Démonstration d'Euclide de l'infinitude de l'ensemble des nombres premiers et son application au problème de l'infinitude de l'ensemble des nombres premiers jumeaux, Denise Vella-Chemla, septembre 2025

Tout le monde connaît la démonstration d'Euclide de l'infinitude de l'ensemble des nombres premiers (voir sa traduction en Annexe).

Essayons d'utiliser un argument similaire à celui d'Euclide pour démontrer l'infinitude de l'ensemble des nombres premiers jumeaux.

1. Énoncé

On appelle nombres premiers jumeaux deux nombres premiers dont la différence est 2.

Exemples :

- 3 et 5 sont des nombres premiers jumeaux.
- 29 et 31 sont des nombres premiers jumeaux.

La conjecture des nombres premiers jumeaux stipule qu'il y a une infinité de couples de nombres premiers jumeaux.

On appellera "pair de jumeaux" le nombre pair (qui, excepté 4 compris entre 3 et 5, est toujours également divisible par 3) qui est entre deux nombres premiers jumeaux. Le "pair" des nombres premiers jumeaux 3 et 5 est 4, celui de 29 et 31 est 30.

On essaie ci-après de démontrer la conjecture des nombres premiers jumeaux en utilisant un argument similaire à celui d'Euclide pour démontrer l'infinitude de l'ensemble des nombres premiers.

2. Euclide et l'infinitude de l'ensemble des pairs de jumeaux

Appelons $\mathcal{P}$ l'ensemble des nombres premiers.

Supposons que l'ensemble $\mathcal{PP} = \{k \mid k-1 \in \mathcal{P} \text{ et } k+1 \in \mathcal{P}\}$, i.e. l'ensemble des pairs de nombres premiers jumeaux, soit fini. Fournissons la définition en extension de $\mathcal{PP}$:

$$\mathcal{PP} = \{4, 6, 12, 18, 30, 42, \ldots, \mathrm{pp}_{\max}\}.$$

On appelle $\mathrm{pp}_{\max}$ le plus grand élément de $\mathcal{PP}$, i.e. le plus grand pair de nombres premiers jumeaux. $\mathrm{pp}_{\max} - 1$ et $\mathrm{pp}_{\max} + 1$ sont deux nombres premiers.

Calculons

$$\mathrm{Prod}_+ = \left(\prod_{\substack{p \in \mathcal{P} \\ p \leq \mathrm{pp}_{\max}+1}} p \right) + 1$$

et

$$\mathrm{Prod}_- = \left(\prod_{\substack{p \in \mathcal{P} \\ p \leq \mathrm{pp}_{\max}+1}} p \right) - 1$$

qui sont le successeur et le prédécesseur du produit de tous les nombres premiers inférieurs au nombre premier $\mathrm{pp}_{\max} + 1$.

Dans la démonstration d'Euclide, il y a deux possibilités pour Prod_+ et Prod_-. Soit, dans le premier cas, ce sont deux nombres premiers (le premier a pour reste $+1$ dans toute division euclidienne par un nombre premier p avec $p \leq \mathrm{pp}_{\max} + 1$, et le second a pour reste $p - 1$ dans toute division euclidienne par un nombre premier p avec $p \leq \mathrm{pp}_{\max} + 1$. Soit, dans le second cas, chacun d'eux a un diviseur premier qui n'est pas dans l'ensemble $\mathcal{PP}$, appelons p le diviseur premier de Prod_+ et q le diviseur premier de Prod_-.

Dans le premier cas, on a trouvé un nombre $\displaystyle\prod_{\substack{p \in \mathcal{P} \\ p \leq \mathrm{pp}_{\max}+1}} p$, qui est un nombre pair entre deux nombres premiers, et qui n'appartient pas à l'ensemble $\mathcal{PP}$, ce qui contredit l'hypothèse que $\mathcal{PP}$ est un ensemble fini de pairs de nombres premiers. Mais dans le second cas, on ne peut pas déduire qu'on a trouvé un nouveau pair de nombres premiers, parce qu'on ne sait rien sur les diviseurs premiers p et q. On ne peut donc pas étendre la démonstration d'Euclide de l'infinitude de l'ensemble des nombres premiers pour démontrer l'infinitude de l'ensemble des paires de nombres premiers jumeaux.

3. Démonstration de l'infinitude de l'ensemble des pairs de nombres premiers jumeaux utilisant une infinité dénombrable de systèmes de congruences

Il y a une infinité de nombres premiers, l'ensemble des nombres premiers est à nouveau noté $\mathcal{P}$.

