

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
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: 04.04.2026

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

DIVISIBILITÉ DE CERTAINES FONCTIONS ARITHMÉTIQUES

par Jean-Pierre SERRE

On connaît de nombreux exemples de fonctions arithmétiques $n \mapsto a_n$ jouissant de la propriété suivante: pour tout entier $m \geq 1$, l'ensemble des n tels que $a_n \equiv 0 \pmod{m}$ est de densité 1; autrement dit, on a

$$a_n \equiv 0 \pmod{m} \quad \text{pour « presque tout » entier } n .$$

Il en est notamment ainsi lorsque les a_n sont les coefficients d'une forme modulaire de poids entier sur un sous-groupe de congruence de $\mathbf{SL}_2(\mathbf{Z})$: cela se démontre en appliquant la méthode de Landau [8] aux fonctions L d'Artin fournies par la théorie de Deligne [4]. Cette démonstration est esquissée dans la Note [23]. Je reprends ici la question, en donnant davantage de détails: les §§ 1 à 3 rappellent les résultats généraux de Landau, Watson, Raikov, Delange, ...; les §§ 4 à 5 appliquent ces résultats aux coefficients de formes modulaires, ainsi qu'à ceux de la fonction j ; le § 6 contient divers compléments, rédigés sous forme d'exercices, avec esquisses de démonstrations.

A des changements mineurs près, le texte qui suit est extrait du Séminaire DELANGE-PISOT-POITOU 1974/75. Je remercie les organisateurs de ce Séminaire de m'avoir autorisé à le reproduire.

TABLE DES MATIÈRES

	<i>Pages</i>
§ 1. Ensembles de nombres premiers	228
§ 2. Théorèmes de densité	230
§ 3. Premiers exemples	236
§ 4. Exemples modulaires	239
§ 5. Divisibilité des coefficients de j	245
§ 6. Exercices	249
Bibliographie	259

§ 1. ENSEMBLES DE NOMBRES PREMIERS

Soit P un ensemble de nombres premiers. Considérons les propriétés suivantes :

$$(1.1) \quad \sum_{p \in P} 1/p = +\infty ;$$

(1.2) P est de *densité* $\alpha > 0$, i.e. le nombre des $p \in P$ qui sont $\leq x$ est égal à $\alpha x / \log x + o(x / \log x)$ quand $x \rightarrow \infty$.

(1.3) P est *régulier* de densité $\alpha > 0$, au sens de Delange [3], i.e.

$$\sum_{p \in P} p^{-s} = \alpha \log 1/(s-1) + \theta_P(s),$$

où $\theta_P(s)$ se prolonge en une fonction holomorphe pour $\Re(s) \geq 1$.

(1.4) P est *frobénien* de densité $\alpha > 0$, i. e. il existe une extension finie galoisienne K/\mathbf{Q} , et une partie H du groupe $G = \text{Gal}(K/\mathbf{Q})$ telles que

(a) H est stable par conjugaison,

(b) $|H| / |G| = \alpha$ (on note $|X|$ le nombre d'éléments d'un ensemble fini X),

(c) pour tout p assez grand, on a $p \in P \Leftrightarrow \sigma_p(K/\mathbf{Q}) \in H$, où $\sigma_p(K/\mathbf{Q})$ désigne la substitution de Frobenius [1] de p dans G (définie à conjugaison près lorsque p ne divise pas le discriminant de K).

PROPOSITION 1.5. On a $(1.4) \Rightarrow (1.3) \Rightarrow (1.2) \Rightarrow (1.1)$.

L'implication $(1.2) \Rightarrow (1.1)$ est facile. L'implication $(1.3) \Rightarrow (1.2)$ est prouvée dans [3], p. 57, comme conséquence d'un théorème taubérien. D'autre part, sous les hypothèses de (1.4), on a

$$(1.6) \quad \sum_{p \in P} p^{-s} = \frac{1}{|G|} \sum_{\chi} \bar{\chi}(H) \log L(s, \chi)^1 + g(s),$$

où :

χ parcourt l'ensemble des caractères irréductibles de G ,

$L(s, \chi)$ est la fonction L d'Artin [1] relative à l'extension K/\mathbf{Q} et au caractère χ ,

¹⁾ Ici, comme au §2, la détermination choisie de « log » est celle que l'on obtient par prolongement analytique sur les horizontales à partir de la détermination « évidente » pour $\Re(s) > 1$ (i. e. celle fournie par le développement en série — on peut aussi la caractériser par le fait qu'elle tend vers 0 quand $\Re(s)$ tend vers $+\infty$).

g est une série de Dirichlet qui converge absolument pour $\Re(s) > 1/2$ (donc est holomorphe pour $\Re(s) \geq 1$),

$$\bar{\chi}(H) = \sum_{h \in H} \bar{\chi}(h).$$

Il résulte alors des propriétés élémentaires des fonctions $L(s, \chi)$ que $\log L(s, \chi) = \delta_\chi \log 1/(s-1) + \theta_\chi(s)$, où $\delta_\chi = 0$ (resp. $\delta_\chi = 1$) si $\chi \neq 1$ (resp. si $\chi = 1$), et $\theta_\chi(s)$ est holomorphe pour $\Re(s) \geq 1$. La propriété (1.3) en résulte.

Exemples.

(1) Si a et m sont des entiers ≥ 1 tels que $(a, m) = 1$, l'ensemble des nombres premiers p tels que $p \equiv a \pmod{m}$ est frobenien de densité $1/\varphi(m)$.

(2) L'ensemble des nombres premiers qui se décomposent complètement (resp. ont un facteur premier de degré 1) dans une extension finie de \mathbf{Q} est frobenien de densité > 0 .

(3) Soit τ la fonction de Ramanujan (cf. [6], [19], [27]). Si m est un entier ≥ 1 , l'ensemble des p tels que $\tau(p) \equiv 0 \pmod{m}$ est frobenien de densité $\alpha(m) > 0$; cela résulte de Deligne [4] (voir aussi [19], [27], ainsi que le §4 ci-après). Lorsque m est premier, on peut calculer $\alpha(m)$ grâce à [27]. On trouve:

$$\alpha(m) = \begin{cases} 1, 1/2, 1/4, 1/2, 1/2, 1/690 & \text{si } m = 2, 3, 5, 7, 23, 691 \\ m/(m^2 - 1) & \text{sinon.} \end{cases}$$

Remarque. Lorsque P est frobenien, on peut préciser un peu le comportement de la fonction $f_P(s) = \sum_{p \in P} p^{-s}$ à gauche de la droite critique $\Re(s) = 1$:

PROPOSITION 1.7. *La fonction f_P se prolonge en une fonction holomorphe dans une région de la forme*

$$(1.8) \quad \begin{cases} \Re(s) \geq 1 - b/\log^A T, & \text{avec } b, A > 0, T = 2 + |\mathcal{F}(s)| \\ \mathcal{F}(s) \neq 0 \text{ ou } s \text{ réel } > 1, \end{cases}$$

et y admet une majoration

$$(1.9) \quad |f_P(s)| = O(\log \log T) \text{ pour } T \rightarrow \infty.$$

Cela se démontre de la manière suivante: vu (1.6), il suffit de prouver l'énoncé analogue pour $\log L(s, \chi)$; grâce au théorème d'induction de Brauer, on peut en outre supposer que χ est un caractère de degré 1 de

Gal (K/E), où E est un sous-corps de K . On peut alors appliquer à $\log L(s, \chi)$ les méthodes classiques de Hadamard et de La Vallée Poussin, cf. par exemple [10], p. 336-337. [En fait, [10] se borne à prouver l'existence d'une région (1.8) où $L = L(s, \chi)$ est holomorphe $\neq 0$, et où $|L'/L| = O(\log^A T)$. Pour passer de là à la majoration

$$|\log L(s, \chi)| = O(\log \log T),$$

on distingue deux cas, suivant que $\mathcal{R}(s)$ est ou non $\geq 1 + 1/\log^A T$. Dans le premier cas, on a :

$$\begin{aligned} |\log L(s, \chi)| &\leq [E:Q] \log \zeta(\mathcal{R}(s)) \leq [E:Q] A \log \log T + O(1) \\ &= O(\log \log T). \end{aligned}$$

Le deuxième cas se ramène au premier: on applique le théorème des accroissements finis au segment horizontal I_s joignant s au point s_0 tel que

$$\mathcal{I}(s_0) = \mathcal{I}(s), \quad \mathcal{R}(s_0) = 1 + 1/\log^A T,$$

et l'on obtient

$$\begin{aligned} |\log L(s, \chi)| &\leq |\log L(s_0, \chi)| + |s - s_0| \sup_{\sigma \in I_s} |L'/L(\sigma, \chi)| \\ &= O(\log \log T) + O(1) = O(\log \log T). \end{aligned}$$

§2. THÉORÈMES DE DENSITÉ

2.1. *Définitions.* Soit E une partie de l'ensemble \mathbf{N}^* des entiers > 0 ; on note E' le complémentaire $\mathbf{N}^* - E$ de E . Si $x \in \mathbf{N}^*$, on note $E(x)$ le nombre des $n \leq x$ qui appartiennent à E ; on a $E(x) + E'(x) = x$. Lorsque E est l'ensemble des n satisfaisant à une relation R , on écrit aussi

$$N\{n \leq x: R(n)\}$$

à la place de $E(x)$.

On dit que E est de *densité* c si $\lim_{x \rightarrow \infty} E(x)/x = c$, autrement dit si

$$E(x) = cx + o(x) \quad \text{pour } x \rightarrow \infty.$$

Soit P un ensemble de nombres premiers. Nous dirons que P est *associé* à E si, pour tout $p \in P$ et tout entier $m \geq 1$ non divisible par p , on a $pm \in E$.

THÉORÈME 2.2. *Si P est associé à E , et si P jouit de la propriété (1.1), à savoir $\sum_{p \in P} 1/p = +\infty$, alors E est de densité 1.*

Soit I une partie finie de P , et soit E_I l'ensemble des entiers de la forme pm , avec $p \in I$ et $m \geq 1$ non divisible par p . Le complémentaire E'_I de E_I est l'ensemble des entiers $n \geq 1$ tels que

$$n \not\equiv p, 2p, 3p, \dots, (p-1)p \pmod{p^2} \quad \text{pour tout } p \in I.$$

Sa densité est $c_I = \prod_{p \in I} (1 - (p-1)/p^2)$. Mais, vu (1.1), le produit infini $\prod_{p \in P} (1 - (p-1)/p^2)$ diverge, i. e. tend vers 0. Les c_I tendent donc vers 0, et comme E' est contenu dans tous les E'_I , on a

$$\limsup E'(x)/x \leq \lim c_I = 0,$$

d'où le fait que E' est de densité 0.

