# Plaquette 5 – L'anneau Z/nZ, théorème chinois et corps finis

## Structures algébriques — Prépa MPSI / MP2I (1re année)

Exercices

### Méthode

$\mathbb{Z}/n\mathbb{Z}$ est l'anneau où l'on calcule « modulo $n$ ». On y **résout** des équations comme dans $\mathbb{R}$, à condition de savoir quels éléments sont **inversibles** ($k \wedge n = 1$) et si l'anneau est un **corps** ($n$ premier). Quand $n = mm'$ avec $m \wedge m' = 1$, le **théorème chinois** découpe le problème en deux problèmes plus petits, modulo $m$ et modulo $m'$. On termine par de vrais usages : clés de contrôle, chiffrement, et construction de corps finis qui ne sont pas des $\mathbb{Z}/p\mathbb{Z}$.

### Exercice 1 – Équations du premier degré modulo n

Résoudre dans l'anneau indiqué, en justifiant l'existence et le nombre de solutions :

a) $\overline{7}x = \overline{3}$ dans $\mathbb{Z}/12\mathbb{Z}$ ;

b) $\overline{4}x = \overline{6}$ dans $\mathbb{Z}/10\mathbb{Z}$ ;

c) $\overline{6}x = \overline{4}$ dans $\mathbb{Z}/9\mathbb{Z}$ ;

d) $\overline{15}x = \overline{9}$ dans $\mathbb{Z}/21\mathbb{Z}$.

### Exercice 2 – Équations du second degré dans Z/pZ

a) Soit $p$ un nombre premier impair et $a \neq \overline{0}$ dans $\mathbb{Z}/p\mathbb{Z}$. Montrer que la mise sous forme canonique reste valable : $ax^2 + bx + c = \overline{0} \Leftrightarrow (2ax + b)^2 = \Delta$ avec $\Delta = b^2 - 4ac$.

b) Résoudre $x^2 + x + \overline{1} = \overline{0}$ dans $\mathbb{Z}/7\mathbb{Z}$, puis dans $\mathbb{Z}/5\mathbb{Z}$.

c) Résoudre $x^2 = \overline{1}$ dans $\mathbb{Z}/8\mathbb{Z}$. Pourquoi ce résultat ne contredit-il pas le cours ?

### Exercice 3 – Le théorème chinois

Soient $m, m' \geq 2$ premiers entre eux, et $\psi : \mathbb{Z}/mm'\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m'\mathbb{Z}$, $k \bmod mm' \mapsto (k \bmod m,\ k \bmod m')$.

a) Montrer que $\psi$ est bien défini et que c'est un morphisme d'anneaux.

b) Montrer que $\psi$ est injectif, puis bijectif.

c) Avec $um + u'm' = 1$, montrer que $k = bum + au'm'$ vérifie $k \equiv a \pmod{m}$ et $k \equiv b \pmod{m'}$.

d) (Problème de Sunzi, IIIe siècle.) Trouver le plus petit entier naturel dont les restes dans la division par 3, 5 et 7 sont 2, 3 et 2.

### Exercice 4 – Indicatrice d'Euler

On note $\varphi(n)$ le nombre d'inversibles de $\mathbb{Z}/n\mathbb{Z}$.

a) Montrer, avec le théorème chinois et l'égalité $(A \times B)^\times = A^\times \times B^\times$, que $\varphi(mm') = \varphi(m)\varphi(m')$ si $m \wedge m' = 1$.

b) Montrer que $\varphi(p^k) = p^k - p^{k-1}$ pour $p$ premier et $k \geq 1$.

c) En déduire $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$, et calculer $\varphi(360)$ et $\varphi(1\,001)$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

d) Montrer que $\varphi(n)$ est pair pour $n \geq 3$ (associer $\overline{k}$ et $-\overline{k}$).

