Table des matières

IV. Théorie des nombres

V. Équations diophantiennes

Avant-propos

Au delà du découpage en chapitres, ce livre se déroule en trois temps autour de l'étude

- ▷ tout d'abord de l'arithmétique classique sur les entiers relatifs, autour des nombres premiers et quelques-unes de leurs applications ;
- ▷ on introduit ensuite le lecteur à la théorie des corps, avec les nombres algébriques, les corps finis et la théorie de Galois ;
- ▷ on donne enfin des applications en étudiant les équations diophantiennes, la cryptographie et la théorie des codes correcteurs.

1) Le joyau de l'arithmétique ou le théorème d'or comme l'appelait Gauss est *la loi de réciprocité quadratique*, donnée dans le premier chapitre. Il existe plus de deux cent cinquante preuves différentes de ce résultat, et nous en présentons six, dont la plus ancienne est due à Gauss, une relativement récente reposant sur des idées de V.A. Lebesgue et deux autres illustrant parfaitement l'idée selon laquelle toute formule avec un signe doit permettre de démontrer la loi de réciprocité quadratique. Enfin, une autre preuve utilisant la théorie de Galois et les corps cyclotomiques sera donnée en section §III-5.6, laquelle conduira naturellement aux *lois de réciprocité supérieure*.

Dans le premier chapitre, on s'intéresse essentiellement aux nombres rationnels et à l'approximation des nombres réels par des rationnels.

- ▷ Au delà de la construction abstraite des nombres réels, une vision intuitive d'un nombre réel est donnée par son *développement décimal illimité*, qui consiste à répéter les opérations suivantes : enlever la partie entière et multiplier le résultat par 10.
- ▷ Une autre stratégie voisine et « plus efficace », consiste à enlever la partie entière et à prendre l'inverse du résultat : on arrive ainsi à la notion de *fractions continuées* du §I-5.6, qui permettent de construire les « meilleures approximations » d'un nombre réel par un nombre rationnel du §I-5.7. On présente sur ce thème le remarquable travail de Markoff avec la description explicite du *spectre de Lagrange* à l'aide des solutions de *l'équation diophantienne de Markoff* du chapitre IV.

▷ Une autre façon d'approcher les nombres réels, longtemps utilisée en horlogerie, est d'utiliser, suivant Brocot, *l'addition des cancres*

$$\frac{x}{y} \oplus \frac{x'}{y'} = \frac{x+x'}{y+y'}.$$

À l'aide de cette loi, on construit une numérotation étonnante des nombres rationnels via l'arbre de Stern-Brocot, qui révèle des curiosités mathématiques remarquables, cf. le §I-6.

Ce premier chapitre d'arithmétique est aussi l'occasion d'aborder des thématiques intrigantes sur, par exemple, *les fractions égyptiennes*, les *identités remarquables* autour des sommes de carrés avec les travaux d'Hurwitz et Pfister, les fameux *nombres p-adiques* ainsi que les surprenants *nombres surréels* de Conway.

Les nombres premiers apparaissent bien évidemment tout au long de ce livre avec par exemple la non-finitude de l'ensemble $\mathcal{P}$ des nombres premiers ou l'étude du développement décimal de $\frac{1}{p}$.

Dans le deuxième chapitre, nous avons rassemblé quelques faits spectaculaires sur l'ensemble $\mathcal{P}$: par exemple, il semble évident que $\mathcal{P}$ *n'est pas algébrique*, i.e. n'est pas décrit par un polynôme serait-ce en plusieurs variables ; en revanche, le lecteur sera certainement surpris que $\mathcal{P}$ soit *diophantien*, i.e. contrôlé par les valeurs positives d'un polynôme explicite, ou même qu'il existe des formules relativement simples donnant le n-ième nombre premier. Les liens entre $\mathcal{P}$ et les formes quadratiques sont aussi très intéressants, et nous en donnons quelques aspects au §II-2.

Les besoins cryptographiques de la technologie actuelle, avec par exemple *le cryptosystème RSA* cf. le §VI-4, stimulent la recherche mathématique autour des questions de primalité et de factorisation. En 2002, trois mathématiciens indiens ont proposé *un nouvel algorithme, appelé AKS* des trois initiales des noms de ses découvreurs (voir le §II-3.4), pour tester la primalité d'un entier *en temps polynomial* : le résultat est d'autant plus surprenant que l'algorithme est très simple, reposant sur le fait que n est premier si, et seulement si, la congruence

$$(X+a)^n \equiv X^n + a \mod n$$

est vérifiée pour un a premier avec n. Dans les faits, leur algorithme n'est pas utilisé et on lui préfère *le test probabiliste dit de Rabin-Miller*, que nous présentons au §II-3.3 et qui fournit des nombres n qui sont premiers à $99,9999\%$ de chance, où le nombre de 9 peut être aussi grand qu'on le souhaite, et cela de manière extrêmement rapide : avec les erreurs de transmission, une telle probabilité est largement suffisante pour les besoins.

Symétriquement, la sécurité de RSA repose sur l'impossibilité pratique de factoriser un entier n relativement grand, de quelques centaines de chiffres : au §II-4, on passe en revue quelques-uns des *meilleurs algorithmes de factorisation*.

Enfin, on conclut notre promenade dans l'arithmétique dite classique, par un très rapide aperçu de la théorie analytique des nombres, avec *le théorème des nombres premiers* et le théorème de *progression arithmétique de Dirichlet*.

