COMPTES RENDUS
DE L'ACADÉMIE DES SCIENCES

Tome 350
fascicule 7–8

avril 2012
ISSN 1631-073X

MATHEMATIQUE

69301

ACADÉMIE DES SCIENCES – PARIS

ELSEVIER

C. R. Acad. Sci. Paris, Ser. I 350 (2012) 343–348

Contents lists available at SciVerse ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Théorie des nombres

Formes modulaires modulo 2 : L'ordre de nilpotence des opérateurs de Hecke

The nilpotence order of the mod 2 *Hecke operators*

Jean-Louis Nicolas [a], Jean-Pierre Serre [b]

[a] *CNRS, Université de Lyon, Institut Camille Jordan, Mathématiques, 69622 Villeurbanne cedex, France*
[b] *Collège de France, 3, rue d'Ulm, 75231 Paris cedex 05, France*

INFO ARTICLE

Historique de l'article :
Reçu et accepté 15 mars 2012
Disponible sur Internet le 5 avril 2012

Présenté par Jean-Pierre Serre

RÉSUMÉ

Soit $\Delta = \sum_{m=0}^{\infty} q^{(2m+1)^2} \in \mathbf{F}_2[[q]]$. Une forme modulaire f mod 2 de niveau 1 est un polynôme en Δ. Si p est un nombre premier > 2, l'opérateur de Hecke T_p transforme f en une forme modulaire $T_p(f)$ qui est un polynôme en Δ de degré strictement plus petit que celui de f, de sorte que T_p est nilpotent.
L'ordre de nilpotence de f est défini comme le plus petit entier $g = g(f)$ tel que, pour toute famille de g nombres premiers impairs $p_1, p_2, \ldots, p_g$, on ait $T_{p_1} T_{p_2} \ldots T_{p_g}(f) = 0$. Nous montrons dans ce qui suit comment on peut calculer $g(f)$; on a $g(f) \ll \deg(f)^{1/2}$.

ABSTRACT

Let $\Delta = \sum_{m=0}^{\infty} q^{(2m+1)^2} \in \mathbf{F}_2[[q]]$ be the reduction mod 2 of the Δ series. A modular form f modulo 2 of level 1 is a polynomial in Δ. If p is an odd prime, then the Hecke operator T_p transforms f in a modular form $T_p(f)$ which is a polynomial in Δ whose degree is smaller than the degree of f, so that T_p is nilpotent.
The order of nilpotence of f is defined as the smallest integer $g = g(f)$ such that, for every family of g odd primes $p_1, p_2, \ldots, p_g$, the relation $T_{p_1} T_{p_2} \ldots T_{p_g}(f) = 0$ holds. We show how one can compute explicitly $g(f)$; if f is a polynomial of degree d in Δ, one finds that $g(f) \ll d^{1/2}$.

1. Introduction

Soit $\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$ où τ est la fonction de Ramanujan. Soit k un entier $\geqslant 0$. On écrit $\Delta^k(q) = \sum_{n=k}^{\infty}\tau_k(n)q^n$. Les congruences connues sur $\tau(n) \pmod 2$ (cf. [5]), montrent que $\Delta(q) \equiv \sum_{m=0}^{\infty} q^{(2m+1)^2} \pmod 2$, ce qui entraîne

$$n \not\equiv k \pmod 8 \quad \Longrightarrow \quad \tau_k(n) \equiv 0 \pmod 2. \tag{1}$$

Une forme modulaire modulo 2 de niveau 1 est un polynôme $f(\Delta)$ à coefficients dans $\mathbf{F}_2$ (cf. par exemple [2,4]) ; nous l'identifierons à une série formelle en la variable q, à coefficients dans $\mathbf{F}_2$. Nous ne nous intéresserons qu'aux formes

Adresses e-mail : jlnicola@in2p3.fr (J.-L. Nicolas), jpserre691@gmail.com (J.-P. Serre).
URL : http://math.univ-lyon1.fr/~nicolas/ (J.-L. Nicolas).