## Exercice 5 – Le théorème de Wilson

Soit $p$ un nombre premier.

a) Montrer que les seuls éléments de $\mathbb{Z}/p\mathbb{Z}$ égaux à leur inverse sont $\overline{1}$ et $-\overline{1}$.

b) En regroupant chaque élément non nul avec son inverse, montrer que $(p-1)! \equiv -1 \pmod{p}$.

c) Vérifier pour $p = 7$ et $p = 11$.

d) Montrer la réciproque : si $n \geq 2$ vérifie $(n-1)! \equiv -1 \pmod{n}$, alors $n$ est premier.

## Exercice 6 – Clé de contrôle de l'ISBN

Un ancien numéro ISBN de livre est une suite de dix chiffres $a_1 a_2 \ldots a_{10}$ (le dernier pouvant valoir 10, noté X) telle que

$$\sum_{i=1}^{10} i\, a_i \equiv 0 \pmod{11}$$

a) Calculer la clé $a_{10}$ du numéro commençant par 2 07 036002.

b) Montrer que l'erreur sur **un seul** chiffre est toujours détectée.

c) Montrer que l'échange de **deux chiffres distincts** $a_i \neq a_j$ est toujours détecté.

d) Pourquoi le module 11 (et non 10) est-il indispensable ?

## Exercice 7 – Le chiffrement RSA en miniature

On choisit $p = 11$, $q = 13$, $n = pq = 143$ et l'exposant public $e = 7$.

a) Calculer $\varphi(n)$ et l'exposant secret $d$, inverse de $e$ modulo $\varphi(n)$.

b) Soit $m \in \mathbb{Z}$. Montrer que $m^{ed} \equiv m \pmod{p}$ (distinguer $p \mid m$ et $p \nmid m$), puis que $m^{ed} \equiv m \pmod{n}$.

c) Chiffrer le message $m = 2$ : $c = m^e \bmod n$.

d) Déchiffrer $c$ en calculant $c^d$ modulo 11 et modulo 13 séparément, puis conclure par le théorème chinois.

## Exercice 8 – Un corps à quatre éléments

On travaille dans $M_2(\mathbb{Z}/2\mathbb{Z})$, avec $A = \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}$, et on pose $\mathrm{F}_4 = \{0, I_2, A, A + I_2\}$.

a) Vérifier que $A^2 = A + I_2$.

b) Dresser les tables d'addition et de multiplication de $\mathrm{F}_4$. En déduire que c'est un sous-anneau commutatif de $M_2(\mathbb{Z}/2\mathbb{Z})$, puis un **corps**.

c) Montrer que $(\mathrm{F}_4, +)$ est le groupe de Klein et que $(\mathrm{F}_4^*, \times)$ est cyclique d'ordre 3.

d) Montrer que $\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps : il y a donc deux anneaux à 4 éléments très différents.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

## Exercice 9 – Un corps à neuf éléments

On note $\mathrm{K} = \{a + b\,\mathrm{i} \,;\, a, b \in \mathbb{Z}/3\mathbb{Z}\}$ l'ensemble des « entiers de Gauss modulo 3 », avec les calculs usuels et $\mathrm{i}^2 = -1$ (on admet que c'est un anneau commutatif à 9 éléments).

a) Montrer que $a^2 + b^2 = \overline{0}$ dans $\mathbb{Z}/3\mathbb{Z}$ impose $a = b = \overline{0}$.

b) En déduire que K est un corps, en donnant l'inverse de $a + b\,\mathrm{i} \neq 0$. Calculer l'inverse de $\overline{1} + \mathrm{i}$.

c) Montrer que $\overline{1} + \mathrm{i}$ engendre le groupe multiplicatif $\mathrm{K}^*$ (calculer ses puissances successives).

d) Montrer que la même construction modulo 5 ne donne pas un corps (considérer $\overline{2} + \mathrm{i}$).

## Exercice 10 – Sous-corps de C

Un **sous-corps** de $\mathbb{C}$ est un sous-anneau $K$ de $\mathbb{C}$ tel que $x^{-1} \in K$ pour tout $x \in K \setminus \{0\}$.

a) Montrer que tout sous-corps de $\mathbb{C}$ contient $\mathbb{Q}$.

b) Montrer qu'une intersection de sous-corps de $\mathbb{C}$ est un sous-corps.

c) Montrer que $\mathbb{Q}(\mathrm{i}) = \{a + \mathrm{i}b,\, a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$, et que c'est le plus petit contenant i.

d) $\mathbb{Z}[\mathrm{i}]$ est-il un sous-corps de $\mathbb{C}$ ?

