



Arithmétique : cours et exercices corrigés
 François Liret
 Liret, François
 Dunod, Paris
 Sciences sup. Mathématiques
 ISBN: 978-2-10-056726-3

Table des Matières

Arithmétique

François Liret

Dunod

Chapitre 1 ▫ Relation d'équivalence et ensemble quotient

1.1 Partition et relation d'équivalence	1
1.2 Ensemble quotient	4
1.3 Passage au quotient d'une application	5
Exercices	7
Solutions	8

Chapitre 2 ▫ Divisibilité dans (...)

2.1 Multiple et diviseur	11
2.2 Division euclidienne	13
2.3 PGCD	14
2.4 Équation $ax + by = c$, $(x, y) (\dots) \times (\dots)$	18
2.5 PPCM	19
2.6 Décomposition en facteurs premiers	20
Exercices	22
Solutions	24

Chapitre 3 ▫ Congruence

3.1 Relation de congruence	29
3.2 Règles de calcul	31
3.3 Résolution d'équations	33
3.4 Triplets pythagoriciens	35
Exercices	36
Solutions	37

Chapitre 4 ▫ Groupes

4.1 Notion de groupe	43
4.2 Sous-groupe	46
4.3 Morphisme de groupe	48
4.4 Sous-groupe engendré par un élément	51
4.5 Ordre d'un élément	52
4.6 Classes modulo un sous-groupe	54
4.7 Sous-groupe distingué	58
Exercices	63

Solutions	64
Chapitre 5 ▫ Groupes cycliques	
5.1 Définition et premières propriétés	69
5.2 Sous-groupes d'un groupe cyclique	72
5.3 Morphismes	73
Exercices	75
Solutions	77
Chapitre 6 ▫ Anneaux et corps	
6.1 Notions générales	83
6.2 Anneau quotient	89
6.3 Anneau $(...)/n(...)$	91
6.4 Le corps $(...)_{\mathcal{p}}$	96
Exercices	97
Solutions	98
Chapitre 7 ▫ Polynômes	
7.1 Polynômes à coefficients dans un anneau	103
7.2 Anneau $K[X]$	108
7.3 Polynômes à coefficients dans $(...)_{\mathcal{p}}$	110
7.4 Calcul des coefficients binomiaux modulo \mathcal{p}	113
Exercices	115
Solutions	116
Chapitre 8 ▫ Le corps $(...)_{\mathcal{p}}$	
8.1 Les carrés dans $(...)_{\mathcal{p}}$	119
8.2 Le groupe $(...)^*_{\mathcal{p}}$	124
8.3 Le calcul des puissances modulo	126
8.4 Applications à la cryptographie	126
Exercices	128
Solutions	130
Chapitre 9 ▫ Anneaux principaux, anneaux euclidiens	
9.1 Anneau principal	135
9.2 Polynômes irréductibles de $K[X]$	140
9.3 Anneau euclidien	145
9.4 Des anneaux pour l'arithmétique	146
Exercices	151
Solutions	152
Chapitre 10 ▫ Deux problèmes classiques	
10.1 Entiers somme de deux carrés	157
10.2 L'équation de Pell-Fermat	160
Exercices	165
Solutions	167
Chapitre 11 ▫ Construction de corps	
11.1 Caractéristique d'un corps	173

11.2 Sous-corps	174
11.3 Quotient d'un anneau de polynômes	177
11.4 Extension de corps	181
Exercices	185
Solutions	187
Chapitre 12 ▫ Corps finis	
12.1 Structure des corps finis	195
12.2 L'automorphisme de Frobenius	199
12.3 Sous-corps	200
12.4 Polynômes irréductibles et corps finis	202
12.5 Polynômes irréductibles de $(\dots)_p[X]$	205
12.6 Applications à la cryptographie	207
Exercices	208
Solutions	210
Chapitre 13 ▫ Réciprocité quadratique	
13.1 Symbole de Legendre	215
13.2 La loi de réciprocité quadratique	217
Exercices	221
Solutions	222
Principales notations	227
Index	229

