

Gérald Tenenbaum

Introduction à la théorie analytique et probabiliste des nombres

DUNOD

Graphisme de couverture : Élisabeth Riba

Illustration de couverture : © Chantapa3624 - Shutterstock.com

© Dunod, 2022

11 rue Paul Bert, 92240 Malakoff

www.dunod.com

ISBN 978-2-10-083903-2

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2° et 3° a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

À Catherine Jablon,

*pour la douceur du jour,
ce bouquet de symboles
dont ta conversation
éclaire les secrets.*

Table des matières

Avant-propos	xiii
Notations	xvii
Tome I : Méthodes élémentaires	1
Chapitre I.0. Quelques outils d'analyse réelle	3
0.1 La sommation d'Abel	3
0.2 La formule sommatoire d'Euler–Maclaurin	5
Exercices	8
Chapitre I.1. Les nombres premiers	11
1.1 Introduction	11
1.2 Les estimations de Tchébychev	12
1.3 Valuation p -adique de $n!$	15
1.4 Le premier théorème de Mertens	15
1.5 Deux nouvelles formules asymptotiques	16
1.6 La formule de Mertens	18
1.7 Un autre théorème de Tchébychev	19
Notes	20
Exercices	21
Chapitre I.2. Fonctions arithmétiques	25
2.1 Définitions	25
2.2 Exemples	25
2.3 Séries de Dirichlet formelles	27
2.4 L'anneau des fonctions arithmétiques	27
2.5 Les formules d'inversion de Möbius	29
2.6 La fonction de von Mangoldt	31
2.7 La fonction indicatrice d'Euler	32
Notes	34
Exercices	35
Chapitre I.3. Ordres moyens	37
3.1 Introduction	37
3.2 Le problème de Dirichlet et le principe de l'hyperbole	37
3.3 La fonction somme des diviseurs	39
3.4 La fonction indicatrice d'Euler	40
3.5 Les fonctions ω et Ω	41
3.6 Valeur moyenne de la fonction de Möbius et fonctions sommatoires de Tchébychev	42
3.7 Entiers sans facteur carré	45
3.8 Moyenne d'une fonction multiplicative à valeurs dans $[0, 1]$	47
Notes	50
Exercices	52

Chapitre I.4. Méthodes de crible	59
4.1 Le crible d'Ératosthène	59
4.2 Le crible combinatoire de Brun	60
4.3 Application aux nombres premiers jumeaux	62
4.4 Le grand crible — forme analytique	64
4.5 Le grand crible — forme arithmétique.....	69
4.6 Applications du grand crible	72
4.7 Le crible de Selberg.....	74
4.8 Sommes de deux carrés dans un intervalle	84
Notes	88
Exercices	92
Chapitre I.5. Ordres extrémaux	97
5.1 Introduction et définitions	97
5.2 La fonction nombre de diviseurs, $\tau(n)$	98
5.3 Les fonctions nombre de facteurs premiers, $\omega(n)$ et $\Omega(n)$	99
5.4 La fonction d'Euler $\varphi(n)$	100
5.5 Les fonctions somme des puissances des diviseurs, $\sigma_\kappa(n)$, $\kappa > 0$	101
Notes	103
Exercices	104
Chapitre I.6. La méthode de van der Corput	107
6.1 Introduction et rappels	107
6.2 Intégrales trigonométriques	108
6.3 Sommes trigonométriques.....	109
6.4 Application au théorème de Voronoï	114
6.5 Équirépartition modulo 1.....	116
Notes	119
Exercices	121
Chapitre I.7. Approximation diophantienne	125
7.1 De Dirichlet à Roth.....	125
7.2 Meilleures approximations, fractions continues	127
7.3 Propriétés du développement en fraction continue	132
7.4 Développement en fraction continue des irrationnels	
quadratiques.....	134
Notes	137
Exercices	138
Tome II : Méthodes d'analyse complexe	143
Chapitre II.0. La fonction Gamma d'Euler	145
0.1 Définitions	145
0.2 Formule du produit de Weierstrass	147
0.3 Fonction Bêta	147
0.4 Formule de Stirling complexe	150
0.5 La formule de Hankel.....	154
Exercices	155

Chapitre II.1. Fonctions génératrices : séries de Dirichlet...	159
1.1 Séries de Dirichlet convergentes	159
1.2 Séries de Dirichlet des fonctions multiplicatives	160
1.3 Propriétés analytiques fondamentales des séries de Dirichlet	161
1.4 Abscisse de convergence et valeur moyenne	167
1.5 Une application arithmétique : le noyau d'un entier	169
1.6 Ordre de grandeur dans les bandes verticales	170
Notes	174
Exercices	179
Chapitre II.2. Formules de sommation	183
2.1 Formules de Perron	183
2.2 Applications : deux théorèmes de convergence	188
2.3 Formule de la valeur moyenne	190
Notes	192
Exercices	193
Chapitre II.3. La fonction zêta de Riemann	195
3.1 Introduction	195
3.2 Prolongement analytique	195
3.3 Équation fonctionnelle	198
3.4 Approximations et majorations dans la bande critique	199
3.5 Première localisation des zéros	202
3.6 Lemmes d'analyse complexe	203
3.7 Répartition globale des zéros	205
3.8 Développement en produit de Hadamard	208
3.9 Régions sans zéros	210
3.10 Majorations de ζ'/ζ , $1/\zeta$ et $\log \zeta$	211
Notes	213
Exercices	215
Chapitre II.4. Le théorème des nombres premiers et l'hypothèse de Riemann	221
4.1 Le théorème des nombres premiers	221
4.2 Hypothèses minimales	222
4.3 L'hypothèse de Riemann	224
4.4 Formule explicite pour $\psi(x)$	227
Notes	231
Exercices	233
Chapitre II.5. La méthode de Selberg–Delange	235
5.1 Puissances complexes de $\zeta(s)$	235
5.2 Le résultat principal	238
5.3 Démonstration du Théorème 5.2	240
5.4 Une variante du théorème principal	243
Notes	247
Exercices	251

