

## DM 6 - Loi de réciprocité quadratique

Dans tout le sujet,  $p$  désigne un nombre premier impair. Un entier  $a$  non divisible par  $p$  est un carré modulo  $p$  s'il existe un entier  $n$  tel que  $a \equiv n^2 [p]$ .

### 1 Symbole de Legendre

Pour tout entier  $a$ , on note  $\left(\frac{a}{p}\right)$  le symbole de Legendre défini par

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divise } a ; \\ 1 & \text{si } a \text{ est un carré modulo } p ; \\ -1 & \text{sinon.} \end{cases}$$

Par définition,  $\left(\frac{a}{p}\right)$  ne dépend que de la classe de congruence de  $a$  modulo  $p$  : si  $a \equiv b [p]$ , alors  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ .

Pour tout  $x \in \mathbb{Z}$  non divisible par  $p$ , on note  $r_p(x) \in \llbracket 1, p-1 \rrbracket$  son reste dans la division euclidienne par  $p$ . On définit  $\theta_p : \llbracket 1, p-1 \rrbracket \rightarrow \llbracket 1, p-1 \rrbracket$  par  $\theta_p(x) = r_p(x^2)$ .

1. Identifier l'image de  $\theta_p$  et montrer que chacun des éléments de l'image a exactement deux antécédents par  $\theta_p$ .
2. En déduire que dans  $\llbracket 1, p-1 \rrbracket$ , exactement  $\frac{p-1}{2}$  entiers sont des carrés modulo  $p$ .
3. Montrer que pour tout  $a \in \llbracket 1, p-1 \rrbracket$ ,  $a^{\frac{p-1}{2}} \equiv \pm 1 [p]$ .

On admet<sup>1</sup> que l'ensemble des  $a \in \llbracket 1, p-1 \rrbracket$  tels que  $a^{\frac{p-1}{2}} \equiv 1 [p]$  a pour cardinal au plus  $\frac{p-1}{2}$ .

#### 4. Critère d'Euler.

(a) Montrer le critère d'Euler :  $\forall a \in \mathbb{Z}, \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} [p]$ .

(b) En déduire que pour tous  $a, b \in \mathbb{Z}, \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$ .

---

<sup>1</sup>C'est une conséquence du fait que  $\mathbb{Z}/p\mathbb{Z}$  est un corps et du cours à venir sur les polynômes.

- (c) En limitant les calculs, déterminer si 5 est un carré modulo 23.
- (d) Expliciter le critère d'Euler pour  $a = -1$ .

On note  $S_p = \{1, \dots, \frac{p-1}{2}\}$ .

5. **Un (autre) lemme de Gauss.** Soit  $a \in \mathbb{Z}$ , non divisible par  $p$ .

- (a) Montrer que pour tout  $s \in S_p$ , il existe un unique couple  $(e_s(a), s_a) \in \{\pm 1\} \times S_p$  tel que  $as \equiv e_s(a)s_a [p]$ .
- (b) Montrer que l'application  $f : S_p \rightarrow S_p$  est une bijection.
- (c) En considérant le produit  $\prod_{s \in S_p} s$ , montrer que  $a^{\frac{p-1}{2}} \equiv \prod_{s \in S_p} e_s(a) [p]$ .
- (d) En déduire le lemme de Gauss :  $\left(\frac{a}{p}\right) = \prod_{s \in S_p} e_s(a)$ .

6. On cherche à déduire du lemme de Gauss la valeur de  $\left(\frac{2}{p}\right)$ .

- (a) A quelle condition sur  $s \in S_p$ , a-t-on  $2s \in S_p$  ? En déduire que  $\left(\frac{2}{p}\right) = (-1)^{n(p)}$ , où  $n(p)$  est le nombre d'entiers  $u$  tels que  $\frac{p-1}{4} < u \leq \frac{p-1}{2}$ .
- (b) Calculer  $n(p)$ , selon que  $p$  est congru à 1, -1, 3 ou -3 modulo 8.
- (c) En déduire que  $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1 [8]; \\ -1 & \text{si } p \equiv \pm 3 [8]. \end{cases}$

En guise d'application, montrons qu'il existe une infinité de nombres premiers congrus à -1 modulo 8. On raisonne par l'absurde en supposant qu'il y a un ensemble fini  $\{p_1, \dots, p_n\}$  de tels nombres premiers. On note  $N = (4p_1 \dots p_n)^2 - 2$ .

