

# Table des matières

(see contents page xii)

<b>Préface</b>	v
<b>Avant-propos</b>	xiii
<b>Chapitre 1 : Algorithmique et programmation Ada</b>	1
1 Préliminaire algorithmique	1
1.1 Terminologie et notations	2
1.2 L'affectation	2
1.3 La séquence	3
1.4 L'alternative	3
1.5 L'itération	5
1.6 L'itération calculée, ou boucle pour	6
1.7 La boucle "tant que"	6
1.8 L'itération (suite et fin)	7
2 L'algorithme d'exponentiation dichotomique	8
2.1 L'approche mathématique (ou récursive)	8
2.2 L'approche algorithmique	9
2.3 Etude de complexité	11
3 Introduction à la programmation en Ada	12
3.1 Programme de comparaison de deux méthodes d'exponentiation	12
3.2 De l'utilisation des types	17
3.3 L'itération dans un monoïde — Fonctions génériques	21
3.3.1 Une fonction générique d'exponentiation dichotomique	22
3.3.2 Utilisation de la fonction générique	24
3.4 Une utilisation bizarre d'un compilateur Ada	28
4 Une bonne approximation de l'infini !	29
4.1 Eléments de manipulation de tableaux en Ada	30
4.2 Manipulation de matrices	33
4.3 Entrées/sorties de matrices	37
4.4 Spécification d'un générateur de bijections	39
4.5 Le calcul du déterminant	41
4.6 Calculs de déterminants : quelques chiffres	42
4.7 Les permutations d'un ensemble fini	44
4.8 Un générateur de bijections générique	47
5 Conclusion	49
Exercices	52
Solutions des exercices	66
<b>Chapitre 2 : Euclide et le théorème fondamental de l'arithmétique</b>	107
1 Vers une généralisation de l'arithmétique des entiers	108
1.1 Divisibilité et éléments irréductibles	109
1.2 Qu'est ce qu'un anneau factoriel ?	109
1.3 Généraliser l'arithmétique des entiers : pour quoi faire ?	110
1.4 Les éléments premiers	113
2 Propriétés élémentaires en théorie de la divisibilité	113
2.1 Existence et unicité d'une décomposition primaire	113
2.2 Pgcd et éléments étrangers entre eux	113

2.3 Les concepts dégagés	114
2.4 La relation de Bezout	116
3 Les anneaux euclidiens ou le point de vue effectif	117
3.1 Qu'est ce qu'un anneau euclidien ?	117
3.2 L'algorithme d'Euclide pour le calcul du pgcd	119
3.3 Implémentation en Ada du calcul du pgcd	120
3.4 Efficacité comparée de différentes divisions	122
3.5 Factorialité des anneaux euclidiens intègres	124
4 Polynômes à coefficients dans un corps commutatif	125
4.1 Division euclidienne dans $K[X]$ ( $K$ corps commutatif)	125
4.2 Polynômes irréductibles à coefficients dans $\mathbf{Z}/p\mathbf{Z}$	127
4.3 Un critère modeste d'irréductibilité modulo $p$	129
5 Les anneaux principaux ou le point de vue idéaliste	130
5.1 L'idéalisation	130
5.2 Quotients d'un anneau principal	131
6 Vers des algorithmes optimaux pour le calcul du pgcd	132
6.1 Calcul du pgcd de deux entiers : théorème de Lamé	133
6.2 Anneaux quasi-euclidiens	135
6.3 Calcul du pgcd de plusieurs entiers : le théorème de Dirichlet	137
7 Algorithme d'Euclide étendu	142
7.1 Calcul des coefficients de Bezout dans un anneau quasi-euclidien	142
7.2 Majoration des coefficients de Bezout dans $\mathbf{Z}$	144
8 Factorialité des anneaux de polynômes	145
9 En guise de conclusion	150
Exercices	152
Solutions des exercices	171
<b>Chapitre 3 : Modules sur les anneaux principaux</b>	<b>196</b>
1 L'élimination et quelques conséquences immédiates	198
1.1 Opérations sur les lignes et les colonnes d'une matrice	198
1.2 Le lemme d'élimination	199
1.3 Calcul de déterminants	201
1.4 Modules sans torsion de type fini	203
2 Forme normalisée d'un sous-groupe de $\mathbf{Z}^n$	204
2.1 Etude du sous-groupe $n\mathbf{Z} \times m\mathbf{Z}$ de $\mathbf{Z}^2$	204
2.2 Etude du sous-groupe $a_1\mathbf{Z} \times \dots \times a_n\mathbf{Z}$ de $\mathbf{Z}^n$	205
2.3 Unicité de la décomposition normalisée	209
3 Calcul de l'image et du noyau d'une matrice	211
3.1 Matrices échelonnées	212
3.2 Calcul de l'image d'une matrice	212
3.3 Existence d'une solution d'un système linéaire	216
3.4 Calcul du noyau d'une matrice	219
3.5 Résolution complète d'un système linéaire	219
3.6 Rang des modules	221
4 Réduction d'une matrice	224
5 Modules de type fini sur un anneau principal	229
5.1 Supplémentaire, liberté et torsion	229
5.2 Facteurs invariants d'un sous-module d'un module libre	231
5.3 Facteurs invariants d'un module de type fini	236
6 Un rapide tour d'horizon	237
Exercices	241
Solutions des exercices	250
<b>Chapitre 4 : Quelques méthodes d'algorithmique algébrique</b>	<b>265</b>
1 L'anneau $\mathbf{Z}/n\mathbf{Z}$	266
2 Le théorème chinois	271
2.1 Différentes formes du théorème chinois	271