Chapitre II.6. Deux applications arithmétiques	257
6.1 Entiers ayant k facteurs premiers	257
6.2 Répartition des diviseurs en moyenne : loi de l'arcsinus	263
Notes	268
Exercices	272
Chapitre II.7. Théorèmes taubériens	275
7.1 Introduction. Dualité théorèmes abéliens/taubériens	275
7.2 Le théorème de Tauber	277
7.3 Les théorèmes de Hardy–Littlewood et Karamata	279
7.4 Le terme d'erreur dans le théorème de Karamata	283
7.5 Le théorème d'Ikehara	290
7.6 L'inégalité de Berry–Esseen	295
7.7 L'holomorphie comme condition taubérienne	297
7.8 Théorèmes taubériens arithmétiques	300
Notes	303
Exercices	307
Chapitre II.8. Nombres premiers en progressions arithmétiques	311
8.1 Introduction. Caractères de Dirichlet	311
8.2 Séries L . Le théorème des nombres premiers en progressions arithmétiques	320
8.3 Minoration de $ L(s, \chi) $ pour $\sigma \geq 1$. Preuve du Théorème 8.16	326
8.4 L'équation fonctionnelle des fonctions $L(s, \chi)$	331
8.5 Formule du produit de Hadamard et régions sans zéro	334
8.6 Formules explicites pour $\psi(x; \chi)$	339
8.7 Le théorème des nombres premiers en progressions arithmétiques	343
Notes	348
Exercices	350
Tome III : Méthodes probabilistes	355
Chapitre III.1. Densités	357
1.1 Définitions. Densité naturelle	357
1.2 La densité logarithmique	360
1.3 La densité analytique	361
1.4 La théorie probabiliste des nombres	362
Notes	364
Exercices	365
Chapitre III.2. Loi de répartition d'une fonction arithmétique	369
2.1 Définition — fonctions de répartition	369
2.2 Fonctions caractéristiques	373
Notes	376
Exercices	381

Chapitre III.3. Ordre normal	385
3.1 Définition	385
3.2 L'inégalité de Turán–Kubilius.....	386
3.3 Forme duale de l'inégalité de Turán–Kubilius.....	391
3.4 Le théorème de Hardy–Ramanujan et autres applications.....	392
3.5 Majorations effectives de sommes de fonctions multiplicatives.....	395
3.6 Structure normale de la suite des facteurs premiers d'un entier.....	398
Notes.....	400
Exercices.....	405
 Chapitre III.4. Répartition des fonctions additives et valeur moyenne des fonctions multiplicatives	411
4.1 Le théorème d'Erdős–Wintner	411
4.2 Le théorème de Delange	416
4.3 Le théorème de Halász.....	420
4.4 Le théorème d'Erdős–Kac.....	433
Notes.....	436
Exercices.....	441
 Chapitre III.5. Entiers friables. La méthode du col	445
5.1 Introduction. La méthode de Rankin.....	445
5.2 La méthode géométrique.....	450
5.3 Équations fonctionnelles	451
5.4 La fonction de Dickman	456
5.5 Approximations de $\Psi(x, y)$ par la méthode du col	462
5.6 La fonction de Jacobsthal et le théorème de Rankin	471
Notes.....	475
Exercices.....	482
 Chapitre III.6. Entiers sans petit facteur premier	485
6.1 Introduction.....	485
6.2 Équations fonctionnelles.....	488
6.3 La fonction de Buchstab.....	492
6.4 Approximations de $\Phi(x, y)$ par la méthode du col	496
6.5 Le modèle de Kubilius.....	505
Notes.....	509
Exercices.....	513
 Bibliographie	517
 Index	537

Avant-propos

Issu d'enseignements de troisième cycle dispensés à Bordeaux, Paris et Nancy, ce livre a été initialement conçu dans l'intention de proposer aux jeunes chercheurs un exposé autonome d'initiation aux méthodes analytiques de l'arithmétique et, à leurs aînés, un texte de référence pour certaines questions fondamentales. Un tel programme suppose nécessairement des choix, largement soumis ici à des considérations esthétiques. Au fil des versions successives, le contenu a été significativement développé dans le triple objectif de tenir compte des avancées récentes (et la discipline a connu des progrès spectaculaires ces quinze dernières années), d'assurer la cohérence de l'aspect méthodologique, et de fournir des connaissances de base ou des compléments utiles aux étudiants des seconds cycles universitaires, notamment ceux qui préparent l'agrégation.

Ces motivations ont conduit à un usage particulier de la traditionnelle subdivision des chapitres en texte/notes/exercices. Ainsi, le texte de base, s'il ne contient en règle générale que des assertions démontrées en détail, peut aussi commenter des compléments bibliographiques utiles à la mise en perspective d'une première lecture. À l'inverse, les notes accueillent souvent des énoncés, voire des démonstrations, de théorèmes connexes qu'une première approche sommaire peut omettre. Les exercices remplissent parallèlement une double fonction. Si certains sont dévolus, classiquement, à faciliter la maîtrise des concepts précédemment introduits, d'autres conduisent à de véritables résultats de recherche, parfois nouveaux, notamment dans le tome III. Les questions ouvertes y sont exceptionnelles, les résultats visés étant le plus souvent explicités, et les étapes essentielles dégagées. Un fascicule de solutions, rédigé avec la collaboration de Jie Wu, est encore disponible aux éditions Belin. Toutefois, cette partie du présent ouvrage peut servir, même sans fournir l'effort de la résolution ou consulter les solutions, de réservoir informel de références.

Sont particulièrement destinés aux étudiants et aux futurs agrégés : les compléments concernant la formule d'Euler-Maclaurin (exercices du chapitre I.0) ; la présentation élémentaire du symbole de Legendre et de la théorie des résidus quadratiques (exercices du chapitre I.1) ; l'introduction à la théorie de l'équirépartition modulo 1 (§ I.6.5) ; une première approche, minimaliste mais autonome, de l'approximation diophantienne via un exposé synthétique de la théorie des fractions continues (chap. I.7) ; une introduction aux majorations de sommes d'exponentielles, si cruciales dans la théorie analytique des nombres actuelle ; ainsi qu'un *vade mecum* de la théorie de la fonction Gamma d'Euler — chap. II.0.

