MathComp - Algèbre
Loi de réciprocité quadratique

Pierre-Alain Fouque

Université de Rennes 1

Septembre 2020

Agenda

Symbole de Legendre

Soient m et n des entiers relatifs. m est un résidu quadratique modulo n si $m + n\mathbb{Z}$ est un carré dans $\mathbb{Z}/n\mathbb{Z}$: il existe $a \in \mathbb{Z}$ tq $m = a^2 \bmod n$. (m est un carré modulo n)

Definition

Soient p un nombre premier et n un entier relatif. On note $\left(\frac{n}{p}\right)$ l'entier défini comme suit. On a :

1. $\left(\frac{n}{p}\right) = 0$ si p divise n
2. $\left(\frac{n}{p}\right) = 1$ si p ne divise pas n et si n est un carré mod p
3. $\left(\frac{n}{p}\right) = -1$ si n n'est pas un résidu quadratique mod p

Example

1. $\left(\frac{n}{2}\right) = n \bmod 2$
2. $\left(\frac{n}{3}\right) = n \bmod 3$

Critère d'Euler

Proposition

Soit p un nombre premier impair. On a

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

(-1 est un carré modulo p ssi on a $p = 1 \bmod 4$)

Theorem (Critère d'Euler)

Soit p un nombre premier impair. Pour tout entier relatif n,

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

Lemme

Soit p un nombre premier impair. L'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$ est un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $\frac{p-1}{2}$

Symbole Legendre et plus petit non résidu quadratique

Corollary (Multiplicité)

Soit p un nombre premier. Quels que soient les entiers m et n,

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$$

De plus, si n n'est pas divisible par p,

$$\left(\frac{mn^2}{p}\right) = \left(\frac{m}{p}\right)$$

Proposition

Soit p un nombre premier impair. Soit n le plus petit entier naturel qui ne soit pas un résidu quadratique modulo p. On a

$$n < 1 + \sqrt{p}$$

Le symbole $\left(\frac{2}{p}\right)$

Proposition

Soit p un nombre premier impair. On a

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

(2 est un carré mod p ssi on a $p = \pm 1 \mod 8$)

Lemme (Gauss)

Soit a un entier relatif non divisible par p,

$$\left(\frac{a}{p}\right) = \prod_{s \in S} e_s(a)$$

Sommes de Gauss

Definition (Somme de Gauss)

Soient q un nombre premier impair, A un anneau commutatif, d'élément neutre multiplicatif $1 = 1_A$, et α un élément de A tq $1 + \alpha + \ldots + \alpha^{q-1} = 0$ i.e. $\alpha^q = 1$ (α racine q-ième de l'unité) α^i et $\left(\frac{i}{q}\right)$ ne dépendent que de la classe de i mod q,

$$\tau = \sum_{i \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{i}{q}\right)\alpha^i = \sum_{i=0}^{q-1} \left(\frac{i}{q}\right)\alpha^i$$

Theorem

1. $\tau^2 = (-1)^{\frac{q-1}{2}} q$
2. *p nombre premier impair distinct de q. Si $p\alpha = 0$,*

$$\tau^p = \left(\frac{p}{q}\right)\tau$$

Loi de réciprocité quadratique

Montrer que

$$\tau = \sum_{i=0}^{q-1} \alpha^{i^2}$$

Theorem (Conjecturée par Euler, 1783, montrée par Gauss, 1796)

Soient p et q deux nombres premiers impairs distincts. On a

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \text{ si } p \text{ ou } q \text{ est congru à 1 modulo 4,}$$

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \text{ sinon.}$$

Symbole de Jacobi

Definition

Soient m un entier relatif et n un entier naturel impair,

1. $\left(\frac{m}{1}\right) = 1$
2. Si $n \geq 3$ tq $n = p_1 \dots p_r$ (pas nécessairement distincts)

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{r} \left(\frac{m}{p_i}\right), \text{ donc } \left(\frac{m}{n}\right) = 0, -1 \text{ ou } 1$$

Proposition

1. $\left(\frac{m}{n}\right) = 0$ *ssi m et n ne sont pas premiers entre eux*
2. $\left(\frac{m}{n}\right)$ *ne dépend que la classe de m mod n*
3. $\left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right)$ *et* $\left(\frac{m}{nn'}\right) = \left(\frac{m}{n}\right)\left(\frac{m}{n'}\right)$
4. *Si m et n sont premiers entre eux,* $\left(\frac{m^2}{n}\right) = 1$ *et* $\left(\frac{m}{n^2}\right) = 1$

La loi de réciprocité quadratique aux symboles de Jacobi

Example

$\left(\frac{m}{n}\right) = 1$ n'mplique pas que m soit un carré mod n

Theorem

Soient m et n des entiers naturels impairs.

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

Autrement dit, on a

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) \textit{ si } m \textit{ ou } n \textit{ est congru à } 1 \textit{ mod } 4,$$

$$\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right) \textit{ sinon.}$$