Matrices du groupe affine... (Denise Vella-Chemla, 5.2.2019)

On continue de travailler sur la représentation des nombres par des matrices du groupe affine à coefficients dans les corps premiers.

On fournit dans le tableau ci-dessous les matrices associées aux nombres impairs de 3 à 99, dans le but d'observer une caractérisation des nombres premiers.

A un nombre, sont associées autant de matrices qu'il y a de nombres premiers impairs inférieurs à la racine carrée de ce nombre. Ces matrices sont de la forme :

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

avec a et b appartenant aux différents $\mathbb{Z}/p_k\mathbb{Z}$ notés en tête des colonnes.

Pour alléger la présentation, on omet les coefficients bas des matrices, toujours égaux à 0 et 1. On affecte une matrice à 3, 5, 7 bien qu'il n'y ait pas de nombre premier impair inférieur à leur racine, pour éviter de leur affecter un ensemble de matrices vide.

On observe bien une cyclicité de longueur $18(= 2 \times 3^2)$ dans $\mathbb{Z}/3\mathbb{Z}$ (*nota* : elle est en fait de longueur 9 mais on la voit de 18 ici car on a omis les nombres pairs dans le tableau) : cette cyclicité est telle qu'à 21 est associée la même matrice qu'à 3 ou bien à 35 est associée la même matrice qu'à 17. Cette cyclicité est d'écart $50(= 2 \times 5^2)$ dans la colonne de $\mathbb{Z}/5\mathbb{Z}$, etc.

Une condition nécessaire et suffisante pour qu'un nombre supérieur à 3 soit premier est comme attendu qu'aucun des coefficients b d'aucune de ses matrices associées ne soit nul (ces coefficients sont colorés en bleu pour les nombres premiers supérieurs à 3).

n	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	n	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	n	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$
3	(1 0)			37	(0 1)	(2 2)		71	(2 2)	(4 1)	(3 1)
5	(1 2)			39	(1 0)	(2 4)		73	(0 1)	(4 3)	(3 3)
7	(2 1)			41	(1 2)	(3 1)		75	(1 0)	(0 0)	(3 5)
9	(0 0)			43	(2 1)	(3 3)		77	(1 2)	(0 2)	(4 0)
11	(0 2)			45	(0 0)	(4 0)		79	(2 1)	(0 4)	(4 2)
13	(1 1)			47	(0 2)	(4 2)		81	(0 0)	(1 1)	(4 4)
15	(2 0)			49	(1 1)	(4 4)	(0 0)	83	(0 2)	(1 3)	(4 6)
17	(2 2)			51	(2 0)	(0 1)	(0 2)	85	(1 1)	(2 0)	(5 1)
19	(0 1)			53	(2 2)	(0 3)	(0 4)	87	(2 0)	(2 2)	(5 3)
21	(1 0)			55	(0 1)	(1 0)	(0 6)	89	(2 2)	(2 4)	(5 5)
23	(1 2)			57	(1 0)	(1 2)	(1 1)	91	(0 1)	(3 1)	(6 0)
25	(2 1)	(0 0)		59	(1 2)	(1 4)	(1 3)	93	(1 0)	(3 3)	(6 2)
27	(0 0)	(0 2)		61	(2 1)	(2 1)	(1 5)	95	(1 2)	(4 0)	(6 4)
29	(0 2)	(0 4)		63	(0 0)	(2 3)	(2 0)	97	(2 1)	(4 2)	(6 6)
31	(1 1)	(1 1)		65	(0 2)	(3 0)	(2 2)	99	(0 0)	(4 4)	(0 1)
33	(2 0)	(1 3)		67	(1 1)	(3 2)	(2 4)				
35	(2 2)	(2 0)		69	(2 0)	(3 4)	(2 6)				

Notre problème ici est qu'il est spécifié dans la littérature que le coefficient a (en haut à gauche des matrices 2×2, ou à gauche des couples correspondant aux premières lignes des matrices dans le tableau) ne doit pas être nul mais alors on ne voit pas quoi associer comme matrices aux nombres qui posent ce problème du a nul (comme 37 ou 81 par exemple).