La rédaction a été guidée par le souci constant de privilégier les méthodes sur les résultats — une option spécifiquement heuristique. Cela a induit un découpage quelque peu artificiel du livre en trois tomes, dévolus respectivement aux méthodes élémentaires, d'analyse complexe, et probabilistes. On aura beau jeu de critiquer cette taxinomie : en quoi la méthode de van der Corput, reposant sur la formule sommatoire de Poisson, est-elle plus élémentaire que celle de Selberg-Delange, qui fait usage d'intégration complexe ? Pourquoi qualifier de probabiliste la méthode du col, dont l'étape liminaire consiste à écrire une intégrale de Laplace inverse ? etc. On pourrait multiplier les exemples d'incohérence relatifs à tel ou tel critère, et il est patent que les

choix effectués reposent sur des partis pris contestables. Ainsi la définition adoptée de l'élémentarité repose-t-elle sur l'exclusivité de l'emploi de la *variable réelle*, et l'option d'une vision probabiliste de la méthode du col est-elle étayée autant par référence à son emploi constant en théorie des probabilités qu'en regard de son utilisation arithmétique spécifique, pour la résolution de problèmes de théorie probabiliste des nombres... Autant dire que la classification opérée dans ce volume est tout sauf un choix bourbachique. Son ambition se limite au simple souhait qu'elle puisse éclairer un moment le chemin du néophyte.

Sans prétendre à une complète originalité, le texte témoigne d'une volonté délibérée de sortir des voies trop fréquentées. Lorsque cela a semblé nécessaire, la présentation des résultats classiques a été revisitée : soit en empruntant des approches originales (comme la méthode de Nair pour les estimations de Tchébychev, la présentation spécifique du théorème historique de Tauber, ou encore la preuve du théorème de Halász, selon une approche initiale de Montgomery), soit en introduisant, ici et là, des simplifications opératoires, invisibles à la lecture de la table des matières, mais utiles au lecteur actif.

Certains développements sont cependant inédits. Mentionnons entre autres : les résultats uniformes issus de la méthode de Selberg–Delange (chap. II.5), complétés dans les notes par une discussion de résultats très récents ; la version avec terme résiduel explicite du théorème d'Ikehara–Ingham–Delange (§ II.7.5) ; l'étude de la fonction de crible $\Phi(x, y)$ par la méthode du col (chap. III.6) ; la généralisation friable de l'inégalité de Turán–Kubilius—§ III.6.5. La forme effective du théorème d'Ikehara s'est révélée en étroite corrélation avec l'inégalité de Berry–Esseen — en fait, une véritable identité conceptuelle qui semble ne pas avoir été précédemment notée dans la littérature.

Un souci de complémentarité relativement à la bibliographie existante a pesé sur certaines options, comme le choix de la méthode de démonstration des théorèmes d'Erdős–Wintner ou d'Erdős–Kac.

Le crible de Selberg est décrit sous une forme générale peu connue (§ I.4.7), qui permet non seulement une application (standard) aux petits écarts entre nombres premiers (voir les exercices de ce même chapitre), mais aussi une majoration du nombre des sommes de deux carrés dans un intervalle arbitraire.

La méthode de Ramanujan pour l'ordre maximal de la fonction de diviseurs fait l'objet d'un exercice détaillé — le 92.

L'exposé de la théorie de la fonction zêta de Riemann et des fonctions L de Dirichlet conduit aux formules explicites de la théorie des nombres (§§ II.4.4 et II.8.6). Un développement spécifique (chap. II.8) est consacré à la répartition des nombres premiers dans les progressions arithmétiques.

Enfin, un accent particulier est porté sur les progrès récents de la théorie des entiers friables, qui occupe actuellement une place centrale dans la recherche. On introduit la fonction de Jacobsthal et l'on prouve le théorème classique de Rankin sur les grands écarts entre nombres premiers — § III.5.6, récemment amélioré de manière spectaculaire par Ford, Green, Konyagin, Maynard et Tao.

La description esquissée ci-dessus est évidemment trop sommaire pour refléter les nombreuses corrélations entre développements issus de motivations différentes. Elle n'est pas non plus exhaustive. La mise en perspective est sous-tendue par un sous-ensemble non négligeable des 313 exercices, qui proposent, pour certains théorèmes importants, des variantes de démonstration, ou, comme dans le cas du théorème de van der Corput ou encore de l'inégalité d'Erdős–Turán, des versions simplifiées.

L'auteur tient ici à exprimer sa chaleureuse reconnaissance à Régis de la Bretèche, Armand Lachand, et Bruno Martin pour leur aide lors de la préparation de cette cinquième édition.

Nancy, *septembre 2021*,

G.T.

Notations

Les notations et conventions suivantes sont utilisées librement dans le texte.

Sauf cas particulier signalé explicitement ou résultant du contexte, la lettre p , avec ou sans indice, désigne un nombre premier. Nous notons $\mathbb{P}$ l'ensemble de tous les nombres premiers.

$a|b$ signifie : a divise b ; $p^\nu || a$ signifie : $p^\nu | a$ et $p^{\nu+1} \nmid a$; $a|b^\infty$ signifie : $p|a \Rightarrow p|b$. Nous notons également $[a, b] := \text{ppcm}(a, b)$, et $(a, b) := \text{pgcd}(a, b)$.

$P^+(n)$ (resp. $P^-(n)$) désigne le plus grand (resp. le plus petit) facteur premier de l'entier $n > 1$. Par convention $P^+(1) = 1$, $P^-(1) = +\infty$.

Les parties entière inférieure, entière supérieure, et fractionnaire du nombre réel x sont notées respectivement $\lfloor x \rfloor$, $\lceil x \rceil$ et $\langle x \rangle$.

