

# Table des matières

<b>Introduction</b>	<b>xiii</b>
<b>I Algèbre générale</b>	<b>1</b>
<b>1 Les groupes</b>	<b>3</b>
1.1 Définitions et premières conséquences . . . . .	3
1.1.1 Définitions . . . . .	3
1.1.2 Sous-groupe . . . . .	3
1.1.3 Groupe engendré . . . . .	4
1.1.4 Morphisme de groupe . . . . .	4
1.2 Rel. d'équivalence associées à un sous-groupe . . . . .	5
1.2.1 Définitions . . . . .	5
1.2.2 Application : le théorème de Lagrange . . . . .	6
1.3 Groupes monogènes - Groupes cycliques . . . . .	6
1.3.1 Définitions . . . . .	6
1.3.2 Quelques propriétés des groupes cycliques . . . . .	7
1.4 Groupes opérant sur un ensemble - Applications . . . . .	9
1.4.1 Définitions . . . . .	9
1.4.2 Applications . . . . .	10
1.5 Exposant d'un groupe commutatif fini . . . . .	10
1.5.1 Définition . . . . .	10
1.5.2 Cas où $G$ est commutatif - Applications . . . . .	10
1.6 Exercice . . . . .	12
<b>2 Les anneaux</b>	<b>17</b>
2.1 Introduction . . . . .	17
2.2 Calc. modulo un idéal bilatère dans un anneau . . . . .	18
2.2.1 Généralités . . . . .	18
2.2.2 Notion d'idéal maximal dans un anneau commutatif - Application . . . . .	19
2.3 L'anneau $\mathbb{Z}/n\mathbb{Z}$ . . . . .	20

2.3.1	Généralités . . . . .	20
2.3.2	Cas où $n$ est premier . . . . .	24
2.3.3	Caractérisation des anneaux $\mathbb{Z}/n\mathbb{Z}$ dont le groupe $G_n$ des inversibles est cyclique . . . . .	25
2.3.4	Les tests de primalité . . . . .	28
2.3.5	Indicateur de Carmichael . . . . .	38
2.4	Exercices . . . . .	40
<b>3</b>	<b>Les corps finis</b>	<b>43</b>
3.1	Les polynômes cyclotomiques sur un corps $\mathbb{K}$ . . . . .	43
3.2	Le corps à $p^r$ éléments avec $p$ premier et $r \in \mathbb{N}^*$ . . . . .	46
3.2.1	Généralités . . . . .	46
3.2.2	Etude d'un exemple : le corps des octets . . . . .	48
3.3	Compléments . . . . .	50
3.4	Problème . . . . .	53
3.4.1	Exposant d'un groupe commutatif fini - Applications	53
3.4.2	Polynômes sur un corps fini - Applications . . . . .	54
3.4.3	Le corps fini à $p^r$ éléments ( $p$ premier) - Exemples .	57
3.5	Solution . . . . .	58
3.5.1	Exposant d'un groupe commutatif fini . . . . .	58
3.5.2	Polynômes sur un corps fini - Applications . . . . .	61
3.5.3	Le corps fini à $p^r$ éléments ( $p$ premier, $r \geq 1$ ) . . . . .	65
<b>II</b>	<b>Applications à la cryptographie</b>	<b>69</b>
<b>4</b>	<b>Le R.S.A et le logarithme discret</b>	<b>71</b>
4.1	Définitions . . . . .	71
4.2	Le cryptosystème RSA . . . . .	72
4.3	Un cryptosystème hybride : Hill-RSA . . . . .	74
4.3.1	Des résultats mathématiques utiles dans ce crypto- système . . . . .	74
4.3.2	Création du cryptosystème hybride : Hill-R.S.A . . . . .	77
4.4	Le cryptosystème originel de Hill . . . . .	86
4.4.1	Détermination des $A \in M_2(\mathbb{Z}/N\mathbb{Z})$ telles que $A^2 = I_2$	86
4.4.2	Exemple . . . . .	87
4.5	Le chiffrement El-Gamal (logarithme discret) . . . . .	87
4.5.1	Le logarithme discret . . . . .	87
4.5.2	Le cryptosystème El-Gamal . . . . .	88
4.5.3	Généralisation du cryptosystème El-Gamal . . . . .	89
4.6	Algorithmes de Shanks et de Pohling . . . . .	91
4.6.1	Algorithme de Shanks . . . . .	91
4.6.2	Algorithme de Pohling . . . . .	92

