

Gilles Bailly-Maitre

ARITHMÉTIQUE ET CRYPTOLOGIE



Table des Matières

I	Cryptologie à l'ancienne	1
1	Historique	3
I	De l'Antiquité au Moyen Âge	3
II	Le chiffrement de Vigenère	8
II.1	Description	8
II.2	Cryptanalyse	10
III	Le one-time pad ou masque jetable	12
IV	La machine Enigma	14
V	Et après...	18
VI	Exercices	19
II	Les nombres de la cryptologie	21
2	Divisibilité et congruence	23
I	Divisibilité	23
I.1	Définitions et critères de divisibilité	23
I.2	Division euclidienne	25
II	Congruence	27
II.1	Relation d'équivalence	27
II.2	Relation de congruence	29
II.3	Preuve des critères de divisibilité	30
II.4	Opérations et congruences	32
II.5	Classes d'équivalence	33
III	Réponses aux questions	35
IV	Exercices	36
3	Groupes - Anneaux - Corps	39
I	Groupes	39
I.1	Définitions, premières propriétés	39
I.2	Morphismes de groupes	43
I.3	Sous-groupes	45
I.4	Sous-groupes de $(\mathbb{Z}, +)$	46
II	Anneaux et Idéaux	48
II.1	Généralités	48
II.2	Règles de calcul	49

II.3	Éléments inversibles - Corps	51
II.4	Morphismes d'anneaux	52
II.5	Sous-anneaux et idéaux	53
II.6	Intersection et somme d'idéaux	55
II.7	Anneaux principaux	55
II.8	Anneaux quotients	59
III	Réponses aux questions	61
IV	Exercices	62
4	Arithmétique dans un anneau principal	63
I	Plus grand diviseur commun	64
I.1	Définition - Exemples	64
I.2	Relation de Bézout	67
I.3	Méthode de calcul : Algorithme d'Euclide	68
II	Éléments premiers entre eux	71
III	Plus petit multiple commun	74
IV	PGCD et PPCM de n éléments	76
V	Éléments irréductibles - Éléments premiers	77
V.1	Définitions	77
V.2	Comment trouver les nombres premiers ?	78
V.3	Éléments premiers	79
V.4	Décomposition en facteurs premiers	82
V.5	Polynômes irréductibles	83
V.6	Anneaux euclidiens et factoriels	85
VI	Réponses aux questions	89
VII	Exercices	90
5	Anneau $\mathbb{Z}/n\mathbb{Z}$	93
I	Éléments inversibles et diviseurs de zéros	94
II	Et si n est un nombre premier ?	98
III	Équations et systèmes d'équations	102
III.1	Équation $\mathbf{a}\mathbf{x} = \mathbf{b}$ dans $\mathbb{Z}/n\mathbb{Z}$	102
III.2	Théorème des restes chinois	104
IV	Décomposition de $\mathbb{Z}/n\mathbb{Z}$	106
V	Réponses aux questions	110
VI	Exercices	112

6	Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$	115
I	Groupes cycliques	116
I.1	Sous-groupe monogène	116
I.2	Ordre d'un élément d'un groupe	117
I.3	Éléments primitifs	120
II	Structure de $(\mathbb{Z}/p\mathbb{Z})^\times$	123
III	Structure de $(\mathbb{Z}/p^r\mathbb{Z})^\times$	124
IV	Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$	125
V	L'indicateur de Carmichael	127
VI	Réponses aux questions	133
VII	Exercices	134
7	Résidus quadratiques	137
I	Définition - Exemples	137
II	Résidus quadratiques dans $\mathbb{Z}/p\mathbb{Z}$	138
III	Symbole de Legendre	140
IV	Calcul des racines carrées dans $\mathbb{Z}/p\mathbb{Z}$	150
IV.1	Cas où p est congru à 3 modulo 4	151
IV.2	Cas où p est congru à 1 modulo 4	153
V	Carrés modulo un entier quelconque	155
VI	Nombre de racines carrées modulo n	159
VII	Entiers de Blum	164
VIII	Résidualité quadratique	167
IX	Réponses aux questions	168
X	Exercices	170
III	Cryptologie contemporaine	173
8	Schémas de Feistel - Standards de chiffrement par blocs	175
I	Schémas de Feistel	178
I.1	La construction	179
I.2	Le résultat essentiel	180
I.3	Avec une ou deux rondes seulement	182
I.4	La preuve	183
II	Data Encryption Standard (DES)	187
II.1	Construction	187
II.2	La polémique	191
III	Advanced Encryption Standard (AES)	193
III.1	AddRoundKey	193

III.2	SubBytes	194
III.3	ShiftRows	197
III.4	MixColumns	197
III.5	Fonctionnement	198
IV	Modes opératoires du chiffrement par bloc	198
IV.1	Le mode ECB (Electronic Codebook Mode)	199
IV.2	Le mode CBC (Cipher Block Chaining Mode)	199
IV.3	Le mode OFB (Output Feedback Mode)	199
IV.4	Le mode CFM (Cypher Feedback Mode)	200
V	Réponses aux questions	201
9	Cryptographie à clé publique	203
I	Définitions et principes généraux	205
I.1	Quelques notions de complexité	205
I.2	Fonctions à sens unique	208
I.3	Application	209
II	RSA	210
II.1	Cryptage	211
II.2	Décryptage	211
II.3	Sécurité	213
III	Chiffrement de Rabin	214
III.1	Cryptage	214
III.2	Décryptage	214
III.3	Sécurité	216
IV	Le cryptosystème ElGamal	216
IV.1	Cryptage	217
IV.2	Décryptage	217
IV.3	Sécurité	218
V	ElGamal généralisé	219
VI	Protocole d'échange de Clé de Diffie-Hellman	220
VI.1	Description	221
VI.2	Attaque	222
VII	Cryptographie multivariable	222
VIII	Tests de primalité	224
VIII.1	Test de pseudo-primalité	225
VIII.2	Test de Rabin-Miller	226
IX	Exercices	228

10 Signature - Identification	231
I Procédés de signature	231
II La signature RSA	233
III Généralisation	234
IV La signature ElGamal	235
IV.1 Description	235
IV.2 Sécurité	236
V DSS	237
VI Courbes elliptiques	238
VI.1 Coefficients réels	239
VI.2 Coefficients dans un corps fini	243
VII ECDSA	244
VIII Fonctions de hachage	245
VIII.1 Principes généraux	245
VIII.2 Le paradoxe des anniversaires	246
VIII.3 Une fonction résistante aux collisions	248
IX Procédés d'identification « à clé privée »	249
X Procédés d'identification « à clé publique »	250
XI Procédé d'identification de Guillou - Quisquater	251
XII Réponses aux questions	252
XIII Exercices	253
IV Correction des exercices	257
Bibliographie	295
Index	297