

Une aide qui tombe à point nommée (Denise Vella-Chemla, 4.12.2019)

Du fait de travaux récents que j'ai effectués de secrétariat bibliographique, j'ai pris contact avec Leila Schneps, qui gère sur son site personnel la page du "Grothendieck circle" et elle a eu la gentillesse d'écrire correctement "mes" mathématiques. Je voulais garder ici mémoire de nos échanges.

Extrait d'un mail de Leila Schneps du 3.12.2019

Fixons un nombre pair  $n$  supérieur à 4. Pour tout nombre premier  $p$  entre 3 et  $\sqrt{n}$ , notons  $F(p, n)$  l'ensemble des entiers  $m$  qui sont :

- i) impairs,
- ii) compris entre  $\sqrt{n}$  et  $n/2$ ,
- iii) non congrus à 0 modulo  $p$  (i.e. non divisibles par  $p$ ),
- iv) non congrus à  $n$  modulo  $p$  (i.e. le reste après division de  $m$  par  $p$  n'est pas égal au reste après division de  $n$  par  $p$ ).

On pose maintenant  $D(n) = \cap F(p, n)$ , c'est l'intersection des ensembles  $F(p, n)$  pour tous les premiers 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.

J'applique ce résultat maintenant à  $D(n)$  pour obtenir votre énoncé 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  $p$  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. Il faut maintenant comprendre pourquoi  $D(n)$  est non vide!

*Ma réponse* : Le complémentaire de l'ensemble vide, c'est l'ensemble plein ; dire qu'un ensemble est vide, c'est dire que son complémentaire contient TOUS les nombres. On sait bien (sic ;-)) que TOUS les nombres n'ont pas soit comme reste 0 soit le même reste qu'un nombre donné (je ne sais pas moi, 3, au hasard) quand on les divise par un nombre premier quelconque, même si les nombres en question sont tous compris dans un même intervalle  $[\sqrt{n}, n/2]$ . Si le complémentaire de l'ensemble que l'on suppose vide ne peut pas être "le plein", alors l'ensemble que l'on a supposé vide ne l'est pas (par démonstration par l'absurde).

On est sûr que les conditions "(congru à 0) OU (congru à  $n$ ) selon chaque  $p$ " sont trop faibles pour être couvrantes de TOUS les nombres ; et c'est exactement là-dessus qu'est basée ce que je pense être une démonstration : puisqu'on sait que le contraire (complémentaire) de l'ensemble vide, qui normalement est l'ensemble plein (i.e. tous les nombres, en l'occurrence ceux compris entre  $\sqrt{n}$  et  $n/2$ ), ne peut être plein parce qu'on a, je ne sais pas moi, sur 3 nombres consécutifs, toutes les classes de congruence modulo 3 qui sont couvertes, et que là, en souhaitant que le nombre ne soit ni congru à 0, ni congru à  $n$  selon tout  $p$  compris entre 3 et  $\sqrt{n}$ , on n'élimine que 2 classes au maximum (éventuellement confondues lorsque  $p$  est un diviseur de  $n$ ), on aboutit à une contradiction : on ne peut obtenir le "plein" avec seulement deux classes de congruences possibles selon tout  $p$  ou dit autrement, "on ne peut pas avoir tout le monde en n'ayant que 2 classes selon tout  $p$ , ça laissera des trous". Comme cette contradiction (provenant de "j'ai obtenu un plein qui ne peut pas être plein", qui est une proposition équivalente à "l'intersection des non congrus à 0 et non congrus à  $n$  selon tout  $p$  est vide"), eh bien, on en conclut que l'intersection des (non congrus à 0 et non congrus à  $n$  selon tout  $p$ ) n'est pas vide et comme cela a été démontré plus haut (voir mail de Leila), l'intersection en question (notée  $\cap F(p, n)$ ) contient un décomposant de Goldbach au moins (il a en effet été démontré dans le mail de Leila que l'intersection des ensembles de nombres qui ne sont ni congrus à 0 ni congrus à  $n$  selon tout  $p$  premier compris entre 3 et  $\sqrt{n}$  contient les décomposants de Goldbach de  $n$  qui sont compris entre  $\sqrt{n}$  et  $n/2$  et que cette intersection ne contient qu'eux).

Je trouve que ces échanges illustrent exactement ce que veut dire s'exprimer en langage mathématique : Leila Schneps emploie un langage très précis, ses assertions s'enchaînent logiquement de manière imparable.

Quant à moi, je me dis que peut-être que la conjecture fait finalement partie des énoncés indémontrables... Mais ça m'étonnerait.