70.01M

SESSION 2007

Filière MP

MATHÉMATIQUES MPI 1

Épreuve commune aux ENS de Paris, Lyon et Cachan

Durée : 6 heures

L'usage de calculatrice est interdit

Avertissement

La qualité de la rédaction sera un facteur important d'appréciation des copies. On invite donc le candidat à produire des raisonnements clairs, complets et concis. Le candidat peut utiliser les résultats énoncés dans les questions ou parties précédentes ; il veillera toutefois à préciser la référence du résultat utilisé.

Les parties I à V sont essentiellement indépendantes les unes des autres, à l'exception près de la dernière question de la partie III.

Objectif

Ce problème est consacré à l'étude des solutions entières d'équations de la forme

$$X_1^d + \cdots + X_m^d = t$$

où d et m sont des entiers strictement positifs et t un entier positif ou nul.

Notations

On note $\mathbf{N}$ l'ensemble des entiers positifs ou nuls, $\mathbf{Z}$ l'anneau des entiers relatifs, $\mathbf{Q}$ le corps des nombres rationnels, $\mathbf{R}$ le corps des réels et $\mathbf{C}$ le corps des complexes. Pour tout $n \geqslant 2$, $(\mathbf{Z}/n\mathbf{Z})^\times$ désigne l'ensemble des éléments inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$; la multiplication munit $(\mathbf{Z}/n\mathbf{Z})^\times$ d'une structure de groupe. On note $\mathscr{M}_n(\mathbf{C})$ l'algèbre des matrices $n \times n$ sur $\mathbf{C}$.

Pour tout nombre réel α, on note $\lfloor \alpha \rfloor$ la partie entière de α, définie par :

$$\lfloor \alpha \rfloor = \max\{\, t \in \mathbf{Z} \mid t \leqslant \alpha \,\}.$$

Pour tout ensemble fini X, on note $\sharp X$ son cardinal. Si Y est une partie d'un ensemble X, on note $X - Y$ le complémentaire de Y dans X. Pour tout entier n de $\mathbf{N} - \{0\}$, on note $\mathfrak{S}_n$ le groupe des permutations de $\{1, \ldots, n\}$. Pour tout entier n de $\mathbf{N}$ et tout élément p de $\mathbf{Z}$, on note

$$\binom{n}{p} = \begin{cases} \frac{n!}{p!(n-p)!} \text{ si } 0 \leqslant p \leqslant n, \\ 0 \text{ sinon.} \end{cases}$$

Soit X une partie de $\mathbf{N}$. Si X n'est pas vide, on note $\min(X)$ le plus petit élément de X et on dit que $\min(X)$ est fini ; par contre, si X est vide, on pose $\min(X) = +\infty$.

Partie I

Étude de cas particuliers

1. Soient m un entier strictement positif et t un élément de $\mathbf{N}$.

a. Montrer que l'ensemble

$$\left\{ (x_1, \ldots, x_m) \in \mathbf{N}^m \,\middle|\, \sum_{i=1}^{m} x_i = t \right\}$$

est fini.

On note dans la suite $N_1^m(t)$ son cardinal.

b. Montrer que pour tout entier $m \geqslant 2$ et tout t de $\mathbf{N}$ on a la relation

$$N_1^m(t) = \sum_{k=0}^{t} N_1^{m-1}(k).$$

c. Montrer la formule

$$N_1^m(t) = \binom{t+m-1}{m-1}$$

pour tout m de $\mathbf{N} - \{0\}$ et tout t de $\mathbf{N}$.

d. En déduire pour tout entier strictement positif m, l'équivalence

$$\begin{array}{rcl} N_1^m(t) & \sim & \dfrac{t^{m-1}}{(m-1)!} \\ t & \to & +\infty. \end{array}$$

