# 16 PROBLÈMES INÉDITS DE MATHS

## MP* MPI*

Michel Cognet

# Problème 1 :
# Théorème des deux et quatre carrés

**Notions requises** : calcul matriciel, groupe, $\mathbb{Z}/p\mathbb{Z}$, idéal, théorème chinois.

**ENONCE**
Soit $A = \{ a + ib \ , \ (a, b) \in \mathbb{Z}^2 \}$.
On rappelle que $A$ est un sous-anneau de $\mathbb{C}$ et on admet qu'il est principal, c'est-à-dire que tout idéal de $A$ est engendré par un élément.

Si $z$ est un nombre complexe, on notera $zA$ l'ensemble des éléments $zv$ pour $v$ décrivant $A$.
Si $p$ est un entier naturel premier, si $x$ appartient à $\mathbb{Z}$, on notera $\hat{x}$ la classe de $x$ dans $\mathbb{Z}/p\mathbb{Z}$.
Si $p$ est un entier naturel premier impair, on sait qu'il existe un entier relatif $u$ tel que le carré de $\hat{u}$ est égal à $\hat{-1}$ si et seulement si $p$ est congru à 1 modulo 4 (preuve qu'on peut retrouver dans le problème 0 de ce livre).

**Première partie : entiers qui sont somme de deux carrés d'entiers**
**Q.1** Montrer qu'un élément $z$ de $A$ est inversible dans l'anneau $A$ si et seulement si $| z |$ est égal à 1.

**Q.2** Soit $p$ un entier naturel premier congru à 1 modulo 4 et soit $u$ comme ci-dessus.
Soit $J = \{ px + (u + i)x' \ , \ (x, x') \in A^2 \}$.
Montrer qu'il existe $z$ dans $A$ tel que $J = zA$.
Montrer que, en choisissant l'entier $u$, que $J$ et $pA$ sont deux ensembles distincts.
Montrer qu'il existe $c$ non inversible dans $A$ tel que $p$ est égal à $cz$.

**Q.3** Soit $p$ un entier naturel premier congru à 1 modulo 4.
Montrer en utilisant les questions précédentes qu'il existe deux entiers naturels $x$ et $y$ tels que $p$ est égal à $(x^2 + y^2)$.

**Q.4** Soit $\mathbb{P}_1$ (resp. $\mathbb{P}_2$) l'ensemble des entiers naturels premiers congrus à 1 (resp. à 3) modulo 4.
**Q.4.a** Montrer que, si $n$ est un entier naturel supérieur ou égal à 2, si $p$ est un élément de $\mathbb{P}_2$ divisant $n$, s'il existe deux entiers relatifs $x$ et $y$ tels que $n$ est égal

à $(x^2+y^2)$, alors $p$ divise à la fois $x$ et $y$.
Que dire alors de $\frac{n}{p^2}$ ?

**Q.4.b** Soient $n$ et $m$ deux entiers naturels qui s'écrivent comme la somme de deux carrés d'entiers naturels.
Montrer alors que $(mn)$ s'écrit aussi comme la somme de deux carrés d'entiers naturels.

**Q.4.c** Si $p$ est un entier naturel premier, si $n$ est un entier naturel non nul, on pourra noter $\beta_p^n$ l'entier naturel $k$ tel que $p^k$ divise $n$ et tel que $p^{k+1}$ ne divise pas $n$ (autrement dit, $\beta_p^n$ est la valuation $p$-adique de l'entier $n$).
Montrer qu'un entier naturel $n$ est la somme de deux carrés d'entiers si et seulement s'il est nul ou s'il est égal à 1 ou si, quel que soit $p$ appartenant à $\mathbb{P}_2$, l'entier $\beta_p^n$ est pair.

**Seconde partie : Entiers qui sont somme de quatre carrés d'entiers**
On va obtenir dans cette seconde partie que tout entier naturel est la somme de quatre carrés d'entiers.

