Introduction à la théorie des nombres

avec une introduction de Catherine Goldstein

Bearbeitet von
G.H Hardy, E.M Wright, C Goldstein, F Sauvageot

1. Auflage 2007. Taschenbuch. 608 S. Paperback
ISBN 978 3 540 64332 6
Format (B x L): 15,5 x 23,5 cm

Introduction

Les charmes de la théorie des nombres ont été maintes fois décrits : « [elle est] remarquable », écrit au milieu du 19e siècle le mathématicien Henry J. S. Smith, « pour le nombre et l'importance de ses résultats, pour la précision et la rigueur de ses démonstrations, pour la variété de ses méthodes, pour les relations intimes qu'elle révèle parfois entre des vérités en apparence isolées et pour les nombreuses applications qu'elle est susceptible d'avoir à d'autres branches de l'analyse » [Smith, 1859, p. 38–39].

Subtil dosage entre l'éclat concret des exemples et la puissance des théories développées pour les établir et les connecter : l'équilibre est facilement rompu. Le chant délicieux des sirènes conduit tout droit à deux écueils redoutables, capables de broyer la bonne volonté des amateurs et de mettre à nu les faiblesses des pédagogues. Tantôt Scylla aux pieds difformes et aux multiples têtes, la théorie des nombres semble parfois éparpillée en une foule de théorèmes dont les relations restent indéchiffrables et l'intérêt propre aléatoire : les énoncés les plus inoffensifs sombrent dans la futilité, les plus difficiles (le grand théorème de Fermat en est l'archétype) dévorent tout cru le voyageur naïf. Tantôt Charybde terrible, au contraire, elle engloutit alors une vaste étendue de résultats, les malaxe violemment dans des bouillonnements théoriques et rejette un champ certes unifié, mais que l'ébullition technique a rendu peu compatible avec la navigation de plaisance.

C'est à ce double piège que tout livre de théorie des nombres depuis deux siècles au moins se trouve confronté. Pour ne mentionner qu'un exemple fameux, deux mathématiciens renommés, Louis Mordell et Serge Lang, écrivirent chacun dans les années soixante du 20e siècle un ouvrage sur les équations diophantiennes (une partie de la théorie des nombres consacrée aux solutions en nombres entiers ou rationnels de systèmes d'équations polynômiales). Chacun d'eux rédigea également un compte rendu sur le livre de l'autre[1]. Le livre de Lang propose une synthèse de résultats généraux, unis par et dans un language géométrique sophistiqué. Mordell de commenter : « La plus grande partie du livre est pratiquement illisible sauf si l'on est familier avec, entre autres, Bourbaki, le livre de l'auteur sur la géométrie al-

[1] Les deux comptes rendus ont été reproduits en appendice d'un ouvrage ultérieur de Lang sur le même sujet [Lang, 1983, p. 349–358] ; le débat est relancé dans *Notices of the American Mathematical Society*, Mars 1995, p. 339–350.

gébrique et les variétés abéliennes, et les *Foundations of Algebraic Geometry* de Weil [...]. [Un lecteur peu familier avec cette littérature] sera bientôt désillusionné et confronté à un combat titanique. » Le choix de Mordell, quant à lui, est de consacrer chaque chapitre de son livre à une méthode (élémentaire) ou à un problème spécifique, portant le plus souvent sur une classe particulière d'équations. Et Lang de répliquer ainsi : « Les contenus du livre sont décousus [...]. [Mordell] rassemble des cas spéciaux sans ordre unificateur particulier ni aucun plan que je puisse détecter. [...] Le lecteur inexpérimenté devra comprendre seul qu'une seule formulation du théorème de Roth dans les corps de nombres pourra être utilisée efficacement pour [toute une série d']applications. »

Cinq éditions depuis 1938, sans compter les nombreuses réimpressions : il est clair que Godfrey Hardy et Edward Wright ont navigué avec assurance entre les écueils. C'est moins ici le succès qui impressionne (il existe d'autres best-sellers mathématiques) que sa persistance, en dépit des radicales réorganisations du domaine au cours du siècle écoulé : les comptes rendus des éditions successives témoignent à chaque génération que le charme du livre opère encore. Il résulte, il me semble, d'une part de la nature même du projet, d'autre part d'une exquise mise en œuvre ; toutes deux méritent d'autant plus d'attention qu'elles indiquent des modes de lecture adaptés au livre.

Les auteurs ont pris parti (et en cela ils appartiennent à une tradition plus proche de celle de Mordell que de celle de Lang) pour l'élémentaire et pour la variété. Au lieu d'adopter une théorie centrale ou un point de vue unique, ils ont choisi d'offrir ce qui paraît à la lecture de la table des matières et de leur préface comme une série d'introductions : à la répartition des nombres premiers, aux problèmes d'irrationalité et de transcendance, aux congruences, à la représentation des entiers comme sommes de puissances, aux corps quadratiques, à la géométrie des nombres. Ces thèmes sont classiques et, comme le remarquent les auteurs eux-mêmes, ils n'épuisent pas le domaine. Certaines matières qui iraient presque de soi pour une introduction actuelle manquent complètement : par exemple, l'interprétation géométrique des équations diophantiennes, à laquelle il a été fait allusion plus haut, ou encore les nombres p-adiques, deux ingrédients cruciaux dans la démonstration récente du Grand Théorème de Fermat.

