Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Jean-Pierre Serre

Une interprétation des congruences relatives à la fonction τ de Ramanujan

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 9, n° 1 (1967-1968), exp. n° 14, p. 1-17

<http://www.numdam.org/item?id=SDPP_1967-1968__9_1_A13_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
9e année, 1967/68, n° 14

26 février 1968

UNE INTERPRÉTATION DES CONGRUENCES RELATIVES À LA FONCTION τ DE RAMANUJAN

par Jean-Pierre SERRE

§ 1. La fonction τ

1.1. Définition.

Posons

$$D(x) = x \prod_{m=1}^{\infty} (1 - x^m)^{24} \quad . \tag{1}$$

Le coefficient de x^n $(n \geq 1)$ dans le développement en série entière de $D(x)$ est noté $\tau(n)$. La fonction $n \longmapsto \tau(n)$ est la fonction de Ramanujan (cf. [5], [16]). On a :

$$D(x) = \sum_{n=1}^{\infty} \tau(n)\, x^n \quad . \tag{2}$$

Voici quelques valeurs de τ, empruntées à LEHMER [11] :

$\tau(1) = 1$	$\tau(5) = 4830$	$\tau(9) = -113643$
$\tau(2) = -24$	$\tau(6) = -6048$	$\tau(10) = -115920$
$\tau(3) = 252$	$\tau(7) = -16744$	...
$\tau(4) = -1472$	$\tau(8) = 84480$	$\tau(300) = 945878451840 0$

1.2. Premières propriétés de τ.

On sait que, si l'on pose

$$\Delta(z) = D(e^{2\pi i z}) \quad , \qquad \mathrm{Im}(z) > 0 \quad , \tag{3}$$

la fonction Δ est, à un facteur constant près, l'unique forme parabolique de poids 12 (ou -12, suivant les conventions adoptées) pour le groupe $\underset{\sim}{SL}(2, \underset{\sim}{Z})$. En particulier, pour tout nombre premier p, la fonction Δ est fonction propre de l'opérateur de Hecke T_p, la valeur propre correspondante étant $\tau(p)$ (cf., par exemple, HECKE [6], p. 644-671). Ceci entraîne les propriétés suivantes, conjecturées par RAMANUJAN [16] et démontrées par MORDELL [14] :

(4) $\tau(mn) = \tau(m)\,\tau(n)$ si m et n sont premiers entre eux .

(5) $\tau(p^{n+1}) = \tau(p^n)\,\tau(p) - p^{11}\tau(p^{n-1})$ si p est premier, $n \geqslant 1$.

Ces formules ramènent le calcul de $\tau(n)$ à celui de $\tau(p)$, pour p premier.

1.3. La série de Dirichlet attachée à τ .

Soit

(6) $$L_\tau(s) = \sum_{n=1}^{\infty} \tau(n)/n^s$$

la série de Dirichlet définie par τ . Les formules (4) et (5) équivalent à la suivante :

(7) $$L_\tau(s) = \prod_p \frac{1}{1 - \tau(p)p^{-s} + p^{11-2s}} = \prod_p \frac{1}{H_p(p^{-s})} ,$$

où

(8) $$H_p(X) = 1 - \tau(p)X + p^{11}X^2 .$$

De plus, la théorie de Hecke montre que $L_\tau(s)$ se prolonge en une fonction entière dans le plan complexe, et que la fonction

$$(2\pi)^{-s}\,\Gamma(s)\,L_\tau(s)$$

est invariante par $s \longmapsto 12 - s$.

Signalons à ce sujet la conjecture de Ramanujan que l'on peut formuler de l'une des façons équivalentes suivantes :

- Les racines du polynôme $H_p(X)$ sont imaginaires conjuguées ;
- Les racines du polynôme $H_p(X)$ sont de valeur absolue $p^{-11/2}$;
- On a $|\tau(p)| < 2p^{11/2}$.

§ 2. Les congruences relatives à τ

2.1. Résultats.

On a des formules donnant $\tau(n)$ modulo 2^{11} , 3^7 , 5^3 , 7 , 23 , 691 (cf. LEHMER [13]). Plus précisément :

Puissances de 2 . - On trouve, dans [2], la valeur de $\tau(p)$ mod 2^5 :

(9) $$\tau(p) \equiv 1 + p^{11} \pmod{2^5} \quad \text{si } p \neq 2 .$$

En fait, cette congruence vaut mod 2^8 ; plus précisément, LEHMER [13] démontre :

$$\tau(p) \equiv 1 + p^{11} + 8(41 + x)(p - x)^{2+x} \pmod{2^{11}} \tag{10}$$

avec $x = (-1)^{(p-1)/2}$.

SWINNERTON-DYER (non publié) a également obtenu des congruences modulo 2^{12} , 2^{13} , 2^{14} lorsque $p \equiv 5$, 3 , $7 \pmod 8$.

Puissances de 3 . - On trouve dans [15] la valeur de $\tau(p)$ mod 3 :

$$\tau(p) \equiv 1 + p \pmod 3 \qquad \text{si } p \neq 3 \text{ .} \tag{11}$$

LEHMER [13] donne $\tau(p)$ mod 3^5 ; en particulier :

$$\tau(p) \equiv p^2 + p^9 \pmod{3^3} \text{ .} \tag{12}$$

SWINNERTON-DYER (non publié) a obtenu des congruences modulo 3^6 ou 3^7 suivant que $p \equiv 1 \pmod 3$ ou $p \equiv -1 \pmod 3$.

