XMP 2022-2023

ANNEAUX ET ARITHMÉTIQUE (1)

1. Des anneaux

a. On considère un ensemble non vide X, et l'ensemble $\mathcal{P}(X)$ de ses parties. Laquelle des lois $\cap$ et $\cup$ donne, avec la différence symétrique Δ, une structure d'anneau à $\mathcal{P}(X)$?

b. Soit $\mathbb{H}$ (comme Hamilton) l'ensemble des matrices de $\mathcal{M}_2(\mathbb{C})$ de la forme $A = \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}$. Prouver que $\mathbb{H}$ est un anneau dans lequel tout élément non nul possède un inverse. $\mathbb{H}$ est-il un corps ?

On pose $\overline{A} = \begin{pmatrix} \overline{a} & \overline{b} \\ -b & a \end{pmatrix}$. Comparer, pour A et B dans $\mathbb{H}$, $\overline{AB}$ et $\overline{B}\,\overline{A}$. Calculer $\det(A\overline{A})$, puis $\det(AB\overline{AB})$ de deux manières différentes. En déduire que le produit de deux entiers qui sont sommes de quatre carrés est lui-même une somme de quatre carrés.

---

2. 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. 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 $1_A = 1_A - a^n$).

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 $\mathbb{Q}$.

---

3. On note $\mathbb{Z}[\mathrm{i}\sqrt{2}]$ l'ensemble des nombres complexes de la forme $a + \mathrm{i}b\sqrt{2}$ où a et b sont dans $\mathbb{Z}$.

a. Prouver que $\mathbb{Z}[\mathrm{i}\sqrt{2}]$ est un anneau intègre, dont on déterminera les unités (on pourra pour ce faire prendre les modules).

b. Prouver que pour tout complexe z, il existe un élément q de $\mathbb{Z}[\mathrm{i}\sqrt{2}]$ tel que $|z - q| < 1$ (*indication :* dessin !).

En déduire que pour tout couple (x, y) d'éléments de $\mathbb{Z}[\mathrm{i}\sqrt{2}]$ avec $y \neq 0$, il existe q et r dans $\mathbb{Z}[\mathrm{i}\sqrt{2}]$ tels que :

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

c. Prouver que tout idéal de $\mathbb{Z}[\mathrm{i}\sqrt{2}]$ est principal (c'est-à-dire engendré par un élément).

---

4. Prouver qu'il existe une infinité d'entiers premiers de la forme $4n - 1$ (on pourra supposer qu'il n'y en a qu'un nombre fini $q_1, \ldots, q_k$ et poser $Q = 4q_1 \ldots q_k - 1$: que dire des diviseurs premiers de Q ?).

5. **a.** Par combien de zéros se termine l'écriture décimale de 2020! ?

b. Trouver 2020 entiers consécutifs dont aucun n'est premier.

c. Prouver que tout entier s'écrivant $abcabc$ en base 10 est multiple à la fois de 7, 11 et 13.

Comment le résultat découvert à la question précédente permet-il d'obtenir un test de divisibilité commun aux trois entiers 7, 11 et 13 ? Que donne ce test appliqué à 2018 ?

---

6. Soit p un nombre premier.

a. Soient a, b et c trois entiers tels que $a \wedge c = b \wedge c = 1$. Prouver que $(ab) \wedge c = 1$.

b. Prouver que pour tout entier $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k} k!$ puis p divise $\binom{p}{k}$.

c. Prouver (par récurrence) que pour tout entier n, $n^p \equiv n\ [p]$. En déduire que si p ne divise pas n, $n^{p-1} \equiv 1\ [p]$.

---

7. **a.** Chercher tous les entiers x tels que l'on ait simultanément les deux congruences : $x \equiv 3\ \ [7]$ et $x \equiv 2\ \ [10]$.

b. Résoudre l'équation $x^2 - 3x + 2 = 0$ dans $\mathbb{Z}/77\mathbb{Z}$.

c. Quel est le dernier chiffre de l'écriture décimale de $7^{7^{7^{7^7}}}$?

---

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

b. Résoudre l'équation $x^2 + 4x - 4 = 0$ dans $\mathbb{Z}/47\mathbb{Z}$ (*indication* : $7^2 = 2\ldots$).

c. Donner le reste de la division euclidienne de $2^{10n-7} + 3^{5n-2}$ par 11.

d*. Soit a un nombre impair non multiple de 5. Montrer que $a^4 \equiv 1\ \ [10]$, puis que $a^{4\times 10^k} \equiv 1\ [10^k]$. En déduire qu'il existe un entier dont le cube, écrit en base 10, se termine par la séquence 123456789.

---

9. **a.** Énoncer le théorème de Bézout dans $\mathbb{Z}$.

b. Soient a et b deux entiers premiers entre eux. Soit $c \in \mathbb{N}$. Prouver que :

$$a \text{ divise } c \text{ et } b \text{ divise } c \iff ab \text{ divise } c.$$

c. On considère le système $(S) : \begin{cases} x \equiv 6\ [17] \\ x \equiv 4\ [15] \end{cases}$ d'inconnue $x \in \mathbb{Z}$. Déterminer une solution particulière x_0 de (S).

d. Déduire des questions précédentes *toutes* les solutions de (S).

---

10. Nombres de Mersenne, nombres de Fermat

On cherche ici des nombres premiers sous une forme particulière : $2^n - 1$ pour les nombres de Mersenne, $2^n + 1$ pour les nombres de Fermat :

a. Par quoi peut-on factoriser $a^k - b^k$?

b. Prouver que $2^n - 1$ premier implique n premier.

c. Prouver que $2^n + 1$ premier implique n est une puissance de 2.

ANNEAUX ET ARITHMÉTIQUE (2)

11. On note p_n le $n^{\text{ème}}$ nombre premier ($p_1 = 2$).

a. Prouver que $\forall x \in \mathbb{R},\ \mathrm{e}^x \geq 1 + x$.

b. Prouver que tout entier plus grand que 2 est le produit d'un carré par un produit de nombres premiers deux à deux distincts.

c. Prouver les inégalités :

$$\frac{\pi^2}{6}\mathrm{e}^{\sum_{k=1}^{n}\frac{1}{p_k}} \geq \sum_{k=1}^{n}\frac{1}{k^2}\prod_{k=1}^{n}\left[1+\frac{1}{p_k}\right] \geq \sum_{k=1}^{n}\frac{1}{k}\,.$$

d. Nature de la série $\sum \dfrac{1}{p_k}$?

---

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

---

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

---

14. Théorème de Wilson

Calculer, dans $\mathbb{Z}/n\mathbb{Z}$, le produit des classes non nulles (attention à l'exception).

En déduire que n est premier si et seulement si $(n-1)! + 1 \equiv 0[n]$.

En réassociant les termes différemment dans $(n-1)!$, prouver que si n est un nombre premier de la forme $4k+1$, -1 est un carré dans $\mathbb{Z}/n\mathbb{Z}$.

---

15. Soit p un nombre premier.

a. Résoudre, dans $\mathbb{Z}/p\mathbb{Z}$, l'équation $x^2 = y^2$.

b. Combien y-a-t-il de carrés dans $\mathbb{Z}/p\mathbb{Z}$?

c. Prouver que tout élément de $\mathbb{Z}/p\mathbb{Z}$ est somme de deux carrés.

---

16. Soit $\mathbb{K}$ un éventuel 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.
