CONGRUENCES ET FORMES MODULAIRES

[d'après H. P. F. SWINNERTON-DYER]

par Jean-Pierre SERRE

Diverses fonctions arithmétiques sont définies comme <u>coefficients</u> de fonctions modulaires. Citons notamment :

$\tau(n)$, coef. de q^n dans $\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}$ (fonction de Ramanujan) ,

$c(n)$, coef. de q^n dans l'invariant modulaire $j = q^{-1} + 744 + \dots$,

$p(n)$, coef. de q^n dans $1/\prod_{n=1}^{\infty}(1-q^n)$ (fonction de partition),

$\sigma_h(n) = \sum_{d|n} d^h$, coef. de q^n dans la série d'Eisenstein G_{h+1} ,

$\zeta(-h)$, terme constant de $2\,G_{h+1}$ (h impair ≥ 1).

Ces fonctions sont liées entre elles par de nombreuses congruences, qu'il n'est guère possible de résumer en un exposé ; on en trouvera des échantillons dans [1], [9], [10], [11], [15]. Je me bornerai à un théorème de structure (§ 1) et à deux applications : l'une aux valeurs des fonctions zêta aux entiers négatifs (§ 2), l'autre aux représentations ℓ-adiques attachées aux formes modulaires (§ 3). La méthode suivie est due à Swinnerton-Dyer [18].

§ 1. <u>Réduction</u> mod. p <u>des formes modulaires</u>

1.1. <u>Rappel sur les formes modulaires</u>

(On se borne aux formes modulaires relativement au groupe $SL_2(\mathbf{Z})$ tout entier ; le cas d'un groupe de congruence n'est pas encore au point.)

Soit k un entier. Une <u>forme modulaire</u> de poids k est une fonction holomorphe f sur le demi-plan de Poincaré H , vérifiant les deux conditions suivantes :

1) $f(-1/z) = z^k f(z)$ pour tout $z \in H$,

2) Il existe des $a_n \in \mathbf{C}$ tels que, si l'on pose $q = e^{2\pi i z}$, on ait

$$f(z) = a_0 + a_1 q + \dots + a_n q^n + \dots ,$$

la série étant absolument convergente pour $z \in H$, i.e. pour $|q| < 1$. Si $f \not\equiv 0$, k est nécessairement pair, et ≥ 0.

Lorsque k est pair ≥ 4, un exemple de telle fonction est donné par la série d'Eisenstein de poids k, que nous écrirons :

$$G_k = \tfrac{1}{2}\,\zeta(1-k) + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n ,$$

où ζ est la fonction zêta de Riemann, et $\sigma_{k-1}(n)$ est la somme des puissances $(k-1)$-èmes des diviseurs de n. On sait que $\zeta(1-k) = -b_k/k$, où b_k est le k-ième nombre de Bernoulli ; la série G_k est donc une série à coefficients rationnels (et même entiers, mis à part le terme constant).

Il est souvent commode de normaliser les G_k de telle sorte que leur terme constant soit 1 ; cela conduit aux fonctions :

$$E_k = -\frac{2k}{b_k} G_k = 1 - \frac{2k}{b_k} \sum \sigma_{k-1}(n) q^n .$$

En particulier :

$$E_4 = 240\, G_4 = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \qquad (b_4 = -1/30)$$

$$E_6 = -504\, G_6 = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n \qquad (b_6 = 1/42) .$$

Posons $E_4 = Q$ et $E_6 = R$, cf. Ramanujan [12]. Ces fonctions sont algébriquement indépendantes, et engendrent l'algèbre (graduée) des formes modulaires : toute forme modulaire de poids k s'écrit de façon unique comme combinaison linéaire des monômes $Q^a R^b$ tels que $4a + 6b = k$. On a, par exemple :

$$E_8 = Q^2 , \quad E_{10} = QR , \quad E_{12} = \frac{441\, Q^3 + 250\, R^2}{691} , \quad E_{14} = Q^2 R ,$$

et

$$\frac{Q^3 - R^2}{1728} = \Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n .$$

1.2. Réduction modulo p de l'algèbre des formes modulaires

Soient p un nombre premier, et v_p la valuation correspondante du corps $\mathbb{Q}$. Une série formelle

$$f = \sum_{n \geq 0} a_n q^n , \qquad a_n \in \mathbb{Q} ,$$

est dite *p-entière* si $v_p(a_n) \geq 0$ pour tout n ; sa réduction (mod. p) est la série formelle

$$\tilde{f} = \Sigma \tilde{a}_n q^n \in \mathbb{F}_p[[q]] ,$$

ou $\tilde{a}_n$ désigne l'image de a_n dans $\mathbb{F}_p$. Nous écrirons indifféremment $\tilde{f} = \tilde{f}'$ ou $f \equiv f'$ (mod.p) .

Notons $\tilde{M}_k$ l'ensemble des $\tilde{f}$, où f parcourt les formes modulaires de poids k , à coefficients rationnels, qui sont p-entières. La somme $\tilde{M}$ des $\tilde{M}_k$ est une sous-algèbre de $\mathbb{F}_p[[q]]$; c'est l'algèbre des formes modulaires (mod.p) . Nous allons déterminer sa structure.

Lorsque $p = 2$ ou 3 , on a $\tilde{Q} = \tilde{R} = 1$, et on en déduit que $\tilde{M}$ est l'algèbre de polynômes $\mathbb{F}_p[\tilde{\Delta}]$.

Supposons désormais $p \geq 5$. Soit

$$f = \Sigma\, c_{a,b}\, Q^a R^b$$

une forme modulaire de poids k , écrite comme polynôme isobare en Q et R . Pour que f soit p-entière, il faut et il suffit que les $c_{a,b}$ soient rationnels et p-entiers ; cela se vérifie par récurrence sur k , en utilisant le fait que Δ est combinaison linéaire à coefficients p-entiers de Q^3 et de R^2 . Il en résulte que $\tilde{M}_k$ admet pour base la famille des monômes $\tilde{Q}^a\tilde{R}^b$, où $4a+6b=k$ et l'algèbre $\tilde{M}$ est engendrée par $\tilde{Q}$ et $\tilde{R}$; tout revient donc à déterminer l'idéal $\mathfrak{a} \subset \mathbb{F}_p[X,Y]$ des relations entre $\tilde{Q}$ et $\tilde{R}$, i.e. l'idéal des polynômes f tels que $f(\tilde{Q},\tilde{R}) = 0$.

