Démonstration de la conjecture de Goldbach

"tout nombre entier pair supérieur à 2 peut s'écrire comme la somme de deux nombres premiers."

C.Pokorski

25 mai 2024

Abstract

Ce document propose une démonstration de la conjecture de Goldbach (1742). L'approche consiste à reformuler la conjecture afin de la rendre plus accessible et à exploiter les propriétés des nombres premiers ainsi que leurs relations avec les nombres entiers à travers leurs décompositions.

Lemmes intermédiaires

Lemme 1. Soit n un entier positif composé et P l'ensemble des nombres premiers inférieurs ou égaux à $n/2$. Alors P contient tous les facteurs premiers de n, y compris $n/2$ si n est pair.

Proof. Soit n un entier positif. Par le théorème de la décomposition en facteurs premiers, n peut être décomposé de manière unique en un produit de nombres premiers :

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k},$$

où $p_1, p_2, \ldots, p_k$ sont des nombres premiers distincts et $e_1, e_2, \ldots, e_k$ sont des entiers positifs.

Supposons qu'il existe un facteur premier p_i de n qui n'est pas dans P. Alors $p_i > n/2$.

Si $p_i > n/2$, alors p_i doit être le plus grand facteur premier de n. Cela signifie que le produit des autres facteurs premiers (s'il y en a) doit être inférieur ou égal à $n/2$, car $n = p_i \cdot$ (produit des autres facteurs).

Cependant, $p_i \cdot$ (produit des autres facteurs) $\leq p_i \cdot (n/p_i) = n$ implique que les autres facteurs doivent être inférieurs ou égaux à $n/p_i \leq n/2$. Ceci est une contradiction car $p_i > n/2$.

Ainsi, tous les facteurs premiers de n doivent être dans P, y compris $n/2$ si n est pair. $\square$

Lemme 2. Si n et m sont des entiers positifs tels que m est composé et $(n-m)$ est également composé, alors n et m partagent au moins un facteur premier.

Proof. Supposons que m et $(n-m)$ soient composés. Alors m a au moins un facteur premier, disons q. Puisque q divise m et $(n-m)$, il doit également diviser n. Donc, n et m partagent au moins le facteur premier q. □

Lemme 3. Soit n un entier positif et P un ensemble de nombres premiers tel que pour chaque facteur premier q de n, il existe un $p \in P$ tel que $\gcd(n, n-p) \neq 1$. Alors le produit $\prod_{p \in P} \gcd(n, n-p)$ partage tous les facteurs premiers de n.

Proof. Supposons que pour chaque facteur premier q de n, il existe un $p \in P$ tel que $\gcd(n, n-p) \neq 1$. Cela signifie que $\gcd(n, n-p)$ a un facteur premier commun avec n.

Considérons chaque facteur premier q de n. Par hypothèse, il existe un $p \in P$ tel que $q \mid n$ et $q \mid (n-p)$. Ainsi, q divise $\gcd(n, n-p)$ pour ce p.

Le produit $\prod_{p \in P} \gcd(n, n-p)$ inclut tous ces $\gcd(n, n-p)$. Puisque chaque $\gcd(n, n-p)$ inclut q pour au moins un $p \in P$, il s'ensuit que q divise le produit total $\prod_{p \in P} \gcd(n, n-p)$.

Pour assurer que le produit $\prod_{p \in P} \gcd(n, n-p)$ partage tous les facteurs premiers de n, vérifions que tous les facteurs premiers q de n sont couverts par les $p \in P$:

- Soit q un facteur premier de n.
- Par hypothèse, il existe un $p \in P$ tel que $\gcd(n, n-p) \neq 1$.
- Cela implique que $q \mid \gcd(n, n-p)$ pour ce p.
- Ainsi, q divise le produit $\prod_{p \in P} \gcd(n, n-p)$.

Puisque chaque facteur premier q de n est inclus dans au moins un des $\gcd(n, n-p)$ pour $p \in P$, le produit $\prod_{p \in P} \gcd(n, n-p)$ partage effectivement tous les facteurs premiers de n. □

Lemme 4. Les deux conjectures suivantes sont équivalentes :

- Conjecture de Goldbach : Tout nombre pair supérieur à 2 peut être exprimé comme la somme de deux nombres premiers.
- Reformulation : Pour tout nombre pair n supérieur à 2, il existe au moins un nombre premier p tel que $n-p$ soit également premier.

Proof. **Sens "conjecture de Goldbach" vers "reformulation"**

Supposons que la conjecture de Goldbach soit vraie. Alors, pour tout nombre pair n supérieur à 2, il existe des nombres premiers p et q tels que $n = p + q$. Posons $q = n - p$. Par définition de p et q comme nombres premiers, $n - p$ est premier puisque c'est simplement q sous une autre désignation. Donc, pour chaque n pair et chaque choix de p, si $p + q = n$ avec q premier, alors $n - p$ est aussi premier. Cela démontre que si la conjecture de Goldbach est vraie, alors la reformulation l'est aussi.

Sens "reformulation" vers "conjecture de Goldbach"

Inversement, supposons que la reformulation soit vraie. Cela signifie que pour tout nombre pair n supérieur à 2, nous pouvons trouver un nombre premier p tel que $n - p$ soit également premier, notons ce deuxième premier par q. Alors, $n = p + (n - p) = p + q$, où p et q sont des nombres premiers. Cela démontre que si la reformulation est vraie, alors la conjecture de Goldbach l'est aussi. $\square$

Théorème principal

Théorème 1. Pour tout nombre pair n supérieur à 2, il existe au moins un nombre premier p tel que $n - p$ soit également un nombre premier.

Proof. Supposons par l'absurde que pour tout p appartenant à l'ensemble P des nombres premiers inférieurs ou égaux à $n/2$, $n - p$ soit composé.

D'après le **Lemme 1**, l'ensemble P contient tous les facteurs premiers de n.

Le **Lemme 2** indique alors que pour tout p dans P, n et $n - p$ partagent au moins un facteur premier.

Par conséquent, d'après le **Lemme 3**, le produit $\prod_{p\in P} \gcd(n, n - p)$ doit contenir tous les facteurs premiers de n.

Supposons que pour tout $p \in P$, $n - p$ soit composé. Cela signifie que chaque $n - p$ partage au moins un facteur premier avec n.

Considérons le produit $\prod_{p\in P} \gcd(n, n - p)$. Puisque chaque $\gcd(n, n - p)$ contient un facteur premier de n et P contient tous les facteurs premiers de n (par le **Lemme 1**), ce produit doit contenir tous les facteurs premiers de n.

Cependant, si tous les $n - p$ sont composés, alors chaque $n - p$ doit avoir un facteur premier qui lui est propre, en plus de ceux qu'il partage avec n. Cela signifierait que le produit $\prod_{p\in P} \gcd(n, n - p)$ contiendrait non seulement les facteurs premiers de n, mais aussi des facteurs premiers supplémentaires propres à chaque $n - p$. Mais cela est impossible, car n a un nombre fixe de facteurs premiers qui ne peut pas inclure tous les facteurs premiers supplémentaires de chaque $n - p$.

Cette contradiction montre que notre hypothèse de départ est fausse : il ne peut pas être vrai que pour tout p dans P, $n - p$ soit composé.

Donc, il existe nécessairement au moins un nombre premier p appartenant à l'ensemble P tel que $n - p$ soit également premier.

Par équivalence et d'après le **Lemme 4**, pour tout nombre pair n supérieur à 2, il existe donc des nombres premiers p et q tels que $n = p + q$. $\square$

Informations

Version du document : 1.0, mai 2024

Contact : cpokorski.fr@gmail.com