

Anneaux, idéaux et $\mathbb{Z}/n\mathbb{Z}$

Exercice 1 : Inversibles de $\mathbb{Z}/n\mathbb{Z}$ et calcul d'inverses

La figure ci-dessous donne la table de multiplication de $\mathbb{Z}/10\mathbb{Z}$. Les cases qui contiennent $\bar{1}$ sont mises en évidence.

$\times$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

1. À l'aide de la table, donnez les inversibles de $\mathbb{Z}/10\mathbb{Z}$ et leurs inverses. Retrouvez ce résultat par le cours.
2. Donnez la liste des inversibles de $\mathbb{Z}/20\mathbb{Z}$, puis l'inverse de $\bar{7}$ dans $\mathbb{Z}/20\mathbb{Z}$.
3. Par l'algorithme d'Euclide étendu, déterminez l'inverse de $\bar{17}$ dans $\mathbb{Z}/60\mathbb{Z}$.
4. Montrez que $\bar{6}$ est un diviseur de zéro dans $\mathbb{Z}/20\mathbb{Z}$.

Exercice 2 : Calculs de l'indicatrice d'Euler

1. Calculez $\varphi(360)$, $\varphi(1001)$, $\varphi(2^{10})$ et $\varphi(343)$.
2. Sachant que 1013 est premier, calculez $\varphi(2026)$.
3. Montrez que $\varphi(n)$ est pair pour tout entier $n \geq 3$.

Exercice 3 : Puissances modulo n par le théorème d'Euler

1. Déterminez le reste de la division euclidienne de 3^{1000} par 7.
2. Déterminez le reste de 2^{100} modulo 13.
3. Calculez 7^4 modulo 100, puis déterminez les deux derniers chiffres de 7^{2026} .
4. Déterminez le chiffre des unités de 13^{2026} .

Exercice 4 : Un système de trois congruences

On cherche les entiers x tels que $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$ et $x \equiv 2 \pmod{7}$.

1. Justifiez que les solutions forment une classe modulo 105.
2. Résolvez le système formé des deux premières congruences.
3. Résolvez le système complet.
4. Quel est le plus petit entier supérieur ou égal à 1000 solution du système ?

Exercice 5 : Idéaux de $\mathbb{Z}$ et PGCD

1. Déterminez les idéaux $12\mathbb{Z} + 18\mathbb{Z}$ et $12\mathbb{Z} \cap 18\mathbb{Z}$.
2. Déterminez l'idéal $84\mathbb{Z} + 60\mathbb{Z} + 105\mathbb{Z}$. Trouvez des entiers u, v tels que $84u + 60v = 12$.
3. Montrez que, pour $a, b \in \mathbb{N}$, on a $a\mathbb{Z} \subset b\mathbb{Z}$ si et seulement si b divise a .
4. Déterminez tous les idéaux de $\mathbb{Z}$ qui contiennent $18\mathbb{Z}$.

Exercice 6 : Parties qui sont ou non des idéaux

Pour chacune des parties suivantes, dites si c'est un idéal de l'anneau indiqué. Lorsque c'est le cas, donnez un générateur.

1. $I_1 = \{P \in \mathbb{R}[X], P(1) = P'(1) = 0\}$ dans $\mathbb{R}[X]$.
2. $I_2 = \left\{ \begin{array}{l} P \\ \mathbb{R}[X], \\ P(0) = 1 \end{array} \right\}$ dans $\mathbb{R}[X]$.
3. $I_3 = \left\{ \begin{array}{l} P \in \mathbb{R}[X], \\ \deg P \leq 2 \end{array} \right\}$ dans $\mathbb{R}[X]$.
4. $I_4 = \left\{ \begin{array}{l} P \\ \mathbb{R}[X], \\ P(i) = 0 \end{array} \right\}$ dans $\mathbb{R}[X]$.
5. $I_5 = 2\mathbb{Z} \cup 3\mathbb{Z}$ dans $\mathbb{Z}$.

Exercice 7 : Équations linéaires modulo n

Soit $n \geq 2$, $a, b \in \mathbb{Z}$ et $d = a \wedge n$.

1. Montrez que l'équation $ax \equiv b \pmod{n}$ a une solution si et seulement si d divise b .
Montrez qu'elle a alors exactement d solutions modulo n .
2. Résolvez $6x \equiv 4 \pmod{10}$.
3. Résolvez $6x \equiv 5 \pmod{9}$.
4. Résolvez $91x \equiv 35 \pmod{133}$.

