CPGE MPSI
2016-2017

Le 03.12.16

Devoir Surveillé n°4
CORRECTION

Exercice 1

Pour l'ensemble de cet exercice, on note $c = \cos 1$ et $s = \sin a$.
On considère les suites (u_n) définie par récurrence par :

$$\forall\ n \in \mathbb{N}, u_{n+2} = 2c \times u_{n+1} - u_n$$

ainsi que deux conditions initiales ($u_0 = \dots$, $u_1 = \dots$), non précisées pour le moment.

1. Nous reconnaissons une suite récurrente linéaire d'ordre 2 à coefficients constants et homogène.
   L'équation caractéristique associée est

   $$x^2 - 2cx + 1 = 0$$

   Son discriminant est $\Delta = 4c^2 - 4 = -4s^2$, et les racines sont complexes : $r_1 = c + is = e^i$ et $r_1 = c - is = e^{-i}$.
   On peut donc affirmer : /1

   il existe λ et $\mu \in \mathbb{R}$ tel que pour tout $n \in \mathbb{N}$, $u_n = \lambda \cos n + \mu \sin n$

2. On voit bien que (v_n) et (w_n) sont des solutions avec $\lambda = 1$ et $\mu = 0$ ou $\lambda = 0$ et $\mu = 1$, respectivement.
   Mais pour réfléchir aux conditions initiales, il suffit tout simplement de calculer les valeurs initiales de ces deux suites, par unicité de la suite définies par une relation de récurrence linéaire homogène) de degré 2 et deux conditions initiales, on peut affirmer que /1

   (v_n) est parfaitement définie par $v_0 = 1$, $v_1 = \cos 1 = c$ et $\forall\ n \in \mathbb{N}$, $v_{n+2} = 2c \times v_{n+1} - v_n$
   (w_n) est parfaitement définie par $w_0 = 0$, $w_1 = \sin 1 = s$ et $\forall\ n \in \mathbb{N}$, $w_{n+2} = 2c \times w_{n+1} - w_n$

3. On suppose que (v_n) converge vers ℓ.
   (a) Alors les suites extraites (v_{n+2}) et (v_{n+1}) convergeraient également vers ℓ.
   Et donc la suite (x_n) définie par : $\forall\ n \in \mathbb{N}$, $x_n = v_{n+2} - 2c \times v_{n+1} + v_n$
   convergerait vers $2(1-c)\ell$.
   Or cette suite est nulle, donc par unicité de la limite : $2(1-c)\ell = 0$, donc $\ell = 0$. /1

   Dans ce cas (v_n) converge nécessairement vers $\ell = 0$

   (b) On a pour tout $n \in \mathbb{N}$: $v_{2n} = \cos(2n) = \cos^2 n - \sin^2 n = v_n^2 - w_n^2$, donc $w_n^2 = v_n^2 - v_{2n}$.
   Or la suite (v_n) tend vers 0 et donc la suite extraite (v_{2n}) également. /1

   Par soustraction (w_n^2) converge également vers 0

   (c) On a donc $(1) = (v_n^2 + w_n^2)$ qui converge vers 0 (par addition de limite).
   Cela est contradictoire. /0,5

   Donc (v_n) diverge.

4. Supposons que (w_n) converge vers ℓ.
   Alors comme pour tout $n \in \mathbb{N}$, $w_{n+2} - 2cw_n + w_n = 0$,
   on a donc, là aussi, $2(1-c)\ell = 0$ et donc $\ell = 0$.
   Puis $w_{n+1} = \sin(n+1) = \cos(n)\sin(1) + \sin(n)\cos(1) = sv_n + cw_n$,
   et donc (v_n) tend aussi vers 0 ($s \neq 0$).
   Et encore $(1) = (v_n^2 + w_n^2)$ qui converge vers 0 (par addition de limite).
   On a donc une contradiction $(1 = 0)$, /2

   Donc (w_n) diverge.

5. La suite (v_n) est bornée : $\forall\, n \in \mathbb{N},\ |v_n| \leqslant 1$.
Donc, */0,5*

d'après le théorème de Bolzano-Weierstrass, on peut extraire de (v_n) une suite convergente.

6. $(*)$ Soit $\ell \in [-1,1]$. Soit $\epsilon > 0$.
Il suffit de montrer qu'il y a une infinité de terme de la suite (v_n) dans $]\ell-\epsilon, \ell+\epsilon[$.
(on pourrait alors construire, terme après terme une extraction φ comme fait au DM4).
Soit $\theta = \arccos \ell$. D'après l'inégalité des accroissements finis,

$$|\cos(m+2k\pi) - \cos\theta| = |\cos m - \cos\theta| < 1 \times |m-\theta|$$

Donc si $|m-\theta| < \epsilon$, alors $\cos m \in]\ell-\epsilon, \ell+\epsilon[$.
Ainsi, la question qui se pose est : existe-t-il une infinité de $n, k \in \mathbb{Z}$ tels que $n - 2k\pi \in]\theta-\epsilon, \theta+\epsilon[$?
$E = \{n + 2k\pi ; n, k \in \mathbb{Z}\}$. Si on montre que E est dense dans $\mathbb{R}$, c'est gagné.
Soit $a = \inf(E \cap \mathbb{R}_+)$.
— Si $a > 0$,
si $a \notin E$, on construit une suite $(a_n) \in E^{\mathbb{N}}$, décroissante telle que $\lim(a_n) = a$.
On a alors $a_n - a_{n+1} \in E \cap \mathbb{R}_+$ et donc $\lim(a_n - a_{n+1}) \geqslant \inf E$, donc $a \leqslant 0$.
C'est impossible, on en déduit que $a \in E$ et dans difficulté que $a\mathbb{Z} \subset E$.
Et si $b \in E$, notons $p = \lfloor \frac{b}{a} \rfloor$, et donc $b = pa + q$ avec $0 \leqslant q < a$.
On a donc $q \in E$, et par définition de a, nécessairement : $q = 0$ donc $b = ap$ et $E \subset a\mathbb{Z}$.
Par double inclusion : $a\mathbb{Z} = E$. Enfin, comme $\pi \in E$, il existe $n \in \mathbb{Z}$ tel que $\pi = na$.
De même $1 \in E$, il existe $m \in \mathbb{Z}$ tel que $1 = ma$.
Donc $\pi = \frac{n}{m}$, ce qui est absurde.
— Donc $a = 0$. Et donc il est impossible d'avoir un intervalle $]x-\epsilon, x+\epsilon[\cap E = \emptyset$
Bilan : */3*

Pour tout $\ell \in [-1,1]$, on peut trouver $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante telle que $(v_{\varphi(n)})$ converge vers ℓ

Problème

A. Interprétation géométrique de la divisibilité dans $\mathbb{Z}[i]$

Soit $z_0 = a_0 + ib_0 \in \mathbb{Z}[i]$. On note $\varphi_0 : \mathbb{C} \to \mathbb{C}$, $z \mapsto z_0 \times z$