Puissances de 5 . - On a (cf. [2]) :

$$\tau(p) \equiv p + p^{10} \pmod{5^2} \text{ .} \tag{13}$$

LEHMER [13] donne une congruence mod 5^3 (valable si $p \neq 5$) :

$$\tau(p) \equiv -24p(1 + p^9) - 10p(1 + p^5) - 90p^2(1 + p^3) \pmod{5^3} \text{ ;}$$

on peut aussi l'écrire sous la forme :

$$\tau(p) \equiv p^{41} + p^{-30} \pmod{5^3} \text{ ,} \qquad p \neq 5 \text{ .} \tag{14}$$

Puissances de 7 . - On a (cf. [15]) :

$$\tau(p) \equiv p + p^4 \pmod 7 \text{ .} \tag{15}$$

On ne connait, pour l'instant, la valeur de $\tau(p)$ mod 7^2 que lorsque p est non résidu quadratique mod 7 , et dans ce cas c'est $p + p^{10}$ (LEHMER [13]).

Puissances de 23 . - Le résultat a ici une forme un peu différente des précédents. On a (cf. WILTON [21]), pour $p \neq 23$:

$$(16)\quad \begin{cases} \tau(p) \equiv 0 \pmod{23} & \text{si } p \text{ est non résidu quadratique mod } 23 \text{ ,} \\ \tau(p) \equiv 2 \pmod{23} & \text{si } p \text{ est de la forme } u^2 + 23v^2 \text{ ,} \\ \tau(p) \equiv -1 \pmod{23} & \text{si } p \text{ est résidu quadratique mod } 23 \text{ , mais n'est pas de la forme } u^2 + 23v^2 \text{ .} \end{cases}$$

[Soit $K = \mathbb{Q}(\sqrt{-23})$. Dire que p est résidu quadratique mod 23 signifie que p se décompose dans K en deux idéaux premiers distincts $\mathfrak{p}$ et $\bar{\mathfrak{p}}$; pour que p soit de la forme $u^2 + 23v^2$, il faut et il suffit que $\mathfrak{p}$ soit <u>principal</u> (rappelons que le nombre de classes de K est égal à 3).]

<u>Puissances de</u> 691 . - On a (RAMANUJAN [16]) :

$$\tau(p) \equiv 1 + p^{11} \pmod{691} \quad . \tag{17}$$

Telles sont les congruences connues sur $\tau(p)$; bien entendu, en utilisant les formules (4) et (5), on en déduit des congruences pour $\tau(n)$, n quelconque.

2.2. <u>Démonstrations</u>.

Je me bornerai à de brèves indications ; pour plus de détails, voir [2], [12], [13], [15], [16], [21].

(a) Considérons les séries d'Eisenstein de poids 6 et 12 :

$$\begin{cases} E_6(x) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n)\, x^n \\ E_{12}(x) = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n)\, x^n \quad . \end{cases} \qquad \text{où } \sigma_q(n) = \sum_{d \mid n} d^q \tag{18}$$

Puisque le carré de E_6 est une forme modulaire de poids 12, c'est une combinaison linéaire de E_{12} et de D ; d'où :

$$E_6^2 = E_{12} - \frac{a}{691} D, \qquad \text{avec } a \equiv 65520 \pmod{691} \quad . \tag{19}$$

En multipliant par 691, on obtient des séries à coefficients <u>entiers</u>, et, en réduisant modulo 691, on trouve :

$$0 \equiv 65520 \Big(\sum_{n=1}^{\infty} \sigma_{11}(n)\, x^n - \sum_{n=1}^{\infty} \tau(n)\, x^n \Big) \pmod{691} \quad , \tag{20}$$

d'où :

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691} \quad . \tag{21}$$

Lorsque $n = p$ est premier, cela donne bien la congruence (17).

(b) Les congruences mod 2^α, 3^β, 5^γ, 7 se démontrent par des arguments analogues au précédent (mais plus compliqués) utilisant les fonctions

$$\Phi_{r,s}(x) = \sum_{m,n} m^r n^s x^{mn}$$

de Ramanujan (cf. LEHMER [13]).

(c) La congruence modulo 23 résulte facilement de la suivante (cf. WILTON [21]):

$$(22) \qquad \prod_{m=1}^{\infty} (1 - x^m)^{24} \equiv \theta(x)\ \theta(x^{23}) \pmod{23}$$

où

$$\theta(x) = \prod_{m=1}^{\infty} (1 - x^m) = \sum_{-\infty}^{+\infty} (-1)^r\, x^{(3r^2+r)/2} \quad .$$

2.3. Les zéros de la fonction τ .

Y a-t-il des nombres premiers p tels que $\tau(p) = 0$? On n'en connait pas. En tout cas, les congruences ci-dessus entraînent (cf. LEHMER [12], [13]) :

$$(23) \qquad \text{Si } \tau(p) = 0 \text{ , on a } \begin{cases} p \equiv -1 \pmod{2^{11}3^7 5^3 691} \\ p \equiv -1 \text{ , } 19 \text{ ou } 31 \pmod{49} \\ p \text{ non résidu quadratique mod } 23 \quad . \end{cases}$$

En particulier, la densité de l'ensemble des p tels que $\tau(p) = 0$ est inférieure à 10^{-12} , et le plus petit p tel que $\tau(p) = 0$ est un nombre d'au moins 15 chiffres.

§ 3. Les représentations ℓ-adiques attachées à τ

3.1. Notations.

Soit $\bar{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$; pour tout nombre premier ℓ , nous noterons K_ℓ la plus grande sous-extension de $\bar{\mathbb{Q}}$ qui est non ramifiée en dehors de ℓ . Une sous-extension finie de $\bar{\mathbb{Q}}$ est contenue dans K_ℓ si, et seulement si, la valeur absolue de son discriminant est une puissance de ℓ .

L'extension $K_\ell/\mathbb{Q}$ est galoisienne ; soit $\mathrm{Gal}(K_\ell/\mathbb{Q})$ son groupe de Galois ; dans la terminologie de GROTHENDIECK, $\mathrm{Gal}(K_\ell/\mathbb{Q})$ est le groupe fondamental de $\mathrm{Spec}(\mathbb{Z}) - \{\ell\}$. Si p est un nombre premier distinct de ℓ , nous associerons à p son élément de Frobenius F_p , qui est un élément de $\mathrm{Gal}(K_\ell/\mathbb{Q})$, défini à conjugaison près.

