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

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

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

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

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

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

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

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

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

(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

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

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 $G(d)$?

PARTIE I

I.1) a) On note $A_{m,t}$ l'ensemble étudié. Soit $(x_1, \ldots, x_m)$ dans $A_{m,t}$, on a alors, pour $1 \leq i \leq m$, $0 \leq x_i \leq t$ et donc $(x_1, \ldots, x_m) \in [0,t]^m$. En particulier

$$\boxed{\text{l'ensemble } \left\{ (x_1, \ldots, x_m) \in \mathbf{N}^m \mid \sum_{i=1}^{m} x_i = t \right\} \text{ est fini.}}$$

b) Soit p la projection sur la dernière coordonnée. On reprend la notation précédente. On a alors $p(A_{m,t}) \subset [0,t]$ et, pour k dans $[0,t]$, $p^{-1}(t-k)$ est égal à $A_{m-1,k} \times \{t-k\}$ et est donc en bijection avec $A_{m-1,k}$. Il en résulte que $A_{m,t}$ est la réunion disjointe des $A_{m-1,k} \times \{t-k\}$, pour $0 \leq k \leq t$, ce qui se traduit en termes de cardinaux par $\boxed{N_1^m(t) = \sum_{k=0}^{t} N_1^{m-1}(k).}$

c) On pourait procéder par récurrence en utilisant le triangle de Pascal. Voici une autre façon de faire. On reprend les notations précédentes et à tout élément $(x_1, \ldots, x_m)$ dans $A_{m,t}$ on associe une suite strictement croissante d'éléments de $[1, t+m]$ ainsi : pour $1 \leq k \leq m$, on pose $y_k = x_1 + \cdots + x_k + k$ ou, pour $k \geq 2$, $y_k = y_{k-1} + x_k + 1$. Cette dernière formule montre que la suite ainsi construite est strictement croissante et que l'application qui à (x_k) associe (y_k) est injective. La condition d'appartenance à $A_{m,t}$ se traduit par $y_m = t + m$ et il en résulte que $A_{m,t}$ est en bijection avec les suites strictement croissantes d'éléments de $[1, t+m]$ ayant m termes et dont le dernier terme est $t+m$. L'ensemble de telles suites est en bijection avec les parties de $[1, t+m]$ constituées de m éléments et contenant $t+m$, ou encotre avec les parties de $[1, t+m-1]$ constituées de $m-1$ éléments. Il en résulte $\boxed{N_1^m(t) = \binom{t+m-1}{m-1}.}$

d) On écrit $N_1^m(t) = \dfrac{(t+m-1)\cdots(t+1)}{(m-1)!}$ et, alors, à m fixé, chacun des termes du produit dans le numérateur est équivalent à t, d'où $\boxed{N_1^m(t) \underset{t\to+\infty}{\sim} \dfrac{t^{m-1}}{(m-1)!}.}$

I.2) a) La fonction carré étant paire, il suffit de décrire l'image des classes des entiers de 0 à 4 modulo 8, à savoir respectivement 0, 1, 4, 1, 0. Les seuls éléments inversibles sont les classes d'entiers impairs et donc

$$\boxed{\begin{array}{l}\text{l'image de la fonction carré est } \{\overline{0}, \overline{1}, \overline{4}\} \text{ en tant qu'application définie sur } \mathbf{Z}/8\mathbf{Z} \text{ et c'est} \\ \text{la fonction constante égale à } \overline{1} \text{ sur } (\mathbf{Z}/8\mathbf{Z})^\times.\end{array}}$$

b) Soit (X, Y, Z, T) dans $(\mathbf{Z}/8\mathbf{Z})^\times \times (\mathbf{Z}/8\mathbf{Z})^3$ tel que $X^2 + Y^2 + Z^2 + T^2 = 0$. On a donc $X^2 = 1$ et il y a donc un nombre impair de termes inversibles parmi (Y, Z, T). S'il y en a trois, la somme fait $\overline{4}$ et sinon elle est congrue à 2 modulo 4. Par conséquent $\boxed{\text{l'équation } X^2 + Y^2 + Z^2 + T^2 = 0 \text{ n'a pas de solutions dans } (\mathbf{Z}/8\mathbf{Z})^\times \times (\mathbf{Z}/8\mathbf{Z})^3.}$