THÉORÈME 1 ([18]).- *L'idéal $\mathfrak{a}$ est l'idéal principal engendré par $A - 1$, où $A \in \mathbb{F}_p[X,Y]$ est le polynôme isobare de poids $p-1$ tel que $A(\tilde{Q},\tilde{R}) = \tilde{E}_{p-1}$.*

(On rappelle que E_{p-1} est la série d'Eisenstein de poids $p-1$, normalisée de telle sorte que son terme constant soit 1 .)

Exemples

$p = 5$. On a $E_{p-1} = E_4 = Q$, d'où $A = X$; l'idéal des relations entre $\tilde{Q}$ et $\tilde{R}$ est engendré par la relation $\tilde{Q} = 1$; l'algèbre $\tilde{M}$ est isomorphe à $\mathbb{F}_5[\tilde{R}]$.

$p = 7$. On a $E_{p-1} = E_6 = R$; la relation fondamentale est $\tilde{R} = 1$; on a $\tilde{M} = \mathbb{F}_7[\tilde{Q}]$.

$p = 11$. On a $E_{10} = QR$; la relation fondamentale est $\tilde{Q}\tilde{R} = 1$.

$p = 13$. On a $E_{12} \equiv 6Q^3 - 5R^2 \pmod{13}$; la relation fondamentale est $6\tilde{Q}^3 - 5\tilde{R}^2 = 1$.

Démonstration du théorème 1

On sait que $v_p(b_{p-1}) = -1$, cf. par exemple [2], p. 431. La formule $E_{p-1} \equiv 1 \pmod{p}$ en résulte. L'idéal $\mathfrak{a}$ contient donc $A - 1$. De plus, A est sans facteurs multiples (voir ci-après) ; cela entraîne que $A - 1$ est irréductible (et même absolument irréductible), et l'idéal $\mathfrak{a}'$ engendré par $A - 1$ est premier. D'autre part, $\mathfrak{a}$ est premier (puisque $\tilde{M}$ est intègre) et n'est pas un idéal maximal (sinon, $\tilde{M}$ serait fini, ce qui n'est pas le cas puisque les monômes $\tilde{Q}^a\tilde{R}^b$ d'un poids donné sont linéairement indépendants). Soit $\mathfrak{m}$ un idéal maximal de $\mathbb{F}_p[X,Y]$ contenant $\mathfrak{a}$. Si l'on avait $\mathfrak{a}' \neq \mathfrak{a}$, la chaîne d'idéaux premiers

$$0 \subset \mathfrak{a}' \subset \mathfrak{a} \subset \mathfrak{m}$$

serait de longueur 3 , contrairement au fait que la dimension de $\mathbb{F}_p[X,Y]$ est 2 . On a donc $\mathfrak{a}' = \mathfrak{a}$, d'où le théorème

Remarque.- Munissons $\mathbb{F}_p[X,Y]$ de la graduation à valeurs dans $\mathbb{Z}/(p-1)\mathbb{Z}$ déduite par passage au quotient de la graduation où X est de poids 4 et Y de poids 6 . L'élément $A - 1$ est alors de poids 0 ; l'idéal qu'il engendre est donc gradué ; vu le th. 1, cela entraîne que l'algèbre quotient $\tilde{M} = \mathbb{F}_p[X,Y]/\mathfrak{a}$ est graduée, le groupe des degrés étant $\mathbb{Z}/(p-1)\mathbb{Z}$. Ainsi, $\tilde{M}$ est somme directe des $\tilde{M}^{\alpha}$ ($\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$) où $\tilde{M}^{\alpha}$ est réunion croissante des $\tilde{M}_k$, pour $k \equiv \alpha \pmod{(p-1)}$. En particulier :

THÉORÈME 2.- *Soient* f *et* f' *des formes modulaires* p*-entières de poids* k *et* k' . *Si* $f \equiv f' \pmod{p}$, *et si* $f \not\equiv 0 \pmod{p}$, *on a* $k \equiv k' \pmod{(p-1)}$.

Une forme modulaire (mod.p) a donc un "poids" modulo $(p-1)$.

Remarque.- Sous les hypothèses du th. 2, si $f \equiv f' \pmod{p^n}$, on peut montrer que $k \equiv k' \pmod{p^{n-1}(p-1)}$.

1.3. Interprétation elliptique

Soit E une courbe elliptique, définie par une équation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 .$$

Notons c_4 et c_6 les covariants correspondants (les notations étant celles de Tate, cf. [16], n° 5.1), et ω la forme différentielle de 1ère espèce $dx/(2y + a_1y + a_3)$. Si f est un polynôme isobare de poids k en Q , R (i.e. une forme modulaire), la forme différentielle

$$\omega_f = f(c_4, -c_6)\omega^k \qquad \text{(forme " de poids } k \text{ ")}$$

ne dépend que de E , et pas de sa réalisation comme cubique plane.

Ceci s'applique notamment, en caractéristique p , au polynôme A correspondant à la forme modulaire $\widetilde{E}_{p-1}$, cf. th. 1. On a :

THÉORÈME 3 (Deligne).- La forme ω_A est l'invariant de Hasse de E .

(Pour tout ce qui concerne l'invariant de Hasse, voir par exemple Deuring [4].)

L'invariant de Hasse est de la forme $\omega_{A'}$, où A' est un certain polynôme isobare de poids $p-1$, et il s'agit de prouver que $A' = A$. Cela peut se faire par calcul direct, en explicitant la multiplication par p dans le groupe formel attaché à E . Deligne procède autrement ; il commence par le cas de la courbe de Tate sur le corps $\mathbb{F}_p((q))$ des séries formelles en q (cf. [13]), et observe que son invariant de Hasse est $(du/u)^{p-1}$; il en déduit que $A'(\widetilde{Q}, \widetilde{R})$, considérée comme série formelle en q , est égale à 1 , d'où aussitôt $A' = A$.

