Correction

Partie I

1.a $\mathbb{Z}[i]\subset\mathbb{C}$, $1=1+0.i\in\mathbb{Z}[i]$ et $\forall u,v\in\mathbb{Z}[i]$, on peut écrire $u=a+ib$, $v=c+id$ avec $a,b,c,d\in\mathbb{Z}$

On a $u-v=(a-c)+i(b-d)\in\mathbb{Z}[i]$ (car $a-c,b-d\in\mathbb{Z}$),

et $uv=(ac-bd)+i(ad+bc)\in\mathbb{Z}[i]$ car $ac-bd,ad+bc\in\mathbb{Z}$.

Ainsi $\mathbb{Z}[i]$ est un sous anneau de $(\mathbb{C},+,\times)$.

1.b $\forall u,v\in\mathbb{Z}[i]$, $N(uv)=uv\overline{uv}=u\overline{u}v\overline{v}=N(u)N(v)$

$\forall u\in\mathbb{Z}[i]$, on peut écrire $u=a+ib$ avec $a,b\in\mathbb{Z}$ donc $N(u)=u\overline{u}=a^2+b^2\in\mathbb{N}$.

1.c Supposons $u\in\mathbb{Z}[i]$ inversible et introduisons $v\in\mathbb{Z}[i]$ tel que $uv=1$.

On a $N(uv)=N(1)=1$ et $N(uv)=N(u)N(v)$ donc $N(u)N(v)=1$ avec $N(u),N(v)\in\mathbb{N}$.

Par suite $N(u)=N(v)=1$.

On peut écrire $u=a+ib$ avec $a,b\in\mathbb{Z}$.

$N(u)=a^2+b^2=1$ donne $(a,b)=(1,0),(-1,0),(0,1)$ ou $(0,-1)$ donc $u=\pm1$ ou $u=\pm i$.

Inversement, ses éléments sont inversibles car $1\times1=1$, $(-1)\times(-1)=1$, $i\times(-i)=1$ et $(-i)\times i=1$.

$U=\{1,i,-1,-i\}$.

2.a Si $u\mid v$ et $v\mid w$ alors il existe $s,t\in\mathbb{Z}[i]$ tel que $v=su$ et $w=tv$.

On a alors $w=(st)u$ avec $st\in\mathbb{Z}[i]$ et par suite $u\mid w$.

2.b Si $u\mid v$ et $v\mid u$ alors il existe $s,t\in\mathbb{Z}[i]$ tel que $v=su$ et $u=tv$.

Par suite $u=(ts)u$.

Si $u\neq0$, on obtient $ts=1$ donc t est inversible et alors $t=\pm1$ ou $t=\pm i$.

Par suite $u=\pm v$ ou $u=\pm iv$.

Si $u=0$ alors $v=su=u$ et donc $u=v$.

2.c Si $u\mid v$ alors il existe $s\in\mathbb{Z}[i]$ tel que $v=su$. On a alors $N(v)=N(su)=N(s)N(u)$ avec $N(s)\in\mathbb{N}$

donc $N(u)\mid N(v)$.

2.d $N(1+i)=2$ et $\mathrm{Div}(2)\cap\mathbb{N}=\{1,2\}$.

Si u divise $1+i$ alors $N(u)=1$ ou $N(u)=2$.

Si $N(u)=1$ alors $u=\pm1$ ou $u=\pm i$.

Si $N(u)=2$ alors $u=1+i,1-i,-1+i$ ou $-1-i$.

Inversement, les nombres proposés sont diviseurs de $1+i$.

$N(1+3i)=10$ et $\mathrm{Div}(10)\cap\mathbb{N}=\{1,2,5,10\}$.

Si $N(u)=1$ alors $u=\pm1$ ou $u=\pm i$.

Si $N(u)=2$ alors $u=1+i,1-i,-1+i$ ou $-1-i$.

Si $N(u)=5$ alors $u=1+2i,1-2i,-2+i$ ou $-2-i$.

Si $N(u)=10$ alors $u=1+3i,1-3i,-3+i$ ou $-3-i$.

Inversement, les nombres proposés sont diviseurs de $1+3i$.

3.a Soit a et b les entiers respectivement les plus proches de $\mathrm{Re}(z)$ et $\mathrm{Im}(z)$.

Pour $u=a+i.b\in\mathbb{Z}[i]$, on a $N(u-v)=(a-\mathrm{Re}(z))^2+(b-\mathrm{Im}\,z)^2\leq\dfrac{1}{4}+\dfrac{1}{4}\leq\dfrac{1}{2}<1$.