Exercice 8 : Congruences à modules non premiers entre eux

1. Soit $m, n \geq 1$, $d = m \wedge n$ et $a, b \in \mathbb{Z}$. Montrez que le système $x \equiv a \pmod{m}$,
 $x \equiv b \pmod{n}$ a une solution si et seulement si $a \equiv b \pmod{d}$. Montrez qu'alors les
solutions forment une classe modulo $m \vee n$.
2. Résolvez $x \equiv 3 \pmod{4}$ et $x \equiv 5 \pmod{6}$.
3. Le système $x \equiv 1 \pmod{4}$, $x \equiv 2 \pmod{6}$ a-t-il des solutions ?
4. Une troupe compte moins de 400 soldats. Rangés par 2, 3, 4, 5 ou 6, il en reste toujours un. Rangés
par 7, il n'en reste aucun. Combien sont-ils ?

Exercice 9 : Produit d'anneaux et idempotents

1. Montrez que $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ sont isomorphes. Donnez l'image de chaque classe.
2. Montrez que les anneaux $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes.
3. Déterminez les inversibles de l'anneau $\mathbb{Z} \times \mathbb{Z}$.
4. Soit A et B deux anneaux intègres. Déterminez les idempotents de $A \times B$, c'est-à-dire les
éléments e tels que $e^2 = e$.

5. Soit A et B deux anneaux commutatifs. Montrez que les idéaux de $A \times B$ sont exactement les $I \times J$, où I est un idéal de A et J un idéal de B .

Exercice 10 : Éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$

Un élément x d'un anneau est nilpotent s'il existe $m \geq 1$ tel que $x^m = 0$.

1. Soit A un anneau commutatif. Montrez que l'ensemble N des nilpotents de A est un idéal de A .
2. On écrit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et on pose $r_n = p_1 \cdots p_r$. Montrez que $\bar{k}$ est nilpotent dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si r_n divise k .
3. Déterminez les nilpotents de $\mathbb{Z}/72\mathbb{Z}$ et leur nombre.
4. Pour quels entiers $n \geq 2$ l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'a-t-il aucun nilpotent non nul ?

Exercice 11 : Divisibilité dans l'anneau des entiers de Gauss

On note $\mathbb{Z}[i] = \left\{ \begin{matrix} a + ib, \\ a, b \in \mathbb{Z} \end{matrix} \right\}$ et, pour $z \in \mathbb{Z}[i]$, $N(z) = |z|^2$.

1. Montrez que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$, puis qu'il est intègre. Vérifiez que $N(z) \in \mathbb{N}$ et $N(zw) = N(z)N(w)$.
2. Montrez que z est inversible dans $\mathbb{Z}[i]$ si et seulement si $N(z) = 1$. Déterminez $\mathbb{Z}[i]^\times$.
3. Vérifiez que $2 = -i(1+i)^2$. Montrez que $1+i$ et $1-i$ sont associés.
4. Le nombre $3+i$ divise-t-il $5+5i$? Le nombre $1+2i$ divise-t-il 3 ?
5. Montrez que $(1+i)\mathbb{Z}[i] = \left\{ \begin{matrix} a + ib, \\ a + b \text{ pair} \end{matrix} \right\}$.

Exercice 12 : Noyaux de morphismes d'anneaux

1. Soit $\theta : \mathbb{R}[X] \rightarrow \mathbb{C}, P \mapsto P(i)$. Montrez que θ est un morphisme d'anneaux surjectif et que $\ker \theta = (X^2 + 1)\mathbb{R}[X]$.
2. Soit $f : \mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, k \mapsto (k \bmod 4, k \bmod 6)$. Déterminez $\ker f$. L'application f est-elle surjective ?
3. Montrez qu'il n'existe aucun morphisme d'anneaux de $\mathbb{Z}/6\mathbb{Z}$ dans $\mathbb{Z}$.
4. Soit $m, n \geq 1$. Montrez qu'il existe un morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ si et seulement si m divise n .

Exercice 13 : Théorème de Wilson dans le corps $\mathbb{F}_p$

Soit p un nombre premier.