COROLLAIRE 1.- Le polynôme A est sans facteurs multiples.

En effet, c'est là un résultat bien connu pour l'invariant de Hasse ([4],[6]).

COROLLAIRE 2.- L'algèbre $\widetilde{M}^0$ des formes modulaires (mod.p) de poids nul modulo $(p-1)$ est isomorphe à l'algèbre affine sur $\mathbb{F}_p$ de la courbe X obtenue en retirant de la droite projective les valeurs de j correspondant aux courbes d'invariant de Hasse nul.

Si $f \in \widetilde{M}_k$, avec $k = h(p-1)$, on lui associe $f/\widetilde{E}_{p-1}^h$, qui est une fonction rationnelle de $j = \widetilde{Q}^3/\widetilde{\Delta}$, régulière sur X . On vérifie sans peine que l'on obtient ainsi un isomorphisme de $\widetilde{M}^0$ sur l'algèbre affine de X .

Signalons aussi une interprétation "elliptique" de l'algèbre $\widetilde{M}$ tout entière : elle correspond à un certain revêtement galoisien de X , de groupe de Galois $\mathbb{F}_p^*/\{\pm 1\}$, cf. Igusa [7].

1.4. Dérivation des formes modulaires

a) Le cas complexe

Posons

$$P = E_2 = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n , \qquad \text{où } q = e^{2\pi i z} .$$

La fonction $P(z)$ est "presque" modulaire de poids 2 ; elle vérifie, non l'identité $f(-1/z) = z^2 f(z)$, mais :

$$(*) \qquad P(-1/z) = z^2 P(z) + \frac{12\, z}{2i\pi} .$$

D'autre part, si $f = \Sigma a_n q^n$, posons $\theta f = \frac{1}{2i\pi} df/dz = q\, df/dq = \Sigma n a_n q^n$. L'application θ ainsi définie est une dérivation.

THÉORÈME 4 (Ramanujan [12]).- (i) *Si* f *est une forme modulaire de poids* k , $\theta f - \frac{k}{12} Pf$ *est une forme modulaire de poids* $k+2$.

(ii) *On a* $\theta P = \frac{1}{12}(P^2 - Q)$, $\theta Q = \frac{1}{3}(PQ - R)$, $\theta R = \frac{1}{2}(PR - Q^2)$.

L'assertion (i) se démontre en dérivant par rapport à z la formule $f(-1/z) = z^k f(z)$, et en utilisant $(*)$. On en déduit que $\theta Q - PQ/3$ est une forme modulaire de poids $4 + 2 = 6$; comme son terme constant est $-1/3$, c'est nécessairement $-R/3$. On démontre de la même manière la formule donnant θR . Celle donnant θP s'obtient en dérivant $(*)$, et en montrant que $\theta P - P^2/12$ est une forme modulaire de poids 4 .

Exemple.- On a $\partial \Delta = 0$ et $\theta \Delta = P\Delta$; P est la "dérivée logarithmique" de Δ .

COROLLAIRE 1.- *Soit* ∂ *la dérivation de l'algèbre des formes modulaires telle que* $\partial Q = -4R$ *et* $\partial R = -6Q^2$. *Si* f *est une forme modulaire de poids* k , ∂f *est de poids* $k+2$, *et l'on a*

$$12\, \theta f = k Pf + \partial f .$$

Cela résulte de (i) et (ii).

COROLLAIRE 2.- *L'algèbre engendrée par* P , Q , R *est stable par* θ .

Cela résulte de (ii).

b) Passage à la caractéristique p (*)

La dérivation θ , la série P gardent un sens évident en caractéristique p ; il en est de même de ∂ , considérée comme dérivation de l'algèbre $\mathbb{F}_p[X,Y]$ des polynômes en deux variables. Si $F \in \mathbb{F}_p[X,Y]$ est isobare de poids k , et si $f = F(\widetilde{Q},\widetilde{R})$ est l'élément correspondant de $\widetilde{M}_k$, on a encore

$$12\,\theta f = k\,Pf + \partial F(\widetilde{Q},\widetilde{R}) ,$$

formule que l'on se permettra aussi d'écrire $12\,\theta f = k\,Pf + \partial f$.

La différence essentielle (et agréable) avec le cas complexe est que P devient une "vraie" forme modulaire (mod.p) , de poids $p+1$:

THÉORÈME 5 ([18]).- (i) *On a* $P \equiv E_{p+1}$ (mod.p) .

(ii) *Si* B *désigne le polynôme isobare de poids* $p+1$ *tel que* $\widetilde{E}_{p+1} = B(\widetilde{Q},\widetilde{R})$, *on a* $\partial A = B$ *et* $\partial B = -\widetilde{Q}A$.

(A partir de maintenant, on se permet de noter $\widetilde{Q}$, $\widetilde{R}$ les variables X , Y des polynômes A , B ,... considérés.)

Exemple.- Pour $p = 5$, on a $B = \widetilde{E}_6 = \widetilde{R}$, d'où $\partial A = \partial\widetilde{Q} = -4\widetilde{R} = \widetilde{R} = B$, et $\partial B = -6\widetilde{Q}^2 = -\widetilde{Q}^2 = -\widetilde{Q}A$.

Démonstration du théorème 5

L'assertion (i) résulte des deux congruences :

$$\sigma_p(n) = \sum_{d|n} d^p \equiv \sum_{d|n} d = \sigma_1(n) \qquad (\text{mod.}p) ,$$

$$b_{p+1}/(p+1) \equiv b_2/2 = -1/12 \qquad (\text{mod.}p) , \quad \text{cf. [2], p. 433.}$$

D'autre part, puisque $E_{p-1} \equiv 1$ (mod.p) , on a $\theta E_{p-1} \equiv 0$ (mod.p) , d'où $(p-1)\widetilde{P}.\widetilde{E}_{p-1} + \partial A(\widetilde{Q},\widetilde{R}) = 0$, i.e. $\partial A(\widetilde{Q},\widetilde{R}) = \widetilde{P} = \widetilde{E}_{p+1} = B(\widetilde{Q},\widetilde{R})$, ce qui démontre la formule $\partial A = B$. Celle donnant ∂B se démontre par un argument analogue, en dérivant une nouvelle fois.

