ACTA ARITHMETICA
LXVI.2 (1994)

Propriétés additives des suites et de leurs carrés

par

François Hennecart (Talence)

1. Introduction

1.1. *Historique et énoncés des résultats.* Le théorème de Lagrange (tout entier est somme de quatre carrés), plus généralement le problème de Waring (tout entier est somme de neuf cubes, dix-neuf bicarrés, ...), et le problème de Goldbach (tout entier supérieur à deux est somme d'au plus trois nombres premiers), énoncés au XVIII^e siècle, sont des exemples de problèmes additifs, en cela qu'on cherche à représenter tout entier (ou tout entier assez grand) comme somme d'entiers d'une suite donnée. Plus généralement, on dit qu'une suite d'entiers $\mathcal{A}$ est une *base additive* (ou simplement base), s'il existe un entier h tel que tout entier soit somme d'au plus h éléments de $\mathcal{A}$; si c'est le cas, le plus petit entier h ayant la propriété requise s'appelle l'*ordre* de la base.

Le fait que les puissances k-ièmes constituent une base a été démontré par Hilbert en 1909, et le résultat que la suite des nombres premiers, auxquels on joint 0 et 1, est une base, est dû à Shnirel'man, et obtenu en 1930. Motivé par le problème de Waring, F. Dress a posé, au début des années 70, la question de savoir si la suite des puissances k-ièmes des éléments d'une base était encore une base. Une réponse négative a été apportée en 1976 par J.-M. Deshouillers, P. Erdős et A. Sárközy [3] : plus précisément, ils ont montré qu'il existait une base d'ordre trois dont la suite des carrés des éléments n'est pas une base. Plus étonnant encore, ils ont montré aussi l'existence d'une suite qui n'est pas une base, alors que la suite des carrés des éléments est une base d'ordre six. Ce résultat a été étendu par J.-M. Deshouillers et É. Fouvry [4], qui ont prouvé que, pour toute suite $\mathcal{K}$ d'entiers positifs, il existe une suite dont les puissances k-ièmes des éléments constituent une base si et seulement si k est dans $\mathcal{K}$.

L'objet de ce travail est d'améliorer les résultats sur les carrés en donnant les meilleurs énoncés possibles :

THÉORÈME 1. *Il existe une base $\mathcal{B}$ d'ordre deux dont la suite des carrés n'est pas une base.*

THÉORÈME 2. *Il existe une suite $\mathcal{C}$ qui n'est pas une base, dont la suite des carrés est une base d'ordre quatre.*

On note $\mathcal{Q}$ la suite des carrés. Soit $\mathcal{A}$ une suite d'entiers positifs; $A(x)$ désigne le nombre d'éléments de $\mathcal{A}$ inférieurs à x, et $\mathcal{A}^{(2)}$ la suite des carrés des éléments de $\mathcal{A}$. Enfin, pour tout entier h, on note $h\mathcal{A}$ l'ensemble des entiers n de la forme $n = a_1 + a_2 + \ldots + a_h$, où $a_1, a_2, \ldots, a_h$ sont éléments de $\mathcal{A}$. On a $Q(x) \sim x^{1/2}$ et le théorème de Lagrange donne $4\mathcal{Q} = \mathbb{N}$. Dans les années 1980, P. Erdős et M. B. Nathanson (cf. [6] et [12]) ont prouvé, pour tout $\varepsilon > 0$, l'existence d'une suite $\mathcal{A}$ telle que $3\mathcal{A}^{(2)} = 3\mathcal{Q}$, $4\mathcal{A}^{(2)} = 4\mathcal{Q}$ et $A^{(2)}(x) \sim cx^{1/3+\varepsilon}$ pour un certain $c > 0$. Ils ont émis la conjecture suivante, à savoir que pour tout $\varepsilon > 0$, il existe une suite $\mathcal{A}$ d'entiers telle que $\mathcal{A}^{(2)}$ est une base d'ordre 4 et $A^{(2)}(x) \sim cx^{1/4+\varepsilon}$ pour $c > 0$. Cette conjecture a été démontrée par J. Zöllner [17]. Notons que le meilleur résultat possible serait obtenu en éliminant le ε de l'exposant dans le résultat de J. Zöllner, ce qu'a réalisé en partie E. Wirsing en remplaçant x^{ε} par $(\log x)^{1/4}$ (cf. [16]). C'est à l'occasion d'un exposé de M.B. Nathanson à propos de ces problèmes, qui avait pour cadre un cours de troisième cycle à l'université de Rutgers en avril-mai 1991, que J.-M. Deshouillers a posé la question de savoir ce que la méthode de construction de la suite $\mathcal{C}$ du Théorème 2 permettait d'obtenir asymptotiquement pour $C^{(2)}(x)$. On prouve dans un dernier paragraphe, en utilisant une méthode probabiliste due à I. Z. Ruzsa [13] que pour tout $\varepsilon > 0$, il existe une suite d'entiers $\mathcal{C}$, qui n'est pas une base, telle que $\mathcal{C}^{(2)}$ est une base d'ordre 4 vérifiant $C^{(2)}(x) \ll x^{1/4+\varepsilon}$.

1.2. *Définitions et notations.* Dans le cadre de ce travail, on utilise deux notions de base différentes de celle déjà abordée. Pour p entier, une suite $\mathcal{M}$ est une *base modulo p* s'il existe un entier h positif tel qu'il existe un représentant de chaque classe qui s'écrive comme la somme de h éléments de $\mathcal{M}$. Une suite $\mathcal{A}$ est appelée *base asymptotique* s'il existe h tel que tout entier assez grand est somme d'au plus h éléments de $\mathcal{A}$. On définit les ordres respectifs de $\mathcal{M}$ et de $\mathcal{A}$ de la même manière que pour une base additive.

Nous introduisons quelques notations que nous emploierons, tout au long de ce travail, sans en préciser à nouveau leur signification :

• si n et p sont des entiers positifs, on note $r(n,p)$ le reste de la division de n par p; on a $0 \leq r(n,p) \leq p-1$;

• u étant un réel, on définit $[u]$ et $\|u\|$ comme étant respectivement la partie entière de u, et la distance de u au plus proche entier;

• si a, b et c sont trois entiers, alors (a,b) (resp. (a,b,c)) dénote le plus grand commun diviseur de a et b (resp. a, b et c);

• pour a et b deux entiers, $a \mid b$ signifie que a divise b;

• pour u réel quelconque, $\mathrm{e}(u) = \exp(i2\pi u)$;

• on note $\mathbf{x}$ le vecteur (x_1, x_2, x_3, x_4) de $\mathbb{R}^4$;

• pour $\mathbf{x} \in \mathbb{Z}^4$ et q entier positif, la propriété $x_i \equiv 0 \pmod q$ $(1 \le i \le 4)$ sera notée indifféremment $\mathbf{x} \equiv 0 \pmod q$ ou $q \mid \mathbf{x}$;

• si $\mathbf{x}$ et $\mathbf{y}$ sont deux éléments de $\mathbb{R}^4$, on note $\mathbf{x} \cdot \mathbf{y}$ le produit scalaire usuel de $\mathbb{R}^4$. On utilisera aussi la notation $\mathbf{x} \cdot \mathbf{x} = \mathbf{x}^2$;

• les symboles $\sum_{k \bmod q}$ et $\sum_{x \equiv k \,(\mathrm{mod}\, q)}$ désignent respectivement une sommation sur les entiers k parcourant $[0, q-1]$, et une sommation restreinte aux entiers x congrus à k modulo q. On définit aussi les symboles $\sum_{\mathbf{k} \bmod q}$ et $\sum_{\mathbf{x} \equiv \mathbf{k} \,(\mathrm{mod}\, q)}$, leur équivalent sur un quadrivecteur;

• le symbole $\sum_{k=1}^{\star q}$ dénote une sommation restreinte aux entiers k de $[1, q]$, premiers avec q;

• on note $S(a, b, q)$ la somme de Gauss $\sum_{x=0}^{q-1} \mathrm{e}((ax^2 + bx)/q)$;

• soit f et g deux fonctions telles que g est réelle positive et qu'il existe une constante positive C telle que $|f| \le Cg$. Cela se note $f = \mathcal{O}(g)$ dans les notations de Landau, ou $f \ll g$ dans celles de Vinogradov;

• si s et q sont deux entiers premiers entre eux, alors on note s_q l'unique entier modulo q tel que $s \cdot s_q \equiv 1 \bmod q$. Lorsqu'il n'y aura pas ambiguïté sur q, on utilisera plutôt la notation $\overline{s} = s_q$;

• les symboles $A_1, A_2, \ldots$ désignent des constantes strictement positives absolues, et ε un nombre positif arbitrairement petit qui n'est pas forcément le même en toute occasion. On se permettra notamment d'écrire $n^{2\varepsilon} \ll n^{\varepsilon}$.

