Table des matières

1 Carrés dans un corps fini

On note, pour tout entier premier p, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
On rappelle qu'il s'agit d'un corps à p éléments. D'autre part, $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ est un groupe cyclique d'ordre $p-1$.
On dit qu'un élément $a \in \mathbb{F}_p$ est un carré s'il existe $b \in \mathbb{F}_p$ tel que $a = b^2$.

Définition 1 *Pour $n \in \mathbb{N}$ et p un nombre premier supérieur ou égal à 3, le symbole de Legendre $\left(\frac{n}{p}\right)$ est défini par :*

$$\left(\frac{n}{p}\right) = \begin{cases} 0 \text{ si } p \text{ divise } n \\ +1 \text{ si la classe de } n \text{ modulo } p \text{ est un carré dans } \mathbb{F}_p \\ -1 \text{ si la classe de } n \text{ modulo } p \text{ n'est pas un carré dans } \mathbb{F}_p \end{cases}$$

On dispose alors le résultat suivant dû à Euler :

Proposition 2 *Soit p un nombre premier ≥ 3. Il y a autant de carrés que de non carrés dans $\mathbb{F}_p^*$. Pour tout $n \in \mathbb{N}$, on a la formule*

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \quad [p].$$

DEMONSTRATION : L'application $\psi : \mathbb{F}_p^* \to \mathbb{F}_p^*$ défini par $\psi(x) = x^2$ est morphisme de groupe multiplicatif, dont le noyau est $\{-1, 1\}$ (de cardinal 2 car $p \geq 3$) et dont l'image est l'ensemble $\mathbb{F}_p^{*2}$ des carrés de $\mathbb{F}_p^*$. Par un théorème d'isomorphisme, il vient $|\mathbb{F}_p^{*2}| = \dfrac{|\mathbb{F}_p^*|}{2} = \dfrac{p-1}{2}$, ce qui prouve la première assertion.
Pour tout $x \in \mathbb{F}_p^*$, le théorème de Fermat nous donne $x^{p-1} = 1$ et donc

$x^{(p-1)/2} = \pm 1$. Chacune des équations $X^{(q-1)/2} = \pm 1$ a au plus $\dfrac{q-1}{2}$ racines donc exactement $\dfrac{p-1}{2}$ racines.
Si $n = x^2$ est un carré, on a $n^{(p-1)/2} = x^{p-1} = 1 = \left(\frac{n}{p}\right)$. Sinon, c'est que $n^{(p-1)/2} = -1 = \left(\frac{n}{p}\right)$. □

On en déduit immédiatement le

Corollaire 1 *Pour $n, n' \in \mathbb{N}$ et p premier ≥ 3,*

$$\left(\frac{nn'}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{n'}{p}\right).$$

2 Sommes de Gauss

Proposition 3 *Soit q un nombre premier ≥ 3, soit A un anneau et soit $\alpha \in A$ tel que*

$$1 + \alpha + ... + \alpha^{q-1} = 0.$$

On définit la somme de Gauss

$$\tau = \sum_{i \in \mathbb{F}_q} \left(\frac{i}{q}\right)\alpha^i = \sum_{i=1}^{q-1} \left(\frac{i}{q}\right)\alpha^i.$$

1. *On a $\tau^2 = \varepsilon(q)q$ où $\varepsilon(q) = \left(\dfrac{-1}{q}\right)$.*
2. *Si p est la caractéristique de A, et est telle que $p \geq 3$ et $p \neq q$, alors $\tau^p = \left(\dfrac{p}{q}\right)\tau$.*

DEMONSTRATION : Notons tout d'abord que $\alpha^p = 1$; en effet, $\alpha^p - 1 = (\alpha - 1)(1 + \alpha + ... + \alpha^{q-1}) = 0$.
D'autre part, on calcule

$$\begin{aligned}\varepsilon(q)\tau^2 &= \varepsilon(q) \sum_{i,j \in \mathbb{F}_q} \left(\frac{i}{q}\right)\left(\frac{j}{q}\right)\alpha^i\alpha^j = \sum_{i,j \in \mathbb{F}_q} \left(\frac{-ij}{q}\right)\alpha^{i+j} \\ &= \sum_{k \in \mathbb{F}_q} \left(\sum_{i \in \mathbb{F}_q} \left(\frac{i(i-k)}{q}\right)\right)\alpha^k = \sum_{k \in \mathbb{F}_q} s_k\alpha^k\end{aligned}$$

où s_k désigne $\displaystyle\sum_{i \in \mathbb{F}_q} \left(\frac{i(i-k)}{q}\right)$.