Nous posons $\|x\| := \min_{n \in \mathbb{Z}} |x - n|$, $x^+ := \max(x, 0)$ ($x \in \mathbb{R}$) et notons $e(x) := e^{2\pi i x}$ ($x \in \mathbb{R}$), $\ln^+ x := \max\{0, \ln x\}$ ($x > 0$). Pour $k \geq 2$, nous désignons par $\ln_k$ la k -ième itérée de la fonction logarithme népérien, notée $\ln$. La notation $\log$ est réservée au logarithme complexe, pris, sauf mention contraire, en détermination principale.

Lorsque la lettre s désigne un nombre complexe, nous définissons implicitement les nombres réels σ et τ par la relation $s = \sigma + i\tau$.

Nous utilisons indifféremment la notation de Landau $f = O(g)$ et celle de Vinogradov $f \ll g$ pour signifier que $|f| \leq C|g|$ pour une constante positive convenable C , qui peut être absolue ou dépendre de certains paramètres — auquel cas la dépendance pourra être indiquée en indice. De plus, nous écrivons $f \asymp g$ pour dénoter que $f \ll g$ et $g \ll f$ ont simultanément lieu. Nous attirons l'attention du lecteur sur le fait que nous avons étendu l'usage commun de ces notations au cas de quantités à valeurs complexes.

Nous désignons le cardinal d'un ensemble fini $\mathcal{A}$ soit par $\text{card } \mathcal{A}$, soit par $|\mathcal{A}|$.

Nous indiquons ci-dessous les numéros de page correspondant à l'introduction de certaines notations dans le corps du texte.

$b_r(x), B_r, B_r(x)$	5	$\delta \mathcal{A}$	360	σ_a, σ_c	163
$e(x)$	64	$\delta(n)$	27	$\sigma_k(n)$	26
$\mathbf{d} \mathcal{A}$	358	$\zeta(s)$	18	$\tau(n)$	26
$j(n)$	29	$\zeta(s, y)$	445	$\tau(n, \vartheta)$	203
$k(n)$	56	$\lambda(n)$	57	$\varphi(n)$	26
$N(T)$	206	$\Lambda(n)$	26	$\Phi(x, y)$	61
$N(x, y)$	169	$\mu(n)$	26	$\chi(n)$	314
$p_j(n)$	398	ν_N	359	$\chi_0(n)$	315
pp	364	$\xi(s)$	205	$\psi(x)$	31
$S(\mathcal{A}, \mathcal{P}, y)$	60, 80	$\pi(x)$	11	$\psi(x; a, q)$	320
$v_p(n)$	15	$\pi(x; a, q)$	73	$\Psi(x, y)$	445
$\mathbf{1}(n)$	29	$\varrho(u)$	452	$\omega(n), \Omega(n)$	25
				$\Omega_\pm$	97

Tome I

Méthodes élémentaires

I.0

Quelques outils d'analyse réelle

0.1 La sommation d'Abel

On appelle classiquement sommation, ou transformation, d'Abel le procédé consistant à transformer une somme finie de produits de deux termes en faisant apparaître les sommes partielles de l'un d'entre eux.

Théorème 0.1 (Transformation d'Abel). Soient $\{a_n\}_{n=0}^\infty$, $\{b_n\}_{n=0}^\infty$ des suites complexes. Pour tous entiers $N \in \mathbb{Z}$, $M \in \mathbb{N}^*$, on a

$$(0.1) \quad \sum_{N < n \leq N+M} a_n b_n = A_{N+M} b_{N+M+1} + \sum_{N < n \leq N+M} A_n (b_n - b_{n+1}),$$

où l'on a posé $A_n := \sum_{N < m \leq n} a_m$ ($n \geq 0$). En particulier, si

$$\sup_{N < n \leq N+M} |A_n| \leq A,$$

et si $\{b_n\}_{n=0}^\infty$ est positive et décroissante au sens large, alors

$$(0.2) \quad \left| \sum_{N < n \leq N+M} a_n b_n \right| \leq A b_{N+1}.$$

Démonstration. La première assertion résulte d'un simple changement de variable entière en posant $a_n = A_n - A_{n-1}$ ($N < n \leq N+M$). Lorsque $\{b_n\}_{n=0}^\infty$ est positive décroissante, on déduit de (0.1) que

$$\left| \sum_{N < n \leq N+M} a_n b_n \right| \leq A b_{N+M+1} + A \sum_{N < n \leq N+M} (b_n - b_{n+1}) = A b_{N+1}. \quad \square$$

Corollaire 0.2 (Critère de convergence ou règle d'Abel). Soient $\{a_n\}_{n=0}^\infty$ une suite complexe et $\{b_n\}_{n=0}^\infty$ une suite réelle positive et décroissante au sens large. On suppose que

$$\lim_{n \rightarrow \infty} b_n = 0, \quad \sup_{N \geq 0} \left| \sum_{0 \leq n \leq N} a_n \right| \leq A.$$

Alors la série $\sum_{n \geq 0} a_n b_n$ est convergente et l'on a

$$(0.3) \quad \left| \sum_{n > N} a_n b_n \right| \leq 2A b_{N+1}.$$

Démonstration. C'est immédiat à partir du Théorème 0.1. $\square$

Exemple. La série $\sum_{n \geq 1} z^n/n$, de rayon de convergence 1, converge en tous les points du cercle unité sauf $z = 1$.

Dans le formalisme de l'intégrale de Stieltjes, la sommation d'Abel prend l'aspect anodin d'une intégration par parties. Elle constitue un outil simple mais efficace pour la manipulation de sommes arithmétiques. Le lecteur pourra trouver l'essentiel des notions concernant l'intégrale de Stieltjes dans le chapitre 1 du livre de Widder (1946).