2. Une base d'ordre 2 dont les carrés des éléments ne constituent pas une base

2.1. *Principe de la démonstration du Théorème* 1. On commence par construire, pour tout entier k et tout nombre premier p_k assez grand, une base modulo p_k d'ordre deux, constituée des entiers x pour lesquels $r(x^2, p)$ est inférieur à p_k/k. De cette manière, cela permettra de définir, relativement à une suite $(p_k)_{k \ge 1}$ de nombres premiers distincts, une suite décroissante de bases asymptotiques d'ordre deux. On obtient la base $\mathcal{B}$ par une construction diagonale par blocs; elle vérifie le fait que, pour tout entier k, pour tout élément b de $\mathcal{B}$ assez grand, $r(b^2, p_k)/p_k$ est borné par $1/k$. Le critère de non-base énoncé au Lemme 2 assure que $\mathcal{B}^{(2)}$ n'est pas une base.

2.2. *Construction d'une base d'ordre deux pour certains modules.* Soit k un entier strictement positif, et p un nombre premier.

On définit

$$H_p(k) = \{x \in \mathbb{N} : 1 \le r(x^2, p) \le [p/k] - 1\}.$$

On a

LEMME 1. *Pour tout entier k supérieur ou égal à 1, et pour tout nombre premier p tel que*

$$p > (15k)^4 \log^4(k+1)\,, \tag{1}$$

la suite $H_p(k)$ est une base modulo p d'ordre deux.

P r e u v e. On a la décomposition $p = 1 + p - 1 \in 2H_p(k)$ puisque $1^2 \equiv (p-1)^2 \equiv 1 \pmod p$.

On suppose maintenant que h est un entier de $[p+1, 2p-1]$; nous allons établir une formule asymptotique pour le nombre $M_{p,k}(h)$ d'entiers x inférieurs à $p-1$, appartenant à $H_p(k)$ tels que $h-x$ appartienne aussi à $H_p(k)$. On a

$$M_{p,k}(h) = \sum_{\substack{x\in H_p(k)\cap[0,p-1]\\(h-x)\in H_p(k)}} 1\,. \tag{2}$$

Le lemme sera démontré en prouvant que $M_{p,k}(h)$ est strictement positif si p satisfait (1).

Observons que si x est un entier positif, on a

$$\frac{1}{p}\sum_{u=1}^{[p/k]-1}\sum_{v=(1-p)/2}^{(p-1)/2} \mathrm{e}\Big(\frac{v(x^2-u)}{p}\Big) = \begin{cases} 1 & \text{si } x \text{ appartient à } H_p(k)\,,\\ 0 & \text{sinon.}\end{cases}$$

Par conséquent, en appliquant la même remarque à $h-x$, cela conduit à

$$M_{p,k}(h) = \sum_{x=0}^{p-1}\Big(\frac{1}{p}\sum_{u=1}^{[p/k]-1}\sum_{v=(1-p)/2}^{(p-1)/2}\mathrm{e}\Big(\frac{v(x^2-u)}{p}\Big)\Big) \times\Big(\frac{1}{p}\sum_{u'=1}^{[p/k]-1}\sum_{v'=(1-p)/2}^{(p-1)/2}\mathrm{e}\Big(\frac{v'((h-x)^2-u')}{p}\Big)\Big)\,.$$

D'où

$$M_{p,k}(h) = \frac{1}{p^2}\sum_{v=(1-p)/2}^{(p-1)/2}\sum_{v'=(1-p)/2}^{(p-1)/2}\Big(\sum_{u=1}^{[p/k]-1}\mathrm{e}\Big(-\frac{uv}{p}\Big)\Big) \times\Big(\sum_{u'=1}^{[p/k]-1}\mathrm{e}\Big(\frac{(h^2-u')v'}{p}\Big)\Big)S(v+v', -2hxv', p)\,,$$

puis

$$M_{p,k}(h) = \frac{1}{p^2} \sum_{v=(1-p)/2}^{(p-1)/2} \Big(\sum_{u=1}^{[p/k]-1} \mathrm{e}\Big(-\frac{uv}{p}\Big)\Big)$$
$$\times \Big(\sum_{u'=1}^{[p/k]-1} \mathrm{e}\Big(\frac{u'v}{p}\Big)\Big)\Big(\sum_{x=0}^{p-1} \mathrm{e}\Big(\frac{2hxv - vh^2}{p}\Big)\Big)$$
$$+ \frac{1}{p^2} \sum_{v=(1-p)/2}^{(p-1)/2} \sum_{\substack{v'=(1-p)/2 \\ v'\neq -v}}^{(p-1)/2} \Big(\sum_{u=1}^{[p/k]-1} \mathrm{e}\Big(-\frac{uv}{p}\Big)\Big)\Big(\sum_{u'=1}^{[p/k]-1} \mathrm{e}\Big(-\frac{u'v'}{p}\Big)\Big)$$
$$\times S(v+v', -2hxv', p)\mathrm{e}\Big(\frac{v'h^2}{p}\Big).$$

Pour p premier impair et a premier avec p, on a l'égalité

$$S(a,b,p) = \sum_{x=0}^{p-1} \mathrm{e}\Big(\frac{a(x+\overline{2}\overline{a}b)^2}{p}\Big)\mathrm{e}\Big(-\frac{\overline{a}(\overline{2}b)^2}{p}\Big),$$

et les estimations de sommes de Gauss données par le Théorème 4.15 de [1; p. 315] entraînent alors que

$$|S(a,b,p)| = \sqrt{p}\,. \tag{3}$$

D'autre part si $p \,|\, a$ alors la somme $S(a,b,p)$ est égale à p si $p \,|\, b$, et nulle sinon. D'où, puisque $(p, 2h) = 1$, on obtient

$$\Big|M_{p,k}(h) - \frac{1}{p}\Big(\Big[\frac{p}{k}\Big] - 1\Big)^2\Big| \le p^{-3/2}\Big(\sum_{v=(1-p)/2}^{(p-1)/2} \Big| \sum_{u=1}^{[p/k]-1} \mathrm{e}\Big(-\frac{uv}{p}\Big)\Big|\Big)^2; \tag{4}$$

on applique alors à la somme intérieure la majoration classique suivante :

$$\Big|\sum_{x=1}^{X} \mathrm{e}(\alpha x)\Big| \le \min\Big(X, \frac{1}{2|\alpha|}\Big), \tag{5}$$

valable pour tout réel X positif et tout réel α tel que $|\alpha| \le 1/2$. Cela conduit à

$$\sum_{v=(1-p)/2}^{(p-1)/2} \Big| \sum_{u=1}^{[p/k]-1} \mathrm{e}\Big(-\frac{uv}{p}\Big)\Big| \le \Big[\frac{p}{k}\Big] + \sum_{v=1}^{(p-1)/2} \frac{p}{v} \le p\Big(\log p + \frac{1}{k}\Big).$$

D'où finalement

$$\Big|M_{p,k}(h) - \frac{p-1}{k^2}\Big| \le \sqrt{p}(\log p + 1)^2\,.$$

Par conséquent, $M_{p,k}(h)$ est non nul dès que $(p-2)/(\log p+1)^4 > k^4$. Un simple calcul permet de montrer que l'inégalité (1) entraîne la relation précédente.

2.3. *Une famille de bases asymptotiques d'ordre deux et construction diagonale.* Pour tout $k \geq 1$, on note p_k le plus petit nombre premier satisfaisant l'inégalité (1). Soit $K \geq 1$; on pose $N_0 = 0$ et $N_K = p_1 p_2 \dots p_K$ et on définit

$$\mathcal{B}_K = \bigcap_{k=1}^{K} (H_{p_k,k}(k)) .$$

Le Lemme 1 entraîne que $H_{p_k,k}(k)$ est une base modulo p_k d'ordre 2, pour tout $k \geq 1$. D'où, par le Théorème Chinois, la suite $\mathcal{B}_K$ constitue une base modulo p_K d'ordre 2, et puisqu'elle est aussi périodique de période p_K, tout entier supérieur à p_K est somme d'au plus 2 éléments de $\mathcal{B}_K$.

Nous disposons, à présent, d'une suite décroissante $(\mathcal{B}_K)_{K\geq 1}$ de bases asymptotiques d'ordre 2, à partir de laquelle nous allons construire une base d'ordre 2, dont l'ensemble des carrés des éléments n'est pas une base. Le critère de non-base que nous allons appliquer est un cas particulier du critère donné par J.-M. Deshouillers, P. Erdős et A. Sárközy (cf. [3; Lemme 1]), et s'énonce de la façon suivante :

Lemme 2. *Soit $\mathcal{A}$ une suite d'entiers positifs. Supposons qu'il existe deux suites strictement croissantes, l'une de nombres premiers $p_1 < p_2 < \dots < p_k < \dots$, l'autre de nombres entiers positifs $1 \leq N_1 < N_2 < \dots < N_k < \dots$, telles que, pour tout $k \geq 1$, pour tout élément a de $\mathcal{A}$, supérieur à N_k, on a*

$$r(a, p_k) \leq p_k/k . \tag{6}$$

Alors $\mathcal{A}$ n'est pas une base.

