Feuille d'exercices n° 22 **MP**
Anneaux **2024-2025**
Arithmétique

Arithmétique dans $\mathbb{Z}$

Il s'agit principalement de révisions, mais il est vivement conseillé, quand c'est pertinent, d'utiliser des calculs dans l'anneau $\mathbb{Z}/\ell\mathbb{Z}$.

($\star$) Exercice 1

1. Soient a, b, c entiers naturels tels que $a^2 = b^2 + c^2$. Démontrer que l'un au moins des trois entiers a, b, c est pair.
2. Montrer que $2^{123} + 4^{567}$ est divisible par 3.

($\star\star$) Exercice 2 Soit $n \in \mathbb{N}$.

1. Montrer que $3^{2n} - 2^n$ est multiple de 7.
2. Montrer que $6 | 5n^3 + n$ (on pourra effectuer des disjonctions de cas modulo 6).

($\star\star$) Exercice 3 Montrer qu'un entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3. De même, montrer qu'un entier est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9. Enfin, montrer qu'un nombre est divisible par 11 si et seulement si la somme alternée de ses chiffres est divisible par 11.

($\star$) Exercice 4

1. On veut découper un rectangle de 24 cm sur 40 cm en carrés dont le côté est le plus long possible, sans perte. Quel doit être le côté du carré ?
2. On dispose d'un grand nombre de rectangles du type précédent que l'on veut assembler bord à bord pour former un carré le plus petit possible. Quel doit être le côté du carré ?

($\star$) Exercice 5 En suivant l'algorithme d'Euclide :

1. déterminer $1234 \wedge 56$,
2. pour $n \in \mathbb{N}^*$, calculer $(3n + 1) \wedge (2n)$.
3. Soit (F_n) la suite, appelée suite de Fibonacci, définie par

$$F_0 = 0, \quad F_1 = 1, \text{ et } \forall n \in \mathbb{N},\ F_{n+2} = F_{n+1} + F_n$$

Montrer que pour tout $n \in \mathbb{N}$, $F_n \wedge F_{n+1} = 1$.

($\star$) Exercice 6

1. Résoudre dans $\mathbb{N}$ le système $\begin{cases} x \wedge y &= 27 \\ x \vee y &= 108 \end{cases}$
2. Résoudre dans $\mathbb{N}$ le système $\begin{cases} x \wedge y &= 5 \\ x \vee y &= 60 \end{cases}$

($\star$) Exercice 7

1. Donner une relation de Bézout pour $3080 \wedge 525$ par l'algorithme d'Euclide étendu.
2. Montrer que deux entiers naturels supérieurs ou égaux à 2 consécutifs sont premiers entre eux.

3. Résoudre l'équation $5u + 7v = 1$ dans $\mathbb{Z}$ après avoir trouvé une solution particulière.

(⋆⋆) Exercice 8

1. Montrer que pour $n \in \mathbb{N}$, $n^2(n^2 + 11)$ est divisible par 6.
2. Soit p un nombre premier supérieur ou égal à 5. Montrer que $24|p^2 - 1$.

(⋆⋆) Exercice 9 Soient $a, b \in \mathbb{N}^*$. Montrer en utilisant une valuation p-adique que si $b^2 \mid a^2$, alors $b \mid a$.

(⋆) Exercice 10 Soit $n \in \mathbb{N}$.

1. Montrer que $n^5 - n$ est divisible par 5.
2. En remarquant que $n^5 - n = n(n-1)(n+1)(n^2+1)$, montrer alors que $n^5 - n$ est divisible par 30.

(⋆⋆) Exercice 11 Calculer 2016^{2017} modulo 11.

(⋆⋆) Exercice 12 Codage - décodage

1. (a) Donner une relation de Bézout entre 26 et 11, par l'algorithme d'Euclide étendu.
   (b) En déduire un inverse dans $[\![0, 25]\!]$ de 11, c'est-à-dire $b \in [\![0, 25]\!]$ tel que $b \times 11 \equiv 1 \quad [26]$.
2. On donne les correspondances suivantes :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	16	16	17	18	19	20	21	22	23	24	25

Pour $x \in [\![0, 25]\!]$, la fonction de codage est $f(x) =$ (le reste dans la division euclidienne de $11x + 8$ par 26).

