Les calculatrices, téléphones, tablettes, ordinateurs, montres connectées et tous appareils électroniques de communication ou de stockage, ainsi que les documents sont interdits.

La qualité de la rédaction sera un facteur important d'appréciation des copies. On invite donc les candidats à produire des raisonnements clairs, complets et concis.

Les candidats peuvent utiliser les résultats énoncés dans les questions ou parties précédentes, en veillant dans ce cas à préciser la référence du résultat utilisé.

Définitions et rappels

— Soit A un anneau commutatif unitaire intègre dont on note 1_A l'élément unité.

— On rappelle que $u \in A$ est *inversible* s'il existe $u' \in A$ tel que $uu' = 1_A$. On note $A^\times$ l'ensemble des inversibles de A, qui est un groupe multiplicatif.

— Un élément x de A est dit *irréductible* si x n'est pas inversible et si pour tous $\alpha, \beta \in A$, $x = \alpha\beta$ implique $\alpha \in A^\times$ ou $\beta \in A^\times$.

— Deux éléments $x, y \in A$ sont dits *associés* s'il existe $u \in A^\times$ tel que $x = uy$. On note alors $x \sim y$.

— Soit I un idéal de A ; on dit que deux éléments $\alpha, \beta \in A$ sont *congrus modulo* I si $\alpha - \beta \in I$. On écrit alors $\alpha = \beta \pmod{I}$.

— Pour $x \in A$, on note $\langle x \rangle = xA$ l'idéal engendré par x. Un tel idéal est dit *principal*.

— Soient I, J deux idéaux de A. On dit que I *divise* J si $J \subseteq I$. Par ailleurs, on note IJ l'idéal produit de I et J, qui est l'ensemble des sommes finies $\sum_i x_i y_i$ avec $x_i \in I$ et $y_i \in J$.

— On rappelle qu'un nombre complexe α est dit *algébrique* (sur $\mathbf{Q}$) s'il existe un polynôme non nul P de $\mathbf{Q}[X]$ tel que $P(\alpha) = 0$. Il existe alors un polynôme unitaire de plus petit degré annulant α, que l'on appelle *polynôme minimal* de α et que l'on note π_α. Les racines complexes de ce polynôme sont appelées les *conjugués* de α.

— On appelle *entier algébrique* tout nombre complexe qui est racine d'un polynôme unitaire à coefficients dans $\mathbf{Z}$.

— On rappelle une version du lemme de Gauss, que l'on pourra utiliser librement : soit $P \in \mathbf{Z}[X]$ tel que $P = P_1 P_2$ avec P_1 et P_2 des polynômes de $\mathbf{Q}[X]$. Alors il existe un rationnel $r \in \mathbf{Q}$, non-nul, tel que $rP_1 \in \mathbf{Z}[X]$ et $\frac{1}{r}P_2 \in \mathbf{Z}[X]$.

— On dit qu'un groupe abélien G est de *type fini* s'il existe une famille génératrice finie de G, c'est-à-dire un entier r et une famille $(a_1, \ldots, a_r)$ d'éléments de G tels que tout élément de G s'écrit comme une combinaison linéaire à coefficients entiers des $a_1, \ldots, a_r$.

Notations

— Pour un anneau A commutatif et un entier naturel non nul n, on note $\mathcal{M}_n(A)$ l'algèbre des matrices carrées $n \times n$ à coefficients dans A ; la matrice unité est notée I_n.
Si M est une matrice de $\mathcal{M}_n(A)$, on note χ_M son polynôme caractéristique, qui est le polynôme

unitaire défini par $\chi_M = \det(XI_n - M)$ et on note π_M son polynôme minimal.

— Pour un nombre premier p, on note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$.

— Pour tout entier algébrique α, on note $\mathbf{Z}[\alpha]$ l'anneau des éléments de la forme $P(\alpha)$ où P parcourt $\mathbf{Z}[X]$.

Dans le problème, les textes placés entre les symboles ☛ ... ☚ précisent des notations et définitions qui sont utilisées dans la suite de l'énoncé.

