Démonstration de la Conjecture forte de Goldbach

Par Mr.ANNOUAOUI RACHID

Enoncé de la Conjecture : << Tout entier naturel pair est la somme de deux entiers premiers>>.

Démonstration :

Soit n un entier pair.

Notons P_n l'ensemble de tous les nombres premiers strictement inférieurs à n défini comme suit :

$P_n = \{p_1 ; \ldots\ldots ; p_m\}$ ces p_i sont classés par ordre croissant :

$p_1 < p_2 < \ldots\ldots < p_{m-1} < p_m$ ($p_1=2$; $p_2=3$ …)

Donc p_m est le plus grand nombre premier strictement inférieur à n, autrement dit il n'y a plus de nombre premier entre p_m et n

On a donc $\forall\, p_i \in P_n$, $p_i \leq p_m < n$ et $n-p_i < n$.

La négation de la Conjecture de Goldbach s'énonce comme suit :

<< Il existe un entier naturel pair qui n'est égal à aucune somme de deux nombres premiers>> : Supposition 1 → S_1 .

Nous allons donc étudier cette négation pour ce n.

La signification de cette négation avec ce qui a été défini précédemment est :

« $\forall p_i \in P_n$, $n-p_i \notin P_n$ ».

On a $p_1 < p_2 < \ldots\ldots < p_{m-1} < p_m$ donc

$n-p_m < n-p_{m-1} < \ldots\ldots < n-p_2 < n-p_1$.

Supposons alors que $\forall p_i \in P_n$, $p_1 < n-p_i < p_m$: supposition 2 → S_2 .

Donc pour $p_i=p_m$ on obtient $p_1 < n-p_m < p_m$,

$p_1 < n-p_m \Rightarrow p_m < n-p_1$ Contradiction avec $n-p_i < p_m$

Cette supposition S_2 est donc fausse (S_2 est donc clôturée).

Et alors $\exists$ $p_{j/n}$ (qu'on va noter par la suite uniquement p_j) $\in P_n$ tel que $n- p_j \leq p_1$ ou $n- p_j \geq p_m$,

Donc deux cas se présentent :

1er cas :

$\exists$ $p_j \in P_n$ tel que $n- p_j \leq p_1$ comme $n- p_j \notin P_n$ alors $n- p_j < p_1=2$ d'où $n- p_j=1$,

$n- p_j=1 \Rightarrow n=p_j+1$ et comme $n > p_m$ donc $p_j+1 > p_m \Rightarrow p_j \geq p_m$ car p_j et p_m sont premiers et p_j+1 non, or $p_j \leq p_m$ car $p_j \in P_n$ et $p_m= \max(P_n)$ et donc $p_j= p_m$ (car on a $p_j \geq p_m$ et $p_j \leq p_m$).

D'où $n= p_m+1$

nous allons donc étudier ces nombres pairs de la forme p_m+1

Supposons donc que ces nombres ne sont pas décomposables :

N.B:

Décomposable = somme de deux nombres premiers.

Non décomposable n'est égal à aucune somme de deux nombres premiers.

On a, $\forall\ p_i \in P_n$, $n-pm < n-p_{m-1} < \ldots\ldots\ldots < n-p_2 < n-p_1$,

donc pour $n= p_m+1$ on obtient $p_m+1 -p_m =1 <\ldots< n- p_i < \ldots< n-2=p_m+1-2=p_m-1$.

Donc tous les $n-p_i$ sont répartis entre 2 et p_m-2.

Nous allons voir par la suite comment sont répartis ces $n- p_i$:

$\exists\ !\ p_{i1} \in P_n$ et $\exists\ !\ p_{i2} \in P_n$ tel que p_{i1} et p_{i2} nombres premiers successifs avec $p_{i1} < n- p_i < p_{i2}$, strictement car $n- p_i$ n'est pas premier et p_{i1} et p_{i2} sont premiers.

