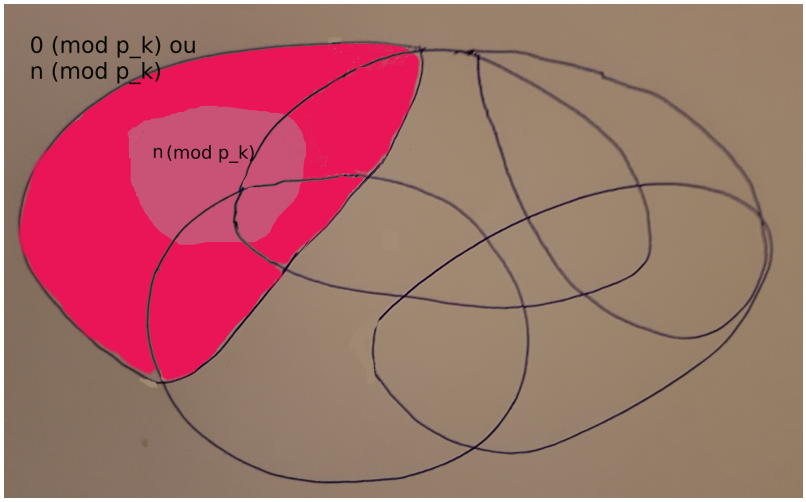
2. Existence d'un décomposant de Goldbach pour tout nombre pair

On a vu que si $D(n)$ est non vide, il ne contient que des nombres premiers qui sont décomposants de Goldbach de n et qu'alors 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 $\{\neg 0_{p_k} \wedge \neg n_{p_k}\}$ 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).

On n'arrive toujours pas à 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.

†. $\neg$ 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*".