<b>5</b>	<b>Le cryptosystème de Vanstone</b>	<b>95</b>
5.1	Rappels mathématiques . . . . .	95
5.2	Les courbes elliptiques sur un corps $\mathbb{K}$ . . . . .	96
5.2.1	Définition . . . . .	96
5.2.2	Loi de groupe sur une courbe elliptique . . . . .	100
5.2.3	Courbes elliptiques sur $\mathbb{F}_p$ , $p$ premier . . . . .	100
5.3	Le chiffrement de Vanstone . . . . .	103
5.3.1	Définition . . . . .	103
5.3.2	Exemples . . . . .	104
5.4	Algorithme elliptique de Lenstra . . . . .	105
5.4.1	Observations générales . . . . .	105
5.4.2	Présentation de l'algorithme de factorisation de Lenstra	107
5.4.3	Mise en forme pratique . . . . .	108
5.5	Conjecture de Sato-Tate . . . . .	109
<b>6</b>	<b>Chiffrement de Blum-Goldwasser</b>	<b>111</b>
6.1	Les P.R.B.G. . . . .	111
6.1.1	Introduction . . . . .	111
6.1.2	Les principaux PRBG . . . . .	111
6.2	Codage de Blum-Goldwasser . . . . .	118
<b>7</b>	<b>Codes linéaires et codes cycliques</b>	<b>125</b>
7.1	Généralités et définitions . . . . .	125
7.1.1	Définition . . . . .	125
7.1.2	Distance de Hamming . . . . .	125
7.1.3	Distance minimale d'un code linéaire . . . . .	126
7.1.4	Code $t$ -correcteur . . . . .	126
7.2	Matrice génératrice, Matrice de parité . . . . .	126
7.2.1	Définition . . . . .	127
7.2.2	Code dual . . . . .	127
7.2.3	Définition d'un code linéaire cyclique . . . . .	127
7.3	Étude algébrique des codes cycliques sur $\mathbb{K}^n$ . . . . .	128
7.4	Polynômes unitaires divisant $(X^n - 1)$ . . . . .	131
7.5	Matrices génératrice et de parité . . . . .	133
7.6	Code cyclique de Reed-Solomon . . . . .	136
7.6.1	Définition . . . . .	136
7.6.2	Exemple . . . . .	137
7.7	Codes cycliques - Résidus quadratiques . . . . .	138
7.7.1	Définition . . . . .	138
7.7.2	Etude d'un exemple : le code binaire de Golay de longueur 23 . . . . .	139

