DEVOIR MAISON 12

Vous traiterez au choix : soit les deux exercices, soit le problème (plus difficile).

► Exercice 1 : triplets pythagoriciens

Nous avons déjà mentionné en cours le grand théorème de Fermat, prouvé par Andrew WILES en 1995 et qui stipule que si $n \geq 3$, alors il n'existe pas de triplet $(x, y, z) \in (\mathbf{N}^*)^3$ tel que $x^n + y^n = z^n$.

En revanche si $n = 2$, il existe de tels triplets, le plus célèbre d'entre eux étant probablement $3^2 + 4^2 = 5^2$.

Le but de cet exercice est de déterminer tous les triplets $(x, y, z) \in (\mathbf{N}^*)^3$ tels que $x^2 + y^2 = z^2$.

Un tel triplet est appelé **triplet pythagoricien**. On parlera de **triplet pythagoricien primitif** si de plus $x \wedge y \wedge z = 1$.

1. **Un lemme utile** : soient a et b deux entiers non nuls. Montrer que si a^2 divise b^2 , alors a divise b . On pourra par exemple montrer que $a \wedge b = a$.
2. Soit (x, y, z) un triplet pythagoricien, et soit $d = x \wedge y \wedge z$. On pose alors $x' = \frac{x}{d}$, $y' = \frac{y}{d}$ et $z' = \frac{z}{d}$. Justifier que (x', y', z') est un triplet pythagoricien primitif, et que x', y', z' sont deux à deux premiers entre eux.
3. Soit (x, y, z) un triplet pythagoricien primitif.
 - a. Prouver que x et y ne sont pas tous deux pairs.
À l'aide de congruences modulo 4, justifier que x et y ne sont pas tous deux impairs.

Dans la suite, quitte à échanger x et y , on suppose que x est pair et y est impair.

- b. Justifier qu'il existe $(u, v, w) \in (\mathbf{N}^*)^3$ tels que $x = 2u$, $z + y = 2v$ et $z - y = 2w$.
 - c. Montrer que $v \wedge w = 1$.
 - d. Prouver que vw est un carré, en déduire que v et w sont des carrés.
On pose alors $v = n^2$ et $w = m^2$, avec $(m, n) \in (\mathbf{N}^*)^2$.
 - e. Montrer que $n > m$ et que n et m sont premiers entre eux.
4. Montrer que (x, y, z) est un triplet pythagoricien primitif si et seulement si il existe deux entiers n et m premiers entre eux, de parités distinctes, avec $n > m > 0$ tels que

$$\begin{cases} x = 2nm \\ y = n^2 - m^2 \\ z = n^2 + m^2 \end{cases} \quad \text{ou} \quad \begin{cases} x = n^2 - m^2 \\ y = 2nm \\ z = n^2 + m^2 \end{cases}$$

En déduire tous les triplets pythagoriciens.

► Exercice 2 : caractérisation du PGCD et du PPCM en termes de sous-groupes.

Pour $n \in \mathbf{Z}$, on note $n\mathbf{Z} = \{nk, k \in \mathbf{Z}\}$. Pour $(a, b) \in \mathbf{Z}^2$, on note $a\mathbf{Z} + b\mathbf{Z} = \{au + bv, (u, v) \in \mathbf{Z}^2\}$.

1. Montrer que pour tout $n \in \mathbf{Z}$, $n\mathbf{Z}$ est un sous-groupe de $(\mathbf{Z}, +)$, et que $n\mathbf{Z} = p\mathbf{Z} \Leftrightarrow n = \pm p$.
2. Dans cette question, on considère G un sous-groupe de $(\mathbf{Z}, +)$, différent de $\{0\}$.
 - a. Justifier que $G \cap \mathbf{N}^*$ possède un plus petit élément, qu'on notera n dans la suite.
 - b. Soit $m \in G$. Prouver que n divise m .
 - c. Montrer alors que $G = n\mathbf{Z}$.
3. Soient $(a, b) \in \mathbf{Z}^2$.

- a. Montrer qu'il existe deux entiers naturels m et d tels que $a\mathbf{Z} \cap b\mathbf{Z} = m\mathbf{Z}$ et $a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$.
- b. Prouver alors que $m = a \vee b$ et $d = a \wedge b$.

► **Problème : théorème des 4 carrés de Lagrange (d'après un sujet ENS)**

Le but de ce problème est de prouver que tout entier naturel s'écrit comme la somme de quatre carrés d'entiers. Par exemple $63 = 1^2 + 1^2 + 5^2 + 6^2$ et $135 = 9^2 + 7^2 + 2^2 + 1^2$.

On note $\mathcal{N} = \{n \in \mathbf{N} \mid \exists(x, y, z, t) \in \mathbf{N}^4, n = x^2 + y^2 + z^2 + t^2\}$ l'ensemble des entiers naturels qui s'écrivent comme somme de quatre carrés. On souhaite donc prouver que $\mathcal{N} = \mathbf{N}$.

Partie I. Quaternions

On définit quatre matrices de $\mathcal{M}_2(\mathbf{C})$ de la manière suivante :

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

Soit A un sous-anneau de $\mathbf{R}$. On note alors $\mathbf{H}_A = \{a1 + b\mathbf{I} + c\mathbf{J} + d\mathbf{K}, (a, b, c, d) \in A^4\}$.

1. Avec le moins de calculs possibles, déterminer $\mathbf{I}^2, \mathbf{J}^2, \mathbf{K}^2$ ainsi que $\mathbf{JI}, \mathbf{IK}, \mathbf{KI}, \mathbf{JK}$ et $\mathbf{KJ}$.
2. Justifier que pour tout $h \in \mathbf{H}_A$, il existe un unique $(a, b, c, d) \in A^4$ tel que $h = a1 + b\mathbf{I} + c\mathbf{J} + d\mathbf{K}$.
3. Montrer que $\mathbf{H}_A$ est un sous-anneau de $\mathcal{M}_2(\mathbf{C})$.
4. Montrer que l'application $\tau : \begin{matrix} \mathbf{H}_A & \longrightarrow & \mathbf{H}_A \\ a1 + b\mathbf{I} + c\mathbf{J} + d\mathbf{K} & \longmapsto & a1 - b\mathbf{I} - c\mathbf{J} - d\mathbf{K} \end{matrix}$ est un morphisme de groupes, vérifiant $\forall x, y \in \mathbf{H}_A, \tau(xy) = \tau(y)\tau(x)$, et que de plus pour tout $x \in \mathbf{H}_A$ et pour tout $\lambda \in A, \tau(\lambda x) = \lambda\tau(x)$.
5. Montrer que pour tout $z \in \mathbf{H}_A, \tau(z)z = z\tau(z)$, et qu'il s'agit là d'un élément de $\{\lambda 1, \lambda \in A\}$, qu'on notera dans la suite $N(z)$.
6. Pour $x = a1 + b\mathbf{I} + c\mathbf{J} + d\mathbf{K}$, exprimer $N(x)$ en fonction de a, b, c, d .
7. Prouver que pour tout $z, z' \in \mathbf{H}_A, N(zz') = N(z)N(z')$.
8. Dans cette question, on suppose que $A = \mathbf{R}$. Montrer que $\mathbf{H}_{\mathbf{R}}^{\times} = \mathbf{H}_{\mathbf{R}} \setminus \{0_2\}$. Est-ce que $\mathbf{H}_{\mathbf{R}}$ est un corps ?