On définit $\mathcal{B}$ comme étant la suite satisfaisant

$$\mathcal{B} \cap [N_K, N_{K+1}[= \mathcal{B}_K \cap [N_K, N_{K+1}[\quad \text{pour } K \geq 0 .$$

Pour tout entier $K \geq 0$, on a les inclusions

$$\mathcal{B}_K \cap [0, N_{K+1}[\subset \mathcal{B} , \tag{7}$$

$$\mathcal{B} \cap [N_K, +\infty[\subset \mathcal{B}_K . \tag{8}$$

Soit n un entier positif. Pour un certain $K \geq 0$, on a $N_K \leq n < N_{K+1}$, et donc n est la somme de 2 éléments de $\mathcal{B}_K$. Par (7), on déduit que n appartient à $2\mathcal{B}$, et par conséquent $\mathcal{B}$ est une base d'ordre 2.

D'autre part, si b est un élément de $\mathcal{B}$ supérieur à N_K, alors l'inclusion (8) implique que b appartient à $\mathcal{B}_K$, et par suite

$$r(b^2, p_k) \leq p_k/k \quad (1 \leq k \leq K) .$$

Le Lemme 2 entraîne alors que $\mathcal{B}^{(2)}$ n'est pas une base.

3. Une suite, non base, dont les carrés constituent une base d'ordre 4

3.1. *Schéma de la démonstration du Théorème* 2. Comme au chapitre précédent, on souhaite exploiter le critère énoncé au Lemme 2; on commence par chercher une suite de nombres premiers $p_1 < p_2 < \ldots < p_k < \ldots$, telle que, pour tout k, l'ensemble des entiers n dont $r(n, p_k)$ est inférieur à $p_k/k-1$ vérifie le fait que la suite de ses carrés est une base modulo p_k d'ordre 4. Puis, appliquant à nouveau le Théorème Chinois, en prenant l'intersection indexée sur $k = 1, 2, \ldots, K$ de ces suites, on obtient un ensemble d'entiers dont les carrés forment une base modulo $p_1 p_2 \ldots p_K$ d'ordre quatre.

On montre alors, grâce à la méthode du cercle, que cette suite de carrés est une base asymptotique d'ordre 4, ceci en justifiant une formule asymptotique non triviale pour le nombre de représentations d'un entier comme la somme de quatre éléments de cette suite. On conclut par une construction par blocs de la suite $\mathcal{C}$ qui satisfait le Théorème 2.

3.2. *Une suite dont les carrés des éléments constituent une base d'ordre au plus quatre pour certains modules.* Soit p un nombre premier supérieur à 3, et k un entier positif non nul. On définit

$$H'_p(k) = \{x \in \mathbb{N} : 1 \le r(x,p) \le [p/k] - 1\}\,.$$

On montre alors

Lemme 3. *Pour tout entier k strictement positif, et pour tout nombre premier p assez grand, la suite des carrés des éléments de $H'_p(k)$ est une base modulo p d'ordre au plus* 4.

P r e u v e. Pour m dans $\{0, 1, \ldots, p-1\}$, on définit $M'_{p,k}(m)$ comme étant le nombre de quadruplets $\mathbf{x} = (x_1, x_2, x_3, x_4)$ solutions de la congruence

$$\begin{cases} m \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \pmod p\,; \\ x_i \in H'_p(k) \cap [0, p-1] \quad (1 \le i \le 4)\,. \end{cases} \tag{9}$$

Le lemme sera démontré lorsqu'on aura prouvé que $M'_{p,k}(m)$ est strictement positif pour tout p suffisamment grand. On écrit

$$M'_{p,k}(m) = \frac{1}{p} \sum_{t=0}^{p-1} \sum_{\substack{\mathbf{x} \bmod p \\ x_i \in H'_p(k) \\ 1 \le i \le 4}} \mathrm{e}\left(\frac{t}{p}(x_1^2 + x_2^2 + x_3^2 + x_4^2 - m)\right). \tag{10}$$

Si x est un entier positif, on a

$$\frac{1}{p} \sum_{u=1}^{[p/k]-1} \sum_{v=(1-p)/2}^{(p-1)/2} \mathrm{e}\left(\frac{v(x-u)}{p}\right) = \begin{cases} 1 & \text{si } x \in H'_p(k)\,, \\ 0 & \text{sinon,} \end{cases}$$

d'où

$$\sum_{\substack{x=0\\ x\in H'_p(k)}}^{p-1} \mathrm{e}\Big(\frac{tx^2}{p}\Big) = \frac{1}{p}\sum_{v=(1-p)/2}^{(p-1)/2}\sum_{u=1}^{[p/k]-1} \mathrm{e}\Big(-\frac{uv}{p}\Big)S(t,v,p)\,. \tag{11}$$

On déduit alors de (3), (5) et (11) que pour $(t,p)=1$, on a

$$\Big|\sum_{\substack{x=0\\ x\in H'_p(k)}}^{p-1} \mathrm{e}\Big(\frac{tx^2}{p}\Big)\Big| \le \frac{1}{\sqrt{p}}\sum_{v=(1-p)/2}^{(p-1)/2}\Big|\sum_{u=1}^{[p/k]-1}\mathrm{e}\Big(-\frac{uv}{p}\Big)\Big| \le \frac{1}{\sqrt{p}}\Big(\Big[\frac{p}{k}\Big]+\sum_{v=1}^{(p-1)/2}\frac{p}{v}\Big);$$

d'où, pour tout entier t premier avec p,

$$\Big|\sum_{\substack{x=0\\ x\in H'_p(k)}}^{p-1} \mathrm{e}\Big(\frac{tx^2}{p}\Big)\Big| \le \sqrt{p}\Big(\log p+\frac{1}{k}\Big)\,. \tag{12}$$

Par conséquent, puisque le nombre de classes modulo p de $H'_p(k)$ est égal à $[p/k]-1$, la relation (10) entraîne

$$M'_{p,k}(m) = \frac{1}{p}\Big(\Big[\frac{p}{k}\Big]-1\Big)^4 + \frac{1}{p}\sum_{t=1}^{p-1}\sum_{\substack{\mathbf{x}\bmod p\\ x_i\in H'_p(k)\\ 1\le i\le 4}} \mathrm{e}\Big(\frac{t}{p}(x_1^2+x_2^2+x_3^2+x_4^2-m)\Big),$$

puis par (12), on obtient

$$M'_{p,k}(m) \ge \frac{([p/k]-1)^4}{p} - p^2(\log p+1)^4\,.$$

Pour que la congruence (9) admette au moins une solution $\mathbf{x}$ pour tout entier m dans $[0,p-1]$, il suffit que le terme de droite dans l'inégalité précédente soit strictement positif, ce qui est réalisé dès que

$$p > (15k)^4\log^4(k+1)\,. \tag{13}$$

Par le choix même de la suite $H'_p(k)$, tout entier modulo p est la somme de 4 éléments de $H'_p(k)$ non divisibles par p; en conséquence, la décomposition n'est pas triviale : ceci va être utile lors de l'étude de la série singulière.

3.3. *Une suite dont les carrés des éléments forment une base asymptotique d'ordre* 4. On pose $p_1=2$ et pour tout entier k supérieur à 2, on note p_k le plus petit nombre premier vérifiant (13); il est clair que la suite $(p_k)_{k\ge1}$ est strictement croissante. Soit alors K un entier positif; on pose

$$P_K = 2p_2\dots p_K\,, \tag{14}$$

et on définit

$$\mathcal{C}_K = \bigcap_{1\le k\le K} H'_{p_k}(k)\,. \tag{15}$$

Puisque P_K est sans facteur carré, du Lemme 3, du Théorème Chinois et du fait que $H_p(1)$ est une base modulo p d'ordre 2 pour tout nombre premier p, on déduit que la suite $\mathcal{C}_K^{(2)}$ des carrés des éléments de $\mathcal{C}_K$ constitue une base modulo P_K d'ordre au plus 4.

Soit n un entier; il existe alors un quadruplet (h_1, h_2, h_3, h_4) d'éléments de $\mathcal{C}_K$ tel que

$$\begin{cases} n \equiv h_1^2 + h_2^2 + h_3^2 + h_4^2 \pmod{P_K}, \\ (h_i, P_K) = 1 \quad (1 \le i \le 4)\,. \end{cases} \tag{16}$$

Il s'agit de montrer alors que l'on peut décomposer n en somme de 4 carrés d'entiers appartenant respectivement aux classes de h_1, h_2, h_3 et h_4 modulo P_K. Cela fera l'objet des prochains paragraphes et donnera la proposition suivante :

PROPOSITION 1. *La suite $\mathcal{C}_K^{(2)}$ est une base asymptotique d'ordre quatre.*

Nos efforts vont maintenant se concentrer sur l'obtention d'une formule asymptotique pour le nombre de représentations d'un entier comme somme de 4 carrés d'éléments de classes modulo P_K données.