La méthode étudiée ici repose sur deux interactions (on dit actions en mathématiques) entre un groupe et un ensemble de matrices à deux lignes et deux colonnes.
On définit :

$$C \;=\; \{\; \begin{pmatrix} m & x \\ x & n \end{pmatrix} \;,\; (m,n,x) \in \mathbb{N}^{*2} \times \mathbb{Z} \;,\; mn - x^2 \;=\; 1 \;\} \text{ et}$$

$$B \;=\; \{\; \begin{pmatrix} m & \overline{z} \\ z & n \end{pmatrix} \;,\; (m,n,z) \in \mathbb{N}^{*2} \times A \;,\quad mn - |\, z \,|^2 = \; 1 \;\} \quad .$$

On définit aussi les deux ensembles :

$$G \;=\; \{\; \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \;,\; a \in \mathbb{Z} \;\} \text{ et}$$

$$G' \;=\; \{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \;,\; a \in A \;\} \quad .$$

On remarquera (mais inutile de le redémontrer) que $G$ (resp. $G'$) est un sous-groupe de $GL_2(\mathbb{R})$ (resp. de $GL_2(\mathbb{C})$).

Si $g$ est un élément de $\mathcal{M}_2(\mathbb{C})$, on notera ${}^t g$ sa transposée et $\overline{g}$ la matrice obtenue à partir de $g$ en conjuguant tous ses coefficients. On fait remarquer qu'ainsi, les deux matrice ${}^t(\overline{g})$ et $\overline{{}^t g}$ sont égales.

**Q.5.a** Vérifier que, si $M$ (resp. $M'$) est un élément de $C$ (resp. de $B$), alors $M^{-1}$ (resp. $M'^{-1}$) est encore un élément de $C$ (resp. de $B$).

**Q.5.b** Montrer que, si $(g, g', M, M')$ appartient à $G \times G' \times C \times B$, alors l'élément $g.M.{}^t g$ (resp. $g'.M'.{}^t\overline{g'}$) appartient à $C$ (resp. à $B$).

Soit $(M, N)$ un élément de $C \times B$.
On définit alors les deux ensembles :

$$\omega_M \ = \ \{ \ g.M.{}^t g \ , \ g \in G \ \} \text{ et}$$

$$\omega'_N \ = \ \{ \ g.N.{}^t \overline{g} \ , \ g \in G' \ \} \quad .$$

D'après ce qui précède, $\omega_M$ (resp. $\omega'_N$) est inclus dans $C$ (resp. dans $B$).

**Q.5.c** Soit $x$ dans $\mathbb{R}$. Montrer qu'il existe un entier $q$ tel que $\mid x - q \mid$ est inférieur ou égal à $\frac{1}{2}$.
En déduire que, si $(a, b)$ appartient à $\mathbb{Z} \times \mathbb{Z}^*$, il existe $(q, r)$ dans $\mathbb{Z}^2$ tel que :

$$a \ = \ bq + r \text{ et } \mid r \mid \leq \ \frac{\mid b \mid}{2} \quad .$$

Montrer que, si $z$ appartient à $\mathbb{C}$, il existe $q$ dans $C$ tel que $\mid z - q \mid$ est inférieur ou égal à $\frac{1}{\sqrt{2}}$.
En déduire que, quel que soit $(a, b)$ dans $A \times A^*$ (où $A^*$ désigne l'ensemble des éléments non nuls de $A$), il existe $(q, r)$ dans $A^2$ tel que :

$$a \ = \ bq + r \text{ et } \mid r \mid^2 \leq \ \frac{\mid b \mid^2}{2} \quad .$$

**Remarque**
C'est à partir de ce résultat qu'on montre que $A$ est un anneau principal, ce qu'on n'a pas fait établir car c'est très souvent fait en TD ou en cours.■

**Q.5.d** Soit $M$ dans $C$ et soit $N$ dans $B$ écrits sous la forme suivante :

$$N \ = \ \begin{pmatrix} m & \overline{z} \\ z & n \end{pmatrix} \text{ et } M \ = \ \begin{pmatrix} m & x \\ x & n \end{pmatrix} \quad .$$

Déterminer les éléments $M$ tels que $\mid x \mid$ est nul ou égal à 1.
Déterminer les éléments $N$ tels que $\mid z \mid$ est nul ou égal à 1.

**Q.5.e** On garde les notations utilisées dans la question précédente.
Montrer que, si $\mid x \mid$ est nul ou égal à 1, il existe $P$ dans $\mathcal{M}_2(\mathbb{R})$, à coefficients entiers, de déterminant égal à 1 ou $(-1)$ tel que :

$$M \ = \ P.{}^t P \quad .$$

Montrer que, si $\mid z \mid^2$ est nul ou égal à 1, il existe $P$ dans $\mathcal{M}_2(\mathbb{C})$, à coefficients dans $A$, de déterminant égal à 1 ou $(-1)$ tel que :

