

Contrôle de maths sup : arithmétique dans $\mathbb{Z}$, groupes et anneaux

Fiche du contrôle

- **Niveau** : maths sup (MPSI)
- **Chapitres** : Arithmétique dans l'ensemble des entiers relatifs + Structures algébriques usuelles : groupes, anneaux, corps
- **Durée conseillée** : 3 heures
- **Barème** : sur 20 points (exercice 1 : 3 points ; exercice 2 : 4 points ; exercice 3 : 5 points ; exercice 4 : 3 points ; exercice 5 : 5 points)
- **Compétences évaluées** :
 - Calculer : PGCD et couple de Bézout par l'algorithme d'Euclide étendu
 - Raisonner : utiliser le lemme de Gauss et les valuations p-adiques
 - Démontrer : reconnaître un sous-groupe, un morphisme, un inversible
 - Modéliser : relier sous-groupes de $\mathbb{Z}$, PGCD et PPCM

Exercice 1 : Nombres premiers et lemme de Gauss (3 points)

Calculatrice interdite. Durée conseillée : 3 heures. Les groupes quotients ne sont pas utilisés dans ce devoir.

- Montrez que tout entier $n \geq 2$ admet un diviseur premier, puis démontrez que l'ensemble des nombres premiers est infini. (1,5 point)
- Énoncez et démontrez le lemme de Gauss, en utilisant le théorème de Bézout. (1,5 point)

Exercice 2 : Algorithme d'Euclide étendu et équation diophantienne (4 points)

- a. À l'aide de l'algorithme d'Euclide, calculez $d = 252 \wedge 198$, puis déterminez un couple d'entiers (u, v) tel que $252u + 198v = d$. (1,5 point)
- b. Résolvez dans $\mathbb{Z}^2$ l'équation $252x + 198y = 36$. (1,5 point)
- c. L'équation $252x + 198y = 30$ admet-elle des solutions entières ? Justifiez. (0,5 point)
- d. Déduisez de a) le PPCM de 252 et 198. (0,5 point)

Exercice 3 : Valuations p-adiques et congruences (5 points)

- a. Décomposez 252 et 198 en produit de facteurs premiers. Retrouvez leur PGCD et leur PPCM à l'aide des valuations p -adiques. (1 point)
- b. Soit p un nombre premier et $n \geq 1$. Justifiez que $v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$. Déduisez-en le nombre de zéros qui terminent l'écriture décimale de $100!$. (1,5 point)
- c. Déterminez l'inverse de 7 modulo 30, puis résolvez la congruence $7x \equiv 3 \pmod{30}$. (1 point)
- d. À l'aide du petit théorème de Fermat, déterminez le reste de la division euclidienne de 3^{2026} par 11. (1 point)
- e. Montrez que, pour tout entier n , $n^7 - n$ est divisible par 42. (0,5 point)

Exercice 4 : Morphismes et groupe des inversibles (3 points)

- a. Soit $n \geq 2$. Montrez que $\varphi : k \rightarrow e^{2ik\pi/n}$ est un morphisme du groupe $(\mathbb{Z}, +)$ dans $(\mathbb{C}^*, \times)$. Déterminez son noyau et son image. Est-il injectif ? (1 point)

- b. On admet que $\mathbb{Z}[i] = \{a + ib ; (a, b) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$. En utilisant $N(z) = |z|^2$, déterminez le groupe des inversibles de $\mathbb{Z}[i]$. (1,5 point)
- c. Soit A un anneau et $a \in A$ nilpotent, c'est-à-dire tel que $a^m = 0$ pour un entier $m \geq 1$. Montrez que $1 - a$ est inversible et donnez son inverse. (0,5 point)

Exercice 5 : Problème - sous-groupes de $\mathbb{Z}$ et arithmétique (5 points)

Dans ce problème, on relie la structure de groupe de $(\mathbb{Z}, +)$ aux notions de PGCD et de PPCM. Pour $n \in \mathbb{Z}$, on note $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.

- Montrez que $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. (0,5 point)
- Soit H un sous-groupe de $(\mathbb{Z}, +)$. Montrez qu'il existe un unique entier $n \geq 0$ tel que $H = n\mathbb{Z}$. On pourra considérer le plus petit élément de $H \cap \mathbb{N}^*$ et une division euclidienne. (1,5 point)
- Soient a, b deux entiers non tous deux nuls. Montrez que $a\mathbb{Z} + b\mathbb{Z} = \{au + bv ; (u, v) \in \mathbb{Z}^2\}$ est un sous-groupe de $\mathbb{Z}$, égal à $d\mathbb{Z}$ avec $d = a \wedge b$. Quel théorème du cours retrouve-t-on ? (1 point)
- Soient a, b deux entiers non nuls. Montrez que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, où m est le PPCM de a et b . (0,5 point)
- Déterminez tous les morphismes de groupes de $(\mathbb{Z}, +)$ dans lui-même. Lesquels sont injectifs ? surjectifs ? Déduisez-en le groupe des automorphismes de $(\mathbb{Z}, +)$. (1 point)
- Soit $n \geq 2$ et $k \in \mathbb{Z}$. Montrez que k est inversible modulo n si et seulement si $k \wedge n = 1$. Donnez la liste des entiers de $\{0, 1, \dots, 11\}$ inversibles modulo 12. (0,5 point)



Réviser avant le contrôle : arithmétique dans $\mathbb{Z}$, groupes et anneaux

Avant de faire ce contrôle, relisez le cours « [Arithmétique dans \$\mathbb{Z}\$](#) » en maths sup et « [Groupes, anneaux et corps](#) » en maths sup puis entraînez-vous avec les **exercices corrigés** [arithmétique dans \$\mathbb{Z}\$](#) , [groupes](#), [anneaux et corps](#).

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