c) Par l'absurde. Soit x, y, t des rationnels tels que $x^2 + y^2 + z^2 = 8b - 1$. On dispose donc de t dans $\mathbf{N}^*$ tel que xt, yt et zt soient entiers naturels. Soit alors T vérifiant cette propriété et minimal parmi ceux-ci. On note $X = xT$, $Y = yT$ et $Z = zT$. On a alors $X^2 + Y^2 + Z^2 + T^2 = 8bT^2$. D'après la question précédente il en résulte que X, Y, Z et T sont divisibles par 2, mais

alors $T/2$ est entier et tel que $xT/2$, $yT/2$ et $zT/2$ sont entiers. Ceci contredit la minimalité de T et donc $\boxed{\text{l'équation } X^2+Y^2+Z^2=8b-1 \text{ n'admet aucune solution dans } \mathbf{Q}^3.}$

d) Si (X,Y,Z) est solution de cette équation, $(2^{-a}X, 2^{-a}Y, 2^{-a}Z)$ est solution de l'équation précédente : $\boxed{\text{l'équation } X^2+Y^2+Z^2=4^a(8b-1) \text{ n'admet aucune solution dans } \mathbf{N}^3.}$

PARTIE II

II.1) a) Soit x dans $\mathbf{Z}/p\mathbf{Z}$. On a $x^2-1=(x-1)(x+1)$, avec $1\neq -1$ puisque p est impair, et donc, puisque p est premier et donc $\mathbf{Z}/p\mathbf{Z}$ un corps,
$\boxed{\text{le noyau du morphisme carré dans } (\mathbf{Z}/p\mathbf{Z})^\times \text{ est } \{-1,1\}.}$

b) Puisque le noyau du morphisme carré est de cardinal 2, chaque image admet exactement deux antécédents et donc, par cardinalité, $\boxed{\text{l'image est de cardinal } (p-1)/2.}$
Le seul élément non inversible étant 0 et étant le seul de carré 0, il en résulte que
$\boxed{\text{l'ensemble des carrés dans } \mathbf{Z}/p\mathbf{Z} \text{ est de cardinal } (p+1)/2.}$

c) Les deux ensembles considérés sont de cardinal $(p+1)/2$ et donc, d'après la formule du crible, le cardinal de leur intersection est égal à $p+1$ moins le cardinal de leur réunion. Cette dernière étant de cardinal au plus p, $\boxed{\text{l'intersection de ces deux ensembles est non vide.}}$

d) D'après ce qui précède on dispose de X et Y dans $\mathbf{Z}/p\mathbf{Z}$ tels que $X^2=-1-Y^2$, i.e. $1+X^2+Y^2=0$. En prenant des représentants de valeur absolue inférieure à $(p-1)/2$, on dispose de x et y dans $[-(p-1)/2,(p-1)/2]$ tels que p divise $1+x^2+y^2$. Or on a alors $1\leq 1+x^2+y^2\leq 1+(p-1)^2/2<1+p^2/2<p^2$, d'où l'existence de m dans $[\![1,p-1]\!]$ tel que $1+x^2+y^2=mp$. Quitte à changer x ou y en $-x$ ou $-y$ respectivement, on en conclut qu' $\boxed{\text{il existe des entiers naturels } x,\ y \text{ et } m \text{ avec } 0<m<p \text{ tels que } 1+x^2+y^2=mp.}$