Partie II. Preuve du théorème des quatre carrés

9. Soit p un nombre premier impair.

- a. Montrer que $\varphi : \begin{matrix} (\mathbf{Z}/p\mathbf{Z})^{\times} & \longrightarrow & (\mathbf{Z}/p\mathbf{Z})^{\times} \\ x & \longmapsto & x^2 \end{matrix}$ est un morphisme de groupes, et déterminer son noyau.
- b. Soient G et H deux groupes, avec G fini, et soit $f : G \rightarrow H$ un morphisme de groupes. Prouver que $\text{Card}(G) = \text{Card}(\text{Im } f) \times \text{Card}(\text{Ker } f)$.
- c. En déduire le cardinal de $\{x^2, x \in \mathbf{Z}/p\mathbf{Z}\}$.
- d. Montrer que $\{x^2, x \in \mathbf{Z}/p\mathbf{Z}\}$ et $\{-1 - y^2, y \in \mathbf{Z}/p\mathbf{Z}\}$ ne sont pas disjoints.
- e. En déduire qu'il existe des entiers naturels x, y et m , avec $0 < m < p$ tels que $1 + x^2 + y^2 = mp$.

10. À l'aide de la première partie, montrer que $\forall(a, b) \in \mathcal{N}^2, ab \in \mathcal{N}$.

11. Soit p un entier premier impair.

- a. Montrer qu'il existe $m \in \llbracket 1, p-1 \rrbracket$ tel que $mp \in \mathcal{N}$.
Dans la suite de cette question, on note m_0 le plus petit entier strictement positif tel que $m_0 p \in \mathcal{N}$.
- b. Soit m un entier pair tel qu'il existe $(x_1, x_2, x_3, x_4) \in \mathbf{N}^4$ tels que $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$.
 - i. Montrer qu'il existe une permutation $\sigma \in \mathfrak{S}_4$ telle que les entiers

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

soient tous les quatre pairs et positifs.

- ii. En déduire que $\frac{m_0 p}{2} \in \mathcal{N}$.
- c. Prouver alors que m_0 est impair.
- d. On suppose dans cette question 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, b_4 tels que les entiers $y_i, 1 \leq i \leq 4$ définis par $y_i = x_i - b_i m_0$ satisfassent les trois conditions suivantes :

$$\begin{cases} \forall i \in \{1, 2, 3, 4\}, |y_i| < \frac{m_0}{2} \\ 0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < m_0^2 \\ y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \quad [m_0] \end{cases}$$

On note alors $m_1 = \frac{y_1^2 + y_2^2 + y_3^2 + y_4^2}{m_0}$.

- 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 pour tout $i \in \llbracket 1, 4 \rrbracket, z_i \equiv 0 \quad [m_0]$.
On pourra considérer le produit $(x_1 \mathbf{1} + x_2 \mathbf{I} + x_3 \mathbf{J} + x_4 \mathbf{K})(y_1 \mathbf{1} - y_2 \mathbf{I} - y_3 \mathbf{J} - y_4 \mathbf{K})$.

- e. Montrer que $m_0 = 1$.

12. Prouver que $\mathcal{N} = \mathbf{N}$, c'est-à-dire que tout entier naturel est somme de quatre carrés.

CORRECTION DU DEVOIR MAISON 12

► Exercice 1 : triplets pythagoriciens

1. Soient donc a et b tels que $a^2 \mid b^2$. Notons alors $d = a \wedge b$, et soient a', b' deux entiers premiers entre eux tels que $a = da'$ et $b = db'$.
Alors $b^2 = d^2 b'^2$ est divisible par $a^2 = d^2 a'^2$, si bien que $a'^2 \mid b'^2$.
Or a' et b' étant premiers entre eux, il en est de même de a'^2 et b'^2 .
Et donc a'^2 est un diviseur commun de a'^2 et de b'^2 , et donc divise leur pgcd qui vaut 1. Ainsi, $a'^2 = 1$, si bien que $a' = 1$, et donc $d = a$, ce qui prouve que $a \mid b$.

Rappel

Un entier est premier avec un produit si et seulement si il est premier avec chacun de ses facteurs.

Alternative : on peut également utiliser des valuations p -adiques pour prouver ce résultat : pour tout premier p , on sait que $v_p(a^2) \leq v_p(b^2)$, soit encore $2v_p(a) \leq 2v_p(b)$, et donc $v_p(a) \leq v_p(b)$.
Et ceci étant vrai pour tout nombre premier, $a \mid b$.

2. Il est évident que x', y' et z' sont premiers entre eux dans leur ensemble.
On a alors $x'^2 + y'^2 = \frac{1}{d^2}(x^2 + y^2) = \frac{z^2}{d^2} = z'^2$.

Donc (x', y', z') est un triplet pythagoricien primitif.

Attention

On n'a à ce stade pas complètement répondu à la question, puisque x', y' et z' pourraient encore ne pas être deux à deux premiers.

Soit k un diviseur commun à x' et y' . Alors k^2 divise $x'^2 + y'^2 = z'^2$. Par la question 1, on a donc $k \mid z'$, et donc k est un diviseur commun de x', y' et z' . Puisque ces entiers sont premiers entre eux dans leur ensemble, k divise 1, et donc $k = 1$. En particulier, $x' \wedge y' = 1$.

Sur le même principe, un diviseur commun de x' et de z' est un diviseur de y' à l'aide de la relation $y'^2 = z'^2 - x'^2$, et donc x' et z' sont premiers entre eux.
Donc x', y', z' sont deux à deux premiers entre eux.