1631-073X/$ – see front matter
http://dx.doi.org/10.1016/j.crma.2012.03.013

paraboliques (celles dont le terme constant est 0). À partir de maintenant (sauf mention expresse du contraire), toutes les séries considérées sont à coefficients mod 2, et nous nous permettrons d'écrire

$$\Delta = \Delta(q) = \sum_{m=0}^{\infty} q^{(2m+1)^2} \in \mathbf{F}_2[[q]]. \tag{2}$$

2. Préliminaires

2.1. Les $\mathbf{F}_2$-espaces vectoriels $\mathcal{F}, \mathcal{F}_1, \mathcal{F}_3, \mathcal{F}_5, \mathcal{F}_7$

Soit $\mathcal{F}$ le sous-espace de $\mathbf{F}_2[\Delta]$ engendré par $\Delta, \Delta^3, \Delta^5, \ldots$. Compte tenu de (1), on a $\mathcal{F} = \mathcal{F}_1 \oplus \mathcal{F}_3 \oplus \mathcal{F}_5 \oplus \mathcal{F}_7$ où, pour $i \in \{1, 3, 5, 7\}$, $\mathcal{F}_i$ a pour base $\{\Delta^i, \Delta^{i+8}, \Delta^{i+16}, \ldots\}$.

Puisque $\Delta^{2k}(q) = \Delta^k(q^2)$, toute forme parabolique f modulo 2 peut s'écrire comme une somme finie

$$f = \sum_{s \geqslant 0} f_s^{2^s} \quad \text{avec } f_s \in \mathcal{F}. \tag{3}$$

2.2. Opérateurs de Hecke

Soit $f(q) = \sum_{n \geqslant 0} c_n q^n$ une forme modulaire modulo 2 et soit p un nombre premier > 2. L'opérateur de Hecke T_p transforme f en la forme

$$T_p | f = \sum_{n \geqslant 0} \gamma_n q^n \quad \text{avec } \gamma(n) = \begin{cases} c(pn) & \text{si } p \text{ ne divise pas } n, \\ c(pn) + c(n/p) & \text{si } p \text{ divise } n. \end{cases} \tag{4}$$

[Nous écrirons parfois $T_p(f)$ à la place de $T_p|f$.]

Si f est de degré $\leqslant k$ (comme polynôme en Δ), alors il en est de même de $T_p|f$; on peut écrire $T_p|\Delta^k$ sous la forme

$$T_p | \Delta^k = \sum_{j=0}^{k} \mu_j \Delta^j, \quad \text{avec } \mu_j \in \mathbf{F}_2. \tag{5}$$

Supposons maintenant k impair. Les formules (1) et (4) entraînent que

$$j \not\equiv pk \pmod 8 \implies \mu_j = 0. \tag{6}$$

En particulier, on a $T_p(\mathcal{F}_i) \subset \mathcal{F}_j$ si $j \equiv pi \pmod 8$.

L'opérateur de Hecke T_p commute avec les opérations $f \mapsto f^{2^s}$ de sorte que, si l'on connaît l'action de T_p sur $\mathcal{F}$, par (3), on la connaît sur toutes les formes paraboliques.

2.3. Nilpotence des opérateurs de Hecke modulo 2

L'une des propriétés essentielles des opérateurs de Hecke modulo 2 est qu'ils sont nilpotents (cf. par exemple [1,3,4]). Cela implique que, dans (5), le coefficient μ_k est nul. Par (5) et (6), on a donc pour tout p premier $\geqslant 3$, et tout k impair positif,

$$T_p | \Delta^k = \sum_{\substack{j \equiv pk \pmod 8 \\ 1 \leqslant j \leqslant k-2}} \mu_j \Delta^j, \quad \text{avec } \mu_j \in \mathbf{F}_2. \tag{7}$$

Exemples :

