Développement: loi de réciprocité quadratique

Arthur Maritch-Roy

Dans ce développement, on montre la loi de réciprocité quadratique par le biais des formes quadratiques. Dans tout le document, p désigne un nombre premier impair.

Définition 1. Soit $a \in \mathbb{Z}$ on définit le *symbole de Legendre*, noté $\left(\frac{a}{p}\right)$ comme valant 0 si p divise a, 1 si a est un carré modulo p et -1 sinon.

Proposition 2. (critère d'Euler)
Avec les mêmes notations :

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

En particulier, le symbole de Legendre est multiplicatif.

Démonstration. Si a est un carré, on a directement par Lagrange $a^{\frac{p-1}{2}} = 1$ dans $\mathbb{F}_p^*$. Mais puisque $\mathbb{F}_p$ est un corps, les carrés non nuls sont les seules racines de $X^{\frac{p-1}{2}} - 1$. Si $a^{\frac{p-1}{2}}$ ne vaut pas 1, c'est forcément -1 puisque son carré vaut 1. □

Proposition 3. Le nombre -1 est un carré modulo p si et seulement si p est congru à 1 modulo 4.

Démonstration. Cela découle directement du résultat précédent. □

Proposition 4. Le symbole de Legendre $\left(\frac{2}{p}\right)$ vaut $(-1)^{\frac{p^2-1}{8}}$, *i.e.* 1 si p est congru à ± 1 modulo 8 et ± 8 sinon.

Démonstration. Il s'agit de regarder le produit $\prod_{k=1}^{(p-1)/2}(2k)$ et de le découper au milieu suivant p modulo 4, d'une part on a $\left(\frac{2}{p}\right)((p-1)/2)!$ et d'autre part le résultat voulu fois $((p-1)/2)!$, par lequel on peut donc simplifier car il est inversible (par primalité de p). □

Lemme 5. Soit q premier impair et $a \in \mathbb{F}_q^*$.

$$|\{x \in \mathbb{F}_q, ax^2 = 1\}| = 1 + \left(\frac{a}{q}\right)$$

Démonstration. L'élément a est un carré mod q si et seulement si on inverse l'est, si et seulement si $X^2 - a$ a deux racines distinctes, et notre cardinal est ce nombre de racines, valant 2 ou 0 selon que a soit un carré ou non (car $\mathrm{car}(K) > 2$). □

Théorème 6. (loi de réciprocité quadratique)
Soient p, q deux nombres premiers impairs. Alors

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

Démonstration. La preuve se base sur deux dénombrements de

$$X := \{(x_1, \dots, x_p) \in \mathbb{F}_q^p, \sum_{i=1}^{p} x_i^2 = 1\} = f^{-1}(1),$$

où f est la forme quadratique sur $\mathbb{F}_q$ de matrice I_p dans la base canonique. On définit alors $d = \frac{p-1}{2}$, $a = (-1)^d$ et $J \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{F}_q)$. Soit alors f' la forme quadratique de matrice

$$\begin{pmatrix} J & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & J & 0 \\ 0 & \dots & 0 & a \end{pmatrix} \in \mathcal{M}_p(\mathbb{F}_q).$$

Cette matrice a même rang et même discriminant que I_p. Par classification des formes quadratiques sur les corps finis, M et I_p sont congruentes ; en particulier

$$|X| = |\{x \in \mathbb{F}_q^p, f'(x) = 1\}| = |\{(y_1, z_1, \dots, y_d, z_d, t) \in \mathbb{F}_q^p, 2\sum_{i=1}^{d} y_i z_i + at^2 = 1\}|.$$

On distingue alors deux possibilités :

- si $y_1 = \dots = y_d = 0$ alors les z_i sont quelconques et $at^2 = 1$ ce qui donne $q^d \left[1 + \left(\frac{a}{q}\right)\right]$ choix
- si un y_i est non nul alors il nous faut choisir $(y_1, \dots, y_d) \in \mathbb{F}_q^d \backslash \{0\}$, on a $q^d - 1$ choix pour cela, puis on choisit t (q choix), puis $(z_1, \dots, z_d)$ qui est dans un hyperplan affine fixé, on a donc q^{d-1} choix. Au total, on a $q^d(q^d - 1)$ choix.

Et au total du total, on a $|X| = q^d \left(q^d + \left(\frac{a}{q}\right)\right)$.

