



La côte de l'ouvrage : 2-513-7

## Résumé

Cet ouvrage propose une introduction progressive et rigoureuse à l'arithmétique, une des branches les plus fascinantes et les plus fécondes des mathématiques. Nous nous intéressons plus précisément à l'arithmétique des nombres entiers et à celle des polynômes en une indéterminée. Ces deux domaines mettent en lumière de profondes analogies dans les concepts et les techniques. Le lecteur y découvre également cette remarquable spécificité de l'arithmétique pour la simplicité de ses énoncés et la variété de ses méthodes. Chacun des cinq premiers chapitres comporte un cours détaillé avec des démonstrations claires et précises, et se termine par une sélection d'exercices soigneusement choisis et entièrement corrigés. La rédaction est globalement conçue pour permettre un accès facile au lecteur débutant. Certains des exercices sont des applications directes du cours afin d'attirer l'attention sur un point délicat d'un théorème ou l'importance notable d'une nouvelle technique.

Pour les corrigés, nous avons systématiquement privilégié la solution méthodique, que peut découvrir le lecteur lui-même, à l'éventuelle approche « miraculeuse ». Un chapitre est entièrement dévolu à une sélection de problèmes de révision et de synthèse, tous entièrement corrigés. Enfin, pour le lecteur débutant, une annexe revient sur les notions de base de l'algèbre générale permettant ainsi un accès direct et confortable au contenu de l'ouvrage. Ce travail est conçu et rédigé de manière à être profitable aussi bien aux étudiants de L1, L2 et L3 des filières scientifiques, qu'aux candidats au CAPES et à l'agrégation interne.

## Table des matières

<b>1</b>	<b>Divisibilité dans <math>\mathbf{Z}</math></b>	<b>1</b>
1	Diviseurs. Multiples . . . . .	1
2	Division euclidienne dans $\mathbf{Z}$ . . . . .	2
3	Numération des entiers naturels . . . . .	4
4	PGCD et PPCM dans $\mathbf{Z}$ . . . . .	8
5	Théorèmes de Bézout et de Gauss. Applications . . . . .	13
6	Énoncés et solutions des exercices du chapitre 1 . . . . .	20
<b>2</b>	<b>Congruences</b>	<b>43</b>
1	Structure de groupe . . . . .	43
2	Structures d'anneau et de corps . . . . .	51
3	Relation et classe d'équivalence . . . . .	54
4	Groupes et anneaux quotients . . . . .	56
5	Congruences et applications. Anneau $(\mathbf{Z}/n\mathbf{Z}, +, \times)$ . . . . .	60
6	Équations et systèmes diophantiens . . . . .	69
7	Énoncés et solutions des exercices du chapitre 2 . . . . .	73
<b>3</b>	<b>Nombres premiers</b>	<b>95</b>
1	Généralités sur les nombres premiers . . . . .	95
2	Décomposition en produit de facteurs premiers . . . . .	98
3	Corps $(\mathbf{Z}/p\mathbf{Z}, +, \times)$ , $p$ premier . . . . .	100
4	Petit théorème de Fermat et théorème de Wilson . . . . .	101
5	L'indicatrice d'Euler . . . . .	104
6	Énoncés et solutions des exercices du chapitre 3 . . . . .	110
<b>4</b>	<b>Polynômes en une indéterminée</b>	<b>135</b>
1	Construction de l'algèbre des polynômes . . . . .	135
2	Degré et valuation d'un polynôme . . . . .	140
3	Fonction polynôme et évaluation . . . . .	143
4	Substitution d'un polynôme dans un autre . . . . .	144
5	Énoncés et solutions des exercices du chapitre 4 . . . . .	146

<b>5</b>	<b>Arithmétique des polynômes</b>	<b>167</b>
1	Divisibilité dans $\mathbf{K}[X]$ . . . . .	167
2	Idéaux de $\mathbf{K}[X]$ . . . . .	171
3	Racines de polynômes et multiplicités . . . . .	172
4	Fonctions symétriques élémentaires . . . . .	177
5	Dérivation des polynômes et applications . . . . .	182
6	Factorisation dans $\mathbf{C}[X]$ et dans $\mathbf{R}[X]$ . . . . .	188
7	PGCD et PPCM dans $\mathbf{K}[X]$ . . . . .	192
8	Théorèmes de Bézout et de Gauss. Applications . . . . .	196
9	Polynômes irréductibles dans $\mathbf{C}[X]$ et $\mathbf{R}[X]$ . . . . .	200
10	Racine primitive modulo $p$ . . . . .	204
11	Énoncés et solutions des exercices du chapitre 5 . . . . .	208
<b>6</b>	<b>Problèmes d'approfondissement et de synthèse</b>	<b>243</b>
1	Congruences et numéro INSEE . . . . .	243
2	Cryptographie à clef publique RSA . . . . .	245
3	Résidus quadratiques . . . . .	251
4	Symbole de Legendre . . . . .	253
5	Somme de deux carrés . . . . .	255
6	Entiers de Gauss . . . . .	257
7	Équation de Pythagore . . . . .	261
8	Équation de Fermat pour $n = 4$ . . . . .	263
9	Nombres de Carmichael . . . . .	265
10	Fonctions multiplicatives . . . . .	267
11	Produit de Dirichlet et applications . . . . .	271
12	Fonctions « somme de diviseurs » . . . . .	276
13	Racines primitives de l'unité . . . . .	279
14	Polynômes cyclotomiques . . . . .	281
<b>7</b>	<b>Rappels d'algèbre élémentaire</b>	<b>287</b>
1	Ensemble ordonné . . . . .	287
2	Principe de récurrence . . . . .	288
3	Formule du binôme de Newton . . . . .	290
4	Applications entre ensembles . . . . .	292
	<b>Bibliographie</b>	<b>299</b>
	<b>Index</b>	<b>301</b>