<b>8</b>	<b>Cryptosystèmes de Mac-Eliece et de Bose</b>	<b>141</b>
8.1	Définition du cryptosystème de Mac-Eliece . . . . .	141
8.1.1	Définition de la clé $K$ . . . . .	141
8.1.2	Codage et décodage . . . . .	142
8.2	Cryptosystème de Bose . . . . .	143
8.2.1	Définition d'un code de Bose . . . . .	143
8.2.2	Etude d'un exemple . . . . .	147
8.2.3	Algorithme de décodage pour un cryptosystème associé à un code de Bose . . . . .	148
8.3	Etude d'un exemple . . . . .	152
8.3.1	Décodage du mot $m'_1$ . . . . .	153
8.3.2	Décodage du mot $m'_2$ . . . . .	154
8.4	Problème : Codes linéaires et codes cycliques . . . . .	155
8.4.1	Etude algébrique des codes linéaires. Cas des codes cycliques. . . . .	155
8.4.2	Distance de Hamming d'un code linéaire . . . . .	158
8.4.3	Construction de certains codes cycliques . . . . .	159
8.5	Solution . . . . .	164
8.5.1	Etude algébrique des codes linéaires. Cas des codes cycliques . . . . .	164
8.5.2	Distance de Hamming d'un code linéaire . . . . .	169
8.5.3	Construction de certains codes cycliques . . . . .	171
<b>III</b>	<b>Applications à l'algorithmique</b>	<b>181</b>
<b>9</b>	<b>Un Algo. de factorisation des polynômes</b>	<b>183</b>
9.1	Rappels d'algèbre linéaire . . . . .	183
9.2	Décomp. de polynômes sans facteurs multiples . . . . .	188
9.2.1	Instance du problème . . . . .	188
9.2.2	Un théorème d'algèbre . . . . .	188
9.2.3	D'où l'algorithme de factorisation (algorithme de Berlekamp) . . . . .	190
9.2.4	Etude de deux exemples . . . . .	190
9.2.5	Applications . . . . .	193
<b>10</b>	<b>Pseudo-inverse d'une matrice</b>	<b>195</b>
10.1	Rappels d'algèbre et instance du problème . . . . .	195
10.1.1	Rappels d'algèbre . . . . .	195
10.1.2	Instance du problème . . . . .	196
10.1.3	Etude de l'application $a^+$ . . . . .	197
10.1.4	Point de vue matriciel . . . . .	199
10.2	Construction algorithmique de la matrice $A^+$ . . . . .	200

10.2.1	L'algorithme . . . . .	200
10.2.2	Mise en forme pratique et exemple . . . . .	202
<b>11</b>	<b>Transformée de Fourier discrète</b>	<b>203</b>
11.1	Définitions de la transformée de Fourier discrète . . . . .	203
11.1.1	Définition 1 . . . . .	203
11.1.2	Définition 2 . . . . .	204
11.2	Propriétés de la transformée discrète . . . . .	205
11.2.1	Valeurs propres de $U(\omega)$ . . . . .	205
11.2.2	Trace de $U(\omega)$ et applications au caractéristique de $U(\omega)$ . . . . .	206
11.3	Comparaison de deux transformées . . . . .	208
11.4	TdF discrète et convolution . . . . .	209
11.4.1	La convolution dans $\mathbb{C}^n$ . . . . .	209
11.4.2	Application : action de la transformée de Fourier sur une convolée . . . . .	210
11.5	Transformée de Fourier rapide . . . . .	213
11.5.1	Définition . . . . .	213
11.5.2	Coût d'une TDFR . . . . .	215
11.6	Un algorithme de calcul pour une TDFR . . . . .	216
11.6.1	L'algorithme . . . . .	216
11.6.2	Coût de l'algorithme . . . . .	218
11.7	Applications de la transformée discrète . . . . .	219
11.7.1	Quelques notions supplémentaires d'arithmétique mo- dulaire . . . . .	219
11.7.2	La transformation de Fourier dans $(\mathbb{Z}/m\mathbb{Z})^N$ . . . . .	220
11.7.3	Application à la multiplication des très grands nombres entiers . . . . .	222
11.8	Programme Maple . . . . .	226
<b>12</b>	<b>Prog. linéaire - Méthode du simplexe</b>	<b>229</b>
12.1	Trois formulations de la prog. linéaire . . . . .	229
12.2	La méthode du simplexe . . . . .	231
12.2.1	Instance du problème . . . . .	231
12.2.2	Les sommets d'un polyèdre . . . . .	231
12.2.3	Le théorème fondamental . . . . .	233
12.2.4	La méthode du simplexe . . . . .	234
12.2.5	Mise en place de l'algorithme et énoncé de celui-ci . . . . .	235
12.3	Exercices de programmation linéaire . . . . .	237