Soit k un anneau, soit N un entier, et soit

$$\rho : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to \underline{\mathrm{GL}}(N, k)$$

une représentation linéaire de degré N de $\mathrm{Gal}(K_\ell/\mathbb{Q})$ dans k. Pour tout $p \neq \ell$, l'élément $\rho(F_p)$ de $\underline{\mathrm{GL}}(N, k)$ est déterminé à conjugaison près ; en particulier, le polynôme

$$P_{p,\rho}(X) = \det(1 - \rho(F_p)X)$$

est bien défini.

Dans ce qui suit, nous nous intéresserons surtout au cas où l'anneau k est $\mathbb{Z}/\ell^n\mathbb{Z}$, ou $\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z}$, ou $\mathbb{Q}_\ell = \mathbb{Z}_\ell[1/\ell]$, l'homomorphisme ρ étant continu.

3.2. Une conjecture.

C'est la suivante :

CONJECTURE. - *Pour tout nombre premier ℓ, il existe une représentation linéaire continue*

$$\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathrm{Aut}(V_\ell) ,$$

où V_ℓ est un $\mathbb{Q}_\ell$-espace vectoriel de dimension 2, satisfaisant à la condition suivante :

(C) *Pour tout nombre premier $p \neq \ell$, le polynôme $P_{p,\rho_\ell}(X)$ est égal au polynôme $H_p(X)$ du n° 1.3.*

La condition (C) peut être reformulée ainsi :

(C') *Pour tout $p \neq \ell$, on a*

$$\mathrm{Tr}(\rho_\ell(F_p)) = \tau(p) \quad \text{et} \quad \det(\rho_\ell(F_p)) = p^{11} . \tag{24}$$

Dans la terminologie de [17] (chap. I, § 2), les ρ_ℓ forment un *système strictement compatible de représentations ℓ-adiques rationnelles de $\mathbb{Q}$*, à ensemble exceptionnel réduit à $\emptyset$.

Remarques.

1° Soit $\chi_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathbb{Q}_\ell^*$ la représentation ℓ-adique de degré 1 donnée par l'action de $\mathrm{Gal}(K_\ell/\mathbb{Q})$ sur les racines ℓ^n-ièmes de l'unité (cf. [17], chap. I, n° 1.2) ; on a $\chi_\ell(F_p) = p$. La deuxième partie de la condition (24) équivaut donc à

$$\det(\rho_\ell) = \chi_\ell^{11} . \tag{25}$$

2° Soit c l'élément d'ordre 2 de $\mathrm{Gal}(K_\ell/\underset{\sim}{\mathbb{Q}})$ induit par la conjugaison complexe ; il est défini à conjugaison près. D'après (25), on a $\det(\rho_\ell(c)) = -1$. On en conclut que $\rho_\ell(c)$ a pour valeurs propres 1 et -1 .

3° La représentation ρ_ℓ dont la conjecture ci-dessus affirme l'existence est unique, à isomorphisme près. Cela résulte de [17] (chap. I, n° 2.3), combiné avec le fait que ρ_ℓ est irréductible (cf. n° 5.1 ci-après).

3.3. Les représentations (mod ℓ^n) .

Observons d'abord que, si $\rho_\ell : \mathrm{Gal}(K_\ell/\underset{\sim}{\mathbb{Q}}) \to \mathrm{Aut}(V_\ell)$ existe, il y a un réseau de V_ℓ qui est stable par $\mathrm{Im}(\rho_\ell)$, cf. [17] (chap. I, n° 1.1). Autrement dit, on peut considérer ρ_ℓ comme un homomorphisme de $\mathrm{Gal}(K_\ell/\underset{\sim}{\mathbb{Q}})$ dans $\underset{\sim}{\mathrm{GL}}(2 , \underset{\sim}{\mathbb{Z}_\ell})$ - et non pas seulement dans $\underset{\sim}{\mathrm{GL}}(2 , \underset{\sim}{\mathbb{Q}_\ell})$. (Noter toutefois qu'il n'y a plus unicité : des réseaux différents peuvent donner des représentations non isomorphes.) Par réduction modulo ℓ^n , on en déduit des représentations (mod ℓ^n)

$$\rho_{\ell,n} : \mathrm{Gal}(K_\ell/\underset{\sim}{\mathbb{Q}}) \to \underset{\sim}{\mathrm{GL}}(2 , \underset{\sim}{\mathbb{Z}}/\ell^n\underset{\sim}{\mathbb{Z}})$$

telles que

$$(26) \qquad \begin{cases} \mathrm{Tr}(\rho_{\ell,n}(F_p)) \equiv \tau(p) \pmod{\ell^n} \\ \det(\rho_{\ell,n}(F_p)) \equiv p^{11} \pmod{\ell^n} \end{cases}$$

pour tout $p \neq \ell$.

Or, pour certains ℓ^n , on connait explicitement $\tau(p)$ modulo ℓ^n , cf. n° 2.1. Une première vérification de la conjecture consiste donc à chercher, pour ces valeurs de ℓ^n , une représentation (mod ℓ^n) ayant les propriétés voulues. C'est ce que nous allons faire.

3.4. Représentations correspondant aux congruences du § 2.

(a) Il n'y a aucune difficulté modulo 2^8 , 3^3 , 5^3 , 7 ou 691 . Dans chaque cas, on a :

$$\tau(p) \equiv p^a + p^{11-a} \pmod{\ell^n}$$

pour $p \neq \ell$, avec $a = 0$, 2 , 41 , 1 ou 0 respectivement. Toute représentation triangulaire

$$\begin{pmatrix} \varphi & \star \\ 0 & \psi \end{pmatrix}$$

où φ , ψ : $\mathrm{Gal}(K_\ell/\mathbb{Q}) \to (\mathbb{Z}/\ell^n\mathbb{Z})^*$ sont congrus (mod ℓ^n) à χ_ℓ^a et χ_ℓ^{11-a} , répond à la question.

