

Table des matières

I. Structures finies	
1. Rappels sur $\mathbf{Z}/n\mathbf{Z}$, $(\mathbf{Z}/n\mathbf{Z})^*$, \mathbf{F}_q , \mathbf{F}_q^*	1
2. Structure des groupes $(\mathbf{Z}/n\mathbf{Z})^*$ et \mathbf{F}_q^*	5
3. Symboles de Legendre et Jacobi	7
4. Sommes de Gauss	11
5. Applications au nombre de solutions d'équations	15
6. Exercices	23
II. Applications : Algorithmes, primalité et factorisation, codes	
1. Algorithmes de base	35
2. Cryptographie, RSA	38
3. Test de Primalité (I)	40
4. Test de Primalité (II)	46
5. Factorisation	51
6. Codes correcteurs	54
6.1. Généralités sur les codes correcteurs	55
6.2. Codes linéaires cycliques	59
7. Exercices	66
III. Algèbre et équations diophantiennes	
1. Sommes de carrés	76
2. Équation de Fermat ($n=3$ et 4)	81
3. Équation de Pell-Fermat $x^2 - dy^2 = 1$	86
4. Anneaux d'entiers algébriques	95
5. Géométrie des nombres	105
6. Exercices	113

IV. Théorie analytique des nombres	
1. Énoncés et estimations élémentaires	127
2. Fonctions holomorphes (résumé/rappels)	133
3. Séries de Dirichlet, fonction $\zeta(s)$	138
4. Caractères et théorème de Dirichlet	141
5. Le théorème des nombres premiers	149
6. Exercices	160
V. Courbes elliptiques	
1. Loi de groupe sur une cubique	171
2. Hauteurs	176
2.1. Hauteurs de Weil	176
2.2. Hauteurs de Néron-Tate	185
3. Le théorème de Mordell-Weil	188
4. Le théorème de Siegel	192
5. Courbes elliptiques sur les complexes	194
6. Courbes elliptiques sur un corps fini	199
7. Fonction L d'une courbe elliptique	201
VI. Développements et problèmes ouverts	
1. Nombre de solutions des équations sur les corps finis	207
2. Équations diophantiennes et géométrie algébrique	214
3. Nombres p -adiques	222
4. Nombres transcendants et approximation diophantienne	231
5. La conjecture a, b, c	242
6. Quelques séries de Dirichlet remarquables	249
A. Factorisation	
1. Factorisation de polynômes	261
2. Factorisation et courbes elliptiques	265
3. Factorisation et corps de nombres	268
B. Géométrie projective élémentaire	
1. L'espace projectif	273
2. Intersection	281
C. Théorie de Galois	
1. Théorie de Galois et corps de nombres	287
2. Extensions abéliennes	291
3. Représentations galoisiennes	295
Bibliographie	301
Notations	307
Index	311