The Higher Arithmetic

H. Davenport

Louis de Forcrand, Kamil Khettabi et Dylan Müller
accompagnés par Charlotte Baumgart et Alan Morier
à l'occasion de PRIMES-Switzerland

16 juin 2018

La loi de la réciprocité quadratique

Fil conducteur

- Énoncé de la loi
- Congruences
- Résidus quadratiques
- Une propriété sur les résidus quadratiques
- Symbole de Legendre
- Critère d'Euler
- Lemme de Gauss
- La conjecture d'Euler
- Preuve de la loi de réciprocité quadratique

Réciprocité quadratique

Approche intuitive

Quand est-ce que $x^k - a$ est divisible par nombre premier donné p ?

Y-a-t-il un lien entre l'existence de x tels que

$$p|(x^2 - q)$$

et l'existence de y tels que

$$q|(y^2 - p)$$

Réciprocité quadratique

Enoncé de la loi

Soient p et q deux nombres premiers plus grands que 2, si

$$p, q \equiv 3 \pmod 4$$

alors on a :

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

sinon on a :

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

Où $\left(\frac{p}{q}\right)$ est le symbole de Legendre de p et q

Réciprocité quadratique

Reformulation symbolique

Cela peut se traduire symboliquement de la manière suivante :

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

Congruence

Défintion

Soient $a, b \in \mathbb{Z}, n \in \mathbb{N}$, on définit la congruence comme suit :

$$a \equiv b \pmod{n}$$

$$\Longleftrightarrow$$

$$a - b \in n\mathbb{Z}$$

Rappel sur la congruence

Exemples

- $771 \equiv 1 \pmod 2$
- $574 \equiv 2 \pmod{52}$
- $17^n \equiv (-1)^n \pmod{18}$
- $x^2 \equiv 0, 1, 4 \pmod 8$

Résidu quadratique

Définition

Soit $p > 2$ un nombre premier, et a un entier. On dit que a est un ***résidu quadratique*** $\pmod{p}$ ssi l'équation

$$x^2 \equiv a \pmod{p}$$

est soluble dans $\mathbb{Z}$.

Résidu quadratique

Exemples

- $8^2 \equiv 7 \pmod{19}$
- Quelque soit le premier p, $1^2 \equiv 1 \pmod{p}$
- On montrera plus bas que si $p > 2$ est un premier, alors -1 est un résidu quadratique $\pmod{p}$ ssi

$$p \equiv 1 \pmod{4}$$

Résidu quadratique

Remarque

Affirmation :
Les nombres $1^2, 2^2, ..., (\frac{p-1}{2})^2$ sont exactement les résidus (mod p). Ainsi il y a exactement $\frac{p-1}{2}$ résidus et $\frac{p-1}{2}$ non-résidus.

Preuve :
D'une part, si $1 \leq q, r \leq \frac{p-1}{2}$, alors

$$\begin{aligned} & q^2 \equiv r^2 \pmod{p} \\ \Rightarrow\ & (q-r)(q+r) \equiv 0 \pmod{p} \\ \Rightarrow\ & q \equiv r \text{ ou } q \equiv -r \pmod{p} \end{aligned}$$

D'autre part,

$$q^2 \equiv (-q)^2 \equiv (p-q)^2 \pmod{p}$$

Une propriété des résidus quadratiques

Proposition

Soient $p > 2$ un premier, a,b des entiers.
Le produit ab est un résidu ssi a et b ont le même caractère quadratique.

Une propriété des résidus quadratiques

Preuve 1

Posons $k := \frac{p-1}{2}$. Par la remarque précédente, il y a exactement k résidus et k non-résidus, ainsi on pose

$$R_1, ..., R_k \text{ les résidus}$$

$$N_1, ..., N_k \text{ les non-résidus}$$

1. $R_i R_j \equiv (x^2)(y^2) \equiv (xy)^2 \pmod{p}$
2. $R_i, ..., (p-1)R_i \equiv 1, ..., p-1$
3. $N_i, ..., (p-1)N_i \equiv 1, ..., p-1$

Une propriété des résidus quadratiques

Preuve 2

Lemme (sans démonstration) : Il existe g un entier tel que lorsqu'on regarde modulo p on a :

$$g, g^2, ..., g^{p-1} \equiv 1, 2, ..., p-1$$

□

Ainsi pour tout entier n non congru à 0, il existe un unique entier $1 \leq a \leq p-1$, nommé ***indice*** de n, tel que

$$g^a \equiv n \pmod{p}$$

Une propriété des résidus quadratiques

Preuve 2 (suite)

Affirmation :
n est un résidu quadratique *ssi* son indice est pair.

