Parité des coefficients de formes modulaires

Joël BELLAÏCHE [*] Jean-Louis NICOLAS [†]

July 2, 2014

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 of level 1, $f = \sum_{n\geqslant 0} c(n)\, q^n$, with integer coefficients, is congruent modulo 2 to a polynomial in Δ.

Let us set $W_f(x) = \sum_{n\leqslant x,\ c(n) \text{ odd}} 1$, the number of odd Fourier coefficients of f of index $\leqslant x$. The order of magnitude of $W_f(x)$ (for $x \to \infty$) has been determined by J.-P. Serre in the seventies. Here, we give an asymptotic equivalent for $W_f(x)$.

Let $p(n)$ be the partition function and $A_0(x)$ (resp. $A_1(x)$) be the number of $n \leqslant x$ such that $p(n)$ is even (resp. odd). In preceding papers, the second-named author has shown that $A_0(x) \geqslant 0.28\sqrt{x\ \log\log x}$ for $x \geqslant 3$ and $A_1(x) > \frac{4.57\sqrt{x}}{\log x}$ for $x \geqslant 7$. Here, it is proved that $A_0(x) \geqslant 0.069\sqrt{x}\ \log\log x$ holds for $x > 1$ and that $A_1(x) \geqslant \frac{0.037\sqrt{x}}{(\log x)^{7/8}}$ holds for $x \geqslant 2$.

The main tools used to prove these results is the determination of the order of nilpotence of a modular form of level 1 modulo 2, and of the structure of the space of those modular forms as a module over the Hecke algebra, which have been given in a recent work of J.-P. Serre and the second-named author.

Keywords: modular forms modulo 2, Hecke operators, order of nilpotence, Selberg–Delange's formula, partition function

Mathematics Subject Classification 2000: 11F33, 11F25, 11N37, 11P83.

1 Introduction

Ramanujan a obtenu plusieurs congruences célèbres vérifiées par des fonctions arithmétiques. Par exemple, $p(n)$, la fonction de partition définie par

$$\sum_{n=0}^{\infty} p(n)q^n = \prod_{m=1}^{\infty} \frac{1}{1-q^m} \tag{1.1}$$

vérifie (cf. [19], ou [8, §19.12])

$$p(5n+4) \equiv 0 \pmod 5$$

tandis que la fonction de Ramanujan, $\tau(n)$, définie par

$$\Delta = \Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$$

[*]Recherche partiellement financée par la NSF, grant DMS 1101615.
[†]Recherche partiellement financée par le CNRS, Institut Camille Jordan, UMR 5208.

vérifie

$$\Delta = \Delta(q) = \sum_{n=1}^{\infty} \tau(n) q^n \equiv \sum_{m=0}^{\infty} q^{(2m+1)^2} \pmod 2. \tag{1.2}$$

La formule (1.2), qui montre que le n-ième coefficient de Fourier de Δ est impair si et seulement si n est le carré d'un nombre impair était connue de Ramanujan. Mais on ne l'a su que récemment, lorsque plusieurs de ses manuscrits longtemps inconnus ont été rendus publics (cf. [20, p. 135–169], [1, p. 81–172]).

Peut-on caractériser les coefficients de Fourier impairs de Δ^k ou, plus généralement, d'une forme modulaire de niveau 1 ? Pour cela, il faut étudier ces formes modulo 2. Il est facile de montrer qu'une telle forme est un polynôme en Δ à coefficients dans $\mathbf{F}_2$ (cf. par exemple [13, 23]) ; nous l'identifierons à une série formelle en la variable q, à coefficients dans $\mathbf{F}_2$:

$$f = \sum_{n=0}^{\infty} c(n)\, q^n, \quad c(n) \in \{0, 1\}. \tag{1.3}$$

Ainsi, à partir de (1.2), nous nous permettrons d'écrire

$$\Delta = \Delta(q) = \sum_{m=0}^{\infty} q^{(2m+1)^2} \quad \in \mathbf{F}_2[[q]]. \tag{1.4}$$

Soit f une forme modulaire de niveau 1 modulo 2, dont on définit les coefficients $c(n)$ par (1.3). On pose

$$W(x) = W_f(x) = \sum_{n \leqslant x} c(n). \tag{1.5}$$

Il est commode d'introduire le sous-espace, noté $\mathcal{F}$, de l'espace des formes modulaires modulo 2, engendré par les puissances impaires de $\Delta : \Delta, \Delta^3, \Delta^5, \ldots$. Toute forme modulaire modulo 2, $f = \sum_{n=0}^{\infty} c(n) q^n$, s'écrit en effet de manière unique $f = c(0) + \sum_{s=0}^{\infty} f_s^{2^s}$ où les formes f_s appartiennent à $\mathcal{F}$ et sont presque toutes nulles. Comme les formes de $\mathcal{F}$ n'ont d'après (1.4) que des coefficients $c(n)$ non nuls pour n impair, on a pour $x \geqslant 0$,

$$W_f(x) = c(0) + \sum_{s=0}^{\infty} W_{f_s}(2^{-s} x), \tag{1.6}$$

ce qui ramène en principe l'étude de $W_f(x)$ au cas où $f \in \mathcal{F}$.

Pour f une forme modulaire de niveau 1 modulo 2, soit $g = g(f)$ *l'ordre de nilpotence* de f, dont la définition est rappelée au §3.6. On a $g(f) \geqslant 1$ pour toute forme $f \neq 0$, et il est prouvé dans [14] que Δ est la seule forme de $\mathcal{F}$ telle que $g(f) = 1$. Il en résulte aisément (voir ci-dessous §5.4 pour plus de détails) que les formes telles que $g(f) = 1$ sont les combinaisons linéaires de Δ^{2^s} pour $s = 0, 1, 2, \ldots$. Pour une telle forme, qu'on peut écrire $f = c(0) + \sum_{s \in \mathcal{S}_1} \Delta^{2^s}$ où $S_1 \subset \mathbf{N}$ est un ensemble fini, il résulte facilement de (1.4) et de (1.6) que

$$W_f(x) = \left(\sum_{s \in \mathcal{S}_1} \frac{1}{2^{s/2+1}} \right) \sqrt{x} + O(1), \quad g(f) = 1. \tag{1.7}$$

Soit donc f une forme modulaire de niveau 1 modulo 2 telle que $g(f) \geqslant 2$. Serre a donné dans [22, §6.6] l'estimation suivante :

$$W_f(x) \asymp \frac{x}{\log x}(\log\log x)^{g(f)-2}. \tag{1.8}$$

Une formule simple énoncée dans [14] (cf. aussi [16] et [6]), et que nous rappelons ci-dessous au §3.6, donne la valeur de $g(f)$ (et de $h(f)$) quand $f = \Delta^k$, et permet de calculer facilement $g(f)$ quand f est donnée comme un polynôme en Δ.

Dans cet article, nous nous proposons de préciser l'estimation (1.8) en donnant un équivalent de $W_f(x)$ (cf. ci-dessous le théorème 3). Plus précsiément, si $g(f) \geqslant 2$, nous montrons qu'il existe une constante $\delta(f) > 0$ telle que

$$W_f(x) = \delta(f)\frac{x}{\log x}(\log\log x)^{g(f)-2}\left(1 + O\left(\frac{1}{\log\log x}\right)\right). \tag{1.9}$$

Nous donnons également une formule pour la valeur de $\delta(f)$ (voir (5.7) et (5.16) ci-dessous), qui, quand $f \in \mathcal{F}$, est de la forme

$$\delta(f) = \frac{\pi^2}{8(g-2)!4^{g-1}}\delta_0(f), \tag{1.10}$$

où $\delta_0(f)$ est un entier compris entre 1 et 2^{g-1}, lui même donné par une formule simple qui fait intervenir les *témoins de* f, notion que nous définissons et étudions au §4. Nous donnons un algorithme permettant de calculer les témoins de Δ^k par récurrence sur k, et de là les témoins d'une forme modulaire donnée comme polynôme en Δ. Nous proposons également une formule simple, mais conjecturale, permettant de calculer directement les témoins de Δ^k : voir la conjecture 1 ci-dessous.

L'équivalent (1.9) ne dit rien sur la dépendance en f du terme d'erreur en $O\left(\frac{1}{\log\log x}\right)$ de $W_f(x)$. Pour remédier partiellement à cela, nous donnons également une minoration effective de $W_f(x)$ (voir le théorème 4) : pour toute forme f telle que $g(f) \geqslant 5$, et pour tout nombre réel x tel que $x > e^{e^{3.5(g(f)-1)}}$, on a

$$W_f(x) > 0.4\ \delta(f)\frac{x}{\log x}(\log\log x - \log\log\log x)^{g(f)-2}. \tag{1.11}$$

Ramanujan s'était aussi intéressé à la parité de la fonction de partition $p(n)$. Quelques mois avant sa mort, il avait écrit à MacMahon pour lui demander s'il savait déterminer la parité de $p(n)$ (cf. [11]).

Pour $i \in \{0, 1\}$, on définit

$$A_i(x) = \#\{0 \leqslant n \leqslant x,\ \ p(n) \equiv i \pmod 2\}. \tag{1.12}$$

Les calculs de [18] indiquent que, vraisemblablement, on a $A_0(x) \sim A_1(x) \sim x/2$ mais ce résultat semble très difficile à prouver. On trouvera dans [3, §2.5] une minoration élémentaire de $A_0(x)$ et de $A_1(x)$.

Les meilleures minorations étaient (cf. [13])

$$A_0(x) \geqslant 0.28\sqrt{x}\sqrt{\log\log x}, \quad x \geqslant e, \tag{1.13}$$

$$A_1(x) \geqslant \frac{4.57\sqrt{x}}{\log x}, \quad x \geqslant 7 \tag{1.14}$$

et

$$A_1(x) \gg_K \frac{\sqrt{x}}{\log x}(\log\log x)^K, \quad \forall K > 0. \tag{1.15}$$

Au §6, nous améliorons légèrement ces inégalités en prouvant :

$$A_0(x) \geqslant 0.069\sqrt{x}\log\log x, \quad x > 1, \tag{1.16}$$

$$A_1(x) \geqslant \frac{0.048\sqrt{x}}{(\log x)^{7/8}}, \quad x \geqslant 2 \tag{1.17}$$

Ces minorations utilisent la valeur de l'ordre de nilpotence $g(f)$ pour $f = \Delta^k$ et certaines valeurs impaires de k, et aussi, en ce qui concerne (1.17), l'inégalité $\delta(f) \geqslant \frac{\pi^2}{8(g-2)!4^{g-1}}$ ainsi que la formule (1.11). On peut légèrement améliorer (1.17) si l'on admet la conjecture 1.

Notations

Dans tout l'article, p désigne un nombre premier, $\mathcal{P} = \{2, 3, 5, 7, 11, \ldots\}$ l'ensemble de tous les nombres premiers, et $\mathcal{P}_i$ l'ensemble des nombes premiers $p \equiv i \pmod 8$. La fonction de Möbius est notée μ.

Soit n un entier $\geqslant 1$; pour p premier, sa valuation p-adique, $v_p(n)$, est le plus grand exposant α tel que p^α divise n.

On désigne par x un nombre réel assez grand. La notation de Landau $f(x) = O(g(x))$ signifie qu'il existe x_0 réel et une constante B telle que, pour $x \geqslant x_0$, on a $|f(x)| \leqslant Bg(x)$.

Remerciements

Les deux auteurs remercient chaleureusement J.-P. Serre qui les a initiés au sujet des formes modulaires modulo 2, et pour l'aide qu'il leur a apportée grâce à l'étendue de ses connaissances.

2 Estimation de fonctions arithmétiques

2.1 Les fonctions $N(x; u, v)$ et $N_1(x; u, v)$

Soit n un entier $\geqslant 1$. Posons

$$\omega(n) = \sum_{p|n} 1, \tag{2.1}$$

$$\omega'(n) = \sum_{\substack{p|n \\ v_p(n)=1}} 1 \tag{2.2}$$

et

$$\omega''(n) = \sum_{\substack{p|n \\ v_p(n) \text{ impair}}} 1. \tag{2.3}$$

On a

$$\omega'(n) \leqslant \omega''(n) \leqslant \omega(n). \tag{2.4}$$

Soit $\mu(n)$ la fonction de Möbius et k un entier $\geqslant 1$. On pose

$$\pi_k(x) = \sum_{\substack{n\leqslant x \\ \mu(n)\neq 0,\ \omega(n)=k}} 1. \tag{2.5}$$

Landau a montré que, pour k fixé $\geqslant 1$, on a (cf. [9], § 56)

$$\pi_k(x) \sim \frac{x}{\log x}\frac{(\log\log x)^{k-1}}{(k-1)!}. \tag{2.6}$$

On trouvera une autre démonstration dans [8, chap. XXII]. Pour estimer $\pi_k(x)$, la meilleure méthode est sans doute celle de Selberg-Delange (cf. [25, II.6]) que nous utilisons ci-dessous au §2.2 pour la preuve du théorème 1.

Hardy et Ramanujan ont obtenu la majoration (cf. [7, Lemma A] et [13, lemme 2.1])

$$\pi_k(x) \leqslant 1.26\ \frac{x}{\log x}\frac{(\log\log x + 1.87)^{k-1}}{(k-1)!}, \quad k \geqslant 1,\ x \geqslant 2. \tag{2.7}$$

Pour $k \geqslant 0$, posons

$$\pi'_k(x) = \sum_{\substack{n\leqslant x \\ \omega'(n)=k}} 1. \tag{2.8}$$

Dans [13, lemme 2.2], pour $x \geq 2$, on donne les majorations

$$\pi'_0(x) \leqslant 2.18\sqrt{x} \tag{2.9}$$

et, à partir de (2.7), pour $k \geq 1$,

$$\pi'_k(x) \leqslant \frac{2.46\ x}{\log x}\left(1 + \frac{3.11}{\log x}\right)\frac{(\log\log x + 1.87)^{k-1}}{(k-1)!} + 4.36\ x^{3/4}. \tag{2.10}$$

Soit $I = \{1, 3, 5, 7\}$. Pour $i \in I$, on pose

$$\mathcal{P}_i = \{p \text{ premier}, \quad p \equiv i \pmod 8\}$$

et

$$\omega_i(n) = \sum_{p|n,\ p\in\mathcal{P}_i} 1. \tag{2.11}$$

Soit u et v deux entiers vérifiant $u \geqslant 0$, $v \geqslant 0$, $u + v \geqslant 1$. On désigne par $N(x; u, v)$ le nombre de $n \leqslant x$ qui sont des produits de $u + v$ nombres premiers distincts

$$n = p_1 p_2 \dots p_u p_{u+1} p_{u+2} \dots p_{u+v}$$

avec $p_1, p_2, \dots, p_u \in \mathcal{P}_3$ et $p_{u+1}, p_{u+2}, \dots, p_{u+v} \in \mathcal{P}_5$.

Théorème 1 *Pour u, v fixés et $x \to \infty$, on a*

$$N(x;u,v) = \kappa\, \frac{x(\log\log x)^{u+v-1}}{\log x}\left(1+O\left(\frac{1}{\log\log x}\right)\right) \tag{2.12}$$

avec

$$\kappa = \kappa(u,v) = \frac{u+v}{4^{u+v}\, u!\, v!} = \frac{1}{4^{u+v}(u+v-1)!}\binom{u+v}{u}. \tag{2.13}$$

[Par les méthodes décrites dans [25, II.5 et II.6], il est possible d'obtenir pour $N(x;u,v)$ une estimation plus précise.