- 3.a. Nous venons de prouver que si (x, y, z) est un triplet pythagoricien primitif, alors x et y sont premiers entre eux, et donc ne peuvent être tous deux multiples de 2.
Si k est un entier impair, alors $k \equiv 1 \pmod{4}$ ou $k \equiv 3 \pmod{4}$, et dans les deux cas, $k^2 \equiv 1 \pmod{4}$.
Supposons par l'absurde que x et y sont impairs tous les deux. Alors $x^2 + y^2 \equiv 2 \pmod{4}$.
Or, $x^2 + y^2 = z^2$, et modulo 4 un carré vaut 0 ou 1, d'où une contradiction.
Ainsi, x et y sont de parités opposées.

- 3.b. Puisque x est pair, il existe $u \in \mathbf{N}^*$ tel que $x = 2u$.
Donc z^2 est de même parité que y^2 , donc¹ z et y sont de même parité, et donc $z + y$ et $z - y$ sont pairs.
Il existe donc $v \in \mathbf{N}^*$ tel que $z + y = 2v$.
Enfin, $z^2 = y^2 + x^2 > y^2$, donc $z > y$, de sorte que $z - y > 0$.
Et donc il existe $w \in \mathbf{N}^*$ tel que $z - y = 2w$.

¹ Un entier et son carré sont toujours de même parité.

- 3.c. Soit d un diviseur commun à v et w .
Alors $d \mid z + y$ et $d \mid z - y$, donc $d^2 \mid (z + y)(z - y) = z^2 - y^2 = x^2$. Par conséquent², $d \mid x$.
Ainsi, d divise $x \wedge y \wedge z = 1$, et donc $d = 1$. On a donc prouvé que $v \wedge w = 1$.

² C'est encore la question 1.

- 3.d. On a $4vw = y^2 - z^2 = x^2 = 4u^2$ et donc $vw = u^2$ est un carré.
Alors pour tout premier p , $v_p(vw) = v_p(u^2) = 2v_p(u)$.
Mais v et w étant premiers entre eux, $v_p(v) = 0$ ou $v_p(w) = 0$.
Et donc soit $v_p(v) = 0$, et alors $v_p(w)$ est pair, soit $v_p(w) = 0$ et alors $v_p(v)$ est pair.
Ainsi, pour tout premier p , $v_p(v)$ et $v_p(w)$ sont pairs, et donc il existe a_p, b_p entiers tels que $v_p(v) = 2a_p$ et $v_p(w) = 2b_p$.
Et alors

$$v = \left(\prod_{p \in \mathcal{P}} p^{a_p} \right)^2 \quad \text{et} \quad w = \left(\prod_{p \in \mathcal{P}} p^{b_p} \right)^2$$

sont des carrés.

- 3.e. Puisque $y \neq 0$, $z + y > z - y$, et donc $2n^2 > 2m^2$, donc $n > m$.
Par ailleurs, tout diviseur commun à m et n est un diviseur commun à $v = n^2$ et $w = m^2$, et

donc est un diviseur de $v \wedge w = 1$.

Donc $m \wedge n = 1$.

4. Nous venons de prouver que si (x, y, z) est primitif, alors il est bien de l'une des deux³ formes annoncées.

En effet, dans le cas où, comme dans les questions précédentes, x est pair, alors

$$x^2 = z^2 - y^2 = (n^2 + m^2)^2 - (n^2 - m^2)^2 = 4n^2m^2 \text{ et donc } x = 2mn.$$

Un seul point n'a alors pas été prouvé : c'est que m et n sont de parités distinctes. Mais si m et n étaient de même parité, alors m^2 et n^2 aussi, et donc y et z seraient tous deux pairs, contredisant le fait que $y \wedge z = 1$.

Inversement, reste à vérifier que pour $n > m$ premiers entre eux et de parités distinctes, $(x, y, z) = (2nm, n^2 - m^2, n^2 + m^2)$ est bien un triplet pythagoricien primitif. Mais

$$(2nm)^2 + (n^2 - m^2)^2 = 4^2n^2m^2 + n^4 - 2n^2m^2 + m^4 = n^4 + 2n^2m^2 + m^4 = (n^2 + m^2)^2.$$

Donc on est bien en présence d'un triplet pythagoricien. Il est primitif puisque si $d = x \wedge y \wedge z$, alors d est un diviseur commun à y et z , et donc aussi un diviseur de $2n^2 = z - y$ et $2m^2 = z + y$. Mais puisque $n \wedge m = 1$, $n^2 \wedge m^2 = 1$, et donc $2n^2 \wedge 2m^2 = 2$.

Donc $d = 1$ ou $d = 2$. Or on ne peut pas avoir $d = 2$, car m et n étant de parités distinctes, il en est de même de m^2 et n^2 , et donc de y et z .

Ainsi, $x \wedge y \wedge z = 1$, et donc (x, y, z) est un triplet pythagorien primitif.

Par la question 1, si (x, y, z) est un triplet pythagoricien, et si $d = x \wedge y \wedge z$, alors $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$ est un triplet pythagoricien primitif.

Donc il existe n, m premiers entre eux, de parités distinctes, avec $n > m$ tels que

$$\begin{cases} \frac{x}{d} = 2mn \\ \frac{y}{d} = n^2 - m^2 \\ \frac{z}{d} = n^2 + m^2 \end{cases} \Leftrightarrow \begin{cases} x = 2mnd \\ y = d(n^2 - m^2) \\ z = d(m^2 + n^2) \end{cases} \text{ ou } \begin{cases} \frac{y}{d} = 2mn \\ \frac{x}{d} = n^2 - m^2 \\ \frac{z}{d} = n^2 + m^2 \end{cases} \Leftrightarrow \begin{cases} y = 2mnd \\ x = d(n^2 - m^2) \\ z = d(m^2 + n^2) \end{cases}$$

Et inversement, si $n > m$ sont premiers entre eux, de parités distinctes, et $d \in \mathbf{N}^*$ alors

$$(2mnd)^2 + (d(n^2 - m^2))^2 = d^2(n^4 + 4m^2n^2 + m^4) = d^2(m^2 + n^2)^2 = (d(n^2 + m^2))^2$$

de sorte que $(2mnd, d(n^2 - m^2), d(n^2 + m^2))$ et $(d(n^2 - m^2), 2mnd, d(n^2 + m^2))$ sont des triplets pythagoriciens.

Et donc les triplets pythagoriciens sont exactement les triplets de la forme

$$(2mnd, d(n^2 - m^2), d(n^2 + m^2)) \text{ ou } (d(n^2 - m^2), 2mnd, d(n^2 + m^2))$$

avec $d \in \mathbf{N}^*$, $n > m$ premiers entre eux de parités distinctes.

