ACTA ARITHMETICA
108.2 (2003)

Une propriété arithmétique des bases additives. Un critère de non-base

par

François Hennecart (Bordeaux)

1. Introduction. En 1994, l'auteur [5] donnait une démonstration à une conjecture orale de F. Dress, selon laquelle il existe une suite $\mathcal{C}$ qui n'est pas une base additive, bien que la suite $\mathcal{C}^{(2)}$ des carrés de ses éléments est une base d'ordre 4. Cela améliorait de façon optimale un résultat antérieur de J.-M. Deshouillers et É. Fouvry [3].

Le résultat ainsi que la structure même de la démonstration ne sont pas remis en cause, mais une obstruction arithmétique, à savoir que le nombre de représentations d'un entier n en somme de 4 carrés ne tend pas vers l'infini lorsque n tend vers l'infini (voir [4]), montre clairement que la Proposition 1 de [5] ne peut se déduire d'une formule asymptotique issue de la méthode du cercle. Cette obstruction se traduit dans cette formule asymptotique par le fait que la série singulière est de l'ordre de $1/n$ si n est un multiple d'une grande puissance de 2. L'erreur commise se situe dans le Lemme 11 de [5] qui ne s'applique pas pour $p = 2$. Nous donnons ici une construction corrigée de la suite $\mathcal{C}$ aux propriétés requises.

L'existence d'une telle suite $\mathcal{C}$ peut paraître étonnant au premier abord, surtout lorsqu'on constate que toute suite est beaucoup plus riche que la suite de ses carrés, si l'on s'en tient à la comparaison des fonctions de comptage respectives. Cependant ce type de paradoxes est fréquent dans la théorie des bases additives, et trouve de nombreuses illustrations notamment dans l'étude des propriétés extrémales des bases : on sait par exemple construire des bases d'ordre h dites économiques, c'est-à-dire dont la fonction de comptage se comporte asymptotiquement comme $cx^{1/h}$ (cf. [7]), alors qu'il existe une suite $\mathcal{A}$ contenant 0 et 1, telle que $\#(\mathcal{A} \cap [1, x]) \gg_\varepsilon x^{1-\varepsilon}$ pour tout $\varepsilon > 0$, qui n'est pas une base. Notons simplement que la répartition des éléments d'une base économique dans toutes les progressions arithmétiques est bien équilibrée, à l'inverse de la répartition des éléments de la suite $\mathcal{A}$.

2000 *Mathematics Subject Classification*: Primary 11B13.

Dans le problème en question, il s'agit donc de trouver une suite $\mathcal{C}$ mal répartie dans les progressions arithmétiques modulo certains modules P, mais dont les carrés des éléments s'y répartissent beaucoup mieux, de sorte que lorsqu'on les additionne 4 par 4, toutes les classes modulo P soient atteintes.

Il y a bien sûr un équilibre à trouver entre la mauvaise répartition de $\mathcal{C}$ et la bonne répartition de la suite des carrés $\mathcal{C}^{(2)} = \{c^2 : c \in \mathcal{C}\}$, les propriétés additives de $\mathcal{C}^{(2)}$ restant cependant intrinsèquement liées à celles de $\mathcal{C}$.

La suite $\mathcal{C}$ aux propriétés requises est sélectionnée parmi les suites qui d'une part satisfont à certaines restrictions arithmétiques (cf. Proposition 1), et d'autre part sont stables par multiplication par toute puissance de 2. Les paramètres sont choisis de telle sorte que la suite $\mathcal{C}^{(2)}$ est une base d'ordre 4 modulo P pour certains modules P du type 2^k (cf. Lemme 2). On montre en dernier lieu que le choix de ces modules conduit, par la méthode du cercle, à la représentation de tout entier n non divisible par 4 comme somme de 4 carrés d'éléments de $\mathcal{C}$, conduisant alors à la même propriété pour les multiples de 4 grâce à la stabilité multiplicative particulière de $\mathcal{C}$.

Le critère de non-base (Proposition 1) est une extension de celui qui fut introduit par J.-M. Deshouillers, P. Erdős et A. Sárközy [2], et établi pour mettre clairement en évidence ces propriétés additives des carrés, et les exploiter efficacement, au contraire de critères antérieurs, notamment ceux dus à Stöhr [8], qui sont tels que, lorsqu'une suite donnée $\mathcal{A}$ satisfait l'un d'eux, celui-ci est automatiquement rempli par la suite des carrés $\mathcal{A}^{(2)}$. Nous montrons ici qu'une suite satisfaisant au critère de [2] augmentée de certains multiples de ses éléments n'est pas une base additive, bien que le critère initial ne s'applique plus.

2. Un critère de non-base. On notera $[x]$ la partie entière du réel x et $\{x\} = x - [x]$ sa partie fractionnaire. Si r est un entier et $\mathcal{B}$ une suite, on note $r \cdot \mathcal{B}$ la suite des nombres rb pour $b \in \mathcal{B}$, la notation $r\mathcal{B}$ étant réservée pour désigner la suite des sommes de r éléments de $\mathcal{B}$.

Le critère de non-base adapté à notre problème est :

PROPOSITION 1. *Soit $\mathcal{C}_0$ une suite d'entiers positifs et $d \geq 1$ un entier. On suppose qu'il existe une suite $(\varepsilon_j)_{j\geq 1}$ de réels strictement positifs qui converge vers 0 lorsque j tend vers $+\infty$, une suite croissante de réels $(N_j)_{j\geq 1}$ et une suite strictement croissante d'entiers positifs $(k_j)_{j\geq 1}$ telles que*

$$c \in \mathcal{C}_0 \text{ et } c \geq N_j \;\Rightarrow\; \{c/d^{k_j}\} \leq \varepsilon_j \quad \text{pour tout } j \geq 1. \tag{1}$$

Alors la suite $\mathcal{C} = \bigcup_{t=0}^{\infty} d^t \cdot \mathcal{C}_0$ n'est pas une base additive.