Le *Snurpf*[1] qu'on avait proposé pour représenter les nombres était plus simple (représenter chaque nombre par la suite de ses représentations dans les différents corps premiers pour les nombres premiers inférieurs à sa racine) et on avait la même condition nécessaire et suffisante (aucune classe nulle, qui correspondait aux coefficients b ici, ou restes des divisions euclidiennes) pour qu'un nombre soit premier. Les cycles étaient dans chaque corps $\mathbb{Z}/p_k\mathbb{Z}$ de longueur p_k au lieu d'être de longueur p_k^2 dans la mesure où seul le reste était pris en compte (ici, reste et quotient sont pris en compte, d'où le carré pour la combinatoire).

Continuons cependant à la recherche d'une modélisation convenable.

1. *Système de Numération par les Restes dans les Parties Finies de* $\mathbb{N}$.

On aimerait, idéalement, “agréger” toutes les matrices associées à un nombre en une seule matrice qui résumerait l'information associée à ce nombre.

On rappelle que c'est la présence d'un $b = 0$ qui correspond à la divisibilité par un nombre premier. Voyons d'abord la non-commutativité de la multiplication matricielle à l'oeuvre sur un exemple : si on multiplie à droite ou bien à gauche par une matrice ayant un coefficient nul en haut à droite, on n'obtient pas le même résultat [2].

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab' \\ 0 & 1 \end{pmatrix}$$

alors que

$$\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a'a & b' \\ 0 & 1 \end{pmatrix}$$

Un moyen d'obtenir que la divisibilité par un nombre premier (le fait d'être composé) absorde toute autre information, du fait de l'ordre très particulier dans lequel s'effectue les calculs intermédiaire d'une multiplication matricielle, serait d'intervertir les positions des coefficients a et b. On aurait alors :

$$\begin{pmatrix} 0 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b' & a' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & 1 \end{pmatrix}$$

On corrige le tableau en conséquence et on associe à chaque nombre le produit de ses matrices (colonnes Π). La multiplication par une matrice indiquant qu'un nombre est composé est absorbante, qu'elle s'effectue à droite ou à gauche, en ce qui concerne le coefficient en haut à gauche des matrices.

En effet, on a :

$$\begin{pmatrix} 0 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b' & a' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & 1 \end{pmatrix}$$

et

$$\begin{pmatrix} b' & a' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & b'a + a' \\ 0 & 1 \end{pmatrix}$$

2. Lors de ma scolarité élémentaire “maths modernes”, on nous faisait utiliser des “moulinettes”, par exemple la moulinette $f(x) = 3x + 2$ et la moulinette $g(x) = 8x + 4$ et l'on attirait notre attention sur le fait que l'application de 2 moulinettes successives faisait qu'on n'obtenait pas obligatoirement le même résultat suivant l'ordre d'application : la composition de deux fonctions affines est non-commutative. $(f \circ g)(x) \neq (g \circ f)(x)$. Par exemple, pour $x = 6$, on a $8 \times (3 \times 6 + 2) + 4 = 164$ qui est différent de $3 \times (8 \times 6 + 4) + 2 = 158$. Il faut pour que les matrices commutent que leurs coefficients vérifient : $ab' + b = a'b + b'$.

