

Propriétés arithmétiques d'une série liée aux fonctions thêta

par

DANIEL DUVERNEY (Lille)

1. Introduction. Soit $q \in \mathbb{Z}$, $|q| \geq 2$. Nous définissons

$$(1) \quad x_q = \sum_{n=0}^{\infty} q^{-n^2}.$$

Il est clair que x_q est un nombre irrationnel, puisque son développement q -adique est formé d'une suite non périodique de 0 et de 1.

J. Liouville a démontré l'irrationalité de x_q en l'approximant par les sommes partielles de la série qui le définit [14].

L'étude des propriétés arithmétiques de x_q s'est poursuivie grâce à l'introduction de la fonction

$$(2) \quad f(z) = \sum_{n=0}^{\infty} q^{-n(n+1)/2} z^n.$$

On peut citer, sur ce sujet, les travaux de L. Tschakaloff [18], de P. Bundschuh [2], de P. Bundschuh et M. Waldschmidt [4]. Pour une bibliographie plus complète sur ce sujet, on pourra consulter [3].

En particulier, P. Bundschuh dans [2] a démontré que x_q n'est pas un nombre de Liouville.

Très récemment, P. Borwein a prouvé dans [1] que

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{q^n + r} \notin \mathbb{Q} \quad \text{si } r \in \mathbb{Q}, r \neq -q^n.$$

On en déduit que $x_q^2 - x_q$ est irrationnel ([12], Th. 312, p. 258).

Les nombres x_q se trouvent liés de manière très simple à la fonction θ_3 de Jacobi, puisque l'on a ([5], p. 65)

$$(3) \quad 2x_q = 1 + \theta_3\left(0, \frac{\log q}{i\pi}\right).$$

Le but de ce travail est de démontrer le résultat suivant :

THÉORÈME 1. Soit $q \in \mathbb{Z}$, $|q| \geq 2$. Alors

$$x_q = \sum_{n=0}^{\infty} q^{-n^2} \text{ est non quadratique.}$$

P. Erdős conjecture par ailleurs dans [7] que, si n_k est une suite d'entiers vérifiant $n_k > ck^2$, alors $\sum_{k=1}^{\infty} q^{-n_k}$ est non quadratique. Cette conjecture pourrait peut-être se démontrer par une méthode analogue à celle utilisée ici, bien que cela paraisse, a priori, beaucoup plus difficile.

Pour démontrer le théorème 1, nous utiliserons le critère d'irrationalité suivant :

THÉORÈME 2. Soit $q \in \mathbb{Z}$, $|q| \geq 2$. Soit $(a(n))_{n \in \mathbb{N}}$ une suite dans $\mathbb{Z}^{\mathbb{N}}$ vérifiant les propriétés suivantes :

- (a) $a(n) \neq 0$ pour une infinité de valeurs de n .
- (b) Pour n assez grand, $|a(n)| \leq r(n)$, avec
 - (b₁) $r(n) > 0$,
 - (b₂) $\limsup r(n+1)/r(n) < |q|$.
- (c) Il existe une infinité d'entiers $k \in \mathbb{N}$, et des entiers $n_k \in \mathbb{N}$, tels que :
 - (c₁) $a(n_k + 1) = a(n_k + 2) = \dots = a(n_k + k) = 0$,
 - (c₂) $\lim_{k \rightarrow \infty} r(n_k + k + 1)/|q|^k = 0$.

Soit $x = \sum_{n=0}^{\infty} a(n)q^{-n}$. Alors si $x = \alpha/\beta \in \mathbb{Q}$, on a pour k assez grand,

$$(4) \quad \alpha q^{n_k} - \beta \sum_{n=0}^{n_k} a(n)q^{n_k-n} = 0.$$

La démonstration du théorème 2 sera donnée au paragraphe 2. Remarquons seulement que ce critère est basé tout simplement sur l'approximation de x par ses sommes partielles et nous n'introduisons, par conséquent, aucun outil nouveau.

Il existe d'autres résultats d'irrationalité pour les séries $x = \sum_{n=0}^{\infty} a(n)q^{-n}$ comportant beaucoup de termes nuls. On peut citer les deux théorèmes suivants :

THÉORÈME 3 ([10]). Si $a(n) \in \mathbb{N}$ pour tout $n \geq 1$, et si $a(n)$ est non nul pour une infinité de valeurs de n , avec

$$(5) \quad \sum_{k=1}^n a(k) = o(n),$$

alors $\sum_{n=1}^{\infty} a(n)q^{-n}$ est irrationnel pour tout entier $q \geq 2$.

THÉORÈME 4 ([6]). Soit $a(1) < a(2) < \dots$ une suite d'entiers satisfaisant $\lim_{n \rightarrow \infty} [a(n+1) - a(n)] = \infty$. Alors $\sum_{n=1}^{\infty} a(n)q^{-a(n)}$ est irrationnel pour tout entier $q \geq 2$.

