

Mohammed El Amrani

Arithmétique dans \mathbb{Z} et dans $\mathbb{K}[X]$

Cours complet avec exercices
et problèmes corrigés



Table des matières

1	Divisibilité dans \mathbf{Z}	1
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
2	Congruences	43
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
3	Nombres premiers	95
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
4	Polynômes en une indéterminée	135
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

5 Arithmétique des polynômes	167
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
6 Problèmes d'approfondissement et de synthèse	243
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
7 Rappels d'algèbre élémentaire	287
1 Ensemble ordonné	287
2 Principe de récurrence	288
3 Formule du binôme de Newton	290
4 Applications entre ensembles	292
Bibliographie	299
Index	301