I Exercices préliminaires

1. Soit $B \in \mathbf{Z}[X]$ un polynôme unitaire et $A \in \mathbf{Z}[X]$. Montrer qu'il existe $Q, R \in \mathbf{Z}[X]$ tels que $A = BQ + R$ avec $\deg R < \deg B$ ou $R = 0$.
   Indication : On pourra faire une preuve par récurrence sur le degré de A.
2. **L'anneau $\mathbf{Z}[j]$.** On note $j = e^{\frac{2i\pi}{3}}$.
   (a) Démontrer que j est un élément algébrique sur $\mathbf{Q}$ et préciser son polynôme minimal.
   (b) Démontrer que $\mathbf{Z}[j] = \{a + bj,\ (a, b) \in \mathbf{Z}^2\}$.
   Pour tout nombre complexe z, on pose $\mathrm{N}(z) = z\overline{z} = |z|^2$.
   (c) Démontrer que pour tout $z \in \mathbf{Z}[j]$, on a $\mathrm{N}(z) \in \mathbf{N}$. En déduire que si $z \in \mathbf{Z}[j]$ est inversible, alors $\mathrm{N}(z) = 1$, puis que $\mathbf{Z}[j]^\times$ possède 6 éléments que l'on précisera.
   (d) Soient $x \in \mathbf{Z}[j]$ et $y \in \mathbf{Z}[j] \setminus \{0\}$. Déterminer un élément $q \in \mathbf{Z}[j]$ tel que $\mathrm{N}\left(\frac{x}{y} - q\right) < 1$. En déduire que l'anneau $\mathbf{Z}[j]$ est euclidien.
3. **Polynômes cyclotomiques**. Soit n un entier naturel non nul. On note Φ_n le n-ième polynôme cyclotomique. On rappelle que si μ_n^* désigne l'ensemble des racines primitives n-ièmes de l'unité dans $\mathbf{C}$, ce polynôme est défini par
$$\Phi_n(X) = \prod_{\mu \in \mu_n^*} (X - \mu).$$
   (a) Démontrer que $X^n - 1 = \prod_{d|n} \Phi_d(X)$.
   (b) En déduire que $\Phi_n(X) \in \mathbf{Z}[X]$.
   (c) Soit p un nombre premier. On note $\pi : \mathbf{Z} \longrightarrow \mathbf{F}_p$ la surjection canonique. Le morphisme d'anneaux π s'étend, coefficient par coefficient, en un morphisme d'anneaux de $\mathbf{Z}[X]$ sur $\mathbf{F}_p[X]$, noté $\widehat{\pi}$ (on ne demande pas de justifier ce point). Si Φ_p désigne le p-ième polynôme cyclotomique, on rappelle que $\Phi_p = \sum_{k=0}^{p-1} X^k$.
      i. Démontrer que $\widehat{\pi}(X^p - 1) = (X - 1_{\mathbf{F}_p})^p$.
      ii. Soient P et Q deux polynômes unitaires et non constants dans $\mathbf{Z}[X]$ tels que $X^p - 1 = PQ$. Démontrer que $P(1)$ et $Q(1)$ sont des entiers multiples de p.
      iii. Retrouver ainsi que Φ_p est un polynôme irréductible de $\mathbf{Q}[X]$.

      ☛*De manière générale, Φ_n est irréductible pour tout $n \in \boldsymbol{N} \setminus \{0\}$, résultat que l'on admet ici et que l'on pourra utiliser librement dans la suite.* ☚

      iv. Soit $\zeta = e^{\frac{2i\pi}{p}}$. Déterminer le polynôme minimal de ζ sur $\mathbf{Q}$ et en déduire le degré de l'extension de corps $\mathbf{Q}(\zeta)/\mathbf{Q}$.

4. **Matrices compagnons**. Soit n un entier naturel non nul. Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme unitaire de $\mathbf{C}[X]$. On lui associe sa *matrice compagnon* C_P définie dans $\mathcal{M}_n(\mathbf{C})$ par

$$\mathrm{C}_P = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}.$$

On note $\mathcal{E} = (e_1, \ldots, e_n)$ la base canonique de $\mathbf{C}^n$.

(a) Pour $k \in \{1, \ldots, n-1\}$, exprimer $\mathrm{C}_P^k e_1$ dans la base $\mathcal{E}$. En déduire que pour tout polynôme $Q \in \mathbf{C}[X]$ non nul et de degré inférieur ou égal à $n-1$, la matrice $Q(\mathrm{C}_P)$ est non nulle.
En déduire le degré du polynôme minimal de C_P.