2. On s'intéresse maintenant au cas où $d = 2$ et $m = 3$.

a. Déterminer l'image des applications

$$\begin{array}{rcl} (\mathbf{Z}/8\mathbf{Z})^\times & \longrightarrow & (\mathbf{Z}/8\mathbf{Z})^\times \\ x & \longmapsto & x^2 \end{array} \qquad \text{et} \qquad \begin{array}{rcl} \mathbf{Z}/8\mathbf{Z} & \longrightarrow & \mathbf{Z}/8\mathbf{Z} \\ x & \longmapsto & x^2. \end{array}$$

b. Donner l'ensemble des solutions de l'équation

$$X^2 + Y^2 + Z^2 + T^2 = 0$$

dans $(\mathbf{Z}/8\mathbf{Z})^\times \times (\mathbf{Z}/8\mathbf{Z})^3$.

c. Soit b un entier strictement positif. Montrer que l'équation

$$X^2 + Y^2 + Z^2 = 8b - 1$$

n'a pas de solution dans $\mathbf{Q}^3$.

d. Soient b un entier strictement positif et a un entier positif ou nul. Montrer que l'équation

$$X^2 + Y^2 + Z^2 = 4^a(8b - 1)$$

n'admet pas de solution dans $\mathbf{N}^3$.

Partie II

Somme de quatre carrés

Dans cette partie on s'intéresse au cas $d = 2$ et $m = 4$.

1. Soit p un nombre premier impair.

a. Déterminer le noyau du morphisme de groupes

$$\begin{array}{rcl} (\mathbf{Z}/p\mathbf{Z})^\times & \longrightarrow & (\mathbf{Z}/p\mathbf{Z})^\times \\ x & \longmapsto & x^2. \end{array}$$

b. En déduire le cardinal de son image et le cardinal de l'ensemble

$$\{\, x^2,\ x \in \mathbf{Z}/p\mathbf{Z} \,\}.$$

c. Montrer que les ensembles

$$\{\, x^2,\ x \in \mathbf{Z}/p\mathbf{Z} \} \qquad \text{et} \qquad \{-1 - y^2,\ y \in \mathbf{Z}/p\mathbf{Z}\}$$

s'intersectent.

d. Montrer qu'il existe des entiers positifs ou nuls x, y et m avec $0 < m < p$ tels que

$$1 + x^2 + y^2 = mp.$$

2. On note $\mathbf{H}$ le $\mathbf{R}$-sous-espace vectoriel du $\mathbf{R}$-espace vectoriel $\mathscr{M}_2(\mathbf{C})$ engendré par les matrices

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \boldsymbol{I} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \boldsymbol{J} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad \boldsymbol{K} = \boldsymbol{IJ}.$$

On identifie $\mathbf{R}$ avec son image par l'application $a \mapsto a\mathbf{1}$. En particulier, on note a pour $a\mathbf{1}$.

a. Montrer que $(\mathbf{1}, \boldsymbol{I}, \boldsymbol{J}, \boldsymbol{K})$ forme une base de $\mathbf{H}$ et que

$$\forall a, b \in \mathbf{H}, \qquad ab \in \mathbf{H}.$$

b. Montrer que l'application $\tau : \mathbf{H} \to \mathbf{H}$ définie par

$$\forall a, b, c, d \in \mathbf{R}, \qquad \tau(a + b\boldsymbol{I} + c\boldsymbol{J} + d\boldsymbol{K}) = a - b\boldsymbol{I} - c\boldsymbol{J} - d\boldsymbol{K}$$

est $\mathbf{R}$-linéaire et vérifie

$$\forall x, y \in \mathbf{H}, \qquad \tau(xy) = \tau(y)\tau(x).$$

c. Montrer qu'il existe une application $N : \mathbf{H} \to \mathbf{R}$ telle que

$$\forall z \in \mathbf{H}, \quad N(z) = z\tau(z) = \tau(z)z.$$

On exprimera cette fonction en termes des coordonnées dans la base $(\mathbf{1}, \boldsymbol{I}, \boldsymbol{J}, \boldsymbol{K})$.

d. Montrer que

$$\forall z_1, z_2 \in \mathbf{H}, \quad N(z_1 z_2) = N(z_1)N(z_2).$$

Dans le reste de cette partie, on note

$$\mathscr{N}_2^4 = \left\{ t \in \mathbf{N} \,\middle|\, \exists (x_1, x_2, x_3, x_4) \in \mathbf{N}^4,\ t = \sum_{i=1}^{4} x_i^2 \right\}.$$

3. Montrer que

$$\forall a, b \in \mathscr{N}_2^4, \qquad ab \in \mathscr{N}_2^4.$$

4. Soit p un nombre premier impair.

a. Montrer qu'il existe $m \in \{1, \ldots, p-1\}$ tel que mp appartienne à $\mathscr{N}_2^4$.