Ce n'est pas dans l'exhaustivité ni dans l'unification méthodique ou thématique qu'il faut chercher la qualité essentielle de ce livre : c'est à une plus petite échelle, dans la sélection originale et le traitement exemplaire des sujets exposés. Si les titres des chapitres semblent conventionnels, leur contenu ne l'est pas : on y trouve des sections inattendues dans une introduction générale, sur les sommes de Gauß et leurs variantes, sur les partitions et les identités formelles, ou sur les tests de primalité, une question longtemps marginale, mais que la théorie du codage a remis au premier plan de la recherche dans les deux dernières décennies. Alors que l'échelle de grandeur des résultats bénéficiant des honneurs de la presse semble maintenant avoisiner la centaine

(centaines de pages pour la rédaction d'une preuve, centaines d'heures de calcul sur ordinateur), Hardy et Wright proposent une foule de théorèmes saisissants dont on peut lire la discussion et la démonstration de manière autonome en quelques pages et dont la variété rend un vibrant hommage à la multiplicité des facettes de la théorie des nombres et de ses applications : on y trouve ainsi une preuve de la transcendance de e et de π (§ 11.13 et § 11.14), l'évaluation de l'ordre moyen de la fonction arithmétique d ($d(n)$ comptant le nombre de diviseurs de l'entier n) (§ 18.2), la construction d'un polygone régulier à 17 côtés inscrit dans un cercle (§ 5.8), une étude, pour tout entier r, des nombres représentables par une somme de deux cubes d'au moins r manières différentes[2] (§ 21.11) et la caractérisation des trajectoires possibles d'un rayon de lumière se réfléchissant répétitivement sur les parois en miroir d'un carré (§ 23.3).

Les auteurs, tous deux de grands stylistes en mathématiques, assument de manière profonde leur choix de l'élémentarité. « Elémentaire » ne signifie pas « d'emblée familier » : à certains endroits, la tâche des lecteurs formés dans la deuxième moitié du 20^{e} siècle[3] serait sans doute facilitée par quelques formulations plus structurales ou un usage moins bridé des fonctions analytiques complexes. « Elémentaire » signifie ici que, partant de connaissances réduites (celles d'un premier cycle scientifique et même beaucoup moins pour la plupart des sections), Hardy et Wright *fabriquent* de la familiarité, une familiarité active qui permet à la lectrice ainsi guidée de construire des exemples numériques si nécessaire, de comprendre pourquoi ses questions spontanées doivent être reformulées, de discerner parmi elles les questions triviales, celles pour un temps encore inaccessibles et celles qui fourniront matière à des résultats intéressants — le premier chapitre sur les nombres premiers illustre parfaitement cette démarche. Les auteurs mettent en lumière comment une intuition première, banale, d'un problème, doit parfois être défaite et reconstruite pour le résoudre. Ils ne cherchent nullement à présenter les choses évidentes de manière rigoureuse, mais écrivent avec une attention profonde aux détails, à ceux qui risquent de déconcerter le débutant tout autant qu'à ceux qui sont révélateurs de phénomènes importants. La précision naît d'une observation alerte, observation des exemples numériques, mais aussi du raisonnement, des résultats déjà établis.

La rédaction évite ainsi la compacité formelle, tout en privilégiant l'économie intellectuelle : la première tentative pour décrire ce qu'est la théorie des nombres n'intervient qu'au chapitre IV, lorsqu'il s'agit de discuter ce qu'elle peut apporter pour l'étude d'un objet (les nombres irrationnels généraux)

[2] Ce problème est connecté à l'anecdote célèbre du « taxi de Ramanujan » : à Hardy se plaignant de ce que 1729, le numéro du taxi qu'il avait emprunté pour lui rendre visite à l'hôpital, n'avait aucune propriété intéresssante, Ramanujan répondit du tac au tac qu'il était le plus petit entier somme de deux cubes de deux façons différentes, voir [Hardy, 1985, p. 112].

[3] Mais peut-être moins celle des lecteurs formés dans la dernière décennie !

hors de sa première juridiction naturelle. Quelques aphorismes bien sentis viennent à point éclairer la signification d'un énoncé un peu technique :« [ce théorème (§ 23.6) énonce à peu près que] ce qui n'est pas impossible se produira quelquefois aussi improbable que cela puisse être ». Certains théorèmes importants sont prouvés de plusieurs manières, chacune conduite avec le minimum de fioritures, mais le maximum d'informations nécessaires, chacune éclairant un cadre possible pour le problème, et témoignant toutes ensemble des embranchements multiples de la théorie des nombres : l'énoncé que « tout nombre entier naturel n est somme de quatre carrés » (§ 20.5 à § 20.12) est ainsi prouvé une première fois par descente, en établissant le théorème pour un multiple du nombre et en montrant comment diminuer ce multiple, une deuxième fois à l'aide de l'arithmétique des quaternions, une troisième fois à l'aide d'identités entre séries formelles (où se profile en filigrane la théorie des fonctions elliptiques). De même pour le théorème de Kronecker sur les approximations rationnelles au chapitre XXIII. Un exemple plus élémentaire encore, la comparaison des mérites de deux preuves presque identiques de l'irrationalité de $\sqrt{2}$ (§ 4.3), résume parfaitement comment les auteurs privilégient la réflexion de leurs lecteurs : Hardy et Wright soulignent que, malgré leurs analogies, l'une des preuves semble logiquement un peu plus simple que l'autre, mais qu'elle se prête aussi moins facilement à la généralisation, parce qu'elle utilise la propriété que si un nombre premier divise un produit de deux nombres, il divise nécessairement l'un des deux nombres.

Destiné aux professionnels, actuels et futurs, c'est-à-dire aux vrais amateurs, le livre de Hardy et Wright n'est donc ni un manuel, ni une somme, mais cette rareté à un tel niveau technique : un livre de vraies mathématiques en action. Tous les sujets abordés restent à un titre ou un autre de pleine actualité. Si beaucoup de nouveaux résultats ont été obtenus depuis 1989 (la date de la dernière mise à jour par E. Wright), il serait illusoire d'indiquer l'état actuel de la recherche pour chacun d'eux : dans un domaine en expansion constante, les avancées sont presque quotidiennes[4]. Pour prendre trois exemples aussi différents que possible, la démonstration du Grand Théorème de Fermat a été bien sûr achevée en 1995 par Andrew Wiles, comme conséquence d'une partie d'une conjecture dite « de modularité », au croisement de la théorie des courbes elliptiques, des formes modulaires et des représentations galoisiennes[5] ; le problème de Képler concernant l'empilement optimal des sphères a été résolu par Thomas Hayes en 1998, à l'aide d'une réduction

[4] Ceci concerne aussi les notices historiques, voir ainsi [Vitrac 1998] pour une mise à jour de nos informations sur les problèmes d'irrationalité en Grèce antique discutés par Hardy et Wright en (4.5).