► Exercice 2 : caractérisation du PGCD et du PPCM en termes de sous-groupes.

1. Soit $n \in \mathbf{Z}$. Il est clair que $n\mathbf{Z} \subset \mathbf{Z}$, et que $0 \in n\mathbf{Z}$.
Pour $x, y \in n\mathbf{Z}$, il existe deux entiers $k_1, k_2 \in \mathbf{Z}$ tels que $x = nk_1$ et $y = nk_2$.
Et alors $x - y = n(k_1 - k_2) \in n\mathbf{Z}$.
Donc $n\mathbf{Z}$ est bien un sous-groupe de $\mathbf{Z}$.

De plus, si $n\mathbf{Z} = p\mathbf{Z}$, alors p , qui est évidemment dans $p\mathbf{Z}$, est dans $n\mathbf{Z}$ et donc n divise p .
Et inversement p divise n . Nous savons que ceci n'est possible que pour $n = \pm p$.

L'implication réciproque est encore plus simple : si $n = p$, alors $n\mathbf{Z} = p\mathbf{Z}$.

Et si $n = -p$, alors les éléments de $n\mathbf{Z}$ sont les $-pk$, $k \in \mathbf{Z}$, c'est-à-dire les $p\ell$, $\ell \in \mathbf{Z}$, et donc $n\mathbf{Z} = p\mathbf{Z}$.

- 2.a. Puisque G est différent de $\{0\}$, il contient au moins un entier $k \in \mathbf{Z} \setminus \{0\}$.
Si $k < 0$, alors, par stabilité de G par passage à l'inverse, $-k \in \mathbf{N}^*$ est un élément de G .
Dans tous les cas, $G \cap \mathbf{N}^*$ est une partie non vide de $\mathbf{N}$, donc possède un plus petit élément.

³ La première si x est pair, la seconde sinon.

Détails

Rappelons qu'un entier est premier avec un produit si et seulement si il est premier avec chacun des facteurs.
Donc $m \wedge n = 1 \Rightarrow m \wedge n^2 = 1$ puis $m^2 \wedge n^2 = 1$.

Remarque

Les éléments de $n\mathbf{Z}$ sont les multiples de n .

2.b. Notons $m = nq + r$, avec $0 \leq r < n$ la division euclidienne de m par n .

Alors $nq = \underbrace{n + n + \dots + n}_{q \text{ fois}} \in G$ et donc $m - nq \in G$.

Ainsi, on a $r \in G$, et $r \geq 0$, donc $r \in G \cap \mathbf{N}$.

On ne peut avoir $r \neq 0$, car alors ceci contredirait la minimalité de n dans $G \cap \mathbf{N}^*$. Donc $r = 0$, de sorte que $m = nq$ est divisible par n .

2.c. Nous avons prouvé à la question précédente que tout élément de G est dans $n\mathbf{Z}$.

Inversement, puisque G contient n , il contient $2n = n + n$, puis $3n = 2n + n$ etc, et contient donc tous les nk , $k \in \mathbf{N}$.

Pas stabilité par passage à l'inverse, il contient également les nk , $k \in \mathbf{Z} \setminus \mathbf{N}$. Et donc $n\mathbf{Z} \subset G$.

Et donc par double inclusion, $n\mathbf{Z} = G$.

3.a. Puisque $a\mathbf{Z}$ et $b\mathbf{Z}$ sont deux sous-groupes de $\mathbf{Z}$, leur intersection l'est encore. Et donc soit $a\mathbf{Z} \cap b\mathbf{Z} = \{0\}$, auquel cas $m = 0$ convient.

Soit $a\mathbf{Z} \cap b\mathbf{Z} \neq \{0\}$, et alors par la question 2, il existe $m \in \mathbf{N}^*$ tel que $a\mathbf{Z} \cap b\mathbf{Z} = m\mathbf{Z}$.

De même, il suffit de prouver que $G = a\mathbf{Z} + b\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$ pour conclure. Soient donc $x, y \in G$. Alors il existe des entiers u_1, v_1, u_2, v_2 tels que $x = au_1 + bv_1$ et $y = au_2 + bv_2$.

Et donc $x - y = a(u_1 - u_2) + b(v_1 - v_2) \in G$.

Donc $a\mathbf{Z} + b\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$ et on conclut comme ci-dessus.

3.b. Commençons par noter que $a\mathbf{Z} \cap b\mathbf{Z}$ est l'ensemble des multiples communs de a et b .

Et donc $a\mathbf{Z} \cap b\mathbf{Z}$ est l'ensemble des multiples communs de a et b : c'est l'ensemble des multiples de $a \vee b$, et donc $a\mathbf{Z} \cap b\mathbf{Z} = (a \vee b)\mathbf{Z}$.

Puisque m et $a \vee b$ sont positifs, par la question 1, $m = a \vee b$.

Puisque $a = a \times 1 + b \times 0 \in a\mathbf{Z} + b\mathbf{Z}$, donc $a \in d\mathbf{Z}$. Donc $d \mid a$. Et de même, $d \mid b$.

On en déduit que d est un diviseur commun à a et à b , et donc un diviseur de $a \wedge b$.

D'autre part, $d \in a\mathbf{Z} + b\mathbf{Z}$, donc il existe $(u, v) \in \mathbf{Z}^2$ tels que $d = au + bv$.

Et alors $a \wedge b$ divise a et b , donc divise $au + bv = d$.

On en déduit alors que⁴ que $a \wedge b = d$.

⁴ Toujours par positivité de $a \wedge b$ et de d .

► Problème : théorème des 4 carrés de Lagrange (d'après ENS MP 2007)

Partie I. Quaternions

1. On a $\mathbf{I}^2 = \mathbf{J}^2 = \mathbf{K}^2 = -1$.

On a de plus $\mathbf{K} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$.

De plus, un calcul nous donne $\mathbf{JI} = \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix} = -\mathbf{K}$, puis

$$\mathbf{IK} = \mathbf{I}^2\mathbf{J} = -\mathbf{J}, \mathbf{KI} = \mathbf{IJI} = -\mathbf{IK} = -\mathbf{J}, \mathbf{KJ} = \mathbf{IJ}^2 = -\mathbf{I}, \mathbf{JK} = \mathbf{JIJ} = -\mathbf{KJ} = -\mathbf{I}.$$

2. L'existence découle de la définition de $\mathbf{H}_A$. Pour l'unicité, notons que pour $a, b, c, d, a', b', c', d' \in A$, on a

$$a\mathbf{1} + b\mathbf{I} + c\mathbf{J} + d\mathbf{K} = a'\mathbf{1} + b'\mathbf{I} + c'\mathbf{J} + d'\mathbf{K} \Leftrightarrow \begin{pmatrix} a + ib & -c - id \\ c - id & a - ib \end{pmatrix} = \begin{pmatrix} a' + ib' & -c' - id' \\ c' - id' & a' - ib' \end{pmatrix}.$$

Mais par unicité des coefficients, si cette égalité est vraie, $\begin{pmatrix} a + ib = a' + ib' \\ -c - id = -c' - id' \end{pmatrix}$.

