

Table des matières

Chapitre 1

Division euclidienne et algorithme d'Euclide	17
1.1. Division euclidienne.....	17
1.1.1. Programmation.....	18
1.1.2. Comment tracer une droite sur un écran d'ordinateur ?.....	18
1.1.3. Extension : La division avec virgule	19
1.2. Diviseurs d'un nombre	21
1.2.1. Définition	21
1.2.2. Comment obtenir tous les diviseurs d'un nombre ?	21
1.2.3. Nombre premier et diviseurs	22
1.3. Pgcd et ppmc de deux nombres.....	23
1.3.1. Diviseurs communs et pgcd	23
1.3.2. Multiples communs et ppmc	24
1.3.3. Programme pour avoir le ppmc	24
1.4. Algorithme d'Euclide pour avoir le pgcd de deux nombres.....	25
1.4.1. Divisions successives	25
1.4.2. Programme	26
1.4.3. Pgcd en binaire	27
1.5. Algorithme d'Euclide étendu	28
1.5.1. Combinaison linéaire de deux nombres	28
1.5.2. Propriété du pgcd	28
1.5.4. Programme de l'algorithme d'Euclide étendu.....	30
1.5.5. Pgcd et diviseurs communs	30
1.6. Nombres premiers entre eux et théorème de Bezout.....	31
1.6.1. Définition	31

6 Algorithmes et théorie des nombres

1.6.2. Théorème de Bezout.....	31
1.6.3. Théorème de Gauss-Euclide.....	32
1.7. Théorème fondamental de l'arithmétique	32
1.7.1. Démonstration	33
1.7.2. Quelques applications	33
1.7.3. Programme de la décomposition d'un nombre en produit de nombres premiers	36

Chapitre 2

Equation de Diophante du premier degré.....	39
2.1. Résolution de l'équation.....	39
2.2. Cas particulier où a et b sont premiers entre eux	41
2.2.1. Équation $ax + by = c$, avec a, b et c positifs	41
2.2.2. Vision géométrique	41
2.2.3. Équation $ax - by = c$, avec a, b, c positifs et a premier avec b	42
2.2.4. Nombre de solutions positives ou nulles de $ax + by = c$	43

Chapitre 3

Fractions continuées.....	63
3.1. Définition	63
3.2. Réduites d'une fraction continuée.....	65
3.3. Propriétés.....	66
3.3.1. Calcul des réduites	66
3.3.2. Relations entre réduites	66
3.3.3. Oscillations des réduites.....	67
3.3.4. Programmation.....	67
3.3.5. Rôle de l'avant-dernière réduite	68
3.4. Fractions continuées d'un nombre irrationnel.....	70
3.4.1. Développement infini en fractions continuées	70
3.4.2. Cas particulier des nombres irrationnels quadratiques.....	72
3.4.3. Équation de Pell	75

Chapitre 4

Nombres modulaires	81
4.1. L'anneau \mathbf{Z}_n	81
4.1.1. Congruences et classes d'équivalence.....	81
4.1.2. Système complet de résidus \mathbf{Z}_n	82
4.1.3. Opérations dans \mathbf{Z}_n	83
4.1.4. L'anneau commutatif \mathbf{Z}_n	83
4.1.5. Propriété de simplification	84
4.2. Système réduit de résidus $\mathbf{U}(n)$ des éléments inversibles de \mathbf{Z}_n	85
4.2.1. Propriété fondamentale et fonction d'Euler	85
4.2.2. Corps \mathbf{Z}_p pour p premier.....	85
4.3. Théorèmes d'Euler et de Fermat	86
4.3.1. Théorème d'Euler.....	86
4.3.2. Théorème de Fermat.....	87
4.4. L'algorithme de puissance	87
4.4.1. Première méthode.....	87
4.4.2. Une méthode plus performante	88
4.4.3. Autre méthode.....	90