   (a) Coder L et W.
   (b) Montrer que $11x \equiv j$ [26] si et seulement si $x \equiv 19j$ [26].
   (c) Donner un procédé de décodage. Vérifier votre résultat avec la question a. Décoder le mot MAY.

Anneaux, arithmétique de MP

(⋆⋆⋆) Exercice 13 Soit α réel. Pour $n \in \mathbb{N}^*$, on considère l'application $f_n : \begin{pmatrix} \mathbb{Z} & \to & \mathbb{C}^* \\ p & \mapsto & e^{2i\pi np\alpha} \end{pmatrix}$ et on admet que f_n est un morphisme de groupes.

1. En considérant le noyau de f_n (qu'on ne cherchera pas à déterminer), montrer que f_n est injective si et seulement si $\alpha \notin \mathbb{Q}$.

Désormais, on suppose que $\alpha \in \mathbb{Q}$. On écrit α sous forme de fraction irréductible $\frac{r}{s}$ avec $r \in \mathbb{Z}$ et $s \in \mathbb{N}^*$ tels que $r \wedge s = 1$.

2. (a) Montrer que $\operatorname{Im} f_1 \subset \mathbb{U}_s$. En écrivant une relation de Bézout entre r et s, montrer que $e^{\frac{2i\pi}{s}} \in \operatorname{Im} f_1$. En déduire que $\operatorname{Im} f_1 = \mathbb{U}_s$.
   (b) Montrer que $\ker f_1 = s\mathbb{Z}$.
3. On pose $m = \frac{s}{n \wedge s}$.
   (a) Rappeler le lemme de Gauss.
   (b) Justifier que m est entier. Montrer que $nr \wedge s = n \wedge s$.
   (c) Montrer que $\operatorname{Im} f_n \subset \mathbb{U}_m$. En écrivant une relation de Bézout entre nr et s, montrer que $e^{\frac{2i\pi}{m}} \in \operatorname{Im} f_n$. En déduire que $\operatorname{Im} f_n = \mathbb{U}_m$.
   (d) Montrer que $\ker f_n = m\mathbb{Z}$.

(⋆) Exercice 14 Montrer que l'ensemble des suites réelles convergeant vers 0 constitue un idéal de l'anneau des suites réelles bornées. S'agit-il d'un idéal de l'anneau de toutes les suites réelles ?

(⋆⋆) Exercice 15 A est un anneau.

1. Montrer qu'un idéal contenant un élément inversible de A est égal à A.
2. Quels sont les idéaux d'un corps ?
3. En déduire que tout morphisme d'anneaux entre deux corps est injectif.

(⋆⋆) Exercice 16 Montrer qu'un anneau commutatif A non trivial ayant pour seuls idéaux A et $\{0\}$ est un corps.

(⋆⋆) Exercice 17 On considère l'ensemble des nombres décimaux : $\mathbb{D} = \left\{ \frac{n}{10^k} \, , \, n \in \mathbb{Z}, \, k \in \mathbb{N} \right\}$.

1. Montrer que $\mathbb{D}$ est un sous-anneau de $(\mathbb{Q}, +, \times)$ et déterminer ses éléments inversibles.
2. (a) Soit I un idéal de $\mathbb{D}$. Montrer qu'il existe $a \in \mathbb{Z}$ tel que $I \cap \mathbb{Z} = a\mathbb{Z}$.
   (b) Montrer que les idéaux de $\mathbb{D}$ sont de la forme $a\mathbb{D}$ avec $a \in \mathbb{Z}$.

(⋆) Exercice 18 Soit a un élément inversible d'un anneau. Vérifier que $f : x \mapsto axa^{-1}$ est un automorphisme de l'anneau A.

(⋆) Exercice 19 Soit $\Psi : \left(\begin{array}{ccc} (\mathcal{F}(\mathbb{R},\mathbb{R}),+,\times) & \to & (\mathbb{R},+,\times) \\ f & \mapsto & f(0) \end{array} \right)$. Montrer que Ψ est un morphisme d'anneaux.

(⋆) Exercice 20 Soit $(A, +, .)$ un anneau vérifiant : $\forall x \in A, \, x^2 = x$.