Si $k = 0$ et $i \neq 0$, alors $\left(\dfrac{i(i-k)}{q}\right) = \left(\dfrac{i^2}{q}\right) = \left(\dfrac{i}{q}\right)^2 = 1$ et on en déduit

$s_0 = q - 1$.
Supposons $k \neq 0$. Alors en notant i^{-1} l'inverse de i dans $\mathbb{F}_q^*$,

$$\Big(\frac{i(i-k)}{q}\Big) = \Big(\frac{i^2(1-ki^{-1}}{q}\Big) = \Big(\frac{1-ki^{-1}}{q}\Big).$$

Or, l'application $\mathbb{F}_q^* \to \mathbb{F}_q \setminus \{1\}$, $i \longmapsto 1 - ki^{-1}$ étant clairement bijective, il vient

$$s_k = \sum_{i \in \mathbb{F}_q \setminus \{1\}} \Big(\frac{i}{q}\Big) = \sum_{i \in \mathbb{F}_q} \Big(\frac{i}{q}\Big) - \Big(\frac{1}{q}\Big) = -1,$$

la dernière inégalité étant une conséquence de la proposition 2.
On a donc trouvé

$$\varepsilon(q)\tau^2 = q - 1 - \sum_{k \in \mathbb{F}_p^*} \alpha^k = q,$$

ce qui prouve la première partie de la proposition.
A étant de caractéristique p, l'application $x \longmapsto x^p$ de $\mathbb{F}_p$ dans lui-même est un morphisme de corps, appelé morphisme de Frobenius. On peut donc calculer

$$\tau^p = \Big(\sum_{i \in \mathbb{F}_q} \Big(\frac{i}{q}\Big)\alpha^i\Big)^p = \sum_{i \in \mathbb{F}_q} \Big(\frac{i}{q}\Big)^p \alpha^{ip}.$$

L'entier p étant impair, $\Big(\frac{i}{q}\Big)^p = \Big(\frac{i}{q}\Big)$ et donc

$$\Big(\frac{p}{q}\Big)\tau^p = \sum_{i \in \mathbb{F}_q} \Big(\frac{ip}{q}\Big)\alpha^{ip} = \sum_{j \in \mathbb{F}_q} \Big(\frac{j}{q}\Big)\alpha^j = \tau.$$

On a utilisé le fait que, p étant inversible dans $\mathbb{F}_q$, l'application $i \longmapsto ip$ est bijective. □

3 Loi de réciprocité quadratique

Voici le résultat principal de cet article.

Théorème 4 *Soit p et q deux nombres premiers distincts ≥ 3. Alors*

$$\Big(\frac{p}{q}\Big) = (-1)^{\frac{(p-1)(q-1)}{4}} \Big(\frac{q}{p}\Big).$$

DEMONSTRATION : On se place dans l'anneau $A = \mathbb{F}_p[X]/(\Phi_q)$ où Φ_q est le polynôme cyclotomique $1 + X + ... + X^{q-1}$. Dans cet anneau quotient de caractéristique p, on note α la classe de X, de sorte que $\Phi_q(\alpha) = 0$. On définit

$$\tau = \sum_{i \in \mathbb{F}_q} \left(\frac{i}{q}\right) \alpha^i.$$

D'après la proposition 2, on a $\tau^2 = \varepsilon(q)q$ et donc $\left(\frac{\varepsilon(q)q}{p}\right) = (\tau^2)^{\frac{p-1}{2}} = \tau^{p-1}$. D'autre part toujours d'après cette proposition, $\tau^p = \left(\frac{p}{q}\right)\tau$ et on en déduit

$$\left(\frac{\varepsilon(q)q}{p}\right)\tau = \tau^p = \left(\frac{p}{q}\right)\tau.$$

Puisque τ est inversible (car τ^2 l'est), c'est que

$$\left(\frac{p}{q}\right) = \left(\frac{\varepsilon(q)q}{p}\right) = (\varepsilon(q))^{\frac{p-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$$

comme annoncé. □