



# Révisions d'arithmétique sur $\mathbb{Z}$ (MP2I)

Voir programme page suivante.

## Groupes monogènes, $\mathbb{Z}/n\mathbb{Z}$

Extrait du programme officiel :

Contenus	Capacités & commentaires
<b>Compléments sur les groupes</b>	
Sous-groupe engendré par une partie. Partie génératrice d'un groupe. Sous-groupes du groupe $(\mathbb{Z}, +)$ . Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ . Générateurs de $\mathbb{Z}/n\mathbb{Z}$ . Groupe monogène, groupe cyclique. Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$ . Tout groupe monogène fini de cardinal $n$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ . Ordre d'un élément d'un groupe. Si $x$ est d'ordre fini $d$ et si $e$ désigne le neutre de $G$ , alors, pour tout $n \in \mathbb{Z}$ , $x^n = e \iff d n$ . L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.	Groupe des racines $n$ -ièmes de l'unité.  L'ordre de $x$ est le cardinal du sous-groupe de $G$ engendré par $x$ .  La démonstration n'est exigible que pour $G$ commutatif.
<b>Anneaux <math>\mathbb{Z}/n\mathbb{Z}</math></b>	
Anneau $\mathbb{Z}/n\mathbb{Z}$ . Inversibles de $\mathbb{Z}/n\mathbb{Z}$ . Condition nécessaire et suffisante pour que $\mathbb{Z}/n\mathbb{Z}$ soit un corps. Théorème chinois : isomorphisme naturel de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si $m \wedge n = 1$ ; extension à plus de deux facteurs. Indicatrice d'Euler $\varphi$ . Calcul à l'aide de la décomposition en produits de facteurs premiers.  Théorème d'Euler.	Notation $\mathbb{F}_p$ lorsque $p$ est premier.  Application aux systèmes de congruences et à la résolution de systèmes d'équations dans $\mathbb{Z}/n\mathbb{Z}$ . Relation $\varphi(mn) = \varphi(m)\varphi(n)$ si $m$ et $n$ sont premiers entre eux ; expression de $\varphi(p^k)$ pour $p$ premier.  Lien avec le petit théorème de Fermat.

## Questions de cours

- Générateurs du groupe  $(\mathbb{Z}/n\mathbb{Z}, +)$ , inversibles de l'anneau  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ .
- Si  $(G, *)$  est un groupe fini de neutre  $e$ , tous ses éléments sont d'ordre fini, leur ordre divise  $|G|$  (cas commutatif) et pour tout  $a \in G$ ,  $a^{|G|} = e$ .
- Si  $p$  est premier et  $k \in \mathbb{N}^*$ , calcul de  $\varphi(p^k)$ , d'où une expression de  $\varphi(n)$  à l'aide de ses diviseurs premiers. Théorème d'Euler, d'où le petit théorème de Fermat.
- Théorème de Lagrange**  
Soit  $(G, *)$  un groupe fini,  $H$  un sous-groupe de  $G$ .
  - Montrer que la relation définie par  $x \mathcal{R} y \iff x^{-1} * y \in H$  est une relation d'équivalence sur  $G$ .
  - Vérifier que les classes d'équivalence ont toutes le même cardinal.
  - Démontrer le théorème de Lagrange :  $|H|$  divise  $|G|$ .
  - En déduire que l'ordre de tout élément de  $G$  divise l'ordre de  $G$ .
- Exercices CCINP : 31, 32, 42, 66, 74, 75, 86, 94.**

## Exercices CCINP

### ■ CCINP 31 :

- Déterminer une primitive de  $x \mapsto \cos^4 x$ .
- Résoudre sur  $\mathbb{R}$  l'équation différentielle :  $y'' + y = \cos^3 x$  en utilisant la méthode de variation des constantes.

- **CCINP 32** : Soit l'équation différentielle :  $x(x-1)y'' + 3xy' + y = 0$ .
  1. Trouver les solutions de cette équation différentielle développables en série entière sur un intervalle  $]-r, r[$  de  $\mathbb{R}$ , avec  $r > 0$ .  
Déterminer la somme des séries entières obtenues.
  2. Est-ce que toutes les solutions de  $x(x-1)y'' + 3xy' + y = 0$  sur  $]0, 1[$  sont les restrictions d'une fonction développable en série entière sur  $]-1, 1[$  ?

- **CCINP 42** : On considère les deux équations différentielles suivantes :

$$2xy' - 3y = 0 \quad (H)$$

$$2xy' - 3y = \sqrt{x} \quad (E)$$

1. Résoudre l'équation (H) sur l'intervalle  $]0, +\infty[$ .
2. Résoudre l'équation (E) sur l'intervalle  $]0, +\infty[$ .
3. L'équation (E) admet-elle des solutions sur l'intervalle  $[0, +\infty[$  ?

- **CCINP 74** :

1. On considère la matrice  $A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}$ .

- (a) Justifier sans calcul que  $A$  est diagonalisable.
- (b) Déterminer les valeurs propres de  $A$  puis une base de vecteurs propres associés.

2. On considère le système différentiel  $\begin{cases} x' = x + 2z \\ y' = y \\ z' = 2x + z \end{cases}$ ,  $x, y, z$  désignant trois fonctions de la variable

$t$ , dérivables sur  $\mathbb{R}$ .

