International Journal of Number Theory
Vol. 2, No. 4 (2006) 469–487

World Scientific
www.worldscientific.com

VALEURS IMPAIRES DE LA FONCTION DE PARTITION $p(n)$

JEAN-LOUIS NICOLAS

Institut Camille Jordan, Bât. Doyen Jean Braconnier
Université Claude Bernard (Lyon 1), 21 Avenue Claude Bernard
F-69622 Villeurbanne Cedex, France
jlnicola@in2p3.fr

Received 30 November 2005
Accepted 3 February 2006

Let $p(n)$ denote the number of partitions of n, and for $i = 0$ (resp. 1), $A_i(x)$ denote the number of $n \leq x$ such that $p(n)$ is even (resp. odd). In this paper, it is proved that for some constant $K > 0$, $A_1(x) \gg \frac{x(\log\log x)^K}{\log x}$ holds for x large enough. This estimation slightly improves a preceding result of S. Ahlgren who obtained the above lower bound for $K = 0$. Let $\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24}$ and $\Delta^k(q) = \sum_{n=k}^{\infty}\tau_k(n)q^n$; the main tool is a result of J.-P. Serre about the distribution of odd values of $\tau_k(n)$. Effective lower bounds for $A_0(x)$ and $A_1(x)$ are also given.

Keywords: Partition function; parity problems; modular forms modulo 2.

Mathematics Subject Classification 2000: 11P83, 11F33

1. Introduction

Soit $p(n)$ le nombre de partitions de n, c'est-à-dire le nombre de façons d'écrire $n = n_1 + n_2 + \cdots + n_r$ avec $n_1 \geq n_2 \geq \cdots \geq n_r \geq 1$. Dans l'article [23], MacMahon rapporte que, quelques mois avant son décès, S. Ramanujan lui avait écrit pour lui demander s'il pouvait déterminer la parité de $p(n)$.

En fait, la fameuse formule de G. H. Hardy et S. Ramanujan, précisée par H. Rademacher (cf. [18,33]) s'écrit

$$p(n) = \frac{1}{\pi\sqrt{2}}\sum_{k=1}^{\infty} a_k(n)\sqrt{k}\frac{d}{dn}\left(\frac{\sinh\left(\frac{C\sqrt{n-1/24}}{k}\right)}{\sqrt{n-1/24}}\right) \tag{1.1}$$

où $C = \pi\sqrt{\frac{2}{3}} = 2.565\ldots$ et où les coefficients $a_k(n)$ sont un peu plus compliqués. La série (1.1) est assez rapidement convergente: pour $n \geq 576$, il faut au plus $\frac{2\sqrt{n}}{3}$ termes pour calculer sa somme avec une erreur inférieure à $1/2$, ce qui suffit pour obtenir la valeur exacte du nombre entier $p(n)$ (cf. [33, Chap. 14]). Par la connaissance de la parité de $p(n)$, S. Ramanujan espérait raccourcir encore ce calcul en remplaçant $1/2$ par 1.

Malheureusement, la parité de $p(n)$ se révèle être un problème très difficile. Notons

$$A_i(x) = \text{Card}\{n \le x, p(n) \equiv i \pmod 2\}, \quad i = 0, 1. \tag{1.2}$$

Dans [32], en 1967, T. R. Parkin et D. Shanks calculent $p(n) \pmod 2$ pour $n \le 2 \cdot 10^6$, montrent que, pour $10^3 \le x \le 2 \cdot 10^6$,

$$\psi_1(x) \stackrel{def}{=} \frac{|A_1(x) - A_0(x)|}{\sqrt{x}} \le 2.882 \tag{1.3}$$

et conjecturent que $\psi_1(x) = \mathcal{O}(x^\varepsilon)$ pour tout $\varepsilon > 0$. Mais, les résultats théoriques restent très loin de cette conjecture.

Pour répondre à S. Ramanujan, MacMahon (cf. [23]) donna un algorithme de calcul de la parité de $p(n)$ et calcula que $p(1000)$ est impair.

En 1959, O. Kolberg (cf. [20]) démontra que $A_i(x)$ tend vers l'infini avec x pour $i = 0$ et $i = 1$.

En 1983, L. Mirsky (cf. [25]) prouva l'inégalité $A_i(x) \ge \frac{\log\log x}{2\log 2}$ pour $i = 0$ et $i = 1$.

Avec A. Sárközy, en 1995 (cf. [27]), nous avons montré $A_i(x) \gg (\log x)^{0.58}$ pour $i = 0$ et $i = 1$.

Grâce à I. Ruzsa, en 1998 (cf. [26]), nous avons obtenu les minorations

$$A_0(x) \gg \sqrt{x} \quad \text{et} \quad A_1(x) \gg \sqrt{x}\exp\left(\frac{-c\log x}{\log\log x}\right) \tag{1.4}$$

où c est une constante supérieure à $\log 2$.

Soit a et b deux entiers positifs. Pour $i = 0$ et $i = 1$, posons

$$A_i(a, b; x) = \ \text{Card}\{n \le x,\ n \equiv b \pmod a),\ p(n) \equiv i \pmod 2)\}. \tag{1.5}$$

Dans [39], M. Subbarao a conjecturé que, pour tout entier a positif et pour tout b, $A_0(a, b; x)$ et $A_1(a, b; x)$ tendent vers l'infini. En utilisant les résultats de J.-P. Serre sur les propriétés arithmétiques des coefficients de formes modulaires (cf. [36,37,31]), K. Ono dans [30] a presque démontré cette conjecture en prouvant que $A_0(a, b; x)$ tend vers l'infini et que, ou bien $A_1(a, b; x) = 0$ pour tout x ou bien $A_1(a, b; x)$ tend vers l'infini. Le comportement de $A_1(a, b; x)$ a été précisé dans [9] lorsque le module a de la progression arithmétique est une puissance de 2.

Dans [1], S. Ahlgren a montré que $A_0(a, b; x) \gg \sqrt{x}$ et que, si $A_1(a, b; x)$ n'était pas nul pour tout x, $A_1(a, b; x) \gg \frac{\sqrt{x}}{\log x}$, ce qui implique

$$A_1(x) \gg \frac{\sqrt{x}}{\log x}. \tag{1.6}$$

En appendice de l'article [26], J.-P. Serre démontre

$$\lim_{x\to\infty} \frac{A_0(a, b; x)}{\sqrt{x}} = +\infty. \tag{1.7}$$

Dans cet article nous améliorons légèrement la minoration (1.6) en prouvant:

Théorèm 1. *Soit $A_1(x)$ défini par (1.2). Il existe une constante K strictement positive telle que*

$$A_1(x) \gg \frac{\sqrt{x}(\log\log x)^K}{\log x}. \tag{1.8}$$

On peut prendre dans (1.8) la valeur

$$\begin{aligned} K &= \pi(4 \cdot 10^{12}) - \pi(2 \cdot 10^{12}) - 1 \\ &= 142966208126 - 73301896139 - 1 = 69664311986 \end{aligned} \tag{1.9}$$

où $\pi(x) = \sum_{p \le x} 1$ désigne la fonction de comptage des nombres premiers.

Pour a et b quelconques, les minorations de $A_i(a, b; x)$ obtenues à l'aide des formes modulaires ne sont pas, pour le moment, effectives alors que les minorations (1.4) le sont. Nous prouverons

Théorèm 2. *On a les minorations effectives suivantes:*

(i) $$x \ge 7 \quad \Rightarrow \quad A_1(x) \ge 4.57\, \frac{\sqrt{x}}{\log x}$$

et

(ii) $$x \ge 10 \quad \Rightarrow \quad A_0(x) \ge 1.05\, \sqrt{x}.$$

Au prix de calculs un peu plus longs, on pourrait augmenter les constantes 4.57 de (i) et 1.05 de (ii) et les rapprocher respectivement de $\frac{\pi^2}{4}\sqrt{6} = 6.04\ldots$ et $\frac{2\sqrt{6}}{3} = 1.63\ldots$ qui sont les limites de la méthode.