On a $p_{i1} < n- p_i < p_{i2} \Rightarrow p_i < n- p_{i1}$ et $p_i > n- p_{i2} \Rightarrow n- p_{i2} < p_i < n- p_{i1}$

De plus pour les nombres de la forme $n- p_k$, $n- p_{i2}$ et $n- p_{i1}$ sont aussi successifs car

$p_{i1} < p_{i2} < p_{i3} < \ldots\ldots\ldots \Rightarrow \ldots\ldots < n- p_{i3} < n- p_{i2} < n- p_{i1} < \ldots\ldots$

ceci montre que deux n- p_k différents ne peuvent appartenir au même intervalle composé par deux nombres premiers successifs puisqu'il existe un nombre premier entre les deux n- p_k (n- p_{i2} < p_i < n- p_{i1})

Or il y a **m** nombres premiers dans P_n et on a **m** nombres n- p_i (avec p_1 < p_i < p_m), en excluant n- p_m= 1 on a exactement **m-1** nombres n- p_i entre 2 et p_m ce qui correspond exactement au nombre d'intervalles entre p_1 et p_m : nombre d'intervalles=(nombre de p_i)-1=**m-1**.

D'où la répartition suivante de tous ces n- p_i entre p_1 et p_m :

n- p_{m-1} est compris strictement entre 2 et 3(impossible car il n'y a pas de nombre entre 2 et 3) ;

n- p_{m-2} est compris strictement entre 3 et 5 (impossible car il n'y a pas de nombre impair entre 3 et 5)

……

Donc contradiction, alors tous les nombres pairs de la forme p_m+1 sont décomposables.

2ème cas :

Il nous reste donc le cas où $n- p_j \geq p_m$:

Donc $\exists\ p_j \in P_n$ $n- p_j > p_m$ car $n- p_j$ n'est pas premier(S_1) et p_m est premier.

$n- p_j > p_m \Rightarrow n- p_m > p_j$ et donc

$n- p_m > p_j > p_{j-1} > p_{j-2} > \ldots\ldots\ldots > p_2 > p_1$.

Nous allons continuer cette analyse avec le plus grand nombre premier p_j de Pn qui permet l'inégalité $n- p_j > p_m$.

On aura alors $n- p_j > p_m$ et $n- p_{j+1} < p_m$

Avec p_{j+1} le nombre premier successif au nombre premier p_j.

Comme $p_j > p_{j-1} > p_{j-2} > \ldots\ldots\ldots > p_2 > p_1$ et

$p_{j+1} < p_{j+2} < \ldots\ldots\ldots < p_{m-1} < p_m$ on obtient alors :

$\rightarrow \forall\ p_k \leq p_j$, $n- p_k > p_m$ car $n- p_k \geq n- p_j > p_m$ (ce qui nous indique la non primalité des $n- p_k$ pour $p_k \leq p_j$ car pas de nombre premier entre p_m et n) Et,

$\rightarrow \forall\ p_k \geq p_{j+1}$, $n- p_k < p_m$ ou $p_1 < n-p_k < p_m$ car $n- p_k < n-p_{j+1} < p_m$

Nous allons démontrer tout d'abord l'existence de ce $p_{j/n}$:

p_j a été défini comme suit :

$\exists\ p_j \in P_n$ tel que $n- p_j > p_m$ et $n- p_{j+1} < p_m$ avec p_{j+1} le nombre premier successif au nombre premier p_j.

Supposons alors le contraire : $\forall\ p_j \in Pn$, $n-p_j > p_m$: Supposition 3 $\rightarrow S_3$

Donc pour $p_j=p_m$ on obtient alors $n- p_m > p_m \Rightarrow n > 2p_m$

Comme $n > p_m$ alors $p_m < 2p_m < n$.

Or d'après le théorème de Tchebychev, il y a toujours un nombre premier entre q et 2q (avec q entier naturel >1) et comme il n'y a pas de nombre premier entre p_m et n alors il n'y a pas aussi de nombre premier entre p_m et $2p_m$ ce qui se contredit avec le théorème de Tchebychev, on en déduit alors qu' $\exists\ p_j \in Pn$ tel que $n- p_j > p_m$ la supposition S_3 est donc clôturée.

Et en même temps on vient de démontrer que $n- p_m < p_m$.

D'autre part,

$\rightarrow$ Si $n- p_{m-1} < p_m$ alors $n- p_{m-1} < n- p_j$ car $n- p_{m-1} < p_m < n- p_j \Rightarrow p_j < p_{m-1}$ et donc p_j est compris entre p_1 et p_{m-2} et alors p_{j+1} est compris entre p_2 et p_{m-1}.

