Loi de réciprocité quadratique

Leçons : 120, 121, 123, 125
Référence : J.-P. Serre, *Cours d'arithmétique*, p. 18.

Théorème 1 (Loi de réciprocité quadratique)**.** *Soit p, q deux nombres premiers impairs distincts. Alors,*

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

Première démonstration (via le lemme de Gauss, pour la leçon 121)

Lemme 2 (Lemme de Gauss)**.** *Si* $\mathrm{pgcd}(a,p)=1$*, alors*

$$\left(\frac{a}{p}\right) = (-1)^{|(aR^+)\cap R^-|},$$

où $R^+ = \left\{1,\dots,\frac{p-1}{2}\right\}$ *et* $R^- = \left\{-1,\dots,-\frac{p-1}{2}\right\}$.

Démonstration du lemme. Soit a un entier tel que $\mathrm{pgcd}(a,p)=1$.

Remarquons d'abord que, pour $r \in R^+$, il existe $m_r \in R^+$ et $\varepsilon_r \in \{\pm 1\}$ tels que

$$ar = \varepsilon_r m_r \bmod(p).$$

Montrons d'abord que $r \mapsto m_r$ est une bijection de R^+ sur lui-même. Il suffit de montrer que c'est une application injective. Supposons $m_r = m_s$. Montrons que $r = s$.

On a $ar\varepsilon_r = as\varepsilon_s \bmod(p)$ et $\mathrm{pgcd}(a,p)=1$, donc $r\varepsilon_r = s\varepsilon_s \bmod(p)$, donc, en multipliant par $\varepsilon_r\varepsilon_s$,

$$r \underbrace{\varepsilon_r^2}_{\varepsilon_r\in R^+}\varepsilon_s = s\varepsilon_r \underbrace{\varepsilon_s^2}_{\varepsilon_s\in R^+} \bmod(p),$$

donc $\varepsilon_r\varepsilon_s = 1$, donc $\varepsilon_r = \varepsilon_s$, donc $r = s \bmod(p)$.

Ainsi, $r \mapsto m_r$ est une bijection de R^+ dans lui-même, donc

$$\prod_{r=1}^{\frac{p-1}{2}} m_r = \prod_{r\in R^+} r = \left(\frac{p-1}{2}\right)! \neq 0 \bmod(p).$$

Alors, en effectuant le produit des égalités $ar = \varepsilon_r m_r \bmod(p)$, on obtient

$$a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! = \prod_{i=1}^{\frac{p-1}{2}}\varepsilon_i \left(\frac{p-1}{2}\right)! \bmod(p),$$

donc

$$a^{\frac{p-1}{2}} = \prod_{i=1}^{\frac{p-1}{2}}\varepsilon_i,$$

et ε_i vaut -1 lorsque la multiplication par a change le signe de i, donc

$$\prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i = (-1)^{|(aR^+)\cap R^-|}.$$

Et d'après la formule d'Euler, $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \mod(p)$, d'où

$$\left(\frac{a}{p}\right) = (-1)^{|(aR^+)\cap R^-|} \mod(p).$$

CQFD

Lemme 3 (Lemme d'Eisenstein)**.** *Pour a impair tel que* $\operatorname{pgcd}(a,p) = 1$*, on a*

$$\left(\frac{a}{p}\right) = (-1)^{S(a,p)}, \qquad \text{où} \qquad S(a,p) = \sum_{r=1}^{\frac{p-1}{2}} \left\lfloor \frac{ar}{p} \right\rfloor.$$

Démonstration du lemme. Soit d'abord a pair ou impair tel que $\operatorname{pgcd}(a,p) = 1$. Pour $r \in R^+$, on a

$$\begin{aligned} ar &= p\left\lfloor \frac{ar}{p} \right\rfloor + \varepsilon_r m_r + p\,\frac{1-\varepsilon_r}{2} \\ &= \left\lfloor \frac{ar}{p} \right\rfloor + m_r + \frac{1-\varepsilon_r}{2} \mod(2). \end{aligned}$$

En sommant, on obtient

$$a\sum_{r=1}^{\frac{p-1}{2}} r = S(a,p) + \underbrace{\sum_{r=1}^{\frac{p-1}{2}} m_r}_{=\sum_{r=1}^{\frac{p-1}{2}} r} + \sum_{r=1}^{\frac{p-1}{2}} \frac{1-\varepsilon_r}{2} \mod(2),$$

donc

$$(a-1)\frac{p^2-1}{8} = S(a,p) + |(aR^+)\cap R^-| \mod(2).$$

Donc, si on suppose a impair, $(a-1)$ est pair, donc

$$S(a,p) + |(aR^+)\cap R^-| = 0 \mod(2),$$

d'où, d'après le lemme précédent,

$$(-1)^{|(aR^+)\cap R^-|} = (-1)^{S(a,p)} = \left(\frac{a}{p}\right).$$

CQFD

Démonstration du théorème. Soit donc maintenant p, q deux entiers premiers impairs distincts. Posons

$$S = [\![1, \tfrac{p-1}{2}]\!] \times [\![1, \tfrac{q-1}{2}]\!], \qquad S_1 = \{(m,n) \in S \mid qm > pn\}, \qquad S_2 = \{(m,n) \in S \mid qm < pn\}.$$

Comme $q \nmid n$ pour $n \in [\![1, \frac{q-1}{2}]\!]$ (et p, q premiers distincts), on a $qm \neq pn$ pour tout $(m,n) \in S$. Donc $S = S_1 \sqcup S_2$, et en particulier $|S| = |S_1| + |S_2|$.

