Préface

Selon la formule de Pythagore « tout est arrangé selon le nombre », de sorte que faire des mathématiques, ou mathématiser les sciences comme la physique, la biologie ou la chimie, consiste à associer des nombres à tout objet d'étude, géométrique, topologique, évolution d'un système, statistique...
La première intuition d'un nombre est celle d'un *entier naturel* puisque ce sont les nombres qui servent à compter les objets. L'utilisation de la calculatrice nous donne une bonne vision des *nombres décimaux* qui sont des *nombres rationnels* particuliers, ceux dont les dénominateurs sont de la forme $2^a 5^b$. La parité d'un *entier relatif*, la périodicité des jours de la semaine nous introduisent à la notion de *nombres congruents*, que l'on utilise par exemple pour les phénomènes stellaires, éclipses, comètes...
La construction des *nombres réels* qui conduit à la branche des mathématiques qu'on appelle l'analyse, est quand à elle beaucoup plus difficile : une approche intuitive consiste à considérer ces nombres comme ayant un développement décimal infini. *Les nombres complexes* avec ses fameux *nombres imaginaires*, ont été introduits dès le XVI$^{\text{e}}$ siècle afin de résoudre les équations du second et troisième degré ; ils restent cependant en dehors du champ de connaissances du grand public. Il existe bien d'autres sortes de nombres, *des nombres surréels* aux *nombres algébriques* en passant par *les nombres p-adiques* et *les nombres transcendants*...
Quel est alors le point commun à toutes ces notions, qu'est ce qui nous autorise à parler de nombre ? Disons en première approximation que l'on a envie d'appeler nombre, tout élément d'un ensemble muni de deux lois, une addition et une multiplication avec la propriété de distributivité. Ainsi, partant du corps des nombres rationnels $\mathbb{Q}$:

- ▷ via la notion *algébrique* de corps de rupture, on construit des extensions algébriques $K/\mathbb{Q}$, comme par exemple $\mathbb{Q}[i]$,
- ▷ la notion de *suite de Cauchy* en analyse permet d'obtenir le corps des nombres réels $\mathbb{R}$ et celui des nombres p-adiques $\mathbb{Q}_p$.

La notion de nombre entier $\mathbb{Z} \subset \mathbb{Q}$ garde un sens dans une extension algébrique $K/\mathbb{Q}$, on parle alors d'entiers algébriques. Dans $\mathbb{Q}_p$, on peut aussi définir un sous-ensemble $\mathbb{Z}_p$ des entiers p-adiques. Ensuite, pour un anneau d'entiers noté A et pour $\mathcal{P}$ un idéal maximal de A, le quotient $A/\mathcal{P}$ est alors aussi un corps, fini dans les cas considérés.
Un autre moyen pour construire des corps est d'utiliser la théorie de Galois. Celle-ci associe à toute extension de corps E/K dite galoisienne, un

groupe dit de Galois. Le théorème de Galois fournit alors une bijection entre d'un côté les sous-groupes du groupe de Galois et de l'autre les extensions intermédiaires $K \subset F \subset E$.
Le but de ce livre est d'introduire le lecteur à tous ces nombres et d'en donner des applications

- ▷ concrètes avec par exemple des problèmes d'horlogerie avec les suites de Brocot, ou sur la théorie de l'information avec la cryptographie et les codes correcteurs,
- ▷ et d'autres de nature plus mathématiques autour des nombres premiers, des équations diophantiennes et la théorie de Galois.

Parmi les fils rouges du livre, les formes quadratiques reviennent tout au long du texte, avec par exemple :

- ▷ des questions autour des carrés du §I-4,
- ▷ les nombres premiers représentés par une forme quadratique §II-2 et les algorithmes de factorisation du §II-4.10,
- ▷ le groupe de classes d'idéaux d'un corps quadratique au §IV-3,
- ▷ les équations diophantiennes du chapitre IV avec par exemple l'équation de Pell-Fermat du §V-2.1, l'équation de Markoff et ses liens avec les questions d'approximation, cf. le théorème I-5.9.7.