$\rightarrow$ Si $n- p_{m-1} > p_m$ alors on a $n- p_m < p_m$ et $n- p_{m-1} > p_m$ donc $p_j = p_{m-1}$ et $p_{j+1}=p_m$.

On vient donc de démontrer l'existence de p_j et p_{j+1} .

On a donc $\forall\ p_i \in P_n$ tel que $p_i \geq p_{j+1}$, $n- p_j > p_m > p_i \Rightarrow\ n- p_j > p_i \Rightarrow$ $n- p_i > p_j$,

et plus particulièrement $\forall\ p_i \geq p_{j+1}$, $n-p_i \leq n- p_{j+1} < p_m$ et donc $p_j < n- p_i < p_m$.

Etudions alors la répartition de ces $n- p_i$ entre p_j et p_m :

On va adopter le même raisonnement que le **1er cas** (sauf qu'en ce **2ème cas** on prend p_j au lieu de p_1), soit p_i entre p_j et p_m, $\exists !\ p_{i1} > p_j$ et $\exists !\ p_{i2} > p_j$ tel que p_{i1} et p_{i2} nombres premiers successifs avec $p_{i1} < n- p_i < p_{i2}$, strictement car $n- p_i$ n'est pas premier et p_{i1} et p_{i2} sont premiers (avec $p_j < n- p_i < p_m$).

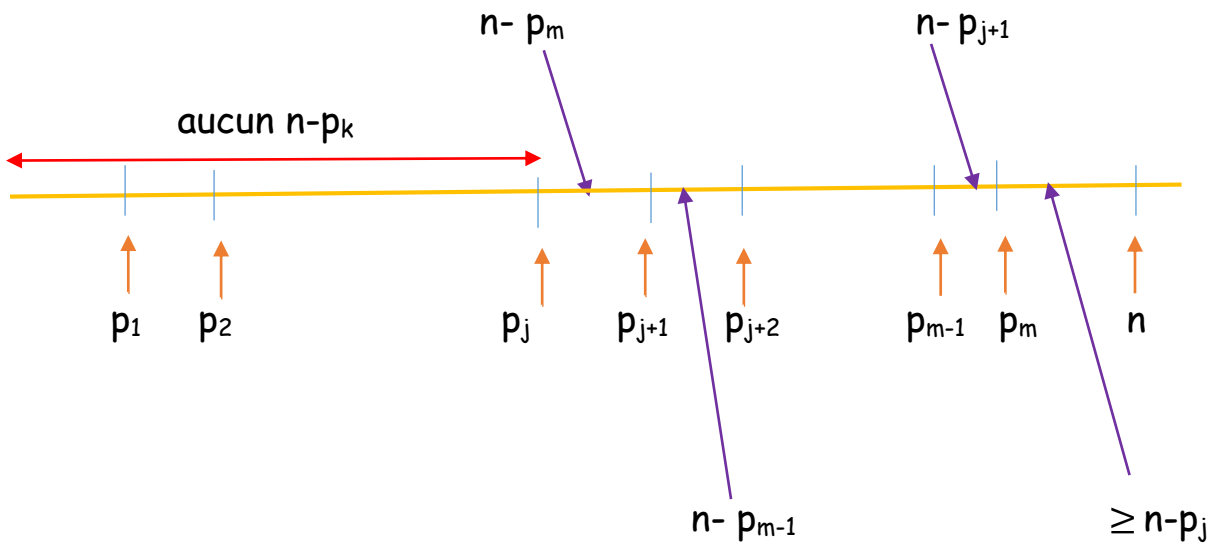
On a $p_{i1} < n- p_i < p_{i2} \Rightarrow\ p_i < n- p_{i1}$ et $p_i > n- p_{i2} \Rightarrow\ n- p_{i2} < p_i < n- p_{i1}$

