La machine des frères Carissan

Pour factoriser des grands nombres premiers, Fermat proposa au XVII^{e} siècle la méthode suivante :

N étant impair et produit des nombres entiers a et b, chercher a et b revient à chercher les entiers x et y tel que : $x = (a + b) / 2$ et $y = (a – b) / 2$. Ce changement d'inconnues permet alors d'écrire : $N = (x + y) (x – y) = x^2 – y^2$. Factoriser N revient dans ces conditions à chercher un entier naturel x plus grand que $\sqrt{N}$ tel que $x^2 – N$ est un carré.

Exemple : N = 25807. On commencera à chercher x tel que x^2 est supérieur à N.
La première valeur à prendre en compte sera donc 161 qui conduit à $y^2 = x^2 – N = 114$ qui n'est pas le carré d'un entier. En continuant :
$x = 162$ donne $y^2 = x^2 – N = 437$
$x = 163$ donne $y^2 = x^2 – N = 762$
$x = 164$ donne $y^2 = x^2 – N = 1089$ qui est le carré de 33. Ainsi en 4 étapes on trouve :
$N = (164 + 33) (164 – 33) = 197 \times 131$.

Cette méthode est très efficace mais il a fallu attendre le début du XX^{e} siècle pour que les frères Carissan (Pierre et Eugène) fassent intervenir les congruences et construisent alors une machine qui évite d'extraire des racines carrées à la chaîne.

L'idée est la suivante :
Si par exemple x est congru à 0, 1, 2, 3, 4, 5, 6 modulo 7 alors son carré est congru à 0, 1, 4, 2, 2, 4, 1. Par conséquent seuls les nombres congrus à 0,1, 2 ou 4 peuvent être des carrés : c'est ce qu'on appelle les résidus quadratiques. On a bien sûr ici une condition nécessaire mais pas suffisante.

Si on reprend la méthode précédente avec N = 202511 alors on peut remarquer que :
$x^2 – 202511 \equiv x^2 – 1$ (modulo 7).
Pour que $x^2 – 1$ soit un carré il faut donc que $x^2 – 1$ soit congru à 0, 1, 2 ou 4 ou encore que x^2 soit congru à 1, 2, 3 ou 5. Mais x^2 est lui-même un carré donc seuls 1 et 2 obtenus pour x valant 1, 3, 4 ou 6 sont acceptables.

De même si x est congru à 0, 1, 2, 3, 4, 5, 6, 7, 8 modulo 9 alors x^2 est congru à 0, 1, 4, 0, 7, 7, 0, 4 et 1. On a alors $x^2 – 202511 \equiv x^2 – 2$ (modulo 9) et pour que $x^2 – 2$ soit un carré il faut donc que x^2 soit congru à 0, 2, 3, 6 et à 0, 1, 4 ou 7. Seule la valeur 0 est acceptable, elle est obtenue pour x = 0, 3 ou 6.
De même les valeurs acceptables « modulo 15 » sont 0, 6 et 9.

La machine des frères Carissan est formée d'un disque comprenant des couronnes où se trouvent les suites des restes modulo 7, 9 et 15. On marque par des picots les valeurs acceptables (nombres de couleur bleue dans l'applet joint) et on positionne les couronnes pour la première valeur de x telle que x^2 soit supérieur à 202511, c'est à dire 451. Par une manivelle on incrémente les restes modulo 7, 9 et 15 et on s'arrête chaque fois que l'on obtient des valeurs acceptables.
La première position est 1-6-6 mais cela ne marche par car $x^2 – 202511 = 5425$ n'est pas un carré. Même chose pour la seconde 4-0-9 car $x^2 – 202511 = 8170$, même chose pour 3-6-0 car $x^2 – 202511 = 13714$. Enfin à la position 4-3-0 on trouve $x^2 – 202511 = 480^2 – 202511 = 167^2$.
Ainsi $202511 = (480 + 167) (480 – 167) = 647 \times 313$.

En fait la machine était formée de 14 couronnes correspondantes aux valeurs 19, 21, 23, 26, 29, 31, 34, 37, 41, 43, 47, 53, 55 et 59.

Bibliographie :
F . Morain, La machine de Carissan, Pour la science de janvier 1998,
http://www.pourlascience.com/numeros/pls-243/presence.htm
J. Buchmann, La factorisation des grands nombres, Pour la science n°251 de septembre 1998,
http://www.pourlascience.com/numeros/pls-251/art-12.htm
M. Bühler, IREM Paris VII,
http://www2.ac-lille.fr/apmep/les_ateliers/Ma01_Buhler.pdf