Gérald Tenenbaum

Introduction à la théorie analytique et probabiliste des nombres

DUNOD

Graphisme de couverture : Élisabeth Riba

Illustration de couverture : © Chantapa3624 - Shutterstock.com

11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-083903-2

À Catherine Jablon,

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

Table des matières

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 $[a,b] := \mathrm{ppcm}(a,b)$, et $(a,b) := \mathrm{pgcd}(a,b)$.

$P^+(n)$ (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 $\mathrm{e}(x) := \mathrm{e}^{2\pi i x}$ $(x \in \mathbb{R})$, $\ln^+ x := \max\{0, \ln x\}$ $(x > 0)$. Pour $k \geqslant 2$, 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 $|f| \leqslant C|g|$ 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 $\mathrm{card}\,\mathcal{A}$, soit par $|\mathcal{A}|$.

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

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*

$$\sum_{N<n\leqslant N+M} a_n b_n = A_{N+M} b_{N+M+1} + \sum_{N<n\leqslant N+M} A_n (b_n - b_{n+1}), \tag{0·1}$$

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

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

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

$$\left| \sum_{N<n\leqslant N+M} a_n b_n \right| \leqslant A b_{N+1}. \tag{0·2}$$

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

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

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*

$$\lim_{n\to\infty} b_n = 0, \qquad \sup_{N\geqslant 0} \left| \sum_{0\leqslant n\leqslant N} a_n \right| \leqslant A.$$

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

$$\left| \sum_{n>N} a_n b_n \right| \leqslant 2 A b_{N+1}. \tag{0·3}$$

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

Exemple. La série $\sum_{n\geqslant 1} z^n/n$, 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*

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

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

$$\sum_{1 \leqslant n \leqslant x} a_n b(n) = A(x)b(x) - \int_1^x A(t)\, b'(t)\, \mathrm{d}t.$$

Démonstration. La quantité à calculer vaut

$$\int_{1^-}^{x} b(t)\, \mathrm{d}A(t) = \Big[A(t)\, b(t)\Big]_{1^-}^{x} - \int_1^x b'(t) A(t)\, \mathrm{d}t,$$

par intégration par parties. Cela fournit le résultat annoncé. □

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 $\vartheta = \vartheta(a, b)$, $0 \leqslant \vartheta \leqslant 1$, tel que*

$$\sum_{a < n \leqslant b} f(n) = \int_a^b f(t)\, \mathrm{d}t + \vartheta\big(f(b) - f(a)\big).$$

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 $\mathrm{d}\lfloor t \rfloor$. Il vient

$$\sum_{a < n \leqslant b} f(n) - \int_a^b f(t)\, \mathrm{d}t = \int_a^b f(t)\, \mathrm{d}\lfloor t \rfloor - \int_a^b f(t)\, \mathrm{d}t = -\int_a^b f(t)\, \mathrm{d}\langle t \rangle .$$

Par intégration par parties, cette expression vaut

$$\Big[- f(t)\, \langle t \rangle \Big]_a^b + \int_a^b \langle t \rangle \ \mathrm{d}f(t) = \int_a^b \langle t \rangle \ \mathrm{d}f(t).$$

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

Corollaire 0.5. *Pour $n \geqslant 1$ 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 , $a \leqslant \xi \leqslant b$, tel que*

$$\int_a^b f(t)\,g(t)\,\mathrm{d}t = f(a)\int_a^\xi g(t)\,\mathrm{d}t + f(b)\int_\xi^b g(t)\,\mathrm{d}t.$$