Aucun de ces deux théorèmes ne peut s'appliquer au cas qui nous occupe, même pour $q \geq 2$. Supposons, en effet, que x_q soit quadratique, c'est-à-dire qu'il existe $A, B, C \in \mathbb{Z}$, $A \neq 0$, tels que

$$(6) \quad Ax_q^2 + Bx_q + C = 0.$$

Ecrivons $x_q = \sum_{n=0}^{\infty} l(n)q^{-n}$ avec $l(n) = 1$ si n est le carré d'un entier naturel, $l(n) = 0$ sinon. Alors

$$x_q^2 = \sum_{n=0}^{\infty} \sum_{k=0}^n l(k)l(n-k)q^{-n}.$$

Des considérations bien connues ([12], p. 258 ; [8], p. 219) montrent que

$$(7) \quad x_q^2 = \sum_{n=0}^{\infty} \frac{\varrho(n)}{q^n}$$

où $\varrho(n)$ désigne le nombre de décompositions de n en somme des carrés de deux entiers positifs.

Alors (6) devient

$$(8) \quad \sum_{n=0}^{\infty} \frac{A\varrho(n) + Bl(n)}{q^n} + C = 0.$$

On se ramène donc à prouver l'irrationalité de $\sum_{n=0}^{\infty} a(n)q^{-n}$, avec $a(n) = A\varrho(n) + Bl(n)$. Puisque $a(n)$ peut changer de signe, ni le théorème 3 ni le théorème 4 ne peuvent être utilisés. Ils ne peuvent même pas permettre de démontrer que x_q^2 est irrationnel. C'est clair pour le théorème 4; en ce qui concerne le théorème 3, on sait que ([12], p. 270, th. 339)

$$(9) \quad \lim_{n \rightarrow \infty} \frac{\varrho(1) + \varrho(2) + \dots + \varrho(n)}{n} = \frac{\pi}{4}.$$

La condition (5) n'est donc pas vérifiée.

Il nous faudra, pour appliquer le théorème 2, un lemme assez fin sur la répartition des zéros de la fonction $\varrho(n)$. Ce lemme sera énoncé et démontré au paragraphe 4. Sa démonstration utilise de manière essentielle le résultat suivant, dû à Yu. Linnik [13] :

THÉORÈME 5. Soit $u_n = \zeta n + \chi$, avec $\zeta, \chi \in \mathbb{N}$, ζ et χ premiers entre eux, et $0 < \chi < \zeta$. Soit $p(\zeta, \chi)$ le plus petit nombre premier de la suite arithmétique u_n . Il existe une constante absolue L (constante de Linnik) telle que

$$(10) \quad p(\zeta, \chi) \leq \zeta^L$$

pour ζ assez grand.

La constante L est effectivement calculable. On sait par exemple que $L \leq 20$ ([11]). Mais nous n'aurons pas besoin de cette estimation.

Le plan de l'article est le suivant : dans le paragraphe 2, nous démontrons le théorème 2. Dans le paragraphe 3, nous donnons un exemple pédagogique d'application du théorème 2. Cet exemple nous permettra de motiver la forme générale du lemme technique sur les zéros de $\varrho(n)$. L'énoncé et la longue démonstration de ce lemme occuperont le paragraphe 4. Dans le paragraphe 5 enfin, nous démontrerons le théorème 1.

2. Démonstration du théorème 2. Si $\beta x - \alpha = 0$, avec $\alpha, \beta \in \mathbb{Z}$, alors

$$\alpha q^{n_k} - \beta \sum_{n=0}^{n_k} a(n) q^{n_k-n} = \beta q^{n_k} \sum_{n=n_k+1}^{\infty} \frac{a(n)}{q^n}.$$

D'où, en vertu de (c₁),

$$(11) \quad \alpha q^{n_k} - \beta \sum_{n=0}^{n_k} a(n) q^{n_k-n} = \beta q^{n_k} \sum_{n=n_k+k+1}^{\infty} \frac{a(n)}{q^n}.$$

Utilisant (b), nous obtenons

$$\left| \alpha q^{n_k} - \beta \sum_{n=0}^{n_k} a(n) q^{n_k-n} \right| \leq |\beta| |q|^{n_k} \sum_{n=n_k+k+1}^{\infty} \frac{r(n)}{|q|^n}.$$

D'après l'hypothèse (b₂), on peut trouver $\eta \in]0, |q|[$ tel que $r(n+1)/r(n) \leq \eta$ pour n assez grand. Mais n_k tend vers l'infini avec k en vertu de (a), donc pour k assez grand,

$$\begin{aligned} \left| \alpha q^{n_k} - \beta \sum_{n=0}^{n_k} a(n) q^{n_k-n} \right| &\leq |\beta| |q|^{n_k} \sum_{n=n_k+k+1}^{\infty} \frac{r(n_k+k+1) \eta^{n-(n_k+k+1)}}{|q|^n} \\ &\leq |\beta| |q|^{n_k} \frac{r(n_k+k+1)}{|q|^{n_k+k+1}} \sum_{n=0}^{\infty} \left(\frac{\eta}{|q|} \right)^n \\ &\leq \frac{|\beta|}{|q| - \eta} \frac{r(n_k+k+1)}{|q|^k}. \end{aligned}$$

Pour k assez grand, l'hypothèse (c₂) et le fait que le membre de gauche de cette inégalité est entier entraînent que

$$\alpha q^{n_k} - \beta \sum_{n=0}^{n_k} a(n) q^{n_k-n} = 0. \blacksquare$$

Remarque. Dans le cas où tous les termes de la série sont positifs, c'est-à-dire $q \geq 2$ et $a(n) \geq 0, \forall n \in \mathbb{N}$, on peut conclure que x est irrationnel (il suffit de reporter le résultat obtenu dans l'égalité (11)). Mais dans le cas général, on ne peut espérer qu'une contradiction de type arithmétique,

faisant intervenir la notion de divisibilité. C'est ce qui apparaîtra nettement dans l'exemple simple que nous étudions maintenant.