Le cas régulier. D'après (2.2), on a $E'(x) = o(x)$ pour $x \rightarrow \infty$. Nous allons voir que l'on peut préciser ce résultat, à condition de faire des hypothèses supplémentaires sur P . Tout d'abord:

THÉORÈME 2.3. *Supposons que P soit associé à E , et soit régulier de densité $\alpha > 0$. On a alors :*

- (a) $E'(x) = O(x/\log^\alpha x)$ si $\alpha < 1$;
- (b) $E'(x) = O(x^{1-\delta})$, avec $\delta > 0$, si $\alpha = 1$.

Disons d'autre part que E est *multiplicatif* s'il possède la propriété:

(M) Si n_1 et n_2 sont des entiers ≥ 1 premiers entre eux, on a

$$n_1 n_2 \in E \Leftrightarrow \{n_1 \in E \text{ ou } n_2 \in E\}.$$

THÉORÈME 2.4. *Supposons E multiplicatif, et soit P l'ensemble des nombres premiers appartenant à E . Alors :*

(a) Si P est régulier de densité α , avec $0 < \alpha < 1$, on a

$$E'(x) \sim cx/\log^\alpha x, \quad \text{avec } c > 0.$$

(b) Si P est régulier de densité 1, on a

$$E'(x) = O(x^{1-\delta}), \quad \text{avec } \delta > 0.$$

(Noter qu'il résulte de (M) que P est associé à E .)

Démonstration de (2.4) (d'après Raikov, Wintner, Delange). — Posons $b_n = 0$ si $n \in E$, et $b_n = 1$ si $n \in E'$, de sorte que:

$$E'(x) = \sum_{n \leq x} b_n;$$

la condition (M) signifie que b_n est une fonction *multiplicative* de n . On a $b_1 = 1$ (mis à part le cas trivial où $E' = \emptyset$). Considérons la série de Dirichlet

$$f(s) = \sum b_n n^{-s} = \sum_{n \in E'} n^{-s},$$

qui converge absolument pour $\Re(s) > 1$. On a

$$f(s) = \prod_p f_p(s), \quad \text{où } f_p(s) = \sum_{p^m \in E'} p^{-ms}.$$

La série $f_p(s)$ commence par le terme $1 + p^{-s}$ si et seulement si p n'appartient pas à P . On peut donc écrire f sous la forme

$$f(s) = \prod_{p \notin P} (1 + p^{-s}) \prod_p h_p(s),$$

où le produit des h_p est absolument convergent pour $\Re(s) > 1/2$. On a donc

$$(2.5) \quad \log f(s) = \sum_{p \notin P} p^{-s} + \theta_1(s),$$

où $\theta_1(s)$ est holomorphe et bornée dans tout demi-plan $\Re(s) \geq c$, avec $c > 1/2$. Plaçons-nous dans le cas (a), i. e. supposons P régulier de densité α , avec $0 < \alpha < 1$; le complémentaire de P est régulier de densité $1 - \alpha$; vu (1.3), et la formule ci-dessus, on a

$$\log f(s) = (1 - \alpha) \log 1/(s - 1) + \theta_2(s),$$

où $\theta_2(s)$ est holomorphe pour $\Re(s) \geq 1$. Revenant à f , on obtient

$$(2.6) \quad f(s) = \frac{1}{(s - 1)^{1 - \alpha}} h(s),$$

où $h(s) = \exp \theta_2(s)$ est holomorphe et $\neq 0$ pour $\Re(s) \geq 1$. D'après une variante du théorème taubérien de Ikehara (cf. [2], [3], [14], [15], [29]), ceci entraîne

$$(2.7) \quad \sum_{n \leq x} b_n \sim cx / \log^\alpha x, \quad \text{avec } c = h(1) / \Gamma(1 - \alpha),$$

d'où (2.4) dans le cas $\alpha < 1$. Si d'autre part $\alpha = 1$, le même argument montre que $f(s)$ est holomorphe pour $\Re(s) \geq 1$; comme c'est une série à coefficients positifs, il en résulte, d'après un lemme classique de Landau, qu'elle converge en un point $s = 1 - \delta$, avec $\delta > 0$; on en déduit aussitôt la majoration cherchée:

$$\sum_{n \leq x} b_n = O(x^{1 - \delta}).$$

Démonstration de (2.3). Soit $E(P)$ l'ensemble des entiers de la forme pm , avec $p \in P$ et $m \geq 1$ premier à p . On a $E(P) \subset E$, d'où $E'(x) \leq E(P)'(x)$. D'autre part, $E(P)$ est multiplicatif, et son intersection avec l'ensemble des nombres premiers est P . En appliquant (2.4) à $E(P)$, on obtient

$$E(P)'(x) = O(x/\log^\alpha x) \quad \text{dans le cas (a),}$$

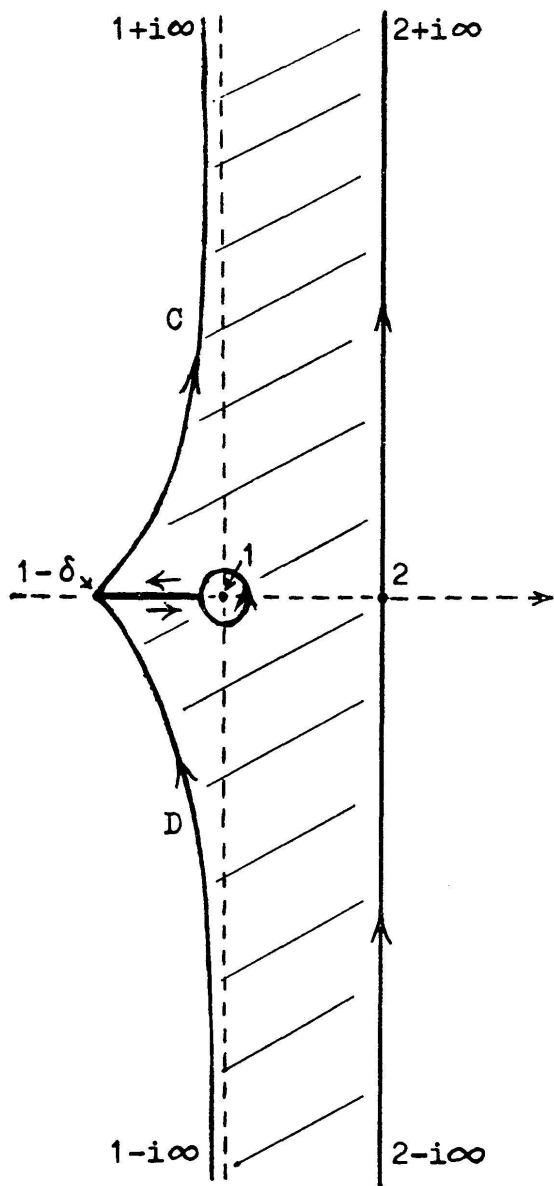
$$E(P)'(x) = O(x^{1-\delta}), \text{ avec } \delta > 0, \quad \text{dans le cas (b),}$$

d'où (2.3) puisque $E'(x) \leq E(P)'(x)$.

Le cas frobenien. Revenons aux hypothèses de (2.4 a); on a

$$E'(x) = cx/\log^\alpha x + o(x/\log^\alpha x), \quad \text{avec } c > 0.$$

Si P est *frobenien*, on peut remplacer le terme d'erreur $o(x/\log^\alpha x)$ par $O(x/\log^{1+\alpha} x)$, et même donner un *développement asymptotique* de $E'(x)$:



THÉORÈME 2.8. *Supposons que E soit multiplicatif, et que l'ensemble P des nombres premiers appartenant à E soit frobenien de densité α , avec $0 < \alpha < 1$. Il existe alors des nombres*

$$c_0, c_1, \dots, c_k, \dots, \text{ avec } c_0 > 0,$$

tels que, pour tout entier $k \geq 0$, on ait

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

La démonstration utilise une méthode due à Landau [8]; je me bornerai à la résumer, renvoyant à [8] ou [28] pour plus de détails:

$$\text{Soit } f(s) = \sum b_n n^{-s} = \sum_{n \in E'} n^{-s},$$

comme ci-dessus. On montre au moyen de (2.5) et (1.7) que f se prolonge en une fonction holomorphe dans une région du type ci-contre (les branches infinies C et D étant définies par

$\mathcal{R}(s) = 1 - b/\log^4 T$, avec $T = 2 + |\mathcal{J}(s)|$, et que l'on a dans cette région

$$|f(s)| = O(\log^4 T) \quad \text{pour } T \rightarrow \infty.$$

Posons alors

$$b(x) = \sum_{n \leq x} b_n \log(x/n).$$

On vérifie que

$$b(x) = \frac{1}{2i\pi} \int_{2-i\infty}^{2+i\infty} f(s) x^s ds/s^2.$$

La formule de Cauchy montre que cette intégrale est égale à l'intégrale analogue prise sur le bord gauche de la région considérée. Les contributions des branches infinies C et D sont négligeables devant $x/\log^N x$, quel que soit N ; celle du cercle centré en 1 tend vers 0 avec le rayon du cercle. Le terme principal est donc fourni par les deux intégrales sur le segment horizontal joignant $1 - \delta$ à 1; ces dernières s'évaluent sans difficulté, à partir du développement de $f(s)$ au voisinage de $s = 1$. On trouve que:

$$b(x) = \frac{x}{\log^\alpha x} (d_0 + d_1/\log x + \dots + d_k/\log^k x + O(1/\log^{k+1} x)).$$

En appliquant ce résultat à $x + \delta x$, avec $\delta \sim 1/\log^{k+1} x$, et en retranchant, on obtient facilement l'estimation cherchée pour $E'(x) = \sum_{n \leq x} b_n$ (cf. [17], p. 277, ou [28], p. 723-724).

De façon plus précise, si le développement de $f(s)/s$ au voisinage de $s = 1$ est:

$$f(s)/s = \frac{1}{(s-1)^{1-\alpha}} (e_0 + e_1(s-1) + \dots + e_k(s-1)^k + \dots),$$

on trouve pour $E'(x)$ le développement asymptotique

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

avec

$$(2.9) \quad c_k = e_k/\Gamma(1-k-\alpha).$$

Remarques.

(1) En utilisant (1.6) on peut ramener le calcul des e_i et des c_i à celui, d'une part de séries absolument convergentes (donc évaluables numériquement), et d'autre part de valeurs des dérivées des $L(s, \chi)$ au point $s = 1$; pour un exemple de tel calcul, voir [24].

(2) La méthode de Landau suivie ci-dessus a l'avantage, non seulement de donner un développement asymptotique, mais encore de fournir un terme d'erreur que l'on peut *effectivement* majorer, pourvu bien sûr que l'on dispose de majorations effectives de $f(s)$, ce qui est le plus souvent faisable (mais rarement fait...). On ne peut rien déduire de tel des théorèmes taubériens à la Ikehara, du moins sous leur forme actuelle.