On peut aussi généraliser le théorème 1 de la façon suivante : soit a un nombre entier $\geqslant 1$, $b_1, b_2, \ldots, b_r$ des classes inversibles distinctes modulo a, $u_1, u_2, \ldots, u_r$ des nombres entiers $\geqslant 0$ non tous nuls et $N(x;u_1,\ldots,u_r)$ le nombre de $n \leqslant x$ qui sont produits de $u_1+u_2+\ldots+u_r$ nombres premiers distincts

$$n = p_1p_2\ldots p_{u_1}\; p_{u_1+1}\ldots p_{u_1+u_2}\;\cdots\; p_{u_1+\ldots+u_{r-1}+1}\ldots p_{u_1+\ldots+u_r}$$

avec $p_1, p_2, \ldots, p_{u_1} \equiv b_1 \pmod a$, …, $p_{u_1+\ldots+u_{r-1}+1}, \ldots, p_{u_1+\ldots+u_r} \equiv b_r \pmod a$. On a

$$N(x;u_1,\ldots,u_r) = \kappa'\, \frac{x(\log\log x)^{u_1+\ldots+u_r-1}}{\log x}\left(1+O\left(\frac{1}{\log\log x}\right)\right) \tag{2.14}$$

avec,

$$\kappa' = \frac{u_1+u_2+\ldots+u_r}{\varphi(a)^{u_1+u_2+\ldots+u_r}\; u_1!\; u_2!\;\ldots\; u_r!}, \tag{2.15}$$

en notant φ la fonction d'Euler.]

Désignons par $N_1(x;u,v)$ le nombre d'entiers impairs $n \leqslant x$ qui s'écrivent

$$n = p_1p_2\ldots p_up_{u+1}p_{u+2}\ldots p_{u+v}\; m^2 \tag{2.16}$$

avec $p_1, p_2, \ldots, p_u \in \mathcal{P}_3$, $p_{u+1}, p_{u+2}, \ldots, p_{u+v} \in \mathcal{P}_5$, $p_1, p_2, \ldots, p_{u+v}$ distincts et $m \geqslant 1$ premier avec $2p_1p_2\ldots p_{u+v}$.

Nous déduisons du théorème 1 le corollaire suivant :

Corollaire 1 *Pour u, v fixés et $x \to \infty$, on a*

$$N_1(x;u,v) = \kappa\, \frac{\pi^2}{8}\frac{x(\log\log x)^{u+v-1}}{\log x}\left(1+O\left(\frac{1}{\log\log x}\right)\right). \tag{2.17}$$

Nous allons démontrer le théorème 1 ainsi que le corollaire 1 par la méthode de Selberg-Delange aux paragraphes 2.2, 2.3 et 2.4.

2.2 La formule de Selberg-Delange

Soit z_3 et z_5 deux nombres complexes dans la boule fermée $\mathcal{B}(0,z_0) \subset \mathbf{C}$ de centre 0 et de rayon $z_0 > 0$. Pour $\Re(s) > 1$, on pose

$$F(s) = F(s;z_3,z_5) = \sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s} z_3^{\omega_3(n)} z_5^{\omega_5(n)} = \prod_{j\in\{3,5\}}\prod_{p\in\mathcal{P}_j}\left(1+\frac{z_j}{p^s}\right),$$

$$F^+(s) = \sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s} z_0^{\omega(n)} = \prod_{p\in\mathcal{P}} \left(1 + \frac{z_0}{p^s}\right).$$

On écrit

$$F(s) = H(s) \prod_{j\in\{3,5\}} \prod_{p\in\mathcal{P}_j} \left(1 - \frac{1}{p^s}\right)^{-z_j}$$

et

$$F^+(s) = H^+(s)\zeta(s)^{z_0} = H^+(s) \prod_{p\in\mathcal{P}} \left(1 - \frac{1}{p^s}\right)^{-z_0}$$

avec

$$H(s) = H(s; z_3, z_5) = \prod_{j\in\{3,5\}} \prod_{p\in\mathcal{P}_j} \left(\left(1 + \frac{z_j}{p^s}\right)\left(1 - \frac{1}{p^s}\right)^{z_j}\right) \tag{2.18}$$

et

$$H^+(s) = \prod_{p\in\mathcal{P}} \left(\left(1 + \frac{z_0}{p^s}\right)\left(1 - \frac{1}{p^s}\right)^{z_0}\right) = \zeta(s)^{-z_0} \prod_{p\in\mathcal{P}} \left(1 + \frac{z_0}{p^s}\right). \tag{2.19}$$

Lemme 1 *Pour $\Re(s) \geqslant \sigma_0 > 1/2$ et $z_3, z_5 \in \mathcal{B}(0, z_0)$, les produits infinis $H(s)$ et $H^+(s)$ convergent uniformément et il existe une constante $B = B(\sigma_0, z_0)$ telle que*

$$|H(s)| \leqslant B \quad \text{et} \quad |H^+(s)| \leqslant B.$$

La fonction $H(s; z_3, z_5)$ est analytique pour $\Re(s) > 1/2$, $(z_3, z_5) \in \mathbf{C}^2$, et l'on a

$$H(1; 0, 0) = 1. \tag{2.20}$$

Démonstration : L'idée de la preuve est d'isoler dans (2.18) ou (2.19) les facteurs contenant les nombres premiers $p \leqslant 2z_0^2$ puis de développer en série le logarithme des facteurs restants. Pour une démonstration similaire, cf. [4, §3] ou [2, p. 237]. □

On définit

$$A(x) = \sum_{n\leqslant x} |\mu(n)| z_3^{\omega_3(n)} z_5^{\omega_5(n)}. \tag{2.21}$$

Proposition 1 *Lorsque $x \to \infty$ on a*

$$A(x) = \frac{x}{(\log x)^{1-(z_3+z_5)/4}} \left(\frac{H(1; z_3, z_5)\, C_3^{-z_3/4}\, C_5^{-z_5/4}}{\Gamma((z_3 + z_5)/4)} + O\left(\frac{1}{\log x}\right)\right) \tag{2.22}$$

avec, pour $j \in \{3, 5\}$,

$$C_j = \prod_{p\in\mathcal{P}_j} \left(1 - \frac{1}{p}\right)^3 \prod_{p\in\mathcal{P}-\mathcal{P}_j} \left(1 - \frac{1}{p}\right)^{-1} = \begin{cases} 0.678\ldots & \text{si } j = 3 \\ 1.595\ldots & \text{si } j = 5 \end{cases} \tag{2.23}$$

où $\mathcal{P}$ désigne l'ensemble de tous les nombres premiers. Dans (2.22), le O est uniforme pour $z_3, z_5 \in \mathcal{B}(0, z_0)$.

Démonstration : On applique le théorème 1 de [2] avec $b = 1$, $\xi = 1$, $k = 8$, $J = \{3, 5\}$, $g(n) = n$, $F_{g,J,\xi} = F$, $H_{g,J,\xi} = H$, $F^+_{g,J,\xi} = F^+$, $H^+_{g,J,\xi} = H^+$, $f_j(s) = z_j$, $f(s) = (z_3 + z_5)/4$ et $f^+(s) = z_0/2$.

Pour c suffisamment petit, le domaine $\mathcal{D}_c$ défini dans [2, (1.14)] par

$$\Re(s) \geqslant 1 - \frac{c}{\log(3 + |\Im(s)|)}$$

est contenu dans le demi-plan $\Re(s) \geqslant \sigma_0$, avec $1/2 < \sigma_0 < 1$ et les conditions requises sur H et H^+ dans [2, (1.17) et (1.19)] sont assurées par le lemme 1.

La formule [2, (1.23)] donne alors la partie principale de (2.22).

Comme il est expliqué dans [2, p. 233], lorsque $g(n) = n$ et que les fonctions $f_j(s)$ sont constantes, on peut remplacer le terme de reste $O((\log\log x)/\log x)$ de [2, (1.23)] par $O(1/\log x)$. □

Les valeurs de C_3 et C_5 calculées par la méthode décrite dans [2, p. 231] sont :

$$C_3 = 0.6788804287\ldots \qquad \text{et} \qquad C_5 = 1.5955189583\ldots$$

2.3 Preuve du théorème 1

Démonstration : Posons

$$G(z_3, z_5) = \frac{H(1; z_3, z_5)\, C_3^{-z_3/4}\, C_5^{-z_5/4}}{\Gamma\left(1 + \frac{z_3+z_5}{4}\right)} = \frac{H(1; z_3, z_5)\, C_3^{-z_3/4}\, C_5^{-z_5/4}}{\left(\frac{z_3+z_5}{4}\right)\, \Gamma\left(\frac{z_3+z_5}{4}\right)}.$$

Par le lemme 1, $H(1; z_3, z_5)$ est analytique pour $(z_3, z_5) \in \mathbf{C}^2$; donc $G(z_3, z_5)$ est aussi analytique dans $\mathbf{C}^2$ et, par (2.20), on a

$$G(0, 0) = 1.$$

Nous allons imposer à z_3 et z_5 de parcourir les cercles $\mathcal{C}_3$ et $\mathcal{C}_5$ de centre O et de rayon

$$\frac{1}{\ell}, \qquad \text{en notant} \quad \ell = \log\log x.$$

Lorsque x tend vers $+\infty$, on a donc

$$G(z_3, z_5) = 1 + R_2(z_3, z_5) \quad \text{avec} \quad R_2(z_3, z_5) = O\left(\frac{1}{\ell}\right) \tag{2.24}$$

et le O est uniforme pour $z_3 \in \mathcal{C}_3$ et $z_5 \in \mathcal{C}_5$.

La formule (2.22) devient alors

$$A(x) = \frac{x}{\log x} e^{\frac{z_3+z_5}{4}\,\ell} \left(\frac{z_3 + z_5}{4}\,((1 + R_2(z_3, z_5)) + R_3(z_3, z_5)\right) \tag{2.25}$$

avec

$$R_3(z_3, z_5) = O\left(\frac{1}{\log x}\right). \tag{2.26}$$

En appliquant la formule des résidus, la définition de $N(x;u,v)$ et (2.25) donnent

$$\begin{aligned} N(x;u,v) &= \left(\frac{1}{2i\pi}\right)^2 \int_{\mathcal{C}_3}\int_{\mathcal{C}_5} \frac{A(x)}{z_3^{u+1}\, z_5^{v+1}}\, \mathrm{d}z_5\, \mathrm{d}z_3 \\ &= \left(\frac{x}{(2i\pi)^2\, \log x}\right) (\mathcal{I}_1+\mathcal{I}_2+\mathcal{I}_3) \end{aligned} \tag{2.27}$$

avec

$$\mathcal{I}_3 = \int_{\mathcal{C}_3}\int_{\mathcal{C}_5} \frac{e^{\frac{z_3+z_5}{4}\ell}}{z_3^{u+1}\, z_5^{v+1}}\, R_3(z_3,z_5)\, \mathrm{d}z_5\, \mathrm{d}z_3,$$

$$\mathcal{I}_2 = \int_{\mathcal{C}_3}\int_{\mathcal{C}_5} \frac{e^{\frac{z_3+z_5}{4}\ell}}{z_3^{u+1}\, z_5^{v+1}} \left(\frac{z_3+z_5}{4}\right) R_2(z_3,z_5)\, \mathrm{d}z_5\, \mathrm{d}z_3$$

et

$$\mathcal{I}_1 = \int_{\mathcal{C}_3}\int_{\mathcal{C}_5} \frac{e^{\frac{z_3+z_5}{4}\ell}}{z_3^{u+1}\, z_5^{v+1}} \left(\frac{z_3+z_5}{4}\right) \mathrm{d}z_5\, \mathrm{d}z_3.$$

En utilisant, pour $j\in\{3,5\}$, les inégalités $\Re(z_j)\leqslant |z_j| = 1/\ell$, et les estimations (2.26) et (2.24), on majore $|\mathcal{I}_3|$ et $|\mathcal{I}_2|$:

$$|\mathcal{I}_3| \leqslant \ell^{u+v+2}\sqrt{e} \int_{\mathcal{C}_3}\int_{\mathcal{C}_5} |R_3(z_3,z_5)|\, \mathrm{d}z_5\, \mathrm{d}z_3 = O\left(\frac{\ell^{u+v}}{\log x}\right), \tag{2.28}$$

et

$$|\mathcal{I}_2| \leqslant \frac{\ell^{u+v+1}\sqrt{e}}{2} \int_{\mathcal{C}_3}\int_{\mathcal{C}_5} |R_2(z_3,z_5)|\, \mathrm{d}z_5\, \mathrm{d}z_3 = O\left(\ell^{u+v-2}\right). \tag{2.29}$$

Enfin, l'intégrale $\mathcal{I}_1$ se calcule par la méthode des résidus, en développant l'exponentielle :

$$\begin{aligned} \mathcal{I}_1 &= \int_{\mathcal{C}_3}\int_{\mathcal{C}_5} \left(\sum_{n_3,n_5\geqslant 0} \frac{z_3^{n_3-u-1}\, z_5^{n_5-v-1}\, \ell^{n_3+n_5}}{4^{n_3+n_5}\, n_3!\, n_5!}\right) \left(\frac{z_3+z_5}{4}\right) \mathrm{d}z_5\, \mathrm{d}z_3 \\ &= \frac{(2i\pi)^2}{4} \left(\frac{\ell^{u+v-1}}{4^{u+v-1}\, (u-1)!\, v!} + \frac{\ell^{u+v-1}}{4^{u+v-1}\, u!\, (v-1)!}\right) \\ &= (2i\pi)^2\, \frac{\ell^{u+v-1}}{4^{u+v}}\, \frac{u+v}{u!\, v!}\cdot \end{aligned} \tag{2.30}$$

Le théorème 1 découle alors de (2.27), (2.30), (2.29) et (2.28). □

2.4 Preuve du corollaire 1

Rappelons d'abord que

$$\sum_{\substack{m=1\\ m\ \text{impair}}}^{\infty} \frac{1}{m^2} = \sum_{n=1}^{\infty} \frac{1}{n^2} - \sum_{\substack{m=1\\ m\ \text{pair}}}^{\infty} = \frac{\pi^2}{6} - \frac{\pi^2}{24} = \frac{\pi^2}{8}$$

et que, lorsque $y\to\infty$,

$$\sum_{\substack{m>y\\ m\ \text{impair}}} \frac{1}{m^2} \leqslant \int_{y-1}^{\infty} \frac{\mathrm{d}t}{t^2} = \frac{1}{y-1} = O\left(\frac{1}{y}\right)\cdot \tag{2.31}$$

Lorsque $y \to \infty$, on a donc

$$\sum_{\substack{m \leqslant y \\ m \text{ impair}}} \frac{1}{m^2} = \frac{\pi^2}{8} + O\left(\frac{1}{y}\right). \tag{2.32}$$

Appelons $N_2(x;u,v)$ le nombre des $n \leqslant x$ qui s'écrivent sous la forme (2.16) avec $(m, p_1 p_2 \ \dots \ p_{u+v}) > 1$. Pour un tel n, on a $\omega'(n) \leqslant u+v-1$ et, avec la définition (2.8) et les majorations (2.9) et (2.10), il vient

$$N_2(x;u,v) \leqslant \sum_{0 \leqslant k \leqslant u+v-1} \pi'_k(x) = O\left(\frac{x}{\log x} \ell^{u+v-2}\right). \tag{2.33}$$

Par ailleurs, si l'on désigne par $N_3(x;u,v)$ le nombre des $n \leqslant x$ qui s'écrivent sous la forme (2.16) avec m quelconque, on a

$$N_1(x;u,v) = N_3(x;u,v) - N_2(x;u,v). \tag{2.34}$$

Pour évaluer $N_3(x;u,v)$, posons $y = (\log x)^2$; en utilisant la majoration banale $N_3(t;u,v) \leqslant t$, il vient

$$N_3(x;u,v) = \sum_{\substack{m \leqslant y \\ m \text{ impair}}} N\left(\frac{x}{m^2};u,v\right) + R \tag{2.35}$$

avec, par (2.31),

$$R = \sum_{\substack{m > y \\ m \text{ impair}}} N\left(\frac{x}{m^2};u,v\right) \leqslant \sum_{\substack{m > y \\ m \text{ impair}}} \frac{x}{m^2} = O\left(\frac{x}{(\log x)^2}\right). \tag{2.36}$$

Uniformément pour $m \leqslant (\log x)^2$, on a $\log(x/m^2) = (\log x)\,(1 + O(\ell/\log x))$ et $\log\log(x/m^2) = \ell\,(1 + O(1/\log x))$, ce qui, reporté dans (2.12), donne

$$N\left(\frac{x}{m^2};u,v\right) = \kappa\, \frac{x}{m^2 \log x}\, \ell^{u+v-1} \left(1 + O\left(\frac{1}{\ell}\right)\right). \tag{2.37}$$

Les formules (2.35), (2.36), (2.37) et (2.32) entraînent alors

$$N_3(x;u,v) = \kappa \frac{\pi^2}{8} \frac{x}{\log x} \ell^{u+v-1} \left(1 + O\left(\frac{1}{\ell}\right)\right)$$

ce qui, avec (2.34) et (2.33), prouve le corollaire 1. □

2.5 Minoration effective de $N(x;u,v)$

Lemme 2 *Pour tout $i \in \{1,3,5,7\}$, il existe une constante réelle M_i telle que pour tout $x > e^{9900}$, on ait*

$$\frac{1}{4}\log\log x + M_i - \frac{1}{\log x} < \sum_{\substack{p \in \mathcal{P}_i \\ p \leqslant x}} \frac{1}{p} < \frac{1}{4}\log\log x + M_i + \frac{1}{\log x}.$$

On a $M_3 \simeq 0.162323$ et $M_5 \simeq -0.000324$.