Chapitre 5

Le théorème chinois	97
5.1. Le contexte du théorème chinois.....	97
5.1.1. Une généralisation du ppmc	97
5.1.2. L'origine historique du théorème	98
5.2. Le théorème chinois	98
5.3. Isomorphismes	101
5.3.1. Isomorphisme d'anneaux entre \mathbf{Z}_m et $\mathbf{Z}_{m_1} \mathbf{Z}_{m_2} \dots \mathbf{Z}_{m_n}$	101
5.3.2. Isomorphisme de groupe entre $\mathbf{U}(m)$ et $\mathbf{U}(m_1)\mathbf{U}(m_2)\dots\mathbf{U}(m_n)$	102
5.4. Programmes.....	103
5.4.1. Isomorphisme entre \mathbf{Z}_m et $\mathbf{Z}_{m_1} \mathbf{Z}_{m_2}$	103
5.4.2. Résolution d'un système d'équations.....	104

5.5. Conséquences	104
5.5.1. Fonction d'Euler φ	104
5.5.2. Résolution d'une équation polynomiale.....	106
5.5.3. Récurrences modulaires.....	107

Chapitre 6

Nombres premiers.....	113
6.1. Distribution des nombres premiers	114
6.2. Le crible d'Eratosthène	116
6.2.1. Propriété préliminaire.....	116
6.2.2. La méthode du crible.....	117
6.2.3. Programmation	117
6.3. Algorithmes de factorisation d'entiers	118
6.3.1. La méthode des divisions successives.....	119
6.3.2. La méthode de Fermat.....	120
6.4. Comment savoir si un nombre est premier.....	123
6.4.1. Recherche de nombres probablement premiers.....	123
6.4.2. Nombres fort probablement premiers.....	124
6.5. La méthode rho de Pollard	126
6.5.1. Algorithme de l'éternel retour.....	126
6.5.2. La méthode de Pollard.....	130
6.5.3. Validité de l'algorithme	132
6.5.4. Programmes.....	133
6.5.5. Résultats	134
6.6. L'algorithme $p - 1$ de Pollard	135
6.6.1. Explication de la méthode dans le cas général	135
6.6.2. Que faire lorsque l'algorithme ne fonctionne pas ?.....	137
6.6.3. Variantes de l'algorithme	138
6.6.4. Méthode finale.....	141
6.6.5. Conclusion sur la méthode $p - 1$	142
6.7. Théorème de Wilson	142

6.8. Prolongement : Entiers de Gauss et nombres premiers	143
--	-----

Chapitre 7

Puissances de nombres modulaires.....151

7.1. Sous-groupe des puissances et ordre d'un élément de $U(n)$	151
7.1.1. Propriété 1 : Ordre d'un élément.....	151
7.1.2. Propriété 2 : Théorème de Lagrange	152
7.1.3. Sous-groupe des puissances de a , et ses cosets dans $U(n)$	152
7.1.4. Propriété 3 : Ordre des puissances d'un nombre.....	153
7.1.5. Propriété 4 : Ordre d'un produit.....	154
7.2. Puissances dans $U(p)$ avec p premier impair.....	154
7.2.1. Théorème préliminaire	154
7.2.2. Propriété 5 : Ordre d'un diviseur.....	155
7.3. Générateurs	156
7.3.1. Définition	156
7.3.2. Propriété 6 : Nombre de générateurs.....	156
7.4. Algorithmes et programmes dans $U(p)$	159
7.4.1. Programme pour avoir l'ordre des éléments de $U(p)$	159
7.4.2. Algorithmes pour obtenir un générateur dans $U(p)$	160
7.5. Le problème du logarithme discret.....	166
7.5.1. Algorithme pas de bébé-pas de géant.....	166
7.5.2. Programme	167
7.6. Éléments inversibles, réguliers, nilpotents, diviseurs de zéro	169
7.6.1. Définitions.....	170
7.6.2. Propriétés (dans un anneau)	170
7.6.3. Trajectoire des puissances de a dans Z_n	171

Chapitre 8

Étude du groupe multiplicatif $U(n)$175

8.1. Groupe cyclique additif et produit direct de groupes.....	175
8.1.1. Groupe Z_n muni de l'addition	175

8.1.2. Produit direct de groupes.....	176
8.1.3. Sous-groupe d'un groupe cyclique.....	177
8.2. Étude de $U(2^n)$	178
8.2.1. Premiers cas	178
8.2.2. Ordre de 5 dans $U(2^n)$ pour $n > 2$	178
8.2.3. Propriété de $U(2^n)$	179
8.3. Étude de $U(p^n)$ pour p premier impair.....	180
8.3.1. Propriété 1	180
8.3.2. Propriété 2	181
8.3.3. Isomorphisme de $U(p^n)$ avec $Z_{p^{n-1}} \times Z_{p-1}$	182
8.3.4. Propriété 3	182
8.3.5. Étude particulière de $U(p^2)$	183
8.3.6. Retour à l'isomorphisme de $U(p^n)$	184
8.4. Étude de $U(n)$	191
8.5. Suite géométrique modulaire dans $U(m)$	194
8.6. Suite arithmético-géométrique modulaire	196