(3) A la place de l'intégrale de $f(s) x^s/s^2$, on pourrait songer à utiliser celle de $f(s) x^s/s$, qui conduit directement à $\sum_{n \leq x} b_n$. Malheureusement, il ne semble pas facile de majorer cette dernière intégrale sur les branches infinies C et D .

Voici maintenant une variante du théorème (2.8), dans le cas où l'ensemble P est frobénien de densité 1, i. e. de complémentaire fini :

THÉORÈME 2.10. *Supposons que E soit multiplicatif, et contienne tous les nombres premiers, à l'exception d'un nombre fini. Alors :*

(a) *On a $E'(x) = O(x^{1-2})$.*

(b) *Si l'ensemble des nombres premiers p tels que $p^2 \in E'$ est régulier de densité $\delta > 0$, on a*

$$E'(x) \sim cx^{1/2}/\log^{1-\delta}x, \quad \text{avec } c > 0.$$

L'assertion (a) est facile, et peut d'ailleurs se ramener à (b). Plaçons-nous donc dans le cas (b), et posons ici encore

$$f(s) = \sum_{n \in E'} n^{-s} = \sum b_n n^{-s}.$$

Les hypothèses faites sur E entraînent que

$$\log f(s) = \sum_{p^2 \in E'} p^{-2s} + \theta_1(s) = \delta \log 1/(2s-1) + \theta_2(s),$$

où les $\theta_i(s)$ sont holomorphes pour $\Re(s) \geq 1/2$. Il en résulte que

$$f(s/2) = \frac{1}{(s-1)^\delta} h(s),$$

où $h(s)$ est holomorphe et $\neq 0$ pour $\Re(s) \geq 1$. En appliquant à $f(s/2)$ les théorèmes taubériens cités plus haut (cf. [2], [14], [29]), on en déduit

$$\sum_{\sqrt{n} < x} b_n \sim c_1 x / \log^{1-\delta} x, \quad \text{avec } c_1 = h(1)/\Gamma(\delta);$$

en remplaçant x par $x^{1/2}$, on obtient le résultat cherché :

$$E'(x) \sim cx^{1/2}/\log^{1-\delta}x, \quad \text{avec } c = 2^{1-\delta}c_1.$$

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 $p \mid n \Rightarrow p^2 \mid n$ 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:

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

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*

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

(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*

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

Si de plus P_a est frobénien, 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{a} 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:

$$\text{THÉORÈME 3.7. } N\{n \leq x: a_n \not\equiv 0 \pmod{\mathfrak{m}}\} = O(x/\log^{\alpha(\mathfrak{m})} x),$$

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 frobenien; 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

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

telles que $\text{Tr}(\rho_m(\sigma_p(K_m/\mathbf{Q}))) \equiv a_p \pmod{m}$ pour tout nombre premier p , à l'exception d'un nombre fini. Si l'on suppose en outre qu'il existe $\sigma \in \text{Im}(\rho_m)$ tel que $\text{Tr}(\sigma) = 0$, 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 $\mathbf{SL}_2(\mathbf{Z})$ 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 $\mathbf{SL}_2(\mathbf{Z})$.

THÉORÈME 4.2.

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

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

(ii) *Soit N un entier ≥ 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*

fonction propre des opérateurs de Hecke T_p (pour $p \nmid N$) et U_p (pour $p \mid N$), cf. [5], § 1. Si $f \neq 0$, on a un développement asymptotique

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

avec $0 < \alpha < 1$ et $c_0 > 0$.

Plaçons-nous d'abord dans le cas (ii). Quitte à multiplier f par une constante, on peut supposer que $a_1 = 1$, et la fonction $n \mapsto a_n$ est alors multiplicative. De plus, d'après [5], il existe une extension galoisienne finie K_f de \mathbf{Q} , et une représentation

$$\rho_f: \text{Gal}(K_f/\mathbf{Q}) \rightarrow \text{GL}_2(\mathbf{C})$$

dont la fonction L d'Artin coïncide (à un nombre fini de facteurs près) avec la série de Dirichlet $\sum a_n n^{-s}$. Si l'on note G l'image de ρ_f , et H la partie de G formée des éléments de trace nulle, on a $H \neq \emptyset$ car H contient l'image de la conjugaison complexe ([5], n° 4.5) et $H \neq G$ car H ne contient pas 1. L'ensemble P_a des p tels que $a_p = 0$ est frobenien, et défini par H . Sa densité $\alpha = |H|/|G|$ est $\neq 0, 1$: toutes les conditions de (3.4) sont bien vérifiées. D'où (ii).

L'assertion (i) résulte de (ii) et du fait bien connu¹⁾ que toute forme modulaire est somme de fonctions $z \mapsto f_i(d_i z)$, où les d_i sont des entiers ≥ 1 et les f_i des formes modulaires de type (ii).

Exemples.

(4.3) La forme

$$\theta^2 = (1 + 2q + 2q^4 + 2q^9 + \dots)^2 = \sum_{a,b \in \mathbf{Z}} q^{a^2+b^2}$$

est du type (ii), avec $N = 4$, et $\varepsilon(n) = (-4/n) = (-1)^{(n-1)/2}$; la représentation correspondante est la représentation réductible $1 \oplus \varepsilon$; on a $\alpha = 1/2$. On retrouve une nouvelle fois l'exemple de Landau (3.1).

(4.4) La forme

$$f = \Delta^{1/12}(12z) = q \prod_{m=1}^{\infty} (1 - q^{12m})^2 = \sum_{\substack{a \equiv 1 \pmod{3} \\ b \equiv 0 \pmod{3} \\ a+b \equiv 1 \pmod{2}}} (-1)^b q^{a^2+b^2}$$

est du type (ii), avec $N = 144$, et $\varepsilon(n) = (-4/n)$; la représentation correspondante est la représentation irréductible de degré 2 du groupe

¹⁾ Mais pour lequel je ne connais pas de référence satisfaisante, en dehors du cas des formes paraboliques qui se traite facilement grâce à la théorie des *formes primitives* (« newforms ») d'Atkin-Lehner-Miyake-Casselman-Li.

$\text{Gal}(\mathbf{Q}(i, \sqrt[4]{12}), \mathbf{Q})$, groupe qui est isomorphe au groupe diédral \mathbf{D}_4 d'ordre 8 (E. Hecke, *Math. Werke*, p. 426 et 448); on a $\alpha = 3/4$.

4.5. *Remarques.* Il devrait être possible de préciser (i) en montrant que, si $f \neq 0$, il existe $\alpha > 0$ tel que

$$N \{ n \leq x : a_n \neq 0 \} \asymp x/\log^\alpha x,$$

et cela sans supposer que f soit fonction propre des opérateurs de Hecke. Peut-être y a-t-il même un développement asymptotique du genre

$$N \{ n \leq x : a_n \neq 0 \} = c_\alpha x/\log^\alpha x + c_\beta x/\log^\beta x + \dots \quad (0 < \alpha < \beta < \dots)?$$

Des questions analogues se posent pour $N \{ n \leq x : a_n = a \}$, où a est un nombre complexe non nul donné.

4.6. *Réduction mod \mathfrak{m} des formes de poids entier* (cf. [23]). — Soit $f = \sum a_n q^n$ une forme modulaire de poids entier $k \geq 1$ sur un sous-groupe de congruence de $\mathbf{SL}_2(\mathbf{Z})$. Supposons que les coefficients a_n de f appartiennent pour $n \geq 1$ à l'anneau O_F des entiers d'une extension finie F de \mathbf{Q} , et soit \mathfrak{m} un idéal non nul de O_F . L'analogie « mod \mathfrak{m} » de (4.2) est alors vrai, à de légères modifications près:

THÉORÈME 4.7.

(i) *Il existe $\alpha(\mathfrak{m}) > 0$ tel que*

$$N \{ n \leq x : a_n \not\equiv 0 \pmod{\mathfrak{m}} \} = O(x/\log^{\alpha(\mathfrak{m})} x).$$

(ii) *Supposons que f soit de type (k, ε) sur $\Gamma_0(N)$, soit fonction propre des T_p (pour $p \nmid N$) et des U_p (pour $p \mid N$), cf. [5], § 1, et que $a_1 = 1$. Supposons que \mathfrak{m} soit un idéal premier. Alors :*

(ii₁) *Si la caractéristique du corps O_F/\mathfrak{m} est différente de 2, ou s'il existe $p \nmid 2N$ tel que $a_p \not\equiv 0 \pmod{\mathfrak{m}}$, on a un développement asymptotique*

$$N \{ n \leq x : a_n \not\equiv 0 \pmod{\mathfrak{m}} \} = \frac{x}{\log^{\alpha(\mathfrak{m})} x} (c_0 + c_1/\log x + \dots)$$

avec $0 < \alpha(\mathfrak{m}) < 1$ et $c_0 > 0$.

(ii₂) *Si la caractéristique de O_F/\mathfrak{m} est 2, et si $a_p \equiv 0 \pmod{\mathfrak{m}}$ pour tout $p \nmid 2N$, il existe $c > 0$ tel que*

$$N \{ n \leq x : a_n \not\equiv 0 \pmod{\mathfrak{m}} \} \sim cx^{1/2}.$$

Comme pour (4.2), le cas (i) se ramène au cas (ii). Supposons donc que f satisfasse aux conditions (ii), ce qui entraîne en particulier que la fonction

$n \mapsto a_n$ est multiplicative. Soit l la caractéristique du corps O_F/m . D'après Deligne (cf. [4], ainsi que [5], § 6), il existe une extension galoisienne finie $K = K_{f,m}$ de \mathbf{Q} , non ramifiée en dehors de lN , et une représentation semi-simple

$$\rho_m: \text{Gal}(K/\mathbf{Q}) \rightarrow \text{GL}_2(O_F/m)$$

telles que, pour tout $p \nmid lN$, on ait

$$\text{Tr } \rho_m(\sigma_p(K/\mathbf{Q})) \equiv a_p \pmod{m}$$

et

$$\det \rho_m(\sigma_p(K/\mathbf{Q})) \equiv p^{k-1} \varepsilon(p) \pmod{m}.$$

[Cela revient à dire que, pour tout $p \nmid lN$, le p -ième facteur de la série de Dirichlet $\sum a_n n^{-s}$ est congru (mod m) au p -ième facteur de la « série L » de la représentation ρ_m , cette dernière étant considérée comme une série de Dirichlet formelle à coefficients dans O_F/m .]

