Nombre de solutions de l'équation $x^2 = 1\ (mod\ n)$ pour n impair (Denise Vella-Chemla, 4/12/2017)

Les nombres premiers et leurs puissances sont les seuls nombres impairs modulo lesquels la seule racine de 1 est 1.

Selon (modulo) les modules impairs composés notés n qui ne sont pas des puissances de premiers, le nombre de racines de 1 modulo n comprises entre 1 et $n-1$ est 2^k avec k le nombre de facteurs premiers de la factorisation de n.

L'explication conceptuelle de ce phénomène est trouvée en considérant que résoudre l'équation $x^2 = 1\ (mod\ n)$ est équivalent à résoudre l'équation $(x-1)(x+1) = 1\ (mod\ n)$, i.e. à trouver dans la réunion des facteurs des factorisations de $x-1$ et $x+1$ l'ensemble complet des facteurs de n. On imagine qu'il y a autant de manières différentes de réaliser cette "séparation des facteurs de n" en deux ensembles, l'un inclus dans l'ensemble des facteurs de $x-1$ et l'autre inclus dans l'ensemble des facteurs de $x+1$ que d'affecter des booléens, autant que de facteurs différents de n, chacun de ces booléens valant 0 ou 1 selon que le facteur va être retrouvé dans la décomposition de $x-1$ ou dans celle de $x+1$. C'est pour cette raison que le nombre de racines de 1 modulo n comprises entre 1 et $n-1$ est 2^k avec k le nombre de facteurs premiers de la factorisation de n.