La démonstration des Théorèmes 1 et 2 reprend la Démonstration de (1.7) dans le cas le plus simple $a = 1$ et $b = 0$. La forme modulaire qui intervient est une puissance de la fonction Δ (définie ci-dessous en (3.1)) et l'on utilise les résultats connus sur la distribution des coefficients du développement de Fourier de Δ^k modulo 2, rappelés dans le théorème 3 ci-dessous. Enfin, on emploie l'argument combinatoire (cf. Lemmes 1 et 2) qu'un produit de deux séries formelles lacunaires ne peut pas contenir trop de termes non nuls. L'exposant $k = 5$ donne des résultats effectifs sur le coefficient de Δ^5 modulo 2 (cf. Sec. 4) qui conduisent au Théorème 2.

Curieusement, la démonstration fait intervenir la décomposition en facteurs premiers de $2^n - 1$ et les nombres de Wieferich (cf. Sec. 7).

Soit $\mathcal{B}$ un ensemble de nombres entiers naturels non nuls. On appelle $p(\mathcal{B}, n)$ le nombre de partitions de n dont les parts sont dans $\mathcal{B}$. La parité de $p(\mathcal{B}, n)$ a été considérée dans quelques rares cas particuliers. La parité de $p(\{1, 2, \ldots, k\}, n)$, le nombre de partitions de n en au plus k parts, est étudiée dans [15]. Par ailleurs, on peut construire des ensembles $\mathcal{B}$ tels que, pour n assez grand, $p(\mathcal{B}, n)$ soit toujours pair (ou ait une parité donnée) cf. [2–6, 26, 28, 29, 21, 22]. Enfin, dans [7, 8], on donne une minoration de $A_i(\mathcal{B}, x) = \text{Card}\{n \le x, p(\mathcal{B}, n) \equiv i \pmod 2\}$ pour $i = 0$ et $i = 1$

pour certains ensembles $\mathcal{B}$ particuliers, par exemple, lorsque $\mathcal{B}$ contient tous les nombres impairs.

Lors des Journées Arithmétiques de Limoges en 1996, J.-P. Serre m'avait demandé si l'on pouvait rendre effectif son résultat (1.7). Cet article est une réponse très partielle à sa question. J'ai plaisir à le remercier pour les discussions et les échanges de lettres que nous avons eus. Je remercie K. Ono pour diverses informations, A. Schinzel qui m'a indiqué la proposition 5 ci-dessous, O. Ramaré qui n'hésite jamais à faire partager sa grande connaissance sur les nombres premiers dans une progression arithmétique et M. Deléglise pour les calculs sur la fonction π. Enfin, je remercie l'arbitre anonyme pour sa lecture approfondie du manuscrit.

2. Séries Formelles

Soit $\mathcal{K}$ un corps et $F(q)=\sum_{n=0}^{\infty} F_n q^n \in \mathcal{K}[[q]]$ une série formelle à coefficients dans $\mathcal{K}$. On définit

$$\mathcal{P}(F,x)=\mathrm{Card}\{n, 0\le n\le x, F_n\ne 0\}. \tag{2.1}$$

Lemme 1. *Soit F,G,H trois séries formelles à coefficients dans $\mathcal{K}$, avec $F=GH$. On a pour tout $x\ge 0$:*

$$\mathcal{P}(F,x)\le \mathcal{P}(G,x)\mathcal{P}(H,x).$$

Démonstration. Ecrivons $G(q)=\sum_{i=0}^{\infty} G_i q^i$ et $H(q)=\sum_{j=0}^{\infty} H_j q^j$. La relation $F=GH$ se traduit par $F_n=\sum_{i+j=n} G_iH_j$; si le coefficient F_n est différent de 0, il existe donc i et j avec $i+j=n$ et $G_iH_j\ne 0$. Par conséquent

$$\mathcal{P}(F,x)\le \sum_{\substack{i+j\le x\\ G_iH_j\ne 0}} 1 \le \left(\sum_{\substack{i\le x\\ G_i\ne 0}} 1\right)\left(\sum_{\substack{j\le x\\ H_j\ne 0}} 1\right)=\mathcal{P}(G,x)\mathcal{P}(H,x). \qquad \square$$

On suppose maintenant que $F(q)=\sum_{n=0}^{\infty} F_n q^n\in\mathbb{Z}[[q]]$; on pose pour $i=0,1$:

$$\mathcal{P}_i(F,x)=\mathrm{Card}\{n, 0\le n\le x, F_n\equiv i \pmod 2\}. \tag{2.2}$$

Il résulte de cette définition que

$$\mathcal{P}_0(F(q),x)=\mathcal{P}_1\left(\frac{1}{1-q}+F(q),x\right) \tag{2.3}$$

et que, puisque $F^2(q)\equiv \sum_{n=0}^{\infty} F_n q^{2n} \pmod 2$,

$$\mathcal{P}_1(F,x)=\mathcal{P}_1(F^2,2x). \tag{2.4}$$

Lemme 2. *Soit F,G,H trois séries formelles à coefficients dans $\mathbb{Z}$ et $F=GH$. On a pour tout $x\ge 0$:*

$$\mathcal{P}_1(F,x)\le \mathcal{P}_1(G,x)\mathcal{P}_1(H,x). \tag{2.5}$$

Démonstration. Soit Φ le morphisme canonique de $\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}$. On pose $\overline{F}(q)=\sum_{n=0}^{\infty}\Phi(F_n)q^n\in\mathbb{Z}/2\mathbb{Z}[[q]]$; si l'on définit similairement $\overline{G}$ et $\overline{H}$, la relation $F=GH$ implique $\overline{F}=\overline{G}\,\overline{H}$. Par (2.1), (2.2) et le lemme 1, il vient:

$$\mathcal{P}_1(F,x)=\mathcal{P}(\overline{F},x)\le\mathcal{P}(\overline{G},x)\mathcal{P}(\overline{H},x)=\mathcal{P}_1(G,x)\mathcal{P}_1(H,x)$$

ce qui établit (2.5). $\square$

D'autre part, $\mathcal{P}_1(F,x)$ est le poids de Hamming (cf. [24], ch. 1, Sec. 3) du vecteur $(\Phi(F_0),\Phi(F_1),\ldots,\Phi(F_{\lfloor x\rfloor}))$, et il est facile de voir que, si pour $i=1$ et $i=2$, $F^{(i)}(q)\in\mathbb{Z}/2\mathbb{Z}[[q]]$, on a

$$\mathcal{P}_1(F^{(1)}+F^{(2)},x)\ge\mathcal{P}_1(F^{(1)},x)-\mathcal{P}_1(F^{(2)},x). \tag{2.6}$$

On définit la congruence entre deux séries formelles à coefficients entiers $G(q)=\sum_{n=0}^{\infty}G_nq^n$ et $H(q)=\sum_{n=0}^{\infty}H_nq^n$ par

$$(G\equiv H \pmod 2)\Leftrightarrow(\forall n\ge 0, G_n\equiv H_n \pmod 2). \tag{2.7}$$

On pose $f(q)=\prod_{n=1}^{\infty}(1-q^n)$. L'identité d'Euler (cf. [19, Théoréme 353]) s'écrit

$$f(q)=\prod_{n=1}^{\infty}(1-q^n)=1+\sum_{n=1}^{\infty}(-1)^n\left(q^{\frac{n(3n-1)}{2}}+q^{\frac{n(3n+1)}{2}}\right). \tag{2.8}$$

On pose $u_0=1$ et, pour $i\ge 1$,

$$u_{2i-1}=\frac{i(3i-1)}{2} \quad\text{et}\quad u_{2i}=\frac{i(3i+1)}{2}. \tag{2.9}$$