Notons encore G l'image de ρ_m et H la partie de G formée des éléments de trace 0; on a $H \neq \emptyset$, car H contient l'image de la conjugaison complexe. Distinguons alors deux cas:

(ii₁) On a $H \neq G$. [C'est le cas si $l \neq 2$, car $1 \notin H$; c'est aussi le cas si $l = 2$, et si ρ_m n'est pas la représentation unité, ce qui revient aussi à dire qu'il existe $p \nmid 2N$ tel que $a_p \not\equiv 0 \pmod{m}$. Ce sont bien là les conditions de (ii₁).] Comme l'ensemble $P_{a,m}$ des p tels que $a_p \equiv 0 \pmod{m}$ est frobenien, et défini par H , on peut appliquer (3.4) avec $\alpha(m) = |H|/|G|$, et l'on obtient le développement asymptotique cherché.

(ii₂) On a $H = G$, ce qui signifie que $l = 2$, et que ρ_m est la représentation unité. On a alors

$$a_p \equiv 0 \pmod{m} \quad \text{et} \quad a_{p^2} \equiv 1 \pmod{m} \quad \text{pour tout } p \nmid 2N,$$

et l'on peut appliquer (2.10 b) avec $\delta = 0$, d'où le résultat cherché:

$$N \{ n \leq x : a_n \not\equiv 0 \pmod{m} \} \sim cx^{1/2}.$$

Exemples. Prenons $F = \mathbf{Q}$, de sorte que $O_F = \mathbf{Z}$ et $m = m\mathbf{Z}$, avec $m \geq 1$.

(4.8) Soit $\Phi(\mathbf{X}) = \Phi(X_1, \dots, X_{2k})$ une forme quadratique positive non dégénérée à $2k$ variables, et à coefficients entiers. Soit a_n le nombre de représentations de n par Φ , i.e. le nombre de points $\mathbf{x} \in \mathbf{Z}^{2k}$ tels que $\Phi(\mathbf{x}) = n$. On sait que la série

$$\theta_\Phi = \sum a_n q^n = \sum_{\mathbf{x}} q^{\Phi(\mathbf{x})}$$

est modulaire de poids k . On peut donc lui appliquer (4.7 i); en particulier, quel que soit $m \geq 1$, les a_n sont « presque toujours » divisibles par m .

(4.9) La série

$$\Delta = q \prod_{r=1}^{\infty} (1 - q^r)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n$$

satisfait aux hypothèses de (4.7 ii) avec $N = 1$, $\varepsilon = 1$, $k = 12$. Si m est premier $\neq 2$, elle est de type (ii₁), avec un exposant $\alpha(m)$ facile à déterminer (cf. § 1, exemple 3); on en déduit

$$N \{ n \leq x : \tau(n) \not\equiv 0 \pmod{m} \} = \frac{x}{\log^{\alpha(m)} x} (c_0 + c_1/\log x + \dots).$$

[Ce résultat était connu (cf. Watson [28]) pour $m = 3, 5, 7, 691$, car la représentation ρ_m correspondante est alors réductible, ce qui se traduit par une congruence (mod m) reliant $\tau(n)$ à l'une des fonctions élémentaires $\sigma_{r,s}(n)$, cf. [19], [27]; dans ce cas, ainsi que dans celui où $m = 23$, on pourrait même calculer explicitement les valeurs des constantes c_0, c_1, \dots , calcul qui paraît par contre fort difficile pour les autres valeurs de m , faute de renseignements sur les corps K_m qui interviennent, ainsi que sur leurs fonctions L d'Artin.]

Le cas $m = 2$ est exceptionnel: la représentation ρ_2 est la représentation unité, on se trouve dans le cas (ii₂). On a d'ailleurs

$$\tau(n) \equiv \begin{cases} 1 \pmod{2} & \text{si } n \text{ est un carré impair} \\ 0 \pmod{2} & \text{sinon,} \end{cases}$$

de sorte que

$$N \{ n \leq x : \tau(n) \not\equiv 0 \pmod{2} \} = \left[\frac{1}{2} (1 + \sqrt{x}) \right] = \frac{1}{2} \sqrt{x} + O(1),$$

en accord avec (4.7 ii₂).

Questions.

(4.10) Il devrait être possible de préciser (4.7 i) en donnant une estimation de

$$N \{ n \leq x : a_n \not\equiv 0 \pmod{m} \}$$

ou même un développement asymptotique modulo $O(x/\log^N x)$, N arbitraire, de

$$N \{ n \leq x : a_n \equiv \lambda \pmod{m} \} \quad \text{pour } \lambda \text{ donné.}$$

Lorsque $n \mapsto a_n$ est multiplicative, Delange m'a signalé que l'on peut résoudre affirmativement la première question, en utilisant la méthode de [3], §§ 4, 5 (cf. exerc. 6.8, ainsi que Scourfield [17], [18]). L'estimation obtenue est

$$N \{ n \leq x : a_n \not\equiv 0 \pmod{m} \} \sim cx (\log \log x)^h / \log^\alpha x,$$

avec $c > 0$, $\alpha > 0$, h entier ≥ 0 (mis à part un cas exceptionnel, analogue à (4.7 ii₂), où l'on a une majoration en $x^{1/2}$).

Le cas général devrait être analogue, à cela près qu'il y intervient, non seulement les $x (\log \log x)^h / \log^\alpha x$, mais aussi leurs produits par les termes oscillants

$$\cos(\gamma \log \log x) \quad \text{et} \quad \sin(\gamma \log \log x), \quad \gamma \in \mathbf{R}.$$

On trouvera dans les exercices du § 6 quelques résultats dans cette direction.

(4.11) Soit $f = \sum a_n q^n$ une forme parabolique de type (4.7 ii), de poids $k \geq 2$, et à coefficients dans \mathbf{Z} . Écartons le cas « à multiplication complexe » où il existe un caractère ϖ d'ordre 2 tel que $\varpi(p) = -1$ entraîne $a_p = 0$; cela revient à demander que les représentations l -adiques attachées à f aient pour images des sous-groupes *ouverts* de \mathbf{GL}_2 . On devrait alors pouvoir montrer que l'ensemble des n tels que $a_n \neq 0$ a une densité > 0 , contrairement à ce qui se passe pour $k = 1$. Il est d'ailleurs plus intéressant de se poser la question de la *nullité*, et de la *croissance*, des a_p , pour p premier. D'après Deligne on a

$$|a_p| \leq 2p^{(k-1)/2}.$$

On sait d'autre part que l'ensemble des p tels que $a_p = 0$ est de densité 0 (cf. [19], 4.4). Des arguments probabilistes simples (qui m'ont été signalés par Atkin) rendent vraisemblable ¹⁾ la minoration

$$(4.11_k?) \quad |a_p| \gg p^{(k-3)/2-\varepsilon} \quad (\text{si } k \geq 4)$$

pour tout $\varepsilon > 0$, minoration qui entraînerait que a_p tend vers l'infini en valeur absolue, et ne peut donc s'annuler qu'un nombre fini de fois. Pour $k = 2, 3$, des arguments analogues suggèrent:

$$(4.11_2?) \quad N \{ p \leq x : a_p = 0 \} \asymp x^{1/2} / \log x \quad (\text{si } k = 2)$$

$$(4.11_3?) \quad N \{ p \leq x : a_p = 0 \} \asymp \log \log x \quad (\text{si } k = 3).$$

¹⁾ Si l'on écrit a_p sous la forme $2p^{(k-1)/2} \cos \varphi_p$, avec $0 \leq \varphi_p < \pi$, (4.11_k?) équivaut à dire que $|\varphi_p - \pi/2| \gg 1/p^{1+\varepsilon}$, autrement dit que φ_p ne s'approche « pas trop » de $\pi/2$.

On trouvera dans Lang-Trotter [9] une étude numérique du cas $k = 2$, ainsi qu'une conjecture plus précise que (4.11₂ ?), à savoir :

$$(4.11_2 \text{ ??}) \quad N \{ p \leq x : a_p = 0 \} \sim cx^{1/2}/\log x \quad (\text{si } k = 2),$$

avec une valeur explicite de c .

(4.12) On peut se demander si (4.2 i) et (4.7 i) restent valables lorsque $f = \sum a_n q^n$ est une forme modulaire sur un sous-groupe d'indice fini de $SL_2(\mathbb{Z})$ qui n'est pas un sous-groupe de congruence (il est alors raisonnable de supposer, non plus que les a_n sont entiers, mais que ce sont des « S -entiers »). On manque d'exemples.

(4.13) Il est probable que l'on ne peut pas étendre (4.7 i) aux formes de poids demi-entier, du moins en dehors des deux cas suivants

(a) O_F/m est de caractéristique 2: en effet, on se ramène alors au cas d'un poids entier en multipliant f par la série

$$\theta = 1 + 2q + 2q^4 + 2q^9 + \dots$$

qui est congrue à 1 (mod 2);

(b) la forme $f = \sum a_n q^n$ est de poids 1/2: on peut alors montrer qu'il existe des entiers t_1, \dots, t_r tels que $a_n = 0$ si n n'est pas produit de l'un des t_i par un carré; cela entraîne

$$N \{ n \leq x : a_n \neq 0 \} = O(x^{1/2}).$$

Il serait par exemple intéressant de voir ce qui se passe pour la forme modulaire $\theta^3 = \sum r_3(n) q^n$: comment se répartissent les $r_3(n)$ modulo 3, 5, etc ?

§ 5. DIVISIBILITÉ DES COEFFICIENTS DE j

5.1. Rappelons que l'invariant modulaire j est défini par $j = Q^3/\Delta$, où $Q = E_4 = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n$, $\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$. On a

$$j = q^{-1} + 744 + 196884q + \dots = \sum_{n=-1}^{\infty} c(n) q^n.$$

Les résultats du § 4 ne s'appliquent pas directement à j , car j a un pôle simple à l'infini, et n'est donc pas une « forme » modulaire. J'ignore d'ailleurs si les $c(n)$ sont presque toujours divisibles par tout entier donné; c'est peu probable. On peut toutefois obtenir des renseignements sur certains des $c(n)$ grâce au résultat suivant:

THÉORÈME 5.2. Soit l un nombre premier. Alors :

(a) Les séries

$$j' = \sum c(ln) q^n \quad \text{et} \quad j'' = \sum_{n \equiv 0 \pmod{l}} c(n) q^n$$

sont des formes modulaires l -adiques de poids 0, au sens de [21], § 1.

(b) Si $l \neq 2$, il en est de même de la série

$$j_- = \sum_{\left(\frac{-n}{l}\right) = -1} c(n) q^n.$$

(c) Si $l = 2$, il en est de même des trois séries

$$j_i = \sum_{n \equiv i \pmod{8}} c(n) q^n \quad (i = 1, 3, 5).$$

[Dans (b), la sommation porte sur les n premiers à l qui sont résidus quadratiques $(\text{mod } l)$ si $l \equiv -1 \pmod{4}$, et non résidus si $l \equiv 1 \pmod{4}$. Dans les deux cas, cela exclut $n = -1$. Si $l = 2$, la même remarque s'applique aux j_i , pour $i = 1, 3, 5$.]