3. Un exemple pédagogique

THÉORÈME 6. Soit $(p_n)_{n \in \mathbb{N}^*}$ la suite des nombres premiers de \mathbb{N} . Soit $q \in \mathbb{Z}$, $|q| \geq 2$. Alors

$$x = \sum_{n=1}^{\infty} p_n q^{-p_n} \quad \text{est irrationnel.}$$

Démonstration. Avant de démontrer ce théorème, remarquons qu'il ne peut se déduire du théorème 4, puisque l'on ne connaît pas $\liminf(p_{n+1} - p_n)$ (voir par exemple [16], p. 191 et suivantes). Il ne peut non plus se déduire du théorème 3, même si $q > 0$, car si nous posons

$$x = \sum_{n=0}^{\infty} a(n) q^{-n}$$

avec $a(n) = n$ si n est premier et $a(n) = 0$ si n est composé, nous avons

$$\frac{1}{n} \sum_{i=1}^n a(i) = \frac{1}{n} \sum_{p \leq n} p \geq \frac{1}{n} \sum_{n/2 \leq p \leq n} p \geq \frac{1}{2} \left(\pi(n) - \pi\left(\frac{n}{2}\right) \right) \geq \frac{1}{2}.$$

Démontrons maintenant le théorème 6. Nous prenons $r(n) = n$ et nous utilisons le résultat élémentaire suivant [15] :

LEMME 1. Pour une infinité d'entiers n , on a

$$p_{n+1} - p_n \geq 1.7 \log p_n.$$

Il résulte immédiatement de ce lemme qu'il existe une suite de nombres premiers n_k telle que

$$a(n_k + 1) = a(n_k + 2) = \dots = a(n_k + k) = 0 \quad \text{avec } k \geq \frac{3}{2} \log n_k.$$

On a donc $n_k \leq \exp(\frac{2}{3}k)$, et puisque $\exp(\frac{2}{3}) < 2$, on a

$$\lim_{k \rightarrow \infty} \frac{r(n_k + k + 1)}{|q|^k} = 0.$$

Donc si $x = \alpha/\beta \in \mathbb{Q}$, on a pour k assez grand, en vertu du théorème 2,

$$\alpha q^{n_k} - \beta \sum_{n=0}^{n_k} a(n) q^{n_k - n} = 0.$$

Posons $\beta = q^\gamma \beta'$, où q ne divise par β' . Alors

$$\alpha q^{n_k - \gamma} - \beta' \sum_{n=0}^{n_k} a(n) q^{n_k - n} = 0.$$

On en déduit que q divise $\beta' a(n_k) = \beta' n_k$. Puisque n_k est premier, q divise β' , et cette contradiction démontre le théorème 6.

4. Un lemme sur les zéros de la suite $\varrho(n)$

LEMME 2. Soit $\delta \in \mathbb{N}^*$, et soit $a \in]0, 1[$. On désigne par $p_1 < p_2 < \dots < p_n < \dots$ la suite des nombres premiers de \mathbb{N} qui sont congrus à 3 modulo 4, p_1 étant choisi de façon que

$$(12) \quad \sum_{n=1}^{\infty} \frac{1}{p_n^2} \leq \frac{a}{2}.$$

Alors il existe un entier $m_0 = m_0(a, \delta)$ et une constante L (constante de Linnik, voir théorème 5 ci-dessus) tels que, pour tout $k = p_1 p_2 \dots p_m$, $m \geq m_0$, il existe $n_k \in \mathbb{N}$ tel que,

- (a) $\varrho(n_k - \delta) = \dots = \varrho(n_k - 1) = \varrho(n_k + 1) = \dots = \varrho(n_k + k) = 0$,
- (b) $\varrho(n_k) = 2$,
- (c) $l(n_k - \delta) = \dots = l(n_k) = \dots = l(n_k + k) = 0$,
- (d) $n_k \leq 4^L \exp(4Lp_{2[a/k]})$.

Démonstration. Pour tout $x \in \mathbb{Z}$, et tout nombre premier p , nous notons $\nu_p(x)$ la valuation p -adique de x .

Pour $h \in \mathbb{N}^*$, soit $\mathbb{P}_h = \{p_1, p_2, \dots, p_h\}$.

Pour $m \in \mathbb{N}^*$, notons $k = k(m) = p_1 p_2 \dots p_m$.

