Loi de réciprocité quadratique

Mon développement

On rappelle deux propriétés du symbole de Legendre. Pour tous $x, y \in \mathbb{Z}$ et tout nombre premier impair p, on a :

(i)
$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) ,$$

(ii)
$$\left(\frac{x}{p}\right) \equiv x^{(p-1)/2}[p] .$$

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

Soient p et q deux nombres premiers impairs distincts. Soit α une racine primitive p-ième de l'unité dans une extension de $\mathbb{F}_q$. Comme $\alpha^p = 1$, on peut définir

$$\tau = \sum_{x\in\mathbb{F}_p}\left(\frac{x}{p}\right)\alpha^x .$$

On va calculer τ^2 et τ^q.

On a d'abord, en utilisant (i),

$$\tau^2 = \sum_{x,y\in\mathbb{F}_p}\left(\frac{xy}{p}\right)\alpha^{x+y} .$$

On note ensuite, pour tout $u \in \mathbb{F}_p$,

$$S(u) = \sum_{\substack{x,y\in\mathbb{F}_p \\ x+y=u}}\left(\frac{xy}{p}\right) = \sum_{x\in\mathbb{F}_p}\left(\frac{x(u-x)}{p}\right) .$$

On a
$$S(0) = \sum_{x\in\mathbb{F}_p}\left(\frac{-x^2}{p}\right) = \left(\frac{-1}{p}\right)\sum_{x\in\mathbb{F}_p}\left(\frac{x}{p}\right)^2 = \left(\frac{-1}{p}\right)(p-1)$$

d'après (i).

De plus, pour tout $u \in \mathbb{F}_p^*$, on a

$$\begin{aligned} S(u) &= \sum_{x\in\mathbb{F}_p^*} \left(\frac{-x^2(1-ux^{-1})}{p}\right) \\ &= \left(\frac{-1}{p}\right) \sum_{x\in\mathbb{F}_p^*} \left(\frac{1-ux^{-1}}{p}\right) \qquad \text{(d'après (i))} \\ &= \left(\frac{-1}{p}\right) \sum_{y\in\mathbb{F}_p\setminus\{1\}} \left(\frac{y}{p}\right) \\ &= \left(\frac{-1}{p}\right)(-1) \qquad \left(\text{car } \sum_{y\in\mathbb{F}_p} \left(\frac{y}{p}\right) = 0\right) \end{aligned}$$

donc

$$\tau^2 = \sum_{u\in\mathbb{F}_p} S(u)\alpha^u = \left(\frac{-1}{p}\right)\left(p - 1 - \sum_{u\in\mathbb{F}_p^*} \alpha^u\right) = \left(\frac{-1}{p}\right) p \ .$$

On a ainsi montré que

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

Ensuite, on a

$$\begin{aligned} \tau^q &= \sum_{x\in\mathbb{F}_p} \left(\frac{x}{p}\right)^q \alpha^{qx} \qquad \text{(morphisme de Frobenius en caractéristique } q) \\ &= \sum_{x\in\mathbb{F}_p} \left(\frac{x}{p}\right)\alpha^{qx} \qquad \text{(car } q \text{ est impair)} \\ &= \left(\frac{q}{p}\right) \sum_{x\in\mathbb{F}_p} \left(\frac{qx}{p}\right)\alpha^{qx} \qquad \text{(en utilisant (i))} \\ &= \left(\frac{q}{p}\right)\tau \end{aligned}$$

donc, τ étant non nul d'après le point précédent, on a

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

Finalement, on a

$$\begin{aligned} \left(\frac{p}{q}\right) &= p^{(q-1)/2} \qquad \text{(d'après (ii))} \\ &= \left(\left(\frac{-1}{p}\right)\tau^2\right)^{(q-1)/2} \qquad \text{(d'après (1))} \\ &= (-1)^{(p-1)(q-1)/4}\tau^{q-1} \qquad \text{(d'après (ii))} \\ &= (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right) \qquad \text{(d'après (2))} \ . \end{aligned}$$

Cette égalité est valable dans $\mathbb{F}_q$ et, q étant différent de 2, elle est aussi valable dans $\mathbb{Z}$. □

Références

J'ai utilisé [Hin08, p. 14], [Ser77, p. 16].

Leçons correspondantes

J'utilise ce développement pour les leçons 109, 110, 112, 113.

Remarques

- On a utilisé à plusieurs reprises et sans le mentionner le fait que $\left(\frac{x}{p}\right)$ vaut -1 ou 1 pour x non nul et 0 pour $x = 0$.
- Pour la leçon 113, on fait une preuve légèrement différente, en prenant α dans $\mathbb{C}$.
- Dans la démonstration, τ est une somme de Gauss généralisée. Les sommes de Gauss sont liées à la notion de caractère (voir [Hin08, p. 11]).
- Il existe d'autres preuves de la loi de réciprocité quadratique, dont l'une constitue d'ailleurs un autre de mes développements. Voir par exemple [Hin08, p. 26], [Ser77, p.18], [Hin08, p. 70], [Mér06, p.389].
- Grâce à la loi de réciprocité quadratique et aux autres propriétés du symbole de Legendre, on peut calculer n'importe quel symbole de Legendre.

Questions possibles

1. Citer une application de la loi de réciprocité quadratique.
2. Citer une application des symboles de Legendre.
3. La somme $\sum_x \left(\frac{x}{p}\right)$ est nulle. N'est-ce pas vrai dans un cadre plus général ?
4. Justifier pourquoi on peut sortir la puissance q de la somme.
5. Justifier pourquoi on peut faire les changements de variables $y = 1 - ux^{-1}$ et $y = qx$.
6. Détailler la conclusion.
7. Montrer que pour tout p premier impair,
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$
8. Montrer que pour tout p premier impair,
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$
9. Calculer $\left(\frac{29}{43}\right)$.

Références

[Hin08] Marc Hindry : *Arithmétique*. Calvage & Mounet, 2008.

[Mér06] Jean-Yves Mérindol : *Nombres et algèbre*. EDP Sciences, 2006.

[Ser77] Jean-Pierre Serre : *Cours d'arithmétique*. Presses Universitaires de France, 1977.