1. Résolvez l'équation $x^2 = -1$ dans $\mathbb{F}_p$.
2. En regroupant chaque élément de $\mathbb{F}_p^\times$ avec son inverse, montrez que $(p-1)! \equiv -1 \pmod{p}$.
3. Réciproquement, montrez que si $n \geq 2$ n'est pas premier, alors $(n-1)! \not\equiv -1 \pmod{n}$.
4. Vérifiez que $10! \equiv -1 \pmod{11}$, puis calculez $15!$ modulo 17.

Exercice 14 : PGCD de $X^a - 1$ et $X^b - 1$

1. Calculez $(X^6 - 1) \wedge (X^4 - 1)$ par l'algorithme d'Euclide et donnez une relation de Bézout.

- Décomposez $X^6 - 1$ en produit d'irréductibles dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$.
- Soit $a, b \geq 1$ et $a = bq + r$ la division euclidienne de a par b . Montrez que $(X^a - 1) \wedge (X^b - 1) = (X^b - 1) \wedge (X^r - 1)$, avec la convention $X^0 - 1 = 0$.
- En déduire que $(X^a - 1)\mathbb{K}[X] + (X^b - 1)\mathbb{K}[X] = (X^{a \wedge b} - 1)\mathbb{K}[X]$.

Exercice 15 : Sous-algèbres de matrices

Soit $n \geq 2$ et $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

- Montrez que l'ensemble $\mathcal{T}_n$ des matrices triangulaires supérieures est une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$.
- Soit $A \in \mathcal{M}_n(\mathbb{K})$. Montrez que le commutant $\mathcal{C}(A) = \left\{ M \in \mathcal{M}_n(\mathbb{K}) \mid AM = MA \right\}$ est une sous-algèbre.
- Pour $n = 2$ et $A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, déterminez $\mathcal{C}(A)$ et sa dimension.
- L'ensemble des matrices de trace nulle est-il une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$?

Exercice 16 : Polynômes annulateurs et puissances d'une matrice

On pose $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $I = \left\{ \begin{matrix} P \\ \mathbb{R}[X] \\ P(M) = 0 \end{matrix} \right\}$.

- Montrez que I est un idéal de $\mathbb{R}[X]$.
- Montrez que $I = (X - 1)^2 \mathbb{R}[X]$.
- Pour $n \in \mathbb{N}$, déterminez le reste de la division euclidienne de X^n par $(X - 1)^2$. En déduire

$$M^n.$$

4. Montrez que $\mathbb{R}[M] = \left\{ \begin{pmatrix} P(M) \\ P \end{pmatrix}, P \in \mathbb{R}[X] \right\}$ est une sous-algèbre de dimension 2 de $\mathcal{M}_2(\mathbb{R})$.

Exercice 17 : Petit théorème de Fermat et nombre pseudo-premier

- Décomposez 341 en facteurs premiers.
- Montrez que $2^{10} \equiv 1 \pmod{11}$ et que $2^5 \equiv 1 \pmod{31}$.
- En déduire que $2^{340} \equiv 1 \pmod{341}$. Que penser du test « si $2^{n-1} \equiv 1 \pmod{n}$, alors n est premier » ?
- Calculez 3^{10} modulo 31, puis 3^{340} modulo 31. Conclure sur 3^{340} modulo 341.

Exercice 18 : Racines carrées de 1 modulo n

- Soit p un nombre premier impair. Montrez que $x^2 \equiv 1 \pmod{p}$ si et seulement si $x \equiv \pm 1 \pmod{p}$.
- Résolvez $x^2 \equiv 1 \pmod{8}$. Le résultat de la question 1 reste-t-il vrai modulo 8 ?
- À l'aide du théorème chinois, résolvez $x^2 \equiv 1 \pmod{15}$.
- Combien l'équation $x^2 \equiv 1 \pmod{105}$ a-t-elle de solutions modulo 105 ? Déterminez-les toutes.
- Soit $n = p_1 \cdots p_r$ un produit de r nombres premiers impairs distincts. Montrez que l'équation $x^2 \equiv 1 \pmod{n}$ a exactement 2^r solutions modulo n .