Il n'y a pas unicité de u. Par exemple, pour $z=\dfrac{1+i}{2}$, les quatre complexes $0,1,i$ et $1+i$ conviennent.

3.b Soit $q \in \mathbb{Z}[i]$ tel que $N\left(q-\frac{u}{v}\right)<1$ et $r=u-vq \in \mathbb{Z}[i]$.

On a $u=vq+r$ et $N(r)=N(u-vq)=N(v)N\left(\frac{u}{v}-q\right)<N(v)$ (sachant $N(v)>0$).

Partie II

1. $\delta.\mathbb{Z}[i] \subset \mathbb{Z}[i]$. $0=\delta.0 \in \delta.\mathbb{Z}[i]$. $\forall x,y \in \delta.\mathbb{Z}[i]$, on peut écrire $x=\delta.u$ et $y=\delta.v$ avec $u,v \in \mathbb{Z}[i]$.
On a $x-y=\delta.(u-v) \in \delta.\mathbb{Z}[i]$ car $u-v \in \mathbb{Z}[i]$. Ainsi $\delta.\mathbb{Z}[i]$ est un sous groupe de $(\mathbb{Z}[i],+)$.

2.a $u=u.1+v.0 \in I(u,v)$ et $v=u.0+v.1 \in I(u,v)$.

2.b $A=\{N(w)/w \in I(u,v)\setminus\{0\}\}$ est une partie de $\mathbb{Z}$, minorée par 1 et non vide car $N(u)$ ou $N(v)$ appartient à cet ensemble (selon que $u \neq 0$ ou $v \neq 0$). Par suite A possède un plus petit élément $d>0$.

2.c $\delta \in I(u,v)$ donc on peut écrire $\delta=u\xi+v\xi'$ avec $\xi,\xi' \in \mathbb{Z}[i]$.
$\forall x \in \delta.\mathbb{Z}[i]$, on peut écrire $x=\delta y$ avec $y \in \mathbb{Z}[i]$.
On a alors $x=u(\delta\xi)+v(\delta\xi') \in I(u,v)$. Ainsi $\delta.\mathbb{Z}[i] \subset I(u,v)$.
Inversement, soit $x \in I(u,v)$. On peut écrire $x=uz+vz'$ avec $z,z' \in \mathbb{Z}[i]$
Réalisons la division euclidienne de x par δ : $x=\delta q+r$ avec $N(r)<N(\delta)$.
Or $r=x-\delta q=u(z-\xi q)+v(z'-\xi' q) \in I(u,v)$ donc si $r \neq 0$, on a $N(r) \in A$. Ceci contredit la définition de $d=\min A$ car $N(r)<N(\delta)=d$. Nécessairement $r=0$ et par suite $x \in \delta.\mathbb{Z}[i]$.

2.d $u \in I(u,v)=\delta.\mathbb{Z}[i]$ donc on peut écrire $u=\delta.z$ avec $z \in \mathbb{Z}[i]$. Ainsi $\delta \mid u$. De même $\delta \mid v$.
Si $w \mid \delta$ alors $w \mid u$ et $w \mid v$ par transitivité de la divisibilité.
Inversement si $w \mid u$ et $w \mid v$ alors on peut écrire $u=ws$ et $v=wt$ avec $s,t \in \mathbb{Z}[i]$ et donc l'écriture $\delta=u\xi+v\xi'$ avec $\xi,\xi' \in \mathbb{Z}[i]$ introduite ci-dessus donne $\delta=w(s\xi+t\xi')$. Ainsi $w \mid \delta$.

3.a $I(u,v)=\delta.\mathbb{Z}[i]=\mathbb{Z}[i]$ car $\delta \in \{\pm 1, \pm i\}$.
Or $1 \in \mathbb{Z}[i]$ donc $1 \in I(u,v)$ et par suite $\exists z,z' \in \mathbb{Z}[i]$ tels que $1=uz+vz'$.

3.b Supposons $u \mid vw$. On a $w=w\times 1=uwz+vwz'$, or $u \mid uwz$ et $u \mid vwz'$ donc sans difficultés $u \mid w$.

4.a Posons δ un pgcd de u et v. δ est un diviseur de l'élément irréductible u.
Si $\delta=\pm u$ ou $\delta=\pm iu$ alors, puisque $\delta \mid v$, $u \mid v$. Ceci est exclu.
Il reste $\delta=\pm 1$ ou $\delta=\pm i$ et donc u et v sont premiers entre eux.