II.2) a) Comme K est antidiagonale, $Vect\,(1,I)$ et $Vect\,(J,K)$ sont en somme directe. Comme 1 et I ne sont pas proportionnelles, elles forment une famille libre et par le même argument J et K aussi. Donc $(1,I,J,K)$ est libre et forme donc une base de l'espace qu'elles engendrent :
$\boxed{(1,I,J,K) \text{ est une base de } \mathbf{H}.}$
Comme $\mathbf{H}$ est un espace vectoriel, il est stable par combinaisons linéaires et donc c'est un sous-anneau de $\mathfrak{M}_2(\mathbf{C})$ si et seulement le produit de vecteurs d'une de ses bases est dans $\mathbf{H}$. La multiplication par 1 ne changeant pas les vecteurs, on se restreint aux vecteurs (I,J,K). Par définition on a $IJ=K$. On a également directement $I^2=J^2=-1$, $IK=I^2J=-J$ et $KJ=IJ^2=-I$. On obtient directement, par changement de base, $J^{-1}IJ=-I$ et donc $IJ=-JI$. On a donc $JI=-K$, $KI=IJI=-IK=J$, $JK=JIJ=-KJ=I$ et $K^2=IJIJ=-I(IJ)J=-I^2J^2=-1$. Par conséquent $\boxed{\forall (a,b)\in\mathbf{H}^2,\ ab\in\mathbf{H}.}$

b) Par construction l'application τ est l'application linéaire dont la matrice relativement à la base $(1,I,J,K)$ est diagonale de diagonale $(1,-1,-1,-1)$. $\boxed{\text{Donc } \tau \text{ est linéaire.}}$
La formule $\tau(xy)=\tau(y)\tau(x)$ est vraie si x et y font partie de la base $(1,I,J,K)$ puisque $\tau(1)=1$ et 1 est l'élément neutre pour la multiplication, et dans le cas où x et y sont (I,J,K), xy est dans $(\pm I,\pm J,\pm K)$ et donc $\tau(xy)=-xy$ tandis que $\tau(y)\tau(x)=(-y)(-x)=yx$. Les relations précédemment trouvées montrent qu'on a $xy=-yx$ dans ce cas et l'assertion s'ensuit.

Notons maintenant $(e_i)_{1\leq i\leq 4} = (1, I, J, K)$. Pour des scalaires $(a_i)_{1\leq i\leq 4}$ et $(b_i)_{1\leq i\leq 4}$, on pose $x = \sum_{i=1}^{4} a_i e_i$ et $y = \sum_{i=1}^{4} b_i e_i$. Il vient par linéarité et d'après ce qui précède

$$\tau(xy) = \sum_{1\leq i,j\leq 4} a_i b_j \tau(e_i e_j) = \sum_{1\leq i,j\leq 4} a_i b_j \tau(e_j)\tau(e_i) = \tau(y)\tau(x) \ .$$

Et donc $\boxed{\forall (x,y) \in \mathbf{H}^2,\ \tau(xy) = \tau(y)\tau(x).}$

c) On reprend les notations précédentes. On a alors $x\tau(x) = \sum_{1\leq i,j\leq 4} a_i a_j e_i \tau(e_j)$. Or, pour $i \neq j$, $e_i\tau(e_j) + e_j\tau(e_i) = 0$ par anticommutation de e_i et e_j si $i, j > 1$ et par définition de τ si $i = 1$ ou $j = 1$. Il en résulte

$$x\tau(x) = \sum_{i=1}^{4} a_i^2 e_i \tau(e_i) = \left(\sum_{i=1}^{4} a_i^2\right) 1 \ .$$

L'échange de x avec $\tau(x)$ dans le calcul précédent revient à échanger les i et les j et on trouve donc le même résultat, i.e.