Chapitre 9

Second degré modulaire	201
9.1. Carrés et racines carrées dans $U(p)$	201
9.1.1. Définition	201
9.1.2. Propriété 1	201
9.1.3. Propriété 2	202
9.1.4. Critère d'Euler	202
9.1.5. Symbole de Legendre.....	202
9.1.6. Loi de réciprocité quadratique de Gauss	203
9.1.7. Conséquence.....	206
9.2. Équation $x^2 = a$ modulo m , avec a premier avec m	211
9.2.1. Premier cas : m est un nombre premier impair.....	211
9.2.2. Deuxième cas : m est une puissance de nombre premier impair....	211
9.2.3. Troisième cas : m est une puissance de 2	213

9.2.4. Quatrième cas : cas général	214
9.2.5. Programme pour avoir une racine carrée modulo un nombre premier	218
9.3. Symbole de Jacobi.....	224
9.3.1. Définition	225
9.3.2. Propriétés.....	226
9.3.3. Intérêt du symbole de Jacobi.....	226
9.3.4. Programme du symbole de Jacobi.....	231
9.3.5. Test de primalité de Solovay-Strassen	232

Chapitre 10

Équations polynomiales modulaires	239
10.1. Équation du premier degré	239
10.2. Équation modulo p , nombre premier.....	240
10.3. Quelques équations particulières dans $\mathbf{U}(p)$	242
10.3.1. Équation $x^d = 1 [p]$ avec d diviseur de $p - 1$	242
10.3.2. Équation $x^n = a$ dans $\mathbf{U}(p)$	242
10.4. Équation modulo une puissance p^i de nombre premier	244
10.4.1. Théorème de Hensel.....	244
10.4.2. Les cas singuliers	247

Chapitre 11

Équations à plusieurs inconnues.....	249
11.1. Écriture d'un nombre entier comme somme de deux carrés	250
11.1.1. Résolution de l'équation $x^2 + y^2 = p$ avec p premier	250
11.1.2. Condition d'existence de solutions pour l'équation $x^2 + y^2 = n$	253
11.1.3. Formules donnant le nombre des solutions de $x^2 + y^2 = n$	253
11.1.4. Méthode donnant les solutions de $x^2 + y^2 = n$	254
11.2. Équation $ax^2 + by^2 = 1 [p]$, p étant un nombre premier impair	262
11.2.1. Propriété préliminaire.....	262
11.2.2. Propriété 2	264

12 Algorithmes et théorie des nombres

11.2.3. Propriété 3	266
11.3. Triangles de Pythagore.....	271
11.3.1. Infinité des solutions	271
11.3.2. Solutions primitives.....	272
11.3.3. Propriété préliminaire 1.....	272
11.3.4. Propriété préliminaire 2.....	272
11.3.5. Théorème.....	273
11.3.6. Programme pour avoir toutes les solutions primitives	273
11.4. La méthode de la descente de Fermat	274

Chapitre 12

La fonction de Möbius	279
12.1. Notion de fonction multiplicative	279
12.1.1. Définition d'une fonction multiplicative.....	279
12.1.2. Propriétés.....	279
12.2. La fonction de Möbius	281
12.2.1. Définition	281
12.2.2. Propriété caractéristique de la fonction de Möbius	282
12.3. Intérêt de la fonction de Möbius	284
12.4. Formule d'inversion de Möbius	284
12.5. Colliers formés de perles de deux types.....	286
12.5.1. Colliers et classes de conjugaison d'un mot.....	286
12.5.2. Nombre $N(n)$ de colliers de n perles de deux types.....	287
12.5.3. Colliers sans sous-période.....	291
12.6. Écriture d'une fraction en binaire.....	298
12.6.1. Cas où le dénominateur est impair	298
12.6.2. Cas où le dénominateur est pair	300
12.6.3. Périodes cycliquement équivalentes, et mots de Lyndon.....	301
12.6.4. Détermination d'une fraction à partir de sa période en binaire	303
12.6.5. Nombre de fractions a/b irréductibles ayant une même longueur de période	306