1. Montrer que pour tout $x \in A$, $x + x = 0$.
2. Montrer que pour tout $(x, y) \in A^2$, $xy = -yx$.
3. Calculer $xy(x + y)$ et en déduire que si A possède au moins 3 éléments, alors A n'est pas intègre.

(⋆) Exercice 21 Montrer que l'ensemble des nombres décimaux est un anneau. Est-ce un corps ?

(⋆⋆) Exercice 22 Montrer que $\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2}, \, x, y \in \mathbb{Q}\}$ est un corps.

(⋆) Exercice 23 Soit $A = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} , \, a, b \in \mathbb{Z} \right\}$. Montrer que $(A, +, \times)$ est un anneau. Déterminer $U(A)$.

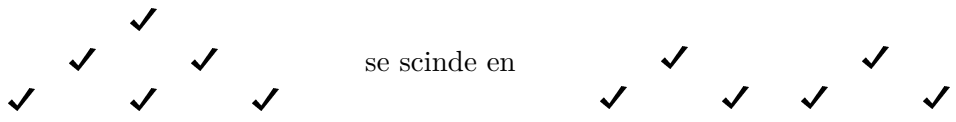
(⋆) Exercice 24 Soit A un anneau. On dit que $x \in A$ est nilpotent, s'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0_A$.

1. Montrer que si xy est nilpotent, alors yx l'est aussi.
2. On suppose que x et y commutent et que x et y sont nilpotents. Montrer que $x+y$ et xy sont nilpotents.

(⋆⋆) Exercice 25 Soit $(A, +, \times)$ un anneau commutatif. Pour $a \in A$, on appelle racine carrée de a tout élément dont le carré vaut a.

1. Prouver que si A est intègre, alors tout élément de A admet au plus deux racines carrées.
2. En revanche, prouver que dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$ la fonction constante $x \mapsto 1$ possède une infinité de racines carrées.

(☕) Exercice 26 – La migration des canards à l'aide des éléments inversibles de $\mathbb{Z}[\sqrt{2}]$.
Un vol de N canards en migration a une formation triangulaire équilatérale de r rangées, la i-ième rangée ayant i canards. Par suite d'une perturbation, le vol se scinde en 2 formations équilatérales identiques. On cherche dans cet exercice pour quelles valeurs de r ce processus est concevable, pour un nombre total de canards $N \leqslant 10000$. Par exemple,



mais le vol ci-contre ne peut pas se scinder :

Soit r le nombre de rangées du vol initial et p le nombre de rangées de chaque vol secondaire. On doit avoir $\frac{r(r+1)}{2} = 2\frac{p(p+1)}{2}$, ce qui se ramène à : $(2r+1)^2 - 2(2p+1)^2 = -1$. Nous sommes donc à la recherche de a et b entiers positifs impairs vérifiant $a^2 - 2b^2 = -1$, soit $(a+b\sqrt{2})(a-b\sqrt{2}) = -1$. Et pour cela, nous allons étudier

$$A = \{a + b\sqrt{2},\ a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{2}]$$

1. Montrer que $(A, +, \times)$ est un anneau intègre.
2. Pour $x = a + b\sqrt{2}$, on pose $N(x) = a^2 - 2b^2$.
   (a) Montrer que pour x et y dans A, $N(xy) = N(x)N(y)$.
   (b) En déduire que $x \in U(A)$ si et seulement si $N(x) = \pm 1$.
3. Montrer que $1 + \sqrt{2} \in U(A)$, et que pour $n \in \mathbb{Z}$, $(1+\sqrt{2})^n \in U(A)$ et $-(1+\sqrt{2})^n \in U(A)$.
4. Réciproquement, soit $x = a + b\sqrt{2}$ un élément inversible de A. On veut montrer qu'il existe $n \in \mathbb{Z}$ tel que $x = \pm(1+\sqrt{2})^n$.
   (a) Montrer qu'on peut se ramener au cas où a et b sont dans $\mathbb{N}$ avec $a \neq 0$.
   (b) Montrer qu'il existe $n \in \mathbb{N}$ tel que $x = (1+\sqrt{2})^n$. *Indication : si $b \geqslant 1$, considérer $x_1 = \frac{x}{1+\sqrt{2}}$.*
5. Résoudre le problème posé. On trouvera $r = 3$, $r = 20$, $r = 119$ (le suivant, $r = 696$, comporterait 242 556 canards).