Démonstration : C'est la formule de Mertens (parfois appelée "second théorème de Mertens") pour les nombres premiers d'une progression arithmétique. Elle est bien connue (pour les valeurs de M_3 et M_5, voir [10] et le fichier informatique associé) sauf pour le fait que le terme d'erreur est en valeur absolue $< \frac{1}{\log x}$. Nous en donnons donc une preuve, qui montrera même que ce terme d'erreur est plus petit que $\frac{1}{100 \log x}$. Les estimations qui vont suivre sont d'ailleurs assez grossières, et on pourrait certainement les améliorer en utilisant notamment les calculs de Platt[1] sur les zéros des fonctions L de Dirichlet concernées jusqu'à la hauteur 12500000.

Pour $i \in \{1,3,5,7\}$, posons $\theta(x;i) = \sum_{\substack{p \in \mathcal{P}_i \\ p \leqslant x}} \log p$. Le théorème 5 de [5] donne un estimation de $\theta(x;i)$, que nous allons rappeler. Dans ce théorème, on prend $k = 8$, et $H = 1000$, ce qui est possible d'après le lemme 2 *loc. cit.* La constante $C_1(8)$ qui apparaît dans l'énoncé du théorème vérifie $9 < C_1(8) < 32\pi$, d'après *loc. cit.* page 1139. Les constantes $X_0, \ldots, X_3$ du théorème 5 vérifient donc $X_0, X_1, X_3 < 10$ et $X_2 < 32$, d'où $X_4 = \max(X_0, X_1, X_2, X_3, 10) < 32$. On pose, comme dans *loc. cit.*, $\epsilon(X) = 3\sqrt{\frac{8}{\varphi(8)C_1(8)}}\sqrt{X}e^{-X}$. On a $\epsilon(X) < \sqrt{2X}e^{-X} < \frac{1}{1000X^2}$ pour $X > 32$. La conclusion du théorème 5 *loc. cit.* est que, pour $R \simeq 9.6459$, si $X = \sqrt{\frac{\log x}{R}} > X_4$, donc en particulier dès que $x > e^{9900}$,

$$\left|\theta(x;i) - \frac{x}{4}\right| < x\epsilon(X) = x\epsilon\left(\sqrt{\frac{\log x}{R}}\right) < \frac{xR}{1000 \log x} < \frac{x}{101 \log x},$$

Nous écrirons $\theta(x;i) = x/4 + \alpha(x;i)\frac{x}{\log x}$ avec $|\alpha(x;i)| < \frac{1}{101}$ pour $x > e^{9900}$.

En sommant par parties (précisément en appliquant la formule (22.5.2) du théorème 421 de [8]), on obtient

$$\begin{aligned}
\sum_{\substack{p \in \mathcal{P}_i \\ p < x}} \frac{1}{p} &= \sum_{\substack{p \in \mathcal{P}_i \\ p \leqslant x}} \log p \cdot \frac{1}{p \log p} \\
&= \frac{\theta(x;i)}{x \log x} + \int_2^x \theta(t;i) \frac{1 + \log t}{t^2 (\log t)^2} dt \\
&= \frac{1}{4 \log x} + \frac{\alpha(x;i)}{(\log x)^2} + \frac{1}{4}(\log\log x - \log\log 2) + \int_2^x \frac{1/4 + \alpha(t;i) + \alpha(t;i)/\log(t)}{t(\log t)^2} dt \\
&= \frac{1}{4}\log\log x + M_i + \frac{1}{4 \log x} + \frac{\alpha(x;i)}{(\log x)^2} - \int_x^\infty \frac{1/4 + \alpha(t;i) + \alpha(t;i)/\log(t)}{t(\log t)^2} dt \\
&= \frac{1}{4}\log\log x + M_i + \frac{\alpha(x;i)}{(\log x)^2} - \int_x^\infty \frac{\alpha(t;i) + \alpha(t;i)/\log(t)}{t(\log t)^2} dt
\end{aligned}$$

où $M_i = -\frac{1}{4}\log\log 2 + \int_2^\infty \frac{1/4 + \alpha(t;i) + \alpha(t;i)/\log(t)}{t(\log t)^2} dt$ (noter que l'intégrale est convergente). Quand $x > e^{9900}$, on a $\alpha(x;i)/\log x < 1/999900$, et donc $|\frac{\alpha(x;i)}{(\log x)^2}| < \frac{1}{999900 \log x}$. De même pour $t > x > e^{9900}$, on a $|\alpha(t;i) + \alpha(t;i)/\log(t)| < \frac{1}{101} + \frac{1}{999900}$ et donc $|\int_x^\infty \frac{\alpha(t;i) + \alpha(t;i)/\log(t)}{t(\log t)^2}| < (\frac{1}{101} + \frac{1}{999900})\frac{1}{\log x}$. En additionnant ces inegalités, on trouve que pour $x > e^{9900}$,

$$\frac{1}{4}\log\log x + M_i - \frac{1}{100 \log x} < \sum_{\substack{p \in \mathcal{P}_i \\ p \leqslant x}} \frac{1}{p} < \frac{1}{4}\log\log x + M_i + \frac{1}{100 \log x},$$

[1] Numerical computations concerning the GRH. PhD Thesis, http ://arxiv.org/abs/1305.3087

ce qui implique le lemme. □

Pour $u \geqslant 0$ et $v \geqslant 0$ deux entiers, introduisons les fonctions

$$R_{u,v,\pm}(x) = (\log\log x + 4M_3 \pm \frac{4}{\log x})^u (\log\log x + 4M_5 \pm \frac{4}{\log x})^v.$$

Si $u < 0$ ou $v < 0$, posons simplement $R_{u,v,\pm}(x) = 0$.

Lemme 3 *Soit $u \geqslant 0$, $v \geqslant 0$, $h = u + v$ et supposons que x satisfait*

$$x > e^{e^{2h}}. \tag{2.38}$$

Alors, pour $h \geqslant 4$, on a

$$0.97(\log\log x)^h < R_{u,v,\pm}(x) < 1.4(\log\log x)^h$$

Démonstration : On a

$$\begin{aligned} \log(R_{u,v,\pm}(x)/(\log\log x)^h) &= u\log(1 + \frac{4M_3}{\log\log x} \pm \frac{4}{\log x \log\log x}) \\ &+ v\log(1 + \frac{4M_5}{\log\log x} \pm \frac{4}{\log x \log\log x}) \end{aligned}$$

En utilisant la majoration $\log(1+t) \leqslant t$, on trouve

$$\log(R_{u,v,\pm}(x)/(\log\log x)^h) < \frac{4uM_3 + 4vM_5}{\log\log x} + \frac{4h}{\log x \log\log x}$$

On a

$$\frac{4uM_3 + 4vM_5}{\log\log x} \leqslant 4hM_3/\log\log x < 2M_3 < 0.33$$

en utilisant l'hypothèse (2.38). De même,

$$\frac{4h}{\log x \log\log x} < 2/\log x < 2/e^{2h} \leqslant 2/e^8 < 0.001.$$

D'où $\log(R_{u,v,\pm}(x)/(\log\log x)^h) < 0.331$ et $R_{u,v,\pm}(x)/(\log\log x)^h < 1.4$.

Notons que $|\frac{4M_3}{\log\log x} \pm \frac{4}{\log x \log\log x}| < \frac{1}{3h} \leqslant 1/12$ et que la même inégalité est vraie avec M_3 remplacé par M_5. En utilisant la minoration[2]

$$\log(1+t) > t - t^2 \text{ pour } t > -1/2, \tag{2.39}$$

on trouve

$$\log(R_{u,v,\pm}(x)/(\log\log x)^h) > \frac{4uM_3 + 4vM_5}{\log\log x} - \frac{4h}{\log x \log\log x} - h\frac{1}{9h^2}$$

On a $\frac{4uM_3+4vM_5}{\log\log x} > \frac{4hM_5}{\log\log x} > 2M_5 > -0.001$. Le terme $-\frac{4h}{\log x \log\log x}$ est aussi plus petit que 0.001 en valeur absolue comme on l'a vu ci-dessus, et $\frac{-1}{9h} \geqslant \frac{-1}{36} > -0.028$. D'où

$$\log(R_{u,v,+}(x)/(\log\log x)^h) > -0.03$$

[2]Dont voici une preuve : si $|t| \geqslant 1/2$, $\log(1+t) = t - t^2/2 + \sum_{n\geqslant 3}(-1)^{n+1}t^n/n \geqslant t - t^2/2 - \frac{1}{3}|t^3|\sum_{n\geqslant 0}|t|^n \geqslant t - t^2/2 - \frac{2}{3}|t^3| \geqslant t - t^2/2 - t^2/3 \geqslant t - t^2$.

et le lemme. □

Notons $N_{u,v}$ l'ensemble des nombres entiers sans facteurs carrés ayant exactement $u+v$ facteurs premiers, u d'entre eux dans $\mathcal{P}_3$ et les v autres dans $\mathcal{P}_5$.

Proposition 2 *Soit $u \geqslant 0$, $v \geqslant 0$ deux entiers, et $h = u+v$. Alors, si $h \geqslant 4$, et si x est un nonbre réel satisfaistant*

$$x > e^{e^{5h/2}}, \tag{2.40}$$

on a

$$\sum_{\substack{m \in N_{u,v} \\ p|m \Rightarrow p<x}} \frac{1}{m} \geqslant 0.63 \frac{1}{u!v!4^h} (\log\log x)^h. \tag{2.41}$$

Démonstration : Notons $S_{u,v}$ l'ensemble des suites de $h = u+v$ nombres premiers $< x$, dont les u premiers termes sont dans $\mathcal{P}_3$ et les v derniers termes dans $\mathcal{P}_5$. Soit $S'_{u,v}$ le sous-ensemble de $S_{u,v}$ formés des suites dont les h éléments sont distincts, et $S''_{u,v}$ son complémentaire dans $S_{u,v}$.

On a

$$\begin{aligned} \sum_{\substack{m=p_1\dots p_h \\ (p_1,\dots,p_h)\in S_{u,v}}} \frac{1}{m} &= \left(\sum_{p<x,\ p\in\mathcal{P}_3} \frac{1}{p}\right)^u \left(\sum_{p<x,\ p\in\mathcal{P}_5} \frac{1}{p}\right)^v \\ &> \frac{1}{4^h}(\log\log x + 4M_3 - 4/\log x)^u (\log\log x + 4M_5 - 4/\log x)^v \qquad (2.42) \\ &= \frac{1}{4^h} R_{u,v,-}(x). \end{aligned}$$

Pour passer de la première ligne à la deuxième, on a utilisé le lemme 2, ce qui est possible puisque sous les hypothèses de la proposition, $x > e^{e^{10}} > e^{9900}$.

Décomposons la somme sur $S_{u,v}$ du membre de gauche de (2.42) en une somme sur $S'_{u,v}$ et une sur $S''_{u,v}$:

$$\sum_{\substack{m=p_1\dots p_h \\ (p_1,\dots,p_h)\in S_{u,v}}} \frac{1}{m} = \sum_{\substack{m=p_1\dots p_h \\ (p_1,\dots,p_h)\in S'_{u,v}}} \frac{1}{m} + \sum_{\substack{m=p_1\dots p_h \\ (p_1,\dots,p_h)\in S''_{u,v}}} \frac{1}{m}. \tag{2.43}$$

La somme sur $S'_{u,v}$ est à un facteur près celle que nous voulons minorer. Précisément, tout élément m de $N_{u,v}$ dont tous les facteurs premiers sont plus petits que x s'écrit $m = p_1 \dots p_h$ pour exactement $u!v!$ suites $(p_1, \dots, p_h)$ de $S'_{u,v}$. Donc

$$\sum_{\substack{m \in N_{u,v} \\ p|m \Rightarrow p<x}} \frac{1}{m} = \frac{1}{u!v!} \sum_{\substack{m=p_1\dots p_h \\ (p_1,\dots,p_h)\in S'_{u,v}}} \frac{1}{m}. \tag{2.44}$$

Majorons la somme restante, celle sur $S''_{u,v}$. Lorsque $u \geqslant 2$, pour tout couple d'entiers (i,j) satisfaisant $1 \leqslant i < j \leqslant u$, définissons l'application $f_{i,j} : \mathcal{P}_3 \times S_{u-2,v} \to S''_{u,v}$ qui envoie $(p, (p_1, \dots, p_{h-2}))$ sur la suite de h nombres premiers

obtenue en intercalant dans $(p_1,\dots,p_{h-2})$ deux fois p, en positions i et j. De même, lorsque $v \geqslant 2$, pour (i,j) satisfaisant $u+1 \leqslant i < j \leqslant h = u+v$, définissons une seconde application $f'_{i,j} : \mathcal{P}_5 \times S_{u,v-2} \to S''_{u,v}$. Comme toute suite $(p_1,\dots,p_h)$ dans $S''_{u,v}$ satisfait par définition $p_i = p_j$ pour un couple (i,j) de l'un des deux types considérés ci-dessus, on voit que $S''_{u,v}$ est la réunion des images des applications $f_{i,j}$ et $f'_{i,j}$. On a :

$$\begin{aligned}\sum_{\substack{m=p_1\cdots p_h\\(p_1,\dots,p_h)\in \mathrm{image}(f_{i,j})}} 1/m &\leqslant \left(\sum_{p\equiv 3 \pmod 8} 1/p^2\right) \sum_{\substack{m=p_1\cdots p_{h-2}\\(p_1,\dots,p_{h-2})\in S_{u-2,v}}} 1/m\\ &< C_3 \left(\sum_{p<x,\ p\in\mathcal{P}_3} \frac{1}{p}\right)^{u-2} \left(\sum_{p<x,\ p\in\mathcal{P}_5} \frac{1}{p}\right)^{v}\\ &< \frac{C_3}{4^{h-2}} R_{u-2,v,+}(x)\end{aligned}$$

où l'on a posé $C_3 = \sum_{p\equiv 3 \pmod 8} 1/p^2 \simeq 0.1238$ et une estimation similaire pour les $f'_{i,j}$ faisant intervenir $C_5 = \sum_{p\equiv 5 \pmod 8} 1/p^2 \simeq 0.04899$. On obtient donc si $u \geqslant 2$ et $v \geqslant 2$, en sommant sur les différents couples (i,j) possibles (il y en a $u(u-1)/2 + v(v-1)/2 \leqslant h(h-1)/2$.)