COROLLAIRE 1.- *Les polynômes* A *et* B *sont étrangers entre eux. Le polynôme* A *est sans facteurs multiples.*

Cela résulte des formules $\partial A = B$ et $\partial B = -\widetilde{Q}A$ par un argument standard

(*) Ici encore, on suppose $p \geq 5$.

(tout polynôme vérifiant une équation différentielle du second ordre est premier à sa dérivée, cf. Igusa [6]).

COROLLAIRE 2.- <u>L'algèbre</u> $\widetilde{M}$ <u>des formes modulaires</u> (mod.p) <u>est stable par</u> θ .

En effet, si $f \in \widetilde{M}_k$, on a

$$12\,\theta f = k\,Pf + \partial f = k\,Bf + A\partial f ,$$

et Bf et $A\partial f$ appartiennent à $\widetilde{M}_{k+p-1}$.

L'argument ci-dessus conduit en fait à un résultat plus précis. Si $f \in \widetilde{M}$, appelons <u>filtration</u> de f , et notons $w(f)$, le plus petit entier k tel que f appartienne à $\widetilde{M}_k$; si $f = 0$, on convient que $w(f) = -\infty$. Dire que f est de filtration k équivaut à dire que f est de la forme $F(\widetilde{Q},\widetilde{R})$, où F est un polynôme isobare de degré k , à coefficients dans $\mathbb{F}_p$, <u>non divisible par</u> A .

COROLLAIRE 3.- <u>On a</u> $w(\theta f) \leq w(f) + p+1$, <u>et il y a égalité si et seulement si</u> $w(f) \not\equiv 0 \pmod{p}$.

Posons $k = w(f)$. L'inégalité $w(\theta f) \leq w(f) + p + 1$ résulte de la formule $12\,\theta f = k\,Bf + A\partial f$. Si k est divisible par p , cette formule montre que $12\,\theta f = \partial f$ est de filtration $\leq k + 2$. Si $k \not\equiv 0 \pmod{p}$, et si $f = F(\widetilde{Q},\widetilde{R})$ comme ci-dessus, le polynôme $k\,B.F$ n'est pas divisible par A (en effet, B est étranger à A , et F n'est pas divisible par A) ; il en résulte que la filtration de θf est bien $k + p + 1$.

<u>Exemples</u>

Prenons $p = 5$, et $f = \widetilde{G}_6 = -\widetilde{R}$. Le cor. 3 montre que θf est modulaire (mod.5) , de poids $6 + p + 1 = 12$. Comme θf commence par q , on a donc $\theta f = \widetilde{\Delta}$, d'où la congruence

$$n\,\sigma_5(n) \equiv \tau(n) \qquad \pmod{5} .$$

Pour $p = 7$, le même argument montre que $\theta\widetilde{G}_4 = \widetilde{\Delta}$, d'où :

$$n\,\sigma_3(n) \equiv \tau(n) \qquad \pmod{7} .$$

§ 2. Valeurs des fonctions zêta aux entiers négatifs

2.1. Résultats

Soient K un corps de nombres algébriques totalement réel de degré r, et ζ_K sa fonction zêta. Si m est un entier pair > 0, on sait, d'après Siegel, que $\zeta_K(1-m)$ est un nombre rationnel non nul. On va donner une estimation du dénominateur de ce nombre rationnel, ainsi que des congruences reliant les $\zeta_K(1-m)$ entre eux.

La méthode utilisée est celle de Klingen [8] et Siegel [17]. Elle consiste à associer à m la série

$$f_m = 2^{-r}\,\zeta_K(1-m) + \sum_{\mathfrak{a}} \sum_{\substack{\nu \gg 0 \\ \nu \in \mathfrak{d}^{-1}\mathfrak{a}}} (N\mathfrak{a})^{m-1}\, q^{\mathrm{Tr}(\nu)} .$$

(Dans cette formule, $\mathfrak{d}$ désigne la différente de K ; la sommation porte sur les idéaux entiers $\mathfrak{a}$ de K, et sur les éléments ν totalement positifs et non nuls de $\mathfrak{d}^{-1}\mathfrak{a}$; pour un tel ν, $\mathrm{Tr}(\nu)$ est un entier ≥ 1.)

On démontre (loc. cit.) que f_m est une forme modulaire de poids $k = rm$ (mis à part le cas $r = 1$, $m = 2$, que nous excluons dans ce qui suit) ; c'est l'image réciproque par le plongement diagonal de H dans $H^r = H \times \ldots \times H$ d'une série d'Eisenstein du corps K, au sens de Hecke ([5], n° 20).

Si l'on écrit f_m sous la forme

$$f_m = a_m(0) + \sum_{n=1}^{\infty} a_m(n)\, q^n ,$$

les coefficients $a_m(n)$ ont les propriétés que voici :

a) $2^r a_m(0)$ est le nombre $\zeta_K(1-m)$ qui nous intéresse,

b) $a_m(n)$ est entier pour tout $n \geq 1$,

c) $a_m(n) \equiv a_{m'}(n) \pmod{p}$ si $n \geq 1$ et $m' \equiv m \pmod{p-1}$.

Nous allons voir que ces renseignements suffisent à entraîner les résultats suivants :

THÉORÈME 6.- Soit p un nombre premier ≥ 3.

(i) Si $rm \not\equiv 0 \pmod{p-1}$, $\zeta_K(1-m)$ est p-entier.

(ii) Si $rm \equiv 0 \pmod{p-1}$, on a $v_p(\zeta_K(1-m)) \geq -1 - v_p(rm)$.

THÉORÈME 6'.- On a $v_2(\zeta_K(1-m)) \geq r-2-v_p(rm)$.

Ces deux théorèmes donnent une estimation du dénominateur de $\zeta_K(1-m)$. Cette estimation, bien que meilleure que celle de Siegel [17], n'est pas comlètement satisfaisante ; par exemple, dans le th. 6 (i), il devrait être possible de remplacer rm par $r'm$, où r' est le degré de l'intersection de K avec le p-ième corps cyclotomique.

