Multiplication binaire et factorisation

Position du problème

On cherche un système dynamique discret qui, étant donné un entier non-premier, trouve un de ses diviseurs. On se base sur la multiplication binaire. En effet, on observe qu'une matrice à coefficients dans $\{0, 1\}$ peut s'interpréter comme une multiplication binaire si ses lignes non-nulles sont égales entre elles, comme illustré dans la figure 1. Les colonnes non-nulles sont alors aussi égales entre elles, et les deux facteurs de la multiplication sont alors lisibles, en base 2, sur les lignes non-nulles pour l'un, et les colonnes non-nulles lues de bas en haut pour l'autre. Si on pose leur multiplication, toujours en base 2, on retrouve en effet la matrice de départ, décalée par les retenues (cf. Figure 1).

1	0	1	1
0	0	0	0
1	0	1	1
1	0	1	1

					1	0	1	1	×
					1	0	1	1	1
+				0	0	0	0	.	0
+			1	0	1	1	.	.	1
+		1	0	1	1	.	.	.	1
	1	0	0	0	1	1	1	1	

FIGURE 1 – La matrice de gauche s'interprète comme la multiplication de 11 (1011 horizontalement) par 13 (1101 verticalement, de haut en bas).

Par ailleurs, étant donné une matrice M à coefficients dans $\{0, 1\}$, on pose $\sigma(M)$ l'entier obtenu en sommant ses lignes décalées par des retenues (cf. Figure 2). Si M représente une multiplication, σ est par construction le produit.
L'idée est donc de partir d'une matrice à coefficients dans $\{0, 1\}$ pour laquelle σ vaut le nombre qu'on cherche à factoriser, et de lui appliquer des transformations qui conservent σ jusqu'à atteindre une matrice qui représente une multiplication.

$$M = \begin{matrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{matrix} \qquad \sigma(M) = \begin{array}{cccccccc} & & & 1 & 1 & 0 & 1 & \\ + & & 0 & 0 & 1 & 1 & . & \\ + & 1 & 0 & 0 & 1 & . & . & \\ \hline & 1 & 1 & 0 & 1 & 1 & 1 & \end{array} = 63$$

FIGURE 2 – Exemple de calcul de σ.