1. C'est une question de cours :

φ_0 est une similitude, centrée en O, de rapport $\lvert z_0\rvert = \sqrt{a^2+b^2}$ et d'angle $\arg(z_0) = \arctan(\frac{b}{a})$

On a tout simplement : */0,5*

$\varphi_0(1) = z_0 = a_0 + ib_0$

2. Ces résultats sont vrais pour toutes les similitude.
Un angle droit (en A) est donné par trois points A, B, C, tels que $\arg(\overrightarrow{AB}, \overrightarrow{AC}) \equiv \pm\frac{\pi}{2}[\pi]$.
Notons m l'affixe de M, on a donc $\arg(\overrightarrow{AB}, \overrightarrow{AC}) = \arg(\frac{c-a}{b-a}) \equiv \pm\frac{\pi}{2}[\pi] \Leftrightarrow \dfrac{c-a}{b-a} \in i\mathbb{R}$. Et

$$\frac{\varphi_0(c)-\varphi_0(a)}{\varphi_0(c)-\varphi_0(a)} = \frac{z_0(c-a)}{z_0(b-a)} = \frac{c-a}{b-a} \in i\mathbb{R}$$

Ce résultat numérique signifie exactement */0,5*

φ_0 conserve les angles droits.

De même considérons que A, B et C sont alignés, donc $\arg(\overrightarrow{AB}, \overrightarrow{AC}) \equiv 0[\pi]$.
On a donc $\arg(\overrightarrow{AB}, \overrightarrow{AC}) = \arg(\frac{c-a}{b-a}) \equiv 0[\pi] \Leftrightarrow \dfrac{c-a}{b-a} \in \mathbb{R}$. Et

$$\frac{\varphi_0(c)-\varphi_0(a)}{\varphi_0(c)-\varphi_0(a)} = \frac{z_0(c-a)}{z_0(b-a)} = \frac{c-a}{b-a} \in \mathbb{R}$$

Ce résultat numérique signifie exactement */0,5*

φ_0 conserve les alignements.

3. On a vu que φ_0 conserve les angles droits et les alignements.
Donc un carré est transformé par φ_0 en un quadrilatère avec 4 angles droits, c'est-à-dire, au moins un rectangle.
Notons qu'en plus il conserve les proportions, ce qui assurera que ce rectangle est un carré.
Supposons $AB = CD$, alors

$$\left\| \frac{\overrightarrow{\varphi_0(A)\varphi_0(B)}}{\overrightarrow{\varphi_0(C)\varphi_0(D)}} \right\| = \left| \frac{\varphi_0(b) - \varphi_0(a)}{\varphi_0(d) - \varphi_0(c)} \right| = \frac{|z_0||b-a|}{|z_0||d-c|} = \left\| \frac{\overrightarrow{AB}}{\overrightarrow{CD}} \right\| = 1$$

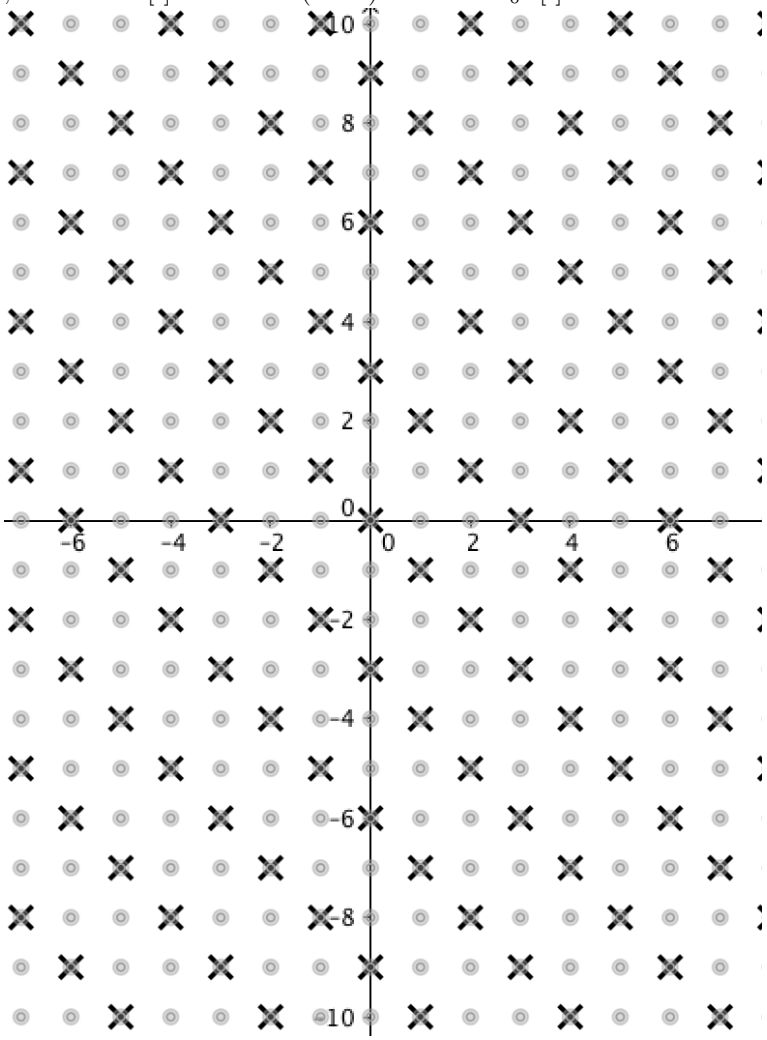
Par conséquent :

$\boxed{\varphi_0 \text{ tranforme les carrés en carrés (mais de longueur « agrandit » d'un facteur } |z_0|).}$

On a vu que l'image de 0, c'est 0 et celle de 1 est z_0.
Donc l'image par φ_0 du carré $ABCD$ est /1

$\boxed{\text{le carré } A'B'C'D',\ A'(0),\ B'(a+ib),\ C'(a-b+i(a+b)) \text{ et } D'(-b+ia)}$

4. En gris, le réseau $\mathbb{Z}[i]$ et en noir (croix) le réseau $z_0\mathbb{Z}[i]$.



/0,5

B. L'anneau des entiers de Gauss

On note $\mathbb{Z}[i] = \{a + ib; a, b \in \mathbb{Z}\}$. On appelle cet ensemble, l'anneau des entiers de Gauss.
On peut donc écrire :

$$z \in \mathbb{Z}[i] \iff \exists\ a, b \in \mathbb{Z} \text{ tels que } x = a + ib$$

1. Soient $z = a + ib$ et $z' = a' + ib' \in \mathbb{Z}[i]$.
Alors $\overline{z} = a - ib \in \mathbb{Z}[i]$, $z + z' = (a + a') + i(b + b') \in \mathbb{Z}[i]$,
et $zz' = (aa' - bb') + i(ab' + a'b) \in \mathbb{Z}[i]$ car $\mathbb{Z}$ est lui-même un anneau.
Donc /0,5

$\boxed{\text{si } z, z' \in \mathbb{Z}[i], \text{ alors } \overline{z},\ z + z' \text{ et } z \times z' \in \mathbb{Z}[i]}$

La stabilité de $\mathbb{Z}[i]$ assuré par ces deux dernières opérations explique ce nom d'anneau.