Et puisque $a, b, c, d, a', b', c', d'$ sont réels, par égalité des parties réelles et imaginaires, $a = a', b = b', c = c'$ et $d = d'$.

Donc tout élément h de $\mathbf{H}_A$ s'écrit bien de manière unique sous la forme $h = a\mathbf{1} + b\mathbf{I} + c\mathbf{J} + d\mathbf{K}$.

3. Il est clair que $\mathbf{I}_2 = \mathbf{1} \in \mathbf{H}_A$, et que si $h \in \mathbf{H}_A$ et $a \in A$, alors $ah \in \mathbf{H}_A$.

Pour alléger les notations, notons $M_1 = \mathbf{1}$, $M_2 = \mathbf{I}$, $M_3 = \mathbf{J}$ et $M_4 = \mathbf{K}$.

Soient donc $h_1 = a_1\mathbf{1} + a_2\mathbf{I} + a_3\mathbf{J} + a_4\mathbf{K} = \sum_{i=1}^4 a_i M_i$ et $h_2 = \sum_{i=1}^4 b_i M_i$ deux éléments de $\mathbf{H}_A$,

donc avec les a_i et les b_j dans A .

Alors $h_1 - h_2 = \sum_{i=1}^4 \underbrace{a_i - b_i}_{\in A} M_i \in \mathbf{H}_A$. Donc $\mathbf{H}_A$ est stable par somme.

Enfin $h_1 h_2 = \sum_{i=1}^4 \sum_{j=1}^4 a_i b_j M_i M_j$. Or par les calculs de la question 1, pour tout $(i, j) \in \llbracket 1, 4 \rrbracket^2$,

$M_i M_j \in \mathbf{H}_A$, et donc par stabilité de $\mathbf{H}_A$ par somme et par multiplication par un élément de A , $h_1 h_2 \in \mathbf{H}_A$.

Donc $\mathbf{H}_A$ est un sous-anneau de $\mathcal{M}_2(\mathbf{C})$.

4. Il est clair que $\tau(\mathbf{1}) = \mathbf{1}$.

Et si $h = a\mathbf{1} + b\mathbf{I} + c\mathbf{J} + d\mathbf{K}$ et $h' = a'\mathbf{1} + b'\mathbf{I} + c'\mathbf{J} + d'\mathbf{K}$, alors

$$\begin{aligned} \tau(h + h') &= (a + a')\mathbf{1} - (b + b')\mathbf{I} - (c + c')\mathbf{J} - (d + d')\mathbf{K} \\ &= a\mathbf{1} - b\mathbf{I} - c\mathbf{J} - d\mathbf{K} + a'\mathbf{1} - b'\mathbf{I} - c'\mathbf{J} - d'\mathbf{K} = \tau(h) + \tau(h'). \end{aligned}$$

Donc déjà, τ est un morphisme de groupes additifs.

Pour $h \in \mathbf{H}_A$ et $\lambda \in A$, avec les notations précédentes,

$$\tau(\lambda h) = \lambda a\mathbf{1} - \lambda b\mathbf{I} - \lambda c\mathbf{J} - \lambda d\mathbf{K} = \lambda \tau(h).$$

A présent, soient $h_1, h_2 \in \mathbf{H}_A$, et reprenons les notations utilisées à la question 3. On a donc

$$\tau(h_1 h_2) = \tau\left(\sum_{i=1}^4 \sum_{j=1}^4 a_i b_j M_i M_j\right) = \sum_{i=1}^4 \sum_{j=1}^4 a_i b_j \tau(M_i M_j).$$

D'autre part,

$$\tau(h_2)\tau(h_1) = \left(\sum_{i=1}^4 a_i \tau(M_i)\right) \left(\sum_{j=1}^4 b_j \tau(M_j)\right) = \sum_{i=1}^4 a_i b_j \tau(M_i)\tau(M_j).$$

Donc si on arrive à prouver que pour tout (i, j) , $\tau(M_i M_j) = \tau(M_j)\tau(M_i)$, alors on aura bien $\tau(h_1 h_2) = \tau(h_2)\tau(h_1)$.

Si $i = 1$ ou $j = 1$, c'est évidemment vrai.

Et si $i \geq 2$ et $j \geq 2$, alors $M_i M_j \in \{\pm\mathbf{I}, \pm\mathbf{J}, \pm\mathbf{K}\}$, et donc grâce aux calculs de la question 1, $\tau(M_i M_j) = -M_i M_j = M_j M_i = (-M_j)(-M_i) = \tau(M_j)\tau(M_i)$.

Donc pour tout $h_1, h_2 \in \mathbf{H}_A$, $\tau(h_1 h_2) = \tau(h_2)\tau(h_1)$.

5. Soit $z = a\mathbf{1} + b\mathbf{I} + c\mathbf{J} + d\mathbf{K} \in \mathbf{H}_A$. Alors un calcul un peu abrutissant⁵ nous donne,

$$\begin{aligned} z\tau(z) &= (a\mathbf{1} + b\mathbf{I} + c\mathbf{J} + d\mathbf{K})(a\mathbf{1} - b\mathbf{I} - c\mathbf{J} - d\mathbf{K}) \\ &= a^2\mathbf{1} - ab\mathbf{I} - ac\mathbf{J} - ad\mathbf{K} + ab\mathbf{I} - b^2\mathbf{I}^2 - bc\mathbf{I}\mathbf{J} - bd\mathbf{I}\mathbf{K} + ac\mathbf{J} - bc\mathbf{J}\mathbf{I} - c^2\mathbf{J}^2 - cd\mathbf{J}\mathbf{K} + da\mathbf{K} - db\mathbf{K}\mathbf{I} - dc\mathbf{K}\mathbf{J} - d^2\mathbf{K}^2 \\ &= a^2\mathbf{1} + b^2\mathbf{1} + c^2\mathbf{1} + d^2\mathbf{1} \\ &= (a^2 + b^2 + c^2 + d^2)\mathbf{1}. \end{aligned}$$

Et exactement sur le même principe, $\tau(z)z = (a^2 + b^2 + c^2 + d^2)\mathbf{1}$.