On note m_0 le plus petit entier strictement positif tel que $m_0 p \in \mathscr{N}_2^4$.

b. Soit m un entier pair tel qu'il existe $(x_1, x_2, x_3, x_4) \in \mathbf{N}^4$ avec

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

(i) Montrer qu'il existe une permutation σ de $\mathfrak{S}_4$ telle que les entiers

$$x_{\sigma(1)} + x_{\sigma(2)}, \qquad x_{\sigma(1)} - x_{\sigma(2)}, \qquad x_{\sigma(3)} + x_{\sigma(4)} \qquad \text{et} \qquad x_{\sigma(3)} - x_{\sigma(4)}$$

soient tous les quatre pairs et positifs.

(ii) En déduire que $\frac{mp}{2}$ appartient à $\mathscr{N}_2^4$.

c. Montrer que m_0 est impair.

d. On suppose que $m_0 \neq 1$. On se donne $(x_1, x_2, x_3, x_4) \in \mathbf{N}^4$ tels que

$$m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

(i) Montrer qu'il existe des entiers b_1, b_2, b_3 et b_4 tels que les entiers donnés par $y_i = x_i - b_i m_0$ pour $i \in \{1, 2, 3, 4\}$ satisfassent les trois conditions suivantes :

$$|y_i| < \frac{1}{2} m_0 \text{ pour } i \in \{1, 2, 3, 4\},$$
$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < m_0^2$$

et

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \text{ modulo } m_0.$$

On note $m_1 = (y_1^2 + y_2^2 + y_3^2 + y_4^2)/m_0$.

(ii) Montrer qu'il existe $(z_1, z_2, z_3, z_4) \in \mathbf{N}^4$ tels que

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = m_0^2 m_1 p$$

et

$$z_i \equiv 0 \text{ modulo } m_0 \text{ pour } i \in \{1, 2, 3, 4\}.$$

(On pourra considérer le produit $(x_1 + x_2\boldsymbol{I} + x_3\boldsymbol{J} + x_4\boldsymbol{K})(y_1 - y_2\boldsymbol{I} - y_3\boldsymbol{J} - y_4\boldsymbol{K})$.)

e. Montrer que $m_0 = 1$.

5. Montrer que $\mathbf{N} = \mathscr{N}_2^4$.

Partie III

Les fonctions g et G

Pour tout entier d strictement positif, on note

$$g(d) = \min\left\{ m \in \mathbf{N} \,\middle|\, \forall t \in \mathbf{N}, \exists (x_1, \ldots, x_m) \in \mathbf{N}^m,\ t = \sum_{i=1}^{m} x_i^d \right\}$$

et

$$G(d) = \min\left\{ m \in \mathbf{N} \,\middle|\, \exists t_0 \in \mathbf{N},\ \forall t \in \mathbf{N}, t \geqslant t_0 \Rightarrow \exists (x_1, \ldots, x_m) \in \mathbf{N}^m,\ t = \sum_{i=1}^{m} x_i^d \right\}.$$

1. Soit d un entier strictement positif.

a. Soit $t = 2^d \lfloor (\frac{3}{2})^d \rfloor - 1$. Soit m un entier strictement positif. Montrer que si $(x_1, \ldots, x_m) \in \mathbf{N}^m$ vérifie

$$t = \sum_{i=1}^{m} x_i^d$$

alors

$$x_i \in \{0, 1, 2\} \text{ pour } i \in \{1, \ldots, m\}.$$

b. Montrer la relation

$$g(d) \geqslant 2^d + \left\lfloor \left(\frac{3}{2}\right)^d \right\rfloor - 2.$$

2. Y a-t-il équivalence entre la finitude de $g(d)$ et celle de $G(d)$? Dans le cas où ils sont tous les deux finis, donner une inégalité entre $G(d)$ et $g(d)$.