(i) $T_p|\Delta = 0$ pour tout p premier > 2.
(ii) Si $p \equiv 3 \pmod 8$, on a $T_p|\Delta^3 = \Delta$; sinon, $T_p|\Delta^3 = 0$.
(iii) Si $p \equiv 5 \pmod 8$, on a $T_p|\Delta^5 = \Delta$; sinon, $T_p|\Delta^5 = 0$.
(iv) On a :

$$T_p | \Delta^7 = \begin{cases} 0 & \text{si } p \equiv 1 \pmod 8 \text{ ou si } p \equiv -1 \pmod{16}, \\ \Delta^5 & \text{si } p \equiv 3 \pmod 8, \\ \Delta^3 & \text{si } p \equiv 5 \pmod 8, \\ \Delta & \text{si } p \equiv 7 \pmod{16}. \end{cases}$$

2.4. L'ordre de nilpotence

Par définition, *l'ordre de nilpotence* d'une forme modulaire $f \in \mathbf{F}_2[\Delta]$ est le plus petit entier $g = g(f)$ tel que, pour toute suite de g nombres premiers impairs $p_1, p_2, \ldots, p_g$, on ait $T_{p_1} T_{p_2} \ldots T_{p_g} | f = 0$. [Comme les T_p commutent entre eux, l'ordre dans lequel on écrit les T_{p_i} n'a pas d'importance. Noter aussi que l'on ne suppose pas que les p_i soient distincts.] Lorsque $f = 0$, on convient que $g(f) = -\infty$.

Nous désignerons par $g(k) = g(\Delta^k)$ l'ordre de nilpotence de Δ^k. Comme chaque T_p abaisse le degré en Δ d'au moins 2 unités, on a $g(k) \leqslant \frac{k+1}{2}$.

Soit p un nombre premier impair ; il résulte de la définition de l'ordre de nilpotence d'une forme modulaire $f \in \mathcal{F}$ que l'on a

$$g(f) \geqslant g(T_p | f) + 1. \tag{8}$$

Exemples :

$$g(0) = -\infty, \qquad g(\Delta) = 1, \qquad g(\Delta^3) = g(\Delta^3 + \Delta) = 2, \tag{9}$$

$$g(\Delta^5) = g(\Delta^5 + \Delta) = g(\Delta^5 + \Delta^3) = g(\Delta^5 + \Delta^3 + \Delta) = 2. \tag{10}$$

3. Calcul des $T_p | \Delta^k$: une récurrence linéaire

Soit p un nombre premier > 2.

Théorème 3.1. *Il existe un unique polynôme symétrique $F_p(X, Y) \in \mathbf{F}_2[X, Y]$,*

$$F_p(X, Y) = Y^{p+1} + s_1(X) Y^p + \cdots + s_p(X) Y + s_{p+1}(X) \tag{11}$$

de degré $p + 1$ tel que

$$T_p(\Delta^k) = \sum_{r=1}^{p+1} s_r(\Delta) T_p(\Delta^{k-r}) \tag{12}$$

pour tout $k \geqslant p + 1$. De plus, pour $1 \leqslant r \leqslant p + 1$, $s_r(X)$ est une somme de monômes en X dont les degrés sont congrus à pr modulo 8 et sont $\leqslant r$.

Esquisse de démonstration. On définit les $s_r(\Delta)$, $1 \leqslant i \leqslant p + 1$, comme les fonctions symétriques élémentaires des $p + 1$ séries

$$f_0 = \Delta(q^p), \qquad f_i = \Delta(z^i q^{1/p}), \quad i = 1, \ldots, p,$$

où z est une racine primitive p-ième de l'unité dans une extension finie de $\mathbf{F}_2$. On déduit (12) de la formule : $T_p | \Delta^k = \sum_{i=0}^{p} (f_i)^k$, $k = 0, 1, \ldots$. $\square$

Exemples[1] : Pour $p = 3$ on a

$$F_3(X, Y) = (X + Y)^4 + XY = X^4 + XY + Y^4. \tag{13}$$

Vu (9), cela donne un procédé de calcul des $T_3 | \Delta^k$; si t est une indéterminée, on a :

$$\sum_{k=1}^{\infty} T_3(\Delta^k) t^k = \frac{\Delta t^3}{1 + \Delta^3 t + \Delta^4 t^4}.$$