THÉORÈME 7.- Si $m' \equiv m \pmod{(p-1)}$, et si $rm \not\equiv 0 \pmod{(p-1)}$, on a

$$\zeta_K(1-m) \equiv \zeta_K(1-m') \pmod{p} .$$

(Pour $K = \mathbb{Q}$, on retrouve la congruence de Kummer, cf. [2], p. 433.)

Il est facile d'obtenir par la même méthode des congruences plus générales. Il est même probablement possible d'obtenir une "fonction zêta p-adique" à la Kubota-Leopoldt, mais cela exige des calculs que je n'ai pas encore menés à bien. De toutes façons, pour obtenir des résultats vraiment satisfaisants, il sera sans doute nécessaire de se placer sur H^r et non plus sur H , i.e. d'utiliser des formes modulaires à r variables.

2.2. Démonstration du théorème 6

(On se borne au cas $p \geq 5$.)

Vu ce qui précède, il suffit de prouver :

THÉORÈME 8.- Soit $f = a_0 + a_1 q + \ldots + a_n q^n + \ldots$ une forme modulaire de poids k dont les coefficients a_n , $n \geq 1$, sont p-entiers. Alors :

(i) Si $k \not\equiv 0 \pmod{(p-1)}$, a_0 est p-entier.

(ii) Si $k \equiv 0 \pmod{(p-1)}$, on a $v_p(a_0) \geq -v_p(k) - 1$.

Supposons que a_0 ne soit pas p-entier, et posons $v_p(a_0) = -s$, avec $s \geq 1$. La forme modulaire $p^s f$ a tous ses coefficients p-entiers, et sa réduction (mod.p) est une constante $\neq 0$. La fonction 1 est donc une forme modulaire (mod.p) de poids k ; comme elle est aussi de poids 0 , le th. 2 du n° 1.2 montre que k est divisible par $(p-1)$, d'où (i).

Supposons maintenant que s soit strictement plus grand que $s' = v_p(k) + 1$. Ecrivons la série d'Eisenstein G_k sous la forme

$$G_k = c + \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, q^n .$$

Le théorème de von Staudt ([2], p. 431) montre que $v_p(c) = -s'$. On a donc $v_p(\frac{c}{a_o}) \geq 1$. Posons

$$g = G_k - \frac{c}{a_o} f .$$

Le terme constant de g est nul ; les autres coefficients sont p-entiers, et l'on a

$$g \equiv \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, q^n \qquad (\text{mod.} p) .$$

Pour tirer de là une contradiction, il suffit donc de prouver :

LEMME.- <u>Si</u> k <u>est divisible par</u> $p-1$, <u>la série formelle à coefficients dans</u> $\mathbf{F}_p$:

$$\varphi = \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, q^n ,$$

<u>n'est pas une forme modulaire de poids</u> k , <u>i.e. n'appartient pas à</u> $\widetilde{M}_k$ (cf. n° 1.2).

Puisque k est divisible par $p-1$, on a

$$\sigma_{k-1}(n) \equiv \sigma_{p-2}(n) \qquad (\text{mod.} p) .$$

Or, on vérifie facilement la congruence

$$\sigma_{p-2}(n) - \sigma_{p-2}(n/p) \equiv n^{p-2}\, \sigma_1(n) \qquad (\text{mod.} p) ,$$

où le terme $\sigma_{p-2}(n/p)$ doit être remplacé par 0 si p ne divise pas n . Cette congruence équivaut à

$$\varphi - \varphi^p \equiv \theta^{p-2}\Big(\sum_{n=1}^{\infty} \sigma_1(n)\, q^n\Big) \qquad (\text{mod.} p) ,$$

d'où finalement

$$(**) \qquad \varphi - \varphi^p = \psi , \quad \text{où} \quad \psi = -\frac{1}{24}\,\theta^{p-2}(\widetilde{P}) = -\frac{1}{24}\,\theta^{p-2}(\widetilde{E}_{p+1}) .$$

Supposons maintenant que φ soit modulaire de poids divisible par $p-1$, et notons h sa <u>filtration</u>, au sens du n° 1.4 ; cela signifie que φ est de la forme $\Phi(\widetilde{Q},\widetilde{R})$, où Φ est un polynôme isobare de poids h , non divisible par A . On a alors $\varphi^p = \Phi^p(\widetilde{Q},\widetilde{R})$, et, puisque A est sans facteurs multiples, A ne divise pas Φ^p . La filtration de φ^p est donc ph , et, puisque $ph > h$, la filtration de $\varphi - \varphi^p$ est aussi ph . D'autre part, $\widetilde{E}_{p+1} = B(\widetilde{Q},\widetilde{R})$ est de filtration $p+1$, puisque B n'est pas divisible par A

(ou bien parce que $M_2 = 0 \ldots$), et le cor. 3 au th. 5 montre que la filtration de $\theta^{p-2}(\tilde{E}_{p+1})$ est $p+1+(p-2)(p+1) = p^2-1$. On devrait donc avoir $ph = p^2-1$, ce qui est absurde, et achève la démonstration.

(En termes "géométriques", l'équation (**) définit un revêtement cyclique de degré p de la droite projective, et le raisonnement ci-dessus revient à montrer que ce revêtement est irréductible à cause de sa ramification aux points d'invariant de Hasse nul.)

2.3. Démonstration du théorème 7

Le th. 7 résulte de :

THÉORÈME 9.- Soient

$$f = a_o + a_1 q + \ldots + a_n q^n + \ldots$$

$$f' = a'_o + a'_1 q + \ldots + a'_n q^n + \ldots$$

deux formes modulaires de poids k et k' respectivement. On suppose que $k' \equiv k \not\equiv 0 \pmod{(p-1)}$, que les a_n et a'_n sont p-entiers pour tout $n \geq 0$, et que $a_n \equiv a'_n \pmod{p}$ pour tout $n \geq 1$.

On a alors $a_o \equiv a'_o \pmod{p}$.