$$\sum_{\substack{m=p_1\cdots p_h\\(p_1,\dots,p_h)\in S''_{u,v}}} \frac{1}{m} \leqslant \frac{h(h-1)}{2\cdot 4^{h-2}}(C_3 R_{u-2,v,+}(x) + C_5 R_{u,v-2,+}(x)) \tag{2.45}$$

L'inégalité (2.45) reste valable si $u \leqslant 1$ ou si $v \leqslant 1$ grâce à la convention $R_{a,b,\pm}(x) = 0$ pour a ou b négatif. En utilisant (2.42), (2.43), (2.44), (2.45) on obtient :

$$\begin{aligned}&\sum_{\substack{m\in N_{u,v}\\ p\mid m \Rightarrow p<x}} \frac{1}{m} > \\ &\frac{1}{u!v!4^h} R_{u,v,-}(x) \quad \left(1 - 8h(h-1)\frac{C_3 R_{u-2,v,+}(x) + C_5 R_{u,v-2,+}(x)}{R_{u,v,-}(x)}\right)\end{aligned} \tag{2.46}$$

Pour minorer le facteur entre parenthèses, on majore :

$$\begin{aligned}8h(h-1)\frac{R_{u-2,v,+}(x)}{R_{u,v,-}(x)} &\leqslant \frac{8h(h-1)}{(\log\log x + 4M_3 + 4/\log(x))^2}\frac{R_{u,v,+}(x)}{R_{u,v,-}(x)}\\ &< \frac{8h^2}{(\log\log x)^2}\frac{1.4}{0.97} \text{ (en utilisant le lemme 3)}\\ &< \frac{8}{2.5^2}\frac{1.4}{0.97} \text{ (en utilisant l'hypothèse (2.40))}\\ &< 1.9\end{aligned}$$

De même

$$\begin{aligned}8h(h-1)\frac{R_{u,v-2,+}(x)}{R_{u,v,-}(x)} &\leqslant \frac{8h(h-1)}{(\log\log x + 4M_5 + 4/\log(x))^2}\frac{R_{u,v,+}(x)}{R_{u,v,-}(x)}\\ &< \frac{8h^2}{(0.99\log\log x)^2}\frac{1.4}{0.97}\\ &< \frac{8}{2.5^2}\frac{1.4}{0.97\times 0.99^2} < 1.9.\end{aligned}$$

On a utilisé que $\log\log x+4M_5+4/\log(x) > 0.99\log\log x$ ce qui résulte aisément de nos hypothèses $\log\log x > 5h/2 \geqslant 10$ et de la valeur de M_5. On a donc

$$1 - 8h(h-1)\frac{C_3 R_{u-2,v,+}(x) + C_5 R_{u,v-2,+}(x)}{R_{u,v,-}(x)} > 1 - 1.9(C_3 + C_5) > 0.65.$$

En introduisant cette minoration dans (2.46), et en utlisant la minoration de $R_{u,v,-}(x)$ donnée par le lemme 3, on obtient

$$\sum_{\substack{m\in N_{u,v}\\ p|m\Rightarrow p<x}} \frac{1}{m} > 0.65\times 0.97\frac{1}{u!v!4^h}(\log\log x)^h.$$

Ceci prouve la proposition. □

Théorème 2 *Pour tout entier $h \geqslant 4$, toute paire (u,v) d'entiers positifs tels que $u+v=h$, et tout x nombre réel tel que*

$$x > e^{e^{3.5h}} \quad \textit{i.e.} \quad \log\log x > 3.5h, \tag{2.47}$$

on a

$$N(x;u,v) > 0.502\frac{1}{4^h(h-1)!}\binom{h}{u}\frac{x}{\log x}(\log\log x - \log\log\log x)^{h-1}.$$

Démonstration : Posons $z = x^{1/\log\log x}$.

On peut évidemment minorer $N(x;u,v)$ par le nombre de $n \in N_{u,v}$, $n \leqslant x$, qui satisfont la condition supplémentaire[3] que tous les facteurs premiers de n sauf exactement un sont $\leqslant z$. Si pour un tel n, on note p l'unique facteur premier qui est $> z$, et m le produit des autres facteurs premiers, on a $n = mp$ et $m \in N_{u-1,v}$ si $p \in \mathcal{P}_3$, $m \in N_{u,v-1}$ si $p \in \mathcal{P}_5$. On a donc

$$\begin{aligned} N(x;u,v) \geqslant & \sum_{\substack{m\in N_{u-1,v}\\ p|m\Rightarrow p<z}} \sum_{\substack{z<p\leqslant x/m\\ p\in\mathcal{P}_3}} 1 \\ & + \sum_{\substack{m\in N_{u,v-1}\\ p|m\Rightarrow p<z}} \sum_{\substack{z<p\leqslant x/m\\ p\in\mathcal{P}_5}} 1 \end{aligned} \tag{2.48}$$

D'après une version effective du théorème des nombres premiers dans une progression arithmétique due à Ramaré et Rumely (cf. [21]), on a $|\theta(x;i) - x/4| < 0.0008x$ pour $x > 10^{10}$, et donc $0.249x < \theta(x;i) < 0.251x$. Comme $z > 10^{10}$ sous les hypothèses faites sur h et x, on en déduit que

$$\sum_{\substack{z<p\leqslant x/m\\ p\in\mathcal{P}_i}} 1 \geqslant \frac{\theta(x/m;i) - \theta(z;i)}{\log x} > \frac{0.249x/m - 0.251z}{\log x}.$$

[3]Cette méthode consistant à séparer les $n \in N_{u,v}$ entre ceux qui ont un facteur premier supérieur à $x^{1/\log\log x}$ et ceux qui n'en ont pas a été expliquée par Kannan Soundararajan à Bellaïche, qui l'en remercie ici.

Comme m est le produit de $h-1$ nombres premiers $< z$, on a $m < z^h$, et donc $x/m > x^{1-h/\log\log x} > x^{5/7}$ tandis que $z \leqslant x^{1/14}$ puisque $\log\log x > 14$ d'après (2.47) et $h \geqslant 4$. Donc $z < 0.0001x/m$, et l'on obtient :

$$1 \geqslant 0.2\frac{x}{m\log x}. \tag{2.49}$$

Introduisant (2.49) dans (2.48), il vient

$$N(x;u,v) > 0.2\frac{x}{\log x}\sum_{\substack{m\in N_{u-1,v}\cup N_{u,v-1}\\ p\mid m\Rightarrow p<z}}\frac{1}{m}. \tag{2.50}$$

On a $\log\log z = \log\log x - \log\log\log x > 3/4\log\log x$ pour $x > e^{e^{12}}$ comme dans nos hypothèses, ce qui implique $\log\log z > \frac{3}{4}3.5h > 5h/2$ d'après (2.47). On peut donc appliquer la proposition 2 avec x remplacé par z afin de minorer la somme sur $N_{u-1,v}$ (si $u \geqslant 1$) et celle sur $N_{u,v-1}$ (si $v \geqslant 1$) dans (2.50). On obtient si $u \geqslant 1$ et $v \geqslant 1$

$$N(x;u,v) > 0.126\frac{1}{4^{h-1}}\left(\frac{1}{(u-1)!v!}+\frac{1}{u!(v-1)!}\right)\frac{x}{\log x}(\log\log x-\log\log\log x)^{h-1}$$

Si $u=0$, l'inégalité ci-dessus est vraie en omettant le terme $\frac{1}{(u-1)!v!}$ et de même si $v=0$. Tenant compte de ce que $\frac{1}{u!(v-1)!}+\frac{1}{(u-1)!v!} = \frac{1}{(h-1)!}\binom{h}{u}$ si $u,v \geqslant 1$, le théorème est prouvé. □

3 Formes modulaires modulo 2

Dans ce paragraphe, nous rappelons certaines propriétés des formes modulaires de niveau 1 modulo 2 (cf. [14, 15, 16, 6]).

3.1 Le $\mathbf{F}_2$-espace vectoriel $\mathcal{F}$

Soit $\mathcal{F}$ le sous-espace de $\mathbf{F}_2[\Delta]$ engendré par $\Delta, \Delta^3, \Delta^5, \ldots$.

Puisque $\Delta^{2k}(q) = \Delta^k(q^2)$, toute forme parabolique modulo 2, $f = \sum_{k\in\mathcal{K}}\Delta^k$ (où $\mathcal{K}$ est un ensemble fini de nombres entiers > 0) peut s'écrire

$$f = \sum_{s\geqslant 0} f_s^{2^s} \quad \text{avec} \quad f_s \in \mathcal{F}, \tag{3.1}$$

en posant

$$f_s = \sum_{k\in\mathcal{K},\, v_2(k)=s}\Delta^{k2^{-s}}.$$

Toute forme modulaire f modulo 2 non parabolique s'écrit

$$f = 1 + \sum_{s\geqslant 0} f_s^{2^s} \quad \text{avec} \quad f_s \in \mathcal{F}. \tag{3.2}$$

3.2 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

$$T_p|f = \sum_{n\geqslant 0} \gamma_n q^n \quad \text{avec } \gamma(n) = \begin{cases} c(pn) & \text{si } p \text{ ne divise pas } n \\ c(pn) + c(n/p) & \text{si } p \text{ divise } n. \end{cases} \tag{3.3}$$

Les opérateurs de Hecke commutent entre eux. D'autre part, ils sont nilpotents. Pour $p \geqslant 3$, et k impair positif, on a

$$T_p|\Delta^k = \sum_{\substack{j\equiv pk \pmod 8 \\ 1\leqslant j\leqslant k-2}} \mu_j \Delta^j, \quad \text{avec } \mu_j \in \mathbf{F}_2. \tag{3.4}$$

L'opérateur de Hecke T_p commute avec l'élévation au carré $f \mapsto f^2$. Soit $f \in \mathcal{F}$ et s un entier $\geqslant 0$. On a

$$T_p|f^{2^s} = (T_p|f)^{2^s}. \tag{3.5}$$

L'action des opérateurs de Hecke sur les formes $\Delta, \Delta^3, \Delta^5$ et Δ^7 est donnée par :

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

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

Les assertions (i), (ii) et (iii) sont faciles. L'assertion (iv) sera démontrée dans [16].

3.3 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 :

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

et

$$h(k) = n_3(k) + n_5(k).$$

Nous appellons

$$[n_3(k), n_5(k)]$$

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 $\mathbf{N}^2$.

3.4 La relation de domination

Si k et ℓ sont deux entiers natuels de même parité, on dit que ℓ domine k et on écrit

$$k \prec \ell \quad \text{ou} \quad \ell \succ k \tag{3.6}$$

si l'on a $h(k) < h(\ell)$ ou bien $h(k) = h(\ell)$ et $n_5(k) < n_5(\ell)$. La relation

$$k \preccurlyeq \ell \quad \text{définie par } k \prec \ell \text{ ou } k = \ell, \tag{3.7}$$

est une relation d'ordre total sur l'ensemble des entiers pairs (resp. impairs) $\geqslant 0$.

3.5 L'exposant dominant

Il est commode d'écrire une forme modulaire $f \in \mathcal{F}$, $f \neq 0$ sous la forme

$$f = \Delta^{k_1} + \Delta^{k_2} \ldots + \Delta^{k_r} \quad \text{avec} \quad k_1 \succ k_2 \succ \ldots \succ k_r. \tag{3.8}$$

On dit que k_1 est l'exposant dominant de f et l'on définit $h(f)$ par

$$h(f) = h(k_1) = \max_{1 \leqslant i \leqslant r} h(k_i). \tag{3.9}$$

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

Les propositions 4 et 5 ci-dessous sont énoncées dans [14] et démontrées dans [16] et [6].

Proposition 4 *(i) Lorsque $n_3(k_1) \geqslant 1$, on a $h(T_3|f) = h(k_1) - 1$ et l'exposant dominant de $T_3|f$ a pour code $[n_3(k_1) - 1, n_5(k_1)]$.*
(ii) Lorsque $n_3(k_1) = 0$, on a $h(T_3|f) \leqslant h(k_1) - 1$.

Proposition 5 *(i) Lorsque $n_5(k_1) \geqslant 1$, on a $h(T_5|f) = h(k_1) - 1$ et l'exposant dominant de $T_5|f$ a pour code $[n_3(k_1), n_5(k_1) - 1]$.*
(ii) Lorsque $n_5(k_1) = 0$, on a $h(T_5|f) \leqslant h(k_1) - 2$.

Il résulte des propositions 4 et 5 que l'on a (cf. [14, théorème 5.1])

$$T_3^{n_3(k_1)} T_5^{n_5(k_1)} | f = \Delta. \tag{3.10}$$

3.6 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 $p_1, p_2, \ldots, p_g$ (pas forcément distincts), on ait $T_{p_1} T_{p_2} \ldots T_{p_g} | f = 0$.

Lorsque $f = 0$, on convient que $g(f) = -\infty$.

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

$$g(f) \geqslant g(T_p|f) + 1. \tag{3.11}$$

Soit $f \in \mathcal{F}$, $f \neq 0$. Le résultat principal de [14] est

$$g(f) = h(f) + 1. \tag{3.12}$$

On déduit de (3.11) et (3.12) :

$$h(f) \geqslant h(T_p|f) + 1. \tag{3.13}$$

Nous utiliserons aussi (cf. [14, corollaire 5.2])

Proposition 6 *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*

$$g(T_p|f) \leqslant g(f) - 2 \tag{3.14}$$

et (cf. [14, corollaire 5.3])

Proposition 7 *Soit $f \in \mathcal{F}$; si $g(f) = 1$ alors $f = \Delta$. Si $g(f) < 1$ alors $f = 0$.*

3.7 La base $m(a,b)$, adaptée à T_3 et T_5

Dans la Note [15, §6], est démontrée la propriété suivante :

Proposition 8 *Il existe une base $m(a,b)_{a,b\geqslant 0}$ du $\mathbf{F}_2$-espace vectoriel $\mathcal{F}$ et une seule qui a les quatre propriétés suivantes* :

i) $m(0,0) = \Delta$.

ii) Si $a+b>0$, le coefficient de q dans $m(a,b)$ est nul.

iii) $T_3|m(a,b) = \begin{cases} m(a-1,b) & si\ a>0 \\ 0 & si\ a=0. \end{cases}$

iv) $T_5|m(a,b) = \begin{cases} m(a,b-1) & si\ b>0 \\ 0 & si\ b=0. \end{cases}$

L'exposant dominant de $m(a,b)$ est l'entier impair de code (a,b). En particulier, par (3.12), l'ordre de nilpotence de $m(a,b)$ est égal à $a+b+1$.