De même, pour $p = 5$, on a :

$$F_5(X, Y) = (X + Y)^6 + XY = X^6 + X^4 Y^2 + X^2 Y^4 + XY + Y^6 \tag{14}$$

et

$$\sum_{k=1}^{\infty} T_5(\Delta^k) t^k = \frac{\Delta t^5}{1 + \Delta^2 t^2 + \Delta^4 t^4 + \Delta^5 t^5 + \Delta^6 t^6}.$$

---

[1] Une table des polynômes F_p pour $p \leqslant 257$, calculée avec SAGE par Marc Deléglise, se trouve sur le site http://math.univ-lyon1.fr/~nicolas/polHecke.html.

4. Les opérateurs de Hecke T_3 et T_5

4.1. Les nombres $n_3(k), n_5(k)$ et $h(k)$

Soit k un nombre entier $\geqslant 0$. Ecrivons-le sous forme dyadique : $k = \sum_{i=0}^{\infty} \beta_i 2^i$ avec $\beta_i = 0$ ou 1. Posons :

$$n_3(k) = \sum_{i=0}^{\infty} \beta_{2i+1} 2^i = \sum_{\substack{i=1 \\ i \text{ impair}}}^{\infty} \beta_i 2^{\frac{i-1}{2}}, \qquad n_5(k) = \sum_{i=0}^{\infty} \beta_{2i+2} 2^i = \sum_{\substack{i=1 \\ i \text{ pair}}}^{\infty} \beta_i 2^{\frac{i-2}{2}}, \qquad h(k) = n_3(k) + n_5(k).$$

L'entier $h(k)$ est du même ordre de grandeur que $k^{1/2}$: si k est impair > 0 on a

$$\frac{1}{2} k^{1/2} < h(k) + 1 < \frac{3}{2} k^{1/2}.$$

Notons que l'on a pour $\ell \geqslant 0$

$$n_3(2\ell + 1) = n_3(2\ell), \qquad n_5(2\ell + 1) = n_5(2\ell), \qquad h(2\ell + 1) = h(2\ell).$$

Nous appellerons $[n_3(k), n_5(k)]$ le *code* du nombre k. L'application $k \mapsto [n_3(k), n_5(k)]$ est une bijection de l'ensemble des nombres impairs (resp. pairs) $\geqslant 0$ sur $\mathbf{N}^2$.

4.2. Relation de domination

Nous utiliserons la relation d'ordre suivante sur l'ensemble des nombres entiers naturels pairs (ou impairs) :

Définition 4.1. Si k et ℓ ont même parité, on dit que ℓ domine k et on écrit $k \prec \ell$ ou $\ell \succ k$ si l'on a $h(k) < h(\ell)$ ou bien $h(k) = h(\ell)$ et $n_5(k) < n_5(\ell)$. La relation $k \preccurlyeq \ell$ définie par $k \prec \ell$ ou $k = \ell$, est une relation d'ordre total sur l'ensemble des entiers pairs (resp. impairs) $\geqslant 0$.

À partir de maintenant, nous écrirons une forme modulaire $f \in \mathcal{F}$, $f \neq 0$ sous la forme

$$f = \Delta^{m_1} + \Delta^{m_2} + \cdots + \Delta^{m_r} \quad \text{avec } m_1 \succ m_2 \succ \cdots \succ m_r. \tag{15}$$

4.3. La fonction h pour les formes modulaires mod 2

Définition 4.2. Soit $f \in \mathcal{F}$.
Si $f \neq 0$, on écrit f sous la forme (15). On dit que m_1 est l'exposant dominant de f et l'on définit $h(f)$ par

$$h(f) = h(m_1) = \max_{1 \leqslant i \leqslant r} h(m_i).$$

Si $f = 0$, on pose $h(f) = -\infty$.