De plus pour les $n- p_k$, $n- p_{i2}$ et $n- p_{i1}$ sont aussi successifs car

$p_{i1} < p_{i2} < p_{i3} < \ldots\ldots\ldots \Rightarrow \ldots\ldots < n- p_{i3} < n- p_{i2} < n- p_{i1} < \ldots\ldots$

ceci montre que deux $n- p_k$ différents ne peuvent appartenir au même intervalle composé par deux nombres premiers successifs puisqu'il existe un nombre premier entre les deux $n- p_k$ ($n- p_{i2} < p_i < n- p_{i1}$)

Schématisons alors cette répartition sur la droite graduée suivante :



En effet,

$n- p_j > p_m \Rightarrow n- p_m > p_j$

et $n- p_{j+1} < p_m \Rightarrow n- p_m < p_{j+1}$ d'où $p_j < n- p_m < p_{j+1}$

le nombre de p_k entre p_m et p_{j+1} est égal à m-(j+1)+1=m-j.

Et le nombre de n-p_k (avec p_k entre p_{j+1} et p_{m-1} car p_m est déjà utilisé entre p_j et p_{j+1}) est égal à (m-1)-(j+1)+1=m-j-1 qui correspond exactement au nombre d'intervalles entre p_{j+1} et p_m, et comme on a $n- p_{m-1} < n- p_{m-2} < \ldots\ldots < n- p_{j+1}$ alors on a exactement la répartition suivante :

$p_{j+1} < n- p_{m-1} < p_{j+2}$; $p_{j+2} < n- p_{m-2} < n- p_{j+3}$ ……. Et $p_{m-1} < n- p_{j+1} < p_m$.

Car on avait démontré qu'entre deux nombres premiers successifs ($\geq p_{j+1}$) il y a un unique n-p_k ($p_k \geq p_{j+1}$)

De même n- $p_j > p_m \Rightarrow p_m < n- p_j < n$,

Donc tous les n-p_k ($p_k \leq p_j$: n- $p_j < n-p_k$) sont au-delà de p_m ce qui confirme la répartition des n-p_i sur la régle graduée tracées ci-avant.

Récapitulons donc tout ce qui précède pour ce 2ème cas :

→ $\forall$ p_i entre p_{j+1} et p_m on a $p_j < n- p_i < p_m$

→ Entre deux nombres premiers successifs supérieurs à p_j , il y a un unique n-p_k avec $p_j < p_k \leq p_m$.

D'autre part,

On a $\forall p_k$ (entre p_j et p_{m-1}) et $\forall p_{k+1}$ (entre p_{j+1} et p_m), nombres premiers successifs, p_k et p_{k+1} ne peuvent être des nombres premiers jumeaux ($p_{k+1} - p_k = 2$) car si c'était le cas alors le seul entier qui existe entre p_k et p_{k+1} est $p_k + 1$ et comme $p_k < n-p_i < p_{k+1}$ alors $n-p_i = p_k + 1$

Ce qui est impossible car $n-p_i$ est impair et $p_k + 1$ est pair

D'où $\forall p_k$ entre p_j et p_{m-1}, p_k et p_{k+1} ne peuvent être des nombres premiers jumeaux.

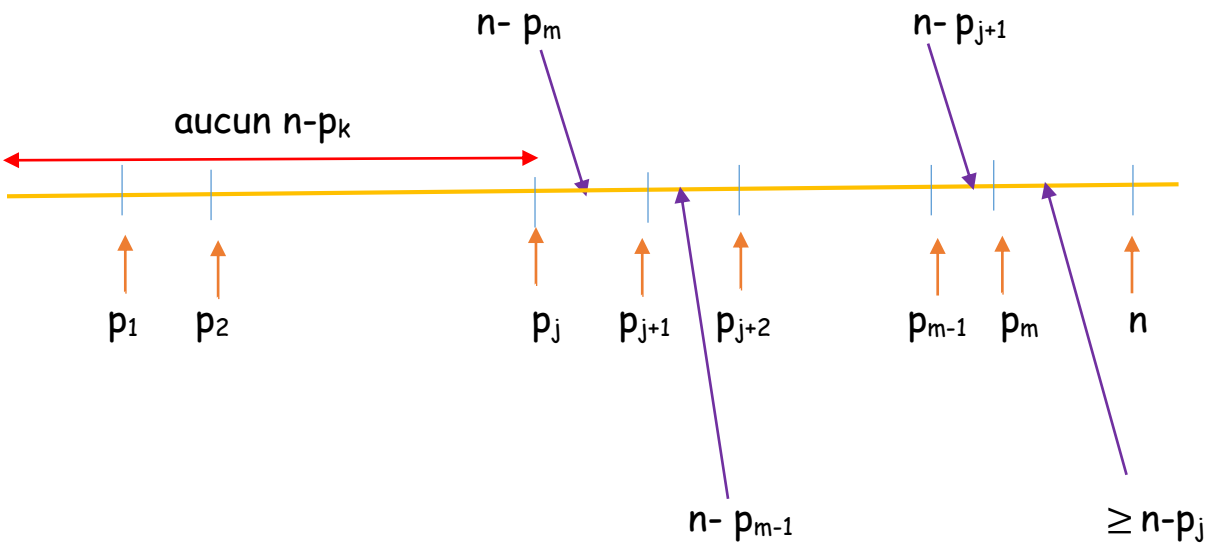
Donc les seuls nombres premiers jumeaux sont ceux compris entre p_1 et p_j ou ceux supérieurs strictement à p_m (c'est à dire supérieurs à p_{m+1} avec p_{m+1} le nombre premier successif à p_m).