Une forme $f \in \mathcal{F}$ d'exposant dominant k s'écrit de manière unique sous la forme

$$f = \sum_{a=0}^{h(f)} \sum_{b=0}^{h(f)-a} \varepsilon_{a,b}\, m(a,b) \quad \text{avec} \quad \varepsilon_{a,b} \in \{0,1\}. \tag{3.15}$$

Lorsque $f \neq 0$, le coefficient $\varepsilon_{n_3(k),n_5(k)}$ est non nul.

On appelle *partie principale* de ce développement la somme

$$P(f) = \sum_{a=0}^{h(f)} \varepsilon_{a,h(f)-a}\, m(a,h(f)-a),$$

que l'on écrira plutôt sous la forme

$$P(f) = \sum_{j=1}^{J} m(a_j,b_j), \quad a_1 < a_2 < \ldots < a_J, \tag{3.16}$$

en désignant par a_j, b_j (pour $1 \leqslant j \leqslant J$) les nombres tels que $a_j + b_j = h(f)$ et $\varepsilon_{a_j,b_j} = 1$. Notons que l'on a

$$h(f - P(f)) \leqslant h(f) - 1. \tag{3.17}$$

Exemples (pour d'autres exemples cf. [26]) :

$m(0,0) = \Delta$; $m(1,0) = \Delta^3$; $m(0,1) = \Delta^5$;

$m(2,0) = \Delta^9$; $m(1,1) = \Delta^7$; $m(0,2) = \Delta^{17}$;

$m(3,0) = \Delta^{11}$; $m(2,1) = \Delta^{13}$; $m(1,2) = \Delta^{11} + \Delta^{19}$; $m(0,3) = \Delta^{13} + \Delta^{21}$;

$m(2^r,0) = \Delta^{1+2^{2r+1}}$, $m(2^r-1,0) = \Delta^{(1+2^{2r+1})/3}$ et $m(0,2^r) = \Delta^{1+2^{2r+2}}$.

4 Témoins d'une forme modulaire $f \in \mathcal{F}$

4.1 Définition

Soit $f \in \mathcal{F}$, $f \neq 0$, k son exposant dominant, $g = g(f)$ son indice de nilpotence et $h = h(f) = h(k)$. Par (3.12), on a

$$g = h + 1 = n_3(k) + n_5(k) + 1.$$

Un témoin t de f est un nombre impair tel que

$$T_3^{n_3(t)}\, T_5^{n_5(t)} \mid f = \Delta \quad \text{et} \quad n_3(t) + n_5(t) = h = g - 1. \tag{4.1}$$

Il résulte de (3.10) que l'exposant dominant k de f est un témoin. Il peut y en avoir d'autres ; par exemple $f = \Delta^{85}$ a quatre témoins : $85, 77, 53, 45$ de codes respectifs $[0, 7], [2, 5], [4, 3], [6, 1]$.

Lemme 4 *Soit t un témoin de f différent de l'exposant dominant k de f. Alors t est dominé par k ; autrement dit, on a*

$$n_5(t) < n_5(k) \qquad et \qquad n_3(t) > n_3(k).$$

Démonstration : Posons $u = n_3(t)$, $v = n_5(t)$ et supposons $v \geqslant n_5(k)$. Si $v = n_5(k)$, on a $t = k$, ce qui est exclu. On a donc $v > n_5(k)$.

Par la proposition 5 (i), l'exposant dominant de $\varphi = T_5^{n_5(k)}|f$ a pour code $[n_3(k), 0]$. En posant $\psi = T_5|\varphi = T_5^{n_5(k)+1}|f$, par la proposition 5 (ii), il vient $h(\psi) \leqslant h(\varphi) - 2 = n_3(k) - 2$. En appliquant $u + v - n_5(k) - 1$ fois la relation (3.13), nous obtenons

$$\begin{aligned} h(T_3^u T_5^v|f) &= h(T_3^u T_5^{v-n_5(k)-1}|\psi) \leqslant h(\psi) - (u + (v - n_5(k) - 1)) \\ &\leqslant n_3(k) - 2 - (u + v - n_5(k) - 1) = -1. \end{aligned}$$

Par (3.12), on a $g(T_3^u T_5^v|f) \leqslant 0$ ce qui, par la proposition 7, entraîne $T_3^u T_5^v|f = 0$ et t n'est pas un témoin de f. □

[Nous ne savons pas prouver qu'un témoin de Δ^k est $\leqslant k$ (cf. ci-dessous le lemme 7).]

On note $\mathcal{T} = \mathcal{T}(f)$ l'ensemble des témoins de f.

4.2 Les témoins d'une somme

Lemme 5 *Soit $f = \sum_{s=1}^{S} f_s$ avec, pour tout s vérifiant $1 \leqslant s \leqslant S$, $f_s \in \mathcal{F}$ et $g(f_s) = g(f) = g$. Soit χ_s la fonction caractéristique de $\mathcal{T}(f_s)$, i.e.*

$$\chi_s(t) = \begin{cases} 1 & si\ t \in \mathcal{T}(f_s) \\ 0 & sinon\ . \end{cases}$$

Alors la fonction caractéristique χ de $\mathcal{T}(f)$ vérifie

$$\chi(t) = \sum_{s=1}^{S} \chi_s(t) \bmod 2. \tag{4.2}$$

Démonstration : Soit t un nombre impair de code $[u, v]$ avec $u + v = g - 1$. Que vaut $\varphi = T_3^u T_5^v | f$? Par (3.11), on a $g(\varphi) \leqslant g(f) - u - v = 1$, donc (cf. proposition 7) $\varphi = 0$ ou Δ. Plus précisément,

$$\varphi = \chi(t)\Delta.$$

En posant $\varphi_s = T_3^u T_5^v | f_s$, on a de même $\varphi_s = \chi_s(t)\Delta$. On a ainsi dans $\mathbf{F}_2[\Delta]$

$$\chi(t)\Delta = \sum_{s=1}^{S} \chi_s(t)\Delta$$

ce qui prouve (4.2). □

Exemple. Les témoins de Δ^{83} sont 83 et 75 ; ceux de Δ^{51} sont 51 et 43. Les témoins de $\Delta^{85} + \Delta^{83} + \Delta^{51}$ sont $85, 83, 77, 75, 53, 51, 45, 43$, de codes respectifs $[0, 7], [1, 6], [2, 5], [3, 4], [4, 3], [5, 2], [6, 1], [7, 0]$ c'est-à-dire tous les nombres impairs t tels que $n_3(t) + n_5(t) = 7$.

4.3 Les témoins et la base $m(a, b)$

Soit a et b deux entiers $\geqslant 0$ non tous deux nuls et la forme $m(a, b) \in \mathcal{F}$ (cf. §3.7).

Lemme 6 *Soit u et v deux entiers $\geqslant 0$. On a*

$$T_3^u\ T_5^v | m(a,b) = \begin{cases} 0 & \text{si } u > a \text{ ou } v > b \\ \Delta & \text{si } u = a \text{ et } v = b \\ m(a-u, b-v) \neq \Delta & \text{sinon .} \end{cases} \tag{4.3}$$

Démonstration : Supposons $u > a$. on a $T_3^a | m(a, b) = m(0, b)$ et, par la proposition 8 (iii), $T_3^{a+1} | m(a, b) = T_3 | m(0, b) = 0$, ce qui entraîne $T_3^u\ T_5^v | m(a, b) = 0$. On traite de même le cas $v > b$.

Reste le cas $u \leqslant a$ et $v \leqslant b$. En appliquant u fois la proposition 8 (iii) puis v fois la proposition 8 (iv), on voit que $T_3^u\ T_5^v | m(a, b) = m(a - u, b - v)$ qui, par la proposition 8 (i), vaut Δ lorsque $u = a$ et $v = b$, mais sinon, est différent de Δ par la proposition 8 (ii). □

Il résulte de (4.3) que la forme modulaire $m(a, b)$ n'a qu'un seul témoin, son exposant dominant de code $[a, b]$.

Proposition 9 *Soit $f \in \mathcal{F}$, $f \neq 0$ et $\mathcal{P}(f) = \sum_{j=1}^{J} m(a_j, b_j)$ la partie principale de son développement dans la base $m(a, b)$ (cf. (3.16)). Pour $1 \leqslant j \leqslant J$, soit t_j le nombre impair de code $[a_j, b_j]$. Alors, on a*

$$\mathcal{T}(f) = \{t_j,\ \ 1 \leqslant j \leqslant J\}.$$

Démonstration : Soit u et v deux entiers $\geqslant 0$ de somme $h(f)$. Par (4.3), les termes de la partie non principale $f - P(f)$ (cf. (3.16)) sont tous tués par $T_3^u\ T_5^v$. D'autre part, toujours par (4.3), $T_3^u\ T_5^v | \mathcal{P}(f) = \Delta$ si et seulement s'il existe j, $1 \leqslant j \leqslant J$, tel que $u = a_j$. □

4.4 Rapport entre les témoins de $T_3|f$ et ceux de f

On note ψ l'application de l'ensemble des nombres entiers impairs positifs dans lui-même qui, au nombre t de code $[u, v]$ fait correspondre le nombre t' de code $[u+1, v]$.

Soit $f \in \mathcal{F}$, $f \neq 0$, k son exposant dominant.

Proposition 10 *(i) Si $n_3(k) > 0$, alors l'application $\psi : \mathcal{T}(T_3|f) \longrightarrow \mathcal{T}(f)$ est une bijection.*

(ii) Si $n_3(k) = 0$ et si f n'a qu'un seul témoin, on a $h(T_3|f) \leqslant h(f) - 2$ et $\mathcal{T}(f) = \{k\}$.

(iii) Si $n_3(k) = 0$ et si f a plusieurs témoins, on a $h(T_3|f) = h(f) - 1$ et l'application $\psi : \mathcal{T}(T_3|f) \longrightarrow \mathcal{T}(f) - \{k\}$ est une bijection.

Démonstration : Écrivons la partie principale de f sous la forme (3.16). En désignant par t_j le nombre impair de code $[a_j, b_j]$, par la proposition 9, on a

$$\mathcal{T}(f) = \{t_j, \ \ 1 \leqslant j \leqslant J\}$$

et, par le lemme 4, $t_1 = k$ est l'exposant dominant de f.

Supposons d'abord $a_1 = n_3(k) > 0$. Par la proposition 4 (i), on a $h(T_3|f) = h(f) - 1$ tandis que, par la proposition 8 (iii), il vient

$$T_3|P(f) = \sum_{j=1}^{J} m(a_j - 1, b_j).$$

Par (3.13) et (3.17), on a

$$h(T_3|(f - P(f))) \leqslant h(f - P(f)) - 1 \leqslant h(f) - 2 = h(T_3|f) - 1. \tag{4.4}$$

Il s'ensuit que

$$P(T_3|f) = T_3|P(f) = \sum_{j=1}^{J} m(a_j - 1, b_j) \tag{4.5}$$

et, par la proposition 9, les témoins de $T_3|f$ sont les nombres impairs t'_j de code $[a_j - 1, b_j]$, ce qui prouve (i).

Supposons maintenant $a_1 = n_3(k) = 0$. Par la proposition 8 (iii), on a

$$T_3|P(f) = \sum_{j=2}^{J} m(a_j - 1, b_j). \tag{4.6}$$

Si $J = 1$, par la proposition 9, f n'a qu'un seul témoin, son exposant dominant k ; la somme dans (4.6) est vide, donc $T_3|P(f) = 0$ et, par (3.13) et (3.17), comme en (4.4), il vient

$$h(T_3|f) = h(T_3|(f - P(f)) \leqslant h(f) - 2.$$

Si $J \geqslant 2$, on a comme en (4.5),

$$P(T_3|f) = \sum_{j=2}^{J} m(a_j - 1, b_j),$$

$h(T_3|f) = h(f)-1$, et, par la proposition 9, les témoins de $T_3|f$ sont les nombres impairs t'_j de code $[a_j - 1, b_j]$ pour $2 \leqslant j \leqslant J$. On a donc $\mathcal{T}(f) = \{k\} \cup \psi(\mathcal{T}(T_3|f))$. □

[Il ne nous a pas été possible de transposer complètement la proposition 10 à l'opérateur de Hecke T_5. Nous n'avons pas vu comment déterminer si le nombre impair t de code $[h(f), 0]$ est un témoin de f.]

4.5 Calcul numérique des témoins

La proposition 10 permet de calculer, par récurrence sur les nombres impairs k, les témoins de Δ^k et, via (4.2), les témoins de toute forme $f \in \mathcal{F}$.

On calcule d'abord $T_3|\Delta^k$ par la formule de récurrence (cf. [14, §3] ou [16, §3])

$$T_3|\Delta^k = \Delta(T_3|\Delta^{k-3}) + \Delta^4(T_3|\Delta^{k-4}).$$

On détermine ensuite les témoins de $T_3|\Delta^k$ à partir de ceux de Δ^i pour $i < k$ par la formule (4.2), puis on en déduit ceux de Δ^k par la proposition 10.

4.6 Une condition pour être témoin

Proposition 11 *Soit $f \in \mathcal{F}$, $f \neq 0$ et t un témoin de f de code $[u, v]$, c'est-à-dire que l'on a*

$$T_3^u T_5^v | f = \Delta \quad et \quad h(t) = u + v = h(f) = g(f) - 1. \tag{4.7}$$

Alors, si $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_u \in \mathcal{P}_3$ et $p_{u+1} \leqslant p_{u+2} \leqslant \ldots \leqslant p_{u+v} \in \mathcal{P}_5$, on a

$$T_{p_1} T_{p_2} \ldots T_{p_{u+v}} | f = \Delta, \quad u + v = g(f) - 1. \tag{4.8}$$

Réciproquement, s'il existe $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_u \in \mathcal{P}_3$, $p_{u+1} \leqslant p_{u+2} \leqslant \ldots \leqslant p_{u+v} \in \mathcal{P}_5$ vérifiant (4.8), alors le nombre impair t de code $[u, v]$ est un témoin de f, ce qui entraîne (4.7).

Démonstration : Cela résulte du développement de T_p dans l'algèbre de Hecke engendrée par T_3 et T_5, comme exposé dans [15, §7].

Nous donnons ci-dessous une démonstration par récurrence sur le degré impair d de f basée sur les propositions 4 et 5.

Si $d \leqslant 5$, il est facile de voir que les formes d'exposant dominant $\leqslant 5$ vérifient le théorème : par exemple, pour $f = \Delta^5 + \Delta^3$, $h(f) = 1$, les témoins sont $t = 3$ (de code $[1, 0]$) et $t = 5$ (de code $[0, 1]$) et, si $p' \in \mathcal{P}_3$ et $p'' \in \mathcal{P}_5$, par la proposition 3, on a bien $T_{p'}|f = T_3|f = \Delta$ et $T_{p''}|f = T_5|f = \Delta$.

Supposons maintenant $d \geqslant 7$ et le théorème vrai jusqu'à $d-2$. Soit $t \in \mathcal{T}(f)$ de code $[u, v]$, $p_1, p_2, \ldots, p_u \in \mathcal{P}_3$ et $p_{u+1}, p_{u+2}, \ldots, p_{u+v} \in \mathcal{P}_5$.

