Nombre de solutions de l'équation $x^4 \equiv 1\ (mod\ n)$ pour n impair (Denise Vella-Chemla, 15/12/2017)

On compte les racines comprises entre 1 et $n-1$ de l'équation modulaire $x^4 \equiv 1\ (mod\ n)$. On note les entiers n pour lesquels le nombre de racines augmente strictement.

Il y a :

- ⋆ 2 solutions pour $n = 3$;
- ⋆ 4 solutions pour $n = 5$;
- ⋆ 8 solutions pour $n = 15 = 3.5$;
- ⋆ 16 solutions pour $n = 65 = 13.5$;
- ⋆ 32 solutions pour $n = 195 = 13.5.3$;
- ⋆ 64 solutions pour $n = 1105 = 17.13.5$;
- ⋆ 128 solutions pour $n = 3315 = 17.13.5.3$;

Note : ci-dessous, on utilisera toujours la lettre k mais il faudrait idéalement utiliser des k', k'', k''', etc.

On comprend les augmentations strictes ainsi ; on observe les facteurs des factorisations successives : $4k+3$ pour 3, $4k+1$ pour 5, $(4k+1).(4k+3)$ pour 15, 2 facteurs $4k+1$ pour 65, 2 facteurs $4k+1$ et un facteur $4k+3$ pour 195, 3 facteurs $4k+1$ pour 1105 et 3 facteurs $4k+1$ et un facteur $4k+3$ pour 3315. Il semble donc qu'il y ait augmentation stricte soit lors de l'ajout d'un facteur $4k+3$, soit lors de la transformation d'un facteur $4k+3$ en un facteur $4k+1$.

Pourquoi y-a-t-il deux fois plus de racines biquadratiques de 1 quand on passe d'un facteur $4k+3$ à un facteur $4k+1$?

-1 est un carré modulo tout nombre premier de la forme $4k+1$ mais n'est pas un carré modulo tout nombre premier de la forme $4k+3$. De ce fait, les nombres qui ont comme carré -1 sont racines de l'équation $x^4 \equiv 1\ (mod\ p)$ des seuls nombres premiers p de la forme $4k+1$ mais ne sont pas racines de cette équation pour les nombres premiers p de la forme $4k+3$. Le nombre de solutions de l'équation $x^4 \equiv 1\ (mod\ p)$ est égal à 2 pour les nombres premiers de la forme $4k+3$ tandis qu'il est égal à 4 pour les nombres premiers de la forme $4k+1$.

On obtient le nombre de solutions de l'équation $x^4 \equiv 1\ (mod\ n)$ pour un nombre n composé en comptant le nombre de facteurs de chaque sorte ($4k+1$ ou $4k+3$) dans sa factorisation $n = \prod_k p_k^{\alpha_k}$ et en multipliant les nombres de solutions dans les différents anneaux $\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$ entre eux. La formule générale pour le nombre de racines quatrièmes de 1 dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ est :

$$4 \times \ nombre\ de\ facteurs\ de\ la\ forme\ 4k+1\ de\ n\ +\ 2 \times \ nombre\ de\ facteurs\ de\ la\ forme\ 4k+3\ de\ n.$$

Résultats de mathématiques expérimentales

On réutilise notre programme Python pour calculer les augmentations strictes du nombre de racines troisièmes de 1 dans $\mathbb{Z}/n\mathbb{Z}$, n impair, puis du nombre de racines cinquièmes de 1, puis du nombre de points fixes $x^5 = x$ dans ces anneaux.

1) $x^3 = 1$

$3 \rightarrow 1$
$7 \rightarrow 3$
$63 \rightarrow 9$
$819 = 3.7.13 \rightarrow 27$
$15561 = 3.7.13.19 \rightarrow 81$

2) $x^5 = 1$

$3 \to 1$
$11 \to 5$
$275 = 5.11 \to 25$
$8525 = 5.11.31 \to 125$
$(69905 = 5.11.31.41 \to 125)$
$4963255 = 5.11.31.41.71 \to 625$
$501288755 = 5.11.31.41.71.101 \to 3125$

Note : On a mis 69905 parce qu'on était sûre que ça augmenterait strictement et ça ne l'a pas fait !

3) $x^5 = x$

On fait apparaître les primorielles en bleu.

$3 \to 2$
$5 \to 4$
$15 = 3.5 \to 14$
$65 = 5.13 \to 24$
$105 = 3.5.7 \to 44$
$195 = 3.5.13 \to 74$
$1105 = 5.13.17 \to 124$
$1155 = 3.5.7.11 \to 134$
$1365 = 3.5.7.13 \to 224$
$3315 = 3.5.13.17 \to 374$
$15015 = 3.5.7.11.13 \to 674$
$23205 = 3.5.7.13.17 \to 1124$