Un ensemble, une transformation, des traces (Denise Vella-Chemla, 10.7.2019)

On se place dans un ensemble très particulier ; il s'agit de l'ensemble des matrices booléennes qui sont puissances de la matrice suivante :

$$G = \begin{pmatrix}
0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 0 & 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 0 & 0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 1 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 1 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 0 & 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 1 & 0 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 1 & 0 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 1 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 1 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 0 & 1 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 1 & 0 & 0 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots
\end{pmatrix}$$

Cette matrice est infinie, elle contient sur sa diagonale des matrices circulantes de taille 2×2, 3×3, 4×4, etc.

On a une opération : l'élévation à la puissance de la matrice ci-dessus qui nous fait atteindre certaines matrices carrées booléennes et pas d'autres.

Une simple étude nous fait comprendre que la trace de la matrice atteinte par élévation à la puissance k de la matrice G permet de caractériser si k est premier ou non.

En effet, on a p est premier $\iff Trace(G^p) = p$.

Quand on élève une matrice circulante de taille $k \times k$ à la puissance k, tous ses 1 s'alignent bien sur la diagonale pour obtenir la matrice Identité de taille k. Il en sera de même des 1 appartenant aux matrices circulantes de taille les diviseurs de k si k est composé.

La complexité d'un tel algorithme pour caractériser la primalité d'un nombre étant de l'ordre de n^7 (en considérant la taille d'une matrice - en $\frac{n(n+1)}{2}$ -, le coût d'une multiplication matricielle en n^3, etc.), elle est complètement prohibitive. L'intérêt de cette idée est peut-être simplement de caractériser la primalité par certaines traces matricielles.

Cette méthode n'utilise qu'un ensemble (celui des matrices booléennes carrées à blocs de matrices circulantes sur leur diagonale) et une transformation (l'élévation d'une matrice à une certaine puissance) ; la transformation en question fait sortir de ou entrer dans l'ensemble des nombres premiers suivant le nombre (l'exposant de G) considéré.