3. Déterminer $g(2)$ et comparer la valeur obtenue avec la borne donnée dans la question 1.b. Déterminer $G(2)$.

Partie IV

Expression intégrale

Soient d et m des entiers strictement positifs. Pour tout entier t de $\mathbf{N}$, on note

$$N_d^m(t) = \sharp\left\{ (x_1, \ldots, x_m) \in \mathbf{N}^m \,\middle|\, \sum_{i=1}^{m} x_i^d = t \right\}.$$

Pour tout nombre réel $B \in [1, +\infty[$, on note

$$N_d^m(t, B) = \sharp\left\{ (x_1, \ldots, x_m) \in \mathbf{N}^m \cap [0, B]^m \,\middle|\, \sum_{i=1}^{m} x_i^d = t \right\}.$$

On désigne par f_d^m la fonction

$$\begin{aligned} \mathbf{R}^m &\longrightarrow \mathbf{R} \\ (x_1, \ldots, x_m) &\longmapsto \sum_{i=1}^{m} x_i^d. \end{aligned}$$

1. Montrer que pour tout n de $\mathbf{Z}$, on a

$$\int_0^1 e^{2i\pi n\alpha}\, \mathrm{d}\alpha = \begin{cases} 1 \text{ si } n = 0, \\ 0 \text{ sinon.} \end{cases}$$

2. Montrer la relation

$$N_d^m(t, B) = \int_0^1 \sum_{\boldsymbol{x} \in \mathbf{Z}^m \cap [0,B]^m} e^{2i\pi(f_d^m(\boldsymbol{x}) - t)\alpha}\, \mathrm{d}\alpha.$$

3. Comparer $N_d^m(t, B)$ et $N_d^m(t)$ si $B \geqslant t^{1/d}$.

Le reste du problème est consacré aux premières étapes de la démonstration de la finitude de $G(d)$, qui passe par une minoration de $N_d^m(t)$.

Partie V

Majoration de sommes d'exponentielles

Soient $(G, +)$ et $(H, +)$ des groupes commutatifs. Pour toute application ϕ de G dans H et tout entier $k \geqslant 1$, on définit

$$\begin{aligned} \phi_k : G^k &\longrightarrow H \\ (g_1, \ldots, g_k) &\longmapsto \sum_{(\epsilon_1, \ldots, \epsilon_k) \in \{0,1\}^k} (-1)^{\epsilon_1 + \cdots + \epsilon_k} \phi\left(\sum_{i=1}^{k} \epsilon_i g_i \right). \end{aligned}$$

En particulier,

$$\forall g \in G, \qquad \phi_1(g) = \phi(0) - \phi(g).$$

1. a. Calculer ϕ_2.

b. Montrer que, pour tout entier k strictement positif,

$$\forall (g_1, \ldots, g_{k-1}) \in G^{k-1}, \qquad \phi_k(g_1, \ldots, g_{k-1}, 0) = 0.$$

c. Montrer que, pour tout entier k de $\mathbf{N} - \{0\}$ et tout $(g_1, \ldots, g_{k+1}) \in G^{k+1}$, on a la relation

$$\begin{aligned} &\phi_{k+1}(g_1, \ldots, g_{k+1}) \\ &= \phi_k(g_1, \ldots, g_{k-1}, g_k) + \phi_k(g_1, \ldots, g_{k-1}, g_{k+1}) - \phi_k(g_1, \ldots, g_{k-1}, g_k + g_{k+1}) \end{aligned}$$

d. Montrer que, pour tout entier $k \geqslant 1$ et toute permutation σ de $\mathfrak{S}_k$, on a

$$\forall (g_1, \ldots, g_k) \in G^k, \quad \phi_k(g_{\sigma(1)}, \ldots, g_{\sigma(k)}) = \phi_k(g_1, \ldots, g_k).$$

2. On se place dans le cas où G est le groupe additif d'un anneau commutatif A. Soit n un entier strictement positif et soit

$$\begin{array}{rcl} \phi : A & \longrightarrow & A \\ x & \longmapsto & x^n. \end{array}$$

a. Calculer ϕ_2.