Soient donc x,y les indices de a,b respectivement. On a :

$$ab \equiv g^x g^y \equiv g^{x+y} \pmod{p}$$

□

Symbole de Legendre

Définition

On définit le symbole de Legendre de a et p par :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{a est résidu} \\ -1 & \text{sinon} \end{cases}$$

Symbole de Legendre

Remarque/propriété

Grâce à la proposition précédente, on a la propriété :

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Symbole de Legendre

Exemples

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

$$\left(\frac{3}{7}\right) = -1 \qquad \left(\frac{2}{7}\right) = 1$$

$$\left(\frac{6}{7}\right) = -1 \qquad \left(\frac{n}{p}\right)^2 = 1$$

Critère d'Euler

Enoncé

Soit $p > 2$ un premier et soit a un entier (non-congrue à 0). On a :

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

Critère d'Euler

Preuve

Lemme : (Petit théorème de Fermat)

$$a^{p-1} \equiv 1 \pmod{p}$$

Preuve du lemme :

$$\begin{aligned} & a, 2a, ..., (p-1)a \equiv 1, 2, ..., p-1 \\ \Rightarrow \quad & a^{p-1}(p-1)! \equiv (p-1)! \pmod{p} \\ \Rightarrow \quad & a^{p-1} \equiv 1 \pmod{p} \end{aligned}$$

□

Critère d'Euler

Preuve (suite)

Sachant que

$$\begin{aligned} & x^2 \equiv 1 \pmod{p} \\ \Rightarrow \quad & x \equiv -1 \text{ ou } x \equiv 1 \pmod{p} \end{aligned}$$

On a :

$$\begin{aligned} & a^{p-1} \equiv 1 \pmod{p} \\ \Rightarrow \quad & a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p} \end{aligned}$$

Critère d'Euler

Preuve (suite)

Maintenant soit k l'indice de a. Il vient :

$$\begin{aligned} & a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\ \iff & g^{k\frac{p-1}{2}} \equiv 1 \pmod{p} \\ \iff & k \text{ est pair} \\ \iff & a \text{ est un résidu} \end{aligned}$$

□

Critère d'Euler

Application

Soit $p > 2$ un nombre premier.

- Si $p \equiv 1 \pmod 4$ alors $\frac{p-1}{2}$ est pair et donc

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

- Si $p \equiv 3 \pmod 4$ alors $\frac{p-1}{2}$ est impair, il en découle :

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

Lemme de Gauss

Enoncé

Soit $p > 2$ un nombre premier, soit $P := \frac{p-1}{2}$, on considère les nombres

$$a, 2a, ..., Pa$$

Plus précisement leurs plus petits résidus positifs modulo p.
On pose n le nombre de ces résidus plus grand que $\frac{p}{2}$
Le lemme de Gauss énonce donc :

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

Lemme de Gauss

Preuve

Affirmation :

$$a, 2a, ..., Pa \equiv \pm 1, \pm 2, ..., \pm P$$

Preuve

1. $ak \equiv am \Rightarrow k \equiv m$
2. $ak \equiv -am \Rightarrow k + m \equiv 0$

□

Ainsi il vient :

$$a^P P! \equiv (-1)^n P!$$

$$\Rightarrow a^{\frac{p-1}{2}} = a^P \equiv (-1)^n$$

Le critère d'Euler permet de conclure.

□

La conjecture d'Euler

Enoncé

Soit $p, q > 2$ deux nombres premiers, soit a un entier.
Si

$$p \equiv \pm q \pmod{4a}$$

alors

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

Preuve de la loi de la réciprocité quadratique

Preuve

On doit montrer que :

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

Soient donc $p, q > 2$ des nombres premiers.

Preuve de la loi de la réciprocité quadratique

Preuve (suite)

Cas 1 :

$$p \equiv q \pmod 4$$

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

Il s'ensuit :

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

Preuve de la loi de la réciprocité quadratique

Preuve (suite)

Cas 2 :

$$p \equiv -q \pmod 4$$

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

D'où :

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = 1$$

□

Loi de la réciprocité quadratique

Exemple

On se propose de calculer :

$$\left(\frac{51}{97}\right)$$

On a :

$$\left(\frac{51}{97}\right) = \left(\frac{3 \cdot 17}{97}\right) = \left(\frac{3}{97}\right)\left(\frac{17}{97}\right)$$

$$= \left(\frac{97}{3}\right)\left(\frac{97}{17}\right) = \left(\frac{1}{3}\right)\left(\frac{12}{17}\right) = \left(\frac{3}{17}\right)$$

$$= \left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

Remerciements

Euler et Gauss pour des raisons évidentes, ainsi que le Massachusetts Institute of Technology pour avoir mis en place ce programme et Claude Eicher qui est venu nous écouter, et bien sûr Alan Morier et Charlotte Baumgart pour nous avoir accompagné ce semestre.