Première étape. (a) Soit $\mathbb{M}_m = \{n \in \{1, 2, \dots, k\} : \exists p \in \mathbb{P}_m, \nu_p(n) > 0\}$. En vertu de la formule du crible ([17], p. 22; [12], th. 261, p. 234),

$$\text{card } \mathbb{M}_m = \sum_i \left[\frac{k}{p_i} \right] - \sum_{i \neq j} \left[\frac{k}{p_i p_j} \right] + \dots + (-1)^{m+1} \left[\frac{k}{p_1 p_2 \dots p_m} \right].$$

Or $\nu_p(k) > 0, \forall p \in \mathbb{P}_m$, donc

$$(13) \quad \text{card } \mathbb{M}_m = k - k \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_m}\right).$$

(b) Soit $\mathbb{H}_m = \{n \in \{1, 2, \dots, k\} : \exists p \in \mathbb{P}_m, \nu_p(n) \geq 2\}$. On a

$$\text{card } \mathbb{H}_m \leq \left[\frac{k}{p_1^2} \right] + \left[\frac{k}{p_2^2} \right] + \dots + \left[\frac{k}{p_m^2} \right].$$

En utilisant (12), on obtient

$$\text{card } \mathbb{H}_m \leq k \sum_{i=1}^m \frac{1}{p_i^2} \leq \frac{a}{2} k.$$

(c) Soit $\mathbb{I}_m = \{n \in \{1, 2, \dots, k\} : \exists p \in \mathbb{P}_m, \nu_p(n) = 1\}$. On a $\text{card } \mathbb{I}_m = \text{card } \mathbb{M}_m - \text{card } \mathbb{H}_m$. Donc

$$\text{card } \mathbb{I}_m \geq k \left(1 - \frac{a}{2} - \prod_{i=1}^m \left(1 - \frac{1}{p_i} \right) \right).$$

Mais le produit infini $\prod_{i=1}^{\infty} (1 - 1/p_i)$ diverge vers 0 car la série $\sum_{i=1}^{\infty} 1/p_i$ diverge. Donc il existe un entier $m_1 = m_1(a)$ tel que

$$(14) \quad \forall m \geq m_1, \quad \text{card } \mathbb{I}_m \geq k(1 - a).$$

(d) Il en résulte que, pour $m \geq m_1$, tous les éléments de $\{1, 2, \dots, k\}$ sont divisibles par un facteur $p \in \mathbb{P}_m$ avec un exposant 1 exactement (et ne sont donc pas des sommes de deux carrés, [12], p. 299, th. 366), sauf $N = N(m)$ d'entre eux que nous noterons $u_1 < u_2 < \dots < u_N$, et on a, en vertu de (14),

$$(15) \quad \forall m \geq m_1, \quad N \leq ak.$$

Deuxième étape. (a) Nous construisons maintenant $k = k(m)$ nombres entiers consécutifs $e_m + 1, e_m + 2, \dots, e_m + k$ tels que

$$(16) \quad \forall m \in \mathbb{N}^*, \quad m \geq m_1 \Rightarrow \forall i \in \{1, 2, \dots, k\}, \\ \exists p \in \mathbb{P}_{m+N}, \quad \nu_p(e_m + i) = 1.$$

On procède de la façon suivante : soit d'abord $r_1 \in \mathbb{N}$ tel que

$$(17) \quad 0 \leq r_1 < 2p_{m+1}, \\ \nu_{p_{m+1}}(r_1(p_1 p_2 \dots p_m)^2 + u_1) = 1.$$

Puis soit r_h ($1 \leq h \leq N$) défini par récurrence par

$$(18) \quad 0 \leq r_h < 2p_{m+h}, \\ \nu_{p_{m+h}}(r_h(p_1 p_2 \dots p_{m+h-1})^2 + r_{h-1}(p_1 p_2 \dots p_{m+h-2})^2 + \dots \\ + r_1(p_1 p_2 \dots p_m)^2 + u_h) = 1.$$

Nous posons

$$(19) \quad e_m = r_N(p_1 p_2 \dots p_{m+N-1})^2 + r_{N-1}(p_1 p_2 \dots p_{m+N-2})^2 + \dots \\ + r_1(p_1 p_2 \dots p_m)^2.$$

Soit $i \in \{1, 2, \dots, k\}$. Il est clair par construction que, si $j \in \{1, 2, \dots, m\}$, $e_m + i \equiv i \pmod{p_j^2}$. Donc si $i \in \mathbb{I}_m$, il existe $p \in \mathbb{P}_m$ tel que $\nu_p(e_m + i) = 1$. Si $i \notin \mathbb{I}_m$, il existe $h \in \{1, 2, \dots, N\}$ tel que $i = u_h$; on a alors

$$e_m + i \equiv r_h(p_1 p_2 \dots p_{m+h-1})^2 + \dots + r_1(p_1 p_2 \dots p_m)^2 + u_h \pmod{p_{m+h}^2},$$

donc $\nu_{p_{m+h}}(e_m + i) = 1$ en vertu de (18).

Par conséquent, le nombre e_m défini par (19) vérifie bien (16).