Supposons d'abord que $k' = k$. Soit $g = (f - f')/p$. Par hypothèse, les coefficients de g d'indice ≥ 1 sont p-entiers. D'après le th. 8, (i), il en est de même du terme constant de g, ce qui prouve bien que $a'_o \equiv a_o \pmod{p}$.

Passons au cas général. On peut supposer que $k' = k + s(p-1)$, avec $s \geq 0$. Soit $f'' = f.E^s_{p-1}$; comme $E_{p-1} \equiv 1 \pmod{p}$, on a $f'' \equiv f \pmod{p}$; de plus, f' et f'' ont même poids. On est donc ramené au cas traité au début.

§ 3. Représentations ℓ-adiques attachées aux formes modulaires

Notations

La lettre ℓ désigne un nombre premier, qui joue le rôle du " p " des §§ 1, 2 ; la lettre p est réservée aux nombres premiers $\neq \ell$.

On choisit une clôture algébrique $\bar{\mathbb{Q}}$ de $\mathbb{Q}$, et on note G le groupe de Galois de $\bar{\mathbb{Q}}$ sur $\mathbb{Q}$.

3.1. Résultats

Soit $f = \sum a_n q^n$ une forme modulaire de poids k ; on suppose que

(1) f est parabolique, et normalisée : on a $a_o = 0$, $a_1 = 1$;

(2) f est fonction propre des opérateurs de Hecke T_p (cf. [5], n° 35) : on a $T_p f = a_p f$ pour tout nombre premier p .

Ces propriétés entraînent (Hecke, loc. cit.) que la série de Dirichlet $\Phi_f(s) = \Sigma\, a_n/n^s$ possède le développement eulérien

$$\Phi_f(s) = \prod_p 1/(1 - a_p p^{-s} + p^{k-1-2s}) .$$

Pour simplifier l'exposé, nous ferons en outre l'hypothèse (très restrictive) suivante :

(3) les coefficients a_p sont entiers (auquel cas tous les a_n le sont aussi, vu la formule donnant Φ_f).

On connait 6 exemples de telles formes modulaires, correspondant aux 6 valeurs de k pour lesquelles la dimension de l'espace des formes paraboliques de poids k est 1 : k = 12 , 16 , 18 , 20 , 22 et 26 . Nous noterons

$$\Delta_k = \sum_{n=1}^{\infty} t_k(n)\, q^n$$

la forme parabolique correspondante. On a

$$\Delta_{12} = \Delta\ ,\quad \Delta_{16} = Q\Delta\ ,\quad \Delta_{18} = R\Delta\ ,\quad \Delta_{20} = Q^2\Delta\ ,\quad \Delta_{22} = QR\Delta\ ,\ \text{et}\quad \Delta_{26} = Q^2R\Delta\ .$$

En particulier $t_{12}(n)$ est égal à $\tau(n)$, fonction de Ramanujan.

D'après un théorème de Deligne [3], on peut attacher à f un système de représentations ℓ-adiques (ρ_ℓ) du groupe de Galois G , au sens de [14], chap. I, § 2 :

ρ_ℓ est un homomorphisme continu de G dans $GL_2(\mathbf{Z}_\ell)$ non ramifié en dehors de $\{\ell\}$, et, si $p \neq \ell$ la trace (resp. le déterminant) de l'élément de Frobenius $F_{p,\rho}$ de $GL_2(\mathbf{Z}_\ell)$ défini par ρ_ℓ est égale à a_p (resp. à p^{k-1}).

Il revient au même de dire que la fonction L d'Artin associée à ρ_ℓ est égale à la série Φ_f débarrassée de son ℓ-ième facteur.

Soit $\chi_\ell : G \to \mathbf{Z}_\ell^*$ le <u>caractère fondamental</u> de G, donnant l'action de G sur les racines ℓ^n-ièmes de l'unité ([14], p. I-3). Le couple

$$\sigma_\ell = (\rho_\ell, \chi_\ell)$$

définit un homomorphisme continu de G dans le sous-groupe H_ℓ de $GL_2(\mathbf{Z}_\ell) \times \mathbf{Z}_\ell^*$ formé des couples (s,u) tels que $\det(s) = u^{k-1}$.

LEMME.- <u>L'image de</u> σ_ℓ <u>est un sous-groupe ouvert de</u> H_ℓ.

En effet, cela équivaut à dire que $\mathrm{Im}(\rho_\ell)$ est ouvert dans $GL_2(\mathbf{Z}_\ell)$, résultat démontré dans [15], n° 5.1.

Disons que ℓ est <u>exceptionnel</u> (pour f) si l'image de σ_ℓ est distincte de H_ℓ.

THÉORÈME 10.- <u>L'ensemble des nombres premiers exceptionnels est fini.</u>

La démonstration sera donnée au n° 3.2. On verra qu'elle est "effective", i.e. qu'elle fournit une majoration explicite des ℓ exceptionnels.

La famille des σ_ℓ définit un homomorphisme continu

$$\sigma : G \to H = \prod_\ell H_\ell .$$

Un argument de ramification sans difficulté montre que l'image de σ est le <u>produit</u> des images des σ_ℓ. Vu le lemme et le th. 10, on en déduit :

COROLLAIRE.- <u>Le groupe</u> $\sigma(G)$ <u>est ouvert dans</u> H.

(Noter l'analogie avec le résultat principal de [16].)

En utilisant le théorème de densité de Čebotarev, on obtient :

THÉORÈME 11.- <u>Soient</u> m_1 <u>et</u> m_2 <u>des entiers</u> ≥ 1, <u>et soient</u> $t \in \mathbf{Z}/m_1\mathbf{Z}$ <u>et</u> $d \in (\mathbf{Z}/m_2\mathbf{Z})^*$. <u>Supposons qu'aucun diviseur premier de</u> m_1 <u>ne soit exceptionnel pour</u> f. <u>L'ensemble des nombres premiers</u> p <u>tels que</u>

$$a_p \equiv t \pmod{m_1} \quad \underline{\text{et}} \quad p \equiv d \pmod{m_2}$$

a une densité > 0 ; en particulier, cet ensemble est infini.