2. On note $N : \mathbb{Z}[i] \to \mathbb{N}, z \mapsto z\overline{z}$.
Pour tout $z = a + ib \in \mathbb{Z}[i]$, on a $N(z) = |z|^2 = a^2 + b^2 \in \mathbb{N}$. Donc /0,5

$$\boxed{N(\mathbb{Z}[i]) \subset \mathbb{N}}$$

3. Soient $z, z' \in \mathbb{Z}[i]$, alors, par propriété bien connue du module :

$$N(zz') = |zz'|^2 = (|z| \times |z'|)^2 = |z|^2 \times |z'|^2 = N(z)N(z')$$

Ainsi /1

$$\boxed{\forall\, z, z' \in \mathbb{Z}[i], \quad N(zz') = N(z)N(z')}$$

4. On note $\mathbb{Z}[i]^*$, l'ensemble des éléments inversibles de $\mathbb{Z}[i]$ et dont l'inverse est dans $\mathbb{Z}[i]$.
Autrement écrit : $\mathbb{Z}[i] = \{z \in \mathbb{Z}[i] \mid \exists\ z' \in \mathbb{Z}[i], z \times z' = 1\}$.
   (a) Soit $z \in \mathbb{Z}[i]^*$. Donc il existe $z' \in \mathbb{Z}[i]$ tel que $z \times z' = 1$.
   Donc $N(zz') = N(1) = 1 = N(z)N(z')$.
   Or $N(z), N(z') \in \mathbb{N}$. Si $N(z) \neq 1$, alors $N(z')$ serait une fraction irréductible $\frac{1}{N(z)}$.
   Par conséquent $N(z) = 1$.
   Réciproquement, supposons que $N(z) = 1$.
   Alors si $z = a + ib$, on a ($a = 0$ et $|b| = 1$) ou ($|a| = 1$ et $b = 0$).
   On obtient quatre nombres : i, $-i$, 1 et -1.
   Tous les quatre sont inversibles dans $\mathbb{Z}[i]$, en effet : $i^{-1} = -i$, $(-i)^{-1} = i$, $1^{-1} = 1$ et $(-1)^{-1} = -1$. /1

$$\boxed{\text{Par double inclusion, } \mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid N(z) = 1\}}$$

   (b) On a déjà répondu à cette question /0,5

$$\boxed{\mathbb{Z}[i]^* = \{1, -1, i, -1\}}$$

5. Dans cette question, nous allons montrer que $\mathbb{Z}[i]$ est un anneau euclidien.
Autrement écrit, il existe « une »(sorte) de division euclidienne sur $\mathbb{Z}[i]$.
   (a) Soit $s = x + iy \in \mathbb{C}$.
   — Notons a, l'entier le plus proche de x :
   $a = \lfloor x \rfloor$ si $x - \lfloor x \rfloor < \frac{1}{2}$ et $a = \lfloor x \rfloor + 1$ si $x - \lfloor x \rfloor \geqslant \frac{1}{2}$, donc $|x - a| \leqslant \frac{1}{2}$
   — Notons b, l'entier le plus proche de y :
   $b = \lfloor y \rfloor$ si $y - \lfloor y \rfloor < \frac{1}{2}$ et $b = \lfloor y \rfloor + 1$ si $y - \lfloor y \rfloor \geqslant \frac{1}{2}$, donc $|y - b| \leqslant \frac{1}{2}$
   On considère alors $z = a + ib$
   donc $|z - s|^2 = |(x - a) + i(y - b)|^2 = (x - a)^2 + (y - b)^2 \leqslant \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$.
   Donc en prenant la racine carrée : /1

$$\boxed{\text{il existe } z \in \mathbb{Z}[i] \text{ tel que } |z - s| \leqslant \frac{\sqrt{2}}{2}.}$$

   (b) Soient $x, y \in \mathbb{Z}[i]$.
   On considère $s = \dfrac{x}{y} \in \mathbb{C}$.
   Alors, d'après la question précédente, il existe $q \in \mathbb{Z}[i]$ tel que $|q - s| \leqslant \dfrac{\sqrt{2}}{2}$ En multipliant tout par y : $|qy - x| = |qy - sy| \leqslant \dfrac{\sqrt{2}}{2}|y|$. Notons donc $r = x - qy$. Comme $q, y \in \mathbb{Z}[i]$, alors $qy \in \mathbb{Z}[i]$ et donc $r \in \mathbb{Z}[i]$.
   Puis $N(r) = |r|^2 \leqslant \left(\dfrac{\sqrt{2}}{2}|y|\right)^2 = \dfrac{1}{2}N(y)$. Ainsi /1

$$\boxed{\forall\, x, y \in \mathbb{Z}[i], \exists\ (q, r) \in \mathbb{Z}[i] \text{ tel que } x = qy + r \text{ avec } 0 \leqslant N(r) < N(y)}$$

   On dit que $\mathbb{Z}[i]$ est muni d'une division euclidienne, ou que $\mathbb{Z}[i]$ est un anneau euclidien.
   (c) On note

$$s = \frac{3 + 2i}{1 - i} = \frac{1}{2}(3 + 2i)(1 + i) = \frac{(3 - 2) + i(3 + 2)}{2} = \frac{1}{2} + i\frac{5}{2} = 2i + \frac{1}{2}(1 + i)$$

On a donc « choisi »(par exemple) comme quotient.
Et donc, comme $(1+i)(1-i)=2$, /0,5

$$\boxed{3+2i=\underbrace{2i}_{q}(1-i)+\underbrace{1}_{r} \text{ on a bien } N(r)=N(1)=1<N(1-i)=2}$$

On aurait pu choisir également :

$$3+2i=\underbrace{3i}_{q}(1-i)+\underbrace{-i}_{q}=\underbrace{1+2i}_{q}(1-i)+\underbrace{i}_{q}=\underbrace{1+3i}_{q}(1-i)+\underbrace{-1}_{q}$$

On voit que les restes sont exactement les éléments de $\mathbb{Z}[i]^*$.

Culture et curiosité :
On peut alors construire, un algorithme d'Euclide adapté aux entiers de Gauss.
Cela conduit à une suite de division euclidienne avec une suite d'entiers $(N(r_k))_k$ strictement décroissante. Donc elle s'annule à partir d'un certain rang. Le dernier reste non nul sera appelé le PGCD des deux entiers de Gauss initiaux (en fait, la non unicité de la division euclidienne est légèrement problématique. Elle conduit à 4 PGCD différents possibles, mais ceux-ci sont exactement les mêmes à multiplication par inversible près. On « quotiente par les classes d'équivalence »).
On retrouve alors également le théorème de Bézout et tutti quanti...

