XMP 2021-2022

ANNEAUX ET ARITHMÉTIQUE

1. Propriétés diverses dans un anneau

a. Soit I un idéal d'un anneau commutatif A contenant une unité de A (*i.e.* un élément inversible de A). Prouver que $I = A$.

b. Montrer qu'un anneau commutatif A ne contenant pas d'autre idéal que $\{0\}$ et lui-même est un corps.

c. Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante (au sens de l'inclusion) d'idéaux d'un anneau commutatif A. Prouver que $I = \bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A.

d. Soit A un anneau. On appelle *caractéristique* de A le plus petit entier positif non nul n, s'il existe, tel que $n.1_A = 0_A$ (si un tel entier n'existe pas, on dit que A est de caractéristique nulle).

Quelle est la caractéristique de $\mathbb{Q}$, de $\mathbb{R}$, de $\mathbb{C}$, de $\mathbb{Z}/n\mathbb{Z}$?

Prouver qu'un anneau intègre est soit de caractéristique nulle, soit de caractéristique égale à un nombre premier.

Prouver qu'un anneau de caractéristique nulle contient un sous-corps isomorphe à $\mathbb{Q}$.

e. Un élément a d'un anneau commutatif A est dit *nilpotent* s'il existe un entier n tel que $a^n = 0_A$.

Quels sont les éléments nilpotents de $\mathbb{Z}/36\mathbb{Z}$?

Montrer que l'ensemble des éléments nilpotents d'un anneau commutatif A est un idéal de A.

Montrer que si a est nilpotent, $1_A - a$ est inversible, et déterminer son inverse (on écrira $1_A = 1_A - a^n$).

f. Soit A un anneau, U le groupe de ses unités. Soient a et b deux éléments de A. Prouver que :

$$1_A - ab \in U \Leftrightarrow 1_A - ba \in U\,.$$

---

2. Soit $\mathbb{K}$ un corps à 4 éléments, de neutres 0 et 1.

a. Prouver que $1+1=0$.

b. Soit a un élément de $\mathbb{K}$ autre que 0 et 1. Qui est le dernier élément de $\mathbb{K}$?

c. Dresser les tables de $(\mathbb{K},+)$ et de $(\mathbb{K}^*,\times)$. Conclure.

---

3. On note $\mathbb{H} = \left\{\begin{bmatrix} a & -\overline{b} \\ b & \overline{a}\end{bmatrix},\ a,b\in\mathbb{C}\right\}$. Prouver que $\mathbb{H}$ est un sous-anneau non commutatif de $\mathcal{M}_2(\mathbb{C})$, et que tout élément non nul de $\mathbb{H}$ possède un inverse dans $\mathbb{H}$. $\mathbb{H}$ *s'appelle le corps des quaternions d'Hamilton, bien qu'à strictement parler ce ne soit pas un corps au sens du programme de MP puisqu'il n'est pas commutatif.*

---

4. Pour n entier, déterminer le pgcd de $10n+1$ et de $4n-3$.

---

5. Quel est le dernier chiffre (en base 10) de $7^{7^{7^{7^{7}}}}$?

---

6. Quels sont les entiers qui sont différence de deux carrés ?

---

7. Résoudre dans $\mathbb{Z}/37\mathbb{Z}$:

a. $\begin{cases} 3x+7y=3 \\ 6x-7y=0 \end{cases}$

b. $x^2-4x+8=0$ (*indication* : $6^2=-1$).

---

8. On écrit un entier n en base 10. Prouver que n est multiple de 17 si et seulement si le nombre N égal à 5 fois le dernier chiffre de n moins le nombre égal à n privé de son dernier chiffre est lui-même multiple de 17.

4513 est-il multiple de 17 ?

---

9. Résoudre, dans $\mathbb{Z}/91\mathbb{Z}$, l'équation $x^2-3x+2=0$.

---

10. On fixe un nombre premier p supérieur ou égal à 3.

a. Prouver (penser à Fermat) que si p est de la forme $4n+3$, -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.

b. On suppose que p est de la forme $4n+1$. En écrivant que $x^{p-1}-1=(x^{\frac{p-1}{2}}-1)(x^{\frac{p-1}{2}}+1)$, prouver que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

c. Résoudre, dans $\mathbb{Z}/p\mathbb{Z}$, l'équation $x^2=y^2$. En déduire le nombre de carrés de $\mathbb{Z}/p\mathbb{Z}$, puis que tout élément de $\mathbb{Z}/p\mathbb{Z}$ est somme de deux carrés.

---

11. **a.** Prouver que pour que 2^n-1 soit premier, il faut que n le soit.

b. Prouver que pour que 2^n+1 soit premier, il faut que n soit une puissance de 2.

---

12. On note $\mathbb{Z}[\mathrm{i}]$ l'ensemble des nombres complexes de la forme $a+\mathrm{i}b$ où a et b sont dans $\mathbb{Z}$.

a. Prouver que pour tout couple (x,y) d'éléments de $\mathbb{Z}[\mathrm{i}]$ avec $y\neq 0$, il existe q et r dans $\mathbb{Z}[\mathrm{i}]$ tels que :

$$x=qy+r, \text{ avec } |r|<|y|$$

Y-a-t-il unicité d'une telle écriture ?

b. Prouver que tout idéal de $\mathbb{Z}[\mathrm{i}]$ est principal (c'est-à-dire engendré par un élément).

---

13. Soit a un entier impair et $n\geq 3$. Prouver que $a^{2^{n-2}}\equiv 1\,[2^n]$. Trouver les entiers n tels que le groupe des éléments inversibles de $\mathbb{Z}/2^n\mathbb{Z}$ soit cyclique.

---

14. <u>Morphisme de Fröbenius</u>

Soit p un nombre premier.

a. Prouver que les coefficients binomiaux $\binom{p}{k}$ sont divisibles par p pour $k=1,\ldots,p-1$.

b. Soit A un anneau commutatif de caractéristique p (cf. exercice **1.c.**). Prouver que l'application $x\mapsto x^p$ est un morphisme d'anneaux de A dans lui-même.