Les valeurs de u_j sont les nombres pentagonaux:

$j=$	0	1	2	3	4	5	6	7	8	9	10
$u_j=$	0	1	2	5	7	12	15	22	26	35	40

et (2.8) entraîne

$$f(q)\equiv\sum_{j=0}^{\infty}q^{u_j} \pmod 2. \tag{2.10}$$

Lemme 3. *Soit x un nombre réel positif et d un entier naturel. Avec les notations (2.2) et (2.8), on a*

$$\sqrt{\frac{8x}{3\cdot 2^d}}-3\le\mathcal{P}_1\left(f^{2^d},x\right)\le\sqrt{\frac{8x}{3\cdot 2^d}}+2 \tag{2.11}$$

et si $x\ge 2^d$,

$$\frac{2x}{3}\left(1-\sqrt{\frac{6\cdot 2^d}{x}}\right)\le\mathcal{P}_1\left(\frac{f(q)^{2^d}}{1-q},x\right)\le\frac{2x}{3}\left(1+\sqrt{\frac{6\cdot 2^d}{x}}\right)^2. \tag{2.12}$$

Démonstration. Supposons d'abord $d = 0$. On définit $i \geq 0$ en fonction de x par

$$\frac{3i^2}{2} \leq u_{2i} = \frac{i(3i+1)}{2} \leq x < u_{2i+2} = \frac{(i+1)(3i+4)}{2} \leq \frac{3(i+2)^2}{2}. \tag{2.13}$$

Compte tenu de (2.9) et de (2.10), on a

$$\sqrt{\frac{8x}{3}} - 3 \leq 1 + 2i \leq \mathcal{P}_1(f,x) \leq 1 + (2i+1) \leq \sqrt{\frac{8x}{3}} + 2,$$

ce qui prouve (2.11) lorsque $d = 0$.

Supposons maintenant $d > 0$. On a

$$f^{2^d}(q) \equiv \sum_{j=0}^{\infty} q^{2^d u_j} \pmod 2 \tag{2.14}$$

et

$$\mathcal{P}_1(f^{2^d}, x) = \mathrm{Card}\{j,\ 0 \leq j,\ 2^d u_j \leq x\} = \mathcal{P}_1(f, x/2^d),$$

ce qui complète la preuve de (2.11) pour tout d.

Soit $v_0 = 0 < v_1 < v_2 < \cdots$ une suite strictement croissante d'entiers et $F(q) = \sum_{i=0}^{\infty} q^{v_i}$. On a alors

$$\frac{F(q)}{1-q} \equiv 1 + q + \cdots + q^{v_1 - 1} + q^{v_2} + q^{v_2+1} + \cdots + q^{v_3-1} + q^{v_4} + \cdots \pmod 2.$$

On déduit ainsi de (2.14) que les coefficients impairs dans le développement de $\frac{f^{2^d}(q)}{1-q}$ sont ceux de q^n avec $2^d u_{2i} \leq n \leq 2^d u_{2i+1} - 1$; ceci implique que, pour $i \geq 0$,

$$\begin{aligned}\mathcal{P}_1\left(\frac{f^{2^d}(q)}{1-q}, 2^d u_{2i+1} - 1\right) &= 2^d(u_1 - u_0 + u_3 - u_2 + \cdots + u_{2i+1} - u_{2i}) \\ &= 2^d(1 + 3 + \cdots + (2i+1)) = 2^d(i+1)^2.\end{aligned}$$

Par conséquent, en définissant i en fonction de $x \geq 2^d$ par

$$\frac{3(i-1)^2}{2} \leq u_{2i-1} \leq \frac{x}{2^d} < u_{2i+1} \leq \frac{3(i+1)^2}{2},$$

on a

$$2^d\left(\sqrt{\frac{2x}{3 \cdot 2^d}} - 1\right)^2 \leq 2^d i^2 \leq \mathcal{P}_1\left(\frac{f^{2^d}(q)}{1-q}, x\right) \leq 2^d(i+1)^2 \leq 2^d\left(\sqrt{\frac{2x}{3 \cdot 2^d}} + 2\right)^2$$

et (2.12) en découle. □

3. La Fonction Δ

On définit

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n. \tag{3.1}$$

On sait que $\Delta\left(e^{2i\pi z}\right)$ est une forme parabolique de poids 12, et τ est la fonction de Ramanujan (cf. [38, VII, 4.5]).

Proposition 1. *On a*

$$\Delta(q) \equiv \sum_{m=0}^{\infty} q^{(2m+1)^2} \pmod 2; \tag{3.2}$$

autrement dit, $\tau(n)$ est impair si et seulement si n est le carré d'un nombre impair.

Démonstration. L'identité de Jacobi (cf. [19, Théorème 357]) donne

$$\prod_{n=1}^{\infty} (1-q^n)^3 = \sum_{m=0}^{\infty} (-1)^m (2m+1) q^{\frac{m(m+1)}{2}} \equiv \sum_{m=0}^{\infty} q^{\frac{m(m+1)}{2}} \pmod 2.$$

Par (3.1), il suit

$$\Delta(q) \equiv q \left(\sum_{m=0}^{\infty} q^{\frac{m(m+1)}{2}}\right)^8 \equiv \sum_{m=0}^{\infty} q^{1+4m(m+1)} \pmod 2. \qquad \square$$

Soit p un nombre premier. Désignons par $v_p(n)$ la valuation p-adique de n, c'est-à-dire le plus grand exposant a tel que p^a divise n. On définit

$$\omega'(n) = \sum_{\substack{p \mid n \\ v_p(n) = 1}} 1. \tag{3.3}$$

Ainsi, pour $n = 415 = 3^2 \cdot 5 \cdot 7$, on a $\omega'(n) = 2$ et pour $n = 36$, $\omega'(n) = 0$.

Soit k un entier positif. On écrit

$$\Delta^k(q) = \sum_{n=k}^{\infty} \tau_k(n) q^n; \tag{3.4}$$

la congruence (3.2) entraîne

$$\Delta^k(q) \equiv q^k + kq^{k+8} + \frac{k(k-1)}{2} q^{k+16} + \frac{k(k^2 - 3k + 8)}{6} q^{k+24} + \cdots \pmod 2 \tag{3.5}$$

et l'on pose, pour x réel positif

$$B_k(x) = \mathcal{P}_1(\Delta^k, x) = \mathrm{Card}\{n \leq x, \tau_k(n) \equiv 1 \pmod 2\}. \tag{3.6}$$

La relation $B_{2k}(x) = B_k(x/2)$ permet de limiter l'étude de B_k aux k impairs. Nous utiliserons le théorème suivant (cf. [37], 6.6, [36], 6.6 et [31], 2.7):

Théorèm 3. *Soit k un nombre impair positif différent de 1. Il existe un entier $g_k \geq 2$, appelé degré de nilpotence de Δ^k, tel que*

$$B_k(x) = \mathcal{P}_1(\Delta^k, x) \asymp_k \frac{x}{\log x}(\log\log x)^{g_k-2}. \tag{3.7}$$

De plus,

$$\omega'(n) \geq g_k \Rightarrow \tau_k(n) \ \text{ est pair} \tag{3.8}$$

ce qui s'écrit encore

$$\tau_k(n) \text{ est impair} \Rightarrow \omega'(n) \leq g_k - 1. \tag{3.9}$$

D'autre part, g_k est minimal, autrement dit, il existe $n \geq k$ tel que

$$\omega'(n) = g_k - 1 \quad \text{et} \quad \tau_k(n) \text{ est impair.} \tag{3.10}$$

Remarquons que, dans (3.4), $\tau_k(k) = 1$ et (3.9) implique

$$g_k \geq 1 + \omega'(k). \tag{3.11}$$

4. Etude de $B_5(x)$

Rappelons que $\tau_k(n)$ est défini par (3.4) et $B_k(x)$ par (3.6). Lorsque $k = 3$ et $k = 5$, on sait décrire les n tels que $\tau_k(n)$ est impair:

