Résumé de l'article de Lehmer sur le nombre de résidus quadratiques d'un nombre quelconque (Denise Vella-Chemla, mai 2023)

Pour trouver le nombre de résidus quadratiques d'un nombre quelconque, on le factorise, on trouve le nombre des résidus quadratiques de chacune des puissances de premiers intervenant dans sa factorisation, et on multiplie les résultats.

Le nombre de résidus quadratiques de 2 est 2.

Le nombre de résidus quadratiques d'un nombre premier impair p est $\frac{p+1}{2}$.

Le nombre de résidus quadratiques d'une puissance 2^α non nulle de 2 est égal à :

$$\begin{cases} \frac{2^{\alpha-1}+4}{3} & \text{si } \alpha \text{ est pair ;} \\ \frac{2^{\alpha-1}+5}{3} & \text{si } \alpha \text{ est impair.} \end{cases}$$

Le nombre de résidus quadratiques d'une puissance p^α non nulle d'un nombre premier impair p est égal à :

$$\begin{cases} \frac{p^{\alpha+1}-p}{2(p+1)}+1 & \text{si } \alpha \text{ est pair ;} \\ \frac{p^{\alpha+1}-1}{2(p+1)}+1 & \text{si } \alpha \text{ est impair.} \end{cases}$$

Exemple : Pour $98 = 2.7^2$, le nombre de résidus quadratiques est

$$\begin{aligned} \#RQ &= 2 \times \left(\frac{7^3-7}{2(7+1)}+1\right) \\ &= 2 \times \left(\frac{336}{2\times 8}+1\right) \\ &= 2 \times 22 = 44. \end{aligned}$$

Les résidus quadratiques sont : 0, 1, 2, 4, 8, 9, 11, 15, 16, 18, 22, 23, 25, 29, 30, 32, 36, 37, 39, 43, 44, 46, (49), 50, 51, 53, 57, 58, 60, 64, 65, 67, 71, 72, 74, 78, 79, 81, 85, 86, 88, 92, 93, 95.

Observer la récurrence du "motif" de longueur 7 : R R N R N N N (R signifiant Résidu quadratique, et N signifiant non-résidu quadratique, voir les Recherches arithmétiques de Gauss, à l'origine de cette notion).