Carrés points fixes des nombres composés (Denise Vella-Chemla, 29/11/2017)

On découvre à la recherche de points fixes dans les tables de résiduosité quadratique qu'on peut distinguer les nombres composés n avec ou sans facteur carré en cherchant deux carrés particuliers modulo n de la façon suivante :

- si n est un nombre composé qui n'est pas une puissance de premier, on trouve toujours modulo n deux entiers consécutifs a et $a+1$, inférieurs ou égaux à $\left\lfloor \frac{n-1}{2} \right\rfloor$ qui ont pour carré l'un lui-même et l'autre son complément à n ; n divise le produit de ces deux nombres ; les deux nombres consécutifs en question vérifient deux équations quadratiques équivalentes modulo n ;
- si n est un nombre composé puissance de premier, un nombre inférieur ou égal à $\left\lfloor \frac{n-1}{2} \right\rfloor$ est de carré nul et on ne semble pas trouver de points fixes tels que notés ci-dessus.

On fournit ci-dessous les nombres consécutifs pour les composés sans facteur carré inférieurs à 100.

$15 : 5, 6$
$21 : 6, 7$
$33 : 11, 12$
$35 : 14, 15$
$39 : 12, 13$
$45 : 9, 10$
$51 : 17, 18$
$55 : 10, 11$
$57 : 18, 19$
$65 : 25, 26$
$69 : 23, 24$
$77 : 21, 22$
$85 : 34, 35$
$87 : 29, 30$
$91 : 13, 14$
$93 : 30, 31$
$95 : 19, 20$

Par programme, on vérifie que :

- les nombres premiers (qu'ils soient de la forme $4k+1$ ou $4k+3$) n'ont pas de carrés points fixes ; si on identifie x à $p-x$ (si on quotiente par une relation $x \equiv p-x$), modulo les premiers $4k+3$, l'élévation au carré réalise simplement une permutation des nombres inférieurs ou égaux à $(p-1)/2$ tandis que modulo les premiers $4k+1$, l'élévation au carré associe une même image aux nombres 2 par 2 (modulo 11, on a la permutation $\{1 \to 1, 2 \to 4, 3 \to 2, 4 \to 5, 5 \to 3\}$ tandis que modulo 17, on a $\{1 \to 1, 2 \to 4, 3 \to 8, 4 \to 1, 5 \to 8, 6 \to 2, 7 \to 2, 8 \to 4\}$ (i.e. 1 et 4 ont même image, 2 et 8 ont même image, 3 et 5 idem, et 6 et 7 idem) ;
- les nombres composés peuvent être classés selon trois sortes différentes ; les puissances d'un seul premier modulo lesquelles un nombre au moins est de carré nul mais modulo lesquelles il n'y a aucun carré fixe ; les puissances produits de plusieurs premiers modulo lesquelles un nombre au moins est de carré nul et modulo lesquelles certains carrés sont fixes (et vont deux par deux nombres consécutifs) et enfin, les nombres composés n'ayant aucun facteur carré modulo lesquels il y aura des nombres fixes par l'élévation au carré (allant par deux consécutivement) mais modulo lesquels aucun nombre ne sera de carré nul.