(b) Le cas de $\ell = 23$ et $n = 1$ s'interprète de la manière suivante :

Soit E le corps obtenu en adjoignant à $\mathbb{Q}$ les racines de l'équation

$$x^3 - x - 1 = 0 \ .$$

C'est une extension galoisienne de $\mathbb{Q}$, ramifiée seulement en 23 ; son groupe de Galois est le groupe $\mathfrak{S}_3$ des permutations de trois lettres. (On sait que E est le corps de classes absolu du corps $\mathbb{Q}(\sqrt{-23})$.) Soit r l'unique représentation irréductible de degré 2 de $\mathfrak{S}_3$; on a, si $s \in \mathfrak{S}_3$,

$$\mathrm{Tr}(r(s)) = 0 \ , \ 2 \ \text{ou} \ -1 \ ,$$

suivant que s est d'ordre 2 , 1 , ou 3 . De plus, puisque $\mathrm{Gal}(E/\mathbb{Q})$ est un quotient de $\mathrm{Gal}(K_{23}/\mathbb{Q})$, on peut considérer r comme une représentation de $\mathrm{Gal}(K_{23}/\mathbb{Q})$. Les formules (16) montrent que ρ_{23} et r ont même polynôme caractéristique (mod 23) . Comme r est irréductible modulo 23 , cela entraîne :

$$\rho_{23,1} \approx r \pmod{23} \ .$$

(c) Le cas de 2^{11} est beaucoup moins évident que les précédents (et m'avait même conduit à douter de la conjecture !). Heureusement, il a été traité par SWINNERTON-DYER (non publié), et son résultat constitue en fait la vérification numérique la plus probante de la conjecture générale. SWINNERTON-DYER obtient même la structure complète du groupe $\mathrm{Im}(\rho_2)$ - et pas seulement de sa réduction mod 2^{11} . D'après ce qu'il m'a communiqué, c'est un sous-groupe ouvert d'indice 3.2^{25} du groupe $\mathrm{GL}(2 , \mathbb{Z}_2)$.

3.5. La représentation $\rho_{11,1}$.

Bien que l'on n'ait pas de congruence donnant $\tau(p)$ (mod 11) comme une fonction simple de p (et pour cause - cf. n° 4.3 ci-dessous), SWINNERTON-DYER m'a fait observer que l'existence de la représentation $\rho_{11,1}$ (i. e. ρ_{11} modulo 11) peut se démontrer de la manière suivante :

On observe que

$$(27) \qquad x \prod_{m=1}^{\infty} (1 - x^m)^{24} = x \prod_{m=1}^{\infty} (1 - x^m)^2 \prod_{m=1}^{\infty} (1 - x^m)^{22}$$

$$\equiv x \prod_{m=1}^{\infty} (1 - x^m)^2 \prod_{m=1}^{\infty} (1 - x^{11m})^2 \pmod{11} \ .$$

Or la fonction $x \prod(1 - x^m)^2 \prod(1 - x^{11m})^2$ est une forme parabolique de poids 2 pour le groupe $\Gamma_0(11)$. De plus, on sait (cf. SHIMURA [19]) qu'il lui correspond, pour tout ℓ , une représentation ℓ-adique : celle associée à la courbe elliptique

$$y^2 + y = x^3 - x^2 - 10x - 20 \quad . \tag{28}$$

On en conclut que $\rho_{11,1}$ est isomorphe à la représentation de $\mathrm{Gal}(K_{11}/\mathbb{Q})$ dans le groupe des points de division par 11 de cette courbe elliptique. On observera (cf. SHIMURA [19]) que l'image de $\rho_{11,1}$, qui est a priori un sous-groupe de $\mathrm{GL}(2 , \mathbb{F}_{11})$, est en fait égale à $\mathrm{GL}(2 , \mathbb{F}_{11})$ tout entier. La situation est donc bien différente de celle du numéro précédent, où l'on ne rencontrait que des groupes résolubles.

§ 4. Applications

Dans ce paragraphe, ainsi que dans le suivant, on admet la conjecture du n° 3.2, i. e. l'existence des représentations ρ_ℓ et $\rho_{\ell,n}$. Les résultats énoncés ne pourront donc être considérés comme démontrés que quand la conjecture elle-même le sera (ce qui est imminent, cf. § 6).

4.1. Densité.

La valeur de $\tau(p)$ modulo ℓ^n dépend uniquement de l'élément

$$\rho_{\ell,n}(\mathrm{Fr}_p) \in \mathrm{GL}(2 , \mathbb{Z}/\ell^n\mathbb{Z}) \quad .$$

Vu le théorème de Čebotarev (cf. par exemple [17], chap. I, n° 2.2), cela implique:

L'ensemble des nombres premiers p , distincts de ℓ , tels que $\tau(p)$ soit congru à un entier donné a modulo ℓ^n , a une densité ; cette densité est > 0 si l'ensemble en question est non vide.

(De façon plus précise, cette densité est égale à A/B , où B est l'ordre de $\mathrm{Im}(\rho_{\ell,n})$, et où A est le nombre d'éléments de $\mathrm{Im}(\rho_{\ell,n})$ dont la trace est congrue à a modulo ℓ^n .)

4.2. Indépendance des divers nombres premiers.

Les extensions K_ℓ ($\ell = 2 , 3 , 5 , \ldots$) sont linéairement disjointes sur $\mathbb{Q}$; cela provient simplement de ce que $\mathbb{Q}$ n'admet aucune extension non ramifiée, à part lui-même. On en conclut que les valeurs de $\tau(p)$ modulo 2^a , 3^b , ... sont indépendantes : si la densité des p tels que $\tau(p) \equiv a_i \pmod{\ell_i^{n_i}}$ est d_i , celle des p vérifiant toutes ces conditions à la fois est le produit des d_i .