6. On dit que $p\in\mathbb{Z}[i]$ est i-premier si
— p n'est pas inversible
— si, pour tout $a,b\in\mathbb{Z}[i]$, $p=ab$, alors a est inversible ou b est inversible

   (a) Pour $\mathbb{N}$, le nombre inversible est unique et c'est exactement 1.
   On aurait alors p de $\mathbb{N}$ est premier, si $p\neq 1$ et si $ab=p$ alors $a=1$ (et donc $b=p$) ou $b=1$ (et $a=p$). /0,5

   On retrouve la même définition.

   (b) Nous allons faire un raisonnement par contraposé.
   Si p n'est pas premier, il existe a et $b\in\mathbb{Z}[i]$, tout deux non inversibles tels que $p=ab$.
   Donc $N(p)=N(a)N(b)$. Or a et b ne sont pas inversibles, donc $N(a)>1$ et $N(b)>1$.
   Et par conséquent, $N(p)$ est nécessairement pas premier.
   Par contraposée : /1

   si $N(p)$ est premier alors p est nécessairement i-premier.

   Considérons $x=1+i$. Si $z=a+ib$ divise x, on suppose $x=zz'$.
   Alors $N(z)N(z')=N(x)=2$. Donc $N(z)=2$ et $N(z')=1$ ou $N(z)=1$.
   Par conséquent z ou z' est inversible et donc

   $x=1+i$ est i-premier

   (c) Avec $p=3\in\mathbb{Z}[i]$, on a donc $N(p)=9$, qui n'est pas un nombre premier.
   Alors que si $zz'=3$, on a $N(z)N(z')=N(3)=9$.
   Donc ou bien $N(z)=1$ ou $N(z')=1$ et 3 est i-premier, ou bien $N(z)=N(z')=3$.
   Dans ce second cas, on a pour $z=a+ib$, $N(z)=3=a^2+b^2$, donc $|a|<2$ et $|b|<2$.
   Si $|a|=1$, alors $b=\pm\sqrt{2}$, c'est impossible, de même pour $a=0$.
   Ainsi, /1

   p est i-premier, alors que $N(p)$ n'est pas premier.

   (d) Soit p un nombre i-premier. Soient $a,b\in\mathbb{Z}[i]$.
   On suppose que $p|a\times b$. Si $p|a$, alors on a obtenu ce qu'il fallait démontrer.
   Supposons donc que p ne divise pas a.
   En appliquant l'algorithme d'Euclide à a et p, on obtient une suite de reste (r_k) dont la norme $N(r_k)$ est strictement entière à valeurs décroissantes.
   Elle est nulle à partir d'un certain rang $N+1$.
   On a alors en remontant l'algorithme :
— $r_N\neq 0$
— $r_N|p$ et $r_N|a$. Comme p est i-premier, $r_N\in\mathbb{Z}[i]^*$
— $\forall\ k\in\mathbb{N}$, $\exists\ u_k,v_k\in\mathbb{Z}[i]$ tels que $r_k=u_kp+v_ka$.

En particulier $\exists\ u_N, v_N \in \mathbb{Z}[i]$ tel que $r_N = u_N p + v_N a$.
Puis p est un diviseur de ab et de pb.
Donc il existe $z \in \mathbb{Z}[i]$, $b = r_N^{-1} \times ((u_N pb) + v_N ab) = p \times z$. Donc p divise b. */2*

On a donc montré que, pour tout $a, b \in \mathbb{Z}[i]$, $p|a \times b \Longrightarrow p|a$ ou $p|b$ *(Lemme de Gauss)*

(e) Comme nous y sommes invités, nous faisons la démonstration en deux temps (ce sont presqu'exactement les mêmes démonstrations que dans le cours sur $\mathbb{Z}$).
Faisons la démonstration par récurrence (forte).
Pour tout $n \in \mathbb{N}$, $n \geqslant 2$, $\mathcal{P}_n$: « tout $z \in \mathbb{Z}[i]$ tel que $2 \leqslant N(z) \leqslant n$ est divisible par un nombre i-premier. »
— Soit $z \in \mathbb{Z}[i]$ tel que $N(z) = 2$.
Comme $N(z)$ est premier, z est nécessairement i-premier.
Donc il est divisible par un nombre i-premier (lui-même).
Ainsi $\mathcal{P}_2$ st vérifiée.
— Soit $n \geqslant 2$. Supposons que $\mathcal{P}_n$ est vraie.
Soit $z \in \mathbb{Z}[i]$ tel que $N(z) \leqslant n+1$.
Si $N(z) \leqslant n$, alors d'après $\mathcal{P}_n$ qui est vraie, n est divisible par un nombre i-premier.
Supposons maintenant que $N(z) = n+1$.
Soit z est i-premier, il est alors divisible par un nombre i-premier (lui-même).
Soit z n'est pas i-premier, il existe $z_1, z_2 \in \mathbb{Z}[i]$ non inversibles tels que $z = z_1 z_2$.
On a donc $N(z_1) \geqslant 2$ et $N(z_2) \geqslant 2$, donc $2 \leqslant N(z_1) \leqslant \frac{n+1}{2} \leqslant n$.
D'après $\mathcal{P}_n$, il existe a i-premier qui divise z_1. Alors a divise également z.
Donc z est divisible par un nombre i-premier. Donc dans tous les cas $\mathcal{P}_{n+1}$ est vérifiée.
La récurrence est démontrée, on peut affirmer

Tout entier de $\mathbb{Z}[i]$ est soit une unité ($N(z) = 1$), soit divisible par un nombre i-premier ($N(z) \geqslant 2$)