6. On vient de faire le calcul...

7. On a donc, pour $z, z' \in \mathbf{H}_A$,

$$N(zz') = zz'\tau(zz') = zz'\tau(z')\tau(z) = zN(z')\tau(z).$$

Mais puisque $N(z') \in \{\lambda\mathbf{1}, \lambda \in A\}$, $N(z')$ commute à toute matrice de $\mathcal{M}_2(\mathbf{C})$, et donc à $\tau(z)$, si bien que

$$N(zz') = z\tau(z)N(z') = N(z)N(z').$$

8. Si z est un élément inversible de $\mathbf{H}_R$, alors il existe $z' \in \mathbf{H}_R$ tel que $zz' = z'z = \mathbf{1}$. Et donc en particulier, $\mathbf{1} = N(zz') = N(z)N(z')$, si bien que $N(z) \neq 0$.

Remarque

Notons que τ n'est bien définie que parce qu'on a l'unicité des a, b, c, d de la question 2.

Remarque

On a utilisé les deux points déjà prouvés : l'image d'une somme est la somme des images, et le fait que $\tau(\lambda h) = \lambda\tau(h)$ pour $\lambda \in A$.

⁵ Mais utilisant de manière cruciale $\mathbf{I}\mathbf{J} = -\mathbf{J}\mathbf{I}$, $\mathbf{I}\mathbf{K} = -\mathbf{K}\mathbf{I}$, etc

Soit $z = a\mathbf{1} + b\mathbf{I} + c\mathbf{J} + d\mathbf{K} \in \mathbf{H}_{\mathbf{R}}$ un quaternion non nul. Puisque a, b, c, d sont non tous nuls, $a^2 + b^2 + c^2 + d^2$ n'est pas nul.

Posons alors $z' = \frac{1}{a^2 + b^2 + c^2 + d^2} \tau(z)$. On a alors

$$zz' = \frac{1}{a^2 + b^2 + c^2 + d^2} z \tau(z) = \frac{1}{a^2 + b^2 + c^2 + d^2} N(z) = \frac{a^2 + b^2 + c^2 + d^2}{a^2 + b^2 + c^2 + d^2} \mathbf{1} = \mathbf{1}.$$

Et puisque $z\tau(z) = \tau(z)z$, on a également $z'z' = \mathbf{1}$.

Donc z est inversible, et ainsi, tout élément non nul de $\mathbf{H}_{\mathbf{R}}$ est inversible, donc $\mathbf{H}_{\mathbf{R}}^{\times} = \mathbf{H}_{\mathbf{R}} \setminus \{0_2\}$.

Cela ne suffit pas tout à fait à faire de $\mathbf{H}_{\mathbf{R}}$ un corps, puisqu'il n'est pas commutatif, condition nécessaire dans la définition de corps.

Certains auteurs parlent quand même de corps non commutatif ou de corps gauche. On appelle aussi parfois algèbres à division de tels anneaux (non commutatifs dans lesquels tout élément non nul est inversible).

Commentaires : on montre assez facilement que $\{\lambda\mathbf{1}, \lambda \in \mathbf{R}\}$ est un sous-anneau de $\mathbf{H}_{\mathbf{R}}$, isomorphe à $\mathbf{R}$.

Et de même, $\{a\mathbf{1} + b\mathbf{I}, (a, b) \in \mathbf{R}^2\}$ est un sous-anneau de $\mathbf{H}_{\mathbf{R}}$ isomorphe à $\mathbf{C}$. Donc en quelque sorte, les quaternions sont une généralisation des complexes.

C'est Hamilton qui les a découverts en 1848, en cherchant un analogue des complexes en dimension 3.

On sait aujourd'hui qu'il n'y a pas de «corps» contenant $\mathbf{C}$ et de «dimension» 3, et que les quaternions sont le seul «corps» de dimension 4 contenant $\mathbf{C}$. Le prix à payer étant la perte de la commutativité du produit.

On peut également construire un analogue en dimension 8, les octaves de Cayley, mais cette fois, en plus de perdre la commutativité du produit, on perd aussi son associativité, ce qui, soyons honnêtes, en font des objets peu fréquentables⁶.

Partie II. Preuve du théorème des quatre carrés

9.a. Déjà il est clair que φ est bien à valeurs dans $(\mathbf{Z}/p\mathbf{Z})^{\times}$ puisque si $x \in (\mathbf{Z}/p\mathbf{Z})^{\times}$, alors x est inversible, et donc x^2 est également inversible.

Par ailleurs, pour tous $x, y \in (\mathbf{Z}/p\mathbf{Z})^{\times}$, par commutativité du produit⁷,

$$\varphi(xy) = (xy)^2 = x^2y^2 = \varphi(x)\varphi(y).$$

Donc φ est bien un morphisme de groupes.

Par ailleurs, pour $x \in (\mathbf{Z}/p\mathbf{Z})^{\times}$, $x \in \text{Ker } \varphi \Leftrightarrow x^2 = 1$.

Or $x^2 = 1 \Leftrightarrow x^2 - 1 = 0 \Leftrightarrow (x+1)(x-1) = 0$. Et $\mathbf{Z}/p\mathbf{Z}$ étant un corps, ceci équivaut $x+1 = 0$ ou $x-1 = 0 \Leftrightarrow x = 1$ ou $x = -1$.

Ainsi, $\text{Ker } \varphi = \{-1, 1\}$. Notons que puisque p impair, $1 \neq -1$, et donc $\text{Ker } \varphi$ est de cardinal 2.

9.b. La relation binaire $\mathcal{R}$ définie sur G par $f(x) = f(y)$ est évidemment une relation d'équivalence.

Mais pour $x, y \in G$, on a $x\mathcal{R}y \Leftrightarrow f(x)f(y)^{-1} = e_H \Leftrightarrow xy^{-1} \in \text{Ker } f \Leftrightarrow x \in (\text{Ker } f)y$.

Autrement dit, $\text{cl}(y) = (\text{Ker } f)y$, qui est en bijection⁸ avec $\text{Ker}(f)$, et donc de même cardinal que $\text{Ker}(f)$.

Enfin, il est clair qu'il y a autant de classes d'équivalence que le nombre d'éléments de $\text{Im } f$. Et donc les classes d'équivalence formant une partition de G , il vient $\text{Card}(G) = \text{Card}(\text{Im } f)\text{Card}(\text{Ker } f)$.