Démonstration. Nous restreignons notre attention au cas $d = 2$, qui est celui que nous appliquerons dans la suite. La démonstration qui suit s'adapte au cas général sans difficulté. Elle s'inspire de celle de [2, Lemma 1].

Nous allons démontrer par récurrence que pour tout $h \geq 1$, il existe une progression arithmétique de raison une puissance de 2 et de residu impair dont les éléments n'appartiennent pas à $h\mathcal{C}$. On commence par étudier le cas $h = 1$.

Puisque $\varepsilon_j \to 0$ quand $j \to +\infty$, il existe $j_0 \geq 1$ tel que $\varepsilon_{j_0} < 1/2$. Par conséquent tout élément c de $\mathcal{C}_0$ supérieur à N_{j_0} satisfait $\{c/2^{k_{j_0}}\} < 1/2$. Donc $\mathcal{C}_0 \cap [N_{j_0}, +\infty[$ ne contient aucun entier congru à -1 modulo $2^{k_{j_0}}$.

On pose alors $L_1 = \max(k_{j_0}, \lfloor \log N_{j_0}/\log 2 + 1 \rfloor)$. Il s'ensuit que $\mathcal{C}_0$ ne contient aucun entier congru à -1 modulo 2^{L_1}. Il en est clairement de même pour la suite $\mathcal{C}$.

Démontrons par récurrence que pour chaque $h \geq 1$, il existe un entier L_h tel que $h\mathcal{C}$ ne contient aucun entier congru à -1 modulo 2^{L_h}.

Supposons donc cette propriété vérifiée pour $(h-1)\mathcal{C}$, c'est-à-dire que $(h-1)\mathcal{C}$ ne contient aucun entier de la progression $-1 + 2^L \cdot \mathbb{N}^*$, où on a posé $L = L_{h-1}$.

Par hypothèse, on peut extraire par récurrence une suite d'entiers strictement positifs $\sigma(1) < \ldots < \sigma(h+1)$ telle que

$$\varepsilon_{\sigma(j)} < \frac{1}{2^L h} \quad \text{pour } j = 1, \ldots, h+1, \tag{2}$$

et

$$\frac{2^{k_{\sigma(j+1)}}}{2^L h} \geq N_{\sigma(j)} \quad \text{pour } j = 1, \ldots, h. \tag{3}$$

On pose $L_h = \max(L, k_{\sigma(h+1)})$. Soit m un entier positif satisfaisant à la congruence

$$m \equiv -1 \bmod 2^{L_h}. \tag{4}$$

Supposons par l'absurde que m est dans $h\mathcal{C}$; alors il existe $c_1, \ldots, c_h$ dans $\mathcal{C}_0$ et des entiers $\alpha_1, \ldots, \alpha_h \geq 0$ tels que

$$m = 2^{\alpha_1} c_1 + \ldots + 2^{\alpha_h} c_h.$$

On peut supposer dans cette écriture que

$$c_1 \geq \ldots \geq c_h. \tag{5}$$

Si pour un certain j, on a $\alpha_j \geq L$, alors l'entier $m - 2^{\alpha_j} c_j$ appartiendrait à $(h-1)\mathcal{C}$ et serait congru à -1 modulo 2^L. Contradiction.

Donc pour tout $j = 1, \ldots, h$, on a $\alpha_j \leq L-1$. Démontrons par récurrence que pour $j = 0, 1, \ldots, h$, on a

$$m - \sum_{\nu=1}^{j} 2^{\alpha_\nu} c_\nu \geq \frac{2^{k_{\sigma(h-j+1)}}}{2}, \tag{6}$$

ce qui conduira à une contradiction pour $j = h$, le second membre de (6) étant strictement positif.

Pour $j=0$, on a grâce à (4), $m \geq 2^{k_{\sigma(h+1)}}-1 \geq 2^{k_{\sigma(h+1)}-1}$. On suppose que (6) est vérifiée pour un certain $j \leq h-1$. On a donc

$$\sum_{\nu=j+1}^{h} 2^{\alpha_\nu} c_\nu = m - \sum_{\nu=1}^{j} 2^{\alpha_\nu} c_\nu \geq \frac{2^{k_{\sigma(h-j+1)}}}{2},$$

donc puisque $\alpha_\nu \leq L-1$ pour chaque ν,

$$\sum_{\nu=j+1}^{h} c_\nu \geq \frac{2^{k_{\sigma(h-j+1)}}}{2^L},$$

impliquant, grâce à la condition (5),

$$c_1 \geq \ldots \geq c_{j+1} \geq \frac{2^{k_{\sigma(h-j+1)}}}{2^L h}.$$

Par (3), on obtient que $c_\nu \geq N_{\sigma(h-j)}$, $\nu = 1, \ldots, j+1$, d'où par (1) et (2), on a

$$\left\{ \frac{c_\nu}{2^{k_{\sigma(h-j)}}} \right\} \leq \varepsilon_{\sigma(h-j)} < \frac{1}{2^L h}, \quad \nu = 1, \ldots, j+1.$$

Par suite

$$\left\{ \frac{2^{\alpha_\nu} c_\nu}{2^{k_{\sigma(h-j)}}} \right\} < \frac{1}{2h}, \quad \nu = 1, \ldots, j+1.$$

Cela donne

$$\left\{ \frac{\sum_{\nu=1}^{j+1} 2^{\alpha_\nu} c_\nu}{2^{k_{\sigma(h-j)}}} \right\} < \frac{1}{2}.$$

Ainsi, puisque par (4), $m \equiv -1 \bmod 2^{k_{\sigma(h-j)}}$, on obtient

$$m - \sum_{\nu=1}^{j+1} 2^{\alpha_\nu} c_\nu \geq 2^{k_{\sigma(h-j)}} - 1 - (2^{k_{\sigma(h-j)}-1} - 1) = \frac{2^{k_{\sigma(h-j)}}}{2},$$

démontrant la relation (6) au rang $j+1$.