En utilisant la question 1. et en le justifiant, résoudre ce système.

- **CCINP 75** : On considère la matrice  $A = \begin{pmatrix} -1 & -4 \\ 1 & 3 \end{pmatrix}$ .

1. Démontrer que  $A$  n'est pas diagonalisable.
2. On note  $f$  l'endomorphisme de  $\mathbb{R}^2$  canoniquement associé à  $A$ .

Trouver une base  $(v_1, v_2)$  de  $\mathbb{R}^2$  dans laquelle la matrice de  $f$  est de la forme  $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ .

On donnera explicitement les valeurs de  $a, b$  et  $c$ .

3. En déduire la résolution du système différentiel  $\begin{cases} x' = -x - 4y \\ y' = x + 3y \end{cases}$ .

- **CCINP 86** : Petit théorème de Fermat

1. Soit  $(a, b, p) \in \mathbb{Z}^3$ . Prouver que : si  $p \wedge a = 1$  et  $p \wedge b = 1$ , alors  $p \wedge (ab) = 1$ .
2. Soit  $p$  un nombre premier.

(a) Prouver que  $\forall k \in \llbracket 1, p-1 \rrbracket$ ,  $p$  divise  $\binom{p}{k}k!$  puis en déduire que  $p$  divise  $\binom{p}{k}$ .

(b) Prouver que :  $\forall n \in \mathbb{N}$ ,  $n^p \equiv n \pmod{p}$ .

**Indication** : procéder par récurrence.

(c) En déduire, pour tout entier naturel  $n$ , que :  $p$  ne divise pas  $n \implies n^{p-1} \equiv 1 \pmod{p}$ .

- **CCINP 94** :

1. Énoncer le théorème de Bézout dans  $\mathbb{Z}$ .
2. Soit  $a$  et  $b$  deux entiers naturels premiers entre eux. Soit  $c \in \mathbb{N}$ . Prouver que :  $(a|c \text{ et } b|c) \iff ab|c$ .

3. On considère le système (S) :  $\begin{cases} x \equiv 6 \pmod{17} \\ x \equiv 4 \pmod{15} \end{cases}$  dans lequel l'inconnue  $x$  appartient à  $\mathbb{Z}$ .

(a) Déterminer une solution particulière  $x_0$  de (S) dans  $\mathbb{Z}$ .

(b) Déduire des questions précédentes la résolution dans  $\mathbb{Z}$  du système (S).

# Programme de MP2I

Contenus

Capacités & commentaires

---

## a) Divisibilité et division euclidienne

Divisibilité dans  $\mathbb{Z}$ , diviseurs, multiples.  
Théorème de la division euclidienne.

Caractérisation des couples d'entiers associés.

---

## b) PGCD et algorithme d'Euclide

PGCD de deux entiers naturels dont l'un au moins est non nul.

Notation  $a \wedge b$ . Le PGCD de  $a$  et  $b$  est défini comme étant le plus grand élément (pour l'ordre naturel dans  $\mathbb{N}$ ) de l'ensemble des diviseurs communs à  $a$  et  $b$ .

Algorithme d'Euclide.

L'ensemble des diviseurs communs à  $a$  et  $b$  est égal à l'ensemble des diviseurs de  $a \wedge b$ .

$a \wedge b$  est le plus grand élément (au sens de la divisibilité) de l'ensemble des diviseurs communs à  $a$  et  $b$ .

Pour  $k \in \mathbb{N}^*$ , PGCD de  $ka$  et  $kb$ .

Extension au cas de deux entiers relatifs.  
Relation de Bézout.

Détermination d'un couple de Bézout par l'algorithme d'Euclide étendu.

PPCM.

Notation  $a \vee b$ .

---

## c) Entiers premiers entre eux

Couple d'entiers premiers entre eux.  
Théorème de Bézout.  
Lemme de Gauss.

Si  $a$  et  $b$  sont premiers entre eux et divisent  $n$ , alors  $ab$  divise  $n$ .

Si  $a$  et  $b$  sont premiers à  $n$ , alors  $ab$  est premier à  $n$ .

PGCD d'un nombre fini d'entiers, relation de Bézout. Entiers premiers entre eux dans leur ensemble, premiers entre eux deux à deux.

Forme irréductible d'un rationnel.

---

## d) Nombres premiers

Nombre premier.  
L'ensemble des nombres premiers est infini.  
Existence et unicité de la décomposition d'un entier naturel non nul en produit de nombres premiers.  
Pour  $p$  premier, valuation  $p$ -adique.  
Valuation  $p$ -adique d'un produit.

Crible d'Ératosthène.

Notation  $v_p(n)$ .

Caractérisation de la divisibilité en termes de valuations  $p$ -adiques.

Expressions du PGCD et du PPCM à l'aide des valuations  $p$ -adiques.

---

## e) Congruences

Relation de congruence modulo un entier sur  $\mathbb{Z}$ .  
Opérations sur les congruences : somme, produit.  
Utilisation d'un inverse modulo  $n$  pour résoudre une congruence modulo  $n$ .  
Petit théorème de Fermat.

Notation  $a \equiv b [n]$ .

Les anneaux  $\mathbb{Z}/n\mathbb{Z}$  sont hors programme.