La méthode développée est la variante de la méthode du cercle, qui apparaît dans les articles de H. D. Kloosterman, traîtant de la représentation des entiers par une forme quadratique diagonale à quatre variables (cf. [11]). Cette méthode a l'intérêt de nous éviter la considération d'arcs mineurs, mais, en contrepartie, elle nous oblige à repérer, avec précision, les bornes des intervalles dans la dissection de Farey du tore : il en résulte, alors, l'apparition de sommes de Gauss et de Kloosterman. C'est alors au niveau de leurs estimations que se gagne un carré par rapport à la méthode de Hua (cf. [4]).

3.4. *Dissection de Farey de l'intervalle unité et méthode de Kloosterman.* Abordons la description de la méthode : soit n un entier positif et on pose

$$N = [\sqrt{n}\,]\,. \tag{17}$$

On note $P = P_K = 2p_2p_3\dots p_K$. Pour h entier, on introduit la somme exponentielle

$$f_h(\alpha) = \sum_{x\equiv h \,(\mathrm{mod}\, P)} \gamma\left(\frac{x}{N}\right)\mathrm{e}(\alpha x^2)\,, \tag{18}$$

où chaque terme est affecté d'un poids défini par la fonction indéfiniment

différentiable

$$\gamma(t) = \begin{cases} \exp\left(-\dfrac{1}{t(1-t)}\right) & \text{si } 0 < t < 1\,, \\ 0 & \text{sinon.} \end{cases} \tag{19}$$

Ce poids facilite l'application de la formule sommatoire de Poisson, et notamment les estimations des intégrales exponentielles complexes qui apparaissent. Toutefois, il n'intervient pas dans la partie arithmétique du problème : les sommes exponentielles ne s'en trouvent pas modifiées, et leurs estimations s'effectuent de manière classique.

Soit H un entier positif et h_1, h_2, h_3 et h_4 quatre éléments de $\mathcal{C}_K$, dont le choix a été décrit précédemment, tels que

$$H \equiv h_1^2 + h_2^2 + h_3^2 + h_4^2 \pmod{P}\,.$$

Notre objectif est de montrer que pour $n \equiv H \pmod{P}$, suffisamment grand, le nombre

$$r_{\mathbf{h}}(n) = \sum_{\substack{\mathbf{x}\equiv\mathbf{h}\,(\mathrm{mod}\,P) \\ n=x_1^2+x_2^2+x_3^2+x_4^2}} 1 \tag{20}$$

est strictement positif. Il sera atteint en obtenant une minoration de $r_{\mathbf{h}}(n)$; puisque $0 \le \gamma(t) \le 1$, il nous suffit d'établir une formule asymptotique non triviale pour

$$R(n) = \int_0^1 S_n(\alpha)\,d\alpha \tag{21}$$

où

$$S_n(\alpha) = \Big(\prod_{i=1}^{4} f_{h_i}(\alpha)\Big)\mathrm{e}(-\alpha n)\,. \tag{22}$$

On a par (21) et par périodicité de $S_n(\alpha)$,

$$R(n) = \int_{-1/(N+1)}^{1-1/(N+1)} S_n(\alpha)\,d\alpha\,.$$

On opère une dissection de Farey de l'intervalle d'intégration $[-1/(N+1), 1-1/(N+1)[$ que l'on combine avec le raffinement de Kloosterman, et on obtient le lemme suivant dû à D. R. Heath-Brown (cf. [8; Lemme 7]) :

Lemme 4. *On a*

$$R(n) = \sum_{q=1}^{N} \int_{-1/(qN)}^{1/(qN)} \sideset{}{^\star}\sum_{s=1}^{q} S_n\left(\frac{s}{q} + z\right) dz + O(E)\,, \tag{23}$$

où

$$E=\frac{1}{N^2}\sum_{q=1}^{N}\sum_{|u|\le q/2}\frac{1}{1+|u|}\max_{1/2\le|z|qN\le 1}\Big|\sideset{}{^\star}\sum_{s=1}^{q}\mathrm{e}\Big(\frac{us}{q}\Big)S_n\Big(\frac{\overline{s}}{q}+z\Big)\Big|. \tag{24}$$

3.5. *La formule sommatoire de Poisson.* Nous appliquons à $S_n(s/q+z)$ la formule sommatoire de Poisson en dimension quatre : cela dissocie les variables u et z dans le terme d'erreur E défini dans (24), et induit une expression composée, d'une part de sommes trigonométriques, et d'autre part d'intégrales exponentielles complexes.

Lemme 5. *On pose* $\underline{\gamma}(\mathbf{x})=\prod_{i=1}^{4}\gamma(x_i)$. *Pour tout entier* s, *on a*

$$S_n\Big(\frac{s}{q}+z\Big)=\sum_{\mathbf{b}\in\mathbb{Z}^4}\frac{1}{(Pq)^4}\sum_{\substack{\mathbf{c}\bmod Pq\\ \mathbf{c}\equiv\mathbf{h}\,(\mathrm{mod}\,P)}}\mathrm{e}\Big(\frac{s\mathbf{c}^2}{q}+\frac{\mathbf{b}\cdot\mathbf{c}}{Pq}\Big)\mathrm{e}\Big(-\frac{sn}{q}\Big)\times\int_{\mathbb{R}^4}\underline{\gamma}\Big(\frac{\mathbf{t}}{N}\Big)\mathrm{e}\Big(z\mathbf{t}^2-\frac{\mathbf{b}\cdot\mathbf{t}}{Pq}\Big)\mathrm{e}(-zn)\,dV(\mathbf{t})\,. \tag{25}$$

P r e u v e. La relation (22) conduit à

$$S_n\Big(\frac{s}{q}+z\Big)=\sum_{\mathbf{x}\equiv\mathbf{h}\,(\mathrm{mod}\,P)}\underline{\gamma}\Big(\frac{\mathbf{x}}{N}\Big)\mathrm{e}\Big(\Big(\frac{s}{q}+z\Big)(\mathbf{x}^2-n)\Big)\,.$$

En scindant cette somme selon les valeurs de $\mathbf{x}$ mod Pq, cela donne

$$S_n\Big(\frac{s}{q}+z\Big)=\sum_{\substack{\mathbf{c}\bmod Pq\\ \mathbf{c}\equiv\mathbf{h}\,(\mathrm{mod}\,P)}}\mathrm{e}\Big(\frac{s(\mathbf{c}^2-n)}{q}\Big)\sum_{\mathbf{x}\equiv\mathbf{c}\,(\mathrm{mod}\,Pq)}\underline{\gamma}\Big(\frac{\mathbf{x}}{N}\Big)\mathrm{e}(z(\mathbf{x}^2-n))\,.$$

On obtient alors le lemme en appliquant la formule sommatoire de Poisson à quatre variables à la somme intérieure.

On en déduit

$$R(n)=\sum_{q=1}^{N}\int_{-1/(qN)}^{1/(qN)}\frac{1}{(Pq)^4}\sum_{\mathbf{b}\in\mathbb{Z}^4}\sideset{}{^\star}\sum_{s=1}^{q}\sum_{\substack{\mathbf{c}\bmod Pq\\ \mathbf{c}\equiv\mathbf{h}\,(\mathrm{mod}\,P)}}\mathrm{e}\Big(\frac{s(\mathbf{c}^2-n)}{q}+\frac{\mathbf{b}\cdot\mathbf{c}}{Pq}\Big)\times\int_{\mathbb{R}^4}\underline{\gamma}\Big(\frac{\mathbf{t}}{N}\Big)\mathrm{e}\Big(z(\mathbf{t}^2-n)-\frac{\mathbf{b}\cdot\mathbf{t}}{Pq}\Big)\,dV(\mathbf{t})\,dz\,. \tag{26}$$

On note $R'(n)$ la contribution de $R(n)$ correspondant à $\mathbf{b}=\mathbf{0}$, et E' la contribution complémentaire. Le terme $R'(n)$ conduira au terme principal dans la formule asymptotique.

3.6. *Majorations d'intégrales exponentielles complexes.* Dans (26), il apparaît des intégrales oscillantes que nous majorons en intégrant par parties.

Soit

$$I(z,v) = \int\limits_{\mathbb{R}} \gamma\left(\frac{t}{N}\right) \mathrm{e}(zt^2+vt)\,dt\,.$$

Lorsque $|v|$ est grand relativement à $|z|$, l'intégrale $I(z,v)$ oscille fortement, et par conséquent, $|I(z,v)|$ est faible. On montre plus précisément

Lemme 6. *On a*

$$I(z,v) \ll \min(N, |z|^{-1/2})\,. \tag{27}$$

Il existe $A \geq 0$ tel que pour $|v/z| > 4N$, on a

$$|I(z,v)| \leq N e^{-A(N|v|)^{1/3}}\,. \tag{28}$$

La majoration (27) s'obtient en intégrant par parties une fois et en appliquant la formule de la moyenne (cf. [14; Chapitre IV]). L'inégalité (28) découle aussi de multiples intégrations par parties et son obtention est semblable à celle du Lemme 1 de [10].