2.2 Arithmétique modulaire et numération mixte	275
2.3 Multiplication des entiers par la méthode de Pollard	279
3 Le groupe des inversibles de $\mathbf{Z}/n\mathbf{Z}$	284
3.1 Générateurs de $\mathbf{Z}/n\mathbf{Z}$ et indicateur d'Euler	284
3.2 Les systèmes de cryptographie à clef publique	286
3.2.1 La méthode RSA	287
3.2.2 L'algorithme du sac à dos	288
3.2.3 Comment partager un secret ?	291
3.3 Sous-groupes multiplicatifs d'un corps fini	291
3.3.1 Annulateur d'un groupe abélien fini	293
3.3.2 Indicateur de Carmichael	294
3.4 Le groupe des inversibles de $\mathbf{Z}/p^r\mathbf{Z}$	296
3.4.1 Quelques congruences utiles	296
3.4.2 Le groupe des inversibles de $\mathbf{Z}/2^r\mathbf{Z}$	299
3.4.3 Le groupe des inversibles de $\mathbf{Z}/p^r\mathbf{Z}$ , $p$ impair	300
4 Suites ultimement périodiques	303
4.1 Générateurs à un pas	303
4.2 Générateurs congruentiels linéaires	306
4.3 Détection de la période par la méthode de Brent	308
5 Résidus quadratiques	312
5.1 Propriétés générales	313
5.2 Racines carrées : la méthode de Zassenhaus-Cantor	316
5.3 Racines carrées : la méthode de Shanks	321
6 Factorisation et primalité	324
6.1 Les nombres de Mersenne	324
6.2 Le test de primalité de Rabin-Miller	329
6.2.1 L'algorithme probabiliste de Rabin	331
6.2.2 La démonstration du théorème de Rabin	332
6.3 La rho-méthode de factorisation de Pollard	337
7 Ce n'est qu'un début	339
Exercices	340
Solutions des exercices	354
<b>Chapitre 5 : La transformée de Fourier discrète</b>	379
1 Complexité de la multiplication de deux polynômes	380
1.1 Interpolation de polynômes sur un corps, sur un anneau	380
1.2 Evaluation de polynômes en des racines de l'unité	381
1.3 Racines primitives de l'unité	383
1.4 Transformée de Fourier discrète et convolution cyclique	385
1.5 Un tour d'horizon des différentes notions	387
2 Fast Fourier transform	388
2.1 Cas où l'ordre est une puissance de 2	388
2.2 Cas où l'ordre est une puissance quelconque	389
2.3 Développement de l'algorithme itératif sur un exemple	390
2.3.1 Du récursif à l'itératif	390
2.3.2 Les sommes de Yates	391
3 Calcul exact avec FFT : produit de polynômes	392
3.1 Implémentation de FFT lorsque l'ordre est une puissance de 2	392
3.2 Comment implémenter FFT ?	393
3.3 La multiplication des polynômes	395
3.4 Implémentation du produit de polynômes	397
3.5 Le calcul de la transformée de Fourier	399
4 Etude fine de la méthode de Cooley et Tuckey	402
4.1 Cooley-Tuckey pour un produit de 2 facteurs	404
4.2 Itération de la méthode de Cooley-Tuckey	407
4.2.1 Complexité de la méthode itérée de Cooley-Tuckey	407
4.2.2 Les formules pour itérer la méthode de Cooley-Tuckey	408

5	La méthode de Good	411
5.1	Etude de l'exemple $15 = 3 \times 5$	411
5.2	Développement du théorème de Good	412
6	Evaluation d'une famille de formes bilinéaires	415
6.1	Quelques rappels, définitions et premières propriétés	416
6.2	Rang tensoriel du produit de deux polynômes	417
6.3	Etude sur un exemple : la convolution cyclique d'ordre 4	420
6.4	Famille de formes bilinéaires et formes trinéaires	421
6.5	Etude sur un exemple : la convolution cyclique d'ordre 4 (suite)	423
7	Petits schémas de transformée de Fourier discrète	425
7.1	DFT d'ordre $p$ et CC d'ordre $p - 1$ (Méthode de Rader)	425
7.2	Composition des schémas de Rader et de Good	426
7.2.1	Etude fine de $DFT_3$	427
7.2.2	$DFT_5$ réapparaît	428
8	De FFT au produit tensoriel	430
	Exercices	432
	Solutions des exercices	441
	<b>Bibliographie</b>	<b>459</b>
	<b>Index</b>	<b>465</b>