$$N \ = \ P.{}^t \overline{P} \quad .$$

**Q.5.f** On garde les notations des questions précédentes (notamment pour l'écriture de $M$ et de $N$).

En utilisant notamment la question précédente, montrer qu'il existe $M_1$ dans $\omega_M$ qu'on va noter $\begin{pmatrix} m' & x' \\ x' & n \end{pmatrix}$ tel que $\mid x' \mid$ est inférieur ou égal à $\frac{n}{2}$ (l'entier $n$ qui paraît dans $M_1$ est le même que celui qui paraît dans $M$).
Montrer qu'il existe $N_1 = \begin{pmatrix} m' & \overline{z'} \\ z' & n \end{pmatrix}$ dans $\omega'_N$ tel que $\mid z' \mid^2$ est inférieur ou égal à $\frac{n^2}{2}$ (l'entier $n$ qui paraît dans $N_1$ est le même que celui qui paraît dans $N$).

**Q.6** On garde les notations des questions précédentes.

**Q.6.a** Vérifier que, si $M$ est un élément de $\mathcal{M}_2(\mathbb{R})$ pour lequel il existe $P$ dans $\mathcal{M}_2(\mathbb{R})$, à coefficients entiers, de déterminant égal à 1 ou $(-1)$ vérifiant $M = P.{}^tP$, alors $M^{-1}$ s'écrit aussi $Q.{}^tQ$ avec $Q$ dans $\mathcal{M}_2(\mathbb{R})$, à coefficients entiers et de déterminant égal à 1 ou $(-1)$.

On admettra (vérification semblable) que, si $N$ est un élément de $\mathcal{M}_2(\mathbb{C})$ pour lequel il existe $Q$ dans $\mathcal{M}_2(\mathbb{C})$, à coefficients dans $A$, de déterminant égal à 1 ou $(-1)$ vérifiant $N = Q{}^t\overline{Q}$, alors $N^{-1}$ s'écrit aussi $R{}^t\overline{R}$ avec $R$ dans $\mathcal{M}_2(\mathbb{C})$, à coefficients dans $A$ et de déterminant égal à 1 ou $(-1)$.

**Q.6.b** Soit $M$ dans $C$. Montrer qu'il existe $P$ dans $\mathcal{M}_2(\mathbb{R})$, à coefficients entiers, de déterminant égal à 1 ou $(-1)$ tel que :

$$M = P.{}^tP \quad .$$

**Q.6.c** Soit $N$ dans $B$.
Montrer qu'il existe $P$ à coefficients dans $A$, de déterminant égal à 1 ou $(-1)$ tel que :

$$N = P.{}^t\overline{P} \quad .$$

**Q.7** Soit $p$ un entier naturel premier.
Si $x$ est un entier relatif, on rappelle la notation $\hat{x}$ pour désigner la classe de $x$ dans $\mathbb{Z}/p\mathbb{Z}$.

Retrouver, en utilisant que $\hat{-1}$ est le carré d'un certain élément $\hat{u}$ de $\mathbb{Z}/p\mathbb{Z}$ et en utilisant une décomposition d'un certain élément de $C$ comme il est établi dans la question Q.6.b, que, si $p$ est un entier naturel premier congru à 1 modulo 4, il existe deux entiers naturels tels que $p$ est égal à $(x^2 + y^2)$.

**Remarque**
On peut montrer, qu'à partir de là, on a retrouvé le résultat obtenu dans la question Q.3 et l'essentiel est fait pour trouver les entiers qui sont somme de deux carrés en suivant la question Q.4.■

**Q.8.a** Soit $p = 2$ dans cette sous-question.
Vérifier qu'il existe $x$ et $y$ entiers tels que :

$$\hat{x}^2 + \hat{y}^2 + \hat{1} = \hat{0} \quad .$$

**Q.8.b** On suppose que $p$ est impair dans cette sous-question.
Soit $\Psi$ l'application de $(\mathbb{Z}/p\mathbb{Z})^*$ dans $(\mathbb{Z}/p\mathbb{Z})^*$ donnée par :

$$\forall x \in \mathbb{Z}\ ,\ \Psi(\hat{x})\ =\ \hat{x}^2\quad .$$

Vérifier que $\Psi$ est un morphisme de groupe et déterminer son noyau.
Si $\hat{x}$ est dans $Im(\Psi)$, déterminer le nombre d'éléments qui sont antécédents de $\hat{x}$.
En déduire le nombre d'éléments de $\{\ \hat{x}^2\ ,\ \hat{x}\ \in \mathbb{Z}/p\mathbb{Z}\ \}$.
Montrer qu'il existe toujours un couple d'entiers relatifs $(x, y)$ tel que :