La démonstration de l'existence, peut également se faire par une récurrence forte.
Pour tout $n \in \mathbb{N}$, $n \geqslant 2$, $\mathcal{Q}_n$: « tout $z \in \mathbb{Z}[i]$ tel que $2 \leqslant N(z) \leqslant n$ s'écrit comme un produit de nombres i-premiers. »
— Soit $z \in \mathbb{Z}[i]$ tel que $N(z) = 2$.
Comme $N(z)$ est premier, alors z est nécessairement i-premier.
Donc $z = z$ et $\mathcal{Q}_2$ st vérifiée.
— Soit $n \geqslant 2$. Supposons que $\mathcal{Q}_n$ est vraie.
Soit $z \in \mathbb{Z}[i]$ tel que $N(z) \leqslant n+1$.
Si $N(z) \leqslant n$, alors d'après $\mathcal{Q}_n$ qui est vraie, n est produit de nombres i-premiers.
Supposons maintenant que $N(z) = n+1$.
Soit z est i-premier, il est alors produit de nombre i-premier (lui-même).
Soit z n'est pas i-premier, il existe z_1, i-premier qui divise z d'après la récurrence précédente.
Puis $z_2 \in \mathbb{Z}[i]$ non inversibles tels que $z = z_1 z_2$.
On a donc $2 \leqslant N(z_2) \leqslant \frac{n+1}{2} \leqslant n$.
D'après $\mathcal{Q}_n$, il z_2 est produit de nombres i-premier. Il en est de même de $z = z_1 z_2$.
Donc dans tous les cas $\mathcal{Q}_{n+1}$ est vérifiée.
Pour l'unicité, on suppose que z s'écrit de deux façons comme produit de nombre i-premier.
Alors il existe $n_1 \neq n_2 \in \mathbb{N}$, p i-premier, (avec n_1 ou n_2 qui peut être nul), tel que p^{n_1} figure dans la première décomposition de z et p^{n_2} dans la seconde.
Supposons que $n_1 < n_2$, en divisant la seconde décomposition de z par la seconde, on a $1 = p^{n_2 - n_1} \prod_j q_j^{\alpha_j}$, avec pour tout j q_j i-premier différent de p et $\alpha_j \in \mathbb{Z}$.
On a donc $p \prod_{j, \alpha_j > 0} = \prod_{j, \alpha_j < 0} q_j$.
Mais d'après le lemme de Gauss, il existe j tel que $p|q_j$, ce qui est faux.
Donc z ne s'écrit que d'une façon unique. */3*

Tout nombre entier de $\mathbb{Z}[i]$ inversible s'écrit comme un produit unique de nombres i-premiers (sans tenir compte des inversibles, des nombres associés et de l'ordre du produit).

C. Un nombre premier comme somme de 2 carrés

Dans cette partie nous montrons que :

$$p \in \mathbb{N} \text{ premier s'écrit sous la forme } a^2+b^2 \text{ si et seulement si } p \equiv 1[4].$$

Dans les questions 1. et 2., nous démontrons le sens direct de la proposition (condition nécessaire).
Dans la question 3., nous faisons un détour pour démontrer le théorème de Wilson.
Nous exploitons ce résultat dans la question 4., pour démontrer constructivement le sens indirect de la proposition (condition suffisante).

1. Si $p = 2 = a^2 + b^2$ Donc $a^2 \leqslant 2$, donc $a = 1$ ou $a = 0$.
   Mais si $a = 0$, alors $b^2 = 2$ n'est pas possible. */0,5*

   $$\boxed{\text{Seul le couple } (1,1) \text{ de } \mathbb{N}^2 \text{ vérifie } 1^2+1^2=2}$$

2. Soit p un nombre premier, différent de 2. Supposons quil existe $a, b \in \mathbb{N}$ tels que $p = a^2+b^2$.
   p est un nombre premier différent de 2, il est donc impair donc $p \equiv 1[4]$ ou $p \equiv 3[4]$.
   Si $a \equiv 0[2]$, alors $a = 2k$ et donc $a^2 = 4k^2$, donc $a \equiv 0[4]$.
   Si $a \equiv 1[2]$, alors $a = 2k+1$ et donc $a^2 = (2k+1)^2 = 4(k^2+1)+1$, donc $a \equiv 1[4]$.
   En prenant chacune des quatre situations (selon la parité de a et de b),
   il est impossible que $a^2 + b^2 \equiv 3[4]$. */1*

   $$\boxed{\text{On a donc nécessairement } p \equiv 1[4]}$$

3. Soit q un entier premier.

   (a) Le théorème s'énonce ainsi : */1*

   $$\boxed{\forall\, q \in \mathcal{P}, \forall\, n \in \mathbb{N} \text{ tel que } n \wedge q = 1, \text{ alors } n^{q-1} \equiv 1[q]}$$

   (b) On considère le polynôme $P(X) = (X^{q-1}-1) - (X-1)(X-2)\cdots(X-(q-1))$.
   Le développement de $(X-1)(X-2)\cdots(X-(q-1))$, donne un polynôme de degré $q-1$, unitaire (de terme dominant X^{q-1}).
   Donc, par soustraction : */0,5*

   $$\boxed{\deg(P) < q-1}$$

   (c) Soit $k \in [\![1, q-1]\!]$, on a donc */0,5*

   $$\boxed{P(k) = k^{q-1} - 1 + (k-1)(k-2)\ldots 0 \ldots (k-q+1) = k^{q-1} - 1 \equiv 0[q]}$$

   d'après le petit théorème de Fermat

   (d) D'après le théorème à admettre, P est de degré au plus $q-2$, avec $q-1$ racines disticntes, toutes inférieures strictement à q (modulo q), donc P est nul modulo p.
   On en déduit en particulier que le coefficient constant $a_0 \equiv 0[p]$.
   Or, après développement, on a

   $$a_0 = -1 + (-1)\times(-2)\times(-q+1) = -1 + (-1)^{q-1}(q-1)! = (q-1)! - 1$$

   car $q-1$ est pair, puisque que q est premier différent de 2.
   Et donc $(q-1)! - 1 \equiv 0[q]$, ou autrement écrit : */2*

   $$\boxed{(q-1)! \equiv -1[q] \qquad \text{Théorème de Wilson}}$$

   <u>*Démonstration du résultat admis*</u> *:*

   Soit P de degré d à coefficients entiers, $P(X) = \sum_{k=0}^{d} a_k X^k$
   Si il existe $d+1$ valeurs entiers, $0 < a_0, \cdots < a_d \leqslant p-1$ tel que : $\forall\, i \leqslant d$, $P(a_i) \equiv 0[p]$, alors pour tout $k \in \{0, 1, \ldots d\}$, $a_k \equiv 0[p]$.
   Pour le démontrer on peut procéder en deux temps, avec $f, g, h \in \mathbb{Z}[X]$:
   — *si $f(x) \equiv g(x)h(x)[p]$, alors toute racine de f est racine de g ou de h.*
   En effet, si $f(a) = 0$, alors $g(a)h(a) \equiv 0[p]$.
   Si $g(a) \not\equiv 0[p]$, alors $p \not| g(a)$, donc $g(a) \wedge p = 1$ (p est premier).
   D'après Bézout, il existe $u, v \in \mathbb{Z}$ tel que $ug(a) + vp = 1$ et donc $ug(a) \equiv 1[p]$.
   Et par conséquent : $h(a) \equiv ug(a)h(a) \equiv u \times 0 = 0[p]$

— *Par récurrence, on démontre le résultat admis.*
Pour vérifier $\mathcal{P}_{n+1}$, on considère : f de degré $< n+1$ qui admet $n+1$ racines distinctes.
Notons a_{n+1}, l'une de ces racines, la division euclidienne polynômiale de f par $(x-a_{n+1})$ donne :

$$f(x) = (x-a_{n+1})g(x) + C$$

où C est une constante. Et donc comme $f(a_{n+1}) \equiv 0[p]$, on a donc $C \equiv 0[p]$.
Donc $f \equiv (x-a_{n+1})g[p]$. Alors $\deg g \leqslant \deg f - 1 < n$ et $a_0, a_1, \dots a_n$, les n autres racines de f sont également des racines de g. D'après le point précédent.
Et donc d'après $\mathcal{P}_n$, g est nul (modulo p), c'est donc aussi le cas de f et $\mathcal{P}_{n+1}$ est vraie.
L'hérédité est donc obtenue.
Concernant l'initialisation, on considère f de degré < 1, donc $f = C$, une constante, avec une racine $f(a) \equiv 0[p]$.
Or $f(a) = C$, donc $C \equiv 0[p]$ et donc $f \equiv 0[p]$.