Théorème 0.3. Soit $\{a_n\}_{n=1}^\infty$ une suite de nombres complexes. On pose

$$A(t) := \sum_{n \leq t} a_n \quad (t > 0).$$

Alors, pour chaque fonction $b \in \mathcal{C}^1([1, x])$, on a

$$\sum_{1 \leq n \leq x} a_n b(n) = A(x)b(x) - \int_1^x A(t) b'(t) dt.$$

Démonstration. La quantité à calculer vaut

$$\int_{1-}^x b(t) dA(t) = \left[A(t) b(t) \right]_{1-}^x - \int_1^x b'(t) A(t) dt,$$

par intégration par parties. Cela fournit le résultat annoncé. $\square$

Le même formalisme permet de retrouver facilement d'autres résultats classiques. Commençons par deux exemples importants.

Théorème 0.4 (Comparaison d'une somme et d'une intégrale). Soit f une fonction réelle monotone sur l'intervalle $[a, b]$, avec $a, b \in \mathbb{Z}$. Il existe un nombre réel $\vartheta = \vartheta(a, b)$, $0 \leq \vartheta \leq 1$, tel que

$$\sum_{a < n \leq b} f(n) = \int_a^b f(t) dt + \vartheta(f(b) - f(a)).$$

Démonstration. Supposant, sans perte de généralité, que f est continue sur $\mathbb{Z}$, on introduit l'intégrale de Stieltjes de f par rapport à la mesure $d[t]$. Il vient

$$\sum_{a < n \leq b} f(n) - \int_a^b f(t) dt = \int_a^b f(t) d[t] - \int_a^b f(t) dt = - \int_a^b f(t) d\langle t \rangle.$$

Par intégration par parties, cette expression vaut

$$\left[-f(t) \langle t \rangle \right]_a^b + \int_a^b \langle t \rangle df(t) = \int_a^b \langle t \rangle df(t).$$

Supposons par exemple f croissante, de sorte que la mesure df est positive. La dernière intégrale vaut alors $\vartheta(f(b) - f(a))$ avec $0 \leq \vartheta \leq 1$, d'où le résultat. $\square$

Corollaire 0.5. Pour $n \geq 1$ on a $\ln n! = n \ln n - n + 1 + \vartheta \ln n$, avec $\vartheta = \vartheta_n \in [0, 1]$.

Théorème 0.6 (Seconde formule de la moyenne). Soit f une fonction monotone et g une fonction intégrable sur l'intervalle réel $[a, b]$. Il existe alors un nombre réel ξ , $a \leq \xi \leq b$, tel que

$$\int_a^b f(t) g(t) dt = f(a) \int_a^\xi g(t) dt + f(b) \int_\xi^b g(t) dt.$$

Démonstration. Posons $G(t) = \int_a^t g(v) dv$. Le membre de gauche vaut

$$\int_a^b f(t) dG(t) = G(b) f(b) - \int_a^b G(t) df(t),$$

par intégration par parties. Supposons par exemple f croissante. Alors $df(t)$ est une mesure de Stieltjes positive et, $G(t)$ étant continue, il existe un nombre ξ , $a \leq \xi \leq b$, tel que la dernière intégrale vaille $G(\xi) \{f(b) - f(a)\}$. On obtient le résultat souhaité en regroupant les termes. $\square$

0.2 La formule sommatoire d'Euler–Maclaurin

Considérons la suite $\{b_r(x)\}_{r=0}^\infty$ des polynômes définis sur $[0, 1]$ par les conditions

$$(0.4) \quad b_0(x) \equiv 1,$$

$$(0.5) \quad b'_r(x) \equiv r b_{r-1}(x) \quad (r \geq 1),$$

$$(0.6) \quad \int_0^1 b_r(x) dx = 0 \quad (r \geq 1).$$

On vérifie facilement que ces hypothèses impliquent l'identité

$$\sum_{r \geq 0} b_r(x) \frac{y^r}{r!} = \frac{y e^{xy}}{e^y - 1}$$

qui permet de calculer les b_r . On a

$$\begin{aligned} b_0(x) &= 1, & b_3(x) &= x^3 - \frac{3}{2}x^2 + \frac{1}{2}x, \\ b_1(x) &= x - \frac{1}{2}, & b_4(x) &= x^4 - 2x^3 + x^2 - \frac{1}{30}, \\ b_2(x) &= x^2 - x + \frac{1}{6}, & b_5(x) &= x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x. \end{aligned}$$

On définit alors la r -ième fonction de Bernoulli $B_r(x)$ comme la fonction périodique de période 1 qui coïncide avec b_r sur $[0, 1]$. On pose

$$B_r := B_r(0).$$

B_r est le r -ième nombre de Bernoulli. Il est facile de voir que $B_{2r+1} = 0$ pour $r \geq 1$.

Le tableau suivant rassemble les premières valeurs numériques.

r	0	1	2	4	6	8	10	12	14	16
B_r	1	$-\frac{1}{2}$	$\frac{1}{6}$	$-\frac{1}{30}$	$\frac{1}{42}$	$-\frac{1}{30}$	$\frac{5}{66}$	$-\frac{691}{2730}$	$\frac{7}{6}$	$-\frac{3617}{510}$

Soit f une fonction numérique de classe $\mathcal{C}^{k+1}$ sur l'intervalle $[a, b]$, avec $a, b \in \mathbb{Z}$. Puisque $B_1(x) = \langle x \rangle - \frac{1}{2}$, on peut écrire

$$\sum_{a < n \leq b} f(n) = \int_a^b f(t) d[t] = \int_a^b f(t) dt - \int_a^b f(t) dB_1(t).$$

Calculons la dernière intégrale par intégration par parties :

$$\begin{aligned} \int_a^b f(t) dB_1(t) &= B_1 \cdot (f(b) - f(a)) - \int_a^b B_1(t) f'(t) dt \\ &= B_1 \cdot (f(b) - f(a)) - \frac{1}{2!} \int_a^b f'(t) dB_2(t). \end{aligned}$$

En effet, on vérifie sans peine que $B_2(t)$ est continue sur $\mathbb{R}$ et dérivable sur $\mathbb{R} \setminus \mathbb{Z}$, où elle satisfait à $B_2'(t) = 2B_1(t)$. De plus, pour $r \geq 3$, $B_r(t)$ est dérivable sur tout $\mathbb{R}$ et satisfait à

$$B_r'(t) = rB_{r-1}(t).$$

On peut donc calculer l'intégrale relative à $B_2(t)$ par une nouvelle sommation partielle, en faisant intervenir $B_3(t)$. On obtient ainsi par itération le théorème célèbre suivant.