Proposition 2. *Les nombres entiers n pour lesquels $\tau_5(n)$ (resp. $\tau_3(n)$) est impair s'écrivent $p^{4m+1}h^2$ où p est un nombre premier congru à 5 (resp. 3) modulo 8, m est un entier naturel et h un nombre impair non multiple de p.*

Démonstration. Ce résultat est proposé en exercice dans [37], 6.7 ou [36], 6.7. On déduit de (3.2) et (3.5) que

$$n \not\equiv 5 \pmod 8 \Rightarrow \tau_5(n) \equiv 0 \pmod 2. \tag{4.1}$$

Par (3.2), on a

$$\Delta^5(q) = \sum_{n=5}^{\infty} \tau_5(n) q^n = \Delta^4(q)\Delta(q) \equiv \left(\sum_{\substack{a=1 \\ a \text{ impair}}}^{\infty} q^{4a^2} \right) \left(\sum_{\substack{b=1 \\ b \text{ impair}}}^{\infty} q^{b^2} \right) \pmod 2$$

et $\tau_5(n)$ est congru modulo 2 au nombre de façons d'écrire $n = 4a^2 + b^2$ avec a et b impairs positifs. Soit $r(n)$ le nombre de solutions dans $\mathbb{Z}^2$ de l'équation $u^2 + v^2 = n$. Pour $n \equiv 5 \pmod 8$, on a donc

$$\tau_5(n) \equiv \frac{1}{8} r(n) \pmod 2. \tag{4.2}$$

Soit n un nombre impair et $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_I^{\alpha_I} q_1^{\beta_1} q_2^{\beta_2} \cdots q_J^{\beta_J}$ sa décomposition en facteurs premiers avec, pour $1 \leq i \leq I$, $p_i \equiv 1 \pmod 4$ et, pour $1 \leq j \leq J$, $q_j \equiv 3 \pmod 4$. On a (cf. [19, Théorème 278])

$$r(n) = 4 \prod_{i=1}^{I} (\alpha_i + 1) \prod_{j=1}^{J} \left(\frac{1 + (-1)^{\beta_j}}{2} \right).$$

Pour que $r(n)$ soit non nul, tous les β_j doivent être pairs. Rangeons les nombres $p_1, p_2, \ldots, p_I$ de façon que $\alpha_1, \alpha_2, \ldots, \alpha_{I'}$ soient impairs et $\alpha_{I'+1}, \alpha_{I'+2}, \ldots, \alpha_I$ soient pairs. On a alors

$$\frac{r(n)}{4} \equiv \prod_{i=1}^{I'} (\alpha_i + 1) \pmod 2$$

et la condition "*$\tau_5(n)$ impair*" et (4.2) impliquent $I' = 1$ et $\alpha_1 \equiv 1 \pmod 4$, ce qui complète la preuve de la proposition pour B_5. Le cas de B_3 est très voisin et utilise le nombre de représentations de n sous la forme $n = 2a^2 + b^2$ (cf. [16, Théorème 64 et Ex. XXII, 1]). □

Lemme 4. *Soit ν un nombre réel, $\nu \geq 3$. On désigne par $S_\nu(x)$ le nombre de couples (M, N) de nombres entiers positifs telles que $M \geq 5$ et $M^\nu N^2 \leq x$. Alors, on a*

$$S_\nu(x) \leq 8 \frac{\sqrt{x}}{2^\nu}.$$

Démonstration. On a

$$\begin{aligned} S_\nu(x) &= \sum_{5 \leq M \leq x^{1/\nu}} \left\lfloor \sqrt{\frac{x}{M^\nu}} \right\rfloor \leq \sum_{5 \leq M \leq x^{1/\nu}} \sqrt{\frac{x}{M^\nu}} \\ &\leq \sqrt{x} \sum_{M=5}^{\infty} \frac{1}{M^{\nu/2}} \leq \sqrt{x} \int_4^\infty \frac{dt}{t^{\nu/2}} \\ &= \frac{1}{\left(\frac{\nu}{2} - 1\right)} \frac{\sqrt{x}}{4^{\frac{\nu}{2}-1}} \leq \frac{1}{\left(\frac{3}{2} - 1\right)} \frac{\sqrt{x}}{4^{\frac{\nu}{2}-1}} = 8 \frac{\sqrt{x}}{2^\nu}. \end{aligned}$$

□

Introduisons les fonctions classiques en théorie des nombres premiers:

$$\pi(x; 8, 5) = \sum_{\substack{p \leq x \\ p \equiv 5 \pmod 8}} 1 \quad \text{et} \quad \theta(x; 8, 5) = \sum_{\substack{p \leq x \\ p \equiv 5 \pmod 8}} \log p, \tag{4.3}$$

et nous utiliserons l'inégalité (cf. [34, Table 1])

$$x \geq 10^{10} \Rightarrow \left| \theta(x; 8, 5) - \frac{x}{4} \right| \leq \frac{0.002811}{4} x \leq \frac{x}{1000}. \tag{4.4}$$

Lemme 5. *On a pour tout $x > 1$:*

$$\pi(x; 8, 5) \leq 0.405 \frac{x}{\log x}.$$

Démonstration. L'inégalité est vérifiée à l'ordinateur pour $x \leq 10^{10}$; le maximum de $\frac{\pi(x;8,5)\log x}{x}$ est obtenu pour $x = 61$ et $\pi(61; 8, 5) = 6$. On peut donc supposer que $x > 10^{10}$. Soit t_1 vérifiant $1 \le t_1 \le x$. On a

$$\theta(x;8,5) \ge \sum_{\substack{t_1 < p \le x \\ p \equiv 5 \pmod 8}} \log p \ge \log t_1 \left(\pi(x;8,5) - \pi(t_1;8,5)\right)$$

qui, via la borne banale

$$\pi(t_1;8,5) \le \frac{t_1+3}{8} \tag{4.5}$$

donne

$$\pi(x;8,5) \le \frac{\theta(x;8,5)}{\log t_1} + \frac{t_1+3}{8}.$$

En appliquant (4.4) et en choisissant $t_1 = x^{0.8}$, on obtient

$$\pi(x;8,5) \le \frac{0.251x}{0.8\log x} + \frac{x^{0.8}+3}{8} \le \frac{0.32x}{\log x}(1+\rho_1(x))$$

avec $\rho_1(x) = \frac{\log x}{2.56}\left(\frac{1}{x^{0.2}} + \frac{3}{x}\right)$. Comme ρ_1 est une fonction décroissante de x pour $x > 10^{10}$, on majore $\rho_1(x)$ par $\rho_1(10^{10}) \le 0.09$, ce qui, puisque $0.32 \times 1.09 \le 0.405$, achève la preuve du lemme. □

Proposition 3. *Soit $B_5(x)$ défini par* (3.6). *Pour $x \ge 10^{10}$, on a*

$$0.249\frac{x}{\log x} \le B_5(x) \le 0.87\frac{x}{\log x} \tag{4.6}$$

et , lorsque $x \to \infty$,

$$B_5(x) \sim \frac{\pi^2}{32}\frac{x}{\log x} \quad \left(\frac{\pi^2}{32} = 0.308\ldots\right). \tag{4.7}$$

Démonstration. Le coefficient dans (4.7) provient de la formule

$$\sum_{\substack{h=1 \\ h \text{ impair}}}^{\infty} \frac{1}{h^2} = \sum_{n=1}^{\infty}\frac{1}{n^2} - \sum_{\substack{j=2 \\ j \text{ pair}}}^{\infty}\frac{1}{j^2} = \left(\sum_{n=1}^{\infty}\frac{1}{n^2}\right)\left(1-\frac{1}{4}\right) = \frac{\pi^2}{8}. \tag{4.8}$$