Soit maintenant $B > 0$ et $y > 0$ deux réels; alors

$$\begin{aligned}
\sum_{r>y} e^{-A(Br)^{1/3}} &< e^{-A(By)^{1/3}} + \int\limits_{y}^{\infty} e^{-A(Bt)^{1/3}}\,dt \\
&< e^{-A(By)^{1/3}} + \frac{3}{B} \int\limits_{(By)^{1/3}}^{\infty} s^2 e^{-As}\,ds \\
&< e^{-A(By)^{1/3}} + \frac{A_1}{B} \int\limits_{(By)^{1/3}}^{\infty} e^{-As/2}\,ds \\
&< A_2\left(1+\frac{1}{B}\right) e^{-A(By)^{1/3}/2}\,.
\end{aligned}$$

Donnons une conséquence immédiate de ce résultat : pour $q \leq N$, on déduit de (28) et de ce qui précède

$$\begin{aligned}
&\sum_{\substack{|b|>Pq(4|z|N+(\log^4 N)/N \\ (P,q)|b}} \left| I\left(z, \frac{b}{Pq}\right)\right| \\
&\qquad = \mathcal{O}\Big(N \sum_{|h|>Pq(4|z|N+(\log^4 N)/N)/(P,q)} e^{-A(|h|N(P,q)/(Pq))^{1/3}}\Big) \\
&\qquad = \mathcal{O}\left(\left(N + \frac{Pq}{(P,q)}\right) e^{-A_3 \log^{4/3} N}\right).
\end{aligned}$$

Par conséquent, on a

$$\sum_{\substack{|b|>Pq(4|z|N+(\log^4 N)/N)\\(P,q)|b}} \left|I\Big(z,\frac{b}{Pq}\Big)\right| = \mathcal{O}\Big(\frac{P}{(P,q)}\Big) \tag{29}$$

(les constantes impliquées dans les symboles $\mathcal{O}$ sont *absolues*).

3.7. *Majorations de sommes exponentielles.* Nous avons, à notre disposition, toutes les estimations nécessaires au traitement de la partie analytique de E et E'. Il nous faut, à présent, examiner la partie arithmétique de ces derniers. On donne des majorations de sommes de Gauss et de Kloosterman dans le cas général, obtenant ainsi des bornes suffisantes pour évaluer le terme d'erreur. Mais, pour estimer la contribution fondamentale dans la formule asymptotique, et principalement, dans l'optique de minorer la série singulière, on fournit des majorations plus précises de ces sommes, dans le cas où la sommation est opérée modulo un nombre premier.

Lemme 7. *Soit q un entier strictement positif, a un entier premier avec q, et w un entier quelconque; alors*

$$S(a,w,q) = \phi_w(a,q)\sqrt{q} \tag{30}$$

où

(31)

$$\phi_w(a,q) = \begin{cases} \Big(\dfrac{a}{q}\Big)\mathrm{e}\Big(-\dfrac{\overline{a}(\overline{2}w)^2}{q}\Big) & \text{si } q\equiv 1 \pmod 4,\\ i\Big(\dfrac{a}{q}\Big)\mathrm{e}\Big(-\dfrac{\overline{a}(\overline{2}w)^2}{q}\Big) & \text{si } q\equiv 3 \pmod 4,\\ (1+i)\Big(\dfrac{a}{q}\Big)\mathrm{e}\Big(-\dfrac{\overline{a}(w/2)^2}{q}\Big) & \text{si } q\equiv 0 \pmod 4 \text{ et } w \text{ pair},\\ \sqrt{2}\cdot\phi_w\Big(2a,\dfrac{q}{2}\Big) & \text{si } q\equiv 2 \pmod 4 \text{ et } w \text{ impair},\\ 0 & \text{dans les autres cas.}\end{cases}$$

Preuve.

• Si $(2,q)=1$, alors

$$S(a,w,q) = \sum_{x=0}^{q-1} \mathrm{e}\Big(\frac{a(x+\overline{2}\overline{a}w)^2}{q}\Big)\mathrm{e}\Big(-\frac{\overline{a}(\overline{2}w)^2}{q}\Big);$$

• Si $4\,|\,q$, alors on pose $q=4r$; en écrivant $x=f+2rg$, on obtient

$$S(a,w,q) = \sum_{f=0}^{2r-1} \mathrm{e}\Big(\frac{af^2+wf}{q}\Big)\sum_{g=1}^{2}\mathrm{e}\Big(\frac{wg}{2}\Big),$$

qui est nulle si w est impair; prenant alors w pair, $S(a,w,q)$ s'écrit

$$\sum_{f=0}^{q-1} \mathrm{e}\Big(\frac{a(f+\overline{a}w/2)^2}{q}\Big)\mathrm{e}\Big(-\frac{\overline{a}(w/2)^2}{q}\Big)\,.$$

• Si $q=2r$ avec $(2,r)=1$, alors en écrivant le changement de variables $x=2f+rl$, on obtient

$$\sum_{f=0}^{r-1} \mathrm{e}\Big(\frac{2af^2+wf}{r}\Big)\sum_{l=1}^{2}\mathrm{e}\Big(\frac{ral^2+wl}{2}\Big)\,;$$

la somme intérieure est égale à 2 si w est impair et 0 sinon.

Pour chacun des trois cas, il apparaît les sommes de Gauss $S(a,0,q)$; or on sait (cf. [1; Théorème 4.15, p. 315]) que $S(a,0,q)=\big(\frac{a}{q}\big)S(1,0,q)$ avec

$$S(1,0,q)=\begin{cases}(1+i)\sqrt{q} & \text{si } q\equiv 0 \pmod 4\,,\\ \sqrt{q} & \text{si } q\equiv 1 \pmod 4\,,\\ 0 & \text{si } q\equiv 2 \pmod 4\,,\\ i\sqrt{q} & \text{si } q\equiv 3 \pmod 4\,.\end{cases}$$

Cela donne (30).

Nous donnons maintenant des majorations de sommes de Kloosterman : on les énonce sous la forme établie par T. Estermann [7]. Pour q entier, on note $d(q)$ le nombre de diviseurs positifs de q.

Lemme 8. *Soit a, b et $q\geq 1$ des entiers; alors*

$$\Big|\sum_{x=1}^{q}{}^{\star}\,\mathrm{e}\Big(\frac{ax+b\overline{x}}{q}\Big)\Big| \leq d(q)\sqrt{q}(a,b,q)^{1/2}\,. \tag{32}$$

Nous pouvons, à présent, montrer le résultat suivant :

Lemme 9. *On a, pour $q\geq 1$ et $\mathbf{b}\in\mathbb{Z}^4$,*

$$\Big|\sum_{s=1}^{q}{}^{\star}\sum_{\substack{\mathbf{c} \bmod Pq\\ \mathbf{c}\equiv\mathbf{h}\,(\mathrm{mod}\,P)}}\mathrm{e}\Big(\frac{\overline{s}(\mathbf{c}^2-n)}{q}+\frac{\mathbf{b}\cdot\mathbf{c}}{Pq}+\frac{us}{q}\Big)\Big| \leq \begin{cases}(q,2)^2 d(q)(P,q)^4 q^{5/2}(q,n)^{1/2} & \textit{si } (P,q)\,|\,\mathbf{b}\,,\\ 0 & \textit{sinon}\,.\end{cases} \tag{33}$$

Si $q=p^l$ où p est un nombre premier différent de 2, on a

$$\Big|\sum_{s=1}^{p^l}{}^{\star}\sum_{\substack{\mathbf{c} \bmod Pp^l\\ \mathbf{c}\equiv\mathbf{h}\,(\mathrm{mod}\,P)}}\mathrm{e}\Big(\frac{\overline{s}(\mathbf{c}^2-n)}{p^l}\Big)\Big| \leq (l+1)(P,p)^4 p^{5l/2}(p^l,n)^{1/2}\,. \tag{34}$$

P r e u v e. On pose pour $(s,q)=1$,

$$S=\sum_{\substack{x \bmod Pq\\ x\equiv h \,(\mathrm{mod}\, P)}} \mathrm{e}\Big(\frac{\overline{s}x^2}{q}+\frac{bx}{Pq}\Big). \tag{35}$$