12.6.6. Nombre de dénominateurs donnant une même longueur de période.....	307
---	-----

Chapitre 13

Tests de primalité et de factorisation.....309

13.1. Faux premiers, et nombres de Carmichael	309
13.1.1. Nombres premiers probables.....	309
13.1.2. Nombres de Carmichael	310
13.2. Algorithme AKS	316
13.2.1. Propriété	316
13.2.2. Les polynômes modulaires.....	317
13.3. Nombres de Mersenne et primalité	318
13.3.1. Nombres de Mersenne.....	318
13.3.2. Test de Lucas-Lehmer	319
13.4. Nombres de Fermat et test de Pépin.....	321
13.4.1. Un test de primalité	321
13.4.2. Les nombres de Fermat	323
13.4.3. Test de Pépin	323
13.5. Factorisation par crible quadratique	328
13.5.1. Au-delà de la méthode de Fermat.....	328
13.5.2. Méthode du crible quadratique.....	332
13.5.3. Programme du crible quadratique	334
13.6. À propos de complexité.....	341

Chapitre 14

Eléments de cryptographie.....343

14.1. Cryptage symétrique et cryptage asymétrique	343
14.2. Partage de secret.....	345
14.2.1. Cryptographie graphique.....	345
14.2.2. Partage modulaire.....	347
14.2.3. Partage par interpolation	347

14	Algorithmes et théorie des nombres	
14.3.	La méthode RSA en cryptographie	350
14.3.1.	Étude de l'application faisant passer de a à $a^k [m]$	351
14.3.2.	Programme de la méthode RSA	351
14.4.	Le cryptage El Gamal	355
14.5.	Le problème de la signature	356

Chapitre 15

Courbes elliptiques	359
15.1. Sécantes et tangentes	361
15.2. Courbe elliptique dans un corps K , et groupe additif de points	363
15.3. Formules d'addition	364
15.4. Courbes elliptiques $E(\mathbf{Z}_p)$	368
15.4.1. Nombre d'éléments d'une courbe elliptique $E(\mathbf{Z}_p)$	368
15.4.2. Programmation des formules d'addition et de doublement	369
15.5. Structure des groupes $E(\mathbf{Z}_p)$	374
15.6. Calcul du point kP par doublements répétés	375
15.7. Factorisation d'un nombre	376
15.8. Le problème du logarithme discret	379
15.9. Cryptographie utilisant les courbes elliptiques	380
15.9.1. Problème de partage	381
15.9.2. La méthode de chiffrement d'El Gamal	381

Chapitre 16

Grille de points et algorithme LLL	383
16.1. Définition et propriétés d'un réseau	383
16.2. Procédé d'orthogonalisation de Gram-Schmidt	386
16.3. Réduction de Gauss en deux dimensions	389
16.4. Réduction de taille en n dimensions	393
16.5. L'algorithme LLL	395
16.6. Le craquage du crypto-système de Merkle et Hellman	396
16.6.1. Le problème du sac à dos	397

16.6.2. Le cas facile d'une suite super-croissante	398
16.6.3. Le brouillage modulaire	400
16.6.4. Le problème de l'unicité	400
16.6.5. Le crypto-système de Merkle-Hellman	401
16.6.6. Comment casser le crypto-système Merkle-Hellman.....	402
Chapitre 17	
Réurrences linéaires	405
17.1. Suites dans \mathbf{Z}	405
17.1.1. Formule explicite.....	405
17.1.2. Les deux suites de Lucas.....	407
17.2. Suite de Lucas dans \mathbf{Z}_p et test de primalité	411
17.3. Réurrences linéaires modulaires et puissances de matrices.....	414
17.3.1 Matrice associée à la récurrence.....	414
17.3.2. La suite à impulsion initiale	415
17.3.3. Cas particulier des suites périodiques	416
17.4. Réurrences modulo un nombre premier impair p	418
17.4.1. Premier cas : $D = 0$	419
17.4.2. Deuxième cas : D est un carré dans $\mathbf{U}(p)$	420
17.4.3. Troisième cas : D est un non carré dans $\mathbf{U}(p)$	421
17.4.4. Le problème de la période maximale	422
Bibliographie	429
Index	431