

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 22 (1976)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: DIVISIBILITÉ DE CERTAINES FONCTIONS ARITHMÉTIQUES
Autor: Serre, Jean-Pierre
Kapitel: §3. PREMIERS EXEMPLES
DOI: <https://doi.org/10.5169/seals-48187>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 21.02.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

Remarque. Dans le cas (b), si l'ensemble des p tels que $p^2 \in E'$ est frobénien, on peut utiliser la méthode de Landau pour obtenir un développement asymptotique de $E'(x)$.

Exemple. Prenons pour E l'ensemble des entiers de la forme pm , avec p premier, et $(p, m) = 1$; l'ensemble E' est formé des entiers $n \geq 1$ tels que $p | n \Rightarrow p^2 | n$ pour tout p premier; les hypothèses de (2.10 b) sont vérifiées avec $\delta = 1$. On a

$$\begin{aligned} f(s) &= \prod_p (1 + p^{-2s} + p^{-3s} + p^{-4s} + \dots) = \prod_p \frac{1 - p^{-s} + p^{-2s}}{1 - p^{-s}} \\ &= \prod_p \frac{1 + p^{-3s}}{1 - p^{-2s}} = \prod_p \frac{1 - p^{-6s}}{(1 - p^{-2s})(1 - p^{-3s})} \\ &= \zeta(2s)\zeta(3s)/\zeta(6s). \end{aligned}$$

D'après (2.10 b), on a $E'(x) \sim cx^{1/2}$, avec $c = \zeta(3/2)/\zeta(3)$. On connaît en fait des résultats bien plus précis, par exemple celui-ci (Bateman-Grosswald, *Illinois J. Math.*, 2, 1958):

$$E'(x) = cx^{1/2} + dx^{1/3} + O(x^{1/6} \exp(-A \log^B x)), \quad \text{avec } A, B > 0.$$

§ 3. PREMIERS EXEMPLES

3.1. *Sommes de deux carrés.* C'est l'exemple traité initialement par Landau [8] (voir aussi [6], [24], [26]):

On prend pour E' l'ensemble des entiers $n \geq 1$ qui sont de la forme $a^2 + b^2$, avec $a, b \in \mathbf{Z}$ (ou $a, b \in \mathbf{Q}$, cela revient au même); on a ainsi:

$$E'(x) = N\{n \leq x : n = [\underline{2}]\}.$$

Soit P l'ensemble des nombres premiers p tels que $p \equiv -1 \pmod{4}$. On sait qu'un entier n appartient à E' si et seulement si, pour tout $p \in P$, l'exposant $v_p(n)$ de p dans n est pair. Il en résulte que le complémentaire E de E' est multiplicatif (au sens du § 2), et que P est l'ensemble des nombres premiers appartenant à E . Comme P est frobénien de densité $1/2$, le théorème (2.8) montre l'existence de constantes c_0, c_1, \dots telles que

$$E'(x) = \frac{x}{\sqrt{\log x}} (c_0 + c_1/\log x + \dots + c_k/\log^k x + O(1/\log^{k+1} x))$$

pour tout $k > 0$. On trouvera dans Shanks [24] (rectifiant Ramanujan [6]

et Stanley [26]) une étude numérique de $E'(x)$ pour $x \leq 2^{26}$, ainsi qu'une détermination des deux premiers coefficients c_0 et c_1 :

$$c_0 = \left(2 \prod_{p \in P} (1 - p^{-2}) \right)^{-1/2} = 0,76422365 \dots$$

$$c_1 = 0,44473893 \dots$$

3.2. *Fonctions multiplicatives.* Soit $n \mapsto a_n$ une fonction multiplicative à valeurs dans un anneau commutatif A , et soit P_a l'ensemble des nombres premiers p tels que $a_p = 0$. Il est clair que P_a est associé à l'ensemble E_a des entiers n tels que $a_n = 0$. En appliquant (2.2) on en déduit:

THÉORÈME 3.3. *Supposons que P_a soit régulier de densité $\alpha > 0$. On a alors*

$$N \{ n \leq x : a_n \neq 0 \} = \begin{cases} O(x/\log^\alpha x) & \text{si } \alpha < 1 \\ O(x^\gamma) \quad \text{avec } \gamma < 1 & \text{si } \alpha = 1. \end{cases}$$

(Ainsi, « presque tous » les a_n sont nuls.)