On a

$$\frac{1}{P}\sum_{v=0}^{P-1}\mathrm{e}\Big(\frac{v(x-h)}{P}\Big)=\begin{cases}1 & \text{si } x\equiv h \pmod P,\\ 0 & \text{sinon,}\end{cases}$$

d'où

$$S=\frac{1}{P}\sum_{v=0}^{P-1}\mathrm{e}\Big(-\frac{vh}{P}\Big)\sum_{x \bmod Pq}\mathrm{e}\Big(\frac{\overline{s}x^2}{q}+\frac{(b+vq)x}{Pq}\Big);$$

en sommant selon les progressions modulo q, puis par (30), on obtient

$$\begin{aligned}S&=\frac{1}{P}\sum_{v=0}^{P-1}\mathrm{e}\Big(-\frac{vh}{P}\Big)\sum_{f=0}^{q-1}\mathrm{e}\Big(\frac{\overline{s}f^2}{q}+\frac{(b+vq)f}{Pq}\Big)\sum_{g=0}^{P-1}\mathrm{e}\Big(\frac{(b+vq)g}{P}\Big)\\ &=\sum_{\substack{v=0\\ P\mid(b+vq)}}^{P-1}\mathrm{e}\Big(-\frac{vh}{P}\Big)\phi_{(b+vq)/P}(\overline{s},q)\sqrt{q}\,.\end{aligned}$$

Par suite,

$$\begin{aligned}&\sum_{\substack{\mathbf{c} \bmod Pq\\ \mathbf{c}\equiv\mathbf{h} \,(\mathrm{mod}\, P)}}\mathrm{e}\Big(\frac{\overline{s}(\mathbf{c}^2-n)}{q}+\frac{\mathbf{b}\cdot\mathbf{c}}{Pq}\Big)\\ &\qquad=q^2\sum_{\substack{\mathbf{v} \bmod P\\ P\mid(\mathbf{b}+q\mathbf{v})}}\mathrm{e}\Big(-\frac{\mathbf{v}\cdot\mathbf{b}}{P}\Big)\Big(\prod_{i=1}^{4}\phi_{(b_i+qv_i)/P}(\overline{s},q)\Big)\mathrm{e}\Big(\frac{-\overline{s}n}{q}\Big).\end{aligned}$$

De plus,

$$\begin{aligned}\mathrm{Card}\{1\le v\le P : P\mid(b+vq)\}&=(q,P)\cdot\mathrm{Card}\Big\{1\le v\le\frac{P}{(P,q)} : P\mid(b+vq)\Big\}\\ &=\begin{cases}(q,P) & \text{si } (q,P)\mid b,\\ 0 & \text{sinon.}\end{cases}\end{aligned}$$

Utilisant la convention $\max_{t\in\emptyset}F(t)=0$ si F est une fonction à valeurs positives et $\emptyset$ désigne l'ensemble vide, le terme de gauche dans la relation (33) est majoré par

$$(P,q)^4q^2\max_{\substack{\mathbf{b}\in\mathbb{Z}^4\\ P\mid(\mathbf{b}+q\mathbf{v})}}\Big|\sum_{s=1}^{q}{}^{\star}\Big(\prod_{i=1}^{4}\phi_{(b_i+qv_i)/P}(\overline{s},q)\Big)\mathrm{e}\Big(\frac{us-\overline{s}n}{q}\Big)\Big|.$$

On remarque alors que $\prod_{i=1}^4 \phi_{w_i}(\overline{s},q) = A\mathrm{e}(-s\vartheta(\mathbf{w})/q)$ pour un certain réel A tel que $|A| \in \{0,(q,2)^2\}$ et une certaine forme quadratique $\vartheta(\mathbf{X}) = a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + a_4X_4^2$, les coefficients a_i prenant leurs valeurs dans $\{0,2_q^2\}$ si q est impair, dans $\{0,1/4\}$ si $4 \,|\, q$, et dans $\{0,2_{q/2}^2\}$ si $q \equiv 2 \pmod 4$. On a donc

$$\Big|\sideset{}{^\star}\sum_{s=1}^{q} \sum_{\substack{\mathbf{c} \bmod Pq\\ \mathbf{c}\equiv\mathbf{h}\,(\mathrm{mod}\,P)}} \mathrm{e}\Big(\frac{\overline{s}(\mathbf{c}^2-n)}{q} + \frac{\mathbf{b}\cdot\mathbf{c}}{Pq} + \frac{us}{q}\Big)\Big|$$
$$\le \begin{cases} (q,2)^2(P,q)^4q^2 \max\limits_{\mathbf{w}\in\mathbb{Z}^4}\Big|\sideset{}{^\star}\sum\limits_{s=1}^{q}\mathrm{e}\Big(\dfrac{(u+\vartheta(\mathbf{w}))s-n\overline{s}}{q}\Big)\Big| & \text{si } (P,q)\,|\,\mathbf{b}\,,\\ 0 & \text{sinon}\,. \end{cases}$$

Notons que l'expression exacte de $\vartheta(\mathbf{w})$ nous importe peu puisqu'on utilise en conjonction avec (32) la majoration triviale $(a,b,q)^{1/2} \le (b,q)^{1/2}$; on applique alors ceci à l'inégalité ci-dessus, on obtient alors (33). L'inégalité (34) est un cas particulier de (33).

3.8. *Majorations des termes d'erreur.* Nous pouvons, à présent, donner des majorations des termes d'erreur E et E' définis dans (24) et (26).

• On obtient, par (25), (27), (29) et (33),

$$\sideset{}{^\star}\sum_{s=1}^{q} S_n\Big(\frac{\overline{s}}{q}+z\Big)\mathrm{e}\Big(\frac{us}{q}\Big)$$
$$\ll q^{-3/2+\varepsilon}(q,n)^{1/2}\frac{(P,q)^4}{P^4}\Big(\sum_{\substack{b\in\mathbb{Z}\\(P,q)|b}}\Big|I\Big(z,\frac{b}{Pq}\Big)\Big|\Big)^4$$
$$\ll q^{-3/2+\varepsilon}(q,n)^{1/2}\frac{(P,q)^4}{P^4}\Big(\frac{P}{(P,q)}+\sum_{\substack{|b|\le Pq(4|z|N+N^\varepsilon/N)\\(P,q)|b}}\min(N,|z|^{-1/2})\Big)^4;$$

pour $|z| \in [1/(2qN), 1/(qN)]$, on a

$$\sideset{}{^\star}\sum_{s=1}^{q} S_n\Big(\frac{\overline{s}}{q}+z\Big)\mathrm{e}\Big(\frac{us}{q}\Big)$$
$$\ll q^{-3/2+\varepsilon}(q,n)^{1/2}\frac{(P,q)^4}{P^4}\Big(\frac{P}{(P,q)}+\frac{Pq}{(P,q)}N^{1+\varepsilon}|z|^{1/2}\Big)^4,$$

d'où, par (24),

$$E \ll N^\varepsilon\sum_{q=1}^{N} q^{1/2+\varepsilon}(q,n)^{1/2} \ll N^{3/2+\varepsilon}\,.$$

• Par (26), (27), (29) et (33), la contribution correspondant à $|z| \geq 1/N^2$ dans E' est

$$\ll \sum_{q=1}^{N} \int_{1/N^2}^{1/(qN)} q^{-3/2+\varepsilon}(q,n)^{1/2}\frac{(P,q)^4}{P^4}\left(\frac{P}{(P,q)}+\frac{Pq}{(P,q)}N^{1+\varepsilon}|z|^{1/2}\right)^4 dz$$

$$\ll N^{1+\varepsilon}\sum_{q=1}^{N} q^{-1/2+\varepsilon}(q,n)^{1/2} \ll N^{3/2+\varepsilon}\,.$$

La contribution dans E' de l'intervalle d'intégration $|z| < 1/N^2$ est

$$\ll \int_{0}^{1/N^2} \sum_{q=1}^{N} q^{-3/2+\varepsilon}(q,n)^{1/2}\frac{(P,q)^4}{P^4}\left(\frac{P}{(P,q)}+\frac{Pq}{(P,q)}N^{\varepsilon}\right)^4 dz$$

$$\ll N^{-2+\varepsilon}\sum_{q=1}^{N} q^{5/2+\varepsilon}(q,n)^{1/2} \ll N^{3/2+\varepsilon}\,.$$

Par conséquent,

$$E + E' \ll N^{3/2+\varepsilon}\,. \tag{36}$$

3.9. *La série singulière.* Les relations (17), (23), (24), (26) et (36) donnent $R(n) = R'(n) + \mathcal{O}(n^{3/4+\varepsilon})$. On débute l'étude du terme principal $R'(n)$ par celle de la série singulière; on pose

$$A_n(P,q) = \sideset{}{^\star}\sum_{s=1}^{q} \frac{1}{(Pq)^4} \sum_{\substack{\mathbf{c} \bmod Pq \\ \mathbf{c}\equiv \mathbf{h} \,(\mathrm{mod}\, P)}} \mathrm{e}\left(\frac{s(\mathbf{c}^2-n)}{q}\right); \tag{37}$$

la *série singulière* est définie par

$$\mathfrak{S}(n) = \sum_{q=1}^{\infty} A_n(P,q)\,. \tag{38}$$

On note

$$A'_n(P,q) = P^4 A_n(P,q) \tag{39}$$

et

$$\mathfrak{S}'(n) = P^4\mathfrak{S}(n) = \sum_{q=1}^{\infty} A'_n(P,q)\,. \tag{40}$$

Dans un premier temps, on va mettre $\mathfrak{S}'(n)$ sous la forme d'un produit eulérien. Les évaluations de sommes exponentielles données en (34) nous permettront, dans un second temps, d'établir une minoration de $\mathfrak{S}'(n)$.