(b) On peut majorer e_m , puisque $r_h < 2p_{m+h}$, $\forall h \in \{1, 2, \dots, N\}$:

$$\begin{aligned} e_m &\leq 2p_{m+N}(p_1 p_2 \dots p_{m+N-1})^2 \\ &\quad + 2p_{m+N-1}(p_1 p_2 \dots p_{m+N-2})^2 + \dots + 2p_{m+1}(p_1 p_2 \dots p_m)^2, \\ e_m &\leq 2(p_1 p_2 \dots p_{m+N})^2 \\ &\quad \times \left(\frac{1}{p_{m+N}} + \frac{1}{p_{m+N-1} p_{m+N}^2} + \dots + \frac{1}{p_{m+1} p_{m+2}^2 \dots p_{m+N}^2} \right), \\ e_m &\leq 2(p_1 p_2 \dots p_{m+N})^2 \left(\frac{1}{3} + \frac{1}{3 \cdot 3^2} + \dots + \frac{1}{3 \cdot 3^{2N-2}} \right). \end{aligned}$$

Donc

$$(20) \quad e_m \leq (p_1 p_2 \dots p_{m+N})^2.$$

Troisième étape. Soit maintenant

$$\mathbb{J}_m = \{j \in \mathbb{N} : \forall i \in \{1, 2, \dots, k\}, \exists p \in \mathbb{P}_{m+N}, \nu_p(j+i) = 1\}.$$

\mathbb{J}_m est non vide puisqu'il contient e_m . Soit q_m le plus petit élément de \mathbb{J}_m . On a alors

$$(21) \quad \begin{aligned} q_m &\leq (p_1 p_2 \dots p_{m+N})^2, \\ \forall p \in \mathbb{P}_{m+N}, \quad \nu_p(q_m) &\neq 1. \end{aligned}$$

Quatrième étape. (a) Notons $v_1 < v_2 < \dots < v_M$ les éléments de $\{1, 2, \dots, \delta\}$ tels que $\forall j \in \{1, 2, \dots, M\}, \forall p \in \mathbb{P}_{m+N}, \nu_p(q_m - v_j) \neq 1$.

On a donc $M \leq \delta$.

De même que dans l'étape 2, nous construisons la suite r'_i par les relations suivantes :

$$(22) \quad \begin{aligned} 0 &\leq r'_1 < 2p_{m+N+1}, \\ \nu_{p_{m+N+1}}(r'_1(p_1 p_2 \dots p_{m+N})^2 + q_m - v_1) &= 1. \end{aligned}$$

Puis par récurrence, pour $1 \leq h \leq M-1$, nous posons

$$(23) \quad \begin{aligned} 0 &\leq r'_h < 2p_{m+N+h}, \\ \nu_{p_{m+N+h}}(r'_h(p_1 p_2 \dots p_{m+N+h-1})^2 + r'_{h-1}(p_1 p_2 \dots p_{m+N+h-2})^2 \\ &\quad + \dots + r'_1(p_1 p_2 \dots p_{m+N})^2 + q_m - v_h) = 1. \end{aligned}$$

Nous imposons à r'_M des conditions supplémentaires; pour cela, nous notons $\mathbb{L}_{m+N} = \{p \in \mathbb{P}_{m+N} : \nu_p(q_m) = 2\}$.

Soit T vérifiant le système de congruences

$$(24) \quad \begin{aligned} T(p_1 p_2 \dots p_{m+N+M-1})^2 + r'_{M-1}(p_1 p_2 \dots p_{m+N+M-2})^2 + \dots \\ + r'_1(p_1 p_2 \dots p_{m+N})^2 + q_m - v_M \equiv 0 \pmod{p_{m+N+M}}, \end{aligned}$$

$$(25) \quad T(p_{m+N+1} p_{m+N+2} \cdots p_{m+N+M-1})^2 \\ + r'_{M-1} (p_{m+N+1} \cdots p_{m+N+M-2})^2 + \cdots + r'_1 \equiv 0 \pmod{p} \\ \text{si } p \in \mathbb{L}_{m+N},$$

$$(26) \quad T(p_{m+N+1} p_{m+N+2} \cdots p_{m+N+M-1})^2 \\ + r'_{M-1} (p_{m+N+1} \cdots p_{m+N+M-2})^2 + \cdots + r'_1 \equiv 1 \pmod{p} \\ \text{si } p \in \mathbb{P}_{m+N} \setminus \mathbb{L}_{m+N}.$$

On sait ([12], th. 121, p. 95) que l'on peut prendre T solution de ce système, et vérifiant

$$0 \leq T \leq p_1 p_2 \cdots p_{m+N} p_{m+N+M}.$$

Soit $H = T(p_1 p_2 \cdots p_{m+N+M-1})^2 + r'_{M-1} (p_1 p_2 \cdots p_{m+N+M-2})^2 + \cdots + r'_1 (p_1 p_2 \cdots p_{m+N})^2 + q_m - v_M$ (voir congruence (24)).

Nous posons $r'_M = T$ si H n'est pas un multiple de p_{m+N+M}^2 , et $r'_M = T + p_1 p_2 \cdots p_{m+N} p_{m+N+M}$ si H est un multiple de p_{m+N+M}^2 .