La contradiction obtenue montre qu'aucun entier congru à -1 modulo 2^{L_h} n'est dans $h\mathcal{C}$. Cela étant vrai pour tout $h \geq 1$, on déduit que $\mathcal{C}$ n'est pas une base additive. ∎

3. Propriétés des suites et de leurs carrés. Dans cette section, nous présentons la démonstration corrigée du résultat

THÉORÈME (cf. [5]). *Il existe une suite d'entiers $\mathcal{C}$ qui n'est pas une base additive alors que les carrés de ses éléments forment une base d'ordre* 4.

Nous ne donnons pas tous les détails de la démonstration, qui restent principalement inchangés. Néanmoins, pour se placer en position d'appliquer

la Proposition 1, nous devons aménager cette démonstration. Il nous semble donc nécessaire de repréciser le problème et aussi de rappeler quelques notations.

3.1. *Préliminaires.* La démonstration s'appuie sur le critère de non-base décrit dans la section précédente, et la méthode du cercle dans sa variante dûe à Kloosterman [6]. Nous décrivons brièvement ce dont il s'agit.

Pour un entier n d'une progression arithmétique fixée de raison $2P$ (on prendra $P = 2^k$), et un quadruplet $\mathbf{h} = (h_1, h_2, h_3, h_4)$ tel que

$$n \equiv h_1^2 + h_2^2 + h_3^2 + h_4^2 \bmod 2P, \tag{7}$$

on s'intéresse au nombre $R_\gamma(n, \mathbf{h}, P)$ de représentations de n sous la forme

$$n = \sum_{j=1}^{4} (h_j + y_j P)^2, \tag{8}$$

chaque représentation (y_1, y_2, y_3, y_4) étant affectée d'un poids induit par la fonction γ à support $]0,1[$ et définie par $\gamma(t) = \exp(-1/t(t-1))$ sur $]0,1[$. Plus précisément, posons comme dans [5], $N = [\sqrt{n}\,]$ et

$$f_{h_i}(\alpha) = \sum_{x \equiv h_i \bmod P} \gamma\Big(\frac{x}{N}\Big) \mathrm{e}(\alpha x^2), \qquad 1 \le i \le 4,$$

où $\mathrm{e}(u) = \exp(2i\pi u)$. On a

$$R(n) = R_\gamma(n, \mathbf{h}, P) = \int_0^1 \Big(\prod_{i=1}^{4} f_{h_i}(\alpha) \Big) \mathrm{e}(-\alpha n)\, d\alpha.$$

On obtient (cf. [5, équation (51)]) pour tout $\varepsilon > 0$ la formule asymptotique

$$R(n) = n \mathfrak{S}(n, \mathbf{h}, P) \mathcal{I}_\gamma + O_\varepsilon(n^{3/4+\varepsilon}), \tag{9}$$

où l'intégrale singulière

$$\mathcal{I}_\gamma = \int_{-\infty}^{+\infty} \Big(\int_0^1 \gamma(u) \mathrm{e}(wu^2)\, du \Big)^4 \mathrm{e}(-w)\, dw$$

est indépendante de n et satisfait

$$\mathcal{I}_\gamma > 0. \tag{10}$$

La série singulière

$$\mathfrak{S}(n, \mathbf{h}, P) = \sum_{q=1}^{\infty} \sum_{\substack{s=1 \\ (s,q)=1}}^{q} \frac{1}{P^4 q^4} \Big(\prod_{i=1}^{4} \Big(\sum_{\substack{x=1 \\ x \equiv h_i \bmod P}}^{Pq} \mathrm{e}\Big(\frac{sx^2}{q}\Big) \Big) \Big) \mathrm{e}\Big(-\frac{sn}{q}\Big)$$

est absolument convergente d'où, par multiplicativité, se développe en produit eulérien

$$\mathfrak{S}(n,\mathbf{h},P)=P^{-4}\prod_{p\,\text{premier}}\chi_p(n,\mathbf{h},P), \tag{11}$$

où

$$\chi_p(n,\mathbf{h},P)=\sum_{l\geq 0}\sum_{\substack{s=1\\ p\nmid s}}^{p^l}\frac{1}{p^{4l}}\Bigg(\prod_{i=1}^{4}\Bigg(\sum_{\substack{x=1\\ x\equiv h_i \bmod P}}^{Pp^l}\mathrm{e}\Big(\frac{sx^2}{p^l}\Big)\Bigg)\Bigg)\mathrm{e}\Big(-\frac{sn}{p^l}\Big).$$

Nous étudierons au paragraphe 3.3 chacun de ces facteurs dans le but de montrer que la série singulière satisfait

$$\mathfrak{S}(n,\mathbf{h},2^k)>c, \tag{12}$$

où $c=c(k)>0$ est une constante indépendante de n telle que $4\nmid n$.

Il est facile de voir que $\mathfrak{S}(n,\mathbf{h},2^k)$ ne se distingue (au facteur P^{-4} près) de la série singulière $\mathfrak{S}_4(n)=\mathfrak{S}(n,\mathbf{0},1)=\prod_p\chi_p(n)$ liée au problème standard de la représentation de n en somme de 4 carrés que par leur comportement local respectif en chaque nombre premier p divisant P, en l'occurrence ici $p=2$. On a en effet

$$\begin{aligned}\chi_p(n,\mathbf{h},2^k)&=\chi_p(n)\\ &=\sum_{l\geq 0}\sum_{\substack{s=1\\ p\nmid s}}^{p^l}\frac{1}{p^{4l}}\Bigg(\sum_{x=1}^{p^l}\mathrm{e}\Big(\frac{sx^2}{p^l}\Big)\Bigg)^4\mathrm{e}\Big(-\frac{sn}{p^l}\Big)\quad\text{si } p\neq 2.\end{aligned} \tag{13}$$