Passons au deuxième dénombrement, qui repose sur de la théorie des groupes. On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X par rotation. On a alors deux sortes d'orbites ; celles pour lesquelles le stabilisateur est $\mathbb{Z}/p\mathbb{Z}$ tout entier, elles sont de la forme $(x, \dots, x)$ avec $px^2 = 1$, et celles pour lesquelles le stabilisateur est trivial. L'équation aux classes donne alors :

$$|X| = \sum_{px^2=1} \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\mathbb{Z}/p\mathbb{Z}|} + \sum_{\text{les autres}} \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\{1\}|} \equiv 1 + \left(\frac{p}{q}\right) \mod p.$$

Par Euler, on a $q^d \equiv \left(\frac{q}{p}\right) \mod p$ et $\left(\frac{a}{q}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. En combinant nos deux résultats et en remarquant que nos membres sont dans $\{-1, 1\}$, on obtient la loi de réciprocité quadratique. □

Définition 7. Pour $n = p_1 \cdots p_r$ un produit de nombres premiers pas forcément distincts, on définit le *symbole de Jacobi*, noté comme le symbole de Legendre, par

$$\left(\frac{a}{p_1 \cdots p_r}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right).$$

Proposition 8. Si $a \wedge n \neq 1$, alors $\left(\frac{a}{n}\right) = 0$, et sinon il vaut ± 1. De plus, pour a, b, m, n des entiers,

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) \text{ et } \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$$

Démonstration. Cela découle directement de la définition et donc des propriétés multiplicatives du symbole de Legendre. □

Proposition 9. (loi de réciprocité quadratique, version Jacobi)
Pour m et n positifs impairs :

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{(m-1)(n-1)}{4}}, \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}, \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Proposition 10. Soit n un entier positif impair différent de 1. Alors n est premier si et seulement si

$$\forall a, a \wedge n = 1, \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \mod n.$$

Démonstration. Le sens direct découle du critère d'Euler. Pour le sens réciproque, on montre d'abord que n est sans facteur carré. On écrit pour cela $n = p^2 m$ avec p premier et on pose $a = 1 + pm$. On a alors la relation de Bezout

$$(1 - pm)a + mn = 1$$

qui montre que a et n sont premiers entre eux. Par hypothèse, on obtient donc que $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \mod n$.

Par ailleurs, le binôme de Newton montre que $a^p \equiv 1 \mod n$ donc l'ordre de a modulo n est égal à 1 ou p. Puisque $a^{n-1} \equiv 1 \mod n$, il doit diviser $n-1$ donc c'est 1. Donc n est sans facteur carré.

On écrit alors $n = p_1 \cdots p_r$ avec les (p_i) distincts. Si jamais $r \geq 2$, on choisit $\alpha_1, \ldots, \alpha_r$ tels que

- $\alpha_1 = 1$
- $\alpha_i \in [\![1, p_i - 1]\!]$
- $\left(\frac{\alpha_i}{p_i}\right) = 1$ si $1 \leq i \leq r-1$
- $\left(\frac{\alpha_r}{p_r}\right) = -1$.

D'après le théorème chinois, on considère un a unique dans $\{1, \ldots, n-1\}$ tel que $a \equiv \alpha_i \mod p_i$ pour tout i. Par définition il est premier avec n sinon un des symboles de Legendre ci-dessus serait nul. Par hypothèse, $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \mod n$. En particulier $\left(\frac{a}{n}\right) \equiv \alpha_1^{\frac{n-1}{2}} \mod p_1 \equiv 1 \mod p_1$. Mais d'autre part

$$\left(\frac{a}{n}\right) = \left(\frac{\alpha_1}{p_1}\right) \cdots \left(\frac{\alpha_r}{p_r}\right) = -1,$$

ce qui est contradictoire. □

Proposition 11. Si n est composé, il y a au plus $\frac{\varphi(n)}{2}$ entiers compris entre 1 et $(n-1)$ tels que

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \mod n$$

Démonstration. Par multiplicativité des symboles de Jacobi, l'ensemble de tels entiers est un sous-groupe. □

Proposition 12. (test de Solovay-Strassen)
Le test consiste à tester l'égalité précédente. Si n est composé, il y a moins d'une chance sur 2^k pour que n passe k fois le test.