Si f est une forme modulaire l -adique, et r un entier > 0 , il existe une forme modulaire au sens usuel, à coefficients entiers, qui est congrue à f modulo l^r . En appliquant (4.7 i) à cette forme, on obtient :

COROLLAIRE 5.3. Pour tout l premier $\neq 2$, et tout r , il existe $\alpha > 0$ tel que

$$N \left\{ x \leq n : c(n) \not\equiv 0 \pmod{l^r} \text{ et } \left(\frac{n}{l}\right) \neq \left(\frac{-1}{l}\right) \right\} = O(x/\log^\alpha x).$$

On trouvera d'autres applications de (5.2) dans les exercices du § 6.

Démonstration de (5.2).

(a) Le fait que $j' = j | U$ soit modulaire l -adique de poids 0 est dû à Deligne, cf. par exemple [21], p. 228. Comme $j'' = j' | V$, il en est de même de j'' ([21], th. 4, p. 209).

(b) Soit $n \mapsto \varepsilon(n) = \left(\frac{n}{l}\right)$ le caractère de Legendre, et notons j_ε la série déduite de j par « torsion » au moyen de ε , i.e.

$$j_\varepsilon = \sum_{n=-1}^{\infty} \varepsilon(n) c(n) q^n.$$

On a

$$2j_- = j - \left(\frac{-1}{l}\right) j_\varepsilon - j'' ,$$

et il suffit donc de montrer que $g = j - \left(\frac{-1}{l}\right) j_\varepsilon$ est modulaire l -adique de poids 0. Cela peut se faire de la manière suivante (pour une autre méthode, voir exerc. 6.15): tout d'abord, un argument standard, basé sur le fait que $\varepsilon^2 = 1$, montre que j_ε est une fonction modulaire de poids 0 sur le groupe $\Gamma_0(l^2)$, holomorphe en dehors des pointes. Il est donc de même de g ; de plus, le développement en série de g montre que g n'a pas de pôle à la pointe ∞ . Le fait que g soit modulaire l -adique résulte alors du théorème général suivant:

THÉORÈME 5.4. *Soit $g = \sum a_n q^n$ une fonction modulaire de poids k sur $\Gamma_0(l^m)$, à coefficients $a_n \in \mathbf{Q}$. On suppose que g est holomorphe dans le demi-plan $\mathcal{I}(z) > 0$, ainsi qu'à la pointe ∞ (i.e. $a_n = 0$ si $n < 0$). Alors g est une forme modulaire l -adique de poids k sur $\mathbf{SL}_2(\mathbf{Z})$.*

Commençons par le cas particulier où g est une forme modulaire de poids $k \geq 4$, et où les coefficients a_n sont l -entiers. On raisonne alors par récurrence sur m . Le cas $m = 1$ est traité dans [21], n° 3.2. Si $m \geq 2$, définissons des formes modulaires f_i, g_i de poids kl^i ($i \geq 0$) au moyen des formules de récurrence:

$$f_0 = 0, \quad g_0 = g, \quad f_i = (g_{i-1})^l | U, \quad g_i = \frac{1}{l} (E_{kli-1(l-1)} g_{i-1} - f_i) \quad (i \geq 1).$$

(Rappelons que E_r désigne la série d'Eisenstein de poids r normalisée de telle sorte que son terme constant soit 1; on a $E_r \equiv 1 \pmod{l^{a+1}}$ si r est divisible par $l^a(l-1)$.)

On vérifie tout de suite que les coefficients des f_i et g_i sont l -entiers. De plus, les f_i sont des formes modulaires sur $\Gamma_0(l^{m-1})$, car il est bien connu que si $m \geq 2$, l'opérateur U fait passer de $\Gamma_0(l^m)$ à $\Gamma_0(l^{m-1})$. Vu l'hypothèse de récurrence, les f_i sont donc des formes modulaires l -adiques de poids kl^i .

Pour tout $i \geq 0$, posons

$$A_i = \prod_{a=i}^{\infty} E_{kla(l-1)},$$

le produit infini ayant un sens du fait que $E_{kla(l-1)}$ est congru à 1 $\pmod{l^{a+1}}$. La série A_i est une forme modulaire l -adique de poids

$$\sum_{a=i}^{\infty} kl^a(l-1) = (0, -kl^i) \quad \text{dans} \quad \mathbf{Z}/(l-1)\mathbf{Z} \times \mathbf{Z}_l.$$

On vérifie sans peine l'identité

$$A_0 g = A_1 f_1 + l A_2 f_2 + \dots + l^{i-1} A_i f_i + \dots$$

Les séries $A_i f_i$ sont modulaires l -adiques de poids

$$(0, -kl^i) + (kl^i, kl^i) = (kl^i, 0) = (k, 0).$$

Il en résulte que $A_0 g$ est modulaire l -adique de poids $(k, 0)$. Mais le fait que $A_0 \equiv 1 \pmod{l}$ entraîne que $A_0^{-1} = \lim_{s \rightarrow \infty} A_0^{l^s - 1}$ est modulaire l -adique de poids $(0, k)$. Comme $g = A_0^{-1} (A_0 g)$, on voit bien que g est modulaire l -adique de poids $(k, k) = k$, ce qui démontre (5.4) dans le cas particulier considéré.

Passons au cas général. Si N est assez grand, la fonction $g' = \Delta^N g$ est holomorphe en toutes les pointes, et son poids $k' = k + 12N$ est ≥ 4 . C'est donc une forme modulaire, et ses coefficients a'_n ont des dénominateurs bornés (cf. [5], prop. 2.7 ou bien [25], Th. 3.52). Quitte à la multiplier par une puissance de l , on peut donc s'arranger pour que ses coefficients soient l -entiers. D'après ce que l'on vient de voir, c'est donc une forme modulaire l -adique de poids $k + 12N$ sur $\mathrm{SL}_2(\mathbf{Z})$. De plus, ses coefficients a'_n sont nuls pour $n < N$. Le fait que $g = g'/\Delta^N$ soit modulaire l -adique résulte alors du lemme élémentaire suivant (appliqué N fois):

LEMME 5.5. Soit $G = \sum_{n=0}^{\infty} c_n q^n$ une forme modulaire l -adique de poids K . Si $c_0 = 0$, la série $H = G/\Delta$ est une forme modulaire l -adique de poids $K - 12$.

Par hypothèse, G est limite de formes modulaires usuelles G_i , de poids K_i tendant vers K (au sens de [21], § 1). Les termes constants $c_{0,i}$ des G_i tendent vers 0. Choisissons, pour chaque i , un monôme M_i en les séries d'Eisenstein $Q = E_4$ et $R = E_6$ qui soit de poids K_i . On peut alors écrire G_i sous la forme

$$G_i = c_{0,i} M_i + \Delta H_i,$$

où H_i est une forme modulaire de poids $K_i - 12$. On a

$$\lim . \Delta H_i = G = \Delta H, \quad \text{d'où} \quad \lim . H_i = H,$$

ce qui montre bien que H est modulaire l -adique de poids $K - 12$.

(c) Si $l = 2$, notons $\varepsilon, \varphi, \psi$ les trois caractères d'ordre 2 de $(\mathbf{Z}/8\mathbf{Z})^*$, et soient $j_\varepsilon, j_\varphi, j_\psi$ les séries déduites de j par torsion au moyen de $\varepsilon, \varphi, \psi$. On a

$$4j_i = j - j'' + \varepsilon(i)j_\varepsilon + \varphi(i)j_\varphi + \psi(i)j_\psi.$$

Le même argument que dans (b) montre que les j_i sont des fonctions modulaires sur $\Gamma_0(2^6)$, puis, en appliquant (5.4), que ce sont des formes modulaires 2-adiques de poids 0 sur $\mathrm{SL}_2(\mathbf{Z})$.

Remarques.

(a) On peut aussi déduire (5.4) et (5.5) de la définition « géométrique » des formes modulaires l -adiques adoptée par Katz dans son exposé à Anvers (*Lect. Notes* 350, p. 69-190).

(b) Le théorème (5.2) « explique » que l'on ait des congruences sur $c(n) \pmod{l}$ lorsque n est, soit divisible par l , soit tel que $\binom{n}{l} = -\binom{-1}{l}$, cf. Kolberg [7], ainsi que les exercices du § 6.

(c) Lorsque $l = 2$, on a $j_1 \equiv j_3 \equiv j_5 \equiv j' \equiv j'' \equiv 0 \pmod{2}$, de sorte que

$$j \equiv \sum_{n=0}^{\infty} c(8n-1) q^{8n-1} \pmod{2},$$

et le théorème (5.2) ne fournit aucun renseignement sur ces coefficients $\pmod{2}$. Il serait intéressant de voir s'ils sont répartis « au hasard », comme cela semble le cas pour la fonction de partition, cf. [13].

§ 6. EXERCICES

Formes modulaires de poids 1.

(6.1) Les hypothèses étant celles de (4.2 ii), montrer que $\alpha \leq 3/4$, et qu'il y a égalité si et seulement si l'image de $\mathrm{Gal}(K_f/\mathbf{Q})$ dans $\mathbf{PGL}_2(\mathbf{C}) = \mathbf{GL}_2(\mathbf{C})/\mathbf{C}^*$ est isomorphe au groupe diédral \mathbf{D}_2 d'ordre 4 (cf. exemple (4.4)).

(6.2) On suppose que f est de type $(1, \varepsilon)$ sur $\Gamma_0(N)$ (mais pas nécessairement que c'est une fonction propre des opérateurs de Hecke). Montrer que, si

$$(*) \quad N \{ n \leq x : a_n \neq 0 \} = o(x/\log^{3/4} x),$$

on a $f = 0$. (Observer que l'espace des f satisfaisant à (*) est stable par les opérateurs de Hecke; s'il n'est pas nul, il contient un vecteur propre; conclure en appliquant (6.1).)

Formes modulaires (mod m).

(6.3) Montrer que, sous les hypothèses de (4.7 ii₁), on a $\alpha(m) \leq 3/4$ (même méthode que pour (6.1)). En déduire un résultat analogue à (6.2).

