

Contrôle de maths spé : idéaux, congruences et indicatrice d'Euler

Fiche du contrôle

- **Niveau** : maths spé (MP)
- **Chapitre** : Anneaux, idéaux, $\mathbb{Z}/n\mathbb{Z}$ et algèbres
- **Durée conseillée** : 2 heures
- **Barème** : sur 20 points (exercice 1 : 4 points ; exercice 2 : 4 points ; exercice 3 : 4 points ; exercice 4 : 3 points ; exercice 5 : 5 points)
- **Compétences évaluées** :
 - Raisonner : décrire les idéaux de $\mathbb{Z}$ et de $\mathbb{K}[X]$ et relier le PGCD à un idéal
 - Calculer : obtenir un inverse modulaire par l'algorithme d'Euclide étendu
 - Chercher : résoudre un système de congruences par le théorème chinois
 - Calculer : utiliser l'indicatrice d'Euler pour réduire une puissance modulo n
 - Modéliser : reconnaître une sous-algèbre et le noyau d'un morphisme d'algèbres

Exercice 1 : Question de cours (4 points)

Calculatrice interdite.

Dans cet exercice, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

- a. Démontrez que tout idéal I de $\mathbb{K}[X]$ non réduit à $\{0\}$ s'écrit $I = P\mathbb{K}[X]$ pour un unique polynôme unitaire P . (2 points)
- b. Soit a et b deux entiers non tous deux nuls. Montrez que $a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$, puis que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ où $d = a \wedge b$. Déduisez-en la relation de Bézout. On admet que les

idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$. (2 points)

Exercice 2 : Inversibles de $\mathbb{Z}/60\mathbb{Z}$ (4 points)

On note $\overline{k}$ la classe de l'entier k dans $\mathbb{Z}/n\mathbb{Z}$.

- Démontrez que $\overline{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$. (1 point)
- Justifiez que $\overline{17}$ est inversible dans $\mathbb{Z}/60\mathbb{Z}$, puis déterminez son inverse à l'aide de l'algorithme d'Euclide. (1,5 point)
- Résolvez dans $\mathbb{Z}$ la congruence $17x \equiv 5 \pmod{60}$. (0,5 point)
- Combien l'anneau $\mathbb{Z}/60\mathbb{Z}$ possède-t-il d'éléments inversibles ? Est-ce un corps ? (1 point)

Exercice 3 : Théorème chinois (4 points)

- Soit m et n deux entiers supérieurs ou égaux à 2 et premiers entre eux. Énoncez le théorème chinois sous la forme d'un isomorphisme d'anneaux, puis démontrez que l'application proposée est injective. (1 point)
- Déterminez tous les entiers x tels que $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$ et $x \equiv 1 \pmod{9}$. (2 points)
- Déduisez du théorème chinois que $\varphi(mn) = \varphi(m)\varphi(n)$ lorsque $m \wedge n = 1$, où φ désigne l'indicatrice d'Euler. (1 point)

Exercice 4 : Théorème d'Euler (3 points)

- a. Calculez $\varphi(100)$. (0,5 point)
- b. Énoncez le théorème d'Euler, puis déterminez les deux derniers chiffres de l'écriture décimale de 7^{2026} . (1,5 point)
- c. Déterminez l'ordre de $\bar{7}$ dans le groupe $((\mathbb{Z}/100\mathbb{Z})^\times, \times)$. Retrouvez ainsi rapidement le résultat de b). (1 point)

Exercice 5 : Le corps $\mathbb{Z}/p\mathbb{Z}$ et une algèbre de matrices (5 points)

Partie A. Soit $n \geq 2$ et p un nombre premier.

- a. Démontrez que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier. (1 point)
- b. Démontrez le petit théorème de Fermat : pour tout entier a non divisible par p ,
 $a^{p-1} \equiv 1 \pmod{p}$. (0,5 point)
- c. Montrez que, dans $\mathbb{F}_p$, l'équation $x^2 = \bar{1}$ a pour seules solutions $\bar{1}$ et $-\bar{1}$. (0,5 point)
- d. On suppose $p \geq 3$. En regroupant chaque élément de $\mathbb{F}_p^*$ avec son inverse, démontrez le théorème de Wilson : $(p-1)! \equiv -1 \pmod{p}$. (1,5 point)

Partie B. On pose $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $\mathcal{A} = \{aI_2 + bN : (a, b) \in {}_\mu\mathbb{K}^2\}$.

- e. Montrez que $\mathcal{A}$ est une sous-algèbre commutative de $\mathcal{M}_2(\mathbb{K})$, de dimension 2. (1 point)
- f. On considère le morphisme d'algèbres $\Phi : \mathbb{K}[X] \rightarrow \mathcal{M}_2(\mathbb{K})$, $P \mapsto P(N)$. Déterminez son image et montrez que son noyau est l'idéal $X^2 \mathbb{K}[X]$. (0,5 point)



Réviser avant le contrôle : idéaux, congruences et indicatrice d'Euler

Avant de faire ce contrôle, relisez le cours [« Anneaux, idéaux et \$\mathbb{Z}/n\mathbb{Z}\$ » en maths spé](#) puis entraînez-vous avec les **exercices corrigés** [anneaux, idéaux et \$\mathbb{Z}/n\mathbb{Z}\$](#) .

Retrouvez tous les [contrôles de maths spé classés par chapitre](#), ou choisissez un autre niveau sur la page [contrôles de maths du CP au post-bac](#).