Ce résultat s'applique notamment à la fonction de Ramanujan $a_p = \tau(p)$, les nombres premiers exceptionnels étant $2, 3, 5, 7, 23$ et 691, cf. n° 3.3 ; ainsi, si $\ell \neq 2, 3, 5, 7, 23, 691$, la valeur de $\tau(p) \pmod{\ell}$ ne peut pas se déduire d'une congruence sur p.

3.2. Démonstration du théorème 10

Soit ℓ un nombre premier ≥ 5. Supposons que ℓ soit exceptionnel. Notons $\tilde{\rho}_\ell : G \to GL_2(\mathbf{F}_\ell)$ la réduction de ρ_ℓ modulo ℓ, et soit $X_\ell = \mathrm{Im}(\tilde{\rho}_\ell)$. D'après le lemme 3 de [14], p. IV-23, X_ℓ ne contient pas $SL_2(\mathbf{F}_\ell)$. En utilisant la liste des sous-groupes de $GL_2(\mathbf{F}_\ell)$ (cf. [16], § 2), ainsi que quelques arguments élémentaires de ramification, on en déduit que X_ℓ a l'une des propriétés suivantes :

(i) X_ℓ est contenu dans un sous-groupe triangulaire de $GL_2(\mathbf{F}_\ell)$; la représentation ρ_ℓ est extension de deux représentations irréductibles de degré 1, données par des puissances $\tilde{\chi}_\ell^m$ et $\tilde{\chi}_\ell^{m'}$ de la réduction mod. ℓ de χ_ℓ ; on a

$$m + m' \equiv k - 1 \pmod{(\ell - 1)} \quad \text{et} \quad a_p \equiv p^m + p^{m'} \pmod{\ell} \quad \text{si } p \neq \ell .$$

(ii) X_ℓ est contenu dans le normalisateur d'un sous-groupe de Cartan C de $GL_2(\mathbf{F}_\ell)$, et n'est pas contenu dans C ; on a

$$a_p \equiv 0 \pmod{\ell} \quad \text{si} \quad \left(\frac{p}{\ell}\right) = -1 .$$

(iii) L'image de X_ℓ dans $PGL_2(\mathbf{F}_\ell) = GL_2(\mathbf{F}_\ell)/\mathbf{F}_\ell^*$ est isomorphe au groupe symétrique $\mathfrak{S}_4$; on a

$$a_p^2/p^{k-1} \equiv 0, 1, 2 \text{ ou } 4 \pmod{\ell} \quad \text{pour tout } p \neq \ell .$$

(Si ce cas se produit, on peut montrer que $\ell \equiv \pm 5 \pmod{8}$, et que le nombre de classes du corps quadratique de discriminant $\pm \ell$ est divisible par 3.)

Nous allons, dans chaque cas, obtenir une majoration de ℓ ; cela démontrera le th. 10.

Majoration dans le cas (i)

C'est le cas crucial, traité par Swinnerton-Dyer [18]. On va voir que, dans ce cas, on a $\ell \leq k + 1$, ou bien ℓ divise le numérateur de $b_k/2k$.

En effet, supposons que (i) se produise et que $\ell > k+1$. On a $a_p \equiv p^m + p^{m'}$ (mod. ℓ) si $p \neq \ell$, et m et m' ne sont définis que modulo $(\ell - 1)$; on peut donc supposer que

$$0 \leq m < m' < \ell - 1 \qquad \text{et} \qquad m + m' \equiv k - 1 \quad (\text{mod.}(\ell - 1)).$$

La congruence $a_p \equiv p^m + p^{m'}$ (mod. ℓ) entraîne :

$$a_n \equiv n^m \sigma_{m'-m}(n) \quad (\text{mod. } \ell) \quad \text{pour tout } n \text{ premier à } \ell, \quad \text{ou encore :}$$

$$\theta_f \equiv \theta^{m+1} G_{m'-m+1} \quad (\text{mod. } \ell),$$

où θ est l'opérateur de dérivation du n°1.4. Comme $\ell > k+1$, la filtration de θf(mod. ℓ) est $k + \ell + 1$, cf. th. 5, cor. 3. D'autre part, celle de $\widetilde{G}_{m'-m+1}$ est $m'-m + 1$ si $m' - m > 1$, et $\ell + 1$ si $m' - m = 1$; il en résulte que celle de $\theta^{m+1}\widetilde{G}_{m'-m+1}$ est $m' - m + 1 + (\ell + 1)(m + 1)$, augmenté de $\ell - 1$ si $m' - m = 1$. On doit donc avoir

$$k + \ell + 1 = \begin{cases} m' - m + 1 + (\ell + 1)(m + 1) & \text{si } m' - m > 1 \\ \ell + 1 + (\ell + 1)(m + 1) & \text{si } m' - m = 1 . \end{cases}$$

Comme $k < \ell - 1$, ceci n'est possible que si $m = 0$, auquel cas on a $\theta f \equiv \theta G_k$ (mod. ℓ), i.e. $\theta(f-G_k) = 0$ (mod. ℓ). Comme k n'est pas divisible par ℓ, le cor. 3 au th. 5, appliqué à $f - G_k$, montre que $f - G_k \equiv 0$ (mod. ℓ), et, comme f est parabolique, cela entraîne que le terme constant de G_k est divisible par ℓ, i.e. que ℓ divise le numérateur de $b_k/2k$.

Majoration dans le cas (ii)

S'il se produit, on a $\ell < 2k$. En effet, la relation

$$a_p \equiv 0 \quad (\text{mod. } \ell) \qquad \text{pour tout } p \text{ tel que } \left(\tfrac{p}{\ell}\right) = -1 ,$$

entraîne la suivante :

$$\theta f \equiv \theta^{(\ell+1)/2} f \quad (\text{mod. } \ell).$$

Si l'on suppose $\ell \geq 2k$, le cor. 3 au th. 5 permet de calculer les filtrations des deux membres; on trouve pour θf la filtration $k + \ell + 1$, et pour $\theta^{(\ell+1)/2} f$ la filtration $k + (\ell+1)^2/2$; il y a contradiction.