2) On aborde ensuite la théorie des nombres en commençant par introduire le vocabulaire autour des extensions de corps, algébriques ou transcendantes, corps de rupture et de décomposition. On donne ensuite quelques exemples de *nombres transcendants*, avec bien entendu celui de π qui clôt par la négative la fameuse *quadrature du cercle*. *Les corps finis* sont présentés au §III-3 sous le point de vue constructif, i.e. en justifiant l'existence d'un polynôme irréductible de degré n à coefficients dans $\mathbb{F}_p$. La factorisation modulo p d'un polynôme unitaire de $\mathbb{Z}[X]$ abordée au §III-3.4 sera utilisée intensivement via le théorème de Dedekind III-5.6.4, pour le calcul des groupes de Galois.

La théorie de Galois est le cœur du chapitre ; elle consiste en « un pont » entre d'un côté des questions sur les extensions de corps et de l'autre la théorie des groupes. Dans ce livre, excepté au §III-7.1, nous nous restreindrons aux extensions finies, et donc aux groupes finis. L'énoncé et la preuve du théorème de Galois sont relativement simples et tout le sel consiste à essayer de calculer explicitement des groupes de Galois. Au §III-5, on donne deux familles de tels calculs, les extensions *cyclotomiques* et celles *de Kummer*. Ces dernières permettent en particulier de répondre à la question pour laquelle la théorie de Galois a été inventée, i.e. de répondre par la négative à la question de savoir si étant donnée une équation quelconque de degré $\geqslant 5$, il est possible d'écrire ses racines en utilisant les symboles $\pm, \times, \sqrt[n]{\cdot}$. Pour autant, le mathématicien ne rend pas les armes, et le lecteur trouvera au §III-6 des moyens de localiser les racines d'un polynôme de degré quelconque.

On fait ensuite, au §III-7, une incursion sur les corps de fonctions avec notamment *les polynômes de Carlitz*, qui fournissent une généralisation en caractéristique p des extensions cyclotomiques. Cette construction de Carlitz vers 1930, a connu depuis les travaux de Lubin-Tate et de Drinfeld vers 1970, des succès spectaculaires dans *le programme de Langlands*, dont un des objectifs est de comprendre les représentations des groupes de Galois $\mathrm{Gal}(F^{sep}/F)$, où F est un corps quelconque et F^{sep} sa clôture séparable ; voir la fin du §IV-4.3. On termine ce rapide tour d'horizon de la théorie de Galois par quelques applications importantes : le théorème

d'Artin-Schreier, qui détermine quels sont les corps F tels que $\bar{F}/F$ est finie, *le théorème d'irréductibilité de Hilbert*, dont une des applications est la construction d'extensions dont le groupe de Galois est $\mathfrak{S}_n$ et nous évoquons le problème de Galois inverse. Enfin, au §IV-4, on revient sur la notion de loi de réciprocité afin de généraliser celle d'Euler dans le cas quadratique.

Les §IV-1 et IV-2 sont une très courte introduction à *la théorie algébrique des nombres*. L'idée est de généraliser l'inclusion $\mathbb{Z} \subset \mathbb{Q}$ avec la distinction entre entiers et nombres. Le contexte général est celui des anneaux de Dedekind, où les idéaux se comportent « idéalement », d'où leur nom, au sens où ils prennent le relais des entiers dans la factorialité : je m'explique, en général, les anneaux d'entiers ne sont pas factoriels ce qui est un problème important, par exemple pour généraliser l'approche pour $n = 2$ de l'équation de Fermat, en revanche dans les anneaux de Dedekind, tout idéal s'écrit de manière unique comme un produit d'idéaux dits premiers. Le défaut de factorialité de l'anneau des entiers se mesure alors à l'aide *du groupe fini des classes d'idéaux*. Cette théorie a été utilisée par Kummer pour démontrer des cas nouveaux du théorème de Fermat, ceux où le groupe de classe de l'extension cyclotomique $\mathbb{Q}(\zeta_p)$ est premier avec p.

3) En première approximation, *une équation diophantienne* est un polynôme en plusieurs variables à coefficients dans $\mathbb{Z}$ dont on cherche les solutions dans $\mathbb{Z}$. D'un point de vue logique, il serait déraisonnable d'espérer disposer d'une théorie générale traitant du sujet, et l'on se contentera d'un corpus de techniques. Le sujet est vaste et très complexe et va bien au delà des outils introduits dans ce livre. Signalons que la fin du XX$^{\text{e}}$ siècle a connu enfin la résolution de la plus fameuse de ces équations, i.e. celle de Fermat par des techniques très élaborées et astucieuses. Dans notre présentation de ce sujet, nous avons mis l'accent sur quelques-unes des plus célèbres équations possédant une infinité de solutions (Pell-Fermat, Markoff, courbes elliptiques...) avec un détour vers $\mathbb{C}[X]$ et les corps finis.

On termine le livre sur un dernier chapitre consacré à *la cryptographie*. Après une introduction historique rapide, on étudie les registres à décalage, le chiffrement symétrique AES et le système à clefs publiques RSA. Plus que l'aspect mathématique théorique de ces cryptosystèmes, ce qui est réellement intéressant est leur mise en œuvre, que nous étudions à travers quelques protocoles. Enfin, nous abordons les codes correcteurs d'erreurs et plus particulièrement ceux liés aux corps finis, les codes BCH utilisés en particulier dans la lecture des CD.