Démonstration. Posons $G(t) = \int_a^t g(v)\,\mathrm{d}v$. Le membre de gauche vaut

$$\int_a^b f(t)\,\mathrm{d}G(t) = G(b)\,f(b) - \int_a^b G(t)\,\mathrm{d}f(t),$$

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

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

$$b_0(x) \equiv 1, \tag{0·4}$$

$$b_r'(x) \equiv r\,b_{r-1}(x) \qquad (r \geqslant 1), \tag{0·5}$$

$$\int_0^1 b_r(x)\,\mathrm{d}x = 0 \qquad (r \geqslant 1). \tag{0·6}$$

On vérifie facilement que ces hypothèses impliquent l'identité

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

qui permet de calculer les b_r. On a

$$b_0(x) = 1, \qquad b_3(x) = x^3 - \tfrac{3}{2}x^2 + \tfrac{1}{2}x,$$
$$b_1(x) = x - \tfrac{1}{2}, \qquad b_4(x) = x^4 - 2x^3 + x^2 - \tfrac{1}{30},$$
$$b_2(x) = x^2 - x + \tfrac{1}{6}, \qquad b_5(x) = x^5 - \tfrac{5}{2}x^4 + \tfrac{5}{3}x^3 - \tfrac{1}{6}x.$$

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 $r \geqslant 1$.

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 $B_1(x)=\langle x\rangle-\frac12$, on peut écrire

$$\sum_{a<n\leqslant b} f(n)=\int_a^b f(t)\,\mathrm{d}\,\lfloor t\rfloor=\int_a^b f(t)\,\mathrm{d}t-\int_a^b f(t)\,\mathrm{d}B_1(t).$$

Calculons la dernière intégrale par intégration par parties :

$$\begin{aligned}\int_a^b f(t)\,\mathrm{d}B_1(t)&=B_1{\cdot}(f(b)-f(a))-\int_a^b B_1(t)f'(t)\,\mathrm{d}t\\&=B_1{\cdot}(f(b)-f(a))-\frac{1}{2!}\int_a^b f'(t)\,\mathrm{d}B_2(t).\end{aligned}$$

En effet, on vérifie sans peine que $B_2(t)$ est continue sur $\mathbb{R}$ et dérivable sur $\mathbb{R}\smallsetminus\mathbb{Z}$, où elle satisfait à $B_2'(t)=2B_1(t)$. De plus, pour $r\geqslant 3$, $B_r(t)$ 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 $k\geqslant 0$ et toute fonction f de classe $\mathcal{C}^{k+1}$ sur $[a,b]$, $a,b\in\mathbb{Z}$, on a*

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

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

Théorème 0.8. *Pour $n\geqslant 1$, on a*

$$\sum_{m\leqslant n}\frac1m=\ln n+\gamma+\frac{1}{2n}-\frac{1}{12n^2}+\frac{\vartheta}{60n^4},$$

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

$$\sum_{2\leqslant m\leqslant n}\frac1m=\ln n+\tfrac12\Big(\frac1n-1\Big)-\tfrac{1}{12}\Big(\frac{1}{n^2}-1\Big)+\tfrac{1}{120}\Big(\frac{1}{n^4}-1\Big)-\int_1^n t^{-5}B_4(t)\,\mathrm{d}t.$$

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

$$\gamma=\tfrac12+\tfrac{1}{12}-\tfrac{1}{120}-\int_1^\infty\frac{B_4(t)}{t^5}\,\mathrm{d}t.$$

Le résultat est donc impliqué par la majoration

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

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

Remarque. Une généralisation immédiate des calculs précédents fournit la formule

$$\gamma = \tfrac{1}{2} + \sum_{2\leqslant r\leqslant k} \frac{B_r}{r} - \int_1^\infty \frac{B_k(t)}{t^{k+1}}\,\mathrm{d}t \qquad (k \geqslant 1),$$

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 $\dfrac{1}{2\pi i}\displaystyle\oint_{|z|=\pi(2k+1)} \frac{z\mathrm{e}^{xz}}{(\mathrm{e}^z-1)}\,\frac{\mathrm{d}z}{z^{2r+1}}$ et établir ainsi le développement de Fourier des fonctions de Bernoulli d'ordre pair :

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

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.