Théorème 0.7 (Formule sommatoire d'Euler–Maclaurin). *Pour tout entier $k \geq 0$ et toute fonction f de classe $\mathcal{C}^{k+1}$ sur $[a, b]$, $a, b \in \mathbb{Z}$, on a*

$$\begin{aligned} \sum_{a < n \leq b} f(n) &= \int_a^b f(t) dt + \sum_{0 \leq r \leq k} \frac{(-1)^{r+1} B_{r+1}}{(r+1)!} (f^{(r)}(b) - f^{(r)}(a)) \\ &\quad + \frac{(-1)^k}{(k+1)!} \int_a^b B_{k+1}(t) f^{(k+1)}(t) dt. \end{aligned}$$

À titre d'application, donnons une estimation des sommes partielles de la série harmonique.

Théorème 0.8. *Pour $n \geq 1$, on a*

$$\sum_{m \leq n} \frac{1}{m} = \ln n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{\vartheta}{60n^4},$$

où γ est la constante d'Euler et où $\vartheta = \vartheta_n \in [0, 1]$.

Démonstration. Appliquons le Théorème 0.7 avec $f(t) = 1/t$, $a = 1$, $b = n$, $k = 3$. Il vient

$$\sum_{2 \leq m \leq n} \frac{1}{m} = \ln n + \frac{1}{2} \left(\frac{1}{n} - 1 \right) - \frac{1}{12} \left(\frac{1}{n^2} - 1 \right) + \frac{1}{120} \left(\frac{1}{n^4} - 1 \right) - \int_1^n t^{-5} B_4(t) dt.$$

Ajoutons le terme correspondant à $m = 1$, et faisons tendre n vers l'infini. On obtient

$$\gamma = \frac{1}{2} + \frac{1}{12} - \frac{1}{120} - \int_1^\infty \frac{B_4(t)}{t^5} dt.$$

Le résultat est donc impliqué par la majoration

$$\left| \int_n^\infty \frac{B_4(t)}{t^5} dt \right| \leq \frac{1}{120n^4},$$

que l'on déduit immédiatement du fait que $|B_4(t)| \leq \frac{1}{30}$ pour tout t . □

Remarque. Une généralisation immédiate des calculs précédents fournit la formule

$$\gamma = \frac{1}{2} + \sum_{2 \leq r \leq k} \frac{B_r}{r} - \int_1^\infty \frac{B_k(t)}{t^{k+1}} dt \quad (k \geq 1),$$

qui peut être utilisée pour calculer numériquement γ en retranchant cette expression du développement de $\sum_{m=1}^n 1/m$ et en optimisant k en fonction de n . Nous obtenons ainsi, par exemple, $\gamma \approx 0,577215664$.

Exercices

1. Pour $k \in \mathbb{Z}^+$, calculer $\frac{1}{2\pi i} \oint_{|z|=\pi(2k+1)} \frac{ze^{xz}}{(e^z - 1)} \frac{dz}{z^{2r+1}}$ et établir ainsi le développement de Fourier des fonctions de Bernoulli d'ordre pair :

$$B_{2r}(x) = (-1)^{r-1} 2(2r)!(2\pi)^{-2r} \sum_{m \geq 1} \frac{\cos(2\pi mx)}{m^{2r}} \quad (r \geq 1).$$

En déduire une formule générale pour $\zeta(2r)$.

2. Établir par la méthode décrite à l'exercice précédent le développement de Fourier de $B_{2r+1}(x)$, i.e.

$$B_{2r+1}(x) = (-1)^{r-1} (2r+1)! (2\pi)^{-2r-1} \sum_{m \geq 1} \frac{\sin(2\pi mx)}{m^{2r+1}} \quad (r \geq 0),$$

où l'égalité n'est valable que pour $x \in \mathbb{R} \setminus \mathbb{Z}$ lorsque $r = 0$.

Pourquoi n'obtient-on pas ainsi une formule pour $\zeta(2r+1)$?

3. *Formule de Stirling.*

(a) En appliquant la formule d'Euler-Maclaurin à l'ordre 0 pour la fonction $f(t) = \ln t$ montrer que l'on a

$$n! = n^n e^{-n} \sqrt{An} \{1 + O(1/n)\} \quad (n \geq 1)$$

avec $\ln A = 2 + 2 \int_1^\infty B_1(t) t^{-1} dt$.

(b) Montrer en utilisant une intégration par parties que la suite

$$W_n = \int_0^{\pi/2} (\cos t)^n dt$$

des intégrales de Wallis satisfait la relation de récurrence

$$n W_n = (n-1) W_{n-2} \quad (n \geq 2).$$

En déduire que, lorsque $n \rightarrow \infty$, $W_{2n} \sim \pi/\sqrt{2An}$ et $W_{2n+1} \sim \sqrt{A/8n}$.

(c) Prouver que $W_n \sim W_{n+1}$ ($n \rightarrow \infty$) et montrer que $A = 2\pi$.

4. Soient $k \in \mathbb{N}$ et $f \in \mathcal{C}^{2k+1}([1, \infty[, \mathbb{R})$ telle que $f^{(2k+1)} \in L^1[1, \infty[$. Montrer qu'il existe une constante $C_k(f)$, que l'on explicitera, telle que l'on ait, pour tout entier $n \geq 1$,

$$(0.7) \quad \sum_{1 \leq m \leq n} f(m) = \int_1^n f(x) dx + \frac{1}{2} f(n) + \sum_{1 \leq j \leq k} \frac{B_{2j}}{(2j)!} f^{(2j-1)}(n) + C_k(f) + R_{k,n}(f)$$

où $R_{k,n}(f) \rightarrow 0$ lorsque $n \rightarrow \infty$.