$$\hat{x}^2\ =\ -\hat{1} - \hat{y}^2\quad .$$

**Q.8.c** Soit $p$ un entier naturel premier impair.
Montrer qu'il existe $z$ dans $A$ et $m$ dans $\mathbb{N}^*$ tels que la matrice $\begin{pmatrix} m & \overline{z} \\ z & p \end{pmatrix}$ appartient à $B$.
Montrer que tout entier naturel premier $q$ est la somme de quatre carrés d'entiers naturels (c'est-à-dire qu'il existe $(a, b, c, d)$ dans $\mathbb{N}^4$ tel que :

$$q\ =\ (a^2 + b^2 + c^2 + d^2)\ ).$$

**Q.9.a** Soit $n$ un entier naturel libre de carrés (id est un entier naturel $n$ différent de 1 tel qu'il s'écrit sous la forme $\prod_{1 \leq j \leq r} p_j$ où $r$ est dans $\mathbb{N}^*$ et où $p_1$, ..., $p_r$ sont $r$ entiers naturels premiers deux à deux distincts).
On suppose dans la suite que $n$ est décomposé comme ci-dessus.
Si $x$ est un entier relatif, soit $\widehat{x}^{(n)}$ sa classe dans $\mathbb{Z}/n\mathbb{Z}$.
Montrer qu'il existe un couple d'entiers naturels $(x, y)$ tel que :

$$(\widehat{x}^{(n)})^2 + (\widehat{x}^{(n)})^2 + \hat{1}\ =\ \hat{0}\quad .$$

Montrer l'existence d'un élément $\begin{pmatrix} m & \overline{z} \\ z & n \end{pmatrix}$ appartenant à $B$ et montrer que $n$ est la somme de quatre carrés d'entiers naturels.

**Q.9.b** Montrer que tout entier naturel est la somme de quatre carrés d'entiers naturels (théorème de Lagrange).

**Remarque**
On s'est posé la question de savoir si tout entier naturel était la somme de trois carrés d'entiers naturels. La réponse est négative et on peut montrer qu'un entier naturel est somme de trois carrés d'entiers naturels si et seulement s'il n'est pas de la forme $4^n(8q + 7)$, une preuve moderne utilisant des objets assez forts (les nombres p-adiques), preuve présentée par le mathématicien Jean-Pierre Serre, médaille Fields, Prix Abel et bien d'autres choses encore dans son "cours d'arithmétique" (chez PUF).
Ah, merveille que le bruissement des nombres ! ■

**UN CORRIGE POSSIBLE**

**Q.1** Si $z$ est inversible dans $A$, alors il existe $z'$ dans $A$ tel que $zz'$ est égal à 1.
Donc : $\mid z \mid^2 . \mid z' \mid^2 = 1$.
Or, tout élément de $A$ est tel que le carré de son module est un entier naturel.
L'égalité ci-dessus implique que $\mid z \mid^2$ est l'entier 1 : $\mid z \mid$ est bien égal à 1.

Réciproquement, si $z$ est un élément de $A$ tel que $\mid z \mid$ est égal à 1, $(z.\overline{z})$ est égal à 1 et $\overline{z}$ qui appartient aussi à $A$ est donc l'inverse de $z$ dans $A$.
Les éléments inversibles de $A$ (pour la multiplication) sont donc bien les éléments de $A$ de module égale à 1.

**Remarque**
Si $z = (a + ib)$ est dans $A$ (avec $a$ et $b$ deux entiers), alors $z$ est inversible dans $A$ si et seulement si $\mid a \mid$ est égal à 1 et $b$ est nul ou si $a$ est nul et $\mid b \mid$ est égal à 1.
les éléments de $A$ qui sont inversibles sont donc au nombre de quatre, à savoir : 1, $(-1)$ , $i$ et $(-i)$.

**Q.2** Il suffit de vérifier que $J$ est un idéal de $A$.
$J$ est non vide ( il contient 0).
Si $\alpha$ (resp. $\alpha'$) appartient à $J$ et est écrit $(px + (u + i)x')$(resp. $(py + (u + i)y')$) avec $x$ et $x'$ (resp. avec $y$ et $y'$) dans $A$, on a bien :

$$(\alpha - \alpha') = p(x - y) + (u + i)(x' - y')$$

$J$ est donc déjà un sous-groupe de $A$ (pour l'addition).
Et si $v$ appartient à $A$, on a aussi :

$$\alpha v = p(xv) + (u + i)(x'v),$$

ce qui montre que $\alpha v$ reste dans $J$ quel que soit $(\alpha, v)$ dans $J \times A$.
Puisque $J$ est un idéal de $A$, puisque $A$ est un anneau principal, il existe bien $z$ dans $A$ tel que $J$ est l'ensemble $zA$.