Puisque $d \geqslant 7$, on a $h(d) \geqslant 2$ et donc $h(f) \geqslant h(d) \geqslant 2$. Par (4.7), on a $h(f) = u + v$ et l'un des nombres u ou v est non nul. Supposons $v \geqslant 1$ (si $v = 0$, on raisonnerait de même en remplaçant T_5 par T_3) et posons

$$\varphi = T_5|f.$$

Par (3.11), on a $g(\varphi) \leqslant g(f) - 1 = u + v$. Ensuite, (4.7) entraîne

$$T_3^u T_5^{v-1} | \varphi = T_3^u T_5^v | f = \Delta, \tag{4.9}$$

ce qui montre que $g(\varphi) \geqslant u + (v-1) + 1 = u + v$ et que le nombre impair t' de code $[u, v-1]$ est un témoin de φ. On a donc

$$g(\varphi) = u + v = g(f) - 1.$$

Cependant, par (3.4), le degré de φ est au plus égal à $d-2$ et on peut appliquer à φ l'hypothèse de récurrence, ce qui donne

$$T_{p_1} T_{p_2} \dots T_{p_{u+v-1}} | \varphi = \Delta. \tag{4.10}$$

On pose alors

$$\psi = T_{p_1} T_{p_2} \dots T_{p_{u+v-1}} | f. \tag{4.11}$$

En appliquant $u + v - 1$ fois l'inégalité (3.11), on obtient

$$g(\psi) \leqslant g(f) - (u + v - 1) = 2.$$

Par (4.11) et (4.10), on a

$$T_5|\psi = T_{p_1} T_{p_2} \dots T_{p_{u+v-1}} | (T_5|f) = T_{p_1} T_{p_2} \dots T_{p_{u+v-1}} | \varphi = \Delta$$

ce qui implique $\psi \neq 0$. Soit d' le degré de ψ en Δ. Par (3.9) et (3.12), il vient

$$h(d') \leqslant h(\psi) = g(\psi) - 1 \leqslant 1$$

On a donc $d' \leqslant 5$ ce qui, puisque $T_5|\psi = \Delta$, restreint, par la proposition 3, le choix de ψ à l'une des quatre formes

$$\Delta^5,\ \Delta^5 + \Delta,\ \Delta^5 + \Delta^3,\ \Delta^5 + \Delta^3 + \Delta. \tag{4.12}$$

Mais, pour chacune de ces quatre formes, toujours par la proposition 3, on a $T_{p_{u+v}}|\psi = \Delta$ ce qui implique

$$T_{p_1} T_{p_2} \dots T_{p_{u+v}} | f = T_{p_{u+v}} | (T_{p_1} T_{p_2} \dots T_{p_{u+v-1}} | f) = T_{p_{u+v}} | \psi = \Delta$$

et démontre (4.8).

La réciproque se fait de la même façon : dans le cas $v \geqslant 1$, on part de (4.8), on pose $\varphi = T_{p_{u+v}}|f$, on démontre $g(\varphi) = g(f) - 1$ et on applique à φ l'hypothèse de récurrence, ce qui donne $T_3^u T_5^{v-1} | \varphi = \Delta$. Puis l'on considère $\psi = T_3^u T_5^{v-1} | f$, on prouve $g(\psi) \leqslant 2$, ce qui implique que ψ est égal à l'une des formes (4.12), et l'on conclut comme précédemment en remarquant que pour chacune de ces quatre valeurs, on a $T_5|\psi = \Delta$. Dans le cas $v = 0$, on raisonne de même en remplaçant v par u et T_5 par T_3. □

4.7 Conjecture sur les témoins de Δ^k

Soit k un nombre impair > 0 et $k = \sum_{i=0}^{\infty} \beta_i 2^i$ son écriture en base 2. Observons que

$$\beta_1 = \begin{cases} 0 & \text{si } k \equiv 1 \pmod 4 \\ 1 & \text{si } k \equiv 3 \pmod 4. \end{cases}$$

Si $n_5(k) = 0$, par le lemme 4, on a $\mathcal{T}(\Delta^k) = \{k\}$.

Si $n_5(k) > 0$, soit I le plus grand nombre tel que $\beta_{2I} = 1$. On désigne par $u_1 < u_2 < \ldots < u_R < I$ les nombres u_r, $1 \leqslant r \leqslant R$, tels que $u_1 \geqslant 1$ et

$$\beta_{2u_r} = 1 - \beta_1 \quad \text{et} \quad \beta_{2u_r+1} = 0.$$

Conjecture 1 *Les témoins t de Δ^k sont les nombres impairs ayant pour code $[n_3(k)+a, n_5(k)-a]$ où a est de la forme*

$$a=\sum_{r=1}^{R}\varepsilon_r 2^{u_r},\quad \textit{avec}\quad \varepsilon_r=\varepsilon_r(t)\in\{0,1\}\quad \textit{et}\quad a=a(t)\leqslant n_5(k). \tag{4.13}$$

La conjecture 1 a été vérifiée pour $k<2^{22}=4194304$. Le calcul des témoins de Δ^k a été fait en utilisant la procédure décrite au §4.5.

Lemme 7 *Sous la conjecture 1, tout témoin t de Δ^k est $\leqslant k$.*

Démonstration : Soit t un témoin de Δ^k, $t\neq k$, et $r_1<r_2<\ldots<r_s$ les indices tels que $\varepsilon_{r_j}(t)=1$. On a $s\geqslant 1$ car $t\neq k$. On pose $t_0=k$, et, pour $1\leqslant j\leqslant s$, on définit le témoin t_j par

$$\begin{cases}\varepsilon_i(t_j)=\varepsilon_i(t) & \text{pour } 1\leqslant i\leqslant r_j\\ \varepsilon_i(t_j)=0 & \text{pour } r_j<i\leqslant R.\end{cases}$$

Notons que l'on a $t_s=t$. Soit j fixé, $1\leqslant j\leqslant s$. Il vient

$$a(t_j)=2^{r_1}+2^{r_2}+\ldots+2^{r_j}\leqslant 2^{r_1}+2^{r_2}+\ldots+2^{r_s}=a(t)\leqslant n_5(k)$$

et

$$n_5(t_{j-1})=n_5(t_j)+2^{r_j}\geqslant 2^{r_j}.$$

Si l'écriture de t_{j-1} en base 2 est $t_{j-1}=\sum_{i=0}^{\infty}\alpha_i 2^i$ (avec $\alpha_i\in\{0,1\}$), il existe donc $i_0\geqslant r_j+1$ tel que $\alpha_{2i_0}=1$; choisissons i_0 minimal. Alors le nombre impair t_j de code $[n_3(t_{j-1})+2^{r_j}, n_5(t_{j-1})-2^{r_j}]$ est égal à

$$t_j=t_{j-1}+2^{2r_j+1}-2^{2i_0}+\sum_{i=r_j+1}^{i_0-1}2^{2i}=t_{j-1}-\frac{2^{2i_0+1}-2^{2r_j+1}}{3}<t_{j-1}.$$

Il s'ensuit que $t_0=k>t_1>\ldots>t_s=t$. □

Supposons $k\equiv 1 \pmod 4$. Pour $1\leqslant r\leqslant R-1$, on désigne par v_r le plus petit nombre tel que $u_r<v_r\leqslant u_{r+1}$ et $\beta_{2v_r}=1$; on appelle v_R le plus petit nombre tel que $u_R<v_R\leqslant I$ et $\beta_{2v_R}=1$. La condition $a\leqslant n_5(k)$ de (4.13) est toujours vérifiée et, sous la conjecture 1, il y a 2^R témoins t de Δ^k donnés par la formule

$$t=k-\sum_{r=1}^{R}\varepsilon_r\left(2^{2v_r}-2^{2u_r+1}+\sum_{i=u_r+1}^{v_r-1}2^{2i}\right)=k-\sum_{r=1}^{R}\varepsilon_r\frac{2^{2v_r+1}-2^{2u_r+1}}{3} \tag{4.14}$$

où les nombres ε_r prennent toutes les 2^R valeurs possibles.

Lorsque $k\equiv 3 \pmod 4$, il est plus difficile d'obtenir une formule du type (4.14). Le nombre de témoins de Δ^k peut être $<2^R$ et n'est pas forcément une puissance de 2 ; par exemple, Δ^{67} a 3 témoins.

5 Estimation de $W_f(x)$

5.1 Majoration de $\omega''(n)$

Soit $f = \sum_{n\geqslant 1} c(n)\, q^n \in \mathcal{F} \subset \mathbf{F}_2[\Delta]$, $f \neq 0$, k son exposant dominant et $g = h(k)+1$ son ordre de nilpotence. On définit ω' par (2.2). Il est facile de voir (cf. [13, proposition 3.2]) que

$$c(n) = 1 \quad \Longrightarrow \quad \omega'(n) \leqslant g-1. \tag{5.1}$$

En effet, si $r = \omega'(n) \geqslant g$, n s'écrit $n = p_1 p_2 \dots p_r\, m$ avec $(m, p_1 p_2 \dots p_r) = 1$; par la définition de l'ordre de nilpotence, on a $T_{p_1} T_{p_2} \dots T_{p_r} | f = 0$ et, par la définition (3.3) des opérateurs de Hecke, cela implique $c(n) = 0$.

Nous prouvons ci-dessous un résultat un peu plus fort (cf. (2.4)), en remplaçant $\omega'(n)$ dans (5.1) par $\omega''(n)$ défini en (2.3).

Proposition 12 *On a*

$$c(n) = 1 \quad \Longrightarrow \quad \omega''(n) \leqslant g-1. \tag{5.2}$$

Démonstration : On raisonne par récurrence sur $g = h(k)+1$. Supposons d'abord $g = 1$ et $h(k) = 0$; on a $k = 1$ et, par la proposition 7, $f = \Delta$. Si $c(n) = 1$, par (1.4), n est un carré, $v_p(n)$ est pair pour tout facteur premier p de n et $\omega''(n) = 0$.

Soit maintenant $g \geqslant 2$, et supposons que, pour toute forme $f' = \sum_{n\geqslant 1} c'(n) q^n \in \mathcal{F}$ dont l'ordre de nilpotence g' vérifie $g' < g$, on ait $(c'(n) = 1) \Longrightarrow (\omega''(n) \leqslant g'-1)$ ou, ce qui est équivalent, $(\omega''(n) \geqslant g') \Longrightarrow (c'(n) = 0)$. Soit $f = \sum_{n\geqslant 1} c(n)\, q^n \in \mathcal{F}$ d'ordre de nilpotence g et N tel que

$$\omega''(N) \geqslant g \geqslant 2.$$

Nous allons montrer $c(N) = 0$. Pour cela, on écrit $N = p^{2a+1} m$, avec p premier impair, $p \nmid m$, $a \geqslant 0$ et $\omega''(m) = \omega''(N) - 1 \geqslant g-1$. Posons

$$\varphi = T_p | f = \sum_{n\geqslant 1} \gamma(n)\, q^n.$$

Par la définition (3.3) des opérateurs de Hecke, on a $c(pm) = \gamma(m)$ et, pour $b \geqslant 1$,

$$c(p^{2b+1} m) \equiv c(p^{2b-1} m) + \gamma(p^{2b} m) \pmod 2.$$

Par (3.11), on a $g(\varphi) \leqslant g-1 < g$ et on peut appliquer à φ l'hypothèse de récurrence : puisque $\omega''(p^{2b} m) = \omega''(m) \geqslant g-1 \geqslant g(\varphi)$, il vient $\gamma(p^{2b} m) = 0$ et

$$c(p^{2b+1} m) = c(p^{2b-1} m).$$

Il en résulte

$$c(N) = c(p^{2a+1} m) = c(p^{2a-1} m) = \dots = c(pm) = \gamma(m).$$

Mais, par l'hypothèse de récurrence, on a $\gamma(m) = 0$ et donc $c(N) = 0$. □

5.2 Caractérisation des N tels que $c(N) = 1$ et $\omega'(N) = g-1$

Soit $f = \sum_{n=1}^{\infty} c(n)\, q^n \in \mathcal{F}$ avec $c(n) \in \{0, 1\}$, $f \neq 0$, g son indice de nilpotence, $h = g - 1$, et $\mathcal{T}(f)$ l'ensemble des témoins de f.

Proposition 13 *Les nombres $N \geqslant 1$ tels que $c(N) = 1$ et $\omega'(N) = g - 1$ sont exactement les nombres qui s'écrivent*

$$N = p_1 p_2 \dots p_u\, p_{u+1} \dots p_{u+v}\, m^2$$

avec $p_1, p_2, \dots, p_u \in \mathcal{P}_3$, $p_{u+1}, p_{u+2}, \dots, p_{u+v} \in \mathcal{P}_5$, $p_1, p_2, \dots, p_{u+v}$ distincts, m impair, $(m, p_1 p_2 \dots p_{u+v}) = 1$ et $t \in \mathcal{T}(f)$ où t est le nombre impair de code $[u, v]$.

Démonstration : Soit N un nombre tel que $c(N) = 1$ et $\omega'(N) = g - 1 = h$. N est impair (car $f \in \mathcal{F}$) et s'écrit

$$N = p_1 p_2 \dots p_h\, M \tag{5.3}$$

avec $p_1, p_2, \dots, p_h$ distincts et premiers avec M et $\omega'(M) = 0$. De plus, par la proposition 12, $\omega''(N) \leqslant g - 1$ et, puisque par (2.4), on a $\omega'(N) \leqslant \omega''(N)$, cela entraîne $\omega''(N) = \omega'(N) = g - 1$. En conséquence, $\omega''(M) = \omega'(M) = 0$ et M est un carré, $M = m^2$. On a donc

$$N = p_1 p_2 \dots p_h\, m^2. \tag{5.4}$$

Posons

$$\Phi = T_{p_1} T_{p_2} \dots T_{p_h} | f = \sum_{n \geqslant 1} \gamma(n)\, q^n.$$

En appliquant h fois la relation (3.11), on voit que

$$g(\Phi) \leqslant g - h = 1.$$

Donc, par la proposition 7, $\Phi = 0$ ou Δ. Par la définition (3.3) de l'opérateur de Hecke, on a

$$\gamma(m^2) = c(N) = 1$$

d'où l'on déduit

$$\Phi = \Delta.$$

Supposons que l'un des nombres $p_1, p_2, \dots, p_h$ soit $\equiv \pm 1 \pmod 8$. En appliquant une fois (3.14) et $h - 1$ fois (3.11), on obtiendrait

$$g(\Phi) \leqslant g - h - 1 = 0$$

en contradiction avec $g(\Phi) = g(\Delta) = 1$. En conséquence, dans (5.4), les nombres $p_1, p_2, \dots, p_h$ sont tous $\equiv 3$ ou $5 \pmod 8$. Quitte à réordonner ces nombres, désignons par $p_1, p_2, \dots, p_u$ ceux qui sont $\equiv 3 \pmod 8$ et par $p_{u+1}, p_{u+2}, \dots, p_{u+v}$ (avec $u + v = h$) ceux qui sont $\equiv 5 \pmod 8$. On a $T_{p_1} T_{p_2} \dots T_{p_{u+v}} | f = \Delta$ et, par la proposition 11, le nombre t de code $[u, v]$ est un témoin de f.

Réciproquement, si $t \in \mathcal{T}(f)$ a pour code $[u, v]$ et si $p_1, p_2, \dots, p_{u+v}$ sont des nombres premiers distincts tels que $p_1, p_2, \dots, p_u \in \mathcal{P}_3$, $p_{u+1}, p_{u+2}, \dots, p_{u+v} \in \mathcal{P}_5$, par la proposition 11, on a

$$T_{p_1} T_{p_2} \dots T_{p_{u+v}} | f = \Delta = \sum_{n \geqslant 1} \gamma(n)\, q^n \tag{5.5}$$

(avec, par (1.4), $\gamma(n) = 1$ si n est un carré impair).

