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: §5. DIVISIBILITÉ DES COEFFICIENTS DE j

DOI: https://doi.org/10.5169/seals-48187

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:

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

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

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

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

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

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

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

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*

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

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 $(\bmod\, l)$ 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*

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

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

Démonstration de (5.2).

(a) Le fait que $j' = j \mid U$ soit modulaire l-adique de poids 0 est dû à Deligne, cf. par exemple [21], p. 228. Comme $j'' = j' \mid V$, 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 $k \geqslant 4$, et où les coefficients a_n sont *l-entiers*. On raisonne alors par récurrence sur m. Le cas $m = 1$ est traité dans [21], nº 3.2. Si $m \geqslant 2$, définissons des formes modulaires f_i, g_i de poids kl^i $(i \geqslant 0)$ au moyen des formules de récurrence:

$$f_0 = 0 , \quad g_0 = g , \; f_i = (g_{i-1})^l \mid U , \quad g_i = \frac{1}{l} \left(E_{kl^{i-1}(l-1)}\, g_{i-1} - f_i\right) (i \geqslant 1).$$

(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 $m \geqslant 2$, 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 $i \geqslant 0$, posons

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

le produit infini ayant un sens du fait que $E_{kl^a(l-1)}$ 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 $A_0^{-1} = \lim_{s \to \infty} A_0^{l^s - 1}$ 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 $\geqslant 4$. 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 $\mathbf{SL}_2(\mathbf{Z})$. 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

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

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

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

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

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).)