On définit la somme de Gauss restreinte à une progression arithmétique modulo P :

$$T(a,q,h,P)=\sum_{\substack{x \bmod Pq\\ x\equiv h \,(\mathrm{mod}\, P)}} \mathrm{e}\Big(\frac{ax^2}{q}\Big). \tag{41}$$

Par des méthodes classiques impliquant l'application du Théorème Chinois, on obtient

Lemme 10. *Soit q_1 et q_2 deux entiers positifs tels que $(q_1,q_2)=1$. Lorsque P est un entier sans facteur carré, on a*

$$T(a_1q_2+a_2q_1,q_1q_2,h,P)=T(a_1,q_1,h,P)T(a_2,q_2,h,P). \tag{42}$$

Puisque

$$A'_n(P,q)=\sum_{s=1}^{q}{}^{\star}\frac{1}{q^4}\Big(\prod_{i=1}^{4}T(s,q,h_i,P)\Big)\mathrm{e}\Big(-\frac{sn}{q}\Big), \tag{43}$$

pour $(q_1,q_2)=1$, on obtient (cf. [2; Lemme 6])

$$A'_n(P,q_1q_2)=A'_n(P,q_1)A'_n(P,q_2). \tag{44}$$

On peut aborder l'étude de la série singulière $\mathfrak{S}(n)$ proprement dite : nous allons en obtenir une minoration suffisamment bonne bien qu'elle dépende de n.

Assurons nous de la convergence absolue de série $\mathfrak{S}'(n)$ définie en (40) : d'après (33) et (36), on a

$$A'_n(P,q)\ll (P,q)^4q^{-3/2+\varepsilon}(q,n)^{1/2};$$

lorsque n et P sont fixés, c'est le terme général d'une série convergente. Par conséquent, par (44), la série $\mathfrak{S}'(n)$ s'écrit sous la forme d'un produit eulérien

$$\mathfrak{S}'(n)=\prod_p\Big(1+\sum_{m=1}^{\infty}A'_n(P,p^m)\Big)=\prod_p\chi_p(n). \tag{45}$$

De (34), on déduit les inégalités

$$|\chi_p(n)-1|<\begin{cases}\dfrac{2p^{3/2}-1}{(p^{3/2}-1)^2} & \text{si } (p,nP)=1,\\[2mm] \dfrac{2}{p}+\dfrac{1}{p(p-1)} & \text{si } p\,|\,n \text{ et } (p,P)=1.\end{cases}$$

Puisque P est pair, cela conduit à

$$\prod_{(p,nP)=1}\chi_p(n)\ge\prod_{p\ge3}\Big(1-\frac{2p^{3/2}-1}{(p^{3/2}-1)^2}\Big)>\frac{1}{5}$$

et

$$\prod_{\substack{(p,P)=1\\ p|n}} \chi_p(n) \geq \Big(\prod_{p|n}\Big(1-\frac{1}{p}\Big)\Big)^2\Big(\prod_{p\geq 3}\Big(1-\frac{2p-1}{(p-1)^3}\Big)\Big) > \frac{0.0001}{(\log\log n)^2}\,,$$

d'où en posant $c = 0.00002$, on a

$$\prod_{(p,P)=1} \chi_p(n) > \frac{c}{(\log\log n)^2}\,. \tag{46}$$

Lorsque p divise P, on traite les $\chi_p(n)$ en étudiant le nombre de solutions de la congruence $n \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \pmod{p^l}$. C'est ici et uniquement ici qu'interviennent les résultats du paragraphe 3.2. On a

Lemme 11. *Pour tout nombre premier p divisant P, on a*

$$\chi_p(n) \geq \frac{1}{p^3}. \tag{47}$$

P r e u v e. Désignons par $M(q)$ le nombre de solutions du système

$$\begin{cases} n \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \pmod{q}\,,\\ \mathbf{x} \bmod Pq\,,\\ \mathbf{x} \equiv \mathbf{h} \pmod{P}\,. \end{cases}$$

Du Théorème Chinois et du fait que P est sans facteur carré, on déduit que pour tout nombre premier p et tout entier $l \geq 1$,

$$1 + \sum_{m=1}^{l} A'_n(P, p^m) = \frac{M(p^l)}{p^{3l}}\,,$$

et par suite

$$\chi_p(n) = \lim_{l\to\infty} \frac{M(p^l)}{p^{3l}}\,. \tag{48}$$

Soit $p \,|\, P$; alors $M(p^l)$ est encore le nombre de solutions de

$$\begin{cases} x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv n \pmod{p^l}\,,\\ \mathbf{x} \bmod p^{l+1}\,,\\ \mathbf{x} \equiv \mathbf{h} \pmod{p}\,. \end{cases}$$

Lorsque $l = 1$, le système (16) entraîne que (h_1, h_2, h_3, h_4) est solution de cette congruence et en outre $h_1 \not\equiv 0 \pmod{p}$. Soit alors $l \geq 2$; on choisit arbitrairement le triplet (x_2, x_3, x_4) tel que

$$x_j \equiv h_j \pmod{p^l} \quad (2 \leq j \leq 4)\,;$$

il y a $p^{3(l-1)}$ choix possibles; d'après le Lemme 9 de [2], puisque $h_1 \not\equiv 0 \pmod{p}$, la congruence

$$x_1^2 \equiv n - x_2^2 - x_3^2 - x_4^2 \pmod{p^l}$$

admet une solution x_1. Par conséquent, pour tout $l \geq 1$, on obtient $M(p^l) \geq p^{3(l-1)}$. Puis (48) entraîne (47).

Le Lemme 11 combiné à (39), (40), (45) et (46) implique la proposition suivante :

PROPOSITION 2. *Il existe c, indépendant de n et de P, réel strictement positif tel que*

$$\mathfrak{S}(n) > \frac{c}{(\log\log n)^2} \cdot \frac{1}{P^7}\,. \tag{49}$$

3.10. *L'intégrale singulière.* Nous achevons l'estimation asymptotique de $R'(n)$ par l'étude de l'intégrale singulière, associée à ce problème de représentation d'un entier en somme de quatre carrés. Notons que celle-ci ne dépend pas du choix de $\mathbf{h}$, elle est semblable à l'intégrale singulière dans le problème de Waring; néanmoins, la présence du poids γ modifie quelque peu son évaluation. Nous n'en obtenons pas une valeur effective, mais seulement un équivalent. Grâce à (27), on a

$$\int\limits_{-1/(qN)}^{1/(qN)} \bigg(\int\limits_0^N \gamma\Big(\frac{t}{N}\Big)\mathrm{e}(zt^2)\,dt\bigg)^4 \mathrm{e}(-zn)\,dz = \mathfrak{I}(n) + \mathcal{O}\bigg(\int\limits_{1/(qN)}^{\infty} \frac{dz}{z^2}\bigg)\,,$$

où

$$\mathfrak{I}(n) = \int\limits_{\mathbb{R}} \bigg(\int\limits_0^N \gamma\Big(\frac{t}{N}\Big)\mathrm{e}(zt^2)\,dt\bigg)\mathrm{e}(-zn)\,dz\,.$$

D'où par (26) et (33), on a

$$R'(n) = \widetilde{\mathfrak{S}}(n)\mathfrak{I}(n) + \mathcal{O}\bigg(N \sum_{q=1}^{N} q^{-1/2+\varepsilon}(q,n)^{1/2}\frac{(P,q)^4}{P^4}\bigg)\,,$$

où

$$\widetilde{\mathfrak{S}}(n) = \sum_{q=1}^{N}\sum_{s=1}^{q}{}^{\star} \frac{1}{(Pq)^4} \sum_{\substack{\mathbf{c} \bmod Pq \\ \mathbf{c}\equiv\mathbf{h}\,(\mathrm{mod}\,P)}} \mathrm{e}\Big(\frac{s(\mathbf{c}^2-n)}{q}\Big)\,;$$

de (33), on déduit $\widetilde{\mathfrak{S}}(n) = \mathfrak{S}(n) + O(N^{-1/2+\varepsilon})$. La majoration (27) donne $|\mathfrak{I}(n)| \leq N^2$, d'où il suit $R'(n) = \mathfrak{S}(n)\mathfrak{I}(n) + O(N^{3/2+\varepsilon})$.

