Loi de réciprocité quad [Gou] p 46.

Th : Soit $p, q > 2$ premiers et distincts.
Alors, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{p'q'}$ avec $p' = \frac{p-1}{2}$ et $q' = \frac{q-1}{2}$.

Dém :
On note $S = \{\overline{1}, \dots, \overline{p'}\} \subset \mathbb{F}_p$.
On sait que si $s \in \{1, \dots, p'\}$, $\overline{sq} = \varepsilon_s(q)\,\overline{s_q}$ avec $\begin{cases} \varepsilon_s(q) = \pm 1 \\ \overline{s_q} \in S \end{cases}$

$\left(\overline{sq} \in \mathbb{F}_p^* = \{-\overline{p'}, \dots, -\overline{1}, \overline{1}, \dots, \overline{p'}\}\right)$
On note alors $\mu_q = \mathrm{Card}\{s \in \{1, \dots, p'\}, \varepsilon_s(q) = -1\}$

$$S_{p,q} = \sum_{s=1}^{p'} \left[\frac{sq}{p}\right]$$

A voir : 1) $\left(\frac{q}{p}\right) = (-1)^{\mu_q}$

2) $S_{p,q}$ et μ_q ont même parité

3) $S_{p,q} + S_{q,p} = p'q'$

Ccl : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu_p}(-1)^{\mu_q} = (-1)^{S_{q,p}}(-1)^{S_{p,q}} = (-1)^{p'q'}$

---

1) • $f : \{1, \dots, p'\} \longrightarrow S$, $s \longmapsto \overline{s_q}$ est bijective :

Il suffit de montrer que f est injective.
Or, si $f(s) = f(s')$, $\varepsilon_s(q)\,\overline{s}\,\overline{q} = \varepsilon_{s'}(q)\,\overline{s'}\,\overline{q}$ donc
$p \mid \varepsilon_s(q)s - \varepsilon_{s'}(q)s' = n$ mais $|n| \leq 2p' < p$ donc
$n = 0$ et donc $s = s'$ ($|\varepsilon_s(q)s| = |\varepsilon_{s'}(q)s'|$)
• Par suite, on sait que $\left(\prod_{s=1}^{p'} \overline{s}\right)\left(\frac{q}{p}\right) = (\overline{1} \times \dots \times \overline{p'})\,\overline{q}^{p'}$

$$= \overline{1 \times q \times \dots \times p'q}$$

$$= \left(\prod_{s=1}^{p'} \varepsilon_s(q)\right)\left(\prod_{s=1}^{p'} \overline{s_q}\right)$$

(f est bij) $= (-1)^{\mu_q}\left(\prod_{s=1}^{p'} \overline{s}\right)$

donc $\left(\frac{q}{p}\right) = (-1)^{\mu_q}$.

2) Il suffit de mq $S_{p,q} \equiv \mu_q \pmod 2$.

on rq que si $s \in \{1, \dots, p'\}$, $sq = p\left[\frac{sq}{p}\right] + u_s$ avec $u_s \in \{1, \dots, p-1\}$

$\left(p\left[\frac{sq}{p}\right] \leq p\,\frac{sq}{p} < p\left[\frac{sq}{p}\right] + p\right.$ donc $0 < sq - p\left[\frac{sq}{p}\right] < p$ mais

$sq - p\left[\frac{sq}{p}\right]$ est un entier (clair) non nul car sinon $p \mid s$ d'après le th de gauss $\left.\right)$ donc $q\,\frac{p'(p'+1)}{2} = p S_{p,q} + \sum_{s=1}^{p'} u_s$

(on somme de 1 à p') et donc $\frac{p'(p+1)}{2} \equiv S_{p,q} + \sum_{s=1}^{p'} u_s \pmod 2$

$(p, q \equiv 1)$.

Il suffit alors de mq $\sum_{s=1}^{p'} u_s \equiv \frac{p'(p'+1)}{2} + \mu_q \pmod 2$.

Or, $\begin{cases} \text{si } u_s \in \{1, \dots, p'\},\ u_s = sq \text{ et } e_s(q) = 1 \\ \text{si } u_s \in \{p'+1, \dots, p-1\},\ u_s = p - sq \text{ et } e_s(q) = -1 \end{cases}$

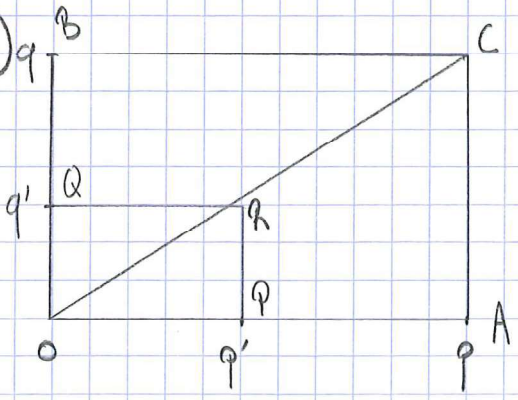
donc $\sum_{s=1}^{p'} u_s = \sum_{e_s(q)=1} sq + \sum_{e_s(q)=-1} (p - sq)$

$\equiv \sum_{s=1}^{p'} sq + \mu_q \qquad (-1 \equiv 1 \text{ et } p \equiv 1)$

$= \sum_{s=1}^{p'} s + \mu_q \qquad (f \text{ est bij})$

$= \frac{p'(p'+1)}{2} + \mu_q$

3) q



On rq que $p \wedge q = 1$ (ils st l'un et $\neq$) donc (OC) ne rencontre pas $\{1, \dots, p'\} \times \{1, \dots, q'\}$ (sinon, $\exists (a,b) \in \{1, \dots, p'\} \times \{1, \dots, q'\}$ tq

$b = \frac{aq}{p}$ donc $p \mid aq$ et donc $p \mid a$ $\}$).

Par ailleurs, $\left[\frac{sq}{p}\right]$ représente le nbre de pts de $\{s\} \times \mathbb{N}^*$ se trouvant sous (OC) donc $S_{p,q}$ représente le nbre de pts de $\{1, \dots, p'\} \times \mathbb{N}^*$ se trouvant sous (OC) et donc $S_{p,q} + S_{q,p}$ représente le nbre de pts de $\{1, \dots, p'\} \times \{1, \dots, q'\}$ se trouvant ds OPRQ ie $p'q'$.