b. Montrer que l'on a

$$\forall (a_1, \ldots, a_n) \in A^n, \qquad \phi_n(a_1, \ldots, a_n) = (-1)^n n! a_1 \cdots a_n.$$

Si U est une partie du groupe abélien G, on note pour tout g de G,

$$U - g = \{\, h - g,\ h \in U \,\}.$$

On pose également

$$U^D = \{\, g - h,\ g \in U \text{ et } h \in U \,\},$$

et pour tout entier $k \geqslant 1$ et tout $(g_1, \ldots, g_k) \in G^k$,

$$U(g_1, \ldots, g_k) = \bigcap_{(\epsilon_1, \ldots, \epsilon_k) \in \{0,1\}^k} (U - (\epsilon_1 g_1 + \cdots + \epsilon_k g_k)).$$

Par convention, si $k = 0$, $U(g_1, \ldots, g_k)$ désigne U.

3. Montrer que pour tout entier $k \geqslant 1$, on a

$$\forall (g_1, \ldots, g_k) \in G^k,\ U(g_1, \ldots, g_k) = U(g_1, \ldots, g_{k-1}) \cap (U(g_1, \ldots, g_{k-1}) - g_k).$$

Soit $\phi : G \to \mathbf{R}$ une application. On note

$$\begin{array}{rcl} \mathbf{e} : \mathbf{R} & \longrightarrow & \mathbf{C} \\ \theta & \longmapsto & e^{2i\pi\theta}. \end{array}$$

Soit U une partie finie de G ; on considère la somme

$$S = \sum_{g \in U} \mathbf{e}(\phi(g)).$$

4. a. Montrer que

$$|S|^2 = \sum_{g \in U} \sum_{h \in U} \mathbf{e}(\phi(g) - \phi(h)).$$

b. Montrer que

$$|S|^2 = \sum_{g_1 \in U^D} \sum_{g_2 \in U(g_1)} \mathbf{e}(\phi(g_1 + g_2) - \phi(g_2)).$$

c. Montrer que

$$|S|^2 \leqslant \sum_{g_1 \in U^D} \left| \sum_{g_2 \in U(g_1)} \mathbf{e}(\phi_2(g_1, g_2)) \right|.$$

5. a. Soit n un entier strictement positif. Montrer que pour tout $(x_1, \ldots, x_n)$ de $\mathbf{R}^n$,

$$\left(\sum_{i=1}^{n} x_i \right)^2 \leqslant n \sum_{i=1}^{n} x_i^2.$$

b. Montrer que pour tout entier $k \geqslant 2$,

$$|S|^{2^{k-1}} \leqslant (\sharp U^D)^{2^{k-1}-k} \sum_{(g_1,\ldots,g_{k-1}) \in (U^D)^{k-1}} \left| \sum_{g_k \in U(g_1,\ldots,g_{k-1})} \mathbf{e}(\phi_k(g_1, \ldots, g_k)) \right|.$$

(On pourra raisonner par récurrence en utilisant le cas $k = 2$.)

Dans la suite de cette partie, on fixe des entiers $d \geqslant 2$ et $m \geqslant 1$. Soit α un nombre réel. Pour tout nombre réel B de $[1, +\infty[$, on pose

$$S_B^1(\alpha) = \sum_{\{ n \in \mathbf{N} | 0 \leqslant n \leqslant B \}} \mathbf{e}(\alpha n^d).$$

6. a. Montrer que pour tous a, b de $\mathbf{Z}$ avec $a \leqslant b$, tout α de $\mathbf{R}$ et tout n de $\mathbf{Z}$, on a l'inégalité

$$\left| \sum_{j=a}^{b} \mathbf{e}(\alpha n j) \right| \leqslant \min \left(\frac{2}{|1 - \mathbf{e}(\alpha n)|}, b - a + 1 \right),$$

avec la convention que le terme de droite vaut $b - a + 1$ si $\mathbf{e}(\alpha n) = 1$.