9.c. L'ensemble⁹ $\{x^2, x \in (\mathbf{Z}/p\mathbf{Z})^{\times}\}$ est l'image du morphisme φ de la question 9.a.

Donc par 9.b est de cardinal $\frac{\text{Card}(\mathbf{Z}/p\mathbf{Z})^{\times}}{\text{Card}(\text{Ker } \varphi)} = \frac{p-1}{2}$.

Puisque par ailleurs $0 = 0^2$ est un carré dans $\mathbf{Z}/p\mathbf{Z}$, l'ensemble des carrés de $\mathbf{Z}/p\mathbf{Z}$ est de cardinal $\frac{p-1}{2} + 1 = \frac{p+1}{2}$.

Remarque

Notons qu'ici on a vraiment besoin d'être dans $\mathbf{R}$, ce serait faux pour des quaternions complexes, car dans $\mathbf{C}$, une somme de carrés non nuls peut être nulle.

Dimension ?

Nous donnerons plus tard une définition précise, l'idée étant que la donnée d'un complexe équivaut à la donnée de deux réels, les complexes sont de dimension 2.

Et la donnée d'un quaternion étant celle de 4 réels, les quaternions sont de dimension 4.

⁶ Ou du moins avec lesquels on souhaite éviter tout calcul.

⁷ Rappelons que les $\mathbf{Z}/n\mathbf{Z}$ sont toujours des anneaux commutatifs.

Remarque

Notons que pour $p = 2$, on aurait $1 = -1$, et donc $\text{Ker } \varphi$ serait de cardinal 1.

⁸ Via la translation à gauche par y :

Autrement dit

Chaque élément de $\text{Im } f$ possède $\text{Card}(\text{Ker } f)$ antécédents par f .

⁹ Formé des carrés non nuls de $\mathbf{Z}/p\mathbf{Z}$.

9.d. Ces deux ensembles sont évidemment en bijection, et donc sont tous deux de cardinal $\frac{p+1}{2}$. S'ils étaient disjoints, leur union serait de cardinal $\frac{p+1}{2} + \frac{p+1}{2} = p+1$. Mais cette union est une partie de $\mathbf{Z}/p\mathbf{Z}$, qui est de cardinal p , donc de cardinal inférieur ou égal à p .

Par conséquent, $\{x^2, x \in \mathbf{Z}/p\mathbf{Z}\}$ et $\{-1 - y^2, y \in \mathbf{Z}/p\mathbf{Z}\}$ ne sont pas disjoints.

9.e. Soient donc $a, b \in \mathbf{Z}/p\mathbf{Z}$ tels que $a^2 = -1 - b^2$.

Rappelons que a et b sont des classes d'équivalence modulo p , et considérons alors x et y deux éléments de $\llbracket 0, p-1 \rrbracket$ tels que $a = \bar{x}$ et $b = \bar{y}$.

On a donc $1 + a^2 + b^2 = 1 + x^2 + y^2$, si bien qu'il existe $m \in \mathbf{Z}$ tel que $1 + x^2 + y^2 = mp$.

Reste à prouver qu'on peut avoir $m < p$.

Pour cela, notons que si $x \geq \frac{p+1}{2}$, alors $(p-x)^2 \equiv (-x)^2 \equiv x^2 \pmod{p}$, avec $0 \leq p-x \leq p < p - \frac{p+1}{2} = \frac{p-1}{2}$.

Donc quitte à changer x en $p-x$, et de même pour y , on peut supposer $x, y \in \llbracket 0, \frac{p-1}{2} \rrbracket$.

Et donc $1 + x^2 + y^2 \leq 1 + \frac{(p-1)^2}{4} + \frac{(p-1)^2}{4} < 1 + \frac{p^2}{2} < p^2$.

Et donc $m = \frac{1 + x^2 + y^2}{p} < p$.

Le fait que m soit strictement positif est immédiat.

10. Soient $a, b \in \mathcal{N}$, et soient $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$ des entiers tels que $a = x_1^2 + x_2^2 + x_3^2 + x_4^2$ et $b = y_1^2 + y_2^2 + y_3^2 + y_4^2$.

Soit alors $z = x_1\mathbf{1} + x_2\mathbf{I} + x_3\mathbf{J} + x_4\mathbf{K} \in \mathbf{HZ}$ et $z' = y_1\mathbf{1} + y_2\mathbf{I} + y_3\mathbf{J} + y_4\mathbf{K} \in \mathbf{HZ}$, de sorte que $a = N(z)$ et $b = N(z')$.

Alors par la question 7, $ab = N(z)N(z') = N(zz')$, avec $zz' \in \mathbf{HZ}$.

Et donc si on note c_1, c_2, c_3, c_4 les entiers relatifs tels que $zz' = c_1\mathbf{1} + c_2\mathbf{I} + c_3\mathbf{J} + c_4\mathbf{K}$, alors

$$ab = c_1^2 + c_2^2 + c_3^2 + c_4^2 = |c_1|^2 + |c_2|^2 + |c_3|^2 + |c_4|^2 \in \mathcal{N}.$$

Et donc $\mathcal{N}$ est bien stable par produit.

Remarque : notons qu'avec un peu de courage, et en calculant explicitement zz' , on pourrait donner une formule générale pour exprimer le produit de deux nombres sommes de quatre carrés comme une somme de quatre carrés.

Cette formule avait été établie par Euler dès 1748 (sans passer par les quaternions).

11.a. C'est la question 9.e., il existe $x, y \in \mathbf{N}$ et $m \in \llbracket 1, p-1 \rrbracket$ tels que

$$mp = 1 + x^2 + y^2 = 0^2 + 1^2 + x^2 + y^2 \in \mathcal{N}.$$

11.b.i. Il faut bien comprendre qu'appliquer une permutation $\sigma \in \mathfrak{S}_4$ revient à échanger les x_i .

Notons que pour tout entier k , les entiers k et k^2 ont même parité.

Puisque mp est pair¹⁰, on ne peut pas avoir trois des x_i qui sont pairs et le dernier impair, ni avoir trois des x_i impairs et le dernier pair.

Supposons, quitte à les échanger que x_1, x_2 sont de même parité, et que x_3, x_4 sont également de même parité.

Et quitte à les échanger de nouveau, on peut supposer $x_1 \geq x_2$ et $x_3 \geq x_4$. Et alors $x_1 + x_2$ et $x_1 - x_2$ sont tous deux pairs et positifs. Et de même pour $x_3 + x_4$ et $x_3 - x_4$.