L'ensemble $pA$ est inclus dans $J$ (tout élément $px$, pour $x$ dans $A$, s'écrit bien $(px + (u + i).0)$).
L'élément $(u + i)$ appartient à $J$ et n'appartient pas à $pA$ : sinon, il existerait $x$ dans $A$ tel que $(u + i)$ est égal à $px$.
On aurait donc :

$$\mid (u + i) \mid^2 = (u^2 + 1) = p^2 \mid x \mid^2 \geq p^2 \quad \text{(RR)}$$

Mais la classe de $u$ modulo $p$ est la classe d'un entier $k$ modulo $p$ tel que $k$ est compris entre 1 et $(p - 1)$.
Si on choisit $k$ ainsi, on a

$$(u^2 + 1) \leq (p - 1)^2 + 1 = (p^2 - 2p + 2) < p^2$$

(rappelons que $p$ est congru à 1 modulo 4 et, donc, $p$ est supérieur ou égal à 5).

Ceci contredit (RR) : $(u+i)$ est dans $J$ sans être dans $pA$.
Les deux ensembles $pA$ et $J$ sont donc distincts (notons que $pA$ est donc strictement inclus dans $J$).

Puisque $p$ appartient à $A$, il existe $c$ dans $A$ tel que $p = cz$.
Si on suppose d'aventure que $c$ est inversible dans $A$, on a :

$$\forall\, k \in A\ ,\ zk = (cz)(c^{-1}k) = p(c^{-1}k) \in pA$$

Ceci impliquerait que $J$ (qui est $zA$) est inclus dans $pA$, ce qui n'est pas : donc $c$ ne peut être inversible dans $A$ (c'est-à-dire que $c$ appartient à $A$ et que $\mid c \mid$ est différent de 1).

**Q.3** Gardons les notations précédentes et soit $c$ dans $A$ non inversible dans $A$ tel que $p$ est égal à $cz$.
On a donc :

$$p^2 = \mid cz \mid^2 = \mid c \mid^2 . \mid z \mid^2$$

Puisque $\mid c \mid^2$ est un entier naturel différent de 1, puisque $\mid z \mid^2$ est un entier naturel, on en déduit que $\mid c \mid^2$ est égal à $p$ ou $p^2$.

Supposons d'aventure que $\mid c \mid^2$ est égal à $p^2$.
L'élément $z$ de $A$ tel que $p$ est égal à $(cz)$ est donc tel que $\mid z \mid^2$ est égal à 1 et $z$ est donc un élément inversible de $A$ (autrement dit $z^{-1}$ appartient à $A$).
Donc $J$ est un idéal de $A$ contenant l'élément inversible $z$ (rappelons que $J$ est égal à $zA$) : ceci signifie que $J$ est égal à $A$ (un idéal de $A$ qui contient un élément inversible est l'anneau tout entier puisque, quel que soit $k$ dans $A$, $k$ est l'élément $(\ z(z^{-1}k))$ qui appartient à $zA$ , donc $k$ appartient $J$ quel que soit $k$ dans $A$ ....).
Puisque $J$ est alors $A$, l'élément 1 est dans $J$ : il existe $x$ et $x'$ dans $A$ tels que $1 = (px + (u+i)x')$, ce qui donne :

$$1 = (px + (u+i)x')\overline{(px + (u+i)x')}$$

$$= p(p \mid x \mid^2 + (u-i)x\overline{x'} + (u+i)\overline{x}x') + (u^2+1) \mid x' \mid^2$$

Puisque $p$ divise $(u^2+1)$, il existe donc $\beta$ dans $A$ (à savoir $(p \mid x \mid^2 + (u-i)\overline{x'}x + (u+i)x')\overline{x} + k \mid x' \mid^2)$ où $k$ vérifie l'égalité $:(u^2+1) = pk)$ tel que 1 est égal à $p\beta$.
En passant aux modules (pour avoir des égalités entre entiers), on aurait donc : $1 = p^2 \mid \beta \mid^2$, ce qui est impossible.
C'est donc que $\mid c \mid^2$ est égal à $p$.
En écrivant $c = (a+ib)$ avec $a$ et $b$ entiers, $p$ est bien l'entier $(\mid a \mid^2 + \mid b \mid^2)$ et $p$ est donc bien somme de deux carrés d'entiers naturels.