4. Nous allons démontrer l'application réciproque. Considérons donc p premier et tel que $p \equiv 1[4]$.

(a) Notons $p = 1 + 4k$, donc $\frac{p-1}{2} = 2k$ et :

$$(p-1)! = 1 \times 2 \times \cdots \times 4k = \big(1 \times 2 \times \cdots 2k\big) \times \big((2k+1) \times (2k+2) \times \cdots 4k\big)$$

Puis $2k \equiv -1 - 2k[4k+1]$, et de manière générale :

$$\forall\ h \in [\![1, 2k]\!], \qquad 2k + h \equiv -1 - 2k + h \equiv -(2k - h + 1)[4k+1](= [p])$$

Ainsi, en posant $i = 2k - h + 1$, dans le second produit :

$$(p-1)! \equiv \prod_{i=1}^{2k} i \times \prod_{h=1}^{2k} -(2k-h+1)) = (-1)^{2k} \prod_{i=1}^{2k} i^2 = ((2k)!)^2[p]$$

Enfin, comme d'après le théorème de Wilson $(p-1)! \equiv -1[p]$, /2

$$\boxed{\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1[p]}$$

(b) Si on note $x = \left(\frac{p-1}{2}\right)!$, on a donc $(x+i)(x-i) = x^2 + 1 \equiv 0[p]$. /0,5

$$\boxed{\text{Il existe } x \in \mathbb{N} \text{ tel que } p|(x+i)(x-i). \ (x \text{ n'est probablement pas unique})}$$

(c) Supposons que p soit i-premier. Il faut maintenant voir p, entier comme entier de Gauss : $p = p + 0i$.
Alors d'après le lemme de Gauss p divise $x+i$ ou p divise $x-i$.
Supposons que ce soit p divise $x+i$, il existe donc $a, b \in \mathbb{Z}$ tels que $p(a+ib) = x+i$.
On a donc $ap = x$ et $bp = 1$. Cette seconde égalité donne $p = 1$, impossible car p est premier.
De même si on suppose que p divise $x-i$, on obtient l'existe de $b' \in \mathbb{Z}$ tel que $pb' = -1$.
Impossible. /2

$$\boxed{\text{Par conséquent, } p \text{ ne peut pas être } i\text{-premier.}}$$

(d) Comme p n'est pas i-premier, alors il existe $z = (a+ib)$ et $z' = (a'+ib')$, non inversibles tels que $p = zz'$.
On a donc $N(z)N(z') = N(p) = p^2$.
Or p est un nombre premier, les diviseurs de p^2 sont donc 1, p et p^2. Or :
— $N(z) \neq 1$, sinon z serait inversible.
— $N(z) \neq p^2$, sinon $N(z') = 1$ et donc z' serait inversible.
— Donc $N(z) = p$.
Et comme $z = a + ib$, on a donc /1

$$\boxed{\exists\ a, b \in \mathbb{Z} \text{ tels que } a^2 + b^2 = p}$$

/0,5

(e)

$$\boxed{13 = 4 + 9 = 2^2 + 3^2}$$

D. Somme de deux carrés

Dans cette partie, nous généralisons le résultat de la partie précédente à tout entier n.
Nous démontrons en particulier :

$$n \in \mathbb{N} \text{ s'écrit sous la forme } a^2+b^2 \text{ si et seulement si}$$
$$\text{chacun de ses facteurs premiers de la forme } 4k+3 \text{ intervient à une puissance paire}$$

Nous terminons cette partie en dénombrant le nombre de telle décomposition, selon la factorisation de n.

1. Soit $n = a^2+b^2 \in \mathbb{N}$, avec $a, b \in \mathbb{N}$.
   On note $\delta = a \wedge b$ et a' et b' tels que $a = a'\delta$ et $b = b'\delta$.
   (a) Soit p diviseur premier impair de $(a')^2+(b')^2$.
   On a donc $p|(a'+ib')(a'-ib')$.
   Si p est i-premier, alors $p|(a'+ib')$ ou $p|(a'-ib')$ d'après le lemme de Gauss (A.6.(e)).
   Mais comme p est entier, cela impose que $p|a'$ et $p|b'$
   (en effet : $a = p\mathfrak{Re}(z)$ et $b = \pm b\mathfrak{Im}(z)$ si z est telle que $pz = a \pm ib$).
   Et donc finalement p divise à la fois $a'+ib'$ et $a'-ib'$.
   Il divise en particulier leur somme : $2a'$ et leur différence $2b'$ (dans $\mathbb{Z}[i]$).
   Enfin, cette division dans $\mathbb{Z}[i]$, impose aussi la division dans $\mathbb{Z}$ (car tous ces nombres sont des entiers réels).
   Ainsi /1,5

   $$\boxed{\text{si } p \text{ est } i\text{-premier dans } \mathbb{Z}[i], \text{ alors } p \text{ divise } 2a' \text{ et } 2b'}$$

   Par conséquent comme p n'est pas le nombre premier 2, $p|a'$ et $p|b'$.
   Ainsi $p|(a' \wedge b') = 1$. /0,5

   $$\boxed{\text{Nous avons donc une contradiction, donc } p \text{ est composé dans } \mathbb{Z}[i]}$$

   (b) D'après la question précédente, $p = z_1 z_2$, avec z_1 et z_2 non inversible.
   On a alors $N(z_1)N(z_2) = N(p) = p^2$.
   Donc, comme p est premier, $N(z_1) = p^\alpha$ avec $\alpha \in \{0,1,2\}$.
   Or $\alpha = 0$ est impossible, sinon z_1 serait inversible.
   De même $\alpha = 2$ est impossible sinon z_2 serait inversible.
   Donc $\alpha = 1$ et /1,5

   $$\boxed{N(z_1) = p = c^2+d^2, \text{ si } z_1 = c+id}$$

   Remarque : La décomposition est alors « unique ».
   En effet si $n = e^2+f^2$, alors $e+if|n = (c+id)(c-id)$.
   Or $N(c+id) = p$, premier, donc nécessairement $c+id$ est i-premier ($c-id$ également).
   Donc $e+if|c+id$ ou $e+if|c-id$,
   donc il existe $I \in \mathbb{Z}[i]^*$ tel que $e+if = I$ ou $e+id = I(c+id)$ ou $e+id = I(c-id)$.
   ce qui donne une certaine unicité (en considérant égal : c^2+d^2 et d^2+c^2...

