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: §6. EXERCICES
DOI: https://doi.org/10.5169/seals-48187

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 $\mathbf{SL}_2(\mathbf{Z})$.

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 $\left(\frac{n}{l}\right) = -\left(\frac{-1}{l}\right)$, 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 (mod 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 $\alpha \leqslant 3/4$, 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

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

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 $\mathfrak{m}$).

(6.3) Montrer que, sous les hypothèses de (4.7 ii_1), on a $\alpha(\mathfrak{m}) \leqslant 3/4$ (même méthode que pour (6.1)). En déduire un résultat analogue à (6.2).

(6.4) On fixe k, $\mathfrak{m}$, N, ε et l'on note m la norme de $\mathfrak{m}$. Soit A l'ensemble des séries formelles $\sum a_n q^n$, à coefficients dans $O_F/\mathfrak{m}$, qui sont réduction (mod $\mathfrak{m}$) de formes modulaires de type (k, ε) sur $\Gamma_0(N)$, à coefficients dans O_F; c'est un $O_F/\mathfrak{m}$-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 $u \in \mathrm{End}(A)$, 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 $p \equiv 1 \pmod{N\mathfrak{m}}$ qui appartiennent à P_2 (i.e. tels que $f \mid T_p = 2f$ pour tout $f \in A$), et soit P_0^- l'ensemble des $p \equiv -1 \pmod{N\mathfrak{m}}$ qui appartiennent à P_0 (i.e. tels que $f \mid T_p = 0$ 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

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

(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 $(n \geqslant 1)$ est un sous-ensemble de $O_F/\mathfrak{m}$ 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

$$N\{n \leqslant x : a_n = a \quad \text{dans} \quad O_F/\mathfrak{m}\} \quad >> \quad x(\log\log x)^h/\log x$$

quel que soit h. (Choisir $r \geqslant 1$ tel que $a_r = 2^{-h-1}\,a$, et remarquer que $a_n = a$ lorsque n est de la forme $p_0 \ldots p_h\, r$, où $p_0, \ldots, p_h$ 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 $\mathbf{SL}_2(\mathbf{Z})$, autrement dit (cf. [21], [27]) l'algèbre des polynômes en la série

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

à coefficients dans $\mathbf{F}_2$. Soit S_0 (resp. S_1) le sous-espace de S engendré par les $\tilde{\Delta}^i$ pour $i \geqslant 1$ (resp. par les $\tilde{\Delta}^{2^j}$, pour $j \geqslant 0$); 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

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

(b) On peut prouver (cf. [22]) que les T_p sont *localement nilpotents* sur S_0. Admettant ce fait, il existe un entier $h \geqslant 0$ tel que f soit annulé par tous les produits $T_{p_0} \ldots T_{p_h}$, 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:

$$N\{n \leqslant x : a_n = 1\} \quad << \quad x(\mathrm{loglog}\, x)^{h-1}/\log x.$$

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

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

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

$$N\{n \leqslant x : a_n = 1\} \quad >> \quad x(\mathrm{loglog}\, x)^{h-1}/\log x,$$

d'où, en vertu de (b):

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

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

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

ainsi qu'à

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

(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 $\geqslant 0$, 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

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

On peut l'écrire sous la forme

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

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

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

Montrer que

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

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 $r \geqslant 0$, notons N_r (resp. P_r) l'ensemble des entiers $n \geqslant 1$ (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

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

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

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

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

(b) On suppose que les P_r sont réguliers de densité $\alpha_r \geqslant 0$ et que $0 < \alpha_0 < 1$; on note m la borne inférieure des $i \geqslant 1$ 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 $\mathscr{R}(s) \geqslant 1$. Cela entraîne:

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

où les $d_{r,j}(s)$ sont holomorphes pour $\mathscr{R}(s) \geqslant 1$. 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

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

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 ii$_1$). Montrer que les conditions de (b) sont satisfaites (les P_r sont même frobéniens) et que l'on a

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

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

(d) Etendre les résultats ci-dessus au cas de produits de puissances $\mathfrak{p}_1^{r_1} \ldots \mathfrak{p}_j^{r_j}$ d'idéaux premiers (utiliser des séries formelles en $T_1, \ldots, T_j$).

(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 $H_l \neq \varnothing$, que $P_1(l) \neq \varnothing$, ou que la densité de $P_1(l)$ est > 0. Or, on a $H_l \neq \varnothing$ 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 $\tau(5) = 2.3.5.7.23$; pour $l = 5$, on a $19 \in P_1(l)$ puisque $\tau(19) = 2^2.5.7^2.11.23.43$; 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 $r \geqslant 0$, il existe une constante $c_{l,r} > 0$ telle que

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

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

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

(6.10) Soit $n \mapsto a_n$ une fonction multiplicative à valeurs dans un anneau commutatif fini Λ. On note r l'ordre du groupe multiplicatif Λ^* des éléments inversibles de Λ. Si $\lambda \in \Lambda^*$, 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 Λ^* est engendré par les éléments λ tels que $\alpha_\lambda > 0$.

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

(a) Si $\lambda \in \Lambda^*$ 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 $\mathscr{R}(s) \geqslant 1$.

On a $\mathscr{R}(\beta(\varphi)) \leqslant \alpha$, avec $\alpha = \sum \alpha_\lambda$, et il n'y a égalité que si φ est le caractère unité de Λ^*.

(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 $\mathscr{R}(s) \geqslant 1$, les β_i sont tels que $\mathscr{R}(\beta_i) < \alpha$, et $c(1) > 0$.

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

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

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 frobéniens. En déduire, pour tout $N \geqslant 1$, un développement asymptotique de $N\{n \leqslant x: a_n = \lambda\}$ modulo $O(x/\log^N x)$.

(e) Enoncer et démontrer des résultats analogues pour

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

où les $a_n^{(i)}$ sont des fonctions multiplicatives à valeurs dans des anneaux commutatifs finis Λ_i. (Se ramener au cas d'une suite unique à valeurs dans $\Lambda = \Lambda_1 \times \ldots \times \Lambda_r$.)

(6.11) Soit m un entier impair $\geqslant 3$. On considère la fonction multiplicative

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

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

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

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

Exemple de minoration de $|a_p|$ *pour* $p \to \infty$.

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

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

Posons

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

de sorte que

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

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

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

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

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

[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 $a_p = \chi(\mathfrak{a})\, z^d + \chi(\overline{\mathfrak{a}})\overline{z}^d = A_d(x, y)$, 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

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

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 $p << N^\delta$ 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

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

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

Passage des fonctions modulaires aux formes modulaires.

(6.14) Soit $f = \sum_{n \geqq -r} a_n\, q^n$ 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 $\mathscr{I}(z) > 0$ 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

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

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 $\geqslant 1$.

(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

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

(b) Déduire de là que, pour tout $a \geqslant 0$, il existe une forme modulaire f_a (mod l^r), de poids $12 + a\left(2 + l^{r-1}(l-1)\right)$, 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 $l \geqslant 13$. En particulier, on a, pour tout $n \geqslant 1$:

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

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

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

d'où

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

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

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

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

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_- 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) Déduire 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 $\geqslant 7$, 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 $\mathbf{GL}_2$-Extensions. Lecture Notes in Mathematics 504, Berlin, Springer-Verlag, 1976.