Toujours trouver un nouveau couple de nombres premiers les plus proches possible (Denise Vella-Chemla, 8.2.16)

Il s'agit de démontrer que l'ensemble des couples de nombres premiers d'écart 2 est infini.

Le couple $(3, 5)$ fait partie de cet ensemble, ainsi que le couple $(41, 43)$.

Posons l'hypothèse que l'ensemble des couples de nombres premiers d'écart 2 est fini, i.e. qu'on a recensé tous les couples de tels nombres premiers (*les plus proches possible*).

Appelons le plus grand de ces couples (p_{petit}, p_{grand}).

Trouvons le plus petit entier naturel qui est solution de la disjonction combinatoire de systèmes de congruences suivante :

$$\begin{cases} x \equiv 0\ (6) \\ (x \equiv 0\ (5)) \vee (x \equiv 2\ (5)) \vee (x \equiv 3\ (5)) \\ (x \equiv 0\ (7)) \vee (x \equiv 2\ (7)) \vee (x \equiv 3\ (7)) \vee (x \equiv 4\ (7)) \vee (x \equiv 5\ (7)) \\ (x \equiv 0\ (11)) \vee (x \equiv 2\ (11)) \vee \ldots \vee (x \equiv 9\ (11)) \\ \ldots \\ (x \equiv 0\ (p_k)) \vee (x \equiv 2\ (p_k)) \vee \ldots \vee (x \equiv p_k - 2\ (p_k)) \\ \ldots \\ (x \equiv 0\ (p_{grand})) \vee (x \equiv 2\ (p_{grand})) \vee \ldots \vee (x \equiv p_{grand} - 2\ (p_{grand})) \end{cases}$$

Le théorème des restes chinois nous assure que chacun des systèmes de congruence de la disjonction de systèmes a une solution (les modules étant tous des nombres premiers).

On est ainsi à la recherche d'un nombre x multiple de 6 et congru à $0, 2, \ldots, p_k - 2$ selon tous les nombres premiers p_k compris au sens large entre 5 et p_{grand}. Appelons x_k le nombre auquel x doit être congru selon le module p_k.

Le nombre x est un nombre pair entre 2 nombres premiers d'écart 2.

En effet, le nombre qui le précède, appelons-le p'_{petit}, est congru à $1\ (2)$, à $2\ (3)$, et à $x_k - 1\ (p_k)$ pour tout p_k compris au sens large entre 5 et p_{grand}. Il est donc premier. Non. On n'est assuré qu'il est premier que s'il est compris entre p_{grand} et $(p_{grand})^2$, ce qui n'est pas forcément le cas, le théorème chinois garantissant seulement l'existence d'une solution inférieure à $\#p_{grand} = \prod_{p_k=2}^{p_{grand}} p_k$ (aussi appelée primorielle de p_{grand}) qui est très supérieure à $(p_{grand})^2$. Peut-être est-il possible de dire que la combinatoire des systèmes de congruence fournit $\prod_{5 \leqslant p_k \leqslant p_{grand}} (p_k - 2)$ solutions différentes et que l'une au moins de ces solutions doit obligatoirement appartenir à l'intervalle $[p_k, (p_k)^2]$ dans la mesure où $\dfrac{\prod p_k}{\prod (p_k - 2)}$ est toujours inférieur strictement à $(p_k)^2 - p_k$ mais un tel raisonnement ne peut se tenir que si l'on est sûr que les solutions sont bien équiréparties.

Le nombre qui le suit, appelons-le p'_{grand}, est quant à lui congru à $1\ (2)$, à $1\ (3)$, et à $x_k + 1\ (p_k)$ pour tout p_k compris au sens large entre 5 et p_{grand}. Il est donc premier également (même remarque : on n'est assuré de sa primalité que s'il est compris entre p_{grand} et $(p_{grand})^2$).

On a trouvé un nouveau couple (p'_{petit}, p'_{grand}) de nombres premiers d'écart 2, dont les deux nombres sont plus grands que p_{grand} qui était pourtant selon notre hypothèse le plus grand des nombres premiers les plus proches possible trouvé jusque là. L'hypothèse est contredite : on peut augmenter à l'infini la taille de l'ensemble des couples de nombres premiers les plus proches possible.