On note pour tout x de $\mathbf{R}$

$$\|x\| = \inf\{|x - n|, n \in \mathbf{Z}\}$$

b. Montrer que

$$\forall a, b \in \mathbf{R}, \quad \|a + b\| \leqslant \|a\| + \|b\|.$$

c. Montrer que pour tout nombre réel x, $|1 - \mathbf{e}(x)| \geqslant \|x\|$.

d. Montrer que

$$|S_B^1(\alpha)|^{2^{d-1}} \leqslant (2B+1)^{2^{d-1}-d} \sum_{(n_1,\ldots,n_{d-1}) \in ([-B,B] \cap \mathbf{Z})^{d-1}} \min \left(\frac{2}{\|d! n_1 \cdots n_{d-1} \alpha\|}, B + 1 \right).$$

e. On note

$$N_B^\alpha = \sharp\left\{ (n_1, \ldots, n_{d-1}) \in ([-B, B] \cap \mathbf{Z})^{d-1} \,\middle|\, \|d! n_1 \cdots n_{d-1}\alpha\| < \frac{1}{B} \right\}$$

et pour tout $(n_1, \ldots, n_{d-2})$ de $([-B, B] \cap \mathbf{Z})^{d-2}$, on note $M_B^\alpha(n_1, \ldots, n_{d-2})$ l'entier

$$\sharp\left\{ n_{d-1} \in [-B, B] \cap \mathbf{Z} \,\middle|\, \|d! n_1 \cdots n_{d-1}\alpha\| < \frac{1}{B} \right\}.$$

(i) Exprimer N_B^α en termes des $M_B^\alpha(n_1, \ldots, n_{d-2})$.

(ii) Pour tout t de $\mathbf{R}$, on note $\{t\} = t - \lfloor t \rfloor$. Montrer que pour tout $(n_1, \ldots, n_{d-2})$ de $([-B, B] \cap \mathbf{Z})^{d-2}$, et tout entier δ de $\mathbf{N} \cap [0, B[$,

$$\sharp\left\{ n_{d-1} \in [-B, B] \cap \mathbf{Z} \,\middle|\, \{d! n_1 \cdots n_{d-1}\alpha\} \in \left[\frac{\delta}{B}, \frac{\delta+1}{B}\right[\right\} \leqslant 2M_B^\alpha(n_1, \ldots, n_{d-2}).$$

(On pourra se donner des éléments convenables n_{d-1}^0 et n_{d-1}^1 de cet ensemble et considérer les différences $n_{d-1} - n_{d-1}^i$.)

(iii) En déduire que

$$|S_B^1(\alpha)|^{2^{d-1}} \leqslant 8(2B+1)^{2^{d-1}-d+1}(\ln(B)+1)N_{\lfloor B \rfloor}^\alpha.$$

(On pourra se ramener d'abord au cas où B est entier.)

7. Soient $\alpha \in \mathbf{R}$, $a \in \mathbf{Z}$, $q \in \mathbf{N} - \{0\}$ tels que $\mathrm{pgcd}(a, q) = 1$ et

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}.$$

a. Fixons $x_0 \in \mathbf{Z}$ et soient y et y' deux entiers tels que $1 \leqslant y \leqslant q$, $1 \leqslant y' \leqslant q$, $\|\alpha(x_0 + y)\| < 1/B$ et $\|\alpha(x_0 + y')\| < 1/B$. Montrer que

$$\left\|\frac{a}{q}(y - y')\right\| < \frac{2}{B} + \frac{1}{q}.$$

b. Montrer que le cardinal de l'image dans $\mathbf{Z}/q\mathbf{Z}$ de $\left\{ z \in \mathbf{Z} \,\middle|\, \left\|\frac{a}{q}z\right\| < \frac{2}{B} + \frac{1}{q} \right\}$ est majoré par $2q(\frac{2}{B} + \frac{2}{q})$.

c. En déduire que

$$\sharp\left\{ y \in \{1, \ldots, q\} \,\middle|\, \|\alpha(y + x_0)\| < \frac{1}{B} \right\} \leqslant 4q\left(\frac{1}{B} + \frac{1}{q}\right).$$

d. Montrer que

$$\sharp\left\{ x \in \mathbf{Z} \,\middle|\, 1 \leqslant x \leqslant d!B^{d-1} \text{ et } \|\alpha x\| < \frac{1}{B} \right\} \leqslant 4d!q\left(\frac{1}{B}+\frac{1}{q}\right)\left(\frac{B^{d-1}}{q}+1\right).$$