Le même argument de disjonction entraîne ceci :

Soient ℓ premier, $n \geqslant 1$, et p_0 premier avec $p_0 \neq \ell$. Il existe alors une infinité de p tels que

$$\tau(p) \equiv \tau(p_0) \pmod{\ell^n}, \qquad p \equiv p_0 \pmod{\ell^n},$$

et il en existe dans toute progression arithmétique $an + b$, avec $(a , b) = 1$ et $(a , \ell) = 1$.

(En termes moins précis : si M et N sont deux entiers premiers entre eux, aucune congruence sur p modulo M ne peut entraîner quoi que ce soit sur la valeur de $\tau(p)$ modulo N.)

4.3. Absence de congruence modulo 11.

Le fait que l'image de $\rho_{11,1}$ soit le groupe $\underline{GL}(2 , \underline{Z}/11\underline{Z})$ tout entier (cf. n° 3.5) implique, en vertu du théorème de Čebotarev :

Aucune congruence sur p n'entraîne quoi que ce soit sur la valeur de $\tau(p)$ modulo 11.

(Plus précisément : quels que soient les entiers a, b, c, avec $(a , b) = 1$, il existe une infinité de nombres premiers p tels que $p \equiv a \pmod{b}$ et $\tau(p) \equiv c \pmod{11}$.)

Bien entendu, on a un résultat analogue chaque fois que $\mathrm{Im}(\rho_{\ell,1})$ contient $\underline{SL}(2 , \underline{Z}/\ell\underline{Z})$, propriété qu'il est facile de vérifier numériquement, par la méthode indiquée dans [19].

4.4. Les nombres premiers p tels que $\tau(p) = 0$ ont une densité nulle.

Plus généralement, si $\Phi(X , Y)$ est un polynôme à deux variables, à coefficients dans un corps de caractéristique zéro, non identiquement nul, l'ensemble des p tels que $\Phi(p , \tau(p)) = 0$ a une densité nulle.

En effet, on se ramène par un argument facile au cas où Φ est de la forme $\Psi(X^{11} , Y)$, le polynôme Ψ ayant tous ses coefficients dans $\underline{Q}$. Soit ℓ un nombre premier, et soit $H_\ell = \mathrm{Im}(\rho_\ell)$, considéré comme sous-groupe de $\underline{GL}(2 , \underline{Q}_\ell)$. On peut montrer (cf. n° 5.1 ci-après) que H_ℓ est ouvert dans $\underline{GL}(2 , \underline{Q}_\ell)$. Soit alors X l'ensemble des $s \in H_\ell$ tels que $\Psi(\det(s) , \mathrm{Tr}(s)) = 0$. L'ensemble X est une "hyper-surface" de la variété ℓ-adique H_ℓ, et son intérieur est vide ; il en résulte que, si μ est la mesure de Haar de H_ℓ, on a $\mu(X) = 0$. Le théorème de Čebotarev entraîne alors que la densité de l'ensemble des p tels que $F_p \in X$ est nulle ; d'où le résultat.

(On a donc remplacé le 10^{-12} du n° 2.3 par 0.)

4.5. Une congruence modulo 23^2 .

(Je me borne ici à un cas particulier trivial. Toutefois, comme SWINNERTON-DYER me l'a fait observer, on peut certainement donner la valeur de $\tau(p)$ modulo 23^2 quel que soit p .)

On a vu plus haut que $\rho_{23,1}$ est congru modulo 23 à la représentation r de $\mathfrak{S}_3$. Prenons, en particulier, p de la forme $u^2 + 23v^2$; on a alors :

$$\rho_{23}(F_p) \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{23} \quad .$$

On peut donc écrire :

$$\rho_{23}(F_p) = \begin{pmatrix} 1 + 23a & 23b \\ 23c & 1 + 23d \end{pmatrix} ,$$

avec a , b , c , $d \in \underset{\sim}{Z}_{23}$, et

$$\tau(p) = 2 + 23(a + d) \quad ,$$

$$p^{11} = 1 + 23(a + d) + 23^2(ad - bc) \quad .$$

En comparant, on en déduit :

(29) $$\tau(p) \equiv 1 + p^{11} \pmod{23^2} \quad ,$$

si $p \neq 23$, p de la forme $u^2 + 23v^2$.

Exemple : $p = 59 = 6^2 + 23.1^2$; $\tau(p) = -5189203740$; on vérifie bien que l'on a

$$-5189203740 \equiv 1 + 59^{11} \pmod{529} \quad .$$

§ 5. Compléments et questions

5.1. L'image de ρ_ℓ est un sous-groupe ouvert de $\underset{\sim}{GL}(2 , \underset{\sim}{Q}_\ell)$.

Ce résultat a été mentionné plus haut. On le démontre par une méthode analogue à celle utilisée pour les "modules de Tate" des courbes elliptiques ([17], chap. IV, n° 2.2) :

Tout d'abord, on peut supposer ρ_ℓ semi-simple (sinon, on la remplace par sa "semi-simplifiée"). Soit $\mathfrak{g}_\ell \subset \underset{\sim}{M}_2(\underset{\sim}{Q}_\ell)$ l'algèbre de Lie de $\mathrm{Im}(\rho_\ell)$, considérée comme groupe de Lie ℓ-adique ; puisque ρ_ℓ est semi-simple, $\mathfrak{g}_\ell$ est une algèbre réductive, donc de la forme $\mathfrak{c} \times \mathfrak{s}$, avec $\mathfrak{c}$ abélienne et $\mathfrak{s}$ semi-simple. Si

$s \neq 0$, s est nécessairement égale à l'algèbre de Lie du groupe $\underset{\sim}{SL}(2 , \underset{\sim}{Q}_\ell)$; en utilisant le fait que $\det(\rho_\ell) = \chi_\ell^{11}$, on en déduit que $g_\ell = \underset{\sim}{M}_2(\underset{\sim}{Q}_\ell)$, ce qui signifie bien que $\mathrm{Im}(\rho_\ell)$ est ouvert.