## Exercice 11 – Générateurs de (Z/11Z)* et échange de clés

a) Montrer que $\overline{2}$ est d'ordre 10 dans $G = \left((\mathbb{Z}/11\mathbb{Z})^*, \times\right)$ : $G$ est cyclique.

b) Déterminer tous les générateurs de $G$.

c) Résoudre $2^k \equiv 5 \pmod{11}$ d'inconnue $k \in \{0, \ldots, 9\}$ (**logarithme discret**).

d) (Échange de Diffie-Hellman.) Alice et Bob conviennent publiquement de $p = 11$ et $g = 2$. Alice choisit en secret $a = 3$ et publie $A = g^a \bmod p$ ; Bob choisit $b = 4$ et publie $B = g^b \bmod p$. Calculer $A$, $B$, puis la clé commune $B^a \bmod p$, et vérifier qu'elle est égale à $A^b \bmod p$.

## Exercice 12 – Le chiffrement affine

On code les lettres A, B, …, Z par $0, 1, \ldots, 25$, vus dans $\mathbb{Z}/26\mathbb{Z}$, et on chiffre chaque lettre par $f_{a,b}(x) = ax + b$.

a) Montrer que $f_{a,b}$ est une bijection de $\mathbb{Z}/26\mathbb{Z}$ si et seulement si $a$ est inversible. Combien y a-t-il de clés $(a, b)$ valables ?

b) Montrer que les $f_{a,b}$ valables forment un groupe pour la composition.

c) Avec $a = 5$ et $b = 8$, chiffrer le mot MATH.

d) Déterminer la fonction de déchiffrement, et déchiffrer le mot obtenu.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

## Exercice 13 – Calculs de restes

a) Déterminer le dernier chiffre de $7^{2026}$.

b) Déterminer les deux derniers chiffres de $3^{100}$ (on pourra calculer $3^{10}$ modulo 100).

c) Montrer que 7 divise $3^{2n+1} + 2^{n+2}$ pour tout $n \in \mathbb{N}$.

d) Déterminer le reste de $2^{2^{10}}$ dans la division par 13.

## Exercice 14 – Morphismes d'anneaux entre les Z/nZ

a) Montrer que le seul sous-anneau de $\mathbb{Z}/n\mathbb{Z}$ est $\mathbb{Z}/n\mathbb{Z}$ lui-même.

b) Montrer qu'il existe un morphisme d'anneaux $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ si et seulement si $m \mid n$, et qu'il est alors unique.

c) Existe-t-il un morphisme d'anneaux de $\mathbb{Z}/12\mathbb{Z}$ dans $\mathbb{Z}/4\mathbb{Z}$ ? de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$ ?

d) Montrer qu'il n'existe aucun morphisme d'anneaux de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathbb{Q}$, ni de $\mathbb{Q}$ dans $\mathbb{Z}/p\mathbb{Z}$.

## Exercice 15 – Synthèse : racines carrées de 1 modulo n

On étudie l'équation $x^2 = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$.

a) Pour $p$ premier impair, montrer qu'elle a exactement deux solutions dans $\mathbb{Z}/p\mathbb{Z}$.

b) Pour $n = 15$, utiliser le théorème chinois pour montrer qu'elle a quatre solutions, et les déterminer.

c) Combien de solutions a-t-elle pour $n = 105 = 3 \times 5 \times 7$ ? Pour $n = pq$, produit de deux premiers impairs distincts ?

d) Soit $n$ impair et $x$ une solution avec $x \neq \pm\overline{1}$. Montrer que $d = (x - 1) \wedge n$ est un diviseur **strict** de $n$ (différent de 1 et de $n$). Vérifier sur $n = 15$ avec $x = \overline{4}$ et $x = \overline{11}$.

e) Interpréter : pourquoi savoir trouver une racine carrée non triviale de $\overline{1}$ modulo $n$ permet de factoriser $n$ ?

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).