De la Proposition 2 et de (4.3), on déduit

$$B_5(x) \ge \pi(x;8,5) \ge \frac{\theta(x;8,5)}{\log x}$$

et la minoration dans (4.6) s'ensuit par (4.4). Ecrivons ensuite

$$B_5(x) = B_5'(x) + B_5''(x) \tag{4.9}$$

où, par la Proposition 2, $B_5'(x)$ compte les éléments de la forme $p^{4m+1}h^2$ avec $m = 0$ tandis que $B_5''(x)$ compte ceux avec $m \ge 1$. Par le Lemme 4, on obtient la majoration:

$$B_5''(x) \le 8\sqrt{x}\sum_{m=1}^{\infty}\frac{1}{2^{4m+1}} = \frac{4}{15}\sqrt{x}. \tag{4.10}$$

Soit t_2 satisfaisant $1 \le t_2 \le \sqrt{x}$. On a

$$B_5'(x) = \sum_{\substack{h \le \sqrt{x} \\ h \text{ impair}}} \left(\sum_{\substack{p \le x/h^2 \\ p \equiv 5 \pmod 8 \\ p \nmid h}} 1\right)$$

$$\le \sum_{\substack{h \le \sqrt{x} \\ h \text{ impair}}} \pi\left(\frac{x}{h^2};8,5\right) = \widehat{B}_5(x,t_2) + \widetilde{B}_5(x,t_2) \tag{4.11}$$

avec

$$\widehat{B}_5(x,t_2) = \sum_{\substack{h \le t_2 \\ h \text{ impair}}} \pi\left(\frac{x}{h^2};8,5\right) \quad \text{et} \quad \widetilde{B}_5(x,t_2) = \sum_{\substack{t_2 < h \le \sqrt{x} \\ h \text{ impair}}} \pi\left(\frac{x}{h^2};8,5\right). \tag{4.12}$$

On majore $\widetilde{B}_5$ par (4.5):

$$\widetilde{B}_5(x,t_2) \le \sum_{t_2 < h \le \sqrt{x}} \left(\frac{x}{8h^2} + \frac{3}{8}\right) \le \frac{x}{8}\int_{t_2-1}^{\infty}\frac{dt}{t^2} + \frac{3\sqrt{x}}{8} = \frac{x}{8(t_2-1)} + \frac{3\sqrt{x}}{8}. \tag{4.13}$$

On majore $\widehat{B}_5$ par le Lemme 5 et par (4.8):

$$\widehat{B}_5(x,t_2) \le 0.405\frac{x}{\log(x/t_2^2)}\sum_{\substack{h \le t_2 \\ h \text{ impair}}}\frac{1}{h^2} \le 0.405\frac{\pi^2}{8}\frac{x}{\log(x/t_2^2)}.$$

En choisissant $t_2 = x^{0.2}$, on obtient

$$\widehat{B}_5(x,x^{0.2}) \le 0.405\frac{\pi^2}{8}\frac{x}{0.6\log x} \le 0.84\frac{x}{\log x}. \tag{4.14}$$

Finalement, il résulte de (4.9), (4.11), (4.13), (4.14) et (4.10) que

$$B_5(x) \le \widehat{B}_5(x,x^{0.2}) + \widetilde{B}_5(x,x^{0.2}) + B_5''(x) \le \frac{x}{\log x}(0.84 + \rho_2(x))$$

avec $\rho_2(x) = \frac{\log x}{8(x^{0.2}-1)} + \left(\frac{3}{8}+\frac{4}{15}\right)\frac{\log x}{\sqrt{x}}$. Comme ρ_2 est une fonction décroissante de x pour $x > 10^{10}$, on majore $\rho_2(x)$ par $\rho_2(10^{10}) \le 0.03$, et la majoration dans (4.6) est ainsi démontrée.

L'équivalence (4.7) est démontrée dans [37], 6.7 et [36], 6.7 en appliquant un théorème taubérien à la série de Dirichlet $\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ où $\chi(n) = 0$ ou 1 suivant que $\tau_5(n)$ est pair ou impair. La démonstration ci-dessus de (4.6) peut être adaptée pour obtenir (4.7).

Les nombres ph^2 où p divise h s'écrivent p^3j^2; donc, par le lemme 4, on a pour tout t_3 tel que $1 \le t_3 \le \sqrt{x}$,

$$B_5'(x) \ge \left(\sum_{\substack{h \le t_3 \\ h \text{ impair}}} \pi\left(\frac{x}{h^2};8,5\right)\right) - S_3(x) = \widehat{B}_5(x,t_3) + \mathcal{O}\left(\sqrt{x}\right). \tag{4.15}$$

En choisissant $t_3 = x^{0.2}$, on a par (4.9)–(4.13) et (4.15)

$$B_5(x) = \left(\sum_{\substack{h \le x^{0.2} \\ h \text{ impair}}} \pi\left(\frac{x}{h^2}; 8, 5\right) \right) + \mathcal{O}(x^{0.8}). \tag{4.16}$$

On applique le théorème des nombres premiers (cf. [17, Théorème 8.8]) sous la forme

$$\pi(x; 8, 5) = \frac{x}{4 \log x} + \mathcal{O}\left(\frac{x}{\log^2 x}\right)$$

qui entraîne, pour $h \le x^{0.2}$

$$\begin{aligned} \pi\left(\frac{x}{h^2}; 8, 5\right) &= \frac{x}{4h^2 \log x \left(1 - \frac{2 \log h}{\log x}\right)} + \mathcal{O}\left(\frac{x}{h^2 \log^2 x}\right) \\ &= \frac{x}{4h^2 \log x} + \mathcal{O}\left(x \frac{\log h + 1}{h^2 \log^2 x}\right). \end{aligned}$$

Comme $\displaystyle\sum_{\substack{h \le t \\ h \text{ impair}}} \frac{1}{h^2} = \frac{\pi^2}{8} + \mathcal{O}\left(\frac{1}{t}\right)$ et que la série $\displaystyle\sum_{\substack{h=1 \\ h \text{ impair}}}^{\infty} \frac{\log h + 1}{h^2}$ est convergente, on obtient

$$\sum_{\substack{h \le x^{0.2} \\ h \text{ impair}}} \pi\left(\frac{x}{h^2}; 8, 5\right) = \frac{\pi^2}{32} \frac{x}{\log x} + \mathcal{O}\left(\frac{x^{0.8}}{\log x}\right) + \mathcal{O}\left(\frac{x}{\log^2 x}\right)$$

qui, avec (4.16), conduit à

$$B_5(x) = \frac{\pi^2}{32} \frac{x}{\log x} + \mathcal{O}\left(\frac{x}{\log^2 x}\right) \tag{4.17}$$

ce qui termine la preuve de (4.7). □

5. Minoration de $A_1(x)$

La série génératrice de $p(n)$ est, par (2.8), (cf. [19], 19.3)

$$P(q) \stackrel{def}{=} \sum_{n=0}^{\infty} p(n) q^n = \prod_{m=1}^{\infty} \frac{1}{1 - q^m} = \frac{1}{f(q)}. \tag{5.1}$$

Soit d un entier naturel pair. On pose

$$k = \frac{2^d - 1}{3} \in \mathbb{N}. \tag{5.2}$$

On écrit alors par (5.1)

$$\left(\sum_{n=0}^{\infty} p(n) q^n \right) f(q)^{2^d} = P(q) f(q)^{2^d} = f(q)^{3k}. \tag{5.3}$$

Par (1.2), (5.1) et (2.2), on a $A_1(x) = \mathcal{P}_1(P, x)$ et le Lemme 2 appliqué à (5.3) donne pour tout x réel positif

$$A_1(x) = \mathcal{P}_1(P, x) \ge \frac{\mathcal{P}_1(f^{3k}, x)}{\mathcal{P}_1(f^{2^d}, x)}. \tag{5.4}$$