Les changements de variables $u = t/N$ et $w = zn$ et la relation (17) conduisent à l'égalité $\mathfrak{I}(n) = n\mathfrak{I} + O(n^{1/2})$ où l'*intégrale singulière* $\mathfrak{I}$ est définie par

$$\mathfrak{I} = \int\limits_{\mathbb{R}} \Big(\int\limits_0^1 \gamma(u)\mathrm{e}(zu^2)\,du\Big)^4 \mathrm{e}(-w)\,dw\,. \tag{50}$$

Par (23), (24), (26) et (36), on obtient alors

$$R(n) = R'(n) + O(n^{3/4+\varepsilon}) = n\mathfrak{S}(n)\mathfrak{I} + O(n^{3/4+\varepsilon})\,. \tag{51}$$

On montre alors, soit par le théorème intégral de Fourier (cf. [2] et [9]), soit en estimant en moyenne $R(n)$, que $\mathfrak{I}$ est un nombre strictement positif. Finalement, (49) et (51) donnent

$$R(n) = n\mathfrak{S}(n)\mathfrak{I}(1+o(1))\,, \tag{52}$$

avec

$$\mathfrak{I} > 0 \quad \text{et} \quad \mathfrak{S}(n) > \frac{c}{(\log\log n)^2}\cdot\frac{1}{P^7}\,.$$

Par conséquent, pour tout n assez grand, $R(n)$ est strictement positif, et par suite n est la somme de 4 carrés d'éléments de $\mathcal{C}_K$.

3.11. *Fin de la démonstration du Théorème* 2. La suite $\mathcal{C}_K^{(2)}$ est donc une base asymptotique d'ordre 4, et $(\mathcal{C}_K^{(2)})_{K\geq 1}$ est une suite strictement décroissante de bases asymptotiques; on pose $N_0 = 0$ et pour tout $K \geq 1$, on note N_K le plus petit entier strictement supérieur à N_{K-1} tel que tout entier n supérieur à N_K^2 est la somme d'au plus quatre carrés d'éléments de $\mathcal{C}_K$. La suite $(N_K)_{K\geq 0}$ est strictement croissante. On est, à présent, en mesure de définir la suite $\mathcal{C}$ aux propriétés désirées : pour tout $K \geq 0$, on pose

$$\mathcal{C}_K \cap [N_K, N_{K+1}[= \mathcal{C} \cap [N_K, N_{K+1}[\,.$$

On a donc les inclusions

$$\mathcal{C}_K \cap [0, N_{K+1}[\subset \mathcal{C}, \qquad [N_K, +\infty[\cap \mathcal{C} \subset \mathcal{C}_K\,.$$

Soit maintenant n un entier; il existe $K \geq 1$ tel que $N_K^2 \leq n < N_{K+1}^2$; il existe donc $x_1, x_2, x_3, x_4 \in \mathcal{C}_K \cap [0, N_{K+1}[$ tels que $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$. La première inclusion ci-dessus assure que $x_1, x_2, x_3, x_4 \in \mathcal{C}$, et par suite que $\mathcal{C}^{(2)}$ est une base d'ordre 4. La seconde inclusion entraîne que la suite $\mathcal{C}$ vérifie les hypothèses du Lemme 2, et par conséquent $\mathcal{C}$ n'est pas une base. Cela achève la démonstration du Théorème 2.

3.12. *Une remarque à propos du nombre d'éléments de* $\mathcal{C}^{(2)}$ *inférieurs à* x. Pour tout σ, on cherche une suite $\mathcal{C}$ vérifiant le Théorème 2 et telle que $C^{(2)}(x) \sim x^\sigma$. La suite $\mathcal{C}^{(2)}$ devant être une base d'ordre 4, par un argument combinatoire, on obtient $\sigma \geq 1/4$. D'autre part, la suite $\mathcal{C}$ n'est pas une base, contient les entiers 0 et 1, donc n'est pas une base asymptotique; par conséquent, sa densité asymptotique inférieure est nulle, d'où $\liminf C^{(2)}(x)/\sqrt{x} = 0$ et $\sigma < 1/2$.

La méthode probabiliste basée sur le lemme de Borel–Cantelli a été initiée en 1954 par P. Erdős [5] et développée récemment par I. Z. Ruzsa [13]. Combinée aux conclusions du Théorème 2 et à la relation (49), elle

permet de prouver l'existence d'une suite $\mathcal{C}$ qui n'est pas une base, dont la suite des carrés $\mathcal{C}^{(2)}$ est une base d'ordre 4 et telle que l'on ait

$$\mathcal{C}^{(2)} \ll (x \log^5 x)^{1/4}\,. \tag{53}$$

Au cours de la construction par blocs du paragraphe précédent, on choisit la suite croissante $(N_K)_{K\geq 1}$ telle que P_K^7 soit un $\mathcal{O}((\log N_K)^{1/2})$. On déduit alors de (52) une suite $\mathcal{C}_0$ non base, telle que $\mathcal{C}_0^{(2)}$ soit une base d'ordre 4, et telle que pour tout entier n suffisamment grand, le nombre de représentations de n en somme de 4 carrés de $\mathcal{C}_0^{(2)}$ est supérieur à $n/\log n$. Observons par ailleurs que pour un tel choix de la suite $(N_K)_{K\geq 1}$, on a aussi $C_0(x) \gg x/\log x$.

Suivant la procédure de I. Z. Ruzsa, on extrait de la suite $\mathcal{C}_0$ une sous-suite aléatoire $\mathcal{C}$ telle que pour chaque carré m de $\mathcal{C}_0^{(2)}$ la probabilité d'appartenir à $\mathcal{C}^{(2)}$ est

$$\Pr[m \in \mathcal{C}^{(2)}] \sim \alpha \frac{(\log m)^{5/4}}{m^{1/4}}\,, \tag{54}$$

où α est une certaine constante positive absolue suffisamment grande.

Le Théorème 3.9 de [13] entraîne donc que presque sûrement, $\mathcal{C}^{(2)}$ est une base d'ordre 4. De plus en tant que sous-suite de $\mathcal{C}_0$, la suite $\mathcal{C}$ n'est pas une base.

Par ailleurs, la relation (54) donne

$$C^{(2)}(x) = \sum_{\substack{m\leq x\\ m\in\mathcal{C}_0^{(2)}}} \Pr[m \in \mathcal{C}^{(2)}] = \mathcal{O}((x\log^5 x)^{1/4})\,, \tag{55}$$

ce qui entraîne le résultat annoncé.

Le Théorème 2 et la méthode probabiliste établie par I. Z. Ruzsa assurent ainsi l'existence d'une suite $\mathcal{C}$ n'étant pas une base, telle que la suite des carrés est une base d'ordre 4, et dont la limite lorsque x tend vers l'infini du rapport $\log C^{(2)}(x)/\log x$ existe et se trouve arbitrairement comprise au sens large entre 1/4 et 1/2.

Références

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

[2] H. Davenport, *Analytic Methods for Diophantine Equations and Diophantine Inequalities*, Ann Arbor, 1962.

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

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

[5] P. Erdős, *Some results on additive number theory*, Proc. Amer. Math. Soc. 5 (1954), 847–853.
[6] P. Erdős and M. B. Nathanson, *Lagrange's theorem and thin subsequences of squares*, dans : Contributions to Probability, J. Gani et V. K. Rohatgi (eds.), Academic Press, New York, 1981, 3–9.
[7] T. Estermann, *On Kloosterman's sums*, Mathematika 8 (1961), 83–86.
[8] D. R. Heath-Brown, *Cubic forms in ten variables*, Proc. London Math. Soc. (3) 47 (1983), 225–257.
[9] C. Hooley, *On nonary cubic forms*, J. Reine Angew. Math. 386 (1988), 32–98.
[10] —, *On Waring's problem*, Acta Math. 157 (1986), 49–97.
[11] H. D. Kloosterman, *On the representation of a number in the form* $ax^2 + by^2 + cz^2 + dt^2$, ibid. 49 (1926), 407–464.
[12] M. B. Nathanson, *Waring's problem for sets of density zero*, dans : Number Theory, Philadelphia, 1980, M. I. Knopp (ed.), Lecture Notes in Math. 899, Springer, Heidelberg, 1981, 301–310.
[13] I. Z. Ruzsa, *On a probabilistic method in additive number theory*, Publ. Math. Orsay, 1989, 71–92.
[14] E. C. Titchmarsh, *The Theory of the Riemann Zeta-function*, Oxford Univ. Press, 1951.
[15] R. C. Vaughan, *The Hardy–Littlewood Method*, Cambridge Univ. Press, 1981.
[16] E. Wirsing, *Thin subbases*, Analysis 6 (1986), 285–308.
[17] J. Zöllner, *Über eine Vermutung von Choi, Erdős und Nathanson*, Acta Arith. 45 (1985), 211–213.

ALGORITHMIQUE ARITHMÉTIQUE EXPÉRIMENTALE
UNITÉ MIXTE DE RECHERCHE 9936 CNRS
UNIVERSITÉ BORDEAUX I
351, COURS DE LA LIBÉRATION
F 33405 TALENCE CEDEX
FRANCE

Reçu le 23.4.1992
et révisé le 26.10.1993 (2254)