Récapitulons encore une fois:

→ $n \in E_p$ (E_p ensemble des entiers pairs), tel que $\forall\ p_i \in P_n$, $n-p_i \notin P_n$.

→ Entre chaque p_k et p_{k+1} (avec k entre j et m-1) il y a un unique $n-p_i$ (avec i entre j+1 et m).

Schématisé sur la droite graduée suivante :



→ Il n'y a pas de nombres premiers jumeaux entre p_j et p_m.

→ Les seuls nombres premiers jumeaux existent entre p_1 et p_j ou ceux supérieurs strictement à p_m (c'est à dire supérieurs à p_{m+1} avec p_{m+1} le nombre premier successif à p_m).

Nous allons alors définir cette propriété P comme tel :

$$[n \text{ non décomposable} \Rightarrow \nexists \text{ de } (p_{ju-1};p_{ju}) \text{ entre } p_j \text{ et } p_m\ ]$$

$$\Updownarrow$$

$$[\ \exists\ (p_{ju-1};p_{ju}) \text{ entre } p_j \text{ et } p_m \Rightarrow n \text{ décomposable}]$$

Avec $(p_{ju-1}\,;\,p_{ju})$ un couple de nombres premiers jumeaux.

Et idem, avec décomposable veut dire s'écrit en une somme de deux nombres premiers et non décomposable veut dire ne s'écrit pas comme somme de deux nombres premiers.

Nous allons étudier par la suite les nombres pairs entre p_m et n,

Le premier entier (sens croissant) dans ce cas est $p_m + 1$ déjà démontré décomposable, pour $p_m + 3$: décomposable ; $p_m + 5$: décomposable ; $p_m + 7$: décomposable.

Nous allons raisonner par la suite sur les nombres de la forme $p_m + 2k+1$ qui sont les nombres pairs entre p_m (strictement) et n, avec 2k+1 non premier car les nombres de la forme $p_m + 2k+1$ avec 2k+1 premier répondent au critère : somme de deux nombres premiers ($\exists\, k_n \in \mathbb{N}$ tel que $n= p_m + 2k_n + 1$).

Les nombres de la forme $p_m + 2k$ sont impairs ce qui ne nous intéresse pas dans notre cas.

Le premier nombre tel que $p_m + 2k+1$ pair et 2k+1 non premier est le nombre $p_m+ 9$ qu'on notera n_1.

Remarquons que $P_{n1} = P_n$ car il n'y a plus de nombre premier entre p_m et n $[p_m(n_1) = p_m(n)=\max(P_n)]$.

Supposons alors que n_1 n'est pas décomposable, on adoptera alors le même raisonnement que pour n, donc $\exists\ p_{j1} \in P_n$ tel que $p_{j1} < n_1 - p_m < p_{j1+1} \Rightarrow p_{j1} < p_m + 9 - p_m < p_{j1+1} \Rightarrow p_{j1} < 9 < p_{j1+1} \Rightarrow$

$p_{j1} = 7$ et $p_{j1+1} = 11$ (puisque p_{j1} et p_{j1+1} sont premiers successifs)

Or on avait démontré comme pour n qu'il n'y a pas de nombres premiers jumeaux entre p_{j1} et p_m alors que dans ce cas il y a plusieurs nombres premiers jumeaux entre $p_{j1} = 7$ et p_m, contradiction $\Rightarrow n_1 = p_m + 9$ s'écrit comme somme de deux nombres premiers(propriété P).

