

Table des matières

IntroductionI

I. Primalité

Introduction à la première partie

Chapitre 1. Trois algorithmes fondamentaux

1.1. Réécriture

1.1.1. Règles de réécriture

1.1.2. Réécriture et déterminisme

1.1.3. Traduction dans un langage de programmation

1.1.4. Récursion et itération

1.2. Calcul rapide des puissances

1.2.1. Des poids faibles vers les poids forts

1.2.2. Des poids forts vers les poids faibles

1.3. Complexité des algorithmes arithmétiques

1.3.1. Coût des opérations arithmétiques élémentaires

1.3.2. Congruences dans \mathbb{Z}

1.3.3. Le coût du calcul modulaire

1.3.4. Le coût de l'exponentielle

1.4. Algorithmes d'Euclide

1.4.1. L'algorithme de base

1.4.2. L'algorithme d'Euclide binaire

1.4.3. La suite de Fibonacci

1.4.4. Le coût de l'algorithme d'Euclide

1.4.5. L'algorithme d'Euclide étendu

1.4.6. Le coût de l'algorithme d'Euclide étendu

1.5. Algorithmes d'Euclide pour les polynômes

1.5.1. Polynômes en une variable

1.5.2. Division euclidienne des polynômes

1.5.3. Algorithmes d'Euclide

1.6. Algorithmes de recherche d'une période

1.6.1. Exemple : écriture décimale d'un nombre rationnel

1.6.2. Période d'une suite récurrente

1.6.3. Algorithme de Floyd

1.6.4. Algorithme de Brent

1.6.5. La méthode de factorisation p de Pollard48

Chapitre 2. Théorème de Fermat et primalité51

2.1. Théorème chinois51

2.1.1. L'énoncé : forme classique51

2.1.2. L'énoncé : forme abstraite52

2.1.3. Les démonstrations du théorème chinois52

2.1.4. Un algorithme53

2.2. L'indicateur d'Euler54

2.2.1. Le groupe $(\mathbb{Z} / n\mathbb{Z})^*$ 54

2.2.2. L'indicateur d'Euler55

2.3. Le petit théorème de Fermat58

2.3.1. Ordre d'un élément d'un groupe58

2.3.2. Le petit théorème de Fermat59

2.3.3. Une application du théorème de Fermat à la factorisation61

2.3.4. Le théorème d'Euler62

2.3.5. Cryptographie à clés publiques et nombres premiers : la méthode RSA63

2.3.6. Critères de non-primalité tirés du petit théorème de Fermat66

2.3.7. Le critère de Miller-Rabin68

Chapitre 3. Racines primitives71

3.1. Structure du groupe K^* 71

3.1.1. Groupes cycliques71

3.1.2. Exposant d'un groupe commutatif fini71

3.1.3. Racines primitives de l'unité73

3.1.4. Racines primitives modulo p74

3.1.5. Recherche des racines primitives75

3.2. Critères de primalité76

3.2.1. Critères de primalité « à la Lehmer »76

3.2.2. Certificats de primalité78

3.2.3. Les nombres de Fermat79

3.2.4. Nombres de Mersenne81

3.2.5. Suites de Lucas82

3.2.6. Construction d'anneaux par adjonction84

3.2.7. Le critère de primalité de Lucas-Lehmer85

3.2.8. Critère de primalité des nombres de Mersenne87

3.3. Indicateur et nombres de Carmichael89

- 3.3.1. Nombres de Carmichael89
- 3.3.2. L'indicateur de Carmichael90
- 3.3.3. Structure du groupe $(\mathbb{Z}/p^n\mathbb{Z})^*$, p premier impair91
- 3.3.4. Structure du groupe $(\mathbb{Z}/2^n\mathbb{Z})^*$ 92
- 3.3.5. Calcul de l'indicateur de Carmichael93
- 3.3.6. Preuve du théorème de Rabin94

Chapitre 4. Transformation de Fourier rapide99

- 4.1. Transformation de Fourier discrète99
 - 4.1.1. Racines principales de l'unité99
 - 4.1.2. L'anneau $A[X]/(X^n - 1)$ 100
 - 4.1.3. Définition de la transformation de Fourier101
- 4.2. Transformation de Fourier rapide102
 - 4.2.1. Le principe102
 - 4.2.2. L'algorithme104
- 4.3. Applications105
 - 4.3.1. Transformation de Fourier rapide modulo N 105
 - 4.3.2. Applications arithmétiques106
 - 4.3.3. Multiplication des grands entiers107
 - 4.3.4. La méthode de Pollard108
 - 4.3.5. La méthode de Schönhage-Strassen109