(⋆) Exercice 27 Calculer $\varphi(2)$. Montrer que pour tout entier $n \geqslant 3$, $\varphi(n)$ est un nombre pair.

(⋆⋆) Exercice 28

1. Résoudre $\overline{x}^2 = \overline{x}$ dans $\mathbb{Z}/p\mathbb{Z}$ avec p premier.
2. Résoudre $\overline{x}^2 = \overline{x}$ dans $\mathbb{Z}/34\mathbb{Z}$.

(⋆) Exercice 29 Soit (I_n) une suite croissante, au sens de l'inclusion, d'idéaux de $\mathbb{K}[X]$. Montrer que la suite (I_n) est stationnaire.

(⋆) Exercice 30 Résoudre les équations suivantes.

1. $\overline{7x} = \overline{2}$ dans $\mathbb{Z}/37\mathbb{Z}$
2. $\overline{10x} = \overline{6}$ dans $\mathbb{Z}/34\mathbb{Z}$
3. $\overline{10x} = \overline{5}$ dans $\mathbb{Z}/34\mathbb{Z}$

(⋆) Exercice 31 Déterminer les inversibles de $\mathbb{Z}/8\mathbb{Z}$. Le groupe des inversibles $U(\mathbb{Z}/8\mathbb{Z})$ est-il cyclique ?

(⋆) Exercice 32 En observant l'ordre des éléments, montrer que les trois groupes

$$\mathbb{Z}/8\mathbb{Z} \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \qquad (\mathbb{Z}/2\mathbb{Z})^3$$

ne sont pas isomorphes. L'hypothèse d'entiers premiers entre eux deux à deux est donc nécessaire dans le théorème chinois.

(⋆) Exercice 33 Montrer que $X^{3n+2} + X^3 + X$ est divisible par $X^2 + X + 1$.

(⋆) Exercice 34 Pour $n \in \mathbb{N}^*$, on pose $P_n = (X-1)^{n+2} + X^{2n+1}$.
Déterminer les racines de $R = X^2 - X + 1$. En déduire que R divise P.

(⋆) Exercice 35

1. Quelles sont les racines du polynôme $X^2 + X + 1$?
2. Donner une condition nécessaire et suffisante sur l'entier $n \in \mathbb{N}^*$ pour que $X^{2n} + X^n + 1$ soit divisible par $X^2 + X + 1$.

(⋆) Exercice 36 Soit $n \in \mathbb{N}^*$. Montrer que $nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$ est divisible par $(X-1)^3$.

(⋆⋆) Exercice 37 (oral HEC)
Déterminer tous les polynômes P de $\mathbb{R}[X]$ de degré n tels que P est divisible par $X+1$ et les restes de P dans les divisions euclidiennes par $X+2$, $X+3$, ..., $X+n+1$ sont égaux.

(⋆) Exercice 38
$P(X) = X^8 + X^4 + 1$.

1. En observant une progression géométrique, résoudre $P(z) = 0$.
2. Factoriser P dans $\mathbb{C}[X]$.
3. Donner la factorisation de P dans $\mathbb{R}[X]$.

(⋆) Exercice 39 Soit u un endomorphisme d'un espace vectoriel E. On considère l'ensemble, appelé commutant de u :

$$\mathcal{C}_u = \{v \in \mathscr{L}(E) \mid u \circ v = v \circ u\}$$

Montrer que $\mathcal{C}_u$ est une sous-algèbre de l'algèbre $\mathscr{L}(E)$.

(⋆) Exercice 40 Soit $E = \left\{M(a,b) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix},\ (a,b) \in \mathbb{R}^2\right\}$. Montrer que E est une sous-algèbre de $\mathcal{M}_2(\mathbb{R})$ et que E est isomorphe à $\mathbb{C}$.

(⋆⋆) Exercice 41 Soient x et y deux éléments d'un groupe G d'ordres respectifs p et q. On suppose que x et y commutent et que $p \wedge q = 1$. Montrer que l'ordre de xy est pq.

Banque épreuve orale CCINP

Algèbre : 86 et 94.