Soit m un nombre impair, $(m, p_1 p_2 \dots p_{u+v}) = 1$ et $N = p_1 p_2 \dots p_{u+v} m^2$. Par la définition (3.3) de l'opérateur de Hecke, (5.5) implique $c(N) = \gamma(m^2) = 1$. □

5.3 Les formes $f \in \mathcal{F}$

Soit $f \in \mathcal{F}$, $f \neq 0$, k son exposant dominant, g son indice de nilpotence, $h = g-1$, et $\mathcal{T}(f)$ l'ensemble des témoins de f. Écrivons $f = \sum_{n=1}^{\infty} c(n)\, q^n$ avec $c(n) \in \{0, 1\}$ et posons

$$W(x) = W_f(x) = \sum_{n \leqslant x} c(n).$$

Théorème 3 *Supposons $f \neq \Delta$. Lorsque $x \to \infty$, on a*

$$W(x) = \delta \frac{x}{\log x} (\log\log x)^{g-2} \left(1 + O\left(\frac{1}{\log\log x}\right)\right) \tag{5.6}$$

avec

$$\delta = \delta(f) = \frac{\pi^2}{8(g-2)!\, 4^{g-1}} \sum_{t \in \mathcal{T}(f)} \binom{g-1}{n_3(t)}. \tag{5.7}$$

[Lorsque le degré de f en Δ est $< 2^{22}$, la constante $\delta(f)$ peut être calculée en déterminant $\mathcal{T}(f)$ à l'aide de la conjecture 1 (cf. §4.7) et du lemme 5 (cf. §4.2).
L'obtention pour $W_f(x)$ d'un développement asymptotique plus précis que (5.6) nécessiterait une meilleure évaluation de W_1 dans (5.10). Pour cela, il faudrait caractériser pour chaque $j \leqslant g-1$ les nombres N tels que $c(N) = 1$ et $\omega'(N) = j$. C'est ce que nous avons fait pour $j = g-1$ dans la proposition 13, mais ce que nous ne savons pas faire pour toute forme $f \in \mathcal{F}$ et tout $j < g-1$.]

Démonstration : Puisque $f \neq \Delta$, on a $h = h(k) \geqslant 1$, $k > 1$ et $g \geqslant 2$. En utilisant la fonction ω' définie en (2.2), on écrit

$$W(x) = W_1 + W_2 + W_3 \tag{5.8}$$

avec

$$W_1 = \sum_{\substack{n \leqslant x \\ \omega'(n) \leqslant g-2}} c(n), \quad W_2 = \sum_{\substack{n \leqslant x \\ \omega'(n) = g-1}} c(n), \quad W_3 = \sum_{\substack{n \leqslant x \\ \omega'(n) \geqslant g}} c(n).$$

Par (5.1), si $\omega'(n) \geqslant g$, on a $c(n) = 0$. Il s'ensuit que

$$W_3 = 0. \tag{5.9}$$

Lorsque $g = 2$, par (2.9), la somme W_1 est $\leqslant \pi'_0(x) \leqslant 2.18\sqrt{x}$, tandis que, pour $g \geqslant 3$, il résulte de (2.10) que

$$W_1 \leqslant \pi'_0 + \pi'_1 + \ldots + \pi'_{g-2} = O\left(x(\log\log x)^{g-3}/\log x\right).$$

Dans les deux cas, on a

$$W_1 = O\left(\frac{x}{\log x}(\log\log x)^{g-3}\right). \tag{5.10}$$

Par la proposition 13 et (2.17), il vient

(5.11)

$$W_2 = \sum_{t\in\mathcal{T}(f)} N_1(x; n_3(t), n_5(t)) = \delta(f)\ \frac{x}{\log x}(\log\log x)^{g-2}\left(1 + O\left(\frac{1}{\log\log x}\right)\right),$$

ce qui, avec (5.8), (5.9) et (5.10) complète la preuve du théorème 3. □

5.4 Cas général

Une forme modulaire mod 2 non parabolique f s'écrit (cf. (3.2))

$$f = 1 + \sum_{s\geqslant 0} f_s^{2^s} \quad \text{avec} \quad f_s \in \mathcal{F}.$$

La forme $\varphi = f - 1$ est parabolique et l'on a, pour $x \geqslant 1$

$$W_f(x) = W_\varphi(x) + 1.$$

Pour estimer $W_f(x)$, on peut donc se restreindre au cas où f est parabolique et s'écrit (cf. (3.1))

$$f = \sum_{s\geqslant 0} f_s^{2^s} \quad \text{avec} \quad f_s \in \mathcal{F}. \tag{5.12}$$

De (3.5), on déduit

$$g(f_s^{2^s}) = g(f_s)$$

et, puisque $f_s^{2^s} \in q^{2^s}\mathbf{F}_2[q^{2^{s+1}}]$, il en résulte que

$$g(f) = \max_{s\geqslant 0} g(f_s).$$

Pour $1 \leqslant j \leqslant g$, on pose

$$S_j = S_j(f) = \{s \geqslant 0;\ \ g(f_s) = j\}. \tag{5.13}$$

Proposition 14 *Soit $f \neq 0$ une forme parabolique modulo 2 que l'on écrit sous la forme* (5.12)*, $g = g(f)$ son ordre de nilpotence et, pour $1 \leqslant j \leqslant g$, $S_j(f)$ défini par* (5.13)*.*

Si $g = 1$, on a

$$W_f(x) = \left(\sum_{s\in\mathcal{S}_1} \frac{1}{2^{s/2+1}}\right)\sqrt{x} + O(1). \tag{5.14}$$

Si $g \geqslant 2$, on a

$$W_f(x) = \delta(f)\ \frac{x}{\log x}(\log\log x)^{g-2}\left(1 + O\left(\frac{1}{\log\log x}\right)\right) \tag{5.15}$$

avec

$$\delta(f) = \sum_{s\in\mathcal{S}_g} \frac{\delta(f_s)}{2^s}. \tag{5.16}$$

Démonstration : Supposons $g = 1$; par la proposition 7, f s'écrit

$$f = \sum_{s \in \mathcal{S}_1} \Delta^{2^s}$$

et, puisque par (1.4), $W_\Delta(x) = \lfloor (\sqrt{x} - 1)/2 \rfloor$, on a

$$W_f(x) = \sum_{s \in \mathcal{S}_1} W_{\Delta^{2^s}}(x) = \sum_{s \in \mathcal{S}_1} W_\Delta\left(\frac{x}{2^s}\right) = \sum_{s \in \mathcal{S}_1} \left\lfloor \sqrt{\frac{x}{2^{s+2}}} - \frac{1}{2} \right\rfloor$$

d'où (5.14).

Supposons maintenant $g \geqslant 2$. On a

$$f = \sum_{j=1}^{g} \Phi_j \quad \text{avec} \quad \Phi_j = \sum_{s \in \mathcal{S}_j} f_s^{2^s}$$

et

$$W_f(x) = \sum_{j=1}^{g} W_{\Phi_j}(x). \tag{5.17}$$

Par (5.14), on a

$$W_{\Phi_1}(x) = O(\sqrt{x}). \tag{5.18}$$

Soit maintenant j, $2 \leqslant j \leqslant g$; par (5.6), il vient

$$\begin{aligned} W_{\Phi_j}(x) &= \sum_{s \in \mathcal{S}_j} W_{f_s}\left(\frac{x}{2^s}\right) \\ &= \sum_{s \in \mathcal{S}_j} \delta(f_s)\, \frac{x(\log\log(x/2^s))^{j-2}}{2^s \log(x/2^s)} \left(1 + O\left(\frac{1}{\log\log x}\right)\right) \\ &= \left(\sum_{s \in \mathcal{S}_j} \frac{\delta(f_s)}{2^s}\right) \frac{x}{\log x} (\log\log x)^{j-2} \left(1 + O\left(\frac{1}{\log\log x}\right)\right). \end{aligned} \tag{5.19}$$

Pour $2 \leqslant j \leqslant g - 1$, (5.19) implique

$$W_{\Phi_j} = O\left(\frac{x}{\log x} (\log\log(x)^{g-3})\right)$$

ce qui, avec (5.17), (5.18) et (5.19) (avec $j = g$) prouve (5.15). □

5.5 Minoration effective de $W_f(x)$

Théorème 4 *Soit $f = \sum c(n) q^n$ une forme modulaire de niveau 1 modulo 2, $g = g(f)$ son ordre de nilpotence. On suppose que $g \geqslant 5$, et que x est un nombre réel satisfaisant*

$$x > e^{e^{3.5(g-1)}}. \tag{5.20}$$

Alors

$$W_f(x) > 0.4\, \delta(f) \frac{x}{\log x} (\log\log x - \log\log\log x)^{g-2}$$

où $\delta(f)$ est la constante strictement positive définie par (5.7) et (5.16).

Démonstration : Supposons d'abord $f \in \mathcal{F}$. La preuve du théorème 3, et en particulier les formules (5.8) et (5.11), montrent que

$$W_f(x) \geqslant \sum_{t \in \mathcal{T}(f)} N_1(x; n_3(t), n_5(t)) \geqslant \sum_{t \in \mathcal{T}(f)} N(x; n_3(t), n_5(t)).$$

Puisque pour $t \in \mathcal{T}(f)$, on a $n_3(t) + n_5(t) = g - 1 \geqslant 4$, et puisque $x > e^{e^{3.5(g-1)}}$, le théorème 2 donne

$$W_f(x) \geqslant \frac{0.502}{(g-2)!4^{g-1}} \left(\sum_{t \in \mathcal{T}(f)} \binom{g-1}{n_3(t)} \right) \frac{x}{\log x} (\log\log x - \log\log\log x)^{g-2}.$$

Vu le définition (5.7) de $\delta(f)$, ceci entraîne que

$$W_f(x) \geqslant 0.502 \frac{8}{\pi^2} \delta(f) \frac{x}{\log x} (\log\log x - \log\log\log x)^{g-2},$$

ce qui prouve le théorème quand $f \in \mathcal{F}$. Le cas général se ramène à ce cas par la même méthode que dans §5.4 □

6 Parité de la fonction de partition $p(n)$

Théorème 5 *La quantité $A_0(x)$, définie en* (1.12)*, vérifie l'inégalité*

$$A_0(x) \geqslant 0.069 \sqrt{x} \log\log x \tag{6.1}$$

pour $x > 1$.

Démonstration : La démonstration est la même que celle de l'inégalité ci-dessus (1.13) dans [13, §5] ; simplement, on remplace la majoration de l'ordre de nilpotence $g(\Delta^k) \leqslant (k+5)/4$ (cf. [13, (3.28)]) par la valeur exacte $g(\Delta^k) = h(k) + 1$ rappelée ci-dessus en (3.12).

Soit d un nombre pair > 0. On pose

$$k = 1 + 4 + 4^2 + \ldots + 4^{d/2-1} = \frac{2^d - 1}{3}.$$

Le code de k est (cf. §3.3)

$$[0, 2^{d/2-1} - 1]$$

et donc

$$h = h(k) = 2^{d/2-1} - 1, \qquad g(\Delta^k) = 2^{d/2-1}. \tag{6.2}$$

ll résulte de (5.1) (avec $f = \Delta^k$) que l'on a en utilisant la notation (2.8)

$$W_{\Delta^k}(x) \leqslant \pi'_0(x) + \pi'_1(x) + \ldots + \pi'_h(x). \tag{6.3}$$

Soit $x \geqslant x_0 = e^{100}$, α réel, $0 < \alpha < 1$, $Q(\alpha) = 1 - \alpha + \alpha \log \alpha$,

$$Y = Y(x) = \log\log x + 1.87,$$

et

$$5 \leqslant h \leqslant 1 + \alpha Y \leqslant 1 + Y. \tag{6.4}$$

La majoration (6.5) ci-dessous, basée sur la formule (2.7), est donnée dans [13, (2.22)] :

$$\pi_0'(x) + \pi_1'(x) + \ldots + \pi_h'(x) \leqslant \frac{3.29\ x}{(1-\alpha)(\log x)^{Q(\alpha)}}. \tag{6.5}$$

On définit d pair par

$$64 \leqslant (2+\alpha Y)^2 < 2^d \leqslant 4(2+\alpha Y)^2 \leqslant 4(2+Y)^2. \tag{6.6}$$

Notons que la condition $2^d > 64$ impose $d \geqslant 8$, ce qui entraîne $h = 2^{d/2-1} - 1 \geqslant 5$ et assure la véracité de (6.4). Posons

$$\beta = \sqrt{\frac{3 \times 2^d}{2x}}.$$

Puisque $x \geqslant x_0 = e^{100}$, par (6.6), il vient

$$\beta \leqslant \sqrt{\frac{6}{x}(2+Y)^2} \leqslant \sqrt{6}\ \frac{\log\log x + 3.87}{\sqrt{x}} \leqslant \beta_0 \tag{6.7}$$

avec

$$\beta_0 = \sqrt{6}\ \frac{\log\log x_0 + 3.87}{\sqrt{x}_0} = 4.00405\ldots 10^{-21}.$$

On a également

$$\frac{k}{x} = \frac{2^d - 1}{3x} < \frac{2^d}{3x} = \frac{2}{9}\ \beta^2 \leqslant \frac{2}{9}\ \beta_0^2 \leqslant \beta_0. \tag{6.8}$$

La formule [13, (5.3)] donne la minoration

$$A_0(x) \geq \sqrt{\frac{3 \cdot 2^d}{8}}\sqrt{x}\left(\frac{1-2\beta}{1+\beta}\right)\left(\frac{2}{3} - \frac{W_{\Delta^k}(8x+k)}{x(1-2\beta)}\right). \tag{6.9}$$

Par (6.3), (6.5) et (6.8), il vient

$$W_{\Delta^k}(8x+k) \leqslant \frac{3.29\ (8x+k)}{(1-\alpha)(\log(8x))^{Q(\alpha)}} \leqslant \frac{3.29\ (8+\beta_0)x}{(1-\alpha)(1-2\beta_0)(\log(8x))^{Q(\alpha)}}. \tag{6.10}$$

Par (6.6), nous avons

$$\sqrt{2^d} > 2 + \alpha Y > \alpha Y > \alpha \log\log x$$

ce qui, avec (6.9) et (6.10) entraîne

$$A_0(x) \geq \frac{1-2\beta}{1+\beta}\ \frac{\alpha\sqrt{x}}{\sqrt{6}} \log\log x \left(1 - \frac{4.935\ (8+\beta_0)}{(1-\alpha)(1-2\beta_0)(\log(8x))^{Q(\alpha)}}\right). \tag{6.11}$$

En observant que

$$\frac{1}{\sqrt{6}}\left(\frac{1-2\beta}{1+\beta}\right) \geqslant \frac{1}{\sqrt{6}}\left(\frac{1-2\beta_0}{1+\beta_0}\right) = 0.40824829\ldots$$

et que $4.935\ (8+\beta_0)/(1-2\beta_0) \leqslant 39.5$, (6.11) implique

$$A_0(x) \geqslant 0.408\ \alpha\ \sqrt{x}\ \log\log x \left(1 - \frac{39.5}{(1-\alpha)(\log(8x))^{Q(\alpha)}}\right). \tag{6.12}$$