**Q.4.a** $p$ est fixé dans $\mathbb{P}_2$ tel que $p$ divise l'entier naturel $n = (x^2+y^2)$.
Pour tout entier $x$, on notera toujours $\hat{x}$ sa classe dans $\mathbb{Z}/p\mathbb{Z}$.
On a donc :

$$\hat{x}^2 + \hat{y}^2 = \hat{0} \quad \text{(RRR)}$$

Si $\hat{y}$ est non nul, $\hat{y}$ est inversible dans le corps $\mathbb{Z}/p\mathbb{Z}$ (pour la multiplication).
Soit $u$ dans $[[1,(p-1)]]$ tel que : $\hat{u} = (\hat{y})^{-1}$.

La relation $(RRR)$ devient :

$$\widehat{xu}^2 \ = \ \hat{-}1$$

Mais on sait que ceci n'est possible que si $p$, étant impair, est dans $\mathbb{P}_1$.
L'élément $\hat{y}$ est donc nul : la relation (RRR) devient donc $\hat{x}^2 \ = \ 0$ et, puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps (donc est un anneau intègre), $\hat{x}$ est nul.
Il existe donc $x'$ et $y'$ deux entiers tels que $x = px'$ et $y = py'$ .
Donc :

$$n \ = \ p^2(x'^2 + y'^2)$$

$\frac{n}{p^2}$ est donc lui aussi un entier qui est somme de deux carrés.

On a donc démontré dans cette question que, si $p$ est dans $\mathbb{P}_2$, si $n$ est un entier divisible par $p$ en étant somme deux carrés, alors $p^2$ divie $n$ et $\frac{n}{p^2}$ reste un entier somme de deux carrés.

**Q.4.b** Soit $m \ = \ (x^2 + y^2)$ avec $x$ et $y$ entiers naturels.
Soit $n \ = \ (a^2 + b^2)$ avec $a$ et $b$ entiers naturels.
On a alors :

$$mn \ = \ (x^2 + y^2)(a^2 + b^2) \ = \mid (x + iy)(a + ib) \mid^2 = \ ((\mid ax - by \mid)^2 + (\mid bx + ay \mid)^2)$$

L'entier $(mn)$ est bien somme de ceux carrées d'entiers naturels.

**Remarque**
Par récurrence simple, on montre qu'un produit en nombre fini d'entiers qui sont somme de deux carrés dentiers naturels reste somme de deux carrés d'entiers naturels.■

**Q.4.c** Si $n$ est 0 ou 1 , $n$ est clairement la somme de deux carrés d'entiers (0 est $(0^2 + 0^2)$ et 1 est $(1^2 + 0^2)$).
Soit $n$ dans $\mathbb{N}^*$ différent de 1 et tel que quel que soit $p$ dans $\mathbb{P}_2$, l'entier $\beta_p^n$ est pair (égal à $2\delta_p^n$).
Soit $A_n$ l'ensemble des nombres premiers naturels appartenant à $\mathbb{P}_1$ divisant $n$.
Soit $B_n$ l'ensemble des nombres premiers naturels appartenant à $\mathbb{P}_2$ divisant $n$.
On a :

$$n \ = \ 2^{\beta_2^n}(\prod_{p \in A_n} p^{\beta_p^n})(\prod_{p \in B_n} (p^2)^{\delta_p^n})$$

(en convenant qu'un produit sur l'ensemble vide vaut 1).
2 est somme de deux carrés d'entiers $(2 \ = \ (1^2 + 1^2))$, $p$ est somme de deux carrées d'entiers si $p$ appartient à $\mathbb{P}_1$ (cf question Q.3) et $p^2$ est bien sûr la somme de deux carrés d'entiers $(p^2 \ = \ (p^2 + 0^2))$.
De la question précédente (cf la remarque faite dans cette question), on déduit que $n$ est bien alors somme de deux carrées d'entiers.

Soit $n$ un entier non nul, différent de 1 et qui s'écrit comme la somme de deux carrés d'entiers .
On garde les notations de la question précédente. Soit $p$ appartenant à $B_n$ : il s'agit de montrer que $\beta_p^n$ est pair.