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

où l'égalité n'est valable que pour $x \in \mathbb{R}\smallsetminus\mathbb{Z}$ 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

$$n! = n^n\,\mathrm{e}^{-n}\sqrt{An}\,\{1+O(1/n)\} \qquad (n\geqslant 1)$$

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

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

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

des intégrales de Wallis satisfait la relation de récurrence

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

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

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

4. Soient $k\in\mathbb{N}$ et $f\in\mathcal{C}^{2k+1}\Big([1,\infty[,\mathbb{R}\Big)$ 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 $n\geqslant 1$,

$$\sum_{1\leqslant m\leqslant n} f(m) = \int_1^n f(x)\,\mathrm{d}x + \tfrac12 f(n) + \sum_{1\leqslant j\leqslant k}\frac{B_{2j}}{(2j)!}f^{(2j-1)}(n) + C_k(f) + R_{k,n}(f) \tag{0·7}$$

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

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

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

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

(a) Montrer que, pour $0\leqslant x\leqslant 1$, on a $\varphi_2(x)=x(1-x)$, $\varphi_3(x)=x(x-\frac12)(1-x)$.

(b) Calculer $\sum_{r\geqslant 0} b_r(\frac12)y^r/r!$. En déduire que $\varphi_{2m+1}(\frac12)=0$ pour $m\geqslant 1$.

(c) Montrer que, pour $m\geqslant 1$, 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 $m\geqslant 1$ que $\varphi_{2m}(x)>0$ pour $0<x<1$ et $(x-\frac12)\varphi_{2m+1}(x)>0$ pour $0<x<1$, $x\neq\frac12$.

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

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

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

$$\sum_{1\leqslant m\leqslant n} f(m) = \int_1^n f(x)\,\mathrm{d}x + S_{k,n}(f) + C_k^*(f) + R_{k,n}^*(f), \tag{0·8}$$

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,

$$R_{k,n}^*(f) := \frac{(-1)^{k+1}}{(2k+2)!} \int_n^\infty f^{(2k+2)}(x)\varphi_{2k+2}(x)\,\mathrm{d}x. \tag{0·9}$$

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

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

(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

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

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 $n \geqslant 1$, $k \geqslant 1$, on a

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

où γ désigne la constante d'Euler et où $|\varepsilon_{kn}| \leqslant |B_{2k}|/\{2kn^{2k}\}$. 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 $\mathrm{e}^{-2\pi n}$. Pour $n = 10$, on obtient déjà 27 décimales exactes sous réserve de de connaître les valeurs de B_{2k} pour $k \leqslant 32$.

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

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

avec $|\varepsilon_{kn}| \leqslant |B_{2k}|/n^{2k+1}$. 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

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

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

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

I.1

Les nombres premiers

1·1 Introduction

L'addition et la multiplication confèrent à l'ensemble des entiers naturels $\{1, 2, 3, \ldots\}$ 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 $p_1 = 2$, $p_2 = 3, \ldots,$ p_n sont les n plus petits nombres premiers alors l'entier

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

n'est divisible par aucun des nombres $p_1, p_2, \ldots, p_n$. 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

$$\pi(x) \to \infty \qquad (x \to \infty).$$

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

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

d'où l'on déduit par une récurrence immédiate

$$p_n \leqslant 2^{2^n} \qquad (n \geqslant 1).$$

On obtient ainsi la minoration suivante.

Théorème 1.2. *On a*

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

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

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

ce qui implique le résultat annoncé. □

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

$$\pi(x) \sim \frac{x}{\ln x} \qquad (x \to \infty),$$

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 $]n, 2n]$, $n \geqslant 1$, contient au moins un nombre premier. Il obtient ce résultat en établissant une forme effective de l'estimation

$$\{c_1 + o(1)\}\frac{x}{\ln x} \leqslant \pi(x) \leqslant \{c_2 + o(1)\}\frac{x}{\ln x} \qquad (x \to \infty),$$

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 $]n, (2+\varepsilon)n]$, $n \geqslant n_0$, contienne au moins un nombre premier.

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

$$\frac{n \ln 2}{\ln n} \leqslant \pi(n) \leqslant \Big\{ \ln 4 + \frac{8 \ln_2 n}{\ln n} \Big\} \frac{n}{\ln n}.$$

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.