Donc il existe bien $\sigma \in \mathfrak{S}_4$ telle que les quatre entiers $x_{\sigma(1)} + x_{\sigma(2)}$, $x_{\sigma(1)} - x_{\sigma(2)}$, $x_{\sigma(3)} + x_{\sigma(4)}$, $x_{\sigma(3)} - x_{\sigma(4)}$ soient pairs et positifs.

11.b.ii. On a donc

$$(x_{\sigma(1)} + x_{\sigma(2)})^2 + (x_{\sigma(1)} - x_{\sigma(2)})^2 + (x_{\sigma(3)} + x_{\sigma(4)})^2 + (x_{\sigma(3)} - x_{\sigma(4)})^2 = 2x_{\sigma(1)}^2 + 2x_{\sigma(2)}^2 + 2x_{\sigma(3)}^2 + 2x_{\sigma(4)}^2 = 2mp.$$

Mais puisque nos quatre nombres sont pairs, leurs carrés sont divisibles par 4, si bien que

$$\frac{mp}{2} = \left(\frac{x_{\sigma(1)} + x_{\sigma(2)}}{2}\right)^2 + \left(\frac{x_{\sigma(1)} - x_{\sigma(2)}}{2}\right)^2 + \left(\frac{x_{\sigma(3)} + x_{\sigma(4)}}{2}\right)^2 + \left(\frac{x_{\sigma(3)} - x_{\sigma(4)}}{2}\right)^2 \in \mathcal{N}.$$

11.c. Supposons par l'absurde m_0 pair. Alors $\frac{m_0 p}{2} \in \mathcal{N}$, contredisant la minimalité de m_0 .

Et par conséquent, m_0 est impair.

Autrement dit

$\mathcal{N}$ est l'ensemble des $N(z)$, pour $z \in \mathbf{HZ}$.

¹⁰ Car m l'est.

Détails

Il peut donc y en avoir 4 pairs, deux pairs et deux impairs ou 4 impairs.

11.d.i. Notons b_i, r_i le reste de la division euclidienne de x_i par m_0 .

Si $y_i < \frac{m_0}{2}$, alors posons $y_i = r_i = x_i - b_i m_0$.

Et sinon, posons $y_i = r_i - m_0 = x_i - (b_i + 1)m_0$, qui vérifie bien $-\frac{m_0}{2} \leq y_i < 0$.

Et comme m_0 impair, $\frac{m_0}{2}$ n'est pas un entier, donc il ne peut pas y avoir égalité, si bien que $|y_i| < \frac{m_0}{2}$.

On a alors clairement $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv m_0 p \equiv 0 \pmod{m_0}$.

Et enfin, les y_i^2 sont tous strictement compris entre 0 et $\frac{m_0^2}{4}$ donc $0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < m_0^2$.

11.d.ii. Utilisons l'indication, et notons z_1, z_2, z_3, z_4 les entiers tels que

$$(x_1 \mathbf{1} + x_2 \mathbf{I} + x_3 \mathbf{J} + x_4 \mathbf{K})(y_1 \mathbf{1} - y_2 \mathbf{I} - y_3 \mathbf{J} - y_4 \mathbf{K}) = z_1 \mathbf{1} + z_2 \mathbf{I} + z_3 \mathbf{J} + z_4 \mathbf{K}.$$

On a alors

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = N(x_1 \mathbf{1} + x_2 \mathbf{I} + x_3 \mathbf{J} + x_4 \mathbf{K})N(y_1 \mathbf{1} - y_2 \mathbf{I} - y_3 \mathbf{J} - y_4 \mathbf{K}) = \left(\sum_{i=1}^4 x_i^2 \right) \left(\sum_{i=1}^4 y_i^2 \right) = m_0 p m_1 m_0.$$

En développant le calcul, on obtient

$$\begin{aligned} z_1 &= x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 = x_1(x_1 - b_1 m_0) + x_2(x_2 - b_2 m_0) + x_3(x_3 - b_3 m_0) + x_4(x_4 - b_4 m_0) \\ &= \underbrace{(x_1^2 + x_2^2 + x_3^2 + x_4^2)}_{=m_0 p} - m_0(x_1 b_1 + x_2 b_2 + x_3 b_3 + x_4 b_4) \equiv 0 \pmod{m_0} \end{aligned}$$

$$\begin{aligned} z_2 &= -x_1 y_2 + x_2 y_1 + x_3 y_4 - x_4 y_3 = -x_1(x_2 - b_2 m_0) + x_2(x_1 - b_1 m_0) + x_3(x_4 - b_4 m_0) - x_4(x_3 - b_3 m_0) \\ &= -m_0(b_1 x_2 - b_2 x_1 - b_3 x_4 + b_4 x_3) \equiv 0 \pmod{m_0} \end{aligned}$$

$$\begin{aligned} z_3 &= -x_1 y_3 + x_2 y_4 + x_3 y_1 - x_4 y_2 = -x_1(x_3 - b_3 m_0) + x_2(x_4 - b_4 m_0) + x_3(x_1 - b_1 m_0) - x_4(x_2 - b_2 m_0) \\ &= -m_0(b_1 x_3 - b_3 x_1 - b_2 x_4 + b_4 x_2) \equiv 0 \pmod{m_0} \end{aligned}$$

$$\begin{aligned} z_4 &= -x_1 y_4 - x_2 y_3 + x_3 y_2 + x_4 y_1 = -x_1(x_4 - b_4 m_0) - x_2(x_3 - b_3 m_0) + x_3(x_2 - b_2 m_0) + x_4(x_1 - b_1 m_0) \\ &= -m_0(b_1 x_4 + b_2 x_3 - b_3 x_2 - b_4 x_1) \equiv 0 \pmod{m_0}. \end{aligned}$$

11.e. Étant données les conditions vérifiées par les y_i , on a $m_1 < m_0$.

Et puisque tous les z_i sont divisibles par m_0 , si on note $z_i = m_0 z'_i$, il vient donc $\sum_{i=1}^4 z_i'^2 = m_1 p$,

avec $0 < m_1 < m_0$, contredisant la minimalité de m_0 .

On en déduit donc que $m_0 = 1$.

12. La question précédente prouve en fait que tout premier impair est somme de quatre carrés.

Il est clair que $2 = 1^2 + 1^2 + 0^2 + 0^2$ est également somme de 4 carrés.

Et donc par la question 10, et puisque tout entier naturel est produit de nombres premiers, tout entier naturel est somme de quatre carrés.

Notons que 4 est optimal en ce sens qu'il existe des entiers qui ne sont pas sommes de 2 ou 3 carrés. C'est par exemple le cas de 7 ou de 15.