$\boxed{\text{il existe une application } N \text{ de } \mathbf{H} \text{ dans } \mathbf{R} \text{ telle que, pour } z \text{ dans } \mathbf{H}, \text{ on ait } N(z) = z\tau(z) = \tau(z)z. \text{ De plus elle correspond au carré de la norme euclidienne canonique via l'isomorphisme } \mathbf{H} \simeq \mathbf{R}^4 \text{ obtenu par le choix de base } (1, I, J, K). \text{ Autrement dit, si } z = a1 + bI + cJ + dK, \text{ avec } (a, b, c, d) \in \mathbf{R}^4, \text{ on a } N(z) = a^2 + b^2 + c^2 + d^2.}$

d) Soit z_1 et z_2 dans $\mathbf{H}$. On a $N(z_1z_2) = z_1z_2\tau(z_1z_2) = z_1N(z_2)\tau(z_1)$, d'après 2(b). Mais $N(z_2)$ est scalaire et donc commute à tout élément de $\mathbf{H}$. Il vient donc $z_1N(z_2)\tau(z_1) = z_1\tau(z_1)N(z_2) = N(z_1)N(z_2)$, i.e. $\boxed{\forall (z_1, z_2) \in \mathbf{H}^2,\ N(z_1z_2) = N(z_1)N(z_2).}$

II.3) Par définition de $\mathcal{N}_2^4$, c'est l'image par N de $\mathbf{N}1+\mathbf{N}I+\mathbf{N}J+\mathbf{N}K$ et donc aussi de $\mathbf{Z}1+\mathbf{Z}I+\mathbf{Z}J+\mathbf{Z}K$, par parité de la fonction carré. On note A l'ensemble $\mathbf{Z}1+\mathbf{Z}I+\mathbf{Z}J+\mathbf{Z}K$, i.e. le sous-groupe de $(\mathbf{H}, +)$ engendré par la base $(1, I, J, K)$. D'après les formules de multiplication des éléments de la base, A est en fait un sous-anneau de $\mathbf{H}$, donc stable par produit. Comme l'application N est multiplicative, $N(A)$ est aussi stable par produit. Autrement dit $\boxed{\forall (a, b) \in \mathcal{N}_2^4,\ ab \in \mathcal{N}_2^4.}$

II.4) a) On dispose, d'après la question II.1(d), d'entiers naturels x et y et de m dans $[\![1, p-1]\!]$ tels que $1 + x^2 + y^2 = mp$ et donc $mp = 0^2 + 1^2 + x^2 + y^2$ montre que

$\boxed{\text{il existe } m \text{ dans } [\![1, p-1]\!] \text{ tel que } mp \text{ appartient à } \mathcal{N}_2^4.}$

b) i. Puisque mp est pair, il y a un nombre pair de nombres impairs parmi $(x_i)_{1\leq i\leq 4}$. S'il n'y en a pas ou s'ils le sont tous, alors σ telle que $i \mapsto x_{\sigma(i)}$ soit décroissante d'une part existe et d'autre part convient. Sinon on note $\sigma(1)$ et $\sigma(2)$ les deux termes pairs ordonnés de façon décroissante et $\sigma(3)$ et $\sigma(4)$ les deux termes impairs également ordonnés de façon décroissante. Alors on a bien

$\boxed{x_{\sigma(1)} + x_{\sigma(2)},\ x_{\sigma(1)} - x_{\sigma(2)},\ x_{\sigma(3)} + x_{\sigma(4)} \text{ et } x_{\sigma(3)} - x_{\sigma(4)} \text{ positifs et pairs.}}$

ii. L'identité de la médiane $(x+y)^2+(x-y)^2 = 2(x^2+y^2)$ appliquée aux termes $x_{\sigma(1)}^2+x_{\sigma(2)}^2$ et $x_{\sigma(3)}^2+x_{\sigma(4)}^2$, entraîne que $2mp$ est la somme de quatre carrés d'entiers naturels pairs et donc, en divisant par 4, que $mp/2$ est somme de quatre carrés d'entiers naturels, i.e. $\boxed{\frac{mp}{2} \in \mathcal{N}_2^4.}$

c) D'après ce qui précède, si m_0 était pair, $m_0/2$ vérifierait la propriété du II.4(a) et ceci contredirait la minimalité de m_0. Donc $\boxed{m_0 \text{ est impair.}}$