Et on a

$$|S_1| = \sum_{1 \leq m \leq \frac{p-1}{2}} \sum_{\substack{1 \leq n \leq \frac{q-1}{2} \\ n < qm/p}} 1 = \sum_{1 \leq m \leq \frac{p-1}{2}} \min\left(\left\lfloor \frac{qm}{p} \right\rfloor, \frac{q-1}{2} \right).$$

Or, on a $\dfrac{qm}{p} \leq \dfrac{q(p-1)}{2p} < \dfrac{q}{2}$, et q est impair, donc $\left\lfloor \dfrac{qm}{p} \right\rfloor \leq \dfrac{q-1}{2}$, donc

$$|S_1| = S(q,p).$$

De même, $|S_2| = S(p,q)$.

Or, $|S| = \dfrac{p-1}{2} \times \dfrac{q-1}{2} = S(q,p) + S(p,q)$, d'où, par le lemme d'Eisenstein,

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

□

Seconde démonstration (via les sommes de Gauss, pour la leçon 123)

Soit Ω le corps de décomposition de $X^q - 1$ sur $\mathbb{F}_p$. Soit ω une racine primitive q-ième de l'unité. Posons

$$y = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x \in \Omega.$$

Cette somme a bien un sens par passage au quotient de $\mathbb{Z} \to \Omega$, $h \mapsto \omega^h$, en $\mathbb{Z}/q\mathbb{Z} \to \Omega$, $x \mapsto \omega^x$.

Lemme 4. $y^2 = (-1)^{\frac{q-1}{2}} q$.

Démonstration du lemme. On a

$$\begin{aligned} y^2 &= \left(\sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x\right)\left(\sum_{t \in \mathbb{F}_q^*} \left(\frac{t}{q}\right) \omega^t\right) = \sum_{x \in \mathbb{F}_q} \sum_{t \in \mathbb{F}_q^*} \left(\frac{xt}{q}\right) \omega^{x+t} \\ &\underset{u=x+t}{=} \sum_{u \in \mathbb{F}_q} \sum_{t \in \mathbb{F}_q^*} \left(\frac{t(u-t)}{q}\right) \omega^u = \sum_{u \in \mathbb{F}_q} \omega^u \sum_{t \in \mathbb{F}_q^*} \left(\frac{-t^2}{q}\right)\left(\frac{1-ut^{-1}}{q}\right) \\ &= (-1)^{\frac{q-1}{2}} \sum_{u \in \mathbb{F}_q} c_u\, \omega^u, \qquad \text{avec } c_u = \sum_{t \in \mathbb{F}_q^*} \left(\frac{1-ut^{-1}}{q}\right). \end{aligned}$$

Pour $u = 0$, on a $c_0 = \sum_{t \in \mathbb{F}_q^*} \underbrace{\left(\frac{1}{q}\right)}_{=1} = q - 1$.

Pour $u \neq 0$, $c_u = \sum_{t \in \mathbb{F}_q^*} \left(\frac{1-ut^{-1}}{q}\right) = \sum_{s \in \mathbb{F}_q \setminus \{1\}} \left(\frac{s}{q}\right) - \left(\frac{1}{q}\right) = -1$ (car $1 - ut^{-1}$ décrit $\mathbb{F}_q \setminus \{1\}$ lorsque t décrit $\mathbb{F}_q^*$, et $\sum_{s \in \mathbb{F}_q} \left(\frac{s}{q}\right) = 0$ car il y a autant de carrés que de non-carrés).

Donc,

$$y^2 = (-1)^{\frac{q-1}{2}} \left(q - 1 - \sum_{u \in \mathbb{F}_q^*} \omega^u \right).$$

Il reste donc à calculer $\sum_{u \in \mathbb{F}_q^*} \omega^u$. On a $\sum_{u \in \mathbb{F}_q} \omega^u = \omega^\alpha \sum_{u \in \mathbb{F}_q} \omega^u$, où α est choisi tel que $\omega^\alpha \neq 1$, et donc $\sum_{u \in \mathbb{F}_q} \omega^u = 0$, donc $\sum_{u \in \mathbb{F}_q^*} \omega^u = -1$.

D'où $y^2 = (-1)^{\frac{q-1}{2}} q$. *CQFD*

Lemme 5. $y^{p-1} = \left(\frac{p}{q}\right)$.

Démonstration du lemme. On a

$$\begin{aligned} y^p &= \left(\sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x \right)^p = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right)^p \omega^{xp} = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^{xp} \\ &\underset{u=xp}{=} \sum_{u \in \mathbb{F}_q} \left(\frac{p^{-1}u}{q}\right) \omega^u = \left(\frac{p}{q}\right) y. \end{aligned}$$

Et $y \neq 0$ (par exemple d'après le lemme précédent, puisque $y^2 = (-1)^{\frac{q-1}{2}} q \neq 0$), donc

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

CQFD

Démonstration du théorème. On a alors

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

donc, d'après le critère d'Euler ($q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right) \mod(p)$),

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

□