Majoration dans le cas (iii)

On commence par remarquer que l'image de G par

$$G \to GL_2(\mathbf{Z}_\ell) \to PGL_2(\mathbf{Z}_\ell)$$

est ouverte, donc n'est pas isomorphe à $\mathfrak{S}_4$. Il en résulte qu'il existe p tel que a_p^2/p^{k-1} soit distinct de $0, 1, 2$ et 4. On en conclut que, si le cas (iii) se produit pour un nombre premier ℓ, ℓ divise nécessairement l'un des entiers non nuls

$$a_p \;,\; a_p^2 - p^{k-1} \;,\; a_p^2 - 2p^{k-1} \;,\; a_p^2 - 4p^{k-1} \;,$$

ou est égal à p ; cela fournit une majoration de ℓ.

(On devrait pouvoir montrer que (iii) entraîne $\ell < 4k$; la question est liée à celle de l'action de "l'inertie modérée" dans $\tilde{\rho}_\ell$, cf. [16], n° 1.13.)

3.3. Exemple : $f = \Delta$

Le cas (i) est impossible pour $\ell > 13$, mis à part 691 qui est le numérateur de b_{12} ; on constate que (i) se produit pour $\ell = 2, 3, 5, 7$ (cf. n° 1.4), mais pas pour $\ell = 11, 13$.

Le cas (ii) se produit pour $\ell = 2k - 1 = 23$, cf. [15], n° 3.4, le groupe X_ℓ correspondant étant isomorphe à $\mathfrak{S}_3$. Vu ce qui précède, ce cas ne se produit pas pour $\ell > 23$; on vérifie par calcul direct qu'il ne se produit pas non plus pour $\ell = 11, 13, 17$ et 19.

Enfin, si (iii) se produisait, on aurait $\tau(2) \equiv 0, \pm 2^6 \pmod{\ell}$, et comme $\tau(2) = -24$, ce n'est possible que si $\ell = 2, 3, 5, 11$, et on constate que ce n'est pas le cas.

Finalement, les nombres premiers exceptionnels pour Δ sont $2, 3, 5, 7, 23$ et 691.

3.4. Exemple : $f = \Delta_{16} = Q\Delta$

On trouve que le cas (i) se produit seulement pour $\ell \leq 11$ et pour $\ell = 3617$, numérateur de b_{16}. Le cas (ii) se produit pour $\ell = 2k-1 = 31$, le groupe X_ℓ correspondant étant isomorphe à $\mathfrak{S}_3$. Le cas (iii) ne se produit pas si $\ell \neq 59$; par contre, il paraît très probable qu'il se produit effectivement pour $\ell = 59$; on aurait

$$p^7 t_{16}(p) \equiv 0, \pm 1, \pm 2 \text{ ou } \pm 36 \pmod{59}$$

pour tout p , mais ce n'est pas encore démontré.

Les nombres premiers exceptionnels pour Δ_{16} sont donc 2 , 3 , 5 , 7 , 11 , 31 , 3617 et sans doute 59 .

3.5. Autres exemples

Pour Δ_{18} , Δ_{20} , Δ_{22} et Δ_{26} , on trouve que les nombres premiers exceptionnels sont tous de type (i). Ce sont :

pour Δ_{18} : 2 , 3 , 5 , 7 , 11 , 13 , 43867 ;

pour Δ_{20} : 2 , 3 , 5 , 7 , 11 , 13 , 283 , 617 ;

pour Δ_{22} : 2 , 3 , 5 , 7 , 13 , 17 , 131 , 593 ;

pour Δ_{26} : 2 , 3 , 5 , 7 , 11 , 17 , 19 , 657931 .

BIBLIOGRAPHIE

[1] A. O. L. ATKIN - Congruences for modular forms, Computers in mathematical research (ed. by R. F. Churchhouse and J-C. Herz), p. 8-19, North-Holland, Amsterdam, 1968.

[2] Z. I. BOREVIČ et I. R. ŠAFAREVIČ - Théorie des nombres (traduit du russe par M. et J-L. Verley), Gauthier-Villars, Paris, 1967.

[3] P. DELIGNE - Formes modulaires et représentations ℓ-adiques, Séminaire Bourbaki, exposé 355 (février 1969), Lecture Notes n° 179, Springer-Verlag, 1971.

[4] M. DEURING - Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hamburg, 14, 1941, p. 197-272.

[5] E. HECKE - Mathematische Werke, Vandenhoeck und Ruprecht, Göttingen, 1959.

[6] J. IGUSA - Class number of a definite quaternion with prime discriminant, Proc. Nat. Acad. Sci. USA, 44, 1958, p. 312-314.

[7] J. IGUSA - On the algebraic theory of elliptic modular functions, J. Math. Soc. Japan, 20, 1968, p. 96-106.

[8] H. KLINGEN - Über die Werte der Dedekindschen Zetafunktionen, Math. Ann., 145, 1962, p. 265-272.

[9] O. KOLBERG - Note on Ramanujan's function $\tau(n)$, Math. Scand. 10, 1962, p. 171-172.

[10] O. KOLBERG - Congruences for the coefficients of the modular invariant $j(\tau)$, Math. Scand. 10, 1962, p. 173-181.

[11] J. LEHNER - Lectures on modular forms, Nat. Bureau of Standards, Appl. Math. Ser. 61, Washington, 1969.

[12] S. RAMANUJAN - On certain arithmetical functions, Trans. Cambridge phil. Soc., 22, 1916, p. 159-184 (Collected Papers, n° 18, p. 136-162).

[13] P. ROQUETTE - Analytic theory of elliptic functions over local fields, Vandenhoeck und Ruprecht, Göttingen, 1970.

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

[15] J.-P. SERRE - Une interprétation des congruences relatives à la fonction τ de Ramanujan, Séminaire Delange-Pisot-Poitou, 1967/1968, exposé 14.

[16] J.-P. SERRE - Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. math., 15, 1972, p. 259-331.

[17] C. L. SIEGEL - Berechnung von Zetafunktionen an ganzzahligen Stellen, Gött. Nach. 1969, n° 10, p. 87-102.

[18] H. P. F. SWINNERTON-DYER - Some implications of Ramanujan's methods of proving congruences for $\tau(n)$ (1971, non publié).