- (d) Montrer que tous les diviseurs premiers impairs  $p$  de  $N$  sont tels que  $p \equiv \pm 1 [8]$ .
- (e) Aboutir à une contradiction, en considérant  $\frac{N}{2}$ .

La loi de réciprocité quadratique dont une preuve est proposée à la section suivante affirme que si  $p$  et  $q$  sont deux nombres premiers impairs distincts, alors  $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$ .

Autrement dit, si  $p$  ou  $q$  est congru à 1 modulo 4, alors  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ ; sinon  $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ .

Couplée avec la multiplicativité du symbole de Legendre (question 5.b) et les calculs de  $\left(\frac{-1}{p}\right)$  et  $\left(\frac{2}{p}\right)$  (questions 5.d et 7.c), la loi de réciprocité quadratique permet de calculer rapidement  $\left(\frac{a}{p}\right)$ , pour un entier  $a$  quelconque.

7. Déterminer pour quels premiers impairs  $p$ , 3 est un carré modulo  $p$ .
8. Montrer que 101 n'est pas un carré modulo 641.

## 2 Une démonstration de la loi de réciprocité quadratique

Une première démonstration de la loi de réciprocité quadratique a été donnée par Gauss en 1801. Nous suivons celle donnée par Eisenstein en 1845.

9. Soit  $m = 2n + 1$  un entier naturel impair. On cherche à montrer l'identité

$$\forall x \in \mathbb{R} \setminus \pi\mathbb{Z}, \frac{\sin(mx)}{\sin x} = (-4)^n \prod_{j=1}^n \left( \sin^2 x - \sin^2 \frac{2\pi j}{m} \right).$$

- (a) Montrer que  $\forall x \in \mathbb{R} \setminus \pi\mathbb{Z}, \frac{\sin(mx)}{\sin x} = \sum_{j=0}^n \binom{2n+1}{2j+1} (-1)^j (\sin^2 x)^j (1 - \sin^2 x)^{n-j}$ .

On considère le polynôme  $P = \sum_{j=0}^n \binom{2n+1}{2j+1} (-1)^j X^j (1 - X)^{n-j}$ .

- (b) Montrer que les réels  $\sin^2 \frac{2\pi j}{m}$ , pour  $j \in \llbracket 1, n \rrbracket$ , sont des racines distinctes de  $P$ .
- (c) En déduire qu'il existe  $\lambda \in \mathbb{R}$  tel que  $P = \lambda \prod_{j=1}^n \left( X - \sin^2 \frac{2\pi j}{m} \right)$ .
- (d) Identifier la valeur de  $\lambda$  et conclure.

Soient  $p$  et  $q$  deux nombres premiers impairs distincts. On rappelle qu'on note  $S_p = \left\{ 1, \dots, \frac{p-1}{2} \right\}$  et  $S_q = \left\{ 1, \dots, \frac{q-1}{2} \right\}$ .

10. En utilisant le lemme de Gauss, montrer que  $\left( \frac{q}{p} \right) = \prod_{s \in S_p} \frac{\sin \frac{2\pi qs}{p}}{\sin \frac{2\pi s}{p}}$ .
11. En déduire que  $\left( \frac{q}{p} \right) = \prod_{s \in S_p} (-4)^{\frac{q-1}{2}} \prod_{t \in S_q} \left( \sin^2 \frac{2\pi s}{p} - \sin^2 \frac{2\pi t}{q} \right)$ .
12. Conclure.