(6.4) On fixe k, m, N, ε et l'on note m la norme de m . Soit A l'ensemble des séries formelles $\sum a_n q^n$, à coefficients dans O_F/m , qui sont réduction (mod m) de formes modulaires de type (k, ε) sur $\Gamma_0(N)$, à coefficients dans O_F ; c'est un O_F/m -module libre de type fini. Les opérateurs de Hecke T_n définissent des endomorphismes $T_{n,A}$ de A . Montrer que l'application $p \mapsto T_{p,A}$ est *frobénienne* au sens suivant: pour tout $u \in \text{End}(A)$, l'ensemble P_u des nombres premiers p , ne divisant pas Nm , tels que $T_{p,A} = u$ est frobénien (et peut être défini par une extension galoisienne finie de \mathbf{Q} non ramifiée en dehors de Nm). Soit P_2^+ l'ensemble des $p \equiv 1 \pmod{Nm}$ qui appartiennent à P_2 (i.e. tels que $f | T_p = 2f$ pour tout $f \in A$), et soit P_0^- l'ensemble des $p \equiv -1 \pmod{Nm}$ qui appartiennent à P_0 (i.e. tels que $f | T_p = 0$ pour tout $f \in A$). Montrer que P_2^+ et P_0^- ont une densité > 0 (cf. [5], 9.6, où est traité le cas analogue des formes de poids 1). Si $p \in P_2^+$, on a $T_{p^r,A} = r + 1$, et si $p \in P_0^-$, on a $T_{p^r,A} = (-1)^{r/2}$ si r est pair, et $T_{p^r,A} = 0$ si r est impair. Si $f = \sum a_n q^n$ est un élément de A , on a donc

$$(n, p) = 1 \Rightarrow \begin{cases} a_{np^r} = (r+1)a_n & \text{si } p \in P_2^+ \\ a_{np^r} = \begin{cases} 0 & \text{si } p \in P_0^-, \quad r \text{ impair} \\ (-1)^{r/2} a_n & \text{si } p \in P_0^-, \quad r \text{ pair.} \end{cases} \end{cases}$$

(6.5) On conserve les notations de (6.4). Soit $f = \sum a_n q^n$ un élément de A . Montrer, en utilisant les dernières formules de (6.4), que l'ensemble des valeurs prises par les a_n ($n \geq 1$) est un sous-ensemble de O_F/m stable par multiplication par \mathbf{Z} . (En particulier, si $O_F = \mathbf{Z}$ et si l'un des a_n est inversible dans $\mathbf{Z}/m\mathbf{Z}$, alors les a_n prennent toutes les valeurs possibles.) Si a appartient à ce sous-ensemble, et si $2 \nmid m$, on a

$$N \{ n \leq x : a_n = a \text{ dans } O_F/m \} \gg x (\log \log x)^h / \log x$$

quel que soit h . (Choisir $r \geq 1$ tel que $a_r = 2^{-h-1} a$, et remarquer que $a_n = a$ lorsque n est de la forme $p_0 \dots p_h r$, où p_0, \dots, p_h sont des éléments de P_2^+ ne divisant pas r , et deux à deux distincts.)

Formes modulaires (mod 2).

(6.6) Soit S la \mathbf{F}_2 -algèbre des formes modulaires (mod 2) sur $\text{SL}_2(\mathbf{Z})$, autrement dit (cf. [21], [27]) l'algèbre des polynômes en la série

$$\tilde{\Delta} = q + q^9 + q^{25} + q^{49} + \dots,$$

à coefficients dans \mathbf{F}_2 . Soit S_0 (resp. S_1) le sous-espace de S engendré par les $\tilde{\Delta}^i$ pour $i \geq 1$ (resp. par les $\tilde{\Delta}^{2^j}$, pour $j \geq 0$); on a $S = \mathbf{F}_2 \oplus S_0$. Soit $f = \sum a_n q^n$ un élément de S_0 .

(a) Montrer que, si $f \in S_1$ et $f \neq 0$, il existe $c > 0$ tel que

$$N \{ n \leq x : a_n = 1 \} \sim cx^{1/2}.$$

(b) On peut prouver (cf. [22]) que les T_p sont *localement nilpotents* sur S_0 . Admettant ce fait, il existe un entier $h \geq 0$ tel que f soit annulé par tous les produits $T_{p_0} \dots T_{p_h}$, p_i premier $\neq 2$. Montrer que $a_n = 1$ entraîne que n est de la forme bc^2 , où b a au plus h facteurs premiers $\neq 2$ (raisonner par récurrence sur h et n). En déduire:

$$N \{ n \leq x : a_n = 1 \} \ll x (\log \log x)^{h-1} / \log x.$$

(c) On suppose $f \notin S_1$, et l'on choisit l'entier h de (b) *minimal*; on a $h \geq 1$. Il résulte alors de (6.4) qu'il existe des ensembles frobénieniens P_1, \dots, P_h de densités > 0 , ainsi qu'un élément non nul g de S_0 , tels que

$$f | T_{p_1} \dots T_{p_h} = g \quad \text{si} \quad p_1 \in P_1, \dots, p_h \in P_h.$$

Si le r -ième coefficient de g est égal à 1, on a $a_n = 1$ pour tout n de la forme $p_1 \dots p_h r$, avec $p_i \in P_i$, les p_i étant distincts, et ne divisant pas r . En conclure que

$$N \{ n \leq x : a_n = 1 \} \gg x (\log \log x)^{h-1} / \log x,$$

d'où, en vertu de (b):

$$N \{ n \leq x : a_n = 1 \} \asymp x (\log \log x)^{h-1} / \log x.$$

(d) Il résulte de (a) et (c) que $f \in S_1$ équivaut à

$$N \{ n \leq x : a_n = 1 \} = o(x / \log x)$$

ainsi qu'à

$$N \{ n \leq x : a_n = 1 \} = O(x^{1/2}).$$

(6.7) On pose $\Delta^3 = \sum e_n q^n$, et l'on note E l'ensemble des n tels que $e_n \equiv 0 \pmod{2}$. Montrer que le complémentaire E' de E est formé des entiers n de la forme $p^{4m+1} a^2$, avec p premier, a impair non divisible par p , m entier ≥ 0 , et $p \equiv 3 \pmod{8}$. (Utiliser la congruence

$$\Delta \equiv \sum_{n=0}^{\infty} q^{(2n+1)^2} \pmod{2}.)$$

La série de Dirichlet $f(s) = \sum_{n \in E'} n^{-s}$ associée à E' est égale à

$$(1 - 2^{-2s}) \zeta(2s) \left\{ \sum_{p \equiv 3 \pmod{8}} p^{-s} / (1 + p^{-2s}) \right\}.$$

On peut l'écrire sous la forme

$$f(s) = c \log 1/(s-1) + h(s),$$

où h est holomorphe pour $\Re(s) \geq 1$, et $c = \pi^2/32$. En déduire (grâce au théorème *b* de [3], p. 26), que l'on a

$$N \{ n \leq x : e_n \equiv 1 \pmod{2} \} \sim cx / \log x.$$

Montrer que

$$\Delta^3 \mid T_p \equiv \begin{cases} \Delta \pmod{2} & \text{si } p \equiv 3 \pmod{8} \\ 0 \pmod{2} & \text{sinon.} \end{cases}$$

Montrer que les mêmes résultats valent pour Δ^5 , à condition de remplacer $p \equiv 3 \pmod{8}$ par $p \equiv 5 \pmod{8}$.

Divisibilité des a_n par une puissance d'un idéal premier.

(6.8) Soit $n \mapsto a_n$ une fonction multiplicative à valeurs dans l'anneau O_F des entiers d'une extension finie F de \mathbf{Q} , et soit v la valuation de F définie par un idéal premier $\mathfrak{p} \neq 0$ de O_F . Pour tout $r \geq 0$, notons N_r (resp. P_r) l'ensemble des entiers $n \geq 1$ (resp. des nombres premiers) tels que $v(a_n) = r$, et posons

$$f_r(s) = \sum_{n \in N_r} n^{-s} \quad \text{et} \quad f_T(s) = \sum_{r=0}^{\infty} T^r f_r(s),$$

où T est une indéterminée.

(a) Montrer que

$$f_T(s) = \prod_p \left(1 + \sum_{m=1}^{\infty} T^{v(a_{p^m})} p^{-ms} \right),$$

où l'on convient de supprimer le coefficient de p^{-ms} si $v(a_{p^m}) = \infty$, i.e. si $a_{p^m} = 0$.

En déduire que

$$f_T(s) = \exp \left\{ \sum_{r=0}^{\infty} T^r (\varphi_{P_r}(s) + \theta_r(s)) \right\},$$

où $\varphi_{P_r}(s) = \sum_{p \in P_r} p^{-s}$, et où les $\theta_r(s)$ sont holomorphes pour $\Re(s) > 1/2$.

(b) On suppose que les P_r sont réguliers de densité $\alpha_r \geq 0$ et que $0 < \alpha_0 < 1$; on note m la borne inférieure des $i \geq 1$ tels que $\alpha_i > 0$. Montrer que $f_r(s)$ est de la forme

$$f_r(s) = \frac{1}{(s-1)^{\alpha_0}} \left\{ \sum_{j=0}^{h(r)} c_{r,j}(s) (\log 1/(s-1))^j \right\},$$

où $h(r)$ est la partie entière de r/m , et où les $c_{r,j}(s)$ sont holomorphes pour $\Re(s) \geq 1$. Cela entraîne:

$$f_0(s) + \dots + f_r(s) = \frac{1}{(s-1)^{\alpha_0}} \left\{ \sum_{j=0}^{h(r)} d_{r,j}(s) (\log 1/(s-1))^j \right\},$$

où les $d_{r,j}(s)$ sont holomorphes pour $\Re(s) \geq 1$. Montrer que l'on a $d_{r,j}(1) > 0$ pour $j = h(r)$. En déduire, grâce au théorème b de [3], p. 26, que

$$N \{ n \leq x : a_n \not\equiv 0 \pmod{p^{r+1}} \} \sim c_r x (\log \log x)^{h(r)} / \log^{1-\alpha_0} x,$$

avec $c_r = d_{r,j}(1) / \Gamma(\alpha_0)$.

(c) On suppose que les a_n sont les coefficients d'une forme modulaire de type (4.7 ii₁). Montrer que les conditions de (b) sont satisfaites (les P_r sont même frobéniens) et que l'on a

$$\alpha_0 + \alpha_1 + \dots + \alpha_r + \dots = 1 - \alpha_\infty,$$

où α_∞ est la densité des p tels que $a_p = 0$.

(d) Etendre les résultats ci-dessus au cas de produits de puissances $p_1^{r_1} \dots p_j^{r_j}$ d'idéaux premiers (utiliser des séries formelles en T_1, \dots, T_j).

(6.9) Soit l un nombre premier $\neq 2$. Soit $P_1(l)$ l'ensemble des nombres premiers $p \neq l$ tels que $\tau(p)$ soit divisible par l , mais pas par l^2 . Montrer que $P_1(l)$ est de densité > 0 . [Soit G_l le sous-groupe de $\mathbf{GL}_2(\mathbf{Q}_l)$ image de la représentation l -adique attachée à Δ , cf. [19], [27]. La densité de $P_1(l)$ est égale à la mesure de l'ouvert H_l de G_l formé des éléments s tels que $v_l(\text{Tr}(s)) = 1$; il revient au même de prouver que $H_l \neq \emptyset$, que $P_1(l) \neq \emptyset$, ou que la densité de $P_1(l)$ est > 0 . Or, on a $H_l \neq \emptyset$ pour $l \neq 3, 5, 7, 23, 691$, vu la « grosseur » de G_l , cf. [27]. Pour $l = 3, 7, 23$, on a $5 \in P_1(l)$ puisque $\tau(5) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 23$; pour $l = 5$, on a $19 \in P_1(l)$ puisque $\tau(19) = 2^2 \cdot 5 \cdot 7^2 \cdot 11 \cdot 23 \cdot 43$; pour $l = 691$, un calcul sur machine montre, paraît-il, que $1381 \in P_1(l)$.]

