



Mathématiques

DEVOIR EN TEMPS LIBRE N°2

Lundi 21 octobre 2002

Les deux problèmes sont indépendants.

On prendra bien soin de préciser toute notation non donnée dans l'énoncé. Toute affirmation devra être justifiée et on hésitera pas à faire référence aux propriétés utilisées.

Il n'est pas interdit d'admettre certains éléments de démonstration (voire des questions entières) afin de ne pas rester bloqué. Mais ils doivent absolument être mentionnés.

On laissera une marge à gauche.

Enfin, les solutions doivent être rédigées et le formalisme utilisé avec parcimonie.

Problème 1 : Lemme de Cauchy

Soit $n \in \mathbb{N}^*$. Soient G un groupe fini d'ordre n dont la loi interne est notée multiplicativement et $p \in \mathbb{N}^*$ un nombre premier divisant n .

On note 1 l'élément neutre de G , $E = \{(x_1, x_2, \dots, x_p) \in G^p, x_1 x_2 \dots x_p = 1\}$, S le sous-groupe de $\mathcal{S}_p$ engendré par le cycle $[1, 2, \dots, p]$ de longueur p .

Enfin, on définit sur E la relation binaire $\mathcal{R}$ de la manière suivante : pour tout $(x_1, \dots, x_p)$ et $(y_1, \dots, y_p)$ dans E , $(x_1, \dots, x_p) \mathcal{R} (y_1, \dots, y_p)$ si et seulement s'il existe $\sigma \in S$ tel que pour tout $i \in \llbracket 1, p \rrbracket$, on ait $y_i = x_{\sigma(i)}$.

1) a. Quelle est la signature de $[1, 2, \dots, p]$?

b. Quel est l'ordre de S ? S est-il abélien?

c. Expliciter S lorsque $p = 5$.

2) a. Montrer que $\mathcal{R}$ est une relation d'équivalence.

b. Soient $(x_1, x_2, \dots, x_p) \in E$ et $\sigma \in S$. Montrer que $(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(p)}) \in E$ (on commencera à le prouver pour $\sigma = [1, 2, \dots, p]$).

c. Soient $(x_1, \dots, x_p) \in E$ et $H = \{\sigma \in S, \forall i \in \llbracket 1, p \rrbracket, x_i = x_{\sigma(i)}\}$. Montrer que H est un sous-groupe de S . En déduire que $H = \{1\}$ ou S .

d. Montrer que chaque classe modulo $\mathcal{R}$ possède 1 ou p éléments.

3) a. Calculer $\text{Card} E$.

b. On note r (resp. s) le nombre de classes modulo $\mathcal{R}$ de cardinal 1 (resp. p). Montrer que $n^{p-1} = r + sp$.

4) En déduire l'existence d'un élément de G d'ordre p .

Conclusion : Ainsi, pour tout groupe fini d'ordre n et tout diviseur premier p de n , il existe un élément de G d'ordre p . Ce résultat constitue le lemme de Cauchy.

Problème 2 : Théorème des deux carrés

Dans tout le problème, p désigne un nombre premier et $\mathcal{P}$ l'ensemble des nombres premiers.

On note N l'ensemble des entiers naturels qui s'écrivent comme somme de deux carrés d'entiers :

$$N = \{n \in \mathbb{N}, \exists (a, b) \in \mathbb{Z}^2, n = a^2 + b^2\}$$

Si $n \in \mathbb{N}^*$, le théorème fondamental de l'Arithmétique permet d'écrire la décomposition de n en produit de facteurs premiers :

$$n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$$

où $(\nu_p(n))_{p \in \mathcal{P}}$ est une famille à support fini de $\mathbb{N}$.

I. Petit théorème de Fermat :

1) Soit $a \in \mathbb{Z}$. On suppose que p ne divise pas a . Montrer que :

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

2) Montrer que 13 divise $2^{70} + 3^{70}$.

3) Soit $n \in \mathbb{N}^*$. Montrer que 21 divise $2^{4n} + 5$.

II. Le théorème de Wilson :

Soit $K = \mathbb{Z}/p\mathbb{Z}$.

1) Soit $x \in K$. Montrer que si $x^2 = 1$, alors $x = 1$ ou $x = -1$.

2) En déduire que $(p-1)! \equiv -1 \pmod{p}$ (on associera $x \in K^*$ et $x^{-1} \in K^*$).

