Un groupe de matrices cyclique masqué

PAR

PATRICK TELLER

Il est bien connu que tout groupe cyclique est isomorphe à un groupe de la forme $(Z/\mathrm{nZ}, \oplus)$, pourtant il est utile de manipuler des groupes cycliques « masqués », c'est à dire des groupes qui se révèlent cycliques mais qui ne portent pas cette particularité sur leur front.

Bien évidemment tout sous-groupe engendré par un élément d'ordre fini est cyclique mais ...cela a moins de charme.

On rappelle

Théorème 1.

Le groupe multiplicatif d'un corps fini est cyclique

(dans tous les bons manuels)

Théorème 2.

Soit p un premier congru à 3 modulo 4 l'ensemble $G_p = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, (a,b) \in F_p^2 \Big\backslash (0,0) \right\}$ *est un groupe cyclique.*

Démonstration.

$(\mathcal{M}_2(F_p), +, \times)$ est bien entendu un anneau et il est immédiat que $\mathcal{F} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, (a,b) \in F_p^2 \right\}$ est un sous-anneau.

Par ailleurs, comme p est un premier congru à 3 modulo 4, -1 n'est pas un carré modulo p, par suite si $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ appartient à G son déterminant $a^2 + b^2$ est inversible dans F_p, d'où il découle que tout élément non nul de $\mathcal{F}$ est inversible, ce qui fait de $(\mathcal{F}, +, \times)$ un corps.

En conséquence le groupe des éléments inversibles est un groupe fini, de cardinal $p^2 - 1$. □