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 1 a deux racines carrées : 1 et -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 $n-1$ semble au premier abord être égal à 2^k avec k le nombre de facteurs premiers de la factorisation de n.

L'analyse des racines carrées modulaires de 1 pour le nombre $n = 66563$ montre qu'il faut bien différencier la factorisation du prédécesseur de 66563 (66562) de celle du successeur de 66563 (66564) (i.e. l'ordre dans lequel sont considérés ces deux nombres n'est pas indifférent).

$66563 = 7.37.257$ a une factorisation contenant trois facteurs premiers distincts.
Les racines de 1 modulo 66563 sont 258, 28526, 28785, 37778, 38037 et 66305.
Ecrivons les factorisations des prédécesseurs et successeurs de ces nombres pour comprendre l'association des $2^3 = 8$ chaînes de 3 booléens aux racines de 1 (i.e. à leur prédécesseur et successeur) : le premier booléen des chaînes correspond à l'appartenance de 7 à la factorisation du prédécesseur, le second booléen à l'appartenance de 37 à la factorisation du prédécesseur et le troisième à l'appartenance de 257 à la factorisation du prédécesseur :
257 et $259 = 7.37$ correspondent à la chaîne de 3 booléens 001 (257 "est à gauche").
$28525 = 5^2.7.163$ et $28527 = 3.37.257$ correspondent à la chaîne 100 (7 "est à gauche").
$28784 = 2^4.7.257$ et $28786 = 2.37.389$ correspondent à la chaîne 101 (7 et 257 "sont à gauche").
$37777 = 37.1021$ et $37779 = 3.7^2.257$ correspondent à la chaîne 010 (37 "est à gauche").
$38036 = 2^2.37.257$ et $38038 = 2.7.11.13.19$ correspondent à la chaîne 011 (37 et 257 "sont à gauche").
$66304 = 2^8.7.37$ et $66306 = 2.3.43.257$ correspondent à la chaîne 110 (7 et 37 "sont à gauche").

Remarque : Les nombres de carré modulaire fixe et les nombres de carré modulaire 1 se déduisent les uns des autres par la transformation $y = 2x - 1$ et sa transformation inverse $x = \frac{y+1}{2}$ ainsi :

- si $x^2 = x$ et $y = 2x - 1$ alors $x^2 - x = 0$ et $y^2 = 4x^2 - 4x + 1 = 4(x^2 - x) + 1 = 1$;
- si $y^2 = 1$ et $x = \frac{y+1}{2}$ alors $x^2 = \left(\frac{y+1}{2}\right)^2 = \frac{1+2y+y^2}{4} = \frac{2+2y}{4} = \frac{1+y}{2} = x$.

Exemples :
1) $12^2 = 12$ (*mod* 33) $\iff$ $23^2 = 1$ (*mod* 33).
2) $19^2 = 1$ (*mod* 45) $\iff$ $10^2 = 10$ (*mod* 45).