Or la série $\mathfrak{S}_4(n)$ a le désagréable défaut de pouvoir être très petite, et notamment lorsque n est une grande puissance de 2. On se rend compte que pour ces entiers n, $\mathfrak{S}_4(n)$ (ainsi que $\mathfrak{S}(n,\mathbf{h},P)$) peut être de l'ordre de $1/n$, rendant inutilisable la formule asymptotique (9). La formule exacte donnant le nombre exacte de représentations de n en somme de 4 carrés d'entiers relatifs $r_4(n)=8\sum_{d|n,\,4\nmid d}d$ montre que toute puissance de 2 supérieure à 2 possède exactement 24 représentations. Ce nombre $r_4(n)$ ne tend donc pas vers l'infini lorsque n tend vers l'infini, rendant vain tout espoir d'obtenir par la méthode du cercle un équivalent asymptotique pour $r_4(n)$ (donc pour $R(n)$) valable pour tout n, le terme reste étant évalué indépendamment des particularités arithmétiques de n.

Par contre, lorsqu'on se restreint aux entiers non divisible par 4, ou par toute autre puissance de 2 fixée, la formule (9) fournit grâce à (10) et (12) un équivalent asymptotique pour $R(n)$, dont on déduit pour n assez grand, non multiple de 4 et satisfaisant (7), l'existence d'une représentation du type (8).

Dans le paragraphe qui suit, nous montrons que chaque classe h_0 modulo $P=2^k$, non multiple de 4, admet au moins une représentation $h_0\equiv h_1^2+h_2^2+$

$h_3^2 + h_4^2 \bmod 2^{k+1}$, les h_i, $1 \le i \le 4$, appartenant à une sélection adéquate de classes modulo 2^k.

3.2. *Représentation d'un entier en somme de 4 carrés de résidus pour certains modules.* On définit les suites $(\varepsilon_j)_{j\ge1}$ et $(k_j)_{j\ge1}$ par

$$k_0 = 0, \quad k_j = 16^j \qquad (j \ge 1), \tag{14}$$

$$\varepsilon_1 = 1, \quad \varepsilon_j = \frac{4k_j}{2^{k_j/8}} \quad (j \ge 2), \tag{15}$$

et on pose

$$\mathcal{C}_j = \Big\{ m = \sum_{\nu=1}^{j} u_\nu 2^{k_{\nu-1}} + w2^{k_j} : \\ w \ge 0 \text{ et } 0 \le u_\nu < \varepsilon_\nu 2^{k_\nu - k_{\nu-1}} \ (\nu = 1, \dots, j) \Big\}. \tag{16}$$

Observons tout de suite que si $m \in \mathcal{C}_j$, alors

$$\left\{ \frac{m}{2^{k_j}} \right\} \le \sum_{\nu=1}^{j} \varepsilon_\nu 2^{k_\nu - k_j} \le \frac{16}{15}\,\varepsilon_j. \tag{17}$$

Notons aussi que la suite $(\mathcal{C}_j)_{j\ge1}$ est décroissante, ce qui s'avèrera essentiel lors de la construction finale de $\mathcal{C}_0$.

Le lemme qui suit est comparable au Lemme 3 de [5] dans sa forme et sa démonstration. La différence principale est que là où nous considérions pour modules une suite croissante de nombres premiers, nous prenons la suite $(2^{k_j})_{j\ge1}$ de certaines puissances de 2. L'argument de coprimalité des modules n'étant ici plus applicable, nous sommes donc conduits à considérer les suites $\mathcal{C}_j$ dont les éléments satisfont plusieurs conditions arithmétiques liées, mais suffisamment indépendantes grâce au choix des suites $(\varepsilon_j)_{j\ge1}$ et $(k_j)_{j\ge1}$.

LEMME 2. *Soit $j \ge 1$. Tout entier n non divisible par 4 admet au moins une solution $\mathbf{h} = (h_1, h_2, h_3, h_4) \in \mathcal{C}_j^4$ à la congruence*

$$n \equiv h_1^2 + h_2^2 + h_3^2 + h_4^2 \bmod 2^{k_j+1}. \tag{18}$$

Il est important de noter ici que l'on recherche des solutions à une congruence modulo 2^{k_j+1} alors que les h_i, $1 \le i \le 4$, sont assujettis à des conditions arithmétiques modulo 2^{k_ν}, $\nu = 1, \dots, j$. Comme on le verra, ce point sera décisif lorsqu'on étudiera le facteur $\chi_2(n, \mathbf{h}, 2^{k_j})$ de la série singulière.

Démonstration du Lemme 2. On note $k = k_j$ et on désigne par $\varrho_j(n)$ le nombre normalisé de solutions $\mathbf{h}$ à la congruence (18), lorsque les h_i,

$1 \le i \le 4$, décrivent l'ensemble $\mathcal{C}_j \cap [1, 2^{k+1}]$, c'est-à-dire

$$\varrho_j(n) = \sum_{a=1}^{2^{k+1}} \left(\frac{T(a, 2^{k+1})}{2^{k+1}}\right)^4 \mathrm{e}\left(-\frac{an}{2^{k+1}}\right) = \sum_{l=0}^{k+1} \sum_{\substack{a=1 \\ 2\nmid a}}^{2^l} \left(\frac{T(2^{k+1-l}a, 2^{k+1})}{2^{k+1}}\right)^4 \mathrm{e}\left(-\frac{an}{2^l}\right) \tag{19}$$

où on a posé

$$T(a, 2^{k+1}) = \sum_{\substack{h=1 \\ h\in\mathcal{C}_j}}^{2^{k+1}} \mathrm{e}\left(\frac{ah^2}{2^{k+1}}\right).$$

On note

$$S(a, v, 2^l) = \sum_{h=1}^{2^l} \mathrm{e}\left(\frac{ah^2 + vh}{2^l}\right).$$

Cette somme de Gauss est évaluée de manière classique après avoir remarqué que :

• Si $2\nmid v$ et $2 \mid a$ alors l'application $h \mapsto ah^2 + vh$ est une permutation de l'ensemble des résidus modulo 2^l. Donc pour $l \ge 1$, on a $S(a, v, 2^l) = 0$.