Idem pour le deuxième nombre pair de la forme $p_m + 2k+1$ et $2k+1$ non premier, ce nombre est égal à $n_2 = p_m + 15$ ($Pn_2 = P_{n1} = P_n$) $\Rightarrow$ $p_{j2} < 15 < p_{j2+1} \Rightarrow p_{j2} = 13$ et $p_{j2+1} = 17$ et comme il y a plusieurs nombres premiers jumeaux entre $p_{j/n2} = 13$ et p_m alors contradiction et donc $p_m + 15$ s'écrit comme somme de deux nombres premiers (propriété P).

Idem pour $n_3 = p_m + 21 \Rightarrow p_{j3} = 19$ et $p_{j3+1} = 23$ et ainsi de suite….,

donc tous les nombres pairs de la forme $p_m + 2k+1$ avec $2k+1$ non premier et $2k+1 \leq a$ qu'on va déterminer par la suite, sont décomposables, ce qui nous permet de déduire que tous les nombres pairs successifs de p_m+1 à $p_m+ a$ ($2k+1$ premier ou non) sont décomposables.

On déduira aussi ce qui suit :

→ (*) : Tous les nombres pairs q entre p_k et $p_k + p_{ju}$ (avec p_{ju} le deuxième terme du dernier couple de nombres premiers jumeaux tous infèrieurs à p_k) sont décomposables, en effet on a :

$p_k < q < p_k + p_{ju} \Rightarrow q-p_k < p_{ju}$

De plus $p_k \leq p_m(q) \Rightarrow q-p_m(q) \leq q- p_k$

Donc en utilisant $p_j(q)$ comme il a été défini pour les q supposés non décomposables on aura : $p_j(q) < q-p_m(q)$

Or $q-p_m(q) \leq q- p_k < p_{ju} < pk \leq p_m(q)$ et puisque $p_{ju} = p_{ju-1} +2$ alors on aura $p_j(q) \leq p_{ju-1} < p_{ju} < pk \leq p_m(q)$, contradiction en appliquant la propriété P à q, donc q est décomposable.

→ Tous les nombres pairs q inférieurs à p_{ju} sont décomposables puisqu'il existera toujours un couple de nombres premiers jumeaux $(p_{ju-1} ; p_{ju})$ tel que $p_j < p_{ju-1} < p_{ju} < p_m$.

→ De même, Tous les nombres pairs q entre p_{ju} et p_{ju+1} (p_{ju+1} nombre premier successif à p_{ju} non forcément jumeau avec p_{ju}) sont décomposables car $q \in]p_{ju} ; p_{ju+1}[$ donc $p_m(q) = p_{ju}$ et alors $p_{ju} < q < p_{ju+1}$ ⇒

$p_{ju} < q < p_{ju+1} < 2p_{ju}$ (théorème de Tchebychev) ⇒ $0 < q - p_{ju} < p_{ju}$ et donc $p_j(q) < q - p_m(q) = q - p_{ju} < p_{ju} = p_m(q)$ (si on suppose q non décomposable).

on aura même $p_j(q) < q - p_{ju} < p_{ju-1} < p_{ju}$ (car $p_{ju} = p_{ju-1} + 2$), contradiction en appliquant la propriété P à q, donc q est décomposable.

→ En prenant même n très grand donc $p_m(n)=p_m$ très grand, et en prenant p'_{ju} comme deuxième terme du dernier couple de nombres premiers jumeaux découvert à ce jour (ordre de grandeur de ce p'_{ju} !) inférieur à p_m et donc à n tel que $p_m < n \leq p_m + p'_{ju}$ et en appliquant le même raisonnement que (*) pour n, on déduira que n est décomposable, donc tous les nombres pairs successifs de p_m+1 jusqu'à $p_m + p'_{ju}$ sont décomposables (donc a = p'_{ju}).