[5] Voir [Hellegouarch 1997] pour une présentation de quelques idées de base de la preuve et les références des articles de Wiles et des autres mathématiciens qui ont contribué de manière décisive à ces recherches. La conjecture de modularité est elle-même complètement démontrée depuis 1999.

à un problème d'optimisation non linéaire et de beaucoup d'informatique[6] ; quant au plus grand nombre premier actuellement connu, depuis le 14 novembre 2001, il s'agit du 39e nombre de Mersenne, $2^{13\,466\,917} - 1$, qui contient 4 053 946 chiffres[7]. D'autres problèmes, en revanche, comme la conjecture de Goldbach ou la nature arithmétique de π^e restent actuellement (fin 2001) ouverts.

Comme le signalent ces exemples, de nombreux terrains d'investigation attendent les lecteurs aventureux. Si leur exploration peut nécessiter l'assimilation d'autres techniques plus délicates, je crois que le principal obstacle est plutôt de s'orienter au sortir des multiples randonnées que le livre propose : la seconde partie de cette introduction vise donc à situer dans le développement de la théorie des nombres moderne les principaux thèmes abordés par Hardy et Wright, à l'aide de quelques instantanés historiques.

« [Hardy et Wright] ont étendu leurs filets loin et largement en collectant des matériaux intéressants et leur pêche est fort jolie en vérité, écrivait Mordell dans un compte rendu du livre en 1939. Il est réellement surprenant de voir quel immense magasin ils ont rempli. Il y a une variété suffisante pour statisfaire le goût le plus orthodoxe et pour pourvoir aux exigences du lecteur dans toutes ses humeurs. Il peut parcourir le livre d'une couverture à l'autre, ou étudier un chapitre ici ou là, ou plonger à tel ou tel moment pour un plaisant morceau. Dans ses heures légères il peut se tourner vers le jeu de Nim, en des occasions plus austères il peut étudier la question des algorithmes euclidiens dans les corps algébriques ou les inégalités de Rogers-Ramanujan dans la théorie des partitions. »

Que dire de plus ? Bonne dégustation.

Les cartes du paysage mathématique se démodent plus vite que les théorèmes. Dans les journaux recensant l'ensemble des articles écrits chaque année, comme les *Mathematical Reviews*, les changements dans les classifications en témoignent éloquemment. Certains thèmes, certaines techniques, deviennent l'objet d'une section autonome, des branches fusionnent, de nouvelles priorités incitent à mettre en valeur des aspects particuliers du domaine au détriment provisoire d'autres aspects. S'il n'est pas question de synthétiser en quelques pages l'histoire de ces transformations pour la théorie des nombres des deux derniers siècles, je voudrais fournir ici quelques points de repère afin de situer le contenu du livre de Hardy et Wright dans l'évolution du domaine, à l'aide de trois photographies prises respectivement au début du 19e siècle, du 20e et du 21e. Comme on le verra, Hardy et Wright ont évité à

[6] Voir le très intéressant site de Hayes lui-même avec les articles de base, `http://www.math.lsa.umich.edu/~hales/countdown/`.

[7] Voir `http://www.mersenne.org`.

peu près sytématiquement les grands axes dans les zones bien défrichées : les restituer, même à grands traits, pourra aider les lecteurs dans leurs parcours futurs.

Deux grands traités de théorie des nombres sont disponibles au début du 19^{e} siècle : les éditions successives de l'*Essai sur la théorie des nombres* d'Adrien-Marie Legendre[8] et les *Disquisitiones Arithmeticae* que Carl-Friedrich Gauß publie en 1801, à l'âge de 24 ans. Le premier ouvrage est un bilan des résultats obtenus dès le 18^{e} siècle par Leonhard Euler, Joseph Lagrange, l'auteur lui-même : il traite des nombres premiers, de partitions, de la résolution en nombres entiers d'équations de degré 1 et 2 et de divers problèmes diophantiens ; il énonce aussi la loi de réciprocité quadratique sur laquelle je reviendrai. Le deuxième traité a un matériel plus restreint (l'analyse diophantienne en est par exemple absente), mais ses notations et notions nouvelles (dont celle de congruences), son unité systématique, l'approfondissement des thèmes qu'il explore, en particulier le souci dont il témoigne pour les preuves inébranlables et les fondements bien établis, définissent de nouveaux standards pour le siècle à venir, bien au-delà de la théorie des nombres proprement dite (il inspira ainsi beaucoup les recherches d'Augustin Cauchy, de Niels Abel et d'Evariste Galois sur les groupes de transformations et les équations algébriques). Les *Disquisitiones* s'organisent autour de deux thèmes principaux : les congruences et la théorie des formes quadratiques, accompagnés d'applications variées. La plus spectaculaire de ces applications concerne la résolution d'un problème géométrique classique, l'inscription à la règle et au compas d'un polygone régulier à n côtés dans un cercle : Gauß détermine les critères sur n pour son existence à partir d'une étude arithmétique de l'équation vérifiée par les racines n-ièmes de l'unité.

Le livre de Hardy et Wright offre une construction du polygone à 17 côtés (§ 5.8), ainsi que les éléments de la théorie des congruences (chapitres V à VIII). Comme les auteurs le signalent dans la préface, en revanche, la théorie des formes quadratiques en tant que telle est à peu près absente. Il s'agit d'un des premiers sujets de théorie des nombres étudiés systématiquement à l'époque moderne et d'un terrain de recherches central au 19^{e} siècle et je voudrais donc en dire quelques mots.

