Table des matières

Introduction 1

I. Primalité

Introduction à la première partie 9

Chapitre 1. Trois algorithmes fondamentaux 15

1.1. Réécriture 15
1.1.1. Règles de réécriture 15
1.1.2. Réécriture et déterminisme 17
1.1.3. Traduction dans un langage de programmation 19
1.1.4. Récursion et itération 21
1.2. Calcul rapide des puissances 23
1.2.1. Des poids faibles vers les poids forts 24
1.2.2. Des poids forts vers les poids faibles 25
1.3. Complexité des algorithmes arithmétiques 27
1.3.1. Coût des opérations arithmétiques élémentaires 27
1.3.2. Congruences dans **Z** 28
1.3.3. Le coût du calcul modulaire 30
1.3.4. Le coût de l'exponentielle 31
1.4. Algorithmes d'Euclide 33
1.4.1. L'algorithme de base 33
1.4.2. L'algorithme d'Euclide binaire 36
1.4.3. La suite de Fibonacci 37
1.4.4. Le coût de l'algorithme d'Euclide 38
1.4.5. L'algorithme d'Euclide étendu 38
1.4.6. Le coût de l'algorithme d'Euclide étendu 40
1.5. Algorithmes d'Euclide pour les polynômes 41
1.5.1. Polynômes en une variable 41
1.5.2. Division euclidienne des polynômes 42
1.5.3. Algorithmes d'Euclide 42
1.6. Algorithmes de recherche d'une période 44
1.6.1. Exemple : écriture décimale d'un nombre rationnel . . . 44
1.6.2. Période d'une suite récurrente 45
1.6.3. Algorithme de Floyd 46

1.6.4. Algorithme de Brent 47
1.6.5. La méthode de factorisation ρ de Pollard 48

Chapitre 2. Théorème de Fermat et primalité **51**

2.1. Théorème chinois 51
2.1.1. L'énoncé : forme classique 51
2.1.2. L'énoncé : forme abstraite 52
2.1.3. Les démonstrations du théorème chinois 52
2.1.4. Un algorithme 53
2.2. L'indicateur d'Euler 54
2.2.1. Le groupe $(\mathbf{Z}/n\mathbf{Z})^*$ 54
2.2.2. L'indicateur d'Euler 55
2.3. Le petit théorème de Fermat 58
2.3.1. Ordre d'un élément d'un groupe 58
2.3.2. Le petit théorème de Fermat 59
2.3.3. Une application du théorème de Fermat à la factorisation 61
2.3.4. Le théorème d'Euler 62
2.3.5. Cryptographie à clés publiques et nombres premiers : la méthode RSA 63
2.3.6. Critères de non-primalité tirés du petit théorème de Fermat 66
2.3.7. Le critère de Miller-Rabin 68

Chapitre 3. Racines primitives **71**

3.1. Structure du groupe K^* 71
3.1.1. Groupes cycliques 71
3.1.2. Exposant d'un groupe commutatif fini 71
3.1.3. Racines primitives de l'unité 73
3.1.4. Racines primitives modulo p 74
3.1.5. Recherche des racines primitives 75
3.2. Critères de primalité 76
3.2.1. Critères de primalité « à la Lehmer » 76
3.2.2. Certificats de primalité 78
3.2.3. Les nombres de Fermat 79
3.2.4. Nombres de Mersenne 81
3.2.5. Suites de Lucas 82
3.2.6. Construction d'anneaux par adjonction 84
3.2.7. Le critère de primalité de Lucas-Lehmer 85
3.2.8. Critère de primalité des nombres de Mersenne 87
3.3. Indicateur et nombres de Carmichael 89
3.3.1. Nombres de Carmichael 89
3.3.2. L'indicateur de Carmichael 90

3.3.3. Structure du groupe $(\mathbf{Z}/p^n\mathbf{Z})^*$, p premier impair 91
3.3.4. Structure du groupe $(\mathbf{Z}/2^n\mathbf{Z})^*$ 92
3.3.5. Calcul de l'indicateur de Carmichael 93
3.3.6. Preuve du théorème de Rabin 94

Chapitre 4. Transformation de Fourier rapide **99**

4.1. Transformation de Fourier discrète 99
4.1.1. Racines principales de l'unité 99
4.1.2. L'anneau $A[X]/(X^n - 1)$ 100
4.1.3. Définition de la transformation de Fourier 101
4.2. Transformation de Fourier rapide 102
4.2.1. Le principe 102
4.2.2. L'algorithme 104
4.3. Applications 105
4.3.1. Transformation de Fourier rapide modulo N 105
4.3.2. Applications arithmétiques 106
4.3.3. Multiplication des grands entiers 107
4.3.4. La méthode de Pollard 108
4.3.5. La méthode de Schönhage-Strassen 109