Pour l'essentiel, notamment les chapitres I, II et V, le contenu de ce livre n'exige pas de connaissances particulières si ce n'est une intuition des entiers, et une certaine familiarité avec les notions de pgcd et de congruence. Pour le reste, il suffira de maîtriser les notions de base de théorie des groupes, d'algèbre linéaire et bilinéaire, notamment le vocabulaire sur les formes quadratiques.
Ce livre se veut un compagnon des amoureux de l'arithmétique, des premières notions du lycée sur la divisibilité des entiers, les congruences et la théorie de Galois jusqu'aux prémisses de la recherche avec le programme de Langlands.

La rédaction de ce livre a été l'occasion pour l'auteur de découvrir de nombreuses pépites dans d'autres ouvrages ou sur Internet, sources qu'il était en général difficile de citer précisément. L'auteur voudrait enfin mentionner le travail considérable de correction et de mise en page auquel se sont prêtés successivement Alain Debreil et Rached Mneimné.
Puisse le lecteur trouver à travers le texte qui lui est ici présenté autant de plaisir qu'a eu l'auteur en l'écrivant.

Antony, avril 2019

Table des matières

I. Arithmétique de $\mathbb{Z}$
1. Les entiers relatifs 4
1.1. Discrétion 4
1.2. Divisibilité 4
1.3. Sous-groupes de $\mathbb{Z}$ 6
1.4. Plus grand diviseur commun 8
1.5. Le groupe $\mathbb{Z}/n\mathbb{Z}$.– Congruences 11
1.6. L'anneau $\mathbb{Z}/n\mathbb{Z}$.– Petit théorème de Fermat 13
2. Quelques applications 16
2.1. Jouer à la marchande 16
2.2. Nombres pratiques 20
2.3. Fractions égyptiennes 24
2.4. Développement décimal de $1/p$, d'après J. Germoni 28
2.5. Contenu et lemme de Gauss 34
2.6. Polygones de Newton 35
3. Le joyau de l'arithmétique du XIX$^{\mathbf{e}}$ siècle 42
3.1. Énoncé de la loi de réciprocité quadratique 43
3.2. Résidus quadratiques : applications 47
3.3. Preuve d'Eisenstein 49
3.4. Zolotarev revisité par Duke-Hopkins 50
3.5. Déterminant de Vandermonde et corps finis 54
3.6. Preuve utilisant les résultants 55
3.7. Une équation diophantienne 56
3.8. Sommes de Gauss 58
4. Histoires de carrés 61
4.1. Théorème des deux carrés 61
4.2. Quaternions et théorème des quatre carrés 64
4.3. Théorème $(1, 2, 4, 8)$ de Hurwitz 67
4.4. Théorème de Pfister 70
4.5. Formes de Pfister et niveau d'un corps 73
5. Nombres réels 76

5.1. Quelques exemples de nombres irrationnels 76
5.2. Construction 80
5.3. Relation d'ordre total 82
5.4. Complétude 84
5.5. Borne supérieure et inférieure 86
5.6. Fractions continuées 87
5.7. Meilleures approximations 96
5.8. Nombres équivalents 100
5.9. Nombres de Markoff 103
6. Suites de Brocot 108
6.1. Fraction médiane ou l'addition des cancres 108
6.2. L'arbre de Stern-Brocot 111
6.3. Suite diatomique de Stern 116
6.4. Arbre de Calkin-Wilf 120
6.5. Suites de Farey et cercles de Ford 123
7. Vers l'infini et au delà 125
7.1. Ordinaux 126
7.2. Cardinaux 130
7.3. Ensembles dénombrables 133
7.4. Le jeu de Nim 135
7.5. Introduction à la théorie des jeux 136
7.6. Le corps des nombres surréels 145
7.7. Exemples de nombres surréels 150
7.8. Forme normale d'un nombre surréel 156
8. Introduction aux nombres p-adiques 160
8.1. Nombres décadiques 160
8.2. Définition algébrique 164
8.3. Définition analytique 166
8.4. Théorème d'Ostrowski 169
9. Exercices 171