Une forme est un polynôme homogène ; une forme quadratique binaire à coefficients entiers f (le cas principal traité par Gauß et avant lui par Lagrange) est ainsi donnée par $f(x, y) = ax^2 + 2bxy + cy^2$ (la normalisation change selon les auteurs). Une motivation pour leur étude, qui apparaît déjà dans des situations particulières au 17^{e} siècle chez Pierre de Fermat et Bernard Frenicle de Bessy, est de déterminer si un nombre entier n peut être représenté par une forme f donnée, c'est-à-dire s'il existe des valeurs entières x et y telles que $f(x, y) = n$; par exemple 5 est représentable par

[8] La première édition date de 1798 ; la troisième, de 1830, s'appelle simplement *Théorie des nombres* et intègre certains résultats des *Disquisitiones*, *cf.* [Legendre, 1830].

la forme $x^2 + y^2$, mais 7 ne l'est pas. Reprenant en partie Lagrange, Gauß a dégagé plusieurs étapes dans cette étude, chacune donnant ensuite lieu à des développements autonomes : les formes sont classées à équivalence près (deux formes étant équivalentes si elles se déduisent réciproquement l'une de l'autre par un changement de variables linéaire inversible à coefficients entiers) ; on cherche à caractériser les classes au moyen d'invariants (comme le discriminant $\Delta = b^2 - ac$), à trouver dans chaque classe d'équivalence des représentants simples et à expliciter tous les changements de variables qui y ramènent les autres formes de la classe. On est ainsi conduit à l'étude des transformations automorphes d'une forme, c'est-à-dire des changements de variables qui laissent inchangée une forme donnée, une étude elle-même connectée avec celle de l'équation dite de Pell-Fermat $x^2 - \Delta y^2 = 1$ et, dans le cas des formes de discriminant positif, avec celle du développement en fraction continue des racines ω de $a\omega^2 + 2b\omega + c = 0$. Un nombre représenté par une forme l'est bien sûr par toutes celles de sa classe ; Gauß améliora sa classification en répartissant les classes de formes en genres, les classes représentant un même nombre appartenant au même genre. Il donna aussi des informations sur les bornes des valeurs minimales prises par une forme de discriminant donné. Enfin, le nombre de classes de formes quadratiques binaires à coefficients entiers de même discriminant est fini : sa détermination suscita aussi d'importants travaux.

L'édifice construit par Gauß fut complété et étendu par de nombreux mathématiciens qui étudièrent également des formes quadratiques de plus de deux variables, certains cas de plus haut degré ou des formes dont les coefficients ne sont plus des entiers. L'examen des transformations automorphes, par exemple, mit en lumière des liens intéressants de la théorie des nombres avec la théorie des groupes, l'analyse, les géométries non-euclidiennes. Il est significatif qu'à la fin du siècle, le *Jahrbuch über die Fortschritte der Mathematik*, qui recensait alors tous les articles parus, ne distinguait à côté d'une section générale de théorie des nombres que deux rubriques particulières, l'une consacrée à la théorie générale des formes, l'autre aux fractions continues. Outre leur utilisation dans l'étude des transformations automorphes, ces dernières constituaient à l'époque un des rares outils disponibles, applicables tout aussi bien aux tests de primalité qu'à des problèmes d'approximation rationnelle ; une bonne introduction est fournie au chapitre X du livre de Hardy et Wright. Si la théorie des formes en général n'est pas décrite, la représentation des entiers par des formes particulières pour lesquelles ont été développées des approches spécifiques (somme de carrés, problème de Waring) est en revanche discutée dans les chapitres XX et XXI.

Pour mon deuxième instantané, au début du 20$^{\text{e}}$ siècle, j'ai choisi de fixer l'objectif sur une synthèse commode, l'*Encyclopédie des sciences mathématiques et de leurs applications*, une vaste entreprise adaptée de l'allemand et destinée aux utilisateurs professionnels des mathématiques. Quatre chapitres du volume consacré à la théorie des nombres sont parus avant la première

guerre mondiale[9] : le premier, élémentaire, contient l'habituel mélange de congruences, de quelques tests de primalité et d'équations diophantiennes variées. Le deuxième chapitre est comme on s'y attend consacré à la théorie des formes, avec une innovation importante : diverses interprétations géométriques et en particulier quelques résultats issus de la géométrie des nombres qu'Hermann Minkowski avait commencé d'ériger.

À la forme quadratique binaire f définie par $f(x,y) = ax^2+2bxy+cy^2$ $(= (\sqrt{a}x + b/\sqrt{a}y)^2 + (\sqrt{(c-b^2/a)}y)^2)$, avec $\Delta = b^2 - ac < 0$, on peut associer le réseau plan de points dont le parallélogramme fondamental a pour sommets $(0,0)$, $(\sqrt{a},0)$, $(b/\sqrt{a}, \sqrt{-\Delta}/\sqrt{a})$; les valeurs aux entiers de la forme correspondent alors aux carrés des distances de points du réseau à l'origine. Un cercle centré à l'origine, de surface πr^2, contient un point du réseau autre que l'origine dès que $\pi r^2 > 4\sqrt{-\Delta}$, d'où une borne pour le minimum des valeurs de le forme. Cette démarche se généralise à plusieurs dimensions et à des figures géométriques autres que le cercle ; en jouant sur ces figures, les réseaux et les distances associées, Minkowski améliora les bornes connues auparavant pour les minima de formes quadratiques et obtint aussi des résultats sur l'approximation des nombres par des rationnels. Le livre de Hardy et Wright consacre à la géométrie des nombres une partie du chapitre III et surtout son dernier chapitre où sont fournies plusieurs jolies applications.

Deux nouvelles directions de recherches sont mises en valeur dans les deux autres chapitres de l'*Encyclopédie* : d'une part la théorie des corps de nombres et d'autre part l'utilisation d'approches analytiques en théorie des nombres.

La première est issue en partie de tentatives pour généraliser la loi de réciprocité quadratique déjà évoquée (*cf.* § 6.12). Celle-ci établit des relations entre les résidus quadratiques (c'est-à-dire les nombres congrus à des carrés) modulo des nombres premiers distincts ; elle affirme par exemple que, pour p et q deux nombres premiers impairs qui ne sont pas tous deux de la forme $4n+3$, p est un résidu quadratique modulo q (c'est-à-dire est égal à un carré à un multiple de q près) si, et seulement si, q est un résidu quadratique modulo p. Legendre considérait « la loi de réciprocité entre deux nombres premiers [comme] la proposition la plus remarquable et la plus féconde de la théorie des nombres » ([Legendre, 1830, p. 238]). Cet enthousiasme fut partagé par la plupart des théoriciens des nombres ; comme l'écrit encore le mathématicien Helmut Hasse en 1950 : « Gauß a appelé à bon droit cette loi le *Theorema fundamentale theoriae residuorum quadraticorum* [dans les *Disquisitiones* ; dans son journal, Gauß qualifie aussi ce résultat de *theorema aureum*]. Il est devenu au cours des 150 années écoulées le théorème central de la nouvelle théorie des nombres, grâce à ses relations multiples formelles et conceptuelles avec toutes les questions et toutes les théories arithmétiques

[9] La guerre a arrêté la publication française. Par rapport à l'édition allemande il ne manque pour la théorie des nombres qu'un chapitre consacré à la théorie de la multiplication complexe, un sujet de toute façon plus technique et qui n'est pas traité dans le livre de Hardy et Wright.

possibles, ainsi que grâce à ses généralisations dans la théorie des nombres algébriques » ([Hasse, 1950, p. 90]).