Chapitre 5. Résidus quadratiques et applications **111**

5.1. Résidus quadratiques 111
5.1.1. Carrés dans un corps fini 111
5.1.2. Le symbole de Legendre 112
5.1.3. Calcul d'une racine carrée dans $\mathbf{Z}/p\mathbf{Z}$ 115
5.1.4. Carrés dans $\mathbf{Z}/p^n\mathbf{Z}$ 116
5.1.5. Les signes $\varepsilon(n)$, $\omega(n)$ et $\theta(a, b)$ 117
5.2. Réciprocité quadratique 118
5.2.1. Deux exemples 118
5.2.2. Sommes de Gauss 120
5.2.3. La loi de réciprocité quadratique 121
5.3. Symbole de Jacobi 122
5.3.1. Définition et réciprocité 122
5.3.2. Algorithmes de calcul du symbole de Jacobi 124
5.3.3. Le critère de Solovay et Strassen 126
5.3.4. Tests probabilistes de primalité 127
5.3.5. Comparaison des algorithmes de Miller-Rabin et de Solovay-Strassen 129
5.4. Algorithmes probabilistes 130
5.4.1. Parties de type $\mathcal{P}$ 130
5.4.2. Parties de type $\mathcal{NP}$ 131
5.4.3. Parties de type $\mathcal{RP}$ 133

5.4.4. Le cas des nombres premiers 134

Pour aller plus loin sur la primalité **137**

II. Codes correcteurs

Introduction à la deuxième partie **141**

Chapitre 6. Codes binaires **147**

6.1. Définitions générales 147
6.1.1. Le corps $\mathbf{F}_2$ 147
6.1.2. Le modèle 147
6.1.3. Le modèle d'erreur : le canal binaire symétrique . . . 149
6.1.4. Le décodage 149
6.1.5. Codes linéaires 151
6.2. Exemples 151
6.2.1. Les codes triviaux : les cas $k = 0, 1, n-1, n$ 151
6.2.2. Codes t-correcteurs, capacité de correction, codes parfaits 152
6.2.3. Le code de Hamming H_3 de longueur 7 154
6.3. Outils de construction de codes 155
6.3.1. Constructions élémentaires 155
6.3.2. Extension paire 156
6.3.3. Orthogonal d'un code 157
6.4. Matrices génératrices et vérificatrices d'un code linéaire 158
6.4.1. Matrices génératrices et vérificatrices 159
6.4.2. Changements de base 159
6.4.3. Conditions de parité généralisées 160
6.4.4. Extension paire 161
6.4.5. Matrice vérificatrice et syndrome 161
6.5. Les codes binaires de Hamming 162
6.5.1. Construction 162
6.5.2. Les codes de Hamming étendus 164

Chapitre 7. Codes, combinatoire, géométrie **167**

7.1. Les codes binaires comme codes de parties 167
7.1.1. Traductions 167
7.1.2. Un exemple 168
7.2. Codes d'hyperplans affines 170
7.2.1. Hyperplans 171
7.2.2. L'orthogonal du code de Hamming : le code simplexe . 171
7.2.3. L'orthogonal du code de Hamming étendu : le code $R_{1,m}$ 172

7.3. Codes de Reed-Muller 173
7.3.1. Fonctions booléennes et polynômes 173
7.3.2. Définition des codes de Reed-Muller 174
7.3.3. Description itérative des codes de Reed-Muller 175
7.3.4. Mots de poids minimal du code $R_{r,m}$ 176
7.4. Géométries finies 178
7.4.1. Corps finis 178
7.4.2. Espaces affines ou projectifs finis 178
7.4.3. Plans projectifs « abstraits » 180
7.5. Systèmes de Steiner 181
7.5.1. Définition des systèmes de Steiner 181
7.5.2. Exemples 181
7.5.3. Codes et systèmes de Steiner 182
7.6. Automorphismes 184
7.6.1. Exemple : les codes cycliques 185
7.6.2. Exemple : les transformations affines 186
7.6.3. Codes et géométries finies 187