En déduire que, si $f^{(j)} \in L^1([1, \infty[)$ pour $j \geq 2m+1$, alors $C_k(f)$ est indépendant de k lorsque $k \geq m$.

5. *Variations des $B_r(x)$.* Posons, pour $m \geq 1$, $\varepsilon \in \{0, 1\}$, $x \in \mathbb{R}$,

$$\varphi_{2m+\varepsilon}(x) := (-1)^m \{B_{2m+\varepsilon}(x) - B_{2m+\varepsilon}\}.$$

(a) Montrer que, pour $0 \leq x \leq 1$, on a $\varphi_2(x) = x(1-x)$, $\varphi_3(x) = x(x - \frac{1}{2})(1-x)$.

(b) Calculer $\sum_{r \geq 0} b_r(\frac{1}{2}) y^r / r!$. En déduire que $\varphi_{2m+1}(\frac{1}{2}) = 0$ pour $m \geq 1$.

(c) Montrer que, pour $m \geq 1$, on a $\varphi'_{2m+1}(x) = (2m+1)\{\varphi_{2m}(x) - |B_{2m}|\}$, et $\varphi'_{2m+2}(x) = -(2m+2)\varphi_{2m+1}(x)$.

(d) Établir par récurrence sur $m \geq 1$ que $\varphi_{2m}(x) > 0$ pour $0 < x < 1$ et $(x - \frac{1}{2})\varphi_{2m+1}(x) > 0$ pour $0 < x < 1$, $x \neq \frac{1}{2}$.

6. Majoration du terme d'erreur de la formule d'Euler-Maclaurin.

Soient $k \in \mathbb{N}$ et $f \in \mathcal{C}^{2k+2}([1, \infty[, \mathbb{R})$ telle que $f^{(2k+2)} \in L^1[1, \infty[$. On pose

$$S_{h,n}(f) := \frac{1}{2}f(n) + \sum_{1 \leq j \leq h} \frac{B_{2j}}{(2j)!} f^{(2j-1)}(n) \quad (0 \leq h \leq k+1, n \in \mathbb{N}^*).$$

(a) Montrer que l'on a, pour tout entier $n \geq 1$,

$$(0.8) \quad \sum_{1 \leq m \leq n} f(m) = \int_1^n f(x) dx + S_{k,n}(f) + C_k^*(f) + R_{k,n}^*(f),$$

où $C_k^*(f)$ est une constante que l'on précisera et où l'on a posé, avec la notation φ_r de l'Exercice 5,

$$(0.9) \quad R_{k,n}^*(f) := \frac{(-1)^{k+1}}{(2k+2)!} \int_n^\infty f^{(2k+2)}(x) \varphi_{2k+2}(x) dx.$$

(b) On effectue désormais l'hypothèse supplémentaire que $f^{(2k)} \in L^1([1, \infty[)$ et $\lim_{x \rightarrow \infty} f^{(2k-1)}(x) = 0$. Montrer que

$$C_{k-1}^*(f) = C_k^*(f), \quad R_{k-1,n}^*(f) - R_{k,n}^*(f) = \frac{B_{2k}}{(2k)!} f^{(2k-1)}(n).$$

(c) Montrer que, si $f^{(2k+2)}$ et $f^{(2k)}$ sont de signe constant et de même signe sur $[1, \infty[$, alors $R_{k-1,n}^*(f)$ et $R_{k,n}^*(f)$ ont des signes opposés. En déduire que

$$|R_{k,n}^*(f)| \leq \left| \frac{B_{2k}}{(2k)!} f^{(2k-1)}(n) \right|,$$

autrement dit, que la valeur absolue du terme d'erreur de la formule d'Euler-Maclaurin (0.8) n'excède pas celle du dernier terme retenu.

7. Montrer que pour tous entiers $n \geq 1$, $k \geq 1$, on a

$$\gamma = \sum_{1 \leq m \leq n} \frac{1}{m} - \ln n - \frac{1}{2n} + \sum_{1 \leq j \leq k} \frac{B_{2j}}{2jn^{2j}} + \varepsilon_{kn}$$

où γ désigne la constante d'Euler et où $|\varepsilon_{kn}| \leq |B_{2k}|/\{2kn^{2k}\}$. Montrer que le choix $n = 50$, $k = 7$, permet de calculer γ avec 24 décimales exactes.

Remarque. Sommation au plus petit terme. On sait que $|B_{2j}| \sim 2(2j)!/(2\pi)^{2j}$. Lorsque n est fixé, le rapport de deux termes consécutifs dans la somme en j est donc, en valeur absolue, voisin de $(j/\pi n)^2$. Il s'ensuit que le meilleur terme d'erreur obtenu par cette méthode correspond au choix de k voisin de πn . La taille de ε_{kn} est alors de l'ordre de $e^{-2\pi n}$. Pour $n = 10$, on obtient déjà 27 décimales exactes sous réserve de connaître les valeurs de B_{2k} pour $k \leq 32$.

8. Montrer que pour tous entiers $n \geq 1$, $k \geq 1$, on a

$$\frac{1}{6}\pi^2 = \sum_{1 \leq m \leq n} \frac{1}{m^2} + \frac{1}{n} - \frac{1}{2n^2} + \sum_{1 \leq j \leq k} \frac{B_{2j}}{n^{2j+1}} + \varepsilon_{kn}$$

avec $|\varepsilon_{kn}| \leq |B_{2k}|/n^{2k+1}$. Montrer que le choix $k = 8$, $n = 100$ permet de calculer $\pi^2/6$ avec 33 décimales exactes.