La discussion de la loi de réciprocité quadratique est simplifiée par l'introduction du symbole de Legendre $\left(\frac{\cdot}{p}\right)$ (*cf.* § 6.5) qui vaut 1 sur les résidus quadratiques non nuls et -1 sur les non-résidus, autrement dit prend pour valeurs les deux racines carrées de 1. Ce sont les racines de l'unité d'ordre supérieur à 2 qui interviennent naturellement pour l'étude de congruences de degrés supérieurs à 2 ; or, ce ne sont plus des entiers ordinaires. Ceci suggéra à Gauß que pour formuler élégamment et prouver une loi de réciprocité biquadratique (c'est-à-dire relative non plus aux carrés, mais aux puissances quatrièmes), il fallait étendre le domaine de l'arithmétique aux nombres complexes de la forme $a+bi$, où a et b sont des entiers usuels et i, comme d'habitude, une racine quatrième primitive de l'unité. Gauß montra en 1831 comment travailler arithmétiquement avec ces nombres (qu'on appelle maintenant les entiers de Gauß), c'est-à-dire comment définir pour eux une factorisation en éléments premiers et un algorithme d'Euclide : c'est ce que Hardy et Wright expliquent en détail au chapitre XII, ainsi que l'arithmétique sur les nombres formés à partir de racines cubiques de 1 (qui servirent pour une loi de réciprocité cubique).

Toutefois, vers 1840-1850, il devint clair que des obstacles sérieux bloquaient cette route vers une loi plus générale : l'algorithme d'Euclide se trouvait vite en défaut pour les nombres formés à partir d'autres racines de l'unité, du type $a_0 + a_1\zeta + \cdots + a_{n-2}\zeta^{n-2}$, où les coefficients a_i sont entiers et ζ est une racine n-ième de l'unité (on appelle maintenant ces nombres des « nombres cyclotomiques »). Ernst Eduard Kummer découvrit (avec une certaine consternation !) que, pour les nombres cyclotomiques associés à $n = 23$ par exemple, il n'est pas possible d'obtenir une factorisation unique en éléments irréductibles, sans même parler d'algorithme d'Euclide. Son idée neuve et fondamentale fut de récupérer cette décomposition unique à l'aide de « facteurs premiers idéaux ». Leur description est trop compliquée pour être donnée ici (voir [Edwards, 1980]), mais entre 1847 et 1859, Kummer publia un bon nombre d'articles détaillant les différents aspects de sa théorie et surtout de spectaculaires applications. Il obtint par exemple le Grand Théorème de Fermat pour tous les exposants inférieurs à 100 sauf trois valeurs (on ne connaissait alors le résultat que pour une poignée de cas), en décomposant $x^n + y^n$ en un produit de nombres cyclotomiques et en utilisant l'arithmétique « idéale » correspondante.

Des problèmes analogues se posaient pour d'autres sortes de nombres complexes algébriques, c'est-à-dire racines de polynômes à coefficients entiers : de l'identité $3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5})$ résulte par exemple qu'il n'y a pas non plus de factorisation unique en nombres premiers pour les nombres de la forme $a + b\sqrt{-5}$ (avec a et b des entiers usuels) (*cf.* aussi § 14.6), car 3, 7, $1+2\sqrt{-5}$, $1-2\sqrt{-5}$, sont tous irréductibles. Plusieurs propositions ont été faites à la fin du 19$^{\text{e}}$ siècle pour définir correctement une arithmétique

entière sur de tels nombres. Celle de Richard Dedekind, qui est axiomatique et ensembliste, a eu une influence considérable au-delà même de la théorie des nombres *stricto sensu*. Dedekind introduisit la notion fondamentale de corps (de nombres), comme un ensemble de nombres complexes algébriques qui est stable sous les quatre opérations usuelles ; il y définit aussi des entiers (un entier algébrique est racine d'une équation polynomiale à coefficients entiers de coefficient dominant 1, en particulier un nombre comme $\frac{1+\sqrt{5}}{2}$ est un entier algébrique dans cette théorie, malgré l'apparent dénominateur 2). Les objets principaux de la théorie de Dedekind sont des idéaux, une terminologie qui rend hommage à Kummer, mais qui désigne maintenant un sous-ensemble d'entiers algébriques du corps considéré, stable par addition, soustraction et multiplication par tous les entiers du corps. C'est au niveau des idéaux et non des entiers eux-mêmes que l'arithmétique peut être développée : tout idéal s'écrit de manière unique comme un produit d'idéaux premiers — la multiplication des idéaux ou la notion d'idéal premier devant bien sûr être préalablement définies. Les notions d'idéal, d'anneau, de corps, ont donc été élaborées d'abord dans ce cadre particulier avec d'être exportées avec le succès qu'on connait dans l'ensemble des mathématiques au cours du 20$^{\text{e}}$ siècle. En 1897, David Hilbert, chargé d'un rapport sur la théorie des nombres pour la *Deutsche Mathematiker-Vereinigung*, la société mathématique allemande, le construisit autour de cette nouvelle théorie des corps de nombres. Il mit en évidence ses analogies profondes avec certaines théories géométriques et les liens étroits avec l'algèbre et l'analyse. Pour Hilbert, l'avénement de la théorie des corps de nombres était la preuve que la théorie des nombres arrivait enfin à maturité et il affirma que le domaine allait servir de modèle de rigueur et de construction architecturale à l'ensemble des mathématiques. C'est le rapport de Hilbert qui forme la base de l'exposé de l'*Encyclopédie* sur ce nouveau développement.

