Loi de réciprocité quadratique

Leçons
121 : Nombres premiers. Applications.
123 : Corps finis. Applications.

Référence *Cours d'arithmétique*, Jean-Pierre Serre.

Je suis passé sur ce développement dans le cadre de la leçon *123 : Corps finis. Applications.* J'ai listé les questions du jury à la fin de ce document.

J'avais proposé comme autre développement le dénombrement des polynômes unitaires irréductibles de degré donné dans $\mathbb{F}_q[X]$.

Théorème (réciprocité quadratique)

Soient $p \neq q$ deux nombres premiers impairs distincts. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.

Preuve. Soit K un surcorps de $\mathbb{F}_p$ contenant ω une racine primitive q-ème de l'unité, et soit $S := \sum_{x\in\mathbb{F}_q} \left(\frac{x}{q}\right)\omega^x$.

Première étape – calcul de S^2.

On a successivement :

$$\begin{aligned}
S^2 &= \sum_{(x,y)\in\mathbb{F}_q^2} \left(\frac{xy}{q}\right)\omega^{x+y} \\
&\overset{\substack{u=x+y\\ v=y}}{=} \sum_{u\in\mathbb{F}_q}\omega^u \sum_{v\in\mathbb{F}_q^*}\left(\frac{v(u-v)}{q}\right) \\
&= \sum_{u\in\mathbb{F}_q}\omega^u \sum_{v\in\mathbb{F}_q^*}\left(\frac{-v^2(1-uv^{-1})}{q}\right) \\
&= \sum_{u\in\mathbb{F}_q}\omega^u \sum_{v\in\mathbb{F}_q^*} \underbrace{\left(\frac{-1}{q}\right)}_{=(-1)^{(q-1)/2}} \underbrace{\left(\frac{v^2}{q}\right)}_{=1}\left(\frac{1-uv^{-1}}{q}\right) \\
&= \sum_{u\in\mathbb{F}_q}(-1)^{(q-1)/2}\omega^u S_u,
\end{aligned}$$

où $S_u = \sum_{v\in\mathbb{F}_q^*}\left(\frac{1-uv^{-1}}{q}\right)$.

Pour $u = 0$, $S_u = q - 1$.

Pour $u \neq 0$, $\mathbb{F}_q^* \to \mathbb{F}_q \backslash \{1\}, v \mapsto 1 - uv^{-1}$ est bijective, donc $S_u = \sum_{w \in \mathbb{F}_q \backslash \{1\}} \left(\frac{w}{q}\right) = \sum_{w \in \mathbb{F}_q} \left(\frac{w}{q}\right) - \left(\frac{1}{q}\right) = -1$.
Ainsi :

$$\begin{aligned} S^2 &= (-1)^{(q-1)/2} \left(q - 1 - \sum_{u \in \mathbb{F}_q^*} \omega^u \right) \\ &= (-1)^{(q-1)/2} \Big(q - \underbrace{\sum_{u \in \mathbb{F}_q} \omega^u}_{=(1-\omega^q)/(1-\omega)=0} \Big) \\ &= (-1)^{(q-1)/2} q. \end{aligned}$$

Deuxième étape – calcul de S^p.

Utilisant le morphisme de Frobenius, on a :

$$\begin{aligned} S^p &= \left(\sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x \right)^p \\ &= \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^{px} \\ &\overset{y=px}{=} \sum_{x \in \mathbb{F}_q} \left(\frac{y}{q}\right) \left(\frac{p}{q}\right) \omega^y \\ &= \left(\frac{p}{q}\right) S. \end{aligned}$$

Par le premier point, $S^2 \neq 0$, donc $S \neq 0$, donc $S^{p-1} = \left(\frac{p}{q}\right)$.

Conclusion.

Ainsi :

$$\begin{aligned} \left(\frac{p}{q}\right) &= S^{p-1} \\ &= (S^2)^{(p-1)/2} \\ &= (-1)^{(p-1)(q-1)/2} q^{(p-1)/2} \\ &= (-1)^{(p-1)(q-1)/2} \left(\frac{q}{p}\right). \end{aligned}$$

□

Théorème (loi supplémentaire)

Soit $p \geqslant 3$ premier. Alors $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Preuve. Soit K un surcorps de $\mathbb{F}_p$ contenant $\alpha \neq 0$ tel que $\alpha^4 + 1 = 0$.