Exercice 19 : L'équation $\varphi(n) = 4$

1. Soit $n \geq 2$ et p un nombre premier qui divise n . Montrez que $p - 1$ divise $\varphi(n)$.
2. Montrez que, pour $n \geq 2$, $\varphi(n) = n - 1$ si et seulement si n est premier.
3. Déterminez tous les entiers $n \geq 1$ tels que $\varphi(n) = 4$.
4. Montrez que l'équation $\varphi(n) = 14$ n'a aucune solution.

Exercice 20 : Formule de Gauss pour l'indicatrice d'Euler

La figure ci-dessous place les douze fractions $k/12$, pour $1 \leq k \leq 12$, écrites sous forme irréductible et rangées selon leur dénominateur.

$d = 1$	$d = 2$	$d = 3$	$d = 4$	$d = 6$	$d = 12$
$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{1}{12}$
		$\frac{2}{3}$	$\frac{3}{4}$	$\frac{5}{6}$	$\frac{5}{12}$
					$\frac{7}{12}$
					$\frac{11}{12}$
1	1	2	2	2	4

1. Vérifiez sur la figure que le nombre de fractions de dénominateur d vaut $\varphi(d)$, pour chaque

diviseur d de 12.

2. Soit $n \geq 1$ et d un diviseur de n . Montrez que le nombre d'entiers $k \in \llbracket 1, n \rrbracket$ tels que k/n ait pour dénominateur réduit d est égal à $\varphi(d)$.

3. En déduire la formule de Gauss : $\sum_{d|n} \varphi(d) = n$.

4. Retrouvez la valeur de $\varphi(p^k)$ à partir de cette formule, pour p premier.

Exercice 21 : Un idéal non principal de $\mathbb{Z}[X]$

On note I l'ensemble des polynômes $P \in \mathbb{Z}[X]$ dont le coefficient constant $P(0)$ est pair.

1. Montrez que I est le noyau d'un morphisme d'anneaux de $\mathbb{Z}[X]$ dans $\mathbb{Z}/2\mathbb{Z}$. En déduire que I est un idéal.

2. Montrez que $I = 2\mathbb{Z}[X] + X\mathbb{Z}[X]$.

3. Montrez qu'il n'existe aucun $D \in \mathbb{Z}[X]$ tel que $I = D\mathbb{Z}[X]$.

4. Expliquez pourquoi la démonstration faite dans le cours pour $\mathbb{K}[X]$ ne s'applique pas à $\mathbb{Z}[X]$.

Exercice 22 : Problème, le chiffrement RSA

On choisit deux nombres premiers distincts p et q , on pose $n = pq$, et on choisit un entier e premier avec $\varphi(n)$. Le message $m \in \llbracket 0, n-1 \rrbracket$ est chiffré en $c = m^e \bmod n$.

1. Exprimez $\varphi(n)$ en fonction de p et q . Justifiez l'existence d'un entier $d \geq 1$ tel que $ed \equiv 1 \pmod{\varphi(n)}$.

2. On prend $p = 11$, $q = 13$ et $e = 7$. Calculez n , $\varphi(n)$ et le plus petit $d \geq 1$ convenable.

3. Chiffrez le message $m = 2$.
4. Revenons au cas général. Montrez que $m^{ed} \equiv m \pmod{n}$ lorsque $m \wedge n = 1$.
5. Montrez que $m^{ed} \equiv m \pmod{p}$ pour tout entier m , y compris lorsque p divise m . En déduire que $m^{ed} \equiv m \pmod{n}$ pour tout $m \in \mathbb{Z}$.
6. En déduire que $x \rightarrow x^e$ est une bijection de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même, et donnez sa réciproque.
7. Dans l'exemple numérique, vérifiez le déchiffrement de $c = 128$ en calculant 128^{103} modulo 11 et modulo 13.

Le corrigé des exercices

Chaque exercice est corrigé en détail, question par question, sur la page suivante.



Pour aller plus loin en maths spé

- Le cours : [anneaux, idéaux et \$\mathbb{Z}/n\mathbb{Z}\$, cours de maths spé](#)
- À maîtriser avant : [Compléments sur les groupes : groupes monogènes et ordre](#)
- Chapitre précédent : [Compléments sur les groupes : groupes monogènes et ordre](#)
- Chapitre suivant : [Éléments propres et polynôme caractéristique](#)
- Tester vos connaissances : [QCM de maths spé par chapitre](#)
- Le sommaire : [tous les chapitres de maths spé](#) et les [chapitres de maths sup](#)