Il est clair alors que r'_M vérifie les conditions suivantes :

$$(27) \quad \left\{ \begin{array}{l} 0 \leq r'_M \leq 2(p_1 p_2 \cdots p_{m+N} p_{m+N+M}), \\ \nu_{p_{m+N+M}}(r'_M (p_1 p_2 \cdots p_{m+N+M-1})^2 \\ \quad + r'_{M-1} (p_1 p_2 \cdots p_{m+N+M-2})^2 + \cdots \\ \quad + r'_1 (p_1 p_2 \cdots p_{m+N})^2 + q_m - v_M) = 1, \\ \nu_p(r'_M (p_{m+N+1} p_{m+N+2} \cdots p_{m+N+M-1})^2 \\ \quad + r'_{M-1} (p_{m+N+1} \cdots p_{m+N+M-2})^2 + \cdots + r'_1) \geq 1 \\ \quad \text{si } p \in \mathbb{L}_{m+N}, \\ \nu_p(r'_M (p_{m+N+1} p_{m+N+2} \cdots p_{m+N+M-1})^2 \\ \quad + r'_{M-1} (p_{m+N+1} \cdots p_{m+N+M-2})^2 + \cdots + r'_1) = 0 \\ \quad \text{si } p \in \mathbb{P}_{m+N} \setminus \mathbb{L}_{m+N}. \end{array} \right.$$

(b) Posons maintenant

$$(28) \quad t_m = r'_M (p_1 p_2 \cdots p_{m+N+M-1})^2 + r'_{M-1} (p_1 p_2 \cdots p_{m+N+M-2})^2 \\ + \cdots + r'_1 (p_1 p_2 \cdots p_{m+N})^2 + q_m.$$

Par construction,

$$(29) \quad \forall i \in \{-\delta, -\delta + 1, \dots, -1, 1, 2, \dots, k\}, \exists p \in \mathbb{P}_{m+N+M}, \text{ tel que :} \\ \nu_p(t_m + i) = 1.$$

(c) Par ailleurs, en vertu de l'avant-dernière condition de (27) : $\forall p \in \mathbb{L}_{m+N}$, $\nu_p(t_m) = 2$, car on a alors $\nu_p(q_m) = 2$ et $\nu_p(t_m - q_m) \geq 3$.

Si $p \in \mathbb{P}_{m+N} \setminus \mathbb{L}_{m+N}$, deux cas peuvent se produire car $\nu_p(q_m) \neq 1$ grâce à (21) :

(α) $\nu_p(q_m) = 0$, auquel cas $\nu_p(t_m) = 0$.

(β) $\nu_p(q_m) \geq 3$; alors $\nu_p(t_m) = 2$ à cause de la dernière condition de (27) qui implique $\nu_p(t_m - q_m) = 2$.

On a donc $\forall p \in \mathbb{P}_{m+N}$, $\nu_p(t_m) = 0$ ou 2 .

De plus, $\forall m \geq \delta$, $\forall i \in \{m+N+1, \dots, m+N+M\}$, $\nu_{p_i}(t_m) = 0$ car il existe un entier j , $1 \leq j \leq M$, tel que $\nu_{p_i}(t_m - v_j) = 1$.

Finalement, nous avons donc :

$$(30) \quad \text{Pour } m \text{ assez grand, } \forall p \in \mathbb{P}_{m+N+M}, \nu_p(t_m) = 0 \text{ ou } 2.$$

(d) Nous majorons maintenant t_m à partir de (21), (22), (23), (27) :

$$\begin{aligned} t_m &\leq 2(p_1 p_2 \dots p_{m+N} p_{m+N+M})(p_1 p_2 \dots p_{m+N+M-1})^2 \\ &\quad + 2p_{m+N+M-1}(p_1 p_2 \dots p_{m+N+M-2})^2 + \dots \\ &\quad + 2p_{m+N+1}(p_1 p_2 \dots p_{m+N})^2 + (p_1 p_2 \dots p_{m+N})^2. \end{aligned}$$

Donc

$$(31) \quad t_m = o((p_1 p_2 \dots p_{m+N+M})^4).$$

Cinquième étape. (a) Soit maintenant $\eta = \eta(m) \in \{0, 1, 2, 3\}$ tel que

$$(32) \quad \eta(p_1 p_2 \dots p_{m+N+M})^4 + t_m \equiv 1 \pmod{4}.$$

Pour $s \in \mathbb{N}$, considérons

$$(33) \quad w_s = 4(p_1 p_2 \dots p_{m+N+M})^4 s + \eta(p_1 p_2 \dots p_{m+N+M})^4 + t_m.$$

On a d'abord

$$(34) \quad \forall s \in \mathbb{N}, \quad w_s \equiv 1 \pmod{4}.$$

De plus, en vertu de (29),

$$(35) \quad \forall s \in \mathbb{N}, \forall i \in \{-\delta, -\delta+1, \dots, -1, 1, 2, \dots, k\}, \\ \exists p \in \mathbb{P}_{m+N+M}, \quad \nu_p(w_s + i) = 1.$$

(b) Soit D le plus grand diviseur commun à $4(p_1 p_2 \dots p_{m+N+M})^4$ et $\eta(p_1 p_2 \dots p_{m+N+M})^4 + t_m$. En utilisant (30) et (32), on voit que, pour m assez grand,

$$(36) \quad D = \prod_{i=1}^{m+N+M} p_i^{\alpha_i}, \quad \text{avec } \alpha_i = 0 \text{ ou } 2.$$

(c) Posons $w_s = D(\zeta s + \chi)$, avec $(\zeta, \chi) \in \mathbb{N} \times \mathbb{N}$. En vertu de (31), puisque $\eta \in \{0, 1, 2, 3\}$, on a $\chi < \zeta$ pour m assez grand. On peut alors utiliser le théorème 5 : il existe un nombre premier $p(\zeta, \chi)$ et un entier naturel σ tels que

$$(37) \quad w_\sigma = D \cdot p(\zeta, \chi) \leq D \left(\frac{4(p_1 p_2 \dots p_{m+N+M})^4}{D} \right)^L.$$

Nous posons

$$(38) \quad n_k = n_{k(m)} = w_\sigma.$$

Nous avons donc, puisque $L \geq 1$:

$$(39) \quad n_k \leq (4(p_1 p_2 \cdots p_{m+N+M})^4)^L.$$

Par ailleurs, $D \equiv 1 \pmod{4}$ d'après (36), et $n_k \equiv 1 \pmod{4}$ d'après (34) et (38). Ainsi $p(\zeta, \chi) \equiv 1 \pmod{4}$, d'où l'on déduit que $p(\zeta, \chi)$ est une *somme de deux carrés*. De plus, puisque la décomposition de D ne contient que des facteurs premiers qui ne sont pas somme de deux carrés (voir (36)), on a

$$(40) \quad \varrho(n_k) = \varrho[p(\zeta, \chi)] = 2$$

(voir [12], formule (16.9.5) et th. 278, p. 242).

Si nous regroupons (35) et (40), nous obtenons les conclusions (a), (b) et (c) du lemme 2. Il reste à démontrer la majoration (d).

Sixième (et dernière) étape. (a) En utilisant le théorème des nombres premiers dans les suites arithmétiques ([9], p. 70), on obtient

$$(41) \quad m + N + M \sim \frac{1}{2} \frac{p_{m+N+M}}{\log p_{m+N+M}} \quad \text{lorsque } m \rightarrow \infty.$$

Donc

$$(42) \quad m + N + M \leq \frac{p_{m+N+M}}{\log p_{m+N+M}} \quad \text{pour } m \geq m_2.$$

Utilisant (39) et (42), nous obtenons

$$(43) \quad n_k \leq 4^L (p_{m+N+M})^{4L(m+N+M)} \leq 4^L \exp(4L p_{m+N+M}).$$

(b) Mais on a aussi $k = p_1 p_2 \cdots p_m \geq p_1^m$, donc

$$(44) \quad m \leq \frac{\log k}{\log p_1}.$$

Et puisque $M \leq \delta$, utilisant (15) et (44), nous obtenons

$$m + N + M \leq \frac{\log k}{\log p_1} + ak + \delta,$$

si bien que, pour $m \geq m_3$,

$$(45) \quad m + N + M \leq 2[ak].$$

Reportons ce résultat dans (43); nous obtenons

$$n_k \leq 4^L \exp(4L p_{2[ak]}),$$

ce qui achève la démonstration du lemme 2.

5. Démonstration du théorème 1. Supposons qu'il existe $A, B, C \in \mathbb{Z}$, $A \neq 0$, tels que $Ax_q^2 + Bx_q + C = 0$.

Nous allons utiliser le théorème 2 avec $a(n) = A\varrho(n) + Bl(n)$, et montrer que nous aboutissons à une contradiction.

(a) Puisque $A \neq 0$, nous pouvons choisir δ tel que q^δ ne divise pas $2A$. Nous choisissons de plus $a \in]0, 1[$ tel que

$$(46) \quad 32L - \frac{\log |q|}{8a} < 0.$$

(b) Majorons maintenant $|a(n)| \leq |A|\varrho(n) + |B|$. On sait que

$$(47) \quad \varrho(n) \leq d(n) \leq \exp\left(\frac{\log n}{\log \log n}\right)$$

pour n assez grand ([12], p. 262, th. 317 et §18-7, p. 270). Nous pouvons donc écrire $|a(n)| \leq r(n)$, $\forall n \geq n_0$ avec

$$(48) \quad r(n) = \exp\left(\frac{2 \log n}{\log \log n}\right).$$

(c) Nous appliquons le lemme 2, a et δ étant définis ci-dessus. On a

$$(49) \quad n_k + k + 1 \leq 4^L \exp(4Lp_{2[ak]}) + k + 1.$$

Or, en utilisant le théorème des nombres premiers dans les suites arithmétiques, on a, pour k assez grand,

$$(50) \quad \frac{1}{4} \frac{p_{2[ak]}}{\log p_{2[ak]}} \leq 2ak \leq \frac{p_{2[ak]}}{\log p_{2[ak]}}.$$

