Tautologies (Denise Vella-Chemla, 22/11/2017)

On voudrait revenir sur le fait que les nombres premiers établissent certaines relations entre d'autres nombres.

Habituellement, on dit qu'un nombre est premier si seuls 1 et lui-même le divisent. Un nombre composé a un diviseur différent de 1 et lui-même. 15 est composé parce que 3 le divise.

Mais on pourrait aussi dire que 15 est composé parce que 3 divise 12, c'est équivalent au fait que 3 divise 15 puisque 12 est le complémentaire de 3 à 15, c'est surprenant parce qu'on énonce quelque chose sur 15 en parlant d'une relation entre 2 autres nombres que 15.

On pourrait aussi dire que 13 est premier parce que 2 ne divise pas 11 et 3 ne divise pas 10 et 4 ne divise pas 9 et 5 ne divise pas 8 et 6 ne divise pas 7, 13 est premier parce qu'aucun nombre de 2 à 6 ne divise son complémentaire à 13. Mais c'est fastidieux et on a l'habitude d'utiliser l'expression la plus courte possible, qui pourrait être qu'aucun nombre de 2 à 6 ne divise 13, mais que l'on raccourcit encore en disant qu'aucun nombre inférieur à la racine carrée de 13 ne le divise, i.e. ni 2 ni 3 ne divisent 13.

12	11	10	9	8	7
1	2	3	4	5	6

Un nombre p premier est caractérisé par le fait qu'il a exactement $\frac{p-1}{2}$ résidus quadratiques (les nombres premiers maximisent le nombre de résidus quadratiques, tous les nombres de 1 à $\frac{p-1}{2}$ ayant des carrés différents modulo p).

Pour les nombres composés, soit il y a des redondances parmi les carrés, soit il y a des carrés nuls (par exemple pour 9), ce qui dans les deux cas rend le nombre de résidus quadratiques strictement inférieur à $\frac{p-1}{2}$.

14	13	12	11	10	9	8
1	2	3	4	5	6	7
1	4	9	1	10	6	4

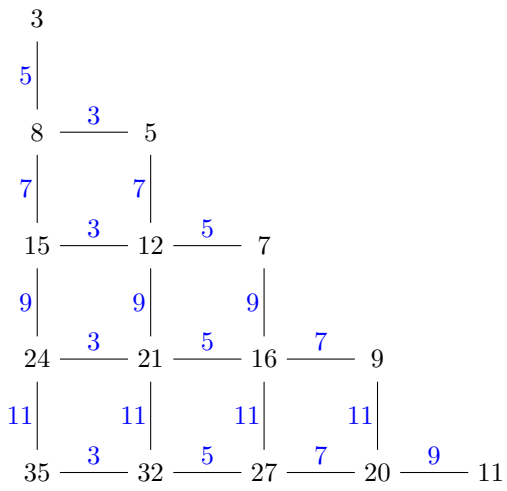
On voit dans la table que, selon le module 15, 4 et 1 ont même carré, ou bien encore 7 et 2. En effet, 15 divise $4^2 - 1^2 = (4-1)(4+1) = 3 \times 5$ ou bien 15 divise $7^2 - 2^2 = (7-2)(7+2) = 5 \times 9$.

Ca semble un peu particulier de dire que 15 est composé parce qu'il divise 3×5 ou encore parce qu'il divise 5×9 mais le fait est là, tous ces énoncés sont équivalents : 15 divise un produit de la forme $(a-b)(a+b)$ avec $1 \leqslant a < b \leqslant \frac{15-1}{2}$, ce qui équivaut au fait que 15 n'a pas $\frac{15-1}{2}$ résidus quadratiques, ce qui équivaut au fait que 15 est composé. Une redondance de carrés est équivalente à la composition du nombre mais une non-redondance de carrés ne garantit pas que le nombre est premier (existent deux carrés égaux modulo 15 et 15 est composé mais tous les carrés sont différents pour 6 ou pour 9 et 6 est composé, ou 9 est composé aussi).

On peut être exhaustif et envisager toutes les redondances éventuelles pour 13 (il y en a 21) :

$(1,2) \rightarrow 1 \times 3 = 3$
$(1,3) \rightarrow 2 \times 4 = 8$ $(2,3) \rightarrow 1 \times 5 = 5$
$(1,4) \rightarrow 3 \times 5 = 15$ $(2,4) \rightarrow 2 \times 6 = 12$ $(3,4) \rightarrow 1 \times 7 = 7$
$(1,5) \rightarrow 4 \times 6 = 24$ $(2,5) \rightarrow 3 \times 7 = 21$ $(3,5) \rightarrow 2 \times 8 = 16$ $(4,5) \rightarrow 1 \times 9 = 9$
$(1,6) \rightarrow 5 \times 7 = 35$ $(2,6) \rightarrow 4 \times 8 = 32$ $(3,6) \rightarrow 3 \times 9 = 27$ $(4,6) \rightarrow 2 \times 10 = 20$ $(5,6) \rightarrow 1 \times 11 = 11$

13 est premier car il ne divise aucun des produits : il s'agit de produits de deux nombres différents, compris entre 1 et 11, et de différence paire. Notons dans le diagramme ci-dessous les écarts entre ces produits :



On rencontre un problème ici car, si on arrive à éliminer les nombres composés ou puissances de premiers, caractérisés par le fait que l'un des carrés est nul lorsqu'on les prend comme modules, on n'arrive pas à distinguer les doubles de premiers des nombres premiers eux-mêmes, pour qui tous les carrés sont différents et non nuls.