• Si $2\nmid va$ et $l \ge 1$ alors l'application $h \mapsto ah^2 + vh$ est, d'une part, une permutation de l'ensemble des résidus non inversibles modulo 2^l, et d'autre part, une bijection de l'ensemble des résidus inversibles modulo 2^l sur l'ensemble des résidus non inversibles modulo 2^l. Par conséquent $S(a, v, 2^l) = 2\sum_{h=1}^{2^{l-1}} \mathrm{e}(h/2^{l-1})$, qui vaut 0 si $l \ge 2$ et 2 si $l = 1$,

• Si $2 \mid v$ et $2\nmid a$, alors $|S(a, v, 2^l)|^2 = |S(a, 0, 2^l)|^2 = 2^{l+1}$ si $l \ge 2$ et 0 si $l = 1$, en utilisant les évaluations classiques des sommes de Gauss quadratiques (cf. [1, Théorème 4.15, p. 315]).

On obtient donc les estimations suivantes :

$$|S(a, v, 2^l)| = \begin{cases} 0 & \text{si } 2^\alpha \parallel a,\ 2^{\alpha+1}\nmid v \text{ et } l \ge \alpha + 2, \\ 2^{(l+\alpha+1)/2} & \text{si } 2^\alpha \parallel a,\ 2^{\alpha+1} \mid v \text{ et } l \ge \alpha + 2. \end{cases} \tag{20}$$

On pose $E_j = \mathcal{C}_j \cup [0, 2^k - 1]$. On a donc

$$\frac{1}{2^k} \sum_{u\in E_j} \sum_{v=-2^{k-1}+1}^{2^{k-1}} \mathrm{e}\left(\frac{v(h-u)}{2^k}\right) = \begin{cases} 1 & \text{si } h \in \mathcal{C}_j, \\ 0 & \text{sinon,} \end{cases}$$

ce qui conduit à

$$T(2^{k+1-l}a, 2^{k+1}) = \frac{1}{2^k} \sum_{v=-2^{k-1}+1}^{2^{k-1}} \sum_{u\in E_j} \mathrm{e}\left(-\frac{uv}{2^k}\right) S(2^{k+1-l}a, 2v, 2^{k+1}). \tag{21}$$

On a donc pour $l \in \{2, \dots, k+1\}$ et $2 \nmid a$,

$$
\begin{aligned}
(22)\qquad |T(2^{k+1-l}a, 2^{k+1})| &\le \frac{1}{2^k} \sum_{v=-2^{k-1}+1}^{2^{k-1}} \Big| \sum_{u\in E_j} \mathrm{e}\Big(-\frac{uv}{2^k}\Big)\Big| |S(2^{k+1-l}a, 2v, 2^{k+1})| \\
&= \frac{1}{2^k} \sum_{\substack{v=-2^{k-1}+1 \\ 2^{k+1-l}\mid v}}^{2^{k-1}} \Big| \sum_{u\in E_j} \mathrm{e}\Big(-\frac{uv}{2^k}\Big)\Big| 2^{k+(3-l)/2} \qquad \text{(cf. (20))} \\
&= 2^{(3-l)/2} \sum_{v=-2^{l-2}+1}^{2^{l-2}} \Big| \sum_{u\in E_j} \mathrm{e}\Big(-\frac{uv}{2^{l-1}}\Big)\Big|.
\end{aligned}
$$

Puisque $\sum_{t=1}^{\nu} \varepsilon_t 2^{k_t} < 2^{k_\nu+1}$ pour tout $\nu \ge 1$, chaque élément $u \in E_j$ possède une unique représentation sous la forme $u = u_1 + u_2 2^{k_1} + u_3 2^{k_2} + \ldots + u_j 2^{k_{j-1}}$ où $0 \le u_t < \varepsilon_t 2^{k_t - k_{t-1}}$, $1 \le t \le j$. On obtient donc

$$
(23)\qquad \sum_{u\in E_j} \mathrm{e}\Big(-\frac{uv}{2^{l-1}}\Big) = \prod_{t=1}^{j} \Big(\sum_{u_t=0}^{\varepsilon_t 2^{k_t-k_{t-1}-1}} \mathrm{e}\Big(-\frac{u_t v}{2^{l-1-k_{t-1}}}\Big)\Big).
$$

On suppose $l \ge k_1 + 1$. Il existe $\nu \in \{2, \dots, j\}$ tel que $k_{\nu-1} + 1 \le l \le k_\nu + 1$. Pour majorer $T(2^{k+1-l}a, 2^{k+1})$, nous allons distinguer deux cas selon que $7k_\nu/8 + 4\nu + 2 \le l \le k_\nu + 1$ ou que $k_{\nu-1} + 1 \le l \le 7k_\nu/8 + 4\nu + 2$.

