Zeitschrift: L'Enseignement Mathématique
Band: 22 (1976)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: DIVISIBILITÉ DE CERTAINES FONCTIONS ARITHMÉTIQUES
Kapitel: §4. EXEMPLES MODULAIRES
Autor: Serre, Jean-Pierre
DOI: https://doi.org/10.5169/seals-48187

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

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

(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 $K_{\mathfrak{m}}$ de $\mathbf{Q}$, et d'une représentation linéaire

$$\rho_{\mathfrak{m}} : \mathrm{Gal}(K_{\mathfrak{m}}/\mathbf{Q}) \to \mathbf{GL}_N(O_F/\mathfrak{m})$$

telles que $\mathrm{Tr}\left(\rho_{\mathfrak{m}}(\sigma_p(K_{\mathfrak{m}}/\mathbf{Q}))\right) \equiv a_p \pmod{\mathfrak{m}}$ pour tout nombre premier p, à l'exception d'un nombre fini. Si l'on suppose en outre qu'il existe $\sigma \in \mathrm{Im}(\rho_{\mathfrak{m}})$ tel que $\mathrm{Tr}(\sigma) = 0$, alors (3.6.1) est vérifié; on peut souvent prendre pour σ l'image par $\rho_{\mathfrak{m}}$ 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 $q = e^{2\pi i z}$, avec $\mathscr{I}(z) > 0$.

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*

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

(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*

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*

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

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

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

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 $H \neq \varnothing$ 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 frobénien, 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 connu [1]) que toute forme modulaire est somme de fonctions $z \mapsto f_i(d_i z)$, où les d_i sont des entiers $\geqslant 1$ et les f_i des formes modulaires de type (ii).

Exemples.

(4.3) La forme

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

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.

$\mathrm{Gal}(\mathbf{Q}(i, \sqrt[4]{12}), \mathbf{Q})$, 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

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

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

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

Des questions analogues se posent pour $N\{n \leqslant x : a_n = a\}$, 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 $k \geqslant 1$ sur un sous-groupe de congruence de $\mathbf{SL}_2(\mathbf{Z})$. Supposons que les coefficients a_n de f appartiennent pour $n \geqslant 1$ 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'analogue « 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*

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

(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:*

(ii$_1$) *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*

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

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

(ii$_2$) *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*

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

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 $O_F/\mathfrak{m}$. D'après Deligne (cf. [4], ainsi que [5], § 6), il existe une extension galoisienne finie $K = K_{f,\mathfrak{m}}$ de $\mathbf{Q}$, non ramifiée en dehors de lN, et une représentation semi-simple

$$\rho_{\mathfrak{m}} : \mathrm{Gal}\,(K/\mathbf{Q}) \to \mathbf{GL}_2(O_F/\mathfrak{m})$$

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

$$\mathrm{Tr}\,\rho_{\mathfrak{m}}(\sigma_p(K/\mathbf{Q})) \equiv a_p \pmod{\mathfrak{m}}$$

et

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

[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 $\mathfrak{m}$) au p-ième facteur de la « série L » de la représentation $\rho_{\mathfrak{m}}$, cette dernière étant considérée comme une série de Dirichlet formelle à coefficients dans $O_F/\mathfrak{m}$.]

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

(ii$_1$) *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 $\rho_{\mathfrak{m}}$ n'est pas la représentation unité, ce qui revient aussi à dire qu'il existe $p \nmid 2N$ tel que $a_p \not\equiv 0 \pmod{\mathfrak{m}}$. Ce sont bien là les conditions de (ii$_1$).] Comme l'ensemble $P_{a,\mathfrak{m}}$ des p tels que $a_p \equiv 0 \pmod{\mathfrak{m}}$ est frobénien, et défini par H, on peut appliquer (3.4) avec $\alpha(\mathfrak{m}) = |H| / |G|$, et l'on obtient le développement asymtotique cherché.

(ii$_2$) *On a* $H = G$, ce qui signifie que $l = 2$, et que $\rho_{\mathfrak{m}}$ est la représentation unité. On a alors

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

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

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

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

(4.8) Soit $\Phi(\mathbf{X}) = \Phi(X_1, \ldots, X_{2k})$ 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 $m \geqslant 1$, 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 (ii$_1$), avec un exposant $\alpha(m)$ facile à déterminer (cf. § 1, exemple 3); on en déduit

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

[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 $c_0, c_1, \ldots$, 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 (ii$_2$). 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

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

en accord avec (4.7 ii$_2$).

Questions.

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

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

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

$$N\{n \leqslant x : a_n \equiv \lambda \pmod{\mathfrak{m}}\} \qquad \text{pour } \lambda \text{ donné.}$$

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

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

avec $c > 0$, $\alpha > 0$, h entier $\geqslant 0$ (mis à part un cas exceptionnel, analogue à (4.7 ii$_2$), 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 $k \geqslant 2$, et à coefficients dans $\mathbf{Z}$. Ecartons 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

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

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

$$(4.11_k?) \qquad |a_p| >> p^{(k-3)/2-\varepsilon} \qquad (\text{si } k \geqslant 4)$$

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:

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

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

---

[1]) Si l'on écrit a_p sous la forme $2p^{(k-1)/2}\cos\varphi_p$, avec $0 \leqslant \varphi_p < \pi$, (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 (4.11_2 ?), à savoir:

(4.11_2 ??) $\qquad N\{p \leqslant x : a_p = 0\} \sim cx^{1/2}/\log x \qquad$ (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 $\mathbf{SL}_2(\mathbf{Z})$ 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) $O_F/\mathfrak{m}$ est de caractéristique 2: en effet, on se ramène alors au cas d'un poids entier en multipliant f par la série

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

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 $t_1, \ldots, t_r$ tels que $a_n = 0$ si n n'est pas produit de l'un des t_i par un carré; cela entraîne

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

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

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

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: