Références :
Un max de maths, Maxime Zavidovique

Théo. *Soit p, l deux nombres premiers distincts différents de 2*

$$\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = (-1)^{\frac{(p-1)(l-1)}{4}}$$

où

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ est un carré dans } \mathbb{F}_p^* \\ 0 & \text{si } x = 0 \\ -1 & \text{sinon} \end{cases}$$

Lemme. Soit $x \in \mathbb{F}_p^*, x$ est un carré de $\mathbb{F}_p^*$ si et seulement si $x^{\frac{p-1}{2}} = 1$. De plus, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}[p]$ et $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$ pour $x, y \in \mathbb{Z}$.

Démonstration. • Montrons que

$$\{x \in \mathbb{F}_p^* : x \text{ est un carré de } \mathbb{F}_p^*\} = \{x \in \mathbb{F}_p^* : x^{\frac{p-1}{2}} = 1\}.$$

Soit $x = y^2$ avec $y \in \mathbb{F}_p^*$. On a alors

$$x^{\frac{p-1}{2}} = y^{p-1} = 1.$$

Ainsi, on a

$$\{x \in \mathbb{F}_p^* : x \text{ est un carré de } \mathbb{F}_p^*\} \subset \{x \in \mathbb{F}_p^* : x^{\frac{p-1}{2}} = 1\}.$$

On sait aussi que

$$|\{x \in \mathbb{F}_p^* : x^{\frac{p-1}{2}} = 1\}| \leq \frac{p-1}{2}$$

car le polynôme $X^{\frac{p-1}{2}}$ admet au plus $\frac{p-1}{2}$ racines. Montrons maintenant que

$$|\{x \in \mathbb{F}_p^* : x \text{ est un carré de } \mathbb{F}_p^*\}| = \frac{p-1}{2}.$$

On définit l'application

$$\begin{array}{rccc} \phi : & \mathbb{F}_p^* & \longrightarrow & \mathbb{F}_p^* \\ & x & \longmapsto & x^2 \end{array}$$

On a donc que $Im(\phi) = \{x \in \mathbb{F}_p^* : x \text{ est un carré de } \mathbb{F}_p^*\}$ et $Ker(\phi) = \{\pm 1\}$. On obtient donc $|Im(\phi)| = \frac{|\mathbb{F}_p^*|}{Ker(\phi)} = \frac{p-1}{2}$.

- Montrons que $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}[p]$
  - ▶ Si $x = 0$, $\left(\frac{1}{p}\right) = 0$ et $0^{\frac{p-1}{2}} = 0[p]$.
  - ▶ Si $x \in \mathbb{Z}\backslash\{0\}$ est un carré de $\mathbb{F}_p^*$.

$$\left(\frac{x}{p}\right) = 1 = x^{\frac{p-1}{2}}[p]$$

  - ▶ Si $x \in \mathbb{Z}\backslash\{0\}$ n'est pas un carré de $\mathbb{F}_p^*$
    On a, d'après le théorème de Fermat $x^{p-1} = 1[p]$. On a donc, comme x n'est pas un carré, $x^{\frac{p-1}{2}} = -1[p]$.
    On a

$$\begin{aligned} \left(\frac{xy}{p}\right) &= (xy)^{\frac{p-1}{2}}[p] \\ &= x^{\frac{p-1}{2}} y^{\frac{p-1}{2}}[p] \\ &= \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)[p] \end{aligned}$$

    On sait que $\left(\frac{xy}{p}\right), \left(\frac{x}{p}\right), \left(\frac{y}{p}\right) \in \{-1, 0, 1\}$. Donc comme $p > 2$, $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{p}\right)$

□

Démonstration. Soit Ω une clôture algébrique de $\mathbb{F}_p$. Soit $\omega \in \Omega$ tel que $\omega^l = 1$.

Soit $y = \sum_{x\in\mathbb{F}_l} \left(\frac{x}{l}\right)\omega^x$
Montrons que cette somme est bien définie. Supposons que $m = n[l]$. Alors, $l|n-m$ et on a donc $\omega^{n-m} = 1$. Ainsi, $\omega^n = \omega^m$.
Donc y est bien défini.
Calculons y^2.

