*Nombre de solutions de l'équation $x^2 = x \ (mod\ n)$ pour n impair (3/12/2017)*

Soit $n$ un nombre impair alors le nombre de solutions de l'équation $x^2 = x \ (mod\ n)$ est égal à $2^k$ avec $k$ le nombre de facteurs premiers de la factorisation de $n$.

On a $n = \prod_k p_j^{\alpha_j}$. $\mathbb{Z}/n\mathbb{Z}$ est isomorphe au produit des $\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$. Les solutions de l'équation $x^2 = x \ (mod\ n)$ sont données en prenant pour chaque $p_j$ une solution de l'équation $x^2 = x$ dans l'anneau $\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$. Il y en a 2 : 0 et 1. Pour trouver les solutions dans $\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$, on regarde le résidu $r$ dans $\mathbb{F}_{p_j}$. Comme $\mathbb{F}_{p_j}$ est un corps, $r = 0$ ou $r = 1$.

- si $r = 0$, $x = 0$ car la valuation $v$ de $x$ (la plus petite puissance de $p_j$ qui divise $x$) ne peut être égale à $2v$ sans être nulle ;
- si $r = 1$, on écrit $x = 1 + y$ et on a $(1 + y)^2 = 1 + y$ d'où $y^2 + y = 0$ et on a $y = 0$ car la valuation amène à une contradiction si $y$ n'est pas nul.