d) i. Soit $(y_i)_{1\leq i\leq 4}$ les représentants respectifs de $(x_i)_{1\leq i\leq 4}$ modulo m_0 dont la valeur absolue est inférieure à $(m_0-1)/2$ (ce qui est licite puisque m_0 est impair). On a alors

$$\sum_{i=1}^{4} y_i^4 \equiv \sum_{i=1}^{4} x_i^4 \equiv 0 \pmod{m_0}$$

et

$$\sum_{i=1}^{4} y_i^4 \leq 4\frac{(m_0-1)^2}{4} < m_0^2 \, .$$

Si cette dernière somme était nulle, alors tous les y_i le seraient et donc tous les x_i seraient multiples de m_0 et la somme de leur carrés serait multiple de m_0^2, i.e. $m_0^2 | pm_0$ ou encore $m_0|p$.

Comme p est premier et $0 < m_0 < p$, on en déduirait $m_0 = 1$, ce qui est exclu par hypothèse, $\boxed{\text{d'où l'assertion demandée.}}$

ii. Puisque $\mathbf{H}$ est stable par multiplication, on peut considérer $(z_i)_{1\leq i\leq 4}$ dans $\mathbf{R}^4$ tel que $x\tau(y) = z$, en notant $x = \sum_{i=1}^{4} x_i e_i$, $y = \sum_{i=1}^{4} y_i e_i$ et $z = \sum_{i=1}^{4} z_i e_i$ et $(e_i)_{1\leq i\leq 4} = (1, I, J, K)$.
Puisque les x_i et les y_i sont entiers, il en va de même pour les z_i et on a $N(z) = N(x)N(\tau(y)) = N(x)N(y) = m_0 p m_0 m_1$, i.e. $\sum_{i=1}^{4} z_i^2 = m_0^2 m_1 p$. Enfin on a

$$z = \sum_{1\leq i,j\leq 4} x_i y_j e_i \tau(e_j) \, .$$

On va calculer les coordonnées de z modulo m_0. Comme $x_i \equiv y_i \pmod{m_0}$ et comme $\mathbf{Z}/m_0\mathbf{Z}$ est un anneau, ces coordonnées modulo m_0 sont les mêmes que celles de $x\tau(x)$ modulo m_0, i.e. celle de $N(x)$. Comme $N(x) = m_0 p 1 + 0I + 0J + 0K$, ces coordonnées modulo m_0 sont toutes nulles et donc $z_i \equiv 0 \pmod{m_0}$ pour $1 \leq i \leq 4$. Enfin, quitte à changer z_i en $-z_i$, on a bien obtenu

$$\boxed{(z_i)_{1\leq i\leq 4} \text{ dans } \mathbf{N}^4 \text{ tel que } \sum_{i=1}^{4} z_i^2 = m_0^2 m_1 p \text{ et } z_i \equiv 0 \pmod{m_0} \text{ pour } 1 \leq i \leq 4.}$$

e) En divisant les z_i obtenus précédemment par m_0, on obtient $m_1 p \in \mathcal{N}_2^4$. Comme $\sum_{i=1}^{4} y_i^2 < m_0^2$, on a $m_1 < m_0$ et ceci contredit la minimalité de m_0. Cette contradiction finale assure $\boxed{m_0 = 1.}$

II.5) Remarquons que 0, 1 et 2 appartiennent à N_2^4 puisque $0 = 0^2+0^2+0^2+0^2$, $1 = 1^2+0^2+0^2+0^2$ et $2 = 1^2+1^2+0^2+0^2$.
D'après ce qui précède, si p est premier impair alors $p \in \mathcal{N}_2^4$. Comme $\mathcal{N}_2^4$ est stable par produit, le théorème fondamental de l'arithmétique permet de conclure $\boxed{\mathcal{N}_2^4 = \mathbf{N}.}$