$$\begin{aligned}
y^2 &= \left(\sum_{x\in\mathbb{F}_l}\left(\frac{x}{l}\right)\omega^x\right)\left(\sum_{z\in\mathbb{F}_l}\left(\frac{z}{l}\right)\omega^z\right)\\
&\underbrace{=}_{\text{Lemme}} \sum_{(x,z)\in(\mathbb{F}_l)^2}\left(\frac{xz}{l}\right)\omega^{x+z}\\
&\underbrace{=}_{\substack{u=x+z\\ t=z}} \sum_{u\in\mathbb{F}_l}\omega^u\sum_{t\in\mathbb{F}_l}\left(\frac{t(u-t)}{l}\right)\\
&= \sum_{u\in\mathbb{F}_l}\omega^u\sum_{t\in\mathbb{F}_l^*}\left(\frac{t(u-t)}{l}\right)\\
&= \sum_{u\in\mathbb{F}_l}\omega^u\sum_{t\in\mathbb{F}_l^*}\left(\frac{-t^2(1-ut^{-1})}{l}\right)\\
&= \sum_{u\in\mathbb{F}_l}\omega^u\sum_{t\in\mathbb{F}_l^*}\underbrace{\left(\frac{-1}{l}\right)}_{=(-1)^{\frac{l-1}{2}}}\underbrace{\left(\frac{t^2}{l}\right)}_{=1}\left(\frac{1-ut^{-1}}{l}\right)
\end{aligned}$$

Ainsi,

$$(-1)^{\frac{l-1}{2}}y^2 = \sum_{u\in\mathbb{F}_l}\omega^u\underbrace{\sum_{t\in\mathbb{F}_l^*}\left(\frac{1-ut^{-1}}{l}\right)}_{:=c_u}$$

Pour $u\neq 0$, posons $s = 1-ut^{-1}\in\mathbb{F}_l\backslash\{1\}$

$$\begin{aligned}
c_u &= \sum_{s\in\mathbb{F}_l\backslash\{1\}}\left(\frac{s}{l}\right)\\
&= \sum_{s\in\mathbb{F}_l}\left(\frac{s}{l}\right)-\left(\frac{1}{l}\right)\\
&= \sum_{s\in\mathbb{F}_l^*}\left(\frac{s}{l}\right)-1\\
&= -1
\end{aligned}$$

car le nombre de carré de $\mathbb{F}_p^*$ est égal à $\frac{p-1}{2}$ et il est donc égal aux nombre d'éléments de $\mathbb{F}_p^*$ qui ne sont pas des carrés. Par définition du symbole de Legendre, la somme est donc nulle.
Pour $u = 0$, on a $c_u = \sum_{t\in\mathbb{F}_l^*}\left(\frac{1}{l}\right) = l-1$.
On obtient donc

$$\begin{aligned}
(-1)^{\frac{l-1}{2}}y^2 &= \sum_{u\in\mathbb{F}_l}\omega^u c_u\\
&= l-1-\sum_{u\in\mathbb{F}_l^*}\omega^u\\
&= l-\sum_{u\in\mathbb{F}_l}\omega^u\\
&= l-\frac{\omega^l-1}{\omega-1}\\
&= l
\end{aligned}$$

Ainsi,

$$y^2 = (-1)^{\frac{l-1}{2}}l.$$

Montrons que $y^{p-1} = \left(\frac{p}{l}\right)$.

$$\begin{aligned} y^p &= \left(\sum_{x\in\mathbb{F}_l} \left(\frac{x}{l}\right)\omega^x\right)^p \\ &\underbrace{=}_{\Omega \text{ est de caractéristique } p} \sum_{x\in\mathbb{F}_l} \left(\frac{x}{l}\right) w^{xp} \\ &\underbrace{=}_{z=xp} \sum_{z\in\mathbb{F}_l} \underbrace{\left(\frac{zp^{-1}}{l}\right)}_{=\left(\frac{z}{l}\right)\left(\frac{p}{l}\right)^{-1}} w^z \end{aligned}$$

Ainsi, on obtient

$$\left(\frac{p}{l}\right) y^p = \sum_{z\in\mathbb{F}_l} \left(\frac{z}{l}\right) w^z = y.$$

Comme $y^2 \neq 0$, on a $y^{p-1} = \left(\frac{p}{l}\right)$.

$$\begin{aligned} \left(\frac{p}{l}\right) &= y^{p-1} \\ &= (y^2)^{\frac{p-1}{2}} \\ &= (-1)^{\frac{(p-1)(l-1)}{4}} l^{\frac{p-1}{2}} \\ &= (-1)^{\frac{(p-1)(l-1)}{4}} \left(\frac{l}{p}\right) \end{aligned}$$

Ainsi,

$$\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = (-1)^{\frac{(p-1)(l-1)}{4}}.$$

□

Leçons possibles : 120 - 121 - 123