8. Soit $f : \mathbf{N}-\{0\} \to \mathbf{R}$ une fonction. On dit que f est multiplicative si elle vérifie les deux conditions suivantes :

(*i*) $f(1) = 1$,

(*ii*) $\forall a, b \in \mathbf{N}-\{0\}$, $\text{pgcd}(a,b) = 1 \Rightarrow f(ab) = f(a)f(b)$.

a. Montrer que la fonction $\tau : \mathbf{N}-\{0\} \to \mathbf{R}$ définie par

$$\forall n \in \mathbf{N}-\{0\}, \quad \tau(n) = \sharp\{\, k \in \mathbf{N}-\{0\} \mid \ k \text{ divise } n \,\}$$

est multiplicative.

b. Montrer que pour tout nombre réel $\epsilon > 0$, il existe un nombre réel C tel que

$$\forall n \in \mathbf{N}-\{0\}, \quad \tau(n) \leqslant Cn^{\epsilon}.$$

(On pourra d'abord considérer le cas où n est une puissance d'un nombre premier.)

9. Montrer que pour tout nombre réel $\epsilon > 0$, il existe un nombre réel C tel que pour tout α de $\mathbf{R}$, tout a de $\mathbf{Z}$ et tout q de $\mathbf{N}-\{0\}$ tels que $\text{pgcd}(a,q) = 1$ et $|\alpha - \frac{a}{q}| \leqslant \frac{1}{q^2}$, on ait pour tout B de $[1, +\infty[$,

$$|S_B^1(\alpha)| \leqslant CB^{1+\epsilon}\left(\frac{1}{B}+\frac{1}{q}+\frac{q}{B^d}\right)^{1/2^{d-1}}.$$

10. Soient $\alpha \in \mathbf{R}$ et N un entier.

a. Montrer qu'il existe $i \in \{0, \ldots, N-1\}$ et $j, k \in \{0, \ldots, N\}$ avec $j < k$ tels que

$$\{j\alpha\} \in \left[\frac{i}{N}, \frac{i+1}{N}\right[\quad \text{et} \quad \{k\alpha\} \in \left[\frac{i}{N}, \frac{i+1}{N}\right[.$$

b. En déduire qu'il existe $a \in \mathbf{Z}$ et $q \in \mathbf{N}-\{0\}$ tels que $\text{pgcd}(a,q) = 1$, $q \leqslant N$ et

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{Nq}.$$

Pour tout $\Delta \in]0,1]$, tout $B \in [1,+\infty[$, tout $a \in \mathbf{Z}$ et tout $q \in \mathbf{N}-\{0\}$, on pose

$$\mathfrak{M}_\Delta(B,q,a) = \left\{ \alpha \in [0,1[\,\middle|\, \left\| \alpha - \frac{a}{q} \right\| < q^{-1} B^{\Delta-d} \right\}.$$

On définit alors

$$\mathfrak{M}_\Delta(B) = \bigcup_{\{(a,q)\in\mathbf{N}^2 \mid 1\leqslant a\leqslant q\leqslant B^\Delta \text{ et } \operatorname{pgcd}(a,q)=1\}} \mathfrak{M}_\Delta(B,q,a)$$

et

$$\mathfrak{m}_\Delta(B) = [0,1[- \mathfrak{M}_\Delta(B).$$

11. a. Décrire l'ensemble $\mathfrak{M}_\Delta(B,1,1)$ comme réunion d'intervalles.

b. Montrer que pour tout $\Delta \in]0,1]$ et tout réel $B \geqslant 1$, $\mathfrak{M}_\Delta(B)$ (resp. $\mathfrak{m}_\Delta(B)$) est une réunion finie d'intervalles.

Les intervalles formant $\mathfrak{M}_\Delta(B)$ (resp. $\mathfrak{m}_\Delta(B)$) sont appelés les *arcs majeurs* (resp. les *arcs mineurs*).