Chapitre 5. Résidus quadratiques et applications111

- 5.1. Résidus quadratiques111
 - 5.1.1. Carrés dans un corps fini111
 - 5.1.2. Le symbole de Legendre112
 - 5.1.3. Calcul d'une racine carrée dans $\mathbb{Z}/p\mathbb{Z}$ 115
 - 5.1.4. Carrés dans $\mathbb{Z}/p^n\mathbb{Z}$ 116
 - 5.1.5. Les signes $\epsilon(n)$, $\omega(n)$ et $\theta(a,b)$ 117
- 5.2. Réciprocité quadratique118
 - 5.2.1. Deux exemples118
 - 5.2.2. Sommes de Gauss120
 - 5.2.3. La loi de réciprocité quadratique121
- 5.3. Symbole de Jacobi122
 - 5.3.1. Définition et réciprocité122
 - 5.3.2. Algorithmes de calcul du symbole de Jacobi124
 - 5.3.3. Le critère de Solovay et Strassen126

5.3.4. Tests probabilistes de primalité127

5.3.5. Comparaison des algorithmes de Miller-Rabin et de Solovay-Strassen129

5.4. Algorithmes probabilistes130

5.4.1. Parties de type P130

5.4.2. Parties de type NP131

5.4.3. Parties de type RP133

5.4.4. Le cas des nombres premiers134

Pour aller plus loin sur la primalité137

II. Codes correcteurs

Introduction à la deuxième partie141

Chapitre 6. Codes binaires147

6.1. Définitions générales147

6.1.1. Le corps F_2 147

6.1.2. Le modèle147

6.1.3. Le modèle d'erreur : le canal binaire symétrique149

6.1.4. Le décodage149

6.1.5. Codes linéaires151

6.2. Exemples151

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 parfaits152

6.2.3. Le code de Hamming H_3 de longueur 7154

6.3. Outils de construction de codes155

6.3.1. Constructions élémentaires155

6.3.2. Extension paire156

6.3.3. Orthogonal d'un code157

6.4. Matrices génératrices et vérificatrices d'un code linéaire158

6.4.1. Matrices génératrices et vérificatrices159

6.4.2. Changements de base159

6.4.3. Conditions de parité généralisées160

6.4.4. Extension paire161

6.4.5. Matrice vérificatrice et syndrome161

6.5. Les codes binaires de Hamming162

6.5.1. Construction162

6.5.2. Les codes de Hamming étendus164

Chapitre 7. Codes, combinatoire, géométrie167

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 $R_{t,m}$	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 $R_{t,m}$	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. Préliminaires196

8.3.4. Existence de bons codes198

8.3.5. Bonnes familles de codes200

8.4. Et Shannon dans tout cela ?201

8.4.1. L'approche probabiliste201

8.4.2. Le décodage total202

8.4.3. Le théorème de Shannon et sa réciproque203

8.4.4. Quel rapport avec ce qui précède ?204

8.4.5. Une idée de la démonstration204

8.4.6. Moralité206

Chapitre 9. Les corps finis207

9.1. Structure des corps finis207

9.1.1. Éléments algébriques, polynômes minimaux207

9.1.2. Construction de corps par adjonction208

9.1.3. Corps premiers209

9.1.4. Structure des corps finis210

9.1.5. Polynômes minimaux sur F_p 211

9.1.6. Automorphismes d'un corps fini212

9.2. Polynômes cyclotomiques212

9.2.1. Le polynôme Φ_n 213

9.2.2. Racines des polynômes cyclotomiques214

9.2.3. Irréductibilité sur \mathbb{Q} des polynômes cyclotomiques215

9.2.4. Corps cyclotomiques216

9.2.5. Décomposition des polynômes cyclotomiques dans un corps fini217

9.3. Construction des corps finis219

9.3.1. Polynômes irréductibles sur F_p 219

9.3.2. Relation entre ordre et degré221

9.3.3. « Le » corps à q éléments222

9.3.4. Racines de l'unité dans un corps fini224

9.4. Calculs explicites dans un corps fini225

9.4.1. Les corps à 2^m éléments225

9.4.2. Exemple : le corps F_{16} 225

9.4.3. Le logarithme de Zech227

9.5. Démonstration du théorème AKS228

9.6. Décomposition des polynômes dans $F_p[X]$ 231

- 9.6.1. Polynômes sans facteur multiple231
- 9.6.2. L'algorithme de Berlekamp232
- 9.6.3. Une variante probabiliste233
- 9.6.4. L'algorithme de Cantor-Zassenhaus234
- 9.6.5. Décomposition des polynômes dans $\mathbb{Q}[X]$ 235