4.b Si u divise v : ok
Sinon, u est premier avec v et donc puisque $u \mid vw$ on a $u \mid w$ en vertu de II.3b.

Partie III

1.a Si $n \in \Sigma$ alors on peut écrire $n=a^2+b^2$ avec $a,b \in \mathbb{Z}$ et alors $n=N(u)$ avec $u=a+i.b \in \mathbb{Z}[i]$.
Inversement, si $n=N(u)$ avec $u \in \mathbb{Z}[i]$, alors on peut écrire $u=a+i.b$ avec $a,b \in \mathbb{Z}$ et on a $N(u)=a^2+b^2 \in \Sigma$.

1.b Si $n,n' \in \Sigma$ alors on peut écrire $n=N(u)$ et $n'=N(v)$ avec $u,v \in \mathbb{Z}[i]$.
On a alors $nn'=N(u)N(v)=N(uv)$ avec $uv \in \mathbb{Z}[i]$ donc $nn' \in \Sigma$.

2.a Puisque p est premier et strictement supérieur à 2, il n'est pas divisible par 2.
Par suite $p \equiv 1$ ou $p \equiv 3$ modulo 4.
Puisque $p \in \Sigma$, on peut écrire $p=a^2+b^2$ avec $a,b \in \mathbb{Z}$.
Or les seuls valeurs possibles de a^2 modulo 4 sont 0 ou 1 donc $p=0$, 1 ou 2 modulo 4.
Compte tenu de ce qui précède, il reste $p=1$ modulo 4.

2.b Si p n'est par irréductible alors on peut écrire $p = uv$ avec $u,v \in \mathbb{Z}[i] \setminus \{\pm 1, \pm i\}$.

On a alors $p^2 = N(p) = N(u)N(v)$. Puisque $N(u) \neq 1$, $N(v) \neq 1$ et p premier, on a $N(u) = N(v) = p$ et donc $p \in \Sigma$.

3.a Puisque $p \equiv 3$ modulo 4, p n'appartient pas à Σ (via III.2a) et donc p est irréductible (via III.2b)

On a $p \mid a^2 + b^2 = (a + i.b)(a - ib)$ or p est irréductible donc $p \mid (a + ib)$ ou $p \mid (a - ib)$.

Or il est clair que $p \mid z \Rightarrow p \mid \overline{z}$, donc $p \mid (a + ib)$ et $p \mid (a - ib)$.

3.b Suite a ce qui précède $p^2 \mid (a + ib)(a - ib) = n$.

Cette dernière divisibilité a lieu a priori dans $\mathbb{Z}[i]$, mais puisque n/p^2 est le rapport de deux entiers, sera un entier et donc la divisibilité a lieu dans $\mathbb{Z}$.

4. Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_N^{\alpha_N}$ de la forme proposée. $\forall 1 \leq i \leq N$:

Si $p_i = 2$ ou $p_i \equiv 1$ modulo 4 alors $p_i \in \Sigma$ (car $2 = 1^2 + 1^2$ et par la réciproque admise en III.2a)

Par suite $p_i^{\alpha_i} \in \Sigma$ car Σ est stable par produit (III.1.b)

Si $p_i \equiv 3$ modulo 4 alors $\alpha_i = 2\beta_i$ et $p_i^{\alpha_i} = p_i^{2\beta_i} = (p_i^2)^{\beta_i} \in \Sigma$ car $p_i^2 = p_i^2 + 0^2 \in \Sigma$.

Puisque tous les $p_1^{\alpha_1}, \ldots, p_N^{\alpha_N}$ appartiennent à Σ, $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_N^{\alpha_N}$ appartient à Σ.

Inversement : Soit $n \in \Sigma \cap \mathbb{N}^*$. Si $n = 1$, n est de la forme voulue.

Si $n \geq 2$, introduisons sa décomposition primaire $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_N^{\alpha_N}$.

Pour tout $1 \leq i \leq N$ tel que $p_i \equiv 3$ modulo 4.

Si $\alpha_i = 0$ alors α_i est pair.

Si $\alpha_i > 0$ alors $p_i \mid n$. Ecrivons $n = a^2 + b^2$ avec $a, b \in \mathbb{Z}$.

Comme vu en III.3a, on a $p_i \mid (a + ib)$ ce qui permet d'écrire $a + ib = p_i(c + id)$.

On a alors $n = p_i^2(c^2 + d^2) = p_i^2 n'$ avec $n' = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i - 2} \ldots p_N^{\alpha_N} \in \Sigma$.

On peut alors reprendre la démarche avec n' et, champagne !, α_i est pair.