12. Soient $\Delta \in]0,1]$, $B \in [1,+\infty[$ et $\alpha \in \mathfrak{m}_\Delta(B)$

a. Si $a \in \mathbf{Z}$ et $q \in \mathbf{N}-\{0\}$ vérifient $\left|\alpha - \frac{a}{q}\right| < \frac{B^{\Delta-d}}{q}$, montrer que $q > B^\Delta$.

b. En déduire que pour tout $\epsilon > 0$, il existe un nombre réel C ne dépendant que de d et ϵ tel que, pour tout B de $[1,+\infty[$, on ait

$$|S_B^1(\alpha)| \leqslant C B^{1-\Delta/2^{d-1}+\epsilon}.$$

13. On définit pour tout α de $\mathbf{R}$,

$$S_B^m(\alpha) = \sum_{(x_1,\ldots,x_m)\in(\mathbf{N}\cap[0,B])^m} \mathbf{e}\left(\alpha \sum_{i=1}^m x_i^d\right).$$

Montrer que, pour tout $\epsilon > 0$, il existe un nombre réel C ne dépendant que de d, m et ϵ tel que, pour tout $\Delta \in]0,1]$, pour tout B de $[1,+\infty[$ et tout α de $\mathfrak{m}_\Delta(B)$, on ait

$$|S_B^m(\alpha)| \leqslant C B^{m-m\Delta/2^{d-1}+\epsilon}.$$

Dans la suite, on notera pour toute fonction f continue sur $[0,1]$ et toute famille finie $(I_i)_{1\leqslant i\leqslant n}$ d'intervalles disjoints contenus dans $[0,1[$,

$$\int_{\cup_{i=1}^n I_i} f(x)\,\mathrm{d}x = \sum_{i=1}^n \int_{I_i} f(x)\,\mathrm{d}x.$$

14. a. Montrer que, pour tout Δ de $]0,1]$ et tout réel $B \geqslant 1$,

$$\int_{\mathfrak{M}_\Delta(B)} 1 \, \mathrm{d}x \leqslant 2B^{2\Delta-d}.$$

b. Montrer que, pour tout nombre réel $\epsilon > 0$, il existe un nombre réel C ne dépendant que de d, m et ϵ tel que, pour tout réel $B \geqslant 1$,

$$\int_{\mathfrak{m}_1(B)} |S_B^m(\alpha)| \, \mathrm{d}\alpha \leqslant CB^{m-m/2^{d-1}+\epsilon}$$

c. Montrer que si Δ_1, Δ_2 appartiennent à $]0,1]$ avec $\Delta_1 < \Delta_2$, alors pour tout nombre réel $\epsilon > 0$ il existe un nombre réel C ne dépendant que de d, m et ϵ tel que, pour tout réel $B \geqslant 1$,

$$\int_{\mathfrak{M}_{\Delta_2}(B)-\mathfrak{M}_{\Delta_1}(B)} |S_B^m(\alpha)| \, \mathrm{d}\alpha \leqslant CB^{m-d-(m/2^{d-1}-2)\Delta_1+2(\Delta_2-\Delta_1)+\epsilon}.$$

15. On suppose que $m > d2^{d-1}$. Montrer que pour tout $\Delta \in]0,1]$, il existe un nombre réel $\delta > 0$ et un nombre réel C tels que pour tout réel $B \geqslant 1$,

$$\int_{\mathfrak{m}_\Delta(B)} |S_B^m(\alpha)| \, \mathrm{d}\alpha \leqslant CB^{m-d-\delta}.$$

(On pourra considérer des nombres réels $\Delta = \Delta_0 < \Delta_1 < \cdots < \Delta_n = 1$.)

16. On suppose que $m > d2^{d-1}$ et qu'il existe un nombre réel $\Delta \in]0,1]$, un entier positif t_0 et un nombre réel strictement positif c tels que, pour tout entier $t \geqslant t_0$,

$$\left| \int_{\mathfrak{M}_\Delta(t^{1/d})} S_{t^{1/d}}^m(\alpha) \mathbf{e}(-\alpha t) \, \mathrm{d}\alpha \right| \geqslant c \, t^{m/d-1}.$$

Que peut-on en déduire sur $G(d)$?