Déduire de là, et de l'exercice précédent, que, pour tout $r \geq 0$, il existe une constante $c_{l,r} > 0$ telle que

$$N \{ n \leq x : \tau(n) \not\equiv 0 \pmod{l^{r+1}} \} \sim c_{l,r} x (\log \log x)^r / \log^{\alpha(l)} x,$$

où $\alpha(l)$ est donné par la formule de l'exemple 3 du § 1.

Equidistribution des valeurs des $a_n \pmod{m}$.

(6.10) Soit $n \mapsto a_n$ une fonction multiplicative à valeurs dans un anneau commutatif fini A . On note r l'ordre du groupe multiplicatif A^* des éléments inversibles de A . Si $\lambda \in A^*$, on note P_λ l'ensemble des nombres premiers p tels que $a_p = \lambda$. On fait les hypothèses suivantes :

(i) Les P_λ sont réguliers de densités α_λ telles que

$$0 < \sum \alpha_\lambda < 1.$$

(ii) Le groupe A^* est engendré par les éléments λ tels que $\alpha_\lambda > 0$.

On note X le groupe des caractères de A^* ; un élément φ de X est un homomorphisme de A^* dans \mathbf{C}^* ; on le prolonge à A en posant $\varphi(\lambda) = 0$ si λ n'est pas inversible.

(a) Si $\lambda \in A^*$ et $\varphi \in X$, on pose

$$f_\lambda(s) = \sum_{a_n = \lambda} n^{-s} \quad \text{et} \quad f_\varphi(s) = \sum_n \varphi(a_n) n^{-s}.$$

Montrer que

$$f_\lambda = \frac{1}{r} \sum_{\varphi \in X} \varphi(\lambda^{-1}) f_\varphi.$$

(b) Décomposer f_φ en produit eulérien, et en déduire que

$$\log f_\varphi(s) = \beta(\varphi) \log 1/(s-1) + h_\varphi(s),$$

où $\beta(\varphi) = \sum_\lambda \alpha_\lambda \varphi(\lambda)$, et $h_\varphi(s)$ est holomorphe pour $\Re(s) \geq 1$.

On a $\Re(\beta(\varphi)) \leq \alpha$, avec $\alpha = \sum \alpha_\lambda$, et il n'y a égalité que si φ est le caractère unité de A^* .

(c) Si β est un nombre complexe, on convient de noter $1/(s-1)^\beta$ la fonction $\exp \{ \beta \log 1/(s-1) \}$. Montrer, en combinant (a) et (b), que l'on a

$$f_\lambda(s) = c(s)/(s-1)^\alpha + \sum_i c_{i,\lambda}(s)/(s-1)^{\beta_i},$$

où $c(s)$ et les $c_{i,\lambda}(s)$ sont holomorphes pour $\Re(s) \geq 1$, les β_i sont tels que $\Re(\beta_i) < \alpha$, et $c(1) > 0$.

En déduire (cf. [3], p. 25, th. a) que

$$N \{ n \leq x : a_n = \lambda \} \sim cx / \log^{1-\alpha} x,$$

avec $c = c(1) / \Gamma(\alpha) > 0$. (Noter que c est indépendant de λ : il y a *équidistribution* des valeurs de (a_n) dans Λ^* .)

(d) Appliquer la méthode de Landau aux f_λ et f_φ , en supposant les P_λ frobénien. En déduire, pour tout $N \geq 1$, un développement asymptotique de $N \{n \leq x : a_n = \lambda\}$ modulo $O(x/\log^N x)$.

(e) Énoncer et démontrer des résultats analogues pour

$$N \{n \leq x : a_n^{(1)} = \lambda_1, \dots, a_n^{(r)} = \lambda_n\},$$

où les $a_n^{(i)}$ sont des fonctions multiplicatives à valeurs dans des anneaux commutatifs finis A_i . (Se ramener au cas d'une suite unique à valeurs dans $\Lambda = A_1 \times \dots \times A_r$.)

(6.11) Soit m un entier impair ≥ 3 . On considère la fonction multiplicative

$$n \mapsto \tau(n) \pmod{m}, \text{ à valeurs dans } \Lambda = \mathbf{Z}/m\mathbf{Z}.$$

Montrer que la condition (i) de (6.10) est satisfaite, et qu'il en est de même de (ii) pourvu que m ne soit pas divisible par 7. [On peut supposer que m est une puissance d'un nombre premier l , cf. [19], 4.2. Il faut alors vérifier que, si $l \neq 2, 7$, les $\tau(p)$, p premier $\neq l$, qui ne sont pas divisibles par l engendrent le groupe multiplicatif $(\mathbf{Z}/l^2\mathbf{Z})^*$. Pour $l \neq 3, 5, 23$ et 691 , cela résulte de ce que $\tau(p)$ peut prendre n'importe quelle valeur modulo l^2 , cf. [27]. Pour $l = 3, 5, 23, 691$, remarquer que le sous-groupe de $(\mathbf{Z}/l^2\mathbf{Z})^*$ engendré par les $\tau(p)$, $p \neq l$, se projette *sur* $(\mathbf{Z}/l\mathbf{Z})^*$ et contient 2 d'après (6.4); utiliser alors le fait connu que $2^{l-1} \not\equiv 1 \pmod{l^2}$ pour $l < 1093$.]

En déduire l'équidistribution des valeurs de $\tau(n)$ appartenant à $(\mathbf{Z}/m\mathbf{Z})^*$, lorsque m n'est pas divisible par 7.

(6.12) Montrer qu'il existe deux constantes c_+, c_- , avec $c_+ > c_- > 0$ telles que

$$N \{n \leq x : \tau(n) \equiv \lambda \pmod{7}\} \sim \begin{cases} c_+ x / \log^{1/2} x & \text{si } \left(\frac{\lambda}{7}\right) = 1 \\ c_- x / \log^{1/2} x & \text{si } \left(\frac{\lambda}{7}\right) = -1. \end{cases}$$

(Utiliser une méthode analogue à celle de (6.10).)

Exemple de minoration de $|a_p|$ pour $p \rightarrow \infty$.

(6.13) Soit $\alpha \mapsto \chi(\alpha)$ un caractère de Hecke d'un corps imaginaire quadratique K . Soit f le conducteur de χ . On suppose que χ est d'exposant entier $d \geq 1$, autrement dit que

$\chi((z)) = z^d$ pour tout $z \in K^*$ tel que $z \equiv 1 \pmod{\times \mathfrak{f}}$.

Posons

$$\sum_{\mathfrak{a}} \chi(\mathfrak{a}) q^{N(\mathfrak{a})} = \sum a_n q^n,$$

de sorte que

$$\sum a_n n^{-s} = L(s, \chi) = \prod_{\mathfrak{p} \notin \mathfrak{f}} (1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s})^{-1}.$$

On sait que la série $\sum a_n q^n$ est une forme modulaire parabolique de poids $k = 1 + d$ et que c'est une fonction propre des opérateurs de Hecke. Si ω est le caractère d'ordre 2 qui correspond à K , on a $a_n = 0$ si $\omega(n) = -1$.

Soit P l'ensemble des nombres premiers p ne divisant pas $N(\mathfrak{f})$, et tels que $\omega(p) = 1$. Si $p \in P$, on a

$$a_p = \chi(\mathfrak{p}) + \chi(\bar{\mathfrak{p}}),$$

où \mathfrak{p} et $\bar{\mathfrak{p}}$ sont les idéaux premiers de O_K divisant p . Montrer que

$$|a_p| \gg p^{(k-3)/2-\varepsilon} \text{ pour tout } \varepsilon > 0.$$

[On peut se restreindre au cas où \mathfrak{p} est contenu dans la classe mod $N(\mathfrak{f})$ d'un idéal fixe \mathfrak{a} . Si l'on écrit alors $\mathfrak{p} = \mathfrak{a}(z)$, avec $z \equiv 1 \pmod{\times N(\mathfrak{f})}$, on a $a_p = \chi(\mathfrak{a}) z^d + \chi(\bar{\mathfrak{a}}) \bar{z}^d = A_d(x, y)$, où x, y sont les coordonnées de z par rapport à une \mathbf{Z} -base de \mathfrak{a}^{-1} , et où A_d est un polynôme homogène de degré d . Les coefficients de A_d sont des nombres algébriques, et A_d n'a aucun facteur multiple. D'après le théorème de Roth, on a

$$A_d(x, y) \gg (\sup(|x|, |y|))^{d-2-\varepsilon} \text{ pour } x, y \text{ premiers entre eux,}$$

d'où aussitôt le résultat cherché.]

Soit δ un nombre > 0 tel que, pour tout secteur angulaire de C de largeur $\sim 1/N$, il existe $p \ll N^\delta$ tel que l'élément z correspondant appartienne au secteur angulaire donné. (D'après Kovalčik, *Dokl.*, t. 219, 1974, on peut prendre pour δ tout nombre > 4 .) Montrer qu'il existe alors une constante $c > 0$ telle que

$$|a_p| \leq c p^{(k-1)/2-1/\delta}$$

pour une infinité de p tels que $\omega(p) = 1$.

Passage des fonctions modulaires aux formes modulaires.

(6.14) Soit $f = \sum_{n \geq -r} a_n q^n$ une fonction modulaire sur $\mathbf{SL}_2(\mathbf{Z})$ de poids $k \in \mathbf{Z}$, à coefficients rationnels. On suppose f holomorphe dans le demi-plan $\mathcal{J}(z) > 0$ mais pas nécessairement à la pointe ∞ .

(a) Soit l un nombre premier tel que $a_n = 0$ pour tout $n < 0$ divisible par l . Montrer que les séries

$$f' = \sum a_{ln} q^n \quad \text{et} \quad f'' = \sum_{l|n} a_n q^n$$

sont des formes modulaires l -adiques de poids k , au sens de [21].

(b) Soient l un nombre premier $\neq 2$, et $\varepsilon = \pm 1$ tels que $a_n = 0$ pour tout $n < 0$ tel que $\left(\frac{n}{l}\right) = \varepsilon$. Montrer que la série

$$f_- = \sum_{\left(\frac{n}{l}\right) = \varepsilon} a_n q^n$$

est une forme modulaire l -adique de poids k . (Même méthode que pour 5.2.)

Divisibilité des coefficients $c(n)$ de j .