4.4. Le cas de $T_3|f$

Proposition 4.3. *Soit $f \in \mathcal{F}$, $f \neq 0$ et soit m_1 son exposant dominant.*

(i) *On a $h(T_3|f) \leqslant h(f) - 1 = h(m_1) - 1$.*
(ii) *Lorsque $n_3(m_1) \geqslant 1$, on a $h(T_3|f) = h(m_1) - 1$ et l'exposant dominant de $T_3|f$ a pour code $[n_3(m_1) - 1, n_5(m_1)]$.*

Démonstration. On considère d'abord le cas où $f = \Delta^k$. On raisonne alors par récurrence sur k en utilisant les relations (11), (12) et (13). La démonstration est assez longue et technique. $\square$

4.5. Le cas de $T_5|f$

Proposition 4.4. *Soit $f \in \mathcal{F}$, $f \neq 0$ et soit m_1 son exposant dominant.*

(i) *On a $h(T_5|f) \leqslant h(f) - 1 = h(m_1) - 1$.*
(ii) *Lorsque $n_5(m_1) \geqslant 1$, on a $h(T_5|f) = h(m_1) - 1$ et l'exposant dominant de $T_5|f$ a pour code $[n_3(m_1), n_5(m_1) - 1]$.*

Démonstration. Même méthode que pour la proposition 4.3 ; on utilise (14) au lieu de (13). $\square$

5. Détermination de l'ordre de nilpotence

Théorème 5.1. *Soit $f \in \mathcal{F}$, $f \neq 0$, que l'on écrit comme en* (15).

(i) *On a*

$$T_3^{n_3(m_1)} T_5^{n_5(m_1)} | f = \Delta. \tag{16}$$

(ii) *La valeur de l'ordre de nilpotence $g(f)$ (cf.* §2.4) *est donnée par*

$$g(f) = h(f) + 1. \tag{17}$$

Démonstration. (i) Soit m l'exposant dominant de $\varphi = T_3^{n_3(m_1)} T_5^{n_5(m_1)} | f$. En appliquant $n_3(m_1)$ fois la proposition 4.3(ii) et $n_5(m_1)$ fois la proposition 4.4(ii), on voit que m a pour code $[0, 0]$; comme m est impair, on a $m = 1$, d'où $\varphi = \Delta$, ce qui démontre (16). Notons que (16) implique

$$g(f) \geqslant n_3(m_1) + n_5(m_1) + 1 = h(m_1) + 1 = h(f) + 1. \tag{18}$$

(ii) Soit $d = \max(m_1, m_2, \dots, m_r)$ le degré de f ; on va démontrer (17) par récurrence sur le nombre impair d.

Si $d = 1, 3$ ou 5, (17) résulte de (9) et (10).

Soit $d \geqslant 7$ et supposons (17) vraie pour toute forme de degré $\leqslant d - 2$. Pour $d \geqslant 7$, on a $h(d) \geqslant 2$ et la définition de l'exposant dominant entraîne $h(f) = h(m_1) \geqslant h(d) \geqslant 2$. Par (18), on a $g(f) \geqslant h(f) + 1 \geqslant 3$; donc il existe des nombres premiers impairs $p_1, p_2, \dots, p_s$ avec $s = g(f) - 1 \geqslant 2$ et

$$T_{p_1} T_{p_2} \dots T_{p_s} | f \neq 0. \tag{19}$$

Posons $\varphi = T_{p_s} | f$, et calculons $g(\varphi)$. De (19), on déduit

$$T_{p_1} T_{p_2} \dots T_{p_{s-1}} | \varphi = T_{p_1} T_{p_2} \dots T_{p_s} | f \neq 0,$$

ce qui implique $g(\varphi) \geqslant s$. Mais (8) entraîne $g(\varphi) = g(T_p | f) \leqslant g(f) - 1 = s$. On en déduit