II. Nombres premiers
1. Quelques propriétés sur l'ensemble des nombres premiers 181
1.1. Retour sur le théorème d'Euclide 181
1.2. L'ensemble $\mathcal{P}$ des nombres premiers n'est pas algébrique . 182
1.3. L'ensemble des nombres premiers est diophantien 184
1.4. Formules décrivant $\mathcal{P}$ 187
1.5. Exemples de familles infinies 189
1.6. Trous dans l'ensemble des nombres premiers 192
1.7. Nombres premiers inévitables 195
2. Premiers représentés par une forme quadratique 197
2.1. Descente à la Fermat et réciprocité 197
2.2. Généralisation de la descente 198

2.3. Formes quadratiques réduites 201
2.4. Composition des formes quadratiques 205
2.5. Résolution du cas général via le corps de classes de Hilbert 206
3. Tests de primalité 208
3.1. Nombres de Fermat 208
3.2. Nombres de Mersenne 210
3.3. Autour du petit théorème de Fermat 212
3.4. AKS 214
4. Factorisation 219
4.1. Nombre et taille des facteurs premiers 219
4.2. L'algorithme de Fermat 220
4.3. Méthode de Gauss 221
4.4. Algorithme $p-1$ de Pollard 221
4.5. Algorithme $p+1$ de Williams 221
4.6. Algorithme ρ de Pollard 222
4.7. Méthode des factorielles 223
4.8. Crible linéaire de Dixon 224
4.9. Crible quadratique de Pomerance 225
4.10. Formes quadratiques et factorisation 226
4.11. Méthode de factorisation de Lenstra 230
4.12. Crible du corps de nombres 232
5. Introduction à la théorie analytique des nombres 233
5.1. Théorème de Tchébychev 233
5.2. La fonction zêta de Riemann 235
5.3. Preuve du théorème des nombres premiers 241
5.4. Séries de Dirichlet 244
5.5. Théorème de Dirichlet 248
5.6. Quelques conjectures en récente évolution 254
5.7. Une brève introduction au programme de Langlands 256
6. Exercices 259

III. Corps et théorie de Galois
1. Théorie des corps 264
1.1. Généralités sur les extensions 264
1.2. Extensions algébriques et transcendantes 266
1.3. Corps de rupture et corps de décomposition 270
2. Nombres algébriques ou transcendants 275
2.1. Mesure d'irrationalité 275
2.2. Nombres de Liouville 278
2.3. Transcendance de e 280
2.4. Transcendance de π 281
2.5. Quelques résultats sur la transcendance 283
2.6. Classification de Malher des nombres transcendants 284

3. Corps finis 286
3.1. Théorème de Wedderburn 286
3.2. Propriétés générales 289
3.3. Existence et unicité des corps finis : preuves constructives . 290
3.4. Factorisation des polynômes de $\mathbb{Q}[X]$ 294
4. Théorie de Galois 300
4.1. Introduction 300
4.2. Extensions séparables 301
4.3. Extensions normales et galoisiennes 305
4.4. Correspondance de Galois 309
4.5. Extensions composées 312
5. Exemples de calculs de groupes de Galois 314
5.1. Groupe de Galois du polynôme $X^n - a$ 314
5.2. Extensions résolubles 318
5.3. Extensions cyclotomiques 321
5.4. Retour sur $X^n - a$ 328
5.5. Le groupe de Galois comme sous-groupe de $\mathfrak{S}_n$ 332
5.6. Le théorème de Dedekind 336
5.7. Résolvantes 341
6. Localisation des racines d'un polynôme 343
6.1. Racines réelles : règle de Descartes et suites de Sturm . . . 344
6.2. Matrices compagnon et valeurs propres 348
6.3. Théorème de Cauchy and co 350
6.4. Théorème de Rouché et applications 351
6.5. Localisation des racines de P' 356
7. Corps de fonctions 360
7.1. L'extension $k(t)/k$ 360
7.2. Polynômes de Carlitz 362
7.3. Module de Carlitz 364
7.4. Extensions de Carlitz de $\mathbb{F}_p(T)$ 367
7.5. Loi de réciprocité quadratique 368
8. Compléments autour de la théorie de Galois 371
8.1. Extensions d'Artin-Schreier 371
8.2. Théorème d'Artin-Schreier 374
8.3. Lemme de Hensel 376
8.4. Théorème de Puiseux 380
8.5. Théorème d'irréductibilité de Hilbert 382
8.6. Problème de Galois inverse 391
9. Exercices 393