Il reste à montrer que le cas $s = 0$ est impossible. Or, si l'on avait $s = 0$, l'algèbre de Lie g_ℓ serait <u>abélienne</u>, et opèrerait de façon semi-simple sur V_ℓ . Si g_ℓ était l'algèbre des <u>homothéties</u> de V_ℓ , il y aurait un sous-groupe ouvert de $\mathrm{Im}(\rho_\ell)$ formé d'homothéties. On en conclut qu'il existerait une infinité de p tels que $\det(\rho_\ell(F_p)) = \mathrm{Tr}(\rho_\ell(F_p))^2/4$, i. e. $4p^{11} = \tau(p)^2$, ce qui est absurde. Ce cas écarté, on voit que le commutant de g_ℓ dans $\mathrm{End}(V_\ell)$ est une <u>algèbre de Cartan</u> h_ℓ , et que $\mathrm{Im}(\rho_\ell)$ est contenu dans le <u>normalisateur</u> N de h_ℓ . Vu la structure de N , il s'ensuit qu'il existe dans $\mathrm{Im}(\rho_\ell)$ un sous-groupe ouvert d'indice 1 ou 2 qui est abélien. En d'autres termes, il existe une extension E de $\underset{\sim}{Q}$, avec $[E:Q] \leqslant 2$, au-dessus de laquelle la représentation ρ_ℓ est <u>abélienne</u>. En appliquant à E et ρ_ℓ le théorème de [17] (chap. III, n° 3.1), on voit que ρ_ℓ est "localement algébrique" sur E . Mais, d'après le théorème de [17] (chap. III, n° 2.3), cela entraîne que toutes les représentations $\rho_{\ell'}$ (relatives aux divers nombres premiers ℓ') ont la même propriété. En particulier, chacun des groupes $\mathrm{Im}(\rho_{\ell'})$ possède un sous-groupe ouvert abélien d'indice 1 ou 2 . C'est absurde, puisque le groupe $\mathrm{Im}(\rho_{11,1})$, par exemple, n'est pas résoluble.

5.2. <u>Questions</u>.

(a) Peut-on déterminer l'image de ρ_ℓ , comme l'a fait SWINNERTON-DYER pour $\ell = 2$? Plus précisément, $\mathrm{Im}(\rho_\ell)$ est contenu dans le sous-groupe H_ℓ de $\underset{\sim}{GL}(2 , \underset{\sim}{Z}_\ell)$ formé des éléments dont le déterminant est une puissance 11-ième. Est-il vrai que $\mathrm{Im}(\rho_\ell) = H_\ell$ pour presque tout ℓ (ou même pour $\ell \neq 2 , 3 , 5 , 7 , 23 , 691$) ?

Il serait également intéressant de trouver une "raison" expliquant la forme si spéciale des représentations modulo $2 , 3 , 5 , 7 , 23 , 691$. Il y a des indications (conjecturales) là-dessus à la fin des notes de KUGA [9].

(b) L'ensemble des p tels que $\tau(p) \equiv 0 \pmod p$ est-il de densité nulle ? Est-il fini ? Est-il réduit à $\{2 , 3 , 5 , 7\}$?

Une analogie (assez vague) avec les représentations associées aux courbes elliptiques suggère que $\tau(p) \equiv 0 \pmod p$ peut avoir un rapport avec la structure du <u>groupe d'inertie</u> I_p de p dans $\mathrm{Im}(\rho_p)$, groupe qui est défini à conjugaison près. Par exemple, est-il vrai que I_p soit <u>ouvert</u> dans $\mathrm{Im}(\rho_p)$ si, et seulement si, $\tau(p) \equiv 0 \pmod p$?

Pour $p = 2, 3, 5, 7$, on a en tout cas $I_p = \mathrm{Im}(\rho_p)$. [Démonstration : pour ces valeurs de p, les congruences du § 2 montrent que $\mathrm{Im}(\rho_p)$ est extension du groupe $(\underset{\sim}{Z}/p\underset{\sim}{Z})^*$ par un pro-p-groupe ; le groupe quotient $(\underset{\sim}{Z}/p\underset{\sim}{Z})^*$ correspond au p-ième corps cyclotomique $\underset{\sim}{Q}(p)$. On en conclut que I_p s'applique sur $(\underset{\sim}{Z}/p\underset{\sim}{Z})^*$, et l'on est ramené à voir que $N \cap I_p = N$. Si l'on avait $N \cap I_p \neq N$, la théorie élémentaire des p-groupes montrerait l'existence d'un sous-groupe distingué fermé d'indice p de N contenant I_p ; ce sous-groupe correspondrait à une extension cyclique de degré p non ramifiée de $\underset{\sim}{Q}(p)$. D'après la théorie du corps de classes, il en résulterait que le nombre de classes du corps $\underset{\sim}{Q}(p)$ serait divisible par p et p serait "irrégulier" au sens de Kummer ; or, ce n'est pas le cas : $2, 3, 5, 7$ sont "réguliers".]

On notera que cet argument ne s'applique pas à $p = 691$, qui est irrégulier (puisqu'il divise le numérateur du nombre de Bernoulli b_{12}). En fait, il me paraît probable que, pour $p = 691$, on a $I_p \neq \mathrm{Im}(\rho_p)$, autrement dit qu'il intervient effectivement une extension non ramifiée de $\underset{\sim}{Q}(691)$. On pourrait peut-être trancher la question en examinant les valeurs de $\tau(p)$ modulo 691^2.

(c) La restriction de ρ_p au sous-groupe d'inertie I_p admet-elle une "décomposition de Hodge" (cf. [17], chap. III, n° 1.2) de type $(0, 11)$?