Les chapitres XIV et XV du livre de Hardy et Wright introduisent cette théorie dans le cas simple des corps quadratiques, mais l'accent y est mis plutôt sur les corps (rares, en fait, comme nous venons de le dire) où il est possible de définir un algorithme d'Euclide ou une factorisation unique au niveau des nombres eux-mêmes. Les idéaux sont définis succinctement par une approche géométrique fondée sur les réseaux plus intuitive pour les lecteurs de l'époque que la définition algébrique standard de nos jours ; l'intérêt récent pour les calculs explicites l'a d'ailleurs remise à l'honneur.

La suprématie accordée par Hilbert à la théorie des corps de nombres n'était pas acceptée par tous, même parmi ceux qui s'intéressaient à l'arithmétique. Pour d'autres au contraire, un des triomphes du domaine au 19$^{\text{e}}$ siècle était plutôt la théorie des nombres premiers et la manière dont l'introduction de l'analyse avait réussi à mettre de la régularité là où le plus grand désordre semblait régner. C'est la deuxième innovation évoquée plus haut.

En fait, dès 1737, Euler avait remarqué que la divergence au voisinage de 1 de la série $\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$ entraînait l'existence d'une infinité de nombres

premiers ; en effet pour $s > 1$, $\sum_{n\geq 1} \frac{1}{n^s} = \prod_p (1 - \frac{1}{p^s})^{-1}$ (la somme est prise sur tous les entiers, le produit sur tous les nombres premiers) et puisque le produit à droite diverge quand s tend vers 1, il doit avoir une infinité de termes. L'idée que des propriétés arithmétiques se traduisent par des propriétés analytiques, et réciproquement, fut reprise près d'un siècle plus tard par Peter Gustav Lejeune Dirichlet, dans des articles de 1837 et 1839. Il y introduisit certaines séries $L(\chi, s) = \sum_{n\geq 1} \frac{a_n}{n^s}$, dans lesquelles les coefficients a_n étaient définis arithmétiquement (les séries de Dirichlet apparaissent dans le chapitre XVII du livre de Hardy et Wright) : un cas typique est celui pour lequel a_n est le symbole de Legendre-Jacobi $\left(\frac{D}{n}\right)$ (une extension du symbole de Legendre rencontré plus haut), pour un D fixé : les coefficients dépendent alors de classes de congruence et ils peuvent servir à isoler les nombres premiers qui appartiennent à chacune d'elles. De ce que $L(\chi, s)$ ne s'annule pas en $s = 1$, Dirichlet déduisit qu'il existe une infinité de nombres premiers dans toute progression arithmétique $a + km$, dès que a, le premier terme de la progression, et m, sa raison, sont premiers entre eux. La démonstration originelle de Dirichlet est assez longue et n'a pas été reproduite par Hardy et Wright. Dirichlet utilisa également ces séries pour déterminer des nombres de classes de formes quadratiques.

Pour mieux comprendre la répartition des nombres premiers, on s'intéressait depuis l'*Essai sur la théorie des nombres* de Legendre à la fonction de comptage arithmétique π, où $\pi(x)$ est le nombre de nombres premiers plus petits que x. Cette fonction semble tout à fait irrégulière et les espoirs pour l'étudier reposaient sur la comparaison à des fonctions analytiques. Gauß suggéra d'utiliser la fonction $Li(x)$, le logarithme intégral, que nous définissons maintenant comme $Li(x) = \int_2^x \frac{dt}{\log t}$. Le mathématicien russe Pafnuti Lvovič Čebyšev confirma cette idée et corrigea également une estimation antérieure proposée par Legendre en prouvant que si le rapport de $\pi(x)$ à $\frac{x}{\log x}$ a une limite, celle-ci ne peut être que 1 (il démontra au passage le postulat de Bertrand, *cf.* § 22.3). Les deux approximations qui viennent d'être mentionnées pour $\pi(x)$, par $\frac{x}{\log x}$ et par $Li(x)$, sont bien sûr asymptotiquement équivalentes ; comme le remarque Jacques Hadamard dans son article de l'*Encyclopédie des sciences mathématiques*, la première exprime que la probabilité de tomber sur un nombre premier en choisissant au hasard un nombre entre 0 et x est $\frac{1}{\log x}$, la seconde que la probabilité qu'un nombre assez proche de x soit premier est $\frac{1}{\log x}$.

L'analyse qui intervient dans tous ces résultats est subtile d'emploi, mais élémentaire : il s'agit de convergence, d'intégration et d'estimations dans le domaine réel, et c'est elle qu'on trouve mise en œuvre dans les chapitres XVI à XVIII et XXII du présent ouvrage. On en trouve d'autres exemples, à la fois dans l'*Encyclopédie* et dans le livre de Hardy et Wright (chapitre XIX), pour le calcul des partitions de nombres.

En 1859, Bernhard Riemann, dans son unique article sur la théorie des nombres, opéra toutefois une transformation décisive en suggérant d'étu-

dier la fonction $\zeta(s)$ comme fonction d'une variable *complexe*; ce domaine était un des plus actifs et des plus difficiles de la recherche de l'époque. Riemann prouva plusieurs propriétés importantes de cette fonction, et en énonça d'autres sur la répartition de ses zéros, dont la fameuse « hypothèse de Riemann » (selon laquelle, à part certains zéros réels triviaux, tous les zéros de ζ devraient se trouver sur la droite verticale de partie réelle $\frac{1}{2}$), un des problèmes ouverts les plus importants des mathématiques actuelles (2001). La liaison entre le comportement des zéros de ζ et la répartion des nombres premiers, dont Riemann formula une version précise, vient de la possibilité de représenter la fonction ζ comme un produit de termes indexés par les nombres premiers : le logarithme de la fonction ζ tend vers $\sum p^{-s}$ et la localisation de ces zéros donne donc des informations sur la fonction de comptage des nombres premiers.