$$g(\varphi) = s = g(f) - 1 \geqslant 2. \tag{20}$$

Observons que (19) et $s \geqslant 2$ entraînent $\varphi \neq 0$. Par (7), le degré de φ est $\leqslant d - 2$; on peut donc appliquer à φ l'hypothèse de récurrence, ce qui donne $g(\varphi) = h(\varphi) + 1$. En désignant par j l'exposant dominant de φ, avec (20), il vient

$$g(\varphi) = h(\varphi) + 1 = h(j) + 1 = s \geqslant 2. \tag{21}$$

Soit $[u, v]$ le code de j, avec $u \geqslant 0$, $v \geqslant 0$ et $u + v = s - 1$. En appliquant (i) à φ et en posant $q_1 = q_2 = \dots = q_u = 3$ et $q_{u+1} = q_{u+2} = \dots = q_{u+v} = 5$, il vient

$$T_{q_1} T_{q_2} \dots T_{q_{s-1}} | \varphi = T_{q_1} T_{q_2} \dots T_{q_{s-1}} T_{p_s} | f = \Delta.$$

Posons $\psi = T_{q_{s-1}} | f$; on a

$$T_{q_1} T_{q_2} \dots T_{q_{s-2}} T_{p_s} | \psi = T_{q_1} T_{q_2} \dots T_{q_{s-1}} T_{p_s} | f = \Delta.$$

Cette formule montre que $g(\psi) \geqslant s$. Mais (8) entraîne $g(\psi) = g(T_{q_{s-1}} | f) \leqslant g(f) - 1 = s$ et $g(\psi) = s$.

Par (7), le degré de ψ est $\leqslant d - 2$ et l'hypothèse de récurrence donne $g(\psi) = h(\psi) + 1$. On a ainsi

$$g(\psi) = s = g(f) - 1 = h(\psi) + 1. \tag{22}$$

Par la proposition 4.3(i) lorsque $q_{s-1} = 3$, et par la proposition 4.4(i) lorsque $q_{s-1} = 5$, on a $h(T_{q_{s-1}} | f) \leqslant h(f) - 1$, d'où, par (22),

$$s - 1 = g(f) - 2 = h(\psi) = h(T_{q_{s-1}} | f) \leqslant h(f) - 1$$

ce qui implique $g(f) \leqslant h(f) + 1$; vu (18), cela entraîne (17). $\square$

Corollaire 5.2. *Soit $f \in \mathcal{F}$, $f \neq 0$, et soit p un nombre premier tel que $p \equiv \pm 1 \pmod 8$. Alors, on a*

$$g(T_p | f) \leqslant g(f) - 2. \tag{23}$$

Démonstration. On observe que, pour $p \equiv \pm 1 \pmod 8$, on a $h(T_p | f) \equiv h(f) \pmod 2$, ce qui, par le théorème 5.1, entraîne $g(T_p | f) \equiv g(f) \pmod 2$. $\square$

Corollaire 5.3. *Soit $f \in \mathcal{F}$, $f \neq 0$. Si $T_3 | f = T_5 | f = 0$, alors $f = \Delta$.*

Démonstration. En effet, d'après (i), on a $n_3(m_1) = n_5(m_1) = 0$, d'où $m_1 = 1$ et $f = \Delta$. $\square$

Références

[1] K. Hatada, Eigenvalues of Hecke operators on $SL(2, \mathbf{Z})$, Math. Ann. 239 (1979) 75–96.

[2] J.-L. Nicolas, Parité des valeurs de la fonction de partition $p(n)$ et anatomie des entiers, in : CRM Proceedings and Lecture Notes, vol. 46, Centre de Recherches Mathématiques, 2008, pp. 97–113.

[3] K. Ono, The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-Series, CBMS, vol. 102, Amer. Math. Soc., 2004.

[4] J.-P. Serre, Valeurs propres des opérateurs de Hecke modulo ℓ, Astérisque 24–25 (1975) 109–117.

[5] H.P.F. Swinnerton-Dyer, On ℓ-Adic Representations and Congruences for Coefficients of Modular Forms, Lect. Notes, vol. 350, Springer, 1973, pp. 1–55.