

# FICHE 05-04 : Sur les carrés de $\mathbb{F}_p$ .

Yvann Le Fay

Août 2019

## Enoncé

Dénombrer les carrés de  $\mathbb{F}_p$  puis démontrer que  $\forall x \in \mathbb{F}_p^*, x$  est un carré  $\iff x^{\frac{p-1}{2}} = 1$ .

## Solution

Si  $p = 2$ , alors l'énoncé est trivial, supposons dorénavant que  $p \geq 3$ .

L'ensemble des carrés de  $\mathbb{F}_p^*$  est l'image de  $\mathbb{F}_p^*$  par l'application  $f : x \mapsto x^2$  qui est un morphisme. Ainsi, on sait que  $\text{im } f \equiv \mathbb{F}_p^* / \ker f$ . Or  $\ker f = \{-1, 1\}$ , ainsi, il y a exactement  $\frac{p-1}{2}$  carrés dans  $\mathbb{F}_p^*$ .

D'après le petit théorème de Fermat, tout élément  $x$  de  $\mathbb{F}_p^*$  est solution de  $x^{p-1} - 1 = 0$ . Or  $x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1)$ . On vérifie bien que  $\forall x \in \mathbb{F}_p^*, (x^2)^{\frac{p-1}{2}} = 1$ , et de plus, le premier membre de la factorisation égalisé à 0, a dans  $\mathbb{F}_p^*$  au plus  $\frac{p-1}{2}$  solutions. Nécessairement, ce sont les carrés de  $\mathbb{F}_p^*$ . Or aucun de ces carrés n'est solution de l'équation du second membre de la factorisation. De plus nécessairement par le petit théorème de Fermat,  $\forall x \in \mathbb{F}_p^*, x^{\frac{p-1}{2}} \in \{-1, 1\}$ . Ainsi, les non-carrés de  $\mathbb{F}_p^*$  sont exactement les solutions du second membre de la factorisation.

Ce qui permet de conclure, que  $x$  est un carré (ou non) dans  $\mathbb{F}_p^*$  est équivalent à  $x^{\frac{p-1}{2}} = 1$  (ou  $-1$ ) respectivement.

On peut montrer avec cela que  $X^4 - 10X^2 + 1$  est réductible sur  $\mathbb{F}_p$  quel que soit  $p$  premier.

En effet, si 2 est un carré dans  $\mathbb{F}_p$ , disons  $2 = a^2$  alors,

$$X^4 - 10X^2 + 1 = (X^2 - 1)^2 - 8X^2 = (X^2 - 1)^2 - (2aX)^2 = (X^2 - 2aX - 1)(X^2 + 2aX - 1)$$

Si 3 est un carré dans  $\mathbb{F}_p$ , disons  $3 = b^2$  alors,

$$X^4 - 10X^2 + 1 = (X^2 + 1)^2 - 12X^2 = (X^2 + 1)^2 - (2bX)^2 = (X^2 - 2bX + 1)(X^2 + 2bX + 1)$$

Enfin si ni 2 ni 3 n'est un carré dans  $\mathbb{F}_p$  alors nécessairement, d'après ce que l'on a vu, 6 est un carré, écrivons  $c^2 = 6$ , alors

$$X^4 - 10X^2 + 1 = (X^2 - 5)^2 - 24 = (X^2 - 2c - 5)(X^2 + 2c - 5)$$

■