Ces idées de Riemann intéressèrent surtout les analystes et les développements de la théorie des fonctions complexes permirent à Hadamard et Charles de La Vallée-Poussin, indépendamment, mais la même année, en 1896, de démontrer les estimations asymptotiques de la fonction $\pi(x)$ mentionnées plus haut (ce qu'on connaît sous le nom de « théorème des nombres premiers ») ; leurs preuves sont distinctes, mais reposent toutes deux sur le fait que la fonction ζ ne s'annule pas sur la droite $Re(s) = 1$. Ces recherches se poursuivirent surtout à partir de 1910 (Godfrey Hardy y fut d'ailleurs un acteur crucial), fournissant alors des interactions réciproques entre théorie des fonctions et théorie des nombres. Après la seconde guerre mondiale, toutefois, des preuves élémentaires, sans analyse complexe, furent aussi développées pour certains de ces résultats, dont le théorème des nombres premiers : ce sont elles qu'ont privilégiées les éditions successives du livre de Hardy et Wright[10].

Outre les fonctions arithmétiques et la répartition des nombres premiers, le même fascicule de l'*Encyclopédie des sciences mathématiques* évoque l'arithmétique des nombres transcendants, c'est-à-dire qui ne sont solutions d'aucune équation algébrique à coefficients entiers. En 1844, Joseph Liouville construisit artificiellement des nombres non algébriques, dans le cadre de recherches sur l'approximation : les nombres algébriques sont en effet mal approchés par les rationnels et un nombre muni d'office, par construction, de très bonnes approximations rationnelles doit donc être transcendant. C'est Charles Hermite qui démontra pour la première fois, trente ans plus tard, qu'un nombre bien connu de l'analyse, e en l'occurrence, était transcendant ; la preuve de la transcendance de π, à partir d'un raffinement des idées d'Hermite, est dû à Carl Louis Ferdinand Lindemann en 1882. Ce dernier montra en fait que l'équation $X_1 e^{x_1} + X_2 e^{x_2} + \cdots X_r e^{x_r} = 0$ est impossible pour des nombres algébriques distincts x_i et des nombres algébriques non tous nuls

[10] Une discussion limpide de la théorie analytique des nombres se trouve dans [Tenenbaum et Mendès-France, 1997], qu'on pourra compléter par [Tenenbaum, 1990].

X_i ; en particulier, si x est un nombre algébrique non nul, $\sin x$, $\tan x$, e^x sont toujours transcendants, ce qui prouve que $2\pi i$ (et donc π) ne peut être algébrique. Ces résultats, avec des preuves plus simples que les preuves originales et des compléments sur l'approximation des nombres par des rationnels, correspondent à peu près au contenu du chapitre XI de Hardy et Wright.

Ce deuxième instantané du début du 20$^{\text{e}}$ siècle permet donc de rendre compte assez complètement des thèmes abordés dans le livre de Hardy et Wright. De fait, si plusieurs transformations importantes ont affecté les mathématiques fondamentales à partir des années 30, sous l'impact du développement de l'algèbre structurale et de la formalisation des notions de valeur absolue ou de distance, elles n'ont souvent été pleinement assimilées et banalisées que dans les années 70 et n'ont donc pas affecté substantiellement l'organisation du livre : je n'indiquerai pour mon dernier aperçu que quelques caractéristiques plus actuelles des thèmes abordés[11].

Le corps des rationnels a d'autres valeurs absolues que celle héritée du corps des réels. Pour tout nombre premier p, on peut définir une valeur absolue p-adique d'un entier n comme l'inverse de la plus grande puissance de p divisant n ; cette définition s'étend facilement aux nombres rationnels et l'on prouve que toute topologie non triviale sur le corps des nombres rationnels est équivalente soit à celle héritée du corps des nombres réels, soit à l'une de celles associées aux valeurs absolues p-adiques. Le corps des nombres p-adiques est alors défini comme le complété du corps des rationnels pour la valeur absolue p-adique, tout comme le corps des réels l'est pour la valeur absolue usuelle ; on peut développer une analyse p-adique au même titre que l'analyse réelle, même si ses difficultés sont différentes[12]. Certains résultats sur les rationnels peuvent être établis au croisement de ces complétions multiples : réinterprétant des résultats de Minkowski, Hasse prouva ainsi qu'une forme quadratique f à m variables et à coefficients rationnels représente un rationnel a sur le corps des rationnels (autrement dit, qu'il existe des rationnels $(x_1, \ldots, x_m)$ non tous nuls avec $f(x_1, \ldots, x_m) = a$) si et seulement si elle représente a dans le corps des réels et dans tous les corps p-adiques (autrement dit, s'il existe des réels $(y_1, \ldots, y_m)$ non tous nuls tels que $f(y_1, \ldots, y_m) = a$ et, pour chaque p, des nombres p-adiques $(z_{1p}, \ldots, z_{mp})$ non tous nuls tels que $f(z_{1p}, \ldots, z_{mp}) = a$) ; or, les critères pour l'existence de telles solutions réelles et p-adiques sont beaucoup plus faciles à établir. Une autre modification importante dans la théorie des formes est son algébrisation, sous l'impulsion des

[11] Je renvoie par exemple pour une mise à jour plus sytématique aux volumes parus ou à paraître de l'*Encyclopaedia of Mathematical Sciences* publiée par Springer.

[12] Voir par exemple [Serre, 1970] et [Amice, 1975] pour deux introductions, l'une plus algébrique, l'autre plus analytique, aux nombres p-adiques. Un mini-cours sur les nombres p-adiques, incluant le point de vue de la théorie des modèles et des connexions avec la démonstration du théorème de Fermat est disponible dans [Fainsbilber et Hobbs, 1999], *cf.* `http://books.hindawi.com/9775945003/` pour la version électronique.

travaux de Ernst Witt, qui proposa dans les années 30 de remplacer l'étude individuelle des formes par celle d'une structure, l'anneau de Witt, devenu l'objet essentiel de la théorie[13].