Si A est intègre, E_a est multiplicatif. D'après (2.4) et (2.8), on en tire:

THÉORÈME 3.4. *Si A est intègre, et $\alpha < 1$, on a*

$$N \{ n \leq x : a_n \neq 0 \} \sim cx/\log^\alpha x, \quad \text{avec } c > 0.$$

Si de plus P_a est frobenien, on a un développement asymptotique

$$N \{ n < x : a_n \neq 0 \} = \frac{x}{\log^\alpha x} (c_0 + c_1/\log x + \dots).$$

Donnons maintenant quelques exemples de fonctions multiplicatives auxquelles on peut appliquer les théorèmes 3.3 et 3.4:

3.5. *Coefficients de fonctions L.* — On prend pour A le corps \mathbf{C} , et pour a_n les coefficients d'une fonction L d'Artin

$$L(s, \chi) = \sum a_n n^{-s},$$

où χ est un caractère de degré $d \geq 1$ d'un groupe de Galois $G = \text{Gal}(K/\mathbf{Q})$, cf. §1. Faisons l'hypothèse:

(3.5.1.) Le sous-ensemble H de G formé des éléments $g \in G$ tels que $\chi(g) = 0$ est non vide.

L'ensemble P_a des nombres premiers p tels que $a_p = 0$ est alors frobénien de densité $\alpha = |H|/|G|$: cela résulte de (1.3) puisque $a_p = \chi(\sigma_p(K/\mathbf{Q}))$ pour tout p ne divisant pas le discriminant de K .

Toutes les conditions de (3.4) sont alors satisfaites (noter que $\alpha < 1$, car $|H| \neq |G|$, l'élément neutre n'appartenant pas à H). On en déduit un développement asymptotique de $N\{n \leq x: a_n \neq 0\}$.

Exemple. Soit k un corps de nombres de degré > 1 ; choisissons pour K une extension galoisienne de \mathbf{Q} contenant k , et soit $G_k = \text{Gal}(K/k)$ le sous-groupe de $G = \text{Gal}(K/\mathbf{Q})$ correspondant à k . Prenons pour χ le caractère de la représentation de permutation de G dans G/G_k ; on a

$$\chi(g) = \text{nombre d'éléments de } G/G_k \text{ laissés fixes par } g$$

et

$$L(s, \chi) = \zeta_k(s) = \sum N\mathfrak{q}^{-s},$$

où \mathfrak{q} parcourt les idéaux entiers $\neq 0$ du corps k . L'ensemble H de (3.5.1) est égal à

$$G - \{\text{union des conjugués de } G_k\}.$$

On a $H \neq \emptyset$ d'après un résultat élémentaire sur les groupes finis (cf. par exemple Bourbaki, A I.130, exerc. 6). Appliquant (3.5), on en déduit:

$$N\{n \leq x: n \text{ est norme d'un idéal de } k\} \sim \frac{x}{\log^\alpha x} (c_0 + c_1/\log x + \dots),$$

résultat dû à Odoni (cf. [11], [12]). Lorsque $k = \mathbf{Q}(i)$, on retrouve l'exemple de Landau (3.1).