Premier cas : $7k_\nu/8 + 4\nu + 2 \le l \le k_\nu + 1$. On a alors

$$
(24)\qquad \varepsilon_\nu 2^{k_\nu} \le 2^l.
$$

Les sommes sur $u_1, \dots, u_{\nu-1}, u_{\nu+1}, \dots, u_j$ dans (23) se majorent par leurs nombres respectifs de termes. En ce qui concerne la somme sur v, on écrit d'abord $v = x + 2^{l-1-k_{\nu-1}} y$; on obtient

$$
\begin{aligned}
&\sum_{v=-2^{l-2}+1}^{2^{l-2}} \Big| \sum_{u_\nu=0}^{\varepsilon_\nu 2^{k_\nu-k_{\nu-1}-1}} \mathrm{e}\Big(-\frac{u_\nu v}{2^{l-1-k_{\nu-1}}}\Big)\Big| \\
&\qquad = 2^{k_{\nu-1}} \sum_{x=-2^{l-2-k_{\nu-1}}+1}^{2^{l-2-k_{\nu-1}}} \Big| \sum_{u_\nu=0}^{\varepsilon_\nu 2^{k_\nu-k_{\nu-1}-1}} \mathrm{e}\Big(-\frac{u_\nu x}{2^{l-1-k_{\nu-1}}}\Big)\Big|.
\end{aligned}
$$

On utilise alors successivement les deux inégalités suivantes

$$
(25)\qquad \Big| \sum_{X\le q\le Y} \mathrm{e}(\theta q)\Big| \le \frac{1}{2\theta}, \qquad \theta \in]0, 1/2],
$$

et

$$\sum_{q=1}^{X}\frac{1}{q}\le \log X+1 \tag{26}$$

pour obtenir, en isolant le terme de la somme relatif à $x=0$ et en tenant compte de la condition (24),

$$\begin{aligned}\sum_{v=-2^{l-2}+1}^{2^{l-2}}&\left|\sum_{u_\nu=0}^{\varepsilon_\nu 2^{k_\nu-k_{\nu-1}}-1}\mathrm{e}\Big(-\frac{u_\nu v}{2^{l-1-k_{\nu-1}}}\Big)\right|\\ &\le 2^{k_{\nu-1}}\left(\varepsilon_\nu 2^{k_\nu-k_{\nu-1}}+\sum_{x=1}^{2^{l-2-k_{\nu-1}}}\left(\frac{x}{2^{l-1-k_{\nu-1}}}\right)^{-1}\right)\\ &\le 2^{k_{\nu-1}}(\varepsilon_\nu 2^{k_\nu-k_{\nu-1}}+(l-2)2^{l-k_{\nu-1}-1})\le (l-1)2^l\le k_\nu 2^l.\end{aligned}$$

Cela donne, en notant $\varepsilon=\varepsilon_1\dots\varepsilon_j$ et en utilisant (22), (14) et (15),

$$|T(2^{k+1-l}a,2^{k+1})|\le \varepsilon 2^k k_\nu 2^{(3+l)/2}2^{k_{\nu-1}-k_\nu}\varepsilon_\nu^{-1}=\varepsilon 2^k 2^{(l-1)/2}2^{-13k_\nu/16},$$

ce qui conduit à

$$\sum_{\substack{a=1\\2\nmid a}}^{2^l}\left|\frac{T(2^{k+1-l}a,2^{k+1})}{2^{k+1}}\right|^4\le \varepsilon^4 2^{3l-7}2^{-13k_\nu/4},$$

puis à

$$\sum_{l=7k_\nu/8+4\nu+2}^{k_\nu+1}\sum_{\substack{a=1\\2\nmid a}}^{2^l}\left|\frac{T(2^{k+1-l}a,2^{k+1})}{2^{k+1}}\right|^4\le \varepsilon^4 2^{-k_\nu/4-1}. \tag{27}$$

Second cas : $k_{\nu-1}+1\le l\le 7k_\nu/8+4\nu+2$. On a $2^{l-1-k_{\nu-1}}\mid \varepsilon_\nu 2^{k_\nu-k_{\nu-1}}$, d'où la somme sur u_ν dans (23) est nulle si $2^{l-1-k_{\nu-1}}\nmid v$ et vaut $\varepsilon_\nu 2^{k_\nu-k_{\nu-1}}$ sinon. Dans la décomposition (23), on majore trivialement les sommes sur $u_1,\dots,u_{\nu-2},u_{\nu+1},\dots,u_j$ par leurs nombres de termes. On a donc

$$\begin{aligned}\sum_{v=-2^{l-2}+1}^{2^{l-2}}&\left|\sum_{u\in E_j}\mathrm{e}\Big(-\frac{uv}{2^{l-1}}\Big)\right|\\ &\le \varepsilon\varepsilon_{\nu-1}^{-1}2^{k+k_{\nu-2}-k_{\nu-1}}\sum_{v=-2^{k_{\nu-1}-1-1}+1}^{2^{k_{\nu-1}-1}}\left|\sum_{u_{\nu-1}=0}^{\varepsilon_{\nu-1}2^{k_{\nu-1}-k_{\nu-2}}-1}\mathrm{e}\Big(-\frac{u_{\nu-1}v}{2^{k_{\nu-1}-k_{\nu-2}}}\Big)\right|.\end{aligned}$$

On écrit $v=x+2^{k_{\nu-1}-k_{\nu-2}}y$, la somme sur v du membre de droite vaut

donc

$$2^{k_{\nu-2}} \sum_{x=-2^{k_{\nu-1}-k_{\nu-2}-1}+1}^{2^{k_{\nu-1}-k_{\nu-2}-1}} \left| \sum_{u_{\nu-1}=0}^{\varepsilon_{\nu-1}2^{k_{\nu-1}-k_{\nu-2}}-1} \mathrm{e}\Big(-\frac{u_{\nu-1}x}{2^{k_{\nu-1}-k_{\nu-2}}}\Big)\right|,$$

que l'on majore, en utilisant à nouveau (25) et (26), par

$$2^{k_{\nu-2}}(\varepsilon_{\nu-1}2^{k_{\nu-1}-k_{\nu-2}} + k_{\nu-1}2^{k_{\nu-1}-k_{\nu-2}}) \le k_{\nu-1}2^{k_{\nu-1}+1}.$$