Choisissons $x_1 = \exp(9.7\times 10^6)$ et $\alpha = 0.335$. Pour $x \geqslant x_1$, on a $2+\alpha\ Y \geqslant 8.015$, la condition (6.6) est remplie, l'inégalité (6.12) donne

$$\frac{A_0(x)}{\sqrt{x}\ \log\log x} \geqslant 0.408\ \alpha \left(1 - \frac{39.5}{(1-\alpha)(\log(8x_1))^{Q(\alpha)}}\right) \geqslant 0.070155$$

tandis que, pour $3 \leqslant x < x_1$, par (1.13), on a

$$\frac{A_0(x)}{\sqrt{x}\ \log\log x} \geqslant \frac{0.28}{\sqrt{\log\log x}} \geqslant \frac{0.28}{\sqrt{\log\log x_1}} \geqslant 0.069809,$$

ce qui prouve (6.1) pour $x \geqslant 3$. Or on a $p(1) = 1$ et $p(2) = 2$, donc pour $1 < x < 2$, $A_0(x) = 0$ et, pour $2 \leqslant x < 3$, $A_0(x) = 1$, ce qui permet de vérifier la validité de (6.1) pour $1 < x < 3$. □

Lorsque $x \to \infty$, $\beta \to 0$ et (6.11) implique $A_0(x) \gtrsim (\alpha/\sqrt{6})\sqrt{x}\log\log x$, ce qui, en faisant tendre α vers 1, entraîne

$$A_0(x) \gtrsim \frac{1}{\sqrt{6}}\ \sqrt{x}\ \log\log x.$$

Théorème 6 *Pour $x \geqslant 2$ on a*

$$A_1(x) > 0.037 \frac{\sqrt{x}}{\log x} \log(x)^{\frac{1}{8}}.$$

Démonstration : Soit $d \geqslant 2$ un entier pair, si bien que $k := \frac{2^d-1}{3}$ est un entier impair. D'après [12], page 481, on a

$$A_1(x) \geqslant \frac{W_{\Delta^k}(8x+k)}{\sqrt{\frac{8x}{9k+3}}\left(1+\sqrt{\frac{9k+3}{2x}}\right)}. \tag{6.13}$$

Notons $g = g_d = g(k)$ l'ordre de nilpotence de Δ^k et $h = h_d = g_d - 1$. D'après (6.2), on a $h_d = 2^{d/2-1} - 1 = \sqrt{3k+1} - 1$, et donc $h_{d+2} = 2h_d + 1$. On peut donc choisir l'entier pair d de telle façon que

$$\frac{1}{8}\log\log 8x < h_d < \frac{1}{4}\log\log 8x + 1. \tag{6.14}$$

Supposons pour l'instant que x est très grand, à savoir :

$$x > \frac{1}{8} e^{e^{24}} \tag{6.15}$$

Cette hypothèse entraîne que $\frac{1}{8}\log\log 8x > 3$, et donc que l'entier $h = h_d$ est $\geqslant 4$. Nous verrons comment nous passer de cette hypothèse à la fin de la preuve.

Sous ces hypothèses, le dénominateur de (6.13) satisfait, puisque $\sqrt{9k+3} = \sqrt{3}(h+1) < \log\log 8x$:

$$\sqrt{\frac{8x}{9k+3}}\left(1+\sqrt{\frac{9k+3}{2x}}\right) < \sqrt{\frac{x}{k}}\sqrt{8/9}(1+\log\log 8x/\sqrt{2x}) < \sqrt{\frac{x}{k}},$$

et (6.13) entraîne donc

$$A_1(x) \geqslant \frac{W_{\Delta^k}(8x+k)}{\sqrt{x/k}}.$$

En notant que $\sqrt{k} > h/\sqrt{3}$ on en déduit :

$$A_1(x) \geqslant \frac{hW_{\Delta^k}(8x)}{\sqrt{3x}}. \tag{6.16}$$

Par (6.14), la condition (5.20) du théorème 4 appliquée à Δ^k et à $8x$ est satisfaite, et l'on a vu que $h \geqslant 4$; la conclusion de ce théorème s'applique donc, et en notant que

$$\delta(\Delta^k) \geqslant \frac{\pi^2}{8(h-1)!4^h}, \tag{6.17}$$

donne la minoration

$$W_{\Delta^k}(8x) > 0.4\frac{\pi^2}{(h-1)!4^h}\frac{x}{\log 8x}(\log\log 8x - \log\log\log 8x)^{h-1}. \tag{6.18}$$

En introduisant cette minoration dans (6.16), on obtient

$$A_1(x) > \frac{0.4}{4\sqrt{3}}\frac{\pi^2 h}{4^{h-1}(h-1)!}\frac{\sqrt{x}}{\log 8x}(\log\log 8x - \log\log\log 8x)^{h-1},$$

et donc, en utilisant que $\log 8x/\log x < 1.001$ sur le domaine considéré,

$$A_1(x) > 0.56\frac{h}{4^{h-1}(h-1)!}\frac{\sqrt{x}}{\log x}(\log\log 8x - \log\log\log 8x)^{h-1} \tag{6.19}$$

Puisque d'après (6.14), $\log\log 8x > 4(h-1)$, et la fonction $\log\log 8x - \log\log\log 8x$ est croissante, on a

$$\begin{aligned}(\log\log 8x - \log\log\log 8x)^{h-1} &> (4(h-1) - \log(4(h-1)))^{h-1} \\ &= 4^{h-1}(h-1)^{h-1}\left(1-\frac{\log(4(h-1))}{4(h-1)}\right)^{h-1}.\end{aligned}$$

Puisque $h \geqslant 4$, on a $\frac{\log(4(h-1))}{4(h-1)} \leqslant \log(12)/12 < 0.21$, si bien que par (2.39), on a

$$\begin{aligned}\log\left(\left(1-\frac{\log(4(h-1))}{4(h-1)}\right)^{h-1}\right) &> -\frac{\log(4(h-1))}{4} - \frac{\log^2(4(h-1))}{16(h-1)} \\ &> -\frac{\log(4(h-1))}{2} \text{ puisque } h \geqslant 4.\end{aligned}$$

Donc $\left(1-\frac{\log(4(h-1))}{4(h-1)}\right)^{h-1} > 1/\sqrt{4(h-1)}$ et

$$(\log\log 8x - \log\log\log 8x)^{h-1} > \frac{4^{h-1}(h-1)^{h-1}}{2\sqrt{h-1}}.$$

En incorporant cette minoration dans (6.19), on trouve

$$A_1(x) > 0.28\frac{\sqrt{h-1}(h-1)^{h-1}}{(h-1)!}\frac{\sqrt{x}}{\log x}$$

En appliquant la majoration de Stirling $(h-1)! \leqslant e\sqrt{h-1}\left(\frac{h-1}{e}\right)^{h-1}$ pour $h \geqslant 2$, on a

$$A_1(x) > 0.28e^{h-2}\frac{\sqrt{x}}{\log x}. \tag{6.20}$$

Comme par (6.14), $e^{h-2} = \frac{1}{e^2}e^h > \frac{(\log x)^{1/8}}{e^2}$ on obtient finalement

$$A_1(x) > \frac{0.28}{e^2}\frac{\sqrt{x}}{\log x}\log(x)^{\frac{1}{8}}$$

et le théorème est prouvé sous l'hypothèse que $x > \frac{1}{8}e^{e^{24}}$. Si $x \leqslant \frac{1}{8}e^{e^{24}}$ mais $x \geqslant 7$, on a $A_1(x) > 4.57\frac{\sqrt{x}}{\log x}$ d'après un théorème de Nicolas (cf. [12]) rappelé ici en (1.14), donc

$$A_1(x) > 4.57\frac{\sqrt{x}}{\log(x)}\frac{\log(x)^{1/8}}{\left(\log\left(\frac{1}{8}e^{e^{24}}\right)\right)^{1/8}} > 4.57\frac{\sqrt{x}}{\log(x)}\log(x)^{1/8}\frac{1}{e^3}$$

ce qui montre également la formule voulue dans ce cas puisque $4.57/e^3 > 0.037$. Enfin, on vérifie cette formule à la main si $2 \leqslant x \leqslant 7$. □

Théorème 7 *Si la conjecture 1 est vraie, on a pour tout $x > 2$:*

$$A_1(x) > 0.018\frac{\sqrt{x}}{(\log x)^{7/8-\log(2)/8}}.$$

Démonstration : La preuve suit de près celle du théorème précédent, dont on reprend les notations.

Si $d \geqslant 2$ est un entier pair, $k = \frac{2^d-1}{3} = \sum \beta_i 2^i$, avec $\beta_i \in \{0,1\}$, on a $\beta_i = 1$ si i est pair, $i \leqslant d-2$, et $\beta_i = 0$ dans les autres cas. On a donc $n_3(k) = 0$, $n_5(k) = h = 2^{d/2-1} - 1$, et les nombres $u_1, \ldots, u_R$ définis au §4.7 sont tous les entiers de 1 à $d/2-2$. D'après la conjecture 1, tous les entiers de code $[u,v]$ avec $u+v=h$ et u pair sont donc témoins de Δ^k. D'après la formule (5.7), on a

$$\delta(\Delta^k) = \frac{\pi^2}{8(h-1)!4^h}\sum_{u\leqslant h, u \text{ pair}}\binom{h}{u} = \frac{\pi^2}{8(h-1)!4^h}2^{h-1}.$$

En remplaçant dans la preuve du théorème précédent la minoration (6.17) par cette égalité, on gagne un facteur 2^{h-1}, si bien qu'on obtient à la fin, au lieu de (6.20) :

$$A_1(x) > 0.28e^{h-2}2^{h-1}\frac{\sqrt{x}}{\log x}. \tag{6.21}$$

d'où

$$A_1(x) > \frac{0.28}{2e^2} e^{h(1+\log 2)} \frac{\sqrt{x}}{\log x}.$$

et donc

$$A_1(x) > \frac{0.28}{2e^2} \frac{\sqrt{x}}{\log x} \log(x)^{\frac{1+\log(2)}{8}}$$

sous l'hypothèse (6.15), i.e. $> \frac{1}{8} e^{e^{24}}$. Pour $7 < x \leqslant \frac{1}{8} e^{e^{24}}$, on a

$$A_1(x) > 4.57 \frac{\sqrt{x}}{\log(x)} \frac{\log(x)^{\frac{1+\log(2)}{8}}}{\left(\log\left(\frac{1}{8} e^{e^{24}}\right)\right)^{\frac{1+\log 2}{8}}} > 4.57 \frac{\sqrt{x}}{\log(x)} \log(x)^{\frac{1+\log 2}{8}} \frac{1}{e^{3+3\log 2}}$$

ce qui implique la formule voulue puisque $\frac{4.57}{e^{3+3\log 2}} \simeq 0.028 > 0.018$, et on vérifie cette formule à la main pour pour $2 \leqslant x < 7$. □

Références

[1] G. E. Andrews, B. C. Berndt and S. A. Ramanujan. Ramanujan's lost Notebook, Part III, Springer-Verlag, 2012.

[2] F. Ben Saïd and J.-L. Nicolas, Sur une application de la formule de Selberg-Delange, Colloquium Mathematicum, 98, 2003, 223-247.

[3] B. C. Berndt. Number Theory in the Spirit of Ramanujan, Student Mathematical Library, vol. 34, Amer. Math. Soc., 2006.

[4] H. Delange. Sur des formules de Atle Selberg, *Acta Arithmetica*, 19, 1971, 105–146.

[5] P. Dusart. Estimates of $\theta(x; k, l)$ for large values of x, *Math. Comp.* 71, 2002, no. 239, 1137-1168.

[6] M. Gerbelli-Gauthier. Modular forms and Galois representations mod p, and the nilpotent action of Hecke operators mod 2, en préparation.

[7] G.H. Hardy and S. Ramanujan. The normal number of prime factors of a munber n, *Quarterly J. of Math.*, 48, 1917, 76–92 and Collected Papers of S. Ramanujan, 262–275.

[8] G.H. Hardy and E.M. Wright. An introduction to the theory of numbers, 4th edition, Oxford at the Clarendon Press, 1964.

[9] E. Landau. Handbuch der Lehre von der Verteilung der Primzahlen, I, 2nd ed, Chelsea, New-York, 1953.

[10] A. Languasco et A. Zaccagnini. Computing the Mertens and Meissel-Mertens constants for Sums over Arithmetic Progressions, *Experimental Mathematics* 19 :3, 2009, 279–284.

[11] P. A. MacMahon. Note on the parity of the number which enumerates the partitions of a number, *Proc. Cambridge Philos. Soc.*, 20, 1920–21, 281–283. Percy Alexander MacMahon Collected Papers, vol. 1, 1087–1089.

[12] J.-L. Nicolas. Valeurs impaires de la fonction de partition $p(n)$, *Int. J. Number Theory*, 2, 2006, no. 4, 469–487.

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

[14] J-L. Nicolas et J-P. Serre. Formes modulaires modulo 2 : l'ordre de nilpotence des opérateurs de Hecke, *C.R. Acad. Sci. Paris, Ser. I*, 350 (2012), 343–348. http://dx.doi.org/10.1016/j.crma.2012.03.019. http://arxiv.org/abs/1204.1036.

[15] J-L. Nicolas et J-P. Serre. Formes modulaires modulo 2 : structure de l'algèbre de Hecke, *C.R. Acad. Sci. Paris, Ser. I*, 350 (2012), 449–454. http://dx.doi.org/10.1016/j.crma.2012.03.013. http://arxiv.org/abs/1204.1039.

[16] J-L. Nicolas et J-P. Serre. L'ordre de nilpotence des opérateurs de Hecke modulo 2, en préparation.

[17] K. Ono. The Web of Modularity : Arithmetic of the Coefficients of Modular Forms and q-series, *Amer. Math. Soc.*, CBMS n° 102, 2004.

[18] T.R. Parkin and D. Shanks. On the Distribution of Parity in the Partition Function, *Math. Comp.*, 21, 1967, 466–480.

[19] S. Ramanujan, Some Properties of $p(n)$, the Number of Partitions of n, Proc. of the Cambridge Philosophical Society, XIX, 1919, 207–210 ; and "Collected papers", Cambridge at the University Press, 1927, 210–213.

[20] S. Ramanujan. *The Lost Notebook and Other Unpublished Papers*, Narosa Publishing House and Springer Verlag, 1988.

[21] O. Ramaré et R. Rumely. Primes in arithmetic progressions, *Math. Comp.*, 65, Number 213, 1996, 397–425.

[22] J.-P. Serre. Divisibilité de certaines fonctions arithmétiques, *L'Enseignement Math.* 22, 1976, 227–260 ou *Séminaire Delange–Pisot–Poitou (Théorie des nombres)*, 16ème année, 1974/75, n°20, 28 p.

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

[24] H. P. F. Swinnerton-Dyer. On ℓ-representations and congruences for coefficients of modular forms, *Springer Lecture Notes* 350, 1973, 1–55.

[25] G. Tenenbaum. Introduction à la théorie analytique et probabiliste des nombres, S.M.F., Paris, 1995. Introduction to analytic and probabilistic number theory, Cambridge studies in advanced mathematics, n°46, Cambridge University Press, 1995.

[26] http://math.univ-lyon1.fr/∼nicolas/polHecke.html

Joël BELLAÏCHE
Brandeis University, Department of Mathemetics,
415 South Street,
Waltham, MA 02453, États-Unis.

jbellaic@brandeis.edu
http://people.brandeis.edu/∼jbellaic

Jean-Louis NICOLAS
Université de Lyon, CNRS, Université Lyon 1,
Institut Camille Jordan, Mathématiques,
43 Bd. du 11 Novembre 1918,
F-69622 Villeurbanne Cedex, France.

jlnicola@in2p3.fr
http://math.univ-lyon1.fr/∼nicolas/