(6.15) Soit D l'opérateur de dérivation $\sum a_n q^n \mapsto \sum n a_n q^n$, noté θ dans [21], [27]. Soient l un nombre premier $\neq 2$, et r un entier ≥ 1 .

(a) Montrer que, si h est une forme modulaire (mod l^r), de poids k , il existe une forme modulaire h' (mod l^r), de poids $k + 2 + l^{r-1}(l-1)$, telle que

$$D(h/\Delta) \equiv h'/\Delta \pmod{l^r}.$$

(Utiliser le lemme 3 de [27], p. 19, ainsi que le fait que

$$P \equiv E_{2+lr-1(l-1)} \pmod{l^r}.)$$

(b) Dédurre de là que, pour tout $a \geq 0$, il existe une forme modulaire f_a (mod l^r), de poids $12 + a(2 + l^{r-1}(l-1))$, telle que

$$D^a(j) \equiv f_a/\Delta \pmod{l^r}.$$

(c) On prend $a = \frac{1}{2} l^{r-1}(l-1)$. Montrer que

$$D^a(j) \equiv j_\varepsilon \pmod{l^r}, \quad \text{où} \quad j_\varepsilon = \sum_{n=-1}^{\infty} \left(\frac{n}{l}\right) c(n) q^n.$$

En déduire, grâce à (b), l'existence d'une forme modulaire h de poids

$$12 + l^{r-1}(l-1) + \frac{1}{2} l^{2r-2}(l-1)^2 = 12 + k,$$

telle que

$$j - \left(\frac{-1}{l}\right) j_{\varepsilon} \equiv h/\Delta \pmod{l^r}.$$

Le terme constant de h est nul. En déduire que $h = f\Delta$, où f est une forme modulaire (mod l^r) de poids k , ce qui fournit une autre démonstration de (5.2 b).

(6.16) On conserve les notations de (6.15), et l'on prend $r = 1$, i.e. on calcule (mod l).

(a) Montrer que $j' \equiv 744 \pmod{l}$ si $l = 3, 5, 7, 11$, et que $j' \pmod{l}$ est de filtration $l - 1$ (au sens de [27], p. 24) si $l \geq 13$. En particulier, on a, pour tout $n \geq 1$:

$$\begin{aligned} c(3n) &\equiv 0 \pmod{3} \\ c(5n) &\equiv 0 \pmod{5} \\ c(7n) &\equiv 0 \pmod{7} \\ c(11n) &\equiv 0 \pmod{11} \\ c(13n) &\equiv c(13) \tau(n) \equiv -\tau(n) \pmod{13} \\ c(17n) &\equiv c(17) t_{16}(n) \equiv 4t_{16}(n) \pmod{17} \\ c(19n) &\equiv c(19) t_{18}(n) \equiv 7t_{18}(n) \pmod{19} \\ c(23n) &\equiv c(23) t_{22}(n) \equiv 4t_{22}(n) \pmod{23}, \end{aligned}$$

où, pour $k = 16, 18, 22$, on note $t_k(n)$ le coefficient de q^n dans l'unique forme parabolique normalisée de poids k .

(b) On a

$$D(j) = Q^2 R/\Delta = Q^2 R \Delta^{l-1}/\Delta^l,$$

d'où

$$D^{a+1}(j) \equiv D^a(Q^2 R \Delta^{l-1})/\Delta^l \pmod{l}.$$

Montrer que, si $l \geq 13$, $Q^2 R \Delta^{l-1}$ est de filtration $12l + 2$. En déduire que $D^a(Q^2 R \Delta^{l-1})$ est de filtration $12l + 2 + a(l+1)$ pour $a \leq l - 2$.

(c) On applique (b) avec $a = (l-3)/2$, de telle sorte que

$$D^a(Q^2 R \Delta^{l-1})/\Delta^l = D^{a+1}(j) \equiv j_{\varepsilon}, \quad \text{cf. (6.15 c).}$$

En déduire que la forme modulaire (mod l) $j - \left(\frac{-1}{l}\right) j_{\varepsilon}$ est de filtration $\frac{1}{2}(l-1)^2$, et que j_{ε} est de filtration $l^2 - l$. En particulier, ces formes sont $\not\equiv 0 \pmod{l}$.

(d) Si $l = 3$ (resp. 5, 7, 11), la forme $j - \left(\frac{-1}{l}\right)j_\varepsilon$ est nulle (resp. de filtration 0, 12, 40).

(e) Dédurre de (b) et (c) les congruences suivantes (dues à Kolberg [7]):

$$c(n) \equiv 0 \pmod{5} \quad \text{si} \quad \left(\frac{n}{5}\right) = -1$$

$$c(n) \equiv 2n \sigma_3(n) \pmod{7} \quad \text{si} \quad \left(\frac{n}{7}\right) = 1$$

$$c(n) \equiv 9n^2 \sigma_5(n) - 3n^3 \sigma_3(n) \pmod{11} \quad \text{si} \quad \left(\frac{n}{11}\right) = 1$$

$$c(n) \equiv 8\tau(n) - 3n^3 \sigma_5(n) - 2n^4 \sigma_3(n) \pmod{13} \quad \text{si} \quad \left(\frac{n}{13}\right) = -1.$$

(6.17) Soient l un nombre premier ≥ 7 , et r un entier > 0 . Montrer que, pour tout entier a , il existe une infinité d'entiers n tels que $c(n) \equiv a \pmod{l^r}$ et $\left(\frac{n}{l}\right) = -\left(\frac{-1}{l}\right)$. (Utiliser les exercices (6.16) et (6.5).)

BIBLIOGRAPHIE

- [1] ARTIN, E. Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren. *Abh. math. Semin. Univ. Hamburg*, 8 (1930), pp. 292-306 [*Collected Papers*, pp. 165-179].
- [2] DELANGE, H. Généralisation du théorème de Ikehara. *Ann. scient. Ec. Norm. Sup., Série 3*, 71 (1954), pp. 213-242 [*Math. Rev.*, t. 16, 921e].
- [3] — Sur la distribution des entiers ayant certaines propriétés. *Ann. scient. Ec. Norm. Sup., Série 3*, 73 (1956), pp. 15-74 [*Math. Rev.*, t. 18, 720a].
- [4] DELIGNE, P. Formes modulaires et représentations l -adiques. *Séminaire Bourbaki*, 1968/69, exposé 355, pp. 139-172. — Berlin, Springer-Verlag, 1971 (Lecture Notes in Mathematics, 179).
- [5] — et SERRE, J.-P. Formes modulaires de poids 1. *Ann. scient. Ec. Norm. Sup., Série 4*, 7 (1974), pp. 507-530.
- [6] HARDY, G. H. *Ramanujan*. Cambridge, Cambridge University Press, 1940; New York, Chelsea publishing Company, 1959 [*Math. Rev.*, t. 3, 71d].
- [7] KOLBERG O. Congruences for the coefficients of the modular invariant $j(\tau)$. *Math. Scand.* 10 (1962), pp. 173-181 [*Math. Rev.*, t. 26, 1287].
- [8] LANDAU, E. Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate. *Arch. der Math. und Phys.*, (3) 13 (1908), pp. 305-312.
- [9] LANG, S. and TROTTER, H. Frobenius Distributions in GL_2 -Extensions. Lecture Notes in Mathematics 504, Berlin, Springer-Verlag, 1976.

- [10] NARKIEWICZ, W. *Elementary and analytic theory of algebraic numbers*. Warszawa, PWN-Polish scientific Publishers, 1974 (Polska Akademia Nauk. Monografie Matematyczne, 57).
- [11] ODONI, R. W. K. The Farey density of norm subgroups of global fields (I). *Mathematika*, London, 20 (1973), pp. 155-169.
- [12] — On the norms of algebraic integers. *Mathematika*, London, 22 (1975), pp. 71-80.
- [13] PARKIN, T. R. and SHANKS, D. On the distribution of parity in the partition function. *Math. Comp.* 21 (1967), pp. 466-480 [Math. Rev., t. 37, 2711].
- [14] RAIKOV, D. A. Généralisation du théorème d'Ikehara-Landau [en russe]. *Mat. Sbornik* 45 (1938), pp. 559-568.
- [15] — Sur la distribution des entiers dont les facteurs premiers appartiennent à une progression arithmétique donnée [en russe]. *Mat. Sbornik* 46 (1938), pp. 563-570.
- [16] RANKIN, R. A. The divisibility of divisor functions. *Proc. Glasgow math. Assoc.* 5 (1961), pp. 35-40 [Math. Rev., t. 26, 2407].
- [17] SCOURFIELD, E. J. On the divisibility of $\sigma_v(n)$. *Acta Arithm.* 10 (1964), pp. 245-285 [Math. Rev., t. 30, 3074].
- [18] — Non-divisibility of some multiplicative functions. *Acta Arithm.* 22 (1973), pp. 287-314 [Math. Rev., t. 47, 4954].
- [19] SERRE, J.-P. Une interprétation des congruences relatives à la fonction τ de Ramanujan. *Séminaire Delange-Pisot-Poitou: Théorie des nombres*, 9^e année, 1967/68, exposé 14: 17 p.
- [20] — *Abelian l -adic representations and elliptic curves*. New York, Benjamin, 1968.
- [21] — Formes modulaires et fonctions zêta p -adiques. *Modular functions of one variable, III*, pp. 191-268. Berlin, Springer-Verlag, 1973 (Lecture Notes in Mathematics, 350).
- [22] — Valeurs propres des opérateurs de Hecke modulo l . *Astérisque* 24-25 (1975), pp. 109-117.
- [23] — Divisibilité des coefficients des formes modulaires, *C. R. Acad. Sc. Paris* 279 (1974), Série A, pp. 679-682.
- [24] SHANKS, D. The second-order term in the asymptotic expansion of $B(x)$. *Math. Comp.* 18 (1964), pp. 75-86 [Math. Rev., t. 28, 2391].
- [25] SHIMURA, G. *Introduction to the arithmetic theory of automorphic functions*. Publ. Math. Soc. Japan, 11, Princeton Univ. Press, 1971.
- [26] STANLEY, G. K. Two assertions made by Ramanujan, *J. London math. Soc.* 3 (1928), pp. 232-237 (Corr. *ibid.*, 4 (1929), p. 32).
- [27] SWINNERTON-DYER, H. P. F. On l -adic representations and congruences for coefficients of modular forms. *Modular functions of one variable, III*, pp. 1-55. Berlin, Springer-Verlag, 1973 (Lecture Notes in Mathematics, 350).
- [28] WATSON, G. N. Über Ramanujansche Kongruenzeigenschaften der Zerfallungsanzahlen (I). *Math. Z.* 39 (1935), pp. 712-731.
- [29] WINTNER, A. On the prime number theorem. *Amer. J. Math.* 64 (1942), pp. 320-326 [Math. Rev., t. 3, 271a].

Jean-Pierre Serre
 Collège de France
 Paris.

(Reçu le 21 mai 1976)