3) Soit $n \in \mathbb{N}^*$. On suppose que $(n-1)! \equiv -1 \pmod{n}$. Montrer que n est premier.

III. Dénombrement des carrés dans $\mathbb{Z}/p\mathbb{Z}$:

On suppose $p \geq 3$ et on pose $K = \mathbb{Z}/p\mathbb{Z}$ et :

$$C = \{a \in K^*, \exists x \in K^*, x^2 = a\}$$

1) Montrer que

$$\begin{array}{ccc} K^* & \longrightarrow & K^* \\ f : x & \longmapsto & x^2 \end{array}$$

est un morphisme de groupes. Préciser son noyau. En déduire que C est un sous-groupe de K^* et préciser son cardinal.

Soit $a \in K^*$. On dit que x et x' dans K^* sont associés si $xx' = a$. L'associé de x est $x' = ax^{-1}$, il est unique.

2) On suppose $a \in C$.

a. Combien y a-t-il de $x \in K^*$ associés à eux-mêmes? Que vaut leur produit?

b. En déduire :

$$\overline{(p-1)!} = \prod_{x \in K^*} x = -a^{\frac{p-1}{2}}$$

3) On suppose $a \notin C$.

a. Combien y a-t-il de $x \in K^*$ associés à eux-mêmes?

b. En déduire :

$$\overline{(p-1)!} = \prod_{x \in K^*} x = a^{\frac{p-1}{2}}$$

- 4) Conclure que $a \in C$ si, et seulement si, $a^{\frac{p-1}{2}} = 1$. Que vaut $a^{\frac{p-1}{2}}$ sinon?
- 5) Montrer l'équivalence des deux propositions suivantes :
 - (i) -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$;
 - (ii) $p \equiv 1 \pmod{4}$.

IV. Stabilité de N par multiplication

Soit A l'ensemble des matrices M de $\mathcal{M}_2(\mathbb{Z})$ tel qu'il existe $(a, b) \in \mathbb{Z}^2$ tel que :

$$M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

- 1) Montrer que A muni des opérations usuelles sur les matrices est un anneau.
- 2) Soit $M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in A$. Calculer $\det M$. Préciser les éléments inversibles de l'anneau A .
- 3) Démontrer que N est stable par multiplication.

V. Valuation p -adique d'un élément de N lorsque $p \equiv 3 \pmod{4}$

On suppose p toujours premier et $p \equiv 3 \pmod{4}$. Soit $n \in N$. On suppose $\nu_p(n) > 0$ i.e. $p|n$. Il existe $(a, b) \in \mathbb{Z}^*$ tel que $n = a^2 + b^2$.

- 1) Montrer que $p|a$ ou $p|b$ (on pourra utiliser **III.5**).
- 2) En déduire que $p^2|n$.
- 3) Conclure que $\nu_p(n)$ est pair.

VI. $p \in N$ lorsque $p \equiv 1 \pmod{4}$

- 1) Montrer que $2 \in N$.
- On suppose p toujours premier et $p \equiv 1 \pmod{4}$. On pose $I = \{k \in \mathbb{N}^*, kp \in N\}$.

- 2) Montrer que I est non vide (on pourra utiliser **III.5**).

On note $m_0 = \min I$. Il existe donc $(a, b) \in \mathbb{N}^2$ tel que $m_0 p = a^2 + b^2$.

- 3) On suppose $m_0 > 1$.

a. Montrer que $m_0 < p$.

b. Montrer que m_0 est premier avec a et premier avec b .

c. Etablir l'existence de $(a', b') \in \mathbb{Z}^2$, $0 < m_1 < m_0$ tels que, modulo m_0 , $a \equiv a'$ et $b \equiv b'$

et :

$$a'^2 + b'^2 = m_1 m_0$$

d. En déduire que :

$$(aa' + bb')^2 + (a'b - ab')^2 = m_1 m_0^2 p$$

e. Démontrer que $m_1 \in I$ et aboutir à une contradiction. Quelle conclusion peut-on en tirer?

VII. Théorème des deux carrés :

- 1) Soit $n \in \mathbb{N}^*$. Montrer l'équivalence des deux conditions suivantes :
 - (i) $n \in N$, i.e. n est somme de deux carrés.
 - (ii) Pour tout nombre premier p tel que $p \equiv 3 \pmod{4}$, $\nu_p(n)$ est pair.
- 2) Montrer que $29250 \in N$ et écrire 29250 comme somme de deux carrés.