   (c) Finalement, on a montré :

   $$\boxed{\begin{array}{c}\text{Si } p, \text{ diviseur premier de } (a')^2+(b')^2, \text{ alors } p \text{ est composée dans } \mathbb{Z}[i] \\ \text{et } p = c^2+d^2 \text{ et donc } p \equiv 1[4]\end{array}}$$

   Mais on doit aller plus loin, en revenant au cas général,
   si p divise $n = a^2+b^2 = \delta^2(a'^2+b'^2)$.
   Alors si $p \equiv 3[4]$, alors $p \not| (a'^2+b'^2)$ et donc $p|\delta^2$.
   Et par conséquent $p|\delta$. Notons $v_p(\delta)$, la valuation p-adique de δ.
   On a donc $\delta = \lambda p^{v_p(\delta)}$ et donc $n = \lambda^2 p^{2v_p(\delta)}(a'^2+b'^2)$.
   Ainsi $v_p(n)$ est pair. /1,5

   $$\boxed{\text{Bilan : si } p \equiv 3[4] \text{ est premier et divise } n \text{ alors } v_p(n) \text{ est pair}}$$

2. Réciproquement, soit $n = 2^a \left(p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right)^2 q_1^{\beta_1} \cdots q_m^{\beta_m}$, avec $p_i \equiv 3[4]$ et $q_j \equiv 1[4]$
   (a) On peut faire le calcul, directement et avec courage, mais il y a plus efficace...
   On note $z = a+ib$ et $z' = c+id$:

   $$(a^2+b^2)(c^2+d^2) = N(z)N(z') = N(z)N(\overline{z'}) = N(z\overline{z'}) = N\big((a+ib)(c-id)\big)$$

   /1

   $$\boxed{(a^2+b^2)(c^2+d^2) = N\big((ac+bd)+i(bc-ad)\big) = (ac+bd)^2+(ad-bc)^2 \quad \textit{Lagrange}}$$

(b) Le théorème de Lagrange affirme que si deux nombres peuvent s'écrire comme somme de deux carrés, alors leur produit peut également s'écrire sous cette forme.
On a alors, par récurrence,
si n nombres peuvent se mettre sous la forme de somme de deux carrés,
alors leur produit peut également se mettre sous forme de deux carrés.
Pour tout $j \in \mathbb{N}_m$, $q_j \equiv 1[4]$, donc il existe $a_j, b_j \in \mathbb{N}$ tel que $q_j = a_j^2 + b_j^2$.
Donc pour tout $\beta_j > 0$, $q_j^{\beta_j}$ est somme de deux carrés.
Leur produit peut également s'écrire sous somme de deux carrés.
Enfin, $2 = (1^2 + 1^2)$, donc 2^a s'écrit aussi comme somme de deux carrés.
Enfin, leur produit général, */1*

$$\boxed{2^a q_1^{\beta_1} \cdots q_m^{\beta_m} \text{ peut s'écrire comme la somme de deux carrés.}}$$

(c) Enfin, $(p_1^{\alpha_1} \cdots p_k^{\alpha_k})^2 = 0^2 + (p_1^{\alpha_1} \cdots p_k^{\alpha_k})^2$, c'est une somme de deux carrés, alors par produit, d'après l'identité de Lagrange : */0,5*

$$\boxed{n \text{ peut s'écrire comme la somme de deux carrés.}}$$

3. Si $p \equiv 3[4]$, alors la seul décomposition possible de p^2 est $p^2 + 0^2$.
Mais si $p \equiv 1[4]$, alors il existe $a_1, b_1 \in \mathbb{N}$ tel que $p = a_1^2 + b_1^2$.
On a alors, d'après l'identité de Lagrange, $p^2 = (a_1^2 + b_1^2)^2 + 0^2 = (2a_1b_1)^2 + (a_1^2 - b_1^2)^2$.
La seconde identité répond à la question. */1*

$$\boxed{\begin{array}{c}\text{Les premiers } p \equiv 1[4] \text{ sont les seuls nombres premiers de longueur} \\ \text{d'une hypothènuse d'un triangle rectangle à longueurs entières.}\end{array}}$$

On peut voir par exemple $5 = 1^2 + 2^2$ et donc $5^2 = (2 \times 1 \times 2)^2 + (2^2 - 1^2)^2 = 4^2 + 3^2$,
ou encore $13 = 2^2 + 3^2$ et donc $13^2 = 12^2 + 5^2 \ldots$

4. On a donc $n = 2\,925 = 3^2 \times 5^2 \times 13$.
On a $3 \equiv 3[4]$, on le garde sous cette forme,
alors que $5 \equiv 1[4]$ et $13 \equiv 1[4]$. On considère donc $5 = 1^2 + 2^2$ et $13 = 2^2 + 3^2$.
Avant de faire les calculs faisons deux remarques dans l'utilisation de l'identité de Lagrange :
— Si l'on change l'ordre des calculs, cela ne change pas le résultat final (associativité) :

$$(a^2+b^2)(c^2+d^2)(e^2+f^2) = [(a^2+b^2)(c^2+d^2)](e^2+f^2) = [(ac+bd)^2+(ad-bc)^2](e^2+f^2)$$
$$= [(ac+bd)e + (ad-bc)f]^2 + [(ac+bd)f - (ad-bc)e]^2$$
$$= (a^2+b^2)[(ce+df)^2 + (de+cf)^2] = (a^2+b^2)[(c^2+d^2)(e^2+f^2)]$$

— Si l'on permute les nombres a et b cela change le résultat final

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bc)^2 \neq (bc+ad)^2+(bd-ac)^2 = (b^2+a^2)(c^2+d^2)$$

(si $a \neq b$ et $c \neq d$)...
On a donc, en plusieurs temps :

$$5^2 = (1^2+2^2)(1^2+2^2) = 5^2+0^2 = (1^2+2^2)(2^2+1^2) = 4^2+3^2$$
$$5^2 \times 13 = (5^2+0^2)(3^2+2^2) = 15^2+10^2 = (0^2+5^2)(3^2+2^2) = 10^2+15^2$$
$$5^2 \times 13 = (4^2+3^2)(3^2+2^2) = 18^2+1^2 = (3^2+4^2)(3^2+2^2) = 17^2+6^2$$

Et enfin, comme $3^2 = (3^2+0^2) = (0^2+3^2)$.
On trouve avec les trois valeurs : $5^2 \times 13 = 15^2+10^2 = 18^2+1^2 = 17^2+6^2$, */2*

$$\boxed{2\,925 = 3^2+54^2 = 54^2+3^2 = 18^2+51^2 = 51^2+18^2 = 30^2+45^2 = 45^2+30^2}$$

On comptera comme représentations disctinctes, les deux représentations $A^2 + B^2$ et $B^2 + A^2$ (si $A \neq B$). On considère $A, B \geqslant 0$.