3.6. Réduction mod \mathfrak{m} de fonctions multiplicatives. Soit $n \mapsto a_n$ une fonction multiplicative à valeurs dans l'anneau O_F des entiers d'un corps de nombres algébriques F . Soit \mathfrak{m} un idéal non nul de O_F , et notons \tilde{a}_n l'image de a_n dans l'anneau fini O_F/\mathfrak{m} ; soit $P_{a,\mathfrak{m}}$ l'ensemble des nombres premiers p tels que $a_p \equiv 0 \pmod{\mathfrak{m}}$. Si l'on fait l'hypothèse:

$$(3.6.1) \quad P_{a,\mathfrak{m}} \text{ est régulier de densité } \alpha(\mathfrak{m}) > 0,$$

on peut appliquer (3.3) à la fonction $n \mapsto \tilde{a}_n$, et l'on en déduit:

THÉORÈME 3.7. $N\{n \leq x: a_n \neq 0 \pmod{\mathfrak{m}}\} = O(x/\log^{\alpha(\mathfrak{m})} x),$

ainsi que des résultats plus précis lorsqu'on suppose en outre que $P_{a,\mathfrak{m}}$ est frobénien et que \mathfrak{m} est premier.

Exemples.

(a) (cf. Scourfield [17], [18]) On suppose que $p \mapsto \tilde{a}_p$ est une fonction *polynomiale* de p , i.e. qu'il existe un polynôme $\varphi_m(T)$, à coefficients dans O_F/m , tel que $\tilde{a}_p = \varphi_m(p)$ pour tout p . L'ensemble $P_{a,m}$ est alors frobénien; pour qu'il soit de densité > 0 , il faut et il suffit que φ_m « représente 0 », i.e. qu'il existe un entier t , premier à m , tel que $\varphi_m(t) = 0$. (*Exemple*: on prend $a_n = \sigma_{r,s}(n) = \sum_{dd'=n} d^r d'^s$, avec r pair et s impair, d'où

$$\varphi_m(T) = T^r + T^s, \text{ et } \varphi_m(t) = 0 \text{ pour } t = -1.)$$

(b) On suppose que la série $\sum a_n n^{-s}$ est associée à un « *système F-rationnel de représentations l-adiques* » (cf. [20], chap. I, § 2, ainsi que [4], [19], [27]). Cela entraîne l'existence d'une extension galoisienne finie K_m de \mathbf{Q} , et d'une représentation linéaire

$$\rho_m : \mathrm{Gal}(K_m/\mathbf{Q}) \rightarrow \mathrm{GL}_N(O_F/m)$$

telles que $\mathrm{Tr}(\rho_m(\sigma_p(K_m/\mathbf{Q}))) \equiv a_p \pmod{m}$ pour tout nombre premier p , à l'exception d'un nombre fini. Si l'on suppose en outre qu'il existe $\sigma \in \mathrm{Im}(\rho_m)$ tel que $\mathrm{Tr}(\sigma) = 0$, alors (3.6.1) est vérifié; on peut souvent prendre pour σ l'image par ρ_m de la *conjugaison complexe* (« Frobenius réel »): c'est le cas pour les systèmes de représentations *l*-adiques définis par une forme modulaire (cf. § 4), ou par la cohomologie $H^i(X)$, i impair, d'une variété projective non singulière X définie sur \mathbf{Q} .

§ 4. EXEMPLES MODULAIRES

Pour les définitions et notations concernant les formes modulaires sur $\mathrm{SL}_2(\mathbf{Z})$ et ses sous-groupes d'indice fini, on renvoie à [5], [19], [25], [27]. Rappelons seulement que l'on pose $q = e^{2\pi iz}$, avec $\mathcal{J}(z) > 0$.

4.1. *Formes de poids 1* (cf. [5], § 9). — Soit $f = \sum a_n q^n$ une forme modulaire de poids 1 sur un sous-groupe de congruence de $\mathrm{SL}_2(\mathbf{Z})$.

THÉORÈME 4.2.

(i) *Il existe $\alpha > 0$ tel que*

$$N\{n \leqslant x : a_n \neq 0\} = O(x/\log^\alpha x).$$

(ii) *Soit N un entier $\geqslant 1$, et soit ε un caractère de $(\mathbf{Z}/N\mathbf{Z})^*$. Supposons que f soit une forme modulaire de type $(1, \varepsilon)$ sur $\Gamma_0(N)$, et soit*