Mais, par (2.4), (3.1) et (3.7), il vient

$$\begin{aligned} \mathcal{P}_1(f^{3k}, x) &= \mathcal{P}_1(f^{24k}, 8x) = \mathcal{P}_1\left(\frac{\Delta^k(q)}{q^k}, 8x\right) \\ &= \mathcal{P}_1(\Delta^k, 8x + k) = B_k(8x + k) \end{aligned} \tag{5.5}$$

et (5.4) et (2.11) entraînent, pour tout d pair et tout x réel positif

$$A_1(x) \ge \frac{B_k(8x + k)}{\sqrt{\frac{8x}{3 \cdot 2^d}} \left(1 + \sqrt{\frac{3 \cdot 2^d}{2x}}\right)} \tag{5.6}$$

où k est défini par (5.2). Fixons d et k tels que $d > 2$ et $\omega'(k) > 1$; l'application du Théorème 3 donne avec (3.8)

$$A_1(x) \gg_d \frac{\sqrt{x}}{\log x} (\log \log x)^{g_k - 2} \ge \frac{\sqrt{x}}{\log x} (\log \log x)^{\omega'(k) - 1}, \tag{5.7}$$

ce qui démontre le Théorème 1 avec

$$K = \omega'(k) - 1 = \omega'\left(\frac{2^d - 1}{3}\right) - 1. \tag{5.8}$$

La valeur de K donnée en (1.9) sera justifiée au paragraphe 7.

Démonstration du Théorème 2(i)

La fonction $t \mapsto \frac{\sqrt{t}}{\log t}$ est décroissante pour $t < e^2 = 7.389\ldots$ et croissante pour $t > e^2$. Comme $A_1(7) = 7$, pour $7 \le x < 8$, on a $\frac{A_1(x)}{\sqrt{x}/\log x} \ge \min\left(\frac{7}{\sqrt{7}/\log 7}, \frac{7}{\sqrt{8}/\log 8}\right) \ge 5.14$. On calcule $A_1(n)$ pour $n \le 50000$ et l'on vérifie que, pour $8 \le n \le 50000$, $A_1(n) \ge 4.57 \frac{\sqrt{n+1}}{\log(n+1)}$. Ensuite, la table 7 de [32] donne $A_1(49999) = 25016 > 4.57 \frac{\sqrt{2 \cdot 10^6}}{\log(2 \cdot 10^6)}$ et $A_1(1999999) = 999497 > 4.57 \frac{\sqrt{4 \cdot 10^{13}}}{\log(4 \cdot 10^{13})}$; donc, $A_1(x) \ge 4.57 \frac{\sqrt{x}}{\log x}$ est vérifiée pour $x \le 4 \cdot 10^{13}$.

Supposons maintenant $x > 4 \cdot 10^{13}$; lorsque $d = 4$, $k = 5$ et $x > 4 \cdot 10^{13}$, on a $\sqrt{\frac{3 \cdot 2^d}{2x}} \le 8 \cdot 10^{-7}$, et, par (4.6),

$$\begin{aligned} B_5(8x + 5) \ge B_5(8x) &\ge 0.249 \frac{8x}{\log x \left(1 + \frac{\log 8}{\log x}\right)} \\ &\ge \frac{x}{\log x} \frac{1.992}{1 + \frac{\log 8}{\log(4 \cdot 10^{13})}} \ge 1.867 \frac{x}{\log x}. \end{aligned}$$

En reportant ces majorations dans (5.6), on obtient

$$A_1(x) \geq \left(\frac{1.867\sqrt{6}}{1+8\cdot 10^{-7}}\right)\frac{\sqrt{x}}{\log x} \geq 4.573\,\frac{\sqrt{x}}{\log x}$$

ce qui achève la démonstration du théorème 2(i).

6. Minoration de $A_0(x)$

Par (2.3) et (5.1), on a $A_0(x) = \mathcal{P}_1\left(\frac{1}{1-q} + P(q), x\right)$. Soit toujours d pair et k défini par (5.2). On déduit de (5.3)

$$\left(\frac{1}{1-q} + P(q)\right) f(q)^{2^d} = \frac{f(q)^{2^d}}{1-q} + f(q)^{3k}.$$

En appliquant le lemme 2 à l'inégalité ci-dessus, puis, successivement (2.6), (2.12), (5.5) et (2.11), il vient

$$\begin{aligned} A_0(x) &\geq \frac{\mathcal{P}_1\left(\frac{f(q)^{2^d}}{1-q} + f(q)^{3k}, x\right)}{\mathcal{P}_1(f(q)^{2^d}, x)} \\ &\geq \frac{\mathcal{P}_1\left(\frac{f(q)^{2^d}}{1-q}, x\right) - \mathcal{P}_1(f(q)^{3k}, x)}{\mathcal{P}_1(f(q)^{2^d}, x)} \\ &\geq \frac{\frac{2x}{3}\left(1-\sqrt{\frac{6\cdot 2^d}{x}}\right) - B_k(8x+k)}{\sqrt{\frac{8x}{3\cdot 2^d}}\left(1+\sqrt{\frac{3\cdot 2^d}{2x}}\right)}. \end{aligned} \tag{6.1}$$

Pour d fixé et x tendant vers l'infini, il résulte de (6.1) et (3.7) que

$$A_0(x) \gtrsim \frac{2^{d/2}}{\sqrt{6}}\sqrt{x}. \tag{6.2}$$

Lorsque $d = k = 0$, on retrouve la démonstration du Théorème 1 de [26] qui n'utilise pas (3.7) (car $B_0(x) = 1$).

Lorsque d tend vers l'infini, on retrouve la démonstration de (1.7) (cf. [26, Appendice]) dans le cas $a = 1$ et $b = 0$.

Démonstration du Théorème 2(ii)

On calcule $A_0(n)$ pour $n \leq 50000$ et l'on vérifie que, pour $10 \leq n \leq 50000$, $A_0(n) \geq 1.05\sqrt{n+1}$. Ensuite, la table 7 de [32] donne $A_0(49999) = 24984 > 1.05\sqrt{2\cdot 10^6}$ et $A_0(1999999) = 1000503 > 1.05\sqrt{9\cdot 10^{11}}$; donc, $A_0(x) \geq 1.05\sqrt{x}$ est vérifiée pour $x \leq 9\cdot 10^{11}$. Supposons maintenant $x > 9\cdot 10^{11}$; lorsque $d = 4$, $k = 5$ et $x > 9\cdot 10^{11}$, on a $\sqrt{\frac{6\cdot 2^d}{x}} \leq 1.04\cdot 10^{-5}$, $\sqrt{\frac{3\cdot 2^d}{2x}} \leq 5.2\cdot 10^{-6}$, puis, par (4.1) et (4.6),

$$\begin{aligned} B_5(8x+5) &\leq 1 + B_5(8x) \leq 1 + 0.87\frac{8x}{\log(8x)} \leq 1 + 0.87\frac{8x}{\log(72\cdot 10^{11})} \\ &\leq 1 + 0.2351\,x \leq x\left(0.2351 + \frac{1}{9\cdot 10^{11}}\right) \leq 0.236\,x. \end{aligned}$$

En reportant ces majorations dans (6.1), on obtient

$$A_0(x) \geq \frac{\frac{2x}{3}\left(1 - 1.04\cdot 10^{-5} - \frac{3}{2}\,0.236\right)}{\sqrt{\frac{x}{6}}\,(1 + 5.2\cdot 10^{-6})} \geq 1.054\,\sqrt{x}$$

ce qui achève la démonstration du Théorème 2(ii).