(d) Si l'on admet la conjecture de Ramanujan $|\tau(p)| < 2p^{11/2}$, on peut écrire le polynôme $H_p(X)$ du n° 1.3 sous la forme

$$H_p(X) = (1 - \alpha_p X)(1 - \bar{\alpha}_p X) \quad , \tag{30}$$

avec $\alpha_p = p^{11/2} e^{i\omega_p}$, $0 < \omega_p < \pi$.

Est-il vrai que les angles ω_p soient équirépartis dans l'intervalle $(0, \pi)$ pour la mesure $\frac{2}{\pi} \sin^2 \omega \, d\omega$, comme SATO et TATE l'ont conjecturé dans le cas elliptique sans multiplication complexe ?

La question est liée ([17], chap. I, A.2) à celle du prolongement analytique des séries de Dirichlet

$$L_m(s) = \prod_p \prod_{n=0}^{m} \frac{1}{(1 - \alpha_p^n \bar{\alpha}_p^{m-n} p^{-s})} \quad , \qquad m = 1, 2, \ldots \quad . \tag{31}$$

Il faudrait démontrer que $L_m(s)$ est prolongeable en une fonction entière de s ne s'annulant pas au point

$$s = 1 + \frac{11m}{2} \quad .$$

Bien entendu, il y a lieu aussi de conjecturer que $L_m(s)$ a une équation fonctionnelle du type usuel. Plus précisément, il doit exister un "terme à l'infini" $\gamma_m(s)$ tel que $\gamma_m(s)\, L_m(s)$ soit invariant (ou anti-invariant) par

$$s \longmapsto 11m + 1 - s \ .$$

On peut même se risquer à conjecturer la forme de $\gamma_m(s)$:

(32)
$$\gamma_m(s) = (2\pi)^{-ks}\, \Gamma(s)\, \Gamma(s - 11) \ldots \Gamma(s - 11(k-1)) \qquad \text{si } m = 2k - 1 \ ,$$
$$\gamma_m(s) = \pi^{-s/2}\, \Gamma\Big(\frac{s - 11k + \varepsilon}{2}\Big)\, \gamma_{m-1}(s) \quad \text{si } m = 2k \ , \ \text{où } \varepsilon = \begin{cases} 0 & (k \text{ pair}) \\ 1 & (k \text{ impair}). \end{cases}$$

Il semble que seuls les cas $m = 1$ et $m = 2$ soient connus : $L_1(s)$ coïncide avec la fonction $L_\tau(s)$ du n° 1.3, et $L_2(s)$ est liée par une formule simple à la fonction

(33)
$$f(s) = \sum_1^\infty \tau^2(n)/n^s$$

étudiée par RANKIN (cf. HARDY [5], p. 174-180).

5.3. Généralisation aux formes modulaires.

Ce qui a été dit pour τ peut l'être aussi pour les coefficients de toute forme parabolique de poids k

(34)
$$\Phi(x) = \sum_{n=1}^\infty a_n X^n \ , \qquad a_1 = 1 \ ,$$

qui est fonction propre des opérateurs de Hecke, et dont les coefficients appartiennent à $\underset{\sim}{Z}$. On peut, ici encore, prouver que $\mathrm{Im}(\rho_\ell)$ est ouvert dans $\underset{\sim}{GL}(2, \underset{\sim}{Q}_\ell)$.

D'après KUGA ([9], dernière partie), on peut s'attendre à ce que les représentations modulo 2 , 3 , 5 , 7 aient des propriétés spéciales ; il serait intéressant de les déterminer, et aussi d'examiner le cas des autres nombres premiers.

Exemple : Prenons $k = 16$, auquel cas on a

(35)
$$\Phi(x) = D(x)\, E_4(x) = \Big(\sum_{n=1}^\infty \tau(n) x^n\Big)\Big(1 + 240 \sum_{n=1}^\infty \sigma_3(n) x^n\Big) \ .$$

On constate facilement que

(36)
$$a_p \equiv p + p^2 \pmod 7 \ ,$$

(37)
$$a_p \equiv 1 + p^{15} \pmod{3617} \ .$$

(Noter que 3617 est le numérateur du nombre de Bernoulli b_{16} ; c'est un nombre premier irrégulier.)

Quant aux formes paraboliques de $\underline{SL}(2 , \underline{Z})$ qui sont fonctions propres des opérateurs de Hecke, mais ne sont pas à coefficients entiers, il doit leur correspondre des représentations " E-rationnelles" au sens de [17] (chap. I, n° 2.3). D'ailleurs, si l'espace des formes paraboliques est de dimension h , on doit pouvoir lui associer des représentations ℓ-adiques de degré $2h$ sur lesquelles opèrent les T_p de Hecke, et c'est en réduisant ces représentations par rapport à l'algèbre de Hecke que l'on trouve les représentations de degré 2 qui nous intéressent.

§ 6. Historique

L'idée d'interpréter certaines fonctions arithmétiques comme des traces d'opérateurs de Frobenius remonte à DAVENPORT-HASSE [3]. Toutefois, il ne s'agissait surtout que de sommes exponentielles dont les propriétés étaient connues (sommes de Gauss, sommes de Jacobi). La note de WEIL [20] va plus loin ; elle donne une interprétation "frobeniusienne" de toutes les sommes exponentielles à une variable, et on obtient (grâce à "l'hypothèse de Riemann pour les courbes") une majoration qui n'était pas connue. Ainsi, pour les sommes de Kloosterman

$$(38) \qquad S_p(a , b) = \sum_{x=1}^{p-1} \exp\left(\frac{2\pi i}{p} (ax + bx^{-1})\right) , \qquad ab \not\equiv 0 \pmod{p} ,$$

on trouve :

$$(39) \qquad |S_p(a , b)| \leqslant 2p^{1/2} .$$

WEIL avait remarqué depuis longtemps l'analogie de la conjecture de Ramanujan

$$|\tau(p)| \leqslant 2p^{11/2}$$

avec l'inégalité (39). Il avait suggéré que l'on devait pouvoir écrire $\tau(p)$ sous la forme $\tau(p) = \alpha_p + \bar{\alpha}_p$, où α_p et $\bar{\alpha}_p$ sont des valeurs propres d'un endomorphisme de Frobenius, opérant sur une cohomologie de dimension 11 convenable. D'autre part, en 1960, il m'avait demandé quelle pouvait être, de ce point de vue, l'interprétation des congruences connues sur $\tau(p)$ (j'avais été incapable de lui répondre, faute d'avoir compris le rapport entre "cohomologie" et "représentations ℓ-adiques").