Grâce à (14), (15) et (22), on obtient

$$|T(2^{k+1-l}a, 2^{k+1})| \le \varepsilon 2^{k+(1-l)/2+3k_{\nu-1}/16},$$

puis

$$\sum_{\substack{a=1\\2\nmid a}}^{2^l} \left|\frac{T(2^{k+1-l}a, 2^{k+1})}{2^{k+1}}\right|^4 \le \varepsilon^4 2^{-l-3+3k_{\nu-1}/4},$$

et enfin

$$\sum_{l=k_{\nu-1}+1}^{7k_\nu/8+4\nu+2} \sum_{\substack{a=1\\2\nmid a}}^{2^l} \left|\frac{T(2^{k+1-l}a, 2^{k+1})}{2^{k+1}}\right|^4 \le \varepsilon^4 2^{-k_{\nu-1}/4-3}. \tag{28}$$

Il vient alors, avec (27), (28) et (14),

$$\sum_{l=k_1+1}^{k+1} \sum_{\substack{a=1\\2\nmid a}}^{2^l} \left|\frac{T(2^{k+1-l}a, 2^{k+1})}{2^{k+1}}\right|^4 \le \varepsilon^4 \sum_{\nu\ge 2}(2^{-k_{\nu-1}/4-3} + 2^{-k_\nu/4-1}) \le \frac{\varepsilon^4}{4}, \tag{29}$$

d'où, par (19),

$$\varrho_j(n) \ge \sum_{l=0}^{16} \sum_{\substack{a=1\\2\nmid a}}^{2^l} \left(\frac{T(2^{k+1-l}a, 2^{k+1})}{2^{k+1}}\right)^4 \mathrm{e}\Big(-\frac{an}{2^l}\Big) - \frac{\varepsilon^4}{4}. \tag{30}$$

On aura observé au préalable que la somme sur l dans (30) qui est, au facteur 2^{-4k} près, le nombre de solutions à la congruence $n \equiv x_1^2+x_2^2+x_3^2+x_4^2 \bmod 2^{16}$, $x_1, x_2, x_3, x_4 \in E_j$, est effectivement un nombre réel.

Soit a impair et l tel que $1 \le l \le k$. On a classiquement

$$S(2^{k+1-l}a, 2v, 2^{k+1}) = \begin{cases} 2^{k+1-l}S(a, v/2^{k-l}, 2^l) & \text{si } 2^{k-l} \mid v,\\ 0 & \text{sinon.}\end{cases} \tag{31}$$

Supposons $l \le k_1 = 16$. Puisque $\varepsilon_1 = 1$, l'ensemble E_j est la réunion disjointe d'un nombre entier d'intervalles de longueur 2^l, donc lorsque $2^{k-l} \mid v$,

on a

$$\sum_{u\in E_j} \mathrm{e}\Big(-\frac{uv}{2^k}\Big) = \sum_{u\in E_j} \mathrm{e}\Big(-\frac{u(v/2^{k-l})}{2^l}\Big) = \begin{cases} \#E_j = \varepsilon 2^k & \text{si } 2^k \mid v,\\ 0 & \text{sinon,}\end{cases}$$

et par suite, on obtient, avec (21) et (31),

$$\begin{aligned}(32)\quad T(2^{k+1-l}a, 2^{k+1}) &= \frac{1}{2^k} \sum_{\substack{v=-2^{k-1}+1\\ 2^{k-l}\mid v}}^{2^{k-1}} \sum_{u\in E_j} \mathrm{e}\Big(-\frac{u(v/2^{k-l})}{2^l}\Big) 2^{k+1-l} S(a, v/2^{k-l}, 2^l)\\ &= \frac{\varepsilon 2^{k+1}}{2^l}\, S(a,0,2^l).\end{aligned}$$

On déduit de [1, Théorème 4.15, p. 315] que $S(1,0,2) = 0$, et $(S(a,0,2^l))^4 = -4^{l+1}$ pour tout $l \geq 2$ et a est impair. Cela donne, avec (30) et (32),

$$\varrho_j(n) \geq \frac{3}{4}\varepsilon^4 - \varepsilon^4 \sum_{l=2}^{16} 4^{1-l} \sum_{\substack{a=1\\ 2\nmid a}}^{2^l} \mathrm{e}\Big(-\frac{an}{2^l}\Big).$$

Puisque $4\nmid n$ la somme de Ramanujan est nulle pour $l \geq 3$. Pour $l = 2$ elle vaut 0 ou $-1/2$ selon que $2\nmid n$ ou $2 \parallel n$, donc $\varrho_j(n) \geq 3\varepsilon^4/4 > 0$. Cela termine la démonstration du Lemme 2. ∎

3.3. *Une suite dont la suite des carrés est une base d'ordre* 4. On montre d'abord

Proposition 3. *Soit $j \geq 1$. Tout entier n assez grand non multiple de* 4 *est la somme de* 4 *carrés d'éléments de $\mathcal{C}_j$.*

Démonstration. La démonstration s'effectue de la même manière que dans l'article [5] dont on reprend les notations avec $P = 2^k$ où $k = k_j$.

Soit n un entier tel que $4\nmid n$. D'après le Lemme 2, il existe un quadruplet (h_1, h_2, h_3, h_4) d'éléments de $\mathcal{C}_j$ tel que $n \equiv h_1^2 + h_2^2 + h_3^2 + h_4^2 \bmod 2^{k+1}$.

L'étude du terme reste est inchangée, ce qui conduit à la formule asymptotique (9). Il s'agit donc de justifier la minoration (12) de la série singulière.