Alors $(\alpha + \frac{1}{\alpha})^2 = 2$, donc :

$$\begin{aligned} 2 \text{ est un carré dans } \mathbb{F}_p &\iff \alpha + \frac{1}{\alpha} \in \mathbb{F}_p \\ &\iff (\alpha + \frac{1}{\alpha})^p = \alpha + \frac{1}{\alpha} \\ &\iff \alpha^p + \frac{1}{\alpha^p} = \alpha + \frac{1}{\alpha}. \end{aligned}$$

Et :

$$\begin{aligned} \alpha^{8k\pm1} + \frac{1}{\alpha^{8k\pm1}} &= \alpha + \frac{1}{\alpha} \\ \alpha^{8k\pm3} + \frac{1}{\alpha^{8k\pm3}} &= \alpha^3 + \frac{1}{\alpha^3} = -\frac{1}{\alpha} - \alpha \end{aligned}$$

avec $-\frac{1}{\alpha} - \alpha \neq \frac{1}{\alpha} + \alpha$, car $\frac{1}{\alpha} + \alpha = 0 \implies \alpha^2 = -1 \implies \alpha^4 = 1$. □

Questions du jury

Jury – Qu'est-ce qu'une racine primitive q-ème de l'unité dans ce contexte ?

Moi – C'est une racine q-ème de l'unité distincte de 1.

Jury – Et pourquoi en existe-t-il ?

Moi – On regarde le polynôme $X^q - 1$, on se place sur son corps de décomposition sur $\mathbb{F}_p$ (ou sur $\overline{\mathbb{F}_p}$) où il est scindé. Il est de plus à racines simples puisque premier avec son polynôme dérivé [1] , il suffit donc de prendre une racine distincte de 1.

Jury – Et que se passerait-il en caractéristique q ?

Moi – Dans ce cas, $X^q - 1 = (X-1)^q$, donc l'unique racine est 1.

Jury – Pour la loi supplémentaire, comment justifiez-vous la première équivalence ? Le sens $\Longleftarrow$ est évident, mais qu'en est-il de $\Longrightarrow$?

Moi – Si 2 est un carré dans $\mathbb{F}_p$, i.e. $2 = \beta^2$ avec $\beta \in \mathbb{F}_p$, alors β est racine dans K de $X^2 - 2$. Or on connaît les deux racines de ce polynôme dans K : $\pm\left(\alpha + \frac{1}{\alpha}\right)$. Donc $\alpha + \frac{1}{\alpha} = \pm\beta \in \mathbb{F}_p$.

Jury – Vous avez mentionné la clôture algébrique de $\mathbb{F}_q$. Pouvez-vous nous expliquer comment elle est construite ?

Moi – L'idée est de montrer que $\bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^{n!}}$ est un corps algébriquement clos, et est une extension algébrique de $\mathbb{F}_p$.
Bon je passe les détails ici, voir le Gozard par exemple.
À vos risques et périls de parler de la clôture algébrique ! J'en avais également parlé dans le plan.

Jury – Vous avez indiqué dans la remarque suivant le théorème dans votre plan que ces résultats permettent de calculer $\left(\frac{n}{p}\right)$ par "réductions successives". Pouvez-vous détailler ?

Moi – On décompose n en produit de facteurs premiers, on utilise la multiplicativité du symbole de Legendre, puis on applique les résultats.

Jury – En pratique cela demande de savoir décomposer n en produits de facteurs premiers. Est-ce que c'est facile en pratique ?

Moi – Non, pas du tout... Cette méthode marche surtout pour de petites valeurs de n (ou plus généralement pour des n qu'on sait facilement décomposer).

Jury – Et sinon, savez-vous comment nous pouvons procéder en pratique ? C'est purement culturel.

Moi – Je sais qu'il existe des algorithmes, mais je ne les connais pas. [2]

[1] Car $(X^q - 1)' = qX^{q-1}$ avec $q \neq 0$ dans un corps de caractéristique p !

[2] C'est dommage, j'avais rencontré l'algorithme de Tonelli-Shanks mais pas étudié ni vraiment retenu... Il permet de plus de calculer une racine carrée si elle existe.