Chapitre 8. Majorations de la taille des codes 189

8.1. Conditions nécessaires 189
8.1.1. Majorations, codes optimaux 189
8.1.2. Projections et raccourcissements d'un code 190
8.1.3. Majoration de Griesmer 191
8.1.4. Majorations de Plotkin 192
8.1.5. Majoration de Hamming 192
8.2. Conditions de Gilbert-Varshamov 193
8.3. Formes asymptotiques 194
8.3.1. Le diagramme $(d/n, k/n)$ 194
8.3.2. Le domaine des codes 195
8.3.3. Préliminaires 196
8.3.4. Existence de bons codes 198
8.3.5. Bonnes familles de codes 200
8.4. Et Shannon dans tout cela ? 201
8.4.1. L'approche probabiliste 201
8.4.2. Le décodage total 202
8.4.3. Le théorème de Shannon et sa réciproque 203
8.4.4. Quel rapport avec ce qui précède ? 204
8.4.5. Une idée de la démonstration 204
8.4.6. Moralité 206

Chapitre 9. Les corps finis **207**

9.1. Structure des corps finis 207
9.1.1. Éléments algébriques, polynômes minimaux 207
9.1.2. Construction de corps par adjonction 208
9.1.3. Corps premiers 209
9.1.4. Structure des corps finis 210
9.1.5. Polynômes minimaux sur $\mathbf{F}_p$ 211
9.1.6. Automorphismes d'un corps fini 212
9.2. Polynômes cyclotomiques 212
9.2.1. Le polynôme Φ_n 213
9.2.2. Racines des polynômes cyclotomiques 214
9.2.3. Irréductibilité sur $\mathbf{Q}$ des polynômes cyclotomiques . . 215
9.2.4. Corps cyclotomiques 216
9.2.5. Décomposition des polynômes cyclotomiques dans un corps fini 217
9.3. Construction des corps finis 219
9.3.1. Polynômes irréductibles sur $\mathbf{F}_p$ 219
9.3.2. Relation entre ordre et degré 221
9.3.3. « Le » corps à q éléments 222
9.3.4. Racines de l'unité dans un corps fini 224
9.4. Calculs explicites dans un corps fini 225
9.4.1. Les corps à 2^m éléments 225
9.4.2. Exemple : le corps $\mathbf{F}_{16}$ 225
9.4.3. Le logarithme de Zech 227
9.5. Démonstration du théorème AKS 228
9.6. Décomposition des polynômes dans $\mathbf{F}_p[X]$ 231
9.6.1. Polynômes sans facteur multiple 231
9.6.2. L'algorithme de Berlekamp 232
9.6.3. Une variante probabiliste 233
9.6.4. L'algorithme de Cantor-Zassenhaus 234
9.6.5. Décomposition des polynômes dans $\mathbf{Q}[X]$ 235

Chapitre 10. Codes linéaires cycliques **237**

10.1. Codes linéaires sur $\mathbf{F}_q$ 237
10.1.1. Paramètres d'un code linéaire 237
10.1.2. Décodage 238
10.1.3. Codes parfaits 238
10.1.4. Codes sur $\mathbf{F}_q$ et codes sur $\mathbf{F}_p$ 239
10.1.5. Un exemple 240
10.1.6. Extension paire 241
10.1.7. Orthogonal 241

10.2. Codes de type MDS 241
10.2.1. La majoration de Singleton 241
10.2.2. Codes triviaux 242
10.2.3. Raccourcissement 242
10.2.4. Première construction des codes de Reed-Solomon . . 244
10.3. Codes cycliques 245
10.3.1. Définitions 245
10.3.2. Représentation des mots par des polynômes 246
10.3.3. Générateurs minimaux des codes cycliques 247
10.3.4. Codages pour un code cyclique 249
10.3.5. Constructions élémentaires 249
10.4. Classes cyclotomiques (n premier à q) 250
10.4.1. Diviseurs de $X^n - 1$ 251
10.4.2. Classes cyclotomiques 251
10.4.3. Exemples 252
10.4.4. Distance minimale des codes cycliques 253
10.4.5. Idempotents des codes cycliques 254