Pour $l \geq k+1$, on note $M(2^l)$ le nombre de solutions satisfaisant

$$\begin{cases} n \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \bmod 2^l,\\ x_j \equiv h_j \bmod 2^k, \quad 1 \leq j \leq 4,\\ 1 \leq x_1, x_2, x_3, x_4 \leq 2^{l+k}.\end{cases}$$

En écrivant $x_j = h_j + 2^k y_j$, $1 \leq j \leq 4$, $M(2^l)$ est encore le nombre de solutions de la congruence

$$\begin{cases} n - h_1^2 + h_2^2 + h_3^2 + h_4^2 \equiv 2^{k+1} \sum_{j=1}^4 (2^{k-1} y_j^2 + h_j y_j) \bmod 2^l, \\ 1 \le y_1, y_2, y_3, y_4 \le 2^l. \end{cases}$$

En notant $2^{k+1}m$ le membre de gauche de la congruence ci-dessus, $M(2^l)$ désigne encore le nombre de solutions de

$$\begin{cases} m \equiv \sum_{j=1}^4 (2^{k-1} y_j^2 + h_j y_j) \bmod 2^{l-k-1}, \\ 1 \le y_1, y_2, y_3, y_4 \le 2^l. \end{cases}$$

Puisque $4 \nmid n$, on peut supposer que $2 \nmid h_1$. D'où l'application $y_1 \mapsto 2^{k-1} y_1^2 + h_1 y_1$ est une permutation de l'ensemble des résidus modulo 2^{l-k-1} si $k \ge 2$. Un choix quelconque du triplet (y_2, y_3, y_4) conduit donc à 2^{k+1} solutions à ce système. Par suite

$$\chi_2(n, \mathbf{h}, 2^k) = \lim_{l \to \infty} \frac{M(2^l)}{2^{3l}} = 2^{k+1}. \tag{33}$$

Soit p un nombre premier impair. De (13) et des évaluations des sommes gaussiennes quadratiques fournies dans [1, Théorème 4.15, p. 315] on déduit, pour $p^\alpha \parallel n$,

$$\chi_p(n) = 1 + \sum_{l \ge 1} \frac{1}{p^{2l}} \sum_{\substack{s=1 \\ p \nmid s}}^{p^l} \mathrm{e}\left(-\frac{sn}{p^l}\right) = 1 + \frac{1}{p} - \frac{1}{p^{\alpha+1}} - \frac{1}{p^{\alpha+2}} \ge 1 - \frac{1}{p^2}.$$

On obtient donc

$$\prod_{\substack{p \ge 3 \\ p \text{ premier}}} \chi_p(n) \ge \prod_{\substack{p \ge 3 \\ p \text{ premier}}} \left(1 - \frac{1}{p^2}\right) = \frac{8}{\pi^2}.$$

Cela donne finalement avec (33), si l'on se réfère à (9), (10) et (11),

$$R(n) \ge \frac{\kappa n}{2^{3k}} + O_\varepsilon(n^{3/4+\varepsilon}) \quad \text{pour tout } \varepsilon > 0,$$

où $\kappa > 0$ est une constante absolue.

On en déduit que pour chaque $j \ge 1$, il existe un entier N_j tel que les conditions $n \ge N_j^2$ et $4 \nmid n$ entraînent que n est la somme de 4 carrés d'éléments de $\mathcal{C}_j$. ∎

Puisque $\mathcal{C}_1 = \mathbb{N}$, on peut choisir $N_1 = 0$. La construction par blocs de la suite $\mathcal{C}_0$ s'effectue alors de la manière suivante : la suite $\mathcal{C}_0$ est telle que

$$\mathcal{C}_j \cap [N_j, N_{j+1}[= \mathcal{C}_0 \cap [N_j, N_{j+1}[\quad \text{pour tout } j \ge 1.$$

On a, d'une part, $[0, N_{j+1}[\cap \mathcal{C}_j \subset \mathcal{C}_0$ pour tout $j \ge 1$, donc, d'après la Proposition 3, tout entier n non divisible par 4 est somme de 4 éléments de $\mathcal{C}_0^{(2)}$. Par ailleurs tout entier n multiple de 4 s'écrit $n = 4^a n_1$ avec $4 \nmid n_1$. On en déduit que $n_1 = c_1^2 + c_2^2 + c_3^2 + c_4^2$ pour $c_1, c_2, c_3, c_4 \in \mathcal{C}_0$, donc que $n = (2^a c_1)^2 + (2^a c_2)^2 + (2^a c_3)^2 + (2^a c_4)^2$. On pose $\mathcal{C} = \bigcup_{t=0}^\infty 2^t \cdot \mathcal{C}_0$. Cela

montre que $\mathcal{C}^{(2)}$ est une base d'ordre 4. D'autre part, pour tout $j \geq 1$ on a $[N_j, \infty[\cap \mathcal{C}_0 \subset \mathcal{C}_j$, donc tout entier $m \geq N_j$ de $\mathcal{C}_0$ satisfait (17). D'après la Proposition 1 avec $d = 2$, on conclut que $\mathcal{C}$ n'est pas une base.

Références

[1] R. Ayoub, *An Introduction to the Analytic Theory of Numbers*, Amer. Math. Soc., Providence, 1963.

[2] J.-M. Deshouillers, P. Erdős and A. Sárközy, *On additive bases*, Acta Arith. 30 (1976), 121–132.

[3] J.-M. Deshouillers and É. Fouvry, *On additive bases (II)*, J. London Math. Soc. (2) 14 (1976), 413–422.

[4] E. Grosswald, *Representations of Integers as Sums of Squares*, Springer, New York, 1985.

[5] F. Hennecart, *Propriétés additives des suites et de leurs carrés*, Acta Arith. 66 (1994), 101–123.

[6] H. D. Kloosterman, *On the representation of a number in the form* $ax^2 + by^2 + cz^2 + dt^2$, Acta Math. 49 (1926), 407–464.

[7] A. Stöhr, *Eine Basis h-ter Ordnung für die Menge aller natürlichen Zahlen*, Math. Z. 42 (1937), 739–743.

[8] —, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe II*, J. Reine Angew. Math. 194 (1955), 111–140.

A2X, Université Bordeaux 1
33405 Talence Cedex, France
E-mail: hennec@math.u-bordeaux.fr

Reçu le 28.12.2001 (4176)