<b>13</b>	<b>Technique du <math>QR</math> - Méthode de Givens</b>	<b>239</b>
13.1	Quelques compléments mathématiques . . . . .	239
13.1.1	Matrices de Householder et matrices de Hessenberg supérieures . . . . .	239
13.1.2	Travail informatique n°1 . . . . .	241
13.2	La décomposition $QR$ d'une matrice . . . . .	242
13.2.1	Décomposition $A = QR$ d'une matrice inversible - Algorithme de construction . . . . .	242
13.2.2	Travail informatique n°2 . . . . .	244
13.3	Recherche des valeurs propres d'une matrice . . . . .	244
13.3.1	Préliminaires . . . . .	244
13.3.2	L'algorithme . . . . .	245
13.3.3	Travail informatique n°3 . . . . .	245
13.4	$A$ symétrique réelle - Méthode de Givens . . . . .	245
13.4.1	Quelques observations mathématiques . . . . .	245
13.4.2	Valeurs propres d'une matrice symétrique réelle : méthode de Givens . . . . .	246
13.4.3	Travail informatique n°4 . . . . .	247
13.5	Améliorations techniques . . . . .	248
13.5.1	Amélioration technique dans le cadre de la recherche des valeurs propres d'une matrice par la méthode du $QR$ itéré . . . . .	248
13.5.2	Cas où l'on cherche les valeurs propres de $A$ symé- trique par le $QR$ . . . . .	249
13.5.3	Exercice d'application . . . . .	249
<b>IV</b>	<b>Annexes</b>	<b>251</b>
<b>A</b>	<b>Merkle-Hellmann - Partage du secret</b>	<b>253</b>
A.1	Le cryptosystème de Merkle-Hellman . . . . .	253
A.1.1	La clé $K$ . . . . .	253
A.1.2	Codage et décodage . . . . .	253
A.2	Partage du secret selon Shamir . . . . .	254
A.2.1	Introduction . . . . .	254
A.2.2	Protocole de Shamir . . . . .	255
<b>B</b>	<b>Polynômes irréductibles dans <math>\mathbb{F}_p[X]</math></b>	<b>257</b>
B.1	La fonction de Möbius . . . . .	257
B.1.1	Définition . . . . .	257
B.1.2	Applications . . . . .	257
B.2	Polynômes irréductibles sur $\mathbb{F}_p$ . . . . .	259
B.2.1	Introduction . . . . .	259

B.2.2	Quelques lemmes . . . . .	259
B.3	Poly. sans facteurs irréductibles multiples . . . . .	261
<b>C</b>	<b>Signatures cryptographiques</b>	<b>263</b>
C.1	Introduction et instance du problème . . . . .	263
C.2	Etude de quelques exemples . . . . .	263
C.2.1	Exemple 1 : signature via le RSA . . . . .	263
C.2.2	Exemple 2 : la signature El-Gamal . . . . .	264
C.2.3	Exemple 3 : le standard de signature électronique . . . . .	264
C.3	Exercices . . . . .	265
C.4	Programmes MAPLE . . . . .	266
C.4.1	Signature El-Gamal classique . . . . .	266
C.4.2	Signature électronique DSS . . . . .	267
C.4.3	Signature électronique DSS avec nos propres procédures	268
<b>D</b>	<b>Miller-Rabin et Solovay-Strassen</b>	<b>271</b>
D.1	Compléments d'algèbre . . . . .	271
D.2	App. au test de Miller-Rabin . . . . .	272
D.3	Fiabilité du test de Solovay-Strassen . . . . .	276
<b>E</b>	<b>Surfaces et cryptographie</b>	<b>279</b>
E.1	Introduction . . . . .	279
E.2	Définitions . . . . .	279
E.2.1	Les notations . . . . .	279
E.2.2	Les définitions . . . . .	280
E.2.3	Un premier exemple . . . . .	283
E.2.4	Détermination de <i>card G</i> dans un cas particulier . . . . .	283
E.3	Chiffrement « à la El-Gamal » sur $E = \mathbb{K}^n$ . . . . .	284
E.3.1	Le codage . . . . .	285
E.3.2	Le décodage . . . . .	285
E.4	Mise en forme pratique . . . . .	285
	<b>Postface</b>	<b>289</b>