Considérons l'infinité de systèmes de congruences définis ainsi :

$$\begin{cases} x_1 & \equiv & 0 \pmod 2 \ ; \\ x_2 & \equiv & 0 \pmod 3 \ ; \\ x_3 & \equiv & 0 \vee 2 \vee 3 \pmod 5 \ ; \\ x_5 & \equiv & 0 \vee 2 \vee 3 \vee 4 \vee 5 \pmod 7 \ ; \\ \quad \vdots & & \\ x_k & \equiv & 0 \vee 2 \vee 3 \vee \ldots \vee p_k - 2 \pmod{p_k} \ ; \\ \quad \vdots & & \end{cases}$$

Dans le système ci-dessus, le symbole $\vee$ représente la disjonction combinatoire de tous les systèmes de congruences que l'on peut écrire en ne considérant dans chacun des systèmes qu'un seul nombre à prendre dans chaque disjonction de nombres.

On peut numéroter chacun des systèmes en question en les mettant en bijection avec $\mathbb{N}$ (numérotation lexicographique selon l'ordre habituel sur les entiers appliquée aux disjonctions de restes).

Or chacun de ces systèmes permet, par application du théorème des restes chinois d'obtenir au moins une (en fait une infinité) solution du système de congruence en question. Ce nombre x est un pair de nombres premiers jumeaux car il vérifie l'équation

$$(x-1)(x+1) \not\equiv 0 \pmod{\prod_{p_k \in \mathcal{P}} p_k},$$

ce qui rend $x-1$ et $x+1$ premiers tous les deux.

Il y a donc au moins une infinité dénombrable de pairs de nombres premiers jumeaux.

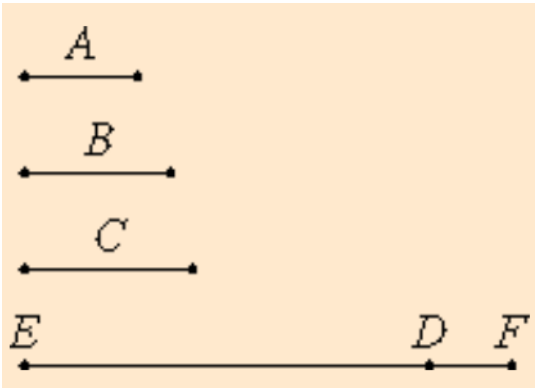
On peut se reporter, pour voir des exemples (finis mais complétables infiniment par des congruences à la solution, selon tous les nombres premiers supérieurs au plus grand nombre premier utilisé dans le système d'un nombre fini de congruences) de tels systèmes de congruences, à la note
Conjecture de Goldbach relative versus Infinitude de l'ensemble des paires de nombres premiers jumeaux absolue ,
qui montre que le problème de l'infinitude de l'ensemble des nombres premiers jumeaux est la variante "absolue" de la conjecture de Goldbach : pour trouver un pair de nombres premiers jumeaux, on cherche une solution d'un système de congruence de la forme $(x-1)(x+1) \not\equiv 0 \pmod{p_k, \forall p_k \in \mathcal{P}}$ alors que pour trouver un décomposant de Goldbach de n supérieur à $\sqrt{n}$, on cherche une solution d'un système de congruence de la forme $x(n-x) \not\equiv 0 \pmod{p_k, \forall p_k \in \mathcal{P} \cap [2..\sqrt{n}]}$.

Pour la démonstration de cette dernière assertion, on peut se reporter à la note
démonstration de la caractérisation des décomposants de Goldbach supérieurs à $\sqrt{n}$ d'un nombre pair n .

Annexe : Démonstration d'Euclide de l'infinitude de l'ensemble des nombres premiers

Proposition 20 du livre IX *des Éléments d'Euclide* :

Les nombres premiers sont plus nombreux que toute multitude possible qui serait assignée à leur ensemble.
Soient A, B, et C trois nombres premiers.
Je dis qu'il y a plus de nombres premiers que les seuls A, B, et C.
Prenons DE le plus petit nombre mesuré à la fois par A, B, et C. Ajoutons l'unité DF à DE.



Alors EF est soit un nombre premier, soit un nombre composé.
D'abord, supposons qu'EF soit un nombre premier. Alors A, B, C et EF sont des nombres premiers, ce qui est davantage que les seuls A, B, C.
(VII.31) Maintenant, supposons que EF soit composé. Alors EF est mesuré par un certain nombre premier. Supposons EF mesuré par le nombre premier G.
Je dis que G n'est égal à aucun des nombres A, B, et C.
Supposons qu'il puisse l'être. Maintenant, A, B et C mesurent DE, donc G mesure également DE. Mais il mesure aussi EF. Par conséquent, G, étant un nombre, mesure leur reste, l'unité DF, ce qui est absurde.
Donc G n'est pas égal à l'un quelconque des nombres A, B, et C. Et par hypothèse, G est un nombre premier. Par conséquent, les nombres A, B, C et G sont des nombres premiers, ce qui est davantage que la multitude initiale des nombres premiers qui était assignée aux seuls nombres A, B et C.
Donc, les nombres premiers sont en nombre plus grand que toute multitude possible qui puisse leur être assignée.