9. En appliquant la formule d'Euler-Maclaurin sur l'intervalle $[1, N]$ à la fonction

$$f(x) := \ln \left(\frac{x\vartheta}{1 - e^{-x\vartheta}} \right),$$

et en faisant tendre N vers l'infini, montrer que, pour tout entier $k \geq 2$ fixé on a, lorsque ϑ tend vers 0 par valeurs positives,

$$\prod_{n \geq 1} \left(\frac{1}{1 - e^{-n\vartheta}} \right) = \left\{ 1 + O(\vartheta^k) \right\} e^{\pi^2/6\vartheta - \vartheta/24} \sqrt{\frac{\vartheta}{2\pi}}.$$

I.1

Les nombres premiers

1.1 Introduction

L'addition et la multiplication confèrent à l'ensemble des entiers naturels $\{1, 2, 3, \dots\}$ une double structure de semi-groupe abélien. La première, associée à une relation d'ordre total, est engendrée par le seul nombre 1. La seconde, image de l'ordre partiel de la divisibilité, possède une infinité de générateurs : les nombres premiers. Défini depuis l'Antiquité, ce concept-clef n'a pas encore, il s'en faut de beaucoup, livré tous ses secrets. La situation centrale de la théorie des nombres premiers en Arithmétique est amplement justifiée par le résultat suivant dont nous esquissons la démonstration, via le premier théorème d'Euclide, aux Exercices 10 à 13.

Théorème 1.1 (Théorème fondamental de l'arithmétique). *Chaque entier naturel > 1 se décompose de manière unique, à l'ordre des facteurs près, sous forme d'un produit de nombres premiers.*

Le second théorème d'Euclide énonce l'infinitude de l'ensemble des nombres premiers. C'est une conséquence immédiate du théorème fondamental de l'arithmétique : si $p_1 = 2, p_2 = 3, \dots, p_n$ sont les n plus petits nombres premiers alors l'entier

$$N = 1 + \prod_{1 \leq j \leq n} p_j$$

n'est divisible par aucun des nombres $p_1, p_2, \dots, p_n$. Son plus petit facteur premier est donc un nombre premier $> p_n$.

On désigne habituellement par $\pi(x)$ le nombre des nombres premiers n'excédant pas x de sorte que, pour tout entier n , on a $\pi(p_n) = n$. Le second théorème d'Euclide exprime le fait que

$$\pi(x) \rightarrow \infty \quad (x \rightarrow \infty).$$

Depuis plus de vingt-trois siècles, les mathématiciens s'attachent à préciser quantitativement cette relation qualitative. C'est l'un des buts de cet ouvrage que de décrire les diverses méthodes qu'ils ont inventées et mises en œuvre pour y parvenir.

La preuve donnée plus haut du second théorème d'Euclide est trop simple pour être ineffective. On a en effet

$$p_{n+1} \leq 1 + \prod_{1 \leq j \leq n} p_j$$

d'où l'on déduit par une récurrence immédiate

$$p_n \leq 2^{2^n} \quad (n \geq 1).$$

On obtient ainsi la minoration suivante.

Théorème 1.2. *On a*

$$\pi(x) > \frac{\ln_2 x}{\ln 2} - \frac{1}{2} \quad (x \geq 2).$$

Démonstration. D'après la majoration de p_n établie plus haut, on peut écrire

$$\pi(x) \geq \max\{m \in \mathbb{N} : 2^{2^m} \leq x\} = \left\lfloor \frac{\ln(\ln x / \ln 2)}{\ln 2} \right\rfloor \geq \frac{\ln_2 x}{\ln 2} - \left(1 + \frac{\ln_2 2}{\ln 2}\right),$$

ce qui implique le résultat annoncé. $\square$

La minoration du Théorème 1.2 est loin d'être optimale. Après avoir été conjecturée pendant plus d'un siècle (notamment par Legendre et Gauss), la formule asymptotique

$$\pi(x) \sim \frac{x}{\ln x} \quad (x \rightarrow \infty),$$

a été établie indépendamment en 1896 par Hadamard (1865–1963) et La Vallée–Poussin (1866–1962). Leurs méthodes reposaient sur des techniques d'analyse complexe qui seront décrites au Tome II. Il a fallu attendre 1949 pour qu'apparaissent les premières démonstrations élémentaires du théorème des nombres premiers, dues à Erdős et Selberg. Depuis cette date, de nombreuses autres démonstrations élémentaires ont été publiées. Celle de Daboussi (1984), est particulièrement élégante et repose sur un principe fondamentalement différent des autres.⁽¹⁾ Elle est notamment exposée en détail au chap. 4 de l'ouvrage de Tenenbaum & Mendès France (2000).

1.2 Les estimations de Tchébychev

C'est au mathématicien russe Pafnouti Tchébychev que l'on doit les premiers travaux significatifs sur la fonction $\pi(x)$. En 1852, il démontre le postulat de Bertrand selon lequel chaque intervalle $]n, 2n]$, $n \geq 1$, contient au moins un nombre premier. Il obtient ce résultat en établissant une forme effective de l'estimation

$$\{c_1 + o(1)\} \frac{x}{\ln x} \leq \pi(x) \leq \{c_2 + o(1)\} \frac{x}{\ln x} \quad (x \rightarrow \infty),$$

avec $c_1 = \ln(2^{1/2} 3^{1/3} 5^{1/5} 30^{-1/30}) \approx 0,92129$, et $c_2 = \frac{6}{5} c_1 \approx 1,10555$.

Nous allons montrer par une méthode simple le résultat suivant qui implique une forme légèrement affaiblie du postulat de Bertrand : pour tout $\varepsilon > 0$, il existe un $n_0 = n_0(\varepsilon)$ tel que chaque intervalle $]n, (2 + \varepsilon)n]$, $n \geq n_0$, contienne au moins un nombre premier.

Théorème 1.3. *Pour $n \geq 4$, nous avons*

$$\frac{n \ln 2}{\ln n} \leq \pi(n) \leq \left\{ \ln 4 + \frac{8 \ln_2 n}{\ln n} \right\} \frac{n}{\ln n}.$$

Démonstration. La majoration est une conséquence facile du résultat classique suivant.

1. Elle ne fait notamment pas appel à l'identité de Selberg — cf. Exercice 76, p. 57 — qui joue un rôle essentiel dans la plupart des autres preuves élémentaires.