Les travaux sur l'irrationalité et la transcendance ont pris une large autonomie par rapport aux approches analytiques[14] : le chapitre XXIII de Hardy et Wright qui fournit trois preuves du même résultat d'approximation donnait à vrai dire déjà une idée de la grande richesse des méthodes et des thématiques dès les années 30 ; on pourra en constater les multiples ramifications dans la récente synthèse de Michel Waldschmidt pour la deuxième moitié du siècle, [Waldschmidt, 2000].

Quant à la théorie des corps de nombres algébriques, Hilbert avait aussi commencé l'étude des extensions relatives, c'est-à-dire des corps formés en ajoutant un ou plusieurs nombres algébriques à un corps de base qui n'est plus nécessairement le corps des nombres rationnels. La description des idéaux premiers, plus généralement la caractérisation de ces extensions, ne sont encore connues que pour certaines familles (théorie du corps de classes pour les extensions dites abéliennes par exemple, voir [Koch, 1992]). Les développements en sont multiples, touchant d'autres branches des mathématiques comme la théorie des représentations de groupes ou la géométrie algébrique et restent encore largement conjecturaux.

Je voudrais pour conclure faire allusion à deux zones de recherche dont les prémices, dans l'*Encyclopédie* du début du 20^{e} siècle, restaient enfouies dans le fascicule assez disparate des résultats élémentaires mais qui se sont tout à fait transformées dans la seconde moitié du siècle : les équations diophantiennes dans un cadre géométrique (surtout à partir des années 70) et la recherche d'algorithmes effectifs (dans les dernières décennies).

Une équation diophantienne (ou un système de telles équations)[15] peut être interprétée comme l'équation d'une courbe algébrique, d'une surface, d'une variété, dans un espace de dimension convenable. Chercher les solutions rationnelles, c'est donc étudier les points à coordonnées rationnelles sur la courbe (ou la surface, la variété)[16].

Pour les courbes, par exemple, on est amené à considérer comme équivalentes deux courbes qui se déduisent l'une de l'autre par des transformations birationnelles à coefficients rationnels — de telles transformations préservent les points à coordonnées rationnelles, à un nombre fini d'entre eux près. Le de-

[13] Voir [Scharlau, 1985] et [Scharlau, 2000].

[14] Voir pour celles-ci le livre déjà mentionné [Tenenbaum, 1990], ainsi que [Narkiewicz, 2000] et sur la théorie additive des nombres et les partitions [Nathanson, 1996].

[15] Pour simplifier, je me limiterai ici au cas où les coefficients des équations sont dans le corps des rationnels, bien que de nombreux résultats restent valables sur des corps de nombres généraux et que l'étude, comme celle des formes quadratiques d'ailleurs, se poursuive aussi pour d'autres corps.

[16] On consultera pour un bilan récent sur ces questions le volume correspondant de la série *Encyclopaedia of Mathematical Sciences* [Lang, 1991].

gré des équations n'est pas invariant sous ces transformations : par exemple, la courbe plane d'équation $y^2 = x^3$ (de degré 3) admet une paramétrisation rationnelle $x = t^2, y = t^3$ (et sa réciproque $t = y/x$) qui montre que cette courbe est birationnellement équivalente à la droite paramétrée par t (définissable par une équation de degré 1). On introduit donc pour les courbes un invariant, le genre, qui tient compte du degré, mais aussi de l'existence de singularités (comme le point de rebroussement en 0 dans notre exemple $y^2 = x^3$). Un des résultats les plus importants sur cette question, utilisant tout l'arsenal de la géométrie algébrique mis au point depuis les années 60, a été la démonstration par Gerd Faltings en 1983 d'une conjecture de Mordell datant de 1922 : toute courbe de genre supérieur ou égal à 2 n'a qu'un nombre fini de points à coordonnées rationnelles. On sait aussi maintenant limiter effectivement ce nombre de points. Remarquons que ce résultat montrait déjà que l'équation de Fermat $X^n + Y^n = Z^n$, pour n assez grand, n'a qu'un nombre fini de solutions avec X, Y, Z premiers entre eux. Le cas des courbes de genre 0 se ramène aisément à celui des droites et des coniques. Quant au cas du genre 1, nous ne connaissons toujours pas de procédure systématique pour déterminer si une courbe de genre 1 a un point rationnel ; mais si c'est le cas (la courbe est alors ce qu'on appelle une courbe elliptique), Mordell a prouvé que tous les points rationnels se déduisent par un procédé simple d'un nombre fini d'entre eux (en fait, à condition d'adjoindre un point à l'infini aux points de la courbe affine, l'ensemble des points rationnels forme un groupe de type fini). La théorie des courbes elliptiques est très riche. C'est en considérant la courbe elliptique d'équation $y^2 = x(x - a^p)(x + b^p)$ pour une hypothétique solution non triviale de l'équation de Fermat $a^p + b^p = c^p$ et en montrant que cette courbe contredirait les propriétés attendues des courbes elliptiques que le théorème de Fermat a finalement été démontré.

Les avancées théoriques des années 60 et 70 avaient quelque peu rejeté dans l'ombre les problèmes de calcul effectif de solutions. Le temps des ordinateurs a remis ces aspects à l'ordre du jour et beaucoup de questions mentionnées jusqu'ici sont désormais examinées de ce point de vue, à la recherche de procédés de calcul performants : factorisation, tests de primalité, mais aussi calcul des caractéristiques explicites des corps de nombres (bases d'entiers, générateurs d'idéaux, nombre de classes d'idéaux), recherche de points sur des courbes elliptiques, ont ainsi bénéficié de ces techniques. Les retombées ne concernent pas que la théorie des nombres elle-même : la cryptographie, par exemple, qui utilise de nombreux outils arithmétiques, en a largement profité[17].

La théorie des nombres se porte à merveille, ses interactions avec les autres secteurs des mathématiques, fondamentales ou très appliquées, se multiplient, et l'air du temps est à l'éclectisme. C'est donc le moment idéal pour se plonger

[17] Sur tous ces points, voir par exemple [Cohen, 1993].

dans le livre de Hardy et Wright, avant de le faire suivre, éventuellement, par de plus longues aventures en haute mer.

Catherine Goldstein
UMN 8628 CNRS-Université de Paris-Sud