Chapitre 10. Codes linéaires cycliques237

- 10.1. Codes linéaires sur F_q 237
 - 10.1.1. Paramètres d'un code linéaire237
 - 10.1.2. Décodage238
 - 10.1.3. Codes parfaits238
 - 10.1.4. Codes sur F_q et codes sur F_p 239
 - 10.1.5. Un exemple240
 - 10.1.6. Extension paire241
 - 10.1.7. Orthogonal241
- 10.2. Codes de type MDS241
 - 10.2.1. La majoration de Singleton241
 - 10.2.2. Codes triviaux242
 - 10.2.3. Raccourcissement242
 - 10.2.4. Première construction des codes de Reed-Solomon244
- 10.3. Codes cycliques245
 - 10.3.1. Définitions245
 - 10.3.2. Représentation des mots par des polynômes246
 - 10.3.3. Générateurs minimaux des codes cycliques247
 - 10.3.4. Codages pour un code cyclique249
 - 10.3.5. Constructions élémentaires249
- 10.4. Classes cyclotomiques (n premier à q)250
 - 10.4.1. Diviseurs de $X^n - 1$ 251
 - 10.4.2. Classes cyclotomiques251
 - 10.4.3. Exemples252
 - 10.4.4. Distance minimale des codes cycliques253
 - 10.4.5. Idempotents des codes cycliques254

Chapitre II. Codes BCH257

- 11.1. Codes cycliques usuels257
 - 11.1.1. Codes de Hamming binaires257
 - 11.1.2. Les codes de Reed-Solomon comme codes cycliques258

- 11.1.3. L'autre description des codes de Reed-Solomon259
- 11.1.4. Codes de Reed-Solomon raccourcis260
- 11.1.5. Codes BCH260
- 11.2. Codes BCH binaires stricts262
 - 11.2.1. Construction des codes BCH binaires stricts262
 - 11.2.2. Exemple : les codes BCH binaires de longueur 15263
 - 11.2.3. Une autre définition des codes BCH binaires stricts264
 - 11.2.4. Automorphismes d'un code BCH binaire strict étendu265
- 11.3. L'algorithme de décodage des codes BCH binaires265
 - 11.3.1. Position du problème266
 - 11.3.2. Syndrome266
 - 11.3.3. L'équation-clé267
 - 11.3.4. Résolution de l'équation-clé267
- 11.4. L'algorithme de décodage des codes BCH généraux268
 - 11.4.1. Correction de t erreurs, $t < 8/2269$
 - 11.4.2. Correction de f effacements, $f < 8269$

Chapitre 12. Le codage des disques compacts271

- 12.1. Position du problème271
 - 12.1.1. La chaîne de codage271
 - 12.1.2. Les contraintes du codage correcteur273
- 12.2. Le code CIRC273
 - 12.2.1. Entrelacement273
 - 12.2.2. Le codage274
 - 12.2.3. Le décodage275
 - 12.2.4. Les détails du codage et du décodage276
- 12.3. Au delà du code CIRC278

Chapitre 13. Codes de résidus quadratiques279

- 13.1. Codes de résidus quadratiques279
 - 13.1.1. Définition générale279
 - 13.1.2. Idempotents des codes QR binaires281
 - 13.1.3. Codes QR binaires étendus282
 - 13.1.4. Automorphismes d'un code QR binaire étendu282
 - 13.1.5. Distance minimale d'un code QR binaire285
- 13.2. Les codes binaires de Golay G_{23} et G_{24} 286
 - 13.2.1. Détermination des codes parfaits288

13.2.2. Automorphismes du code de Golay : le groupe M_{24} 290

13.2.3. Les groupes de Mathieu291

13.3. Codes et réseaux292

13.3.1. Réseaux292

13.3.2. Réseau déduit d'un code binaire293

13.3.3. Exemple : le réseau E_8 294

13.3.4. Vecteurs de carré scalaire 2295

13.3.5. Réseaux et matrices symétriques entières296

13.3.6. Ceci n'est pas une conclusion297

Pour aller plus loin sur les codes299

Glossaire d'algèbre301

Solutions des exercices305

Bibliographie329

Index des notations331