7. Grandes Valeurs de $\omega'\left(\frac{2^n-1}{3}\right)$

La fonction ω' a été définie en (3.3). Pour factoriser $2^n - 1$, on le décompose en produit de facteurs cyclotomiques, et on peut ainsi calculer avec MAPLE, par la méthode de factorisation d'A. Lenstra utilisant les courbes elliptiques, que

$$\omega'\left(\frac{2^{384}-1}{3}\right) = 19, \quad \omega'\left(\frac{2^{1680}-1}{3}\right) = 63.$$

On peut aussi lire ces factorisations dans les tables du projet Cunningham [10]. Notons que $\left|\omega'\left(\frac{2^n-1}{3}\right) - \omega'(2^n-1)\right| \leq 1$. Dans ces calculs, on observe que beaucoup de facteurs premiers p de $2^n - 1$ satisfont $v_p\,(2^n-1) = 1$, et l'on conjecture

$$\limsup_{n\to\infty}\ \omega'(2^n-1) = +\infty. \tag{7.1}$$

Malheureusement, il semble très difficile de démontrer (7.1) à cause des nombres de Wieferich.

Les nombres de Wieferich

On dit qu'un nombre premier p est de Wieferich si (cf. [35], 5, III et [12], 1.3.3)

$$2^{p-1} \equiv 1 \pmod{p^2}. \tag{7.2}$$

On connait deux nombres de Wieferich, 1093 et 3511; il n'y en a pas d'autres jusqu'à $4\cdot 10^{12}$ (cf. [11]). Personne ne s'est hasardé à conjecturer que la proposition

"il existe une infinité de nombres premiers de Wieferich" (7.3)

est vraie ou fausse. La conjecture, pourtant fort vraisemblable,

"il existe une infinité de nombres premiers qui ne sont pas de Wieferich" (7.4) n'a jamais été démontrée. Cependant, (7.4) résulte de la conjecture ABC (cf. [12, Ex. 8.15]). Le lien avec les grandes valeurs de $\omega'\left(\frac{2^n-1}{3}\right)$ est mis en évidence dans les Propositions 4–7.

Lemme 6. *Soit p un nombre premier impair; soit ω_1 (resp. ω_2) l'ordre de 2 dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ (resp. $(\mathbb{Z}/p^2\mathbb{Z})^*$). Alors, ou bien $\omega_2 = \omega_1$, et p est un nombre de Wieferich ou bien $\omega_2 = \omega_1 p$ et p n'est pas un nombre de Wieferich.*

Démonstration. Par le petit théorème de Fermat, on a $2^{p-1} \equiv 1 \pmod p$; de même, $2^{\omega_2} \equiv 1 \pmod{p^2}$ implique $2^{\omega_2} \equiv 1 \pmod p$; ainsi, $p-1$ et ω_2 sont des multiples de ω_1. On peut écrire $2^{\omega_1} = 1 + \lambda p$, où λ est un entier; il s'ensuit que

$$2^{\omega_1 p} = (1+\lambda p)^p = 1 + \lambda p^2 + \sum_{i=2}^{p} \binom{p}{i} \lambda^i p^i \equiv 1 \pmod{p^2}$$

et, en conséquence, ω_2 divise $\omega_1 p$. On a donc ou bien $\omega_2 = \omega_1$ ou bien $\omega_2 = \omega_1 p$. Dans le premier cas, comme $\omega_2 = \omega_1$ divise $p-1$, on a $2^{p-1} \equiv 1 \pmod{p^2}$. Dans le deuxième cas, ω_2 est strictement plus grand que $p-1$ et donc $2^{p-1} \not\equiv 1 \pmod{p^2}$. □

Proposition 4. *Soit p un facteur premier de $2^n - 1$.*
(i) *Si $v_p(2^n-1) = 1$ c'est-à-dire si p^2 ne divise pas $2^n - 1$, alors p n'est pas de Wieferich.*
(ii) *Si $v_p(2^n-1) \geq 2$ c'est-à-dire si p^2 divise 2^n-1, alors ou bien p divise n ou bien p est de Wieferich.*

Démonstration. Utilisons les notations du lemme 6. Comme $2^n \equiv 1 \pmod p$ n est multiple de ω_1.

Si p est de Wieferich, le Lemme 6 affirme que $\omega_2 = \omega_1$ et n est multiple de $\omega_2 = \omega_1$. Ainsi $2^n \equiv 1 \pmod{p^2}$ et $v_p(2^n-1) \geq 2$, ce qui prouve (i).

Si p n'est pas de Wieferich et si p ne divise pas n, on a par le lemme 6 $\omega_2 = \omega_1 p$, et ω_2 qui est multiple de p ne peut pas diviser n; par conséquent, $2^n \not\equiv 1 \pmod{p^2}$ et $v_p(2^n-1) < 2$, ce qui prouve (ii). □

Proposition 5. *On a l'implication*

$$(7.1) \Rightarrow (7.4)$$

autrement dit, si $\omega'(2^n-1)$ n'est pas majoré, il existe une infinité de nombres premiers qui ne sont pas de Wieferich.

Démonstration. Ecrivons la décomposition en facteurs premiers

$$2^n - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_j} p_{j+1} p_{j+2} \cdots p_{j+\ell} \tag{7.5}$$

avec $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_j \geq 2$. On a $\omega'(2^n-1) = \ell$ et par (7.1), on peut choisir n pour que ℓ soit aussi grand que l'on veut. Par la Proposition 4, $p_{j+1}, p_{j+2}, \ldots, p_{j+\ell}$ ne sont pas de Wieferich. □

Proposition 6. *On a l'implication*

$$\text{non } (7.1) \Rightarrow (7.3)$$

autrement dit, s'il existe C tel que $\omega'(2^n-1) \leq C$ pour tout n, alors il existe une infinité de nombres de Wieferich.

Démonstration. Soit $n = 2^r$. On a

$$2^n - 1 = 2^{2^r} - 1 = (2-1)(2+1)(2^2+1)\left(2^{2^2}+1\right)\ldots\left(2^{2^{r-1}}+1\right).$$

Les facteurs $2^{2^i}+1$ ci-dessus sont les nombres de Fermat et sont premiers entre eux deux à deux; en conséquence, $2^n - 1$ a au moins r facteurs premiers. Ecrivons comme en (7.5)

$$2^n - 1 = 2^{2^r} - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_j^{\alpha_j} p_{j+1} p_{j+2} \ldots p_{j+\ell} \tag{7.6}$$

avec $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_j \geq 2$ et $j + \ell \geq r$. On a $\omega'(2^n-1) = \ell \leq C$ par hypothèse et, en conséquence, $j \geq r - \ell \geq r - C$. Mais, $p_1, p_2, \ldots, p_j$ sont impairs et donc ne divisent pas $n = 2^r$; par la proposition 4 (ii) et (7.6), $p_1, p_2, \ldots, p_j$ sont des nombres de Wieferich; comme $j \geq r - C$ et que r peut être choisi arbitrairement grand, cela prouve la proposition. □

Proposition 7. *Soit $\overline{W}(x)$ le nombre de nombres premiers qui ne sont pas de Wieferich et qui sont inférieurs ou égaux à x. Alors, pour $x > 3$, il existe n pair tel que*

$$\omega'\left(\frac{2^n-1}{3}\right) \geq \overline{W}(2x) - \overline{W}(x).$$

Démonstration. Si $\overline{W}(2x) = \overline{W}(x)$, la proposition est évidente; sinon, soit $x < p_1 < p_2 < \cdots < p_r \leq 2x$ avec $r = \overline{W}(2x) - \overline{W}(x) \geq 1$ les nombres premiers compris entre x et $2x$ qui ne sont pas de Wieferich. On pose

$$n = \operatorname{ppcm}(p_1 - 1, p_2 - 1, \ldots, p_r - 1). \tag{7.7}$$

On remarque que n est pair et que les facteurs premiers de n sont au plus égaux à $\frac{p_r-1}{2} < x$; en particulier, n n'est divisible par aucun des nombres $p_1, p_2, \ldots, p_r$. Par le petit théorème de Fermat, pour tout i, $1 \leq i \leq r$, $2^{p_i-1} \equiv 1 \pmod{p_i}$, donc, par (7.7), p_i divise $2^n - 1$. Comme p_i n'est pas de Wieferich et ne divise pas n, par la proposition 4 (ii), $v_{p_i}\left(\frac{2^n-1}{3}\right) = 1$. Ainsi, $\omega'\left(\frac{2^n-1}{3}\right) \geq r = \overline{W}(2x) - \overline{W}(x)$. □