Chapitre 11. Codes BCH **257**

11.1. Codes cycliques usuels 257
11.1.1. Codes de Hamming binaires 257
11.1.2. Les codes de Reed-Solomon comme codes cycliques 258
11.1.3. L'autre description des codes de Reed-Solomon . . . 259
11.1.4. Codes de Reed-Solomon raccourcis 260
11.1.5. Codes BCH 260
11.2. Codes BCH binaires stricts 262
11.2.1. Construction des codes BCH binaires stricts 262
11.2.2. Exemple : les codes BCH binaires de longueur 15 . . . 263
11.2.3. Une autre définition des codes BCH binaires stricts . . . 264
11.2.4. Automorphismes d'un code BCH binaire strict étendu 265
11.3. L'algorithme de décodage des codes BCH binaires 265
11.3.1. Position du problème 266
11.3.2. Syndrome 266
11.3.3. L'équation-clé 267
11.3.4. Résolution de l'équation-clé 267
11.4. L'algorithme de décodage des codes BCH généraux 268
11.4.1. Correction de t erreurs, $t < \delta/2$ 269
11.4.2. Correction de f effacements, $f < \delta$ 269

Chapitre 12. Le codage des disques compacts 271

12.1. Position du problème 271
12.1.1. La chaîne de codage 271
12.1.2. Les contraintes du codage correcteur 273
12.2. Le code CIRC 273
12.2.1. Entrelacement 273
12.2.2. Le codage 274
12.2.3. Le décodage 275
12.2.4. Les détails du codage et du décodage 276
12.3. Au delà du code CIRC 278

Chapitre 13. Codes de résidus quadratiques 279

13.1. Codes de résidus quadratiques 279
13.1.1. Définition générale 279
13.1.2. Idempotents des codes QR binaires 281
13.1.3. Codes QR binaires étendus 282
13.1.4. Automorphismes d'un code QR binaire étendu 282
13.1.5. Distance minimale d'un code QR binaire 285
13.2. Les codes binaires de Golay G_{23} et G_{24} 286
13.2.1. Détermination des codes parfaits 288
13.2.2. Automorphismes du code de Golay : le groupe M_{24} . 290
13.2.3. Les groupes de Mathieu 291
13.3. Codes et réseaux 292
13.3.1. Réseaux 292
13.3.2. Réseau déduit d'un code binaire 293
13.3.3. Exemple : le réseau E_8 294
13.3.4. Vecteurs de carré scalaire 2 295
13.3.5. Réseaux et matrices symétriques entières 296
13.3.6. Ceci n'est pas une conclusion 297

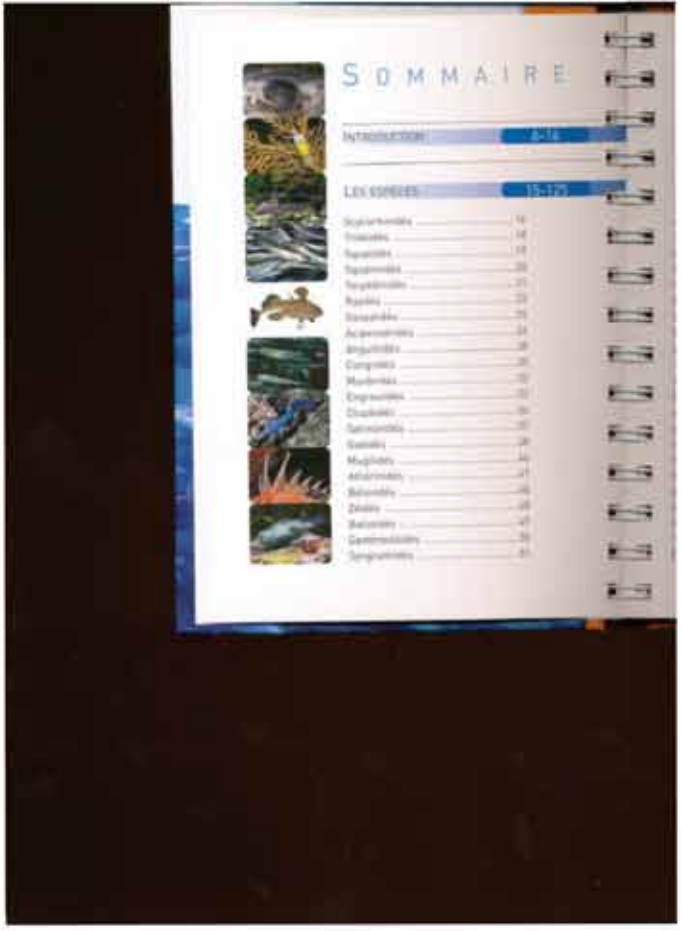
Pour aller plus loin sur les codes 299

Glossaire d'algèbre 301

Solutions des exercices 305

Bibliographie 329

Index des notations 331



Sommaire

Introduction 4-14

Les espèces 15-175