Entiers somme de deux carrés

L'objectif de ce problème est de déterminer quels sont les entiers naturels qui sont somme de deux carrés.

Notations :

$\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{C}$ désignent respectivement les ensembles des entiers naturels, des entiers relatifs et des nombres complexes.
On pose $\mathbb{Z}[i]=\{a+i.b\,/\,a\in\mathbb{Z},b\in\mathbb{Z}\}\subset\mathbb{C}$ et $\mathbb{Z}[i]^*=\mathbb{Z}[i]\setminus\{0\}$.
Pour $z\in\mathbb{C}$, on pose $N(z)=z\overline{z}$.

Partie I :Présentation de l'anneau de $\mathbb{Z}[i]$

1. Présentation de l'anneau $\mathbb{Z}[i]$.

1.a Vérifier que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ muni de l'addition et de la multiplication usuelles.

1.b Etablir que pour tout $u,v\in\mathbb{Z}[i]$, $N(uv)=N(u)N(v)$ et que pour tout $u\in\mathbb{Z}[i]$, $N(u)\in\mathbb{N}$.

1.c Un élément $u\in\mathbb{Z}[i]$ est dit inversible ssi il existe $v\in\mathbb{Z}[i]$ tel que $uv=1$.
Montrer que si u est inversible alors $N(u)=1$.
Déterminer alors l'ensemble, noté U, des éléments inversibles de $\mathbb{Z}[i]$.

2. Divisibilité dans l'anneau $\mathbb{Z}[i]$.
Soit $u,v\in\mathbb{Z}[i]$. On dit que u divise v dans $\mathbb{Z}[i]$, et on note $u\,|\,v$, ssi il existe $s\in\mathbb{Z}[i]$ tel que $v=su$.

2.a Soit $u,v,w\in\mathbb{Z}[i]$. Etablir l'implication que si $u\,|\,v$ et $v\,|\,w$ alors $u\,|\,w$.

2.b Soit $u,v\in\mathbb{Z}[i]$. Etablir que si $u\,|\,v$ et $v\,|\,u$ alors $u=\pm v$ ou $\pm iv$.

2.c Soit $u,v\in\mathbb{Z}[i]$. Montrer que si u divise v alors $N(u)$ divise $N(v)$ dans $\mathbb{Z}$.

2.d Déterminer les diviseurs de $1+i$, puis de $1+3i$ dans $\mathbb{Z}[i]$.

3. Division euclidienne dans $\mathbb{Z}[i]$.

3.a Montrer que pour tout $z\in\mathbb{C}$, il existe $u\in\mathbb{Z}[i]$ tel que $N(u-z)<1$.
Ce u est-il unique ?

3.b Montrer que pour tout $u\in\mathbb{Z}[i]$ et tout $v\in\mathbb{Z}[i]^*$, il existe $(q,r)\in\mathbb{Z}[i]\times\mathbb{Z}[i]$ tel que :
$u=vq+r$ avec $N(r)<N(v)$.
On pourra utiliser la division dans $\mathbb{C}$.

Partie II : Arithmétique dans $\mathbb{Z}[i]$

1. Soit $\delta\in\mathbb{Z}[i]$. On note $\delta.\mathbb{Z}[i]=\{\delta u\,/\,u\in\mathbb{Z}[i]\}$.
Montrer que $\delta.\mathbb{Z}[i]$ est un sous-groupe additif de $\mathbb{Z}[i]$.

2. Soit $u,v\in\mathbb{Z}[i]$ avec $u\neq 0$ ou $v\neq 0$. On note $I(u,v)=\{uz+vz'\,/\,z,z'\in\mathbb{Z}[i]\}$.

2.a Observer que u et v appartiennent à l'ensemble $I(u,v)$.

2.b Montrer que l'ensemble $A=\{N(w)\,/\,w\in I(u,v)\setminus\{0\}\}$ possède un plus petit élément $d>0$.

2.c Soit δ un élément de $I(u,v)$ tel que $N(\delta)=d$. Etablir que $I(u,v)=\delta.\mathbb{Z}[i]$.
On pourra exploiter la division euclidienne présentée en I.3b.

2.d Montrer que δ divise u et v puis que
pour tout $w \in \mathbb{Z}[i]$, on a l'équivalence : ($w \mid u$ et $w \mid v$) $\Leftrightarrow w \mid \delta$.
On dit que δ est un pgcd de u et v.

3. Soit $u, v \in \mathbb{Z}[i]$ avec $u \neq 0$ ou $v \neq 0$.
On dit que u et v sont premiers entre eux ssi le nombre δ défini en II.2.d appartient à $\{\pm 1, \pm i\}$.
Dans les questions 3.a et 3.b, on suppose que u et v sont premiers entre eux.

3.a Justifier qu'il existe $z, z' \in \mathbb{Z}[i]$ tel que $1 = uz + vz'$

3.b Soit $w \in \mathbb{Z}[i]$. Montrer que si u divise vw alors u divise w.

4. Soit $u \in \mathbb{Z}[i] - \{0, \pm 1, \pm i\}$.
On dit que u est irréductible ssi ses seuls diviseurs sont $\pm 1, \pm i, \pm u$ et $\pm iu$.

4.a Soit $v \in \mathbb{Z}[i]$. On suppose que u irréductible et ne divise pas v.
Montrer que u et v sont premiers entre eux.

4.b Soit $v, w \in \mathbb{Z}[i]$. On suppose que u est irréductible et divise vw.
Montrer que u divise v ou divise w.

Partie III : Nombres somme de deux carrés

1. On note $\Sigma = \{a^2 + b^2 / a \in \mathbb{Z}, b \in \mathbb{Z}\}$.

1.a Montrer que $n \in \Sigma \Leftrightarrow \exists u \in \mathbb{Z}[i], n = N(u)$.

1.b En déduire que si $n, n' \in \Sigma$ alors $nn' \in \Sigma$.

2. p désigne un nombre premier strictement supérieur à 2.

2.a Montrer que $p \in \Sigma \Rightarrow p \equiv 1$ modulo 4.
Nous admettrons que l'implication réciproque est vraie (quoique loin d'être immédiate).
Ainsi $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$,... sont des éléments de Σ.

2.b Montrer que si p n'est par irréductible alors $p \in \Sigma$.

3. Soit $a, b \in \mathbb{Z}$ et $n = a^2 + b^2 \in \Sigma$. Soit $p \equiv 3$ modulo 4, un nombre premier diviseur de n.

3.a Montrer que $p \mid a + i.b$ dans $\mathbb{Z}[i]$.

3.b En déduire que p^2 divise n.

4. Etablir que les entiers naturels non nuls appartenant à Σ sont les nombres de la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_N^{\alpha_N}$
avec $p_1, p_2, \ldots, p_N$ nombres premiers deux à deux distincts et $\alpha_1, \alpha_2, \ldots, \alpha_N$ entiers naturels tels que :
$\forall 1 \leq i \leq N$, $p_i \equiv 3$ modulo 4 $\Rightarrow \alpha_i$ est pair.