5. (*) Dans la formule à obtenir, on constate que :
— il n'y a pas de place pour les valuations 2-adique ;
— l'enjeu principal se trouve pour les valuations p_1 adique ;
— la valuation p_3-adique n'intervient que pour signfier si elle est pair ou impair.

Commençons par cette dernière valuation, on voit que :

S'il existe p_3 tel que $v_{p_3}(n)$ est impair, alors $1+(-1)^{v_{p_3}(n}=1-1=0$;

c'est légitime : dans ce cas, n n'est pas décomposable en somme de carrés.

S'il pour tout p_3, $v_{p_3}(n)$ est pair, alors $\frac{1+(-1)^{v_{p_3}(n}}{2}=\frac{1+1}{2}=1$;

le valutation p_3-adique ne jouerait aucun rôle dans le dénombrement attendu.

De même, il faut montrer que la valuation 2-adique ne joue aucun rôle dans ce dénombrement.
Considérons maintenant à nouveau

$$n=2^a\left(p_1^{\alpha_1}\cdots p_k^{\alpha_k}\right)^2 q_1^{\beta_1}\cdots q_m^{\beta_m}$$

avec $p_i\equiv 3[4]$ et $q_j\equiv 1[4]$. Il faut donc montrer que $r_2(n)=\prod_{j=1}^{m}(\beta_j+1)$.
On peut factoriser n sur $\mathbb{Z}[i]$, en produit de i-premier :

$$n=[(1+i)(1-i)]^a\times\prod_{h=1}^{k}p_h^{2\alpha_h}\times\prod_{j=1}^{m}[(a_j+b_ji)(a_j-b_ji)]^{\beta_j}$$

car on a vu les décomposition de nombres premiers en produit de i-premier selon le résidu modulo 4.
q_j étant premier dans $\mathbb{N}$, la décomposition $q_j=(a_j+ib_j)(a_j-ib_j)$ est unique (voir remarque en D.1.b)). /1
La décomposition que l'on vient d'obtenir de n est donc l'unique décomposition en produit de i-premiers (à l'ordre près et produit par irréductibles près).
Supposons maintenant que /1

$$n=A^2+B^2=(A+iB)(A-iB)=[(1+i)(1-i)]^a\times\prod_{h=1}^{k}p_h^{2\alpha_h}\times\prod_{j=1}^{m}[(a_j+b_ji)(a_j-b_ji)]^{\beta_j}$$

D'après le lemme de Gauss, comme nous avons un produit de nombre premiers, on a donc

$$\begin{cases} A+iB &= I\times(1+i)^{a^+}(1-i)^{a^-}\times\prod_{h=1}^{k}p_h^{2\alpha_h^+}\times\prod_{j=1}^{m}(a_j+b_ji)^{\beta_j^+}(a_j-b_ji)^{\beta_j^-} \\ A-iB &= \frac{1}{I}\times(1+i)^{a-a^+}(1-i)^{a-a^-}\times\prod_{h=1}^{k}p_h^{2(\alpha_h-\alpha_h^+)}\times\prod_{j=1}^{m}(a_j+b_ji)^{\beta_j-\beta_j^+}(a_j-b_ji)^{\beta_j-\beta_j^-} \end{cases}$$

avec I un élément inversible de $\mathbb{Z}[i]$.
Les coefficients ont été donnés pour que $(A+iB)(A-iB)=A^2+B^2=n$.
Mais, comme $\overline{A+iB}=A-iB$, et que la décomposition en facteurs i-premiers est unique (aux inversibles près), on a donc $(1-i)^{a^+}=\overline{(1+i)^{a^+}}=(1-a)^{a-a^-}$, donc $a^++a^-=a$.
De même, on trouve que $\beta_j^++\beta_j^-=\beta$.
Enfin, comme $|A+iB|=|A-iB|$, nécessairement, $p_h^{2\alpha_h^+}=p_h^{2(\alpha-\alpha_h^+)}$, ce qui conduit à $2\alpha^+=\alpha.$, finalement, on obtient :

$$\begin{cases} A+iB &= I\times(1+i)^{a^+}(1-i)^{a-a^+}\times\prod_{h=1}^{k}p_h^{\alpha_h}\times\prod_{j=1}^{m}(a_j+b_ji)^{\beta_j^+}(a_j-b_ji)^{\beta-\beta_j^+} \\ A-iB &= \frac{1}{I}\times(1+i)^{a-a^+}(1-i)^{a^+}\times\prod_{h=1}^{k}p_h^{\alpha_h}\times\prod_{j=1}^{m}(a_j+b_ji)^{\beta_j-\beta_j^+}(a_j-b_ji)^{\beta_j^+} \end{cases}$$

Étudions maintenant les répartitions possibles, donc les valeurs possibles des coefficients α^+ et $\beta_j^+\ldots$
Il y a donc a priori $\alpha+1$ valeurs possibles pour α_+ (de 0 à α),

et de même β_j+1 valeurs possibles pour chaque β_j^+.

et enfin 4 valeurs possibles pour I (c'est le card($\mathbb{Z}[i]^*$), les inversibles).

La distribution est indépendante : il y a $4(\alpha+1)\prod_{j=1}^{m}(\beta_j+1)$ décompositions possibles.

Mais remarquons que $\frac{1+i}{1-i}=-i\ldots$, donc le choix sur α_+, ne change qu'au niveau d'un inversible.

Donc il y a plutôt : $4\prod_{j=1}^{m}(\beta_j+1)$ décompositions possibles.

Enfin, avec un tel décomposition on obtient exactement tous les couples $(A,B)\in\mathbb{Z}^2$ tel

que $A^2 + B^2 = n$.
En particulier pour $A, B > 0$, on a compté aussi $(-A)^2+B^2$, $A^2+(-B)^2$ et $(-A)^2+(-B)^4$,

Donc par rapport à notre définition de représentations distinctes, nous en comptons ainsi 4 fois trop.
Donc le nombre de représentations distinctes (pour $p_h^{2\alpha_h}$) est $\prod_j \beta_j + 1$.
Or par définition $\beta_j = v_{q_j}(n)$, on retrouve donc : */1,5*

$$\boxed{r_2(n) = \prod_{p \in \mathcal{P}_1} (v_p(n) + 1) \times \prod_{p \in \mathcal{P}_3} \left(\frac{1 + (-1)^{v_p(n)}}{2} \right)}$$

où $\mathcal{P}_1 = \{p \in \mathcal{P} \mid p \equiv 1[4]\}$ et $\mathcal{P}_3 = \{p \in \mathcal{P} \mid p \equiv 3[4]\}$.