n	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	Π	n	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	Π	n	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	Π
3	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$ (ou $\emptyset$)			$\begin{pmatrix}0&1\\0&1\end{pmatrix}$ (ou $\emptyset$)	37	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$		$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	71	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	$\begin{pmatrix}1&4\\0&1\end{pmatrix}$	$\begin{pmatrix}1&3\\0&1\end{pmatrix}$	$\begin{pmatrix}2&16\\0&1\end{pmatrix}$
5	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$ (ou $\emptyset$)			$\begin{pmatrix}2&1\\0&1\end{pmatrix}$ (ou $\emptyset$)	39	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	$\begin{pmatrix}4&2\\0&1\end{pmatrix}$		$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	73	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}3&4\\0&1\end{pmatrix}$	$\begin{pmatrix}3&3\\0&1\end{pmatrix}$	$\begin{pmatrix}9&13\\0&1\end{pmatrix}$
7	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$ (ou $\emptyset$)			$\begin{pmatrix}1&2\\0&1\end{pmatrix}$ (ou $\emptyset$)	41	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&3\\0&1\end{pmatrix}$		$\begin{pmatrix}2&7\\0&1\end{pmatrix}$	75	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}5&3\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$
9	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$			$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	43	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	$\begin{pmatrix}3&3\\0&1\end{pmatrix}$		$\begin{pmatrix}3&5\\0&1\end{pmatrix}$	77	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&4\\0&1\end{pmatrix}$	$\begin{pmatrix}0&17\\0&1\end{pmatrix}$
11	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$			$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	45	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&4\\0&1\end{pmatrix}$		$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	79	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	$\begin{pmatrix}4&0\\0&1\end{pmatrix}$	$\begin{pmatrix}2&4\\0&1\end{pmatrix}$	$\begin{pmatrix}8&18\\0&1\end{pmatrix}$
13	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$			$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	47	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	$\begin{pmatrix}2&4\\0&1\end{pmatrix}$		$\begin{pmatrix}4&8\\0&1\end{pmatrix}$	81	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}4&4\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$
15	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$			$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	49	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}4&4\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&5\\0&1\end{pmatrix}$	83	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	$\begin{pmatrix}3&1\\0&1\end{pmatrix}$	$\begin{pmatrix}6&4\\0&1\end{pmatrix}$	$\begin{pmatrix}36&26\\0&1\end{pmatrix}$
17	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$			$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	51	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	85	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	$\begin{pmatrix}1&5\\0&1\end{pmatrix}$	$\begin{pmatrix}0&3\\0&1\end{pmatrix}$
19	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$			$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	53	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	$\begin{pmatrix}3&0\\0&1\end{pmatrix}$	$\begin{pmatrix}4&0\\0&1\end{pmatrix}$	$\begin{pmatrix}24&2\\0&1\end{pmatrix}$	87	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	$\begin{pmatrix}3&5\\0&1\end{pmatrix}$	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$
21	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$			$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	55	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	$\begin{pmatrix}6&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	89	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	$\begin{pmatrix}4&2\\0&1\end{pmatrix}$	$\begin{pmatrix}5&5\\0&1\end{pmatrix}$	$\begin{pmatrix}40&46\\0&1\end{pmatrix}$
23	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$			$\begin{pmatrix}2&1\\0&1\end{pmatrix}$	57	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	91	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&3\\0&1\end{pmatrix}$	$\begin{pmatrix}0&6\\0&1\end{pmatrix}$	$\begin{pmatrix}0&9\\0&1\end{pmatrix}$
25	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$		$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	59	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$	$\begin{pmatrix}4&1\\0&1\end{pmatrix}$	$\begin{pmatrix}3&1\\0&1\end{pmatrix}$	$\begin{pmatrix}24&11\\0&1\end{pmatrix}$	93	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	$\begin{pmatrix}3&3\\0&1\end{pmatrix}$	$\begin{pmatrix}2&6\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$
27	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$		$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	61	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	$\begin{pmatrix}5&1\\0&1\end{pmatrix}$	$\begin{pmatrix}5&5\\0&1\end{pmatrix}$	95	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$	$\begin{pmatrix}0&4\\0&1\end{pmatrix}$	$\begin{pmatrix}4&6\\0&1\end{pmatrix}$	$\begin{pmatrix}0&9\\0&1\end{pmatrix}$
29	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	$\begin{pmatrix}4&0\\0&1\end{pmatrix}$		$\begin{pmatrix}8&0\\0&1\end{pmatrix}$	63	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}3&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	97	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	$\begin{pmatrix}2&4\\0&1\end{pmatrix}$	$\begin{pmatrix}6&6\\0&1\end{pmatrix}$	$\begin{pmatrix}12&18\\0&1\end{pmatrix}$
31	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$		$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	65	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&3\\0&1\end{pmatrix}$	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&6\\0&1\end{pmatrix}$	99	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}4&4\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$
33	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	$\begin{pmatrix}3&1\\0&1\end{pmatrix}$		$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	67	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}2&3\\0&1\end{pmatrix}$	$\begin{pmatrix}4&2\\0&1\end{pmatrix}$	$\begin{pmatrix}8&8\\0&1\end{pmatrix}$					
35	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$		$\begin{pmatrix}0&6\\0&1\end{pmatrix}$	69	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	$\begin{pmatrix}4&3\\0&1\end{pmatrix}$	$\begin{pmatrix}6&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$					