Démonstration de (1.9)

R. Crandall, K. Dilcher and C. Pomerance ont montré dans [11] qu'il n'y a pas de nombres de Wieferich entre $2 \cdot 10^{12}$ et $4 \cdot 10^{12}$. On a donc

$$\overline{W}\left(4 \cdot 10^{12}\right) - \overline{W}\left(2 \cdot 10^{12}\right) = \pi\left(4 \cdot 10^{12}\right) - \pi\left(2 \cdot 10^{12}\right). \tag{7.8}$$

La valeur de K donnée en (1.9) résulte de (5.8), de la proposition 7, de (7.8) et des valeurs de $\pi(4 \cdot 10^{12})$ et de $\pi(2 \cdot 10^{12})$ aimablement communiquées par M. Deléglise d'après l'algorithme décrit dans [13,14].

D'après [12], 1.3.3, McKintosh a calculé qu'il n'y a pas de nombres de Wieferich entre $4 \cdot 10^{12}$ et $16 \cdot 10^{12}$. On peut donc augmenter K en conséquence et choisir $K = \pi(16 \cdot 10^{12}) - \pi(8 \cdot 10^{12}) - 1 = 544830816681 - 279010070811 - 1 = 265820745870$.

Remerciements

Recherche partiellement financée par le CNRS, Institut Camille Jordan, UMR 5208.

References

[1] S. Ahlgren, Distribution of parity of the partition function on arithmetic progressions, *Indag. Math. (N. S.)* **10** (1999) 173–181.

[2] F. Ben Saïd, On a conjecture of Nicolas–Sárközy about partitions, *J. Number Theory* **95** (2002) 209–226.

[3] F. Ben Saïd and J.-L. Nicolas, Even partition functions, *Sém. Lothar. Combin.* **46** (2002) B 46i; http://www.mat.univie.ac.at/~slc/.

[4] F. Ben Saïd and J.-L. Nicolas, Sets of parts such that the partition function is even, *Acta Arith.* **106** (2003) 183–196.

[5] F. Ben Saïd, On some sets with even valued partition function, *Ramanujan J.* **9** (2005) 63–75.

[6] F. Ben Saïd, H. Lahouar and J.-L. Nicolas, On the counting function of the sets of parts $\mathcal{A}$ such that the partition function $p(\mathcal{A}, n)$ takes even values for n large enough, to appear in *Discrete Math.*

[7] B. C. Berndt, A. J. Yee and A. Zaharescu, On the parity of partition functions, *Int. J. Math.* **14** (2003) 437–459.

[8] B. C. Berndt, A. J. Yee and A. Zaharescu, New theorems on the parity of partition functions, *J. Reine Angew. Math.* **566** (2004) 91–109.

[9] M. Boylan and K. Ono. Parity of the partition function in arithmetic progressions, II, *Bull. London Math. Soc.* **33** (2001) 558–564.

[10] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman and S. S. Wagstaff, Jr. Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers, Contemporary Mathematics, Vol. 22, 2nd edn. (Amer. Math. Soc. Providence RI, 1988).

[11] R. Crandall, K. Dilcher and C. Pomerance, A search for Wieferich and Wilson primes, *Math. Comp.* **66** (1997) 433–449.

[12] R. Crandall and C. Pomerance, *Prime Numbers A Computational Perspective* (Springer-Verlag, 2001).

[13] M. Deléglise and J. Rivat, Computing $\pi(x)$: The Meissel, Lehmer, Lagarias, Miller, Odlyzko method, *Math. Comp.* **65** (1996) 235–245.

[14] M. Deléglise, P. Dusart and X. F. Roblot, Counting primes in residue classes, *Math. Comp.* **73** (2004) 1565–1575.

[15] J. Dixmier and J.-L. Nicolas, Parité de certains nombres de partitions, *Travaux Mathématiques*, Vol. 13 (Publication du Centre Universitaire de Luxembourg, 2002), pp. 93–153.

[16] L. E. Dickson, *Introduction to the Theory of Numbers* (Dover Pub. Inc., New York, 1957).

[17] W. J. Ellison and M. Mendès-France, *Les Nombres Premiers*, Vol. IX (Publications de l'Institut de mathématique de l'université de Nancago, Hermann, Paris, 1975).

[18] G. H. Hardy and S. Ramanujan, Asymptotic formulae in combinatory analysis. *Proc. London Math. Soc. (2)* **17** (1918) 75–115; *Collected Papers of S. Ramanujan*, eds. G. H. Hardy, P. V. Se Aiyer and B. M. Wilson (American Mathematical Society Chelsea Publications, 2000), pp. 276–309.

[19] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th edn. (Oxford at the Clarendon Press, 1964).

[20] O. Kolberg, Note on the parity of the partition function, *Math. Scand* **7** (1959) 377–378.

[21] H. Lahouar, Fonction de partitions parité périodique, *European J. Combin.* **24** (2003) 1089–1096.

[22] H. Lahouar, Ensembles de fonctions de partitions à parité périodique et leurs fonctions de décompte, thèse (Université de Tunis II, 2004).

[23] 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 (The MIT Press, 1978), pp. 1087–1089.

[24] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Code* (North-Holland, 1977).

[25] L. Mirsky, The distribution of values of the partition function in residue classes, *J. Math. Anal. Appl.* **93** (1983) 593–598.

[26] J.-L. Nicolas, I. Ruzsa and A. Sárközy, On the parity of additive representation function, *J. Number Theory* **73** (1998) 292–317 (with an appendix of J.-P. Serre).

[27] J.-L. Nicolas and A. Sárközy, On the parity of partition functions, *Illinois J. Math.* **39** (1995) 586–597.

[28] J.-L. Nicolas and A. Sárközy, On the parity of generalized partition functions, *Number Theory for the Millennium*, eds. M. A. Bennetts *et al.*, Vol III (A.K. Peters Ltd., 2002), pp. 55–72.

[29] J.-L. Nicolas. On the parity of generalized partition functions II, *Period. Math. Hungar.* **43** (2001) 177–189.

[30] K. Ono. Parity of the partition function in arithmetic progressions, *J. Reine Angew. Math.* **472** (1996) 1–15.

[31] K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, CBMS No. 102 (Amer. Math. Soc. Providence RI, 2004).

[32] T. R. Parkin and D. Shanks, On the distribution of parity in the partition function, *Math. Comp.* **21** (1967) 466–480.

[33] Rademacher, Topics in analytic number theory, *Die Grundlehren der Math. Wiss.*, Band No. 169 (Springer-Verlag, 1973).

[34] O. Ramaré and R. Rumely, Primes in arithmetic progressions, *Math. Comp.* **65** (1996) 397–425.

[35] P. Ribenboim, *The New Book of Prime Numbers Record*, 3rd edn. (Springer-Verlag, 1995).

[36] J.-P. Serre, Divisibilité de certaines fonctions arithmétiques, *Séminaire Delange-Pisot-Poitou (Théorie des nombres)*, 16ème année, No. 20 (1974/75) 28.

[37] J.-P. Serre, Divisibilité de certaines fonctions arithmétiques, *L'Enseignement Math.* **22** (1976) 227–260.

[38] J.-P. Serre, Cours d'arithmétique (Paris, 1970).

[39] M. Subbarao, Some remarks on the partition function, *Amer. Math. Monthly*, **73** (1966) 851–854.