Pour k assez grand, (49) entraîne donc

$$n_k + k + 1 \leq \exp(8Lp_{2[ak]}).$$

La fonction $x \mapsto \log x / \log \log x$ étant croissante pour $x \geq e^e$, on obtient

$$\log r(n_k + k + 1) = \frac{2 \log(n_k + k + 1)}{\log \log(n_k + k + 1)} \leq \frac{16Lp_{2[ak]}}{\log 8L + \log p_{2[ak]}}.$$

Donc, pour k assez grand,

$$(51) \quad r(n_k + k + 1) \leq \exp\left(32L \frac{p_{2[ak]}}{\log p_{2[ak]}}\right).$$

(d) Posons $x = p_{2[ak]} / \log p_{2[ak]}$. Alors x tend vers l'infini avec k . En utilisant (50) et (51), on obtient

$$\frac{r(n_k + k + 1)}{|q|^k} \leq \frac{\exp(32Lx)}{|q|^{x/(8a)}},$$

d'où

$$\frac{r(n_k + k + 1)}{|q|^k} \leq \exp\left(\left(32L - \frac{\log |q|}{8a}\right)x\right)$$

et puisque a vérifie (46), $\lim_{k \rightarrow \infty} r(n_k + k + 1)/|q|^k = 0$.

(e) Il est clair par ailleurs que $\lim_{n \rightarrow \infty} r(n+1)/r(n) = 1$. Comme $a(n_k + 1) = a(n_k + 2) = \dots = a(n_k + k)$ en vertu du lemme 2, le théorème

2 s'applique, et on obtient, pour $k = k(m)$ assez grand,

$$Cq^{n_k} - \sum_{n=0}^{n_k} a(n)q^{n_k-n} = 0.$$

Utilisant les (a), (b) et (c) du lemme 2, on obtient

$$Cq^{n_k} - 2A - \sum_{n=0}^{n_k-\delta-1} a(n)q^{n_k-n} = 0.$$

On en conclut que $q^{\delta+1}$ divise $2A$, ce qui contredit le choix de δ . Le théorème 1 est donc démontré.

Bibliographie

- [1] P. Borwein, *On the irrationality of certain series*, Math. Proc. Cambridge Philos. Soc. 112 (1992), 141–146.
- [2] P. Bundschuh, *Verschärfung eines arithmetischen Satzes von Tschakaloff*, Portugal. Math. 33 (1) (1974), 1–47.
- [3] —, *Quelques résultats arithmétiques sur les fonctions thêta de Jacobi*, Publications mathématiques de l'Université Pierre et Marie Curie no. 64, Fasc. 1, Groupe d'étude sur les problèmes diophantiens, 1983/84.
- [4] P. Bundschuh and M. Waldschmidt, *Irrationality results for theta functions by Gel'fond–Schneider's method*, Acta Arith. 53 (1989), 289–307.
- [5] K. Chandrasekharan, *Elliptic Functions*, Grundlehren Math. Wiss. 281, Springer, 1985.
- [6] P. Erdős, *Sur l'irrationalité d'une certaine série*, C. R. Acad. Sci. Paris Sér. I 292 (1981), 765–768.
- [7] —, *On the irrationality of certain series: problems and results*, dans : New Advances in Transcendence Theory, A. Baker (ed.), Cambridge University Press, 1988, 102–109.
- [8] H. Exton, *q-Hypergeometric Functions and Applications*, Ellis Horwood, Chichester 1983.
- [9] A. Gel'fond et Y. Linnik, *Méthodes élémentaires dans la théorie analytique des nombres*, Gauthier-Villars, 1965.
- [10] S. Golomb, *A new arithmetic function of combinatorial significance*, J. Number Theory 5 (1973), 218–223.
- [11] S. Graham, *On Linnik's constant*, Acta Arith. 39 (1981), 163–179.
- [12] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Sci. Publ., Oxford Univ. Press, 1989.
- [13] Yu. V. Linnik, *Sur le plus petit nombre premier dans une progression arithmétique*, Mat. Sb. 15 (57) (1944), 139–178 (en russe).
- [14] J. Liouville, *Sur des classes très étendues de quantités dont la valeur n'est ni algébrique ni même réductible à des irrationnelles algébriques*, J. Math. Pures Appl. (1) 16 (1851), 133–142.
- [15] B. Powell and E. Schafer, *Difference between consecutive primes*, Amer. Math. Monthly 91 (1984), 310–311.
- [16] P. Ribenboim, *The Book of Prime Numbers Records*, Springer, 1984.

- [17] H. J. Ryser, *Mathématiques combinatoires*, Dunod, 1969.
- [18] L. Tschakaloff, *Arithmetische Eigenschaften der unendlichen Reihe*
 $\sum_{\nu=0}^{\infty} x^{\nu} a^{-\nu(\nu-1)/2}$, Math. Ann. 80 (1921), 62–74.

24 PLACE DU CONCERT
F-59800 LILLE, FRANCE

Reçu le 19.6.1992
et révisé le 1.12.1992

(2268)