Définition : Soit p un nombre premier. Le symbole de Legendre mod p est défini par

$$\left(\frac{\cdot}{p}\right): {F_p}^* \to \{-1,1\}$$

$$a \mapsto \begin{cases} 1 \text{ si } \exists\, b, b^2 \equiv a[p] \\ -1 \text{ sinon} \end{cases}$$

Enoncé : Soit p et q deux nombres premiers impairs distincts. Alors $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}*\frac{q-1}{2}}$

Lemme(admis) : Soit $E=(F_q)^p, \Phi \in Q(E)$ telle $<$ te $rg(\Phi) = p$, alors $\exists \beta = (e_1, \dots, e_p)$une base de E où $Mat(\Phi, \beta) = \begin{pmatrix} 1 & \cdots & & 0 \\ \vdots & \ddots & 0 & \vdots \\ & 0 & 1 & 0 \\ 0 & \cdots & 0 & \alpha \end{pmatrix}$ avec $\alpha = \begin{cases} 1 \text{ si } disc(\Phi) \in ({F_q}^*)^2 \\ \text{sinon } \alpha \in ({F_q}^*)\backslash({F_q}^*)^2 \end{cases}$

Preuve du théorème : Soit Φ la forme quadratique dont la matrice dans la base canonique est

$M=\begin{pmatrix} J & & & \\ & J & (0) & \\ & (0) & J & \\ & & & (-1)^{\frac{p-1}{2}} \end{pmatrix}$ où $J=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

On a alors $Mat(\Phi, \beta) = I_p$

Soit Q la quadrique définie par $\{x \in E, \Phi(x) = 1\}$. On va dénombrer Q de deux manières, profitant des deux écritures matricielles de Φ. Mais d'abord montrons le résultat suivant :

Lemme 2 : $\left|\{\mathbf{x} \in F_q, px^2 = 1\}\right| = 1 + \left(\frac{p}{q}\right)$

Preuve lemme : si p est carré modulo 1, soit b une classe modulo q telle que $b^2=p$ dans F_q

Alors $px^2=1 \Leftrightarrow (bx)^2 = 1 \Leftrightarrow x \in \{b^{-1}, -b^{-1}\}$.

Sinon $px^2 \in ({F_q}^*)\backslash({F_q}^*)^2$ d'où l'équation n'a pas de solution.

Retour à la preuve du théorème : Soit, pour $k \in N$, $\tau_k : [\![1, p]\!] \to [\![1, p]\!]$

$$x \mapsto x + k - pE\left(\frac{x+k}{p+\frac{1}{p^k}}\right)$$

τ_k est bien définie. De plus, $\tau_k \in S_p$. Elle associe à x l'entier de $[\![1, p]\!]$ congru à x+k mod p. Soit θ l'action de Z_p sur Q définie par $\bar{k}.(x_1, \dots, x_p) = (x_{\tau_k(1)}, \dots, x_{\tau_k(p)})$.

L'action θ est bien définie du fait que

$$\Phi(x) = \sum_{i-1}^{p} {x_i}^2 = \sum_{i=1}^{p} {x_{\tau_k(i)}}^2 = \Phi(\bar{k}.x). \forall x, \text{que } \bar{0}.x = x \; \forall x \text{ et que } \forall \bar{k}, \bar{k'} \in Z_p, \bar{k}.(\bar{k'}.x) = \overline{k+k'}.x$$

On remarque que |Q| est congru au cardinal des orbites singleton modulo p. Soit {x} une orbite singleton, alors $\forall i, j \in [\![1, p]\!], x_i = x_j$, ainsi $|\Omega \in orb(\theta), |\Omega| = 1| = \left|\{\mathbf{x} \in F_q, px^2 = 1\}\right| = 1 + \left(\frac{p}{q}\right)$

ainsi $|Q|=1 + \left(\frac{p}{q}\right) + Np$

Autrement, dénombrons Q en utilisant l'écriture matricielle de Φ dans la base canonique.

« $\Phi(x) = \sum_{i=1}^{\frac{p-1}{2}} 2x_{2i-1}x_{2i} + (-1)^{\frac{p-1}{2}} {x_p}^2$ ». Soit la partition suivante :

$Q = Q_1 \cup Q_2$, où $Q_1 = \{x = (x_1, \dots, x_p) \in Q, x_{2i} = 0 \ \forall i \in [\![1, \frac{p-1}{2}]\!]\}$

Dénombrons Q_1 puis Q_2.

- $|Q_1| = q^{\frac{p-1}{2}}(1 + \left(\frac{(-1)^{\frac{p-1}{2}}}{p}\right))$.

Explication : pour $x \in Q_1$, on a $\Phi(x) = (-1)^{\frac{p-1}{2}} {x_p}^2 = 1$. Donc le choix des $(x_{2i-1})_i$ est libre dans $(F_q)^{\frac{p-1}{2}}$, tandis que pour les $(x_{2i})_i$, le seul $\frac{p-1}{2} -$ uplet possible est $(0, \dots, 0)$. Tout ceci bien sûr sous la condition, nécessaire et suffisante pour qu'il y ait des solutions, que $\left(\frac{(-1)^{\frac{p-1}{2}}}{p}\right)$ soit égal à 1. Ce qui donne 2 solutions possibles pour chaque (p-1)-uplet $(x_1, \dots, x_{p-1})$.

- $|Q_2| = q^{\frac{p-1}{2}}(q^{\frac{p-1}{2}} - 1)$.

On commence par un choix aléatoire de x_p, donc q possibilités, puis par le choix des $(x_{2i})_i$, qui est libre dans $(F_q)^{\frac{p-1}{2}} \backslash (0, \dots, 0)$. Ensuite les $(x_{2i-1})_i$ doivent être solution de $f(x) = 1 - (-1)^{\frac{p-1}{2}} x_p$ où $f : (F_q)^{\frac{p-1}{2}} \to F_q$

$$y = (y_1, \dots, y_{p-1}) \mapsto \sum_{i=1}^{\frac{p-1}{2}} x_{2i}\, y_i$$

donc l'ensemble des $(x_{2i-1})_i$ d'une éventuelle solution constitue un hyperplan affine de $(F_q)^{\frac{p-1}{2}}$, donc de cardinal $q^{\frac{p-3}{2}}$.

Les choix de x_p, des $(x_{2i-1})_i$ et des $(x_{2i})_i$ étant indépendants l'un de l'autre, on multiplie les cas possibles de chacun pour avoir le résultat.

Pour conclure, on a dans F_p : $1 + \left(\frac{p}{q}\right) = q^{\frac{p-1}{2}}(q^{\frac{p-1}{2}} + \left(\frac{(-1)^{\frac{p-1}{2}}}{p}\right))$, mais on remarque que $q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right)$, ainsi, et profitant du fait que $\left(\frac{q}{p}\right)^2 = 1$, on aura $\left(\frac{q}{p}\right) + \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2} * \frac{q-1}{2}}$.

Cette congruence modulo p est en effet une égalité, puisque $p > 2$.□