Un pas important vers l'interprétation cohomologique de $\tau(p)$ a été fait par EICHLER [4] ; il a montré comment les coefficients des formes paraboliques de poids

2 (pour certains sous-groupes de congruence du groupe modulaire) sont liés aux "modules de Tate" de la courbe modulaire correspondante. Ses résultats ont été repris par SHIMURA [18], puis complétés sur un point essentiel par IGUSA [7].

Pour un poids k quelconque, SATO (cf. [10], introduction) a eu l'idée de considérer la variété fibrée en produit de k - 2 fois la courbe elliptique générique (la base étant la courbe modulaire). Les idées de SATO ont été précisées et mises en forme par KUGA-SHIMURA [10], à cela près que :

1° Ils s'expriment en "nombre de points" et non en "groupes de cohomologie" ; ils n'obtiennent donc pas de représentations ℓ-adiques.

2° Le groupe qu'ils considèrent n'est pas le groupe modulaire $SL(2, \mathbb{Z})$ mais un groupe d'unités de quaternions, qui est à quotient compact (ce qui facilite leur tâche).

Toutefois, on pouvait espérer que les idées de SATO et KUGA-SHIMURA, combinées avec les théorèmes généraux sur la cohomologie ℓ-adique dus à A. GROTHENDIECK et M. ARTIN [1], permettraient d'aboutir à une théorie applicable au groupe modulaire et à ses sous-groupes de congruence. Cet espoir semble sur le point de se réaliser: P. DELIGNE aurait réussi à démontrer plus qu'il n'en faut pour établir la conjecture du n° 3.2 et pour ramener la conjecture de Ramanujan aux "conjectures standard" de Weil (ce dernier point avait d'ailleurs été déjà traité par IHARA [8] par une méthode extrêmement ingénieuse). Pour plus de détails, voir le séminaire de DELIGNE à l'I. H. E. S., "Conjecture de Ramanujan et représentations ℓ-adiques", qui commence le 28 février 1968.

BIBLIOGRAPHIE

[1] ARTIN (M.) et GROTHENDIECK (A.). - Cohomologie étale des schémas, Séminaire de géométrie algébrique, Institut des Hautes Etudes Scientifiques, Bures-sur-Yvette, 1963/64.

[2] BAMBAH (R. P.). - Two congruence properties of Ramanujan's function $\tau(n)$, J. London math. Soc., t. 21, 1946, p. 91-93.

[3] DAVENPORT (H.) und HASSE (H.). - Die Nullstelle der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. für reine und angew. Math. [J. Crelle], t. 172, 1935, p. 151-182.

[4] EICHLER (M.). - Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion, Archiv der Math., t. 5, 1954, p. 355-366.

[5] HARDY (G. H.). - Ramanujan (Twelve lectures on subjects suggested by his life and his work). - Cambridge University Press, 1940 [Reprint : New York, Chelsea publishing Company, 1959].

[6] HECKE (E.). - Mathematische Werke. - Göttingen, Vandenhoeck und Ruprecht, 1959.

[7] IGUSA (J.). - Kroneckerian model of fields of elliptic modular functions, Amer. J. of Math., t. 81, 1959, p. 561-577.

[8] IHARA (Y.). - Hecke polynomials as congruence ζ functions in elliptic modular case, Annals of Math., Series 2, t. 85, 1967, p. 267-295.

[9] KUGA (M.). - Fiber varieties over a symmetric space whose fibers are abelian varieties [Notes polycopiées], University of Chicago, 1963/64.

[10] KUGA (M.) and SHIMURA (G.). - On the zeta function of a fibre variety whose fibres are abelian varieties, Annals of Math., Series 2, t. 82, 1965, p. 478-539.

[11] LEHMER (D. H.). - Ramanujan's function $\tau(n)$, Duke math. J., t. 10, 1943, p. 483-492.

[12] LEHMER (D. H.). - The vanishing of Ramanujan's function $\tau(n)$, Duke math. J., t. 14, 1947, p. 429-433.

[13] LEHMER (D. H.). - Notes on some arithmetical properties of elliptic modular functions [Notes polycopiées, Berkeley, non datées].

[14] MORDELL (L. J.). - On Mr Ramanujan's empirical expressions of modular functions, Proc. Cambridge phil. Soc., t. 19, 1917, p. 117-124.

[15] RAMANATHAN (K. G.). - Congruence properties of Ramanujan's function $\tau(n)$, (II), J. Indian math. Soc., t. 9, 1945, p. 55-59.

[16] RAMANUJAN (S.). - On certain arithmetical functions, Trans. Cambridge phil. Soc., t. 22, 1916, p. 159-184.

[17] SERRE (J.-P.). - Abelian ℓ-adic representations and elliptic curves. - New York, Benjamin, 1968.

[18] SHIMURA (G.). - Correspondances modulaires et les fonctions zêtas des courbes algébriques, J. Math. Soc. Japan, t. 10, 1958, p. 1-28.

[19] SHIMURA (G.). - A reciprocity law in non-solvable extensions, J. für reine und angew. Math. [J. Crelle], t. 221, 1966, p. 209-220.

[20] WEIL (A.). - On some exponential sums, Proc. Nat. Acad. Sc. U. S. A., t. 34, 1948, p. 204-207.

[21] WILTON (J. R.). - Congruence properties of Ramanujan's function $\tau(n)$, Proc. London math. Soc., t. 31, 1930, p. 1-10.