IV. Théorie des nombres

1. Entiers algébriques 406
   1.1. Théorème de Minkowski 406
   1.2. Normes, traces, discriminant 411
   1.3. Anneaux des entiers d'un corps de nombres 413
   1.4. Deux exemples 416
   1.5. Unités d'un corps de nombres 417
2. Idéaux d'un corps de nombres 422
   2.1. Anneaux de Dedekind 422
   2.2. Idéaux fractionnaires 423
   2.3. Groupes de classes d'idéaux 424
   2.4. Décomposition des idéaux premiers dans une extension . . 428
   2.5. Nombre de classes de $\mathbb{Q}[\sqrt[3]{17}]$ 431
   2.6. Application : une équation diophantienne 433
3. Corps quadratiques, ordres et formes quadratiques 435
   3.1. Entiers et ordres 435
   3.2. Idéaux et formes quadratiques 437
   3.3. Composition des formes quadratiques 442
   3.4. Formes réduites de discriminant $D > 0$ 445
   3.5. Étude de $\mathbb{Q}(\sqrt{-23})$ 448
4. Lois de réciprocité supérieures 449
   4.1. Loi de réciprocité cubique 450
   4.2. Loi de réciprocité quartique 454
   4.3. Loi de réciprocité abélienne : théorie du corps de classe . . 455
5. Exercices 461

V. Équations diophantiennes

1. Quelques techniques élémentaires 466
   1.1. Le cas linéaire 466
   1.2. Congruences 468
   1.3. Méthode géométrique 468
   1.4. Méthode de descente 469
   1.5. Problème de Waring 469
   1.6. Factorisation dans une extension 470
   1.7. Méthode de Strassmann 471
2. Équations possédant un nombre infini de solutions 472
   2.1. Équation de Pell-Fermat 472
   2.2. Équation de Markoff 474
   2.3. Équations d'Hurwitz 476
   2.4. Courbes elliptiques 479
   2.5. Équations de Thue 480
   2.6. Principe de Hasse 480
3. Équations diophantiennes exponentielles 484

3.1. Équation de Lebesgue 484
3.2. Équation de Ramanujan-Nagell 485
3.3. Équation de Fermat 486
3.4. Équation de Catalan 487
4. Équations diophantiennes sur $\mathbb{C}[X]$ 487
4.1. Grand théorème de Fermat 488
4.2. Théorème de Mason et ses corollaires 488
4.3. Problème de Waring 490
5. Équations diophantiennes sur les corps finis 491
5.1. Sommes de Gauss 491
5.2. Équations diophantiennes modulo p 493
5.3. Sommes de Jacobi 494
5.4. Généralisations à plus de deux variables 496
5.5. Fonction zêta 499
6. Exercices 502

VI. Cryptographie
1. Une brève histoire de la cryptographie 509
1.1. Scytale 509
1.2. Les codes de César 510
1.3. Code de Hill 512
1.4. Code de Vigenère 512
1.5. Enigma et VIC : deux codes du XX^{e} siècle 514
1.6. Notions élémentaires de complexité 519
2. Registres à décalage 521
2.1. Codes de Vernam 522
2.2. LFSR 522
2.3. Propriétés 524
2.9. Cryptanalyse 525
3. Chiffrement symétrique : AES 527
4. Chiffrement asymétrique : RSA 529
4.1. Présentation 529
4.2. Authentification et signature 530
4.3. Cryptanalyse 532
5. Logarithme discret 534
5.1. El Gamal 534
5.2. Signature 535
5.3. Sécurité 536
6. La méthode du sac à dos 538
7. Quelques protocoles 539
7.1. Fonctions de hachage 539
7.3. Mots de passe 543
7.4. Signature 543

7.5. Échange de clefs 547
7.6. Jouer à pile ou face au téléphone 549
7.7. Preuve sans transfert de connaissance 549
7.8. Transfert inconscient 550
8. Codes correcteurs 551
8.1. Mise en place 551
8.2. Codes linéaires 553
8.3. Codes linéaires cycliques 555
8.4. Codes BCH 557
9. Exercices 564

VII. Indications de solutions

Bibliographie **637**
Notations **639**
Index **643**