(b) Exprimer $\mathrm{C}_P^n e_1$ dans la base $\mathcal{E}$. En déduire que P est le polynôme minimal de C_P.

(c) En déduire le polynôme χ_{C_P}.

Soit $M \in \mathcal{M}_n(\mathbf{C})$ de polynôme caractéristique χ_M. Soient $\alpha_1, \ldots, \alpha_n$ les racines complexes de χ_M comptées avec leur multiplicité. Soit Q un polynôme de $\mathbf{C}[X]$.

(d) Démontrer que le polynôme caractéristique de la matrice $Q(M)$ est

$$\chi_{Q(M)} = \prod_{k=1}^{n} (X - Q(\alpha_k)).$$

Indication : On pourra commencer par traiter le cas où M est triangulaire.

(e) Soit A un sous-anneau de $\mathbf{C}$. On suppose que le polynôme Q est dans $A[X]$. Soit $P \in A[X]$ un polynôme unitaire dont on note $\alpha_1, \ldots, \alpha_n$ les racines complexes comptées avec leur multiplicité.
Démontrer que $\prod_{k=1}^{n} (X - Q(\alpha_k))$ est un polynôme de $A[X]$.

II Nombres algébriques

1. (a) On désigne par φ l'indicatrice d'Euler, qui à tout entier $n \in \mathbf{N} \setminus \{0\}$ associe le nombre d'entiers non nuls inférieurs à n et premiers avec n. Justifier que pour tout entier $d \geqslant 1$, l'ensemble des entiers n tels que $\varphi(n) \leqslant d$ est fini.

(b) En déduire que si $\mathbf{K}/\mathbf{Q}$ est une extension finie de $\mathbf{Q}$, où $\mathbf{K}$ est un sous-corps de $\mathbf{C}$, alors $\mathbf{K}$ contient un nombre fini de racines de l'unité.

2. Soit $\alpha \in \mathbf{C}$ un nombre algébrique dont on rappelle que l'on a noté π_α son polynôme minimal. On note $\mathbf{K} = \mathbf{Q}(\alpha)$ le plus petit corps contenant α et $\mathbf{Q}$, et $d = [\mathbf{K} : \mathbf{Q}]$, le degré de l'extension de corps $\mathbf{Q}(\alpha)/\mathbf{Q}$.

(a) Montrer que π_α est un polynôme irréductible de $\mathbf{Q}[X]$ et que son degré est égal à d.

(b) Montrer que si σ est un morphisme de $\mathbf{Q}$-algèbre de $\mathbf{K}$ dans $\mathbf{C}$, $\sigma(\alpha)$ est une racine de π_α, c'est-à-dire un conjugué de α.
En déduire qu'il y a exactement d tels morphismes de $\mathbf{Q}$-algèbre, que l'on notera $\sigma_k : \mathbf{K} \to \mathbf{C}$, $k \in \{1, \ldots, d\}$.

3. Soit $\alpha \in \mathbf{C}$ un nombre algébrique et soit $\theta \in \mathbf{K} = \mathbf{Q}(\alpha)$. Comme dans la question précédente, les σ_k avec $k \in \{1, \ldots, d\}$ désignent les morphismes de $\mathbf{Q}$-algèbre de $\mathbf{Q}(\alpha)$.

(a) Justifier que θ est un nombre algébrique.

On pose

$$P_\theta = \prod_{k=1}^{d} (X - \sigma_k(\theta)) \in \mathbf{C}[X].$$

(b) Montrer que $P_\theta \in \mathbf{Q}[X]$.

(c) Justifier que π_θ divise P_θ, puis montrer que P_θ est une puissance de π_θ.

4. Montrer qu'un nombre algébrique α est un entier algébrique si et seulement si son polynôme minimal est à coefficients entiers.

5. Soit α un nombre complexe.

(a) Montrer que si α est un entier algébrique, alors le groupe additif G engendré par la partie $\{\alpha^n,\ n \in \mathbf{N}\}$ est de type fini.

(b) Réciproquement, montrer que si G est de type fini alors α est un entier algébrique.

Indication : En notant $(g_1, \ldots, g_n)$ une famille génératrice finie de G, on pourra considérer le déterminant du système obtenu en écrivant les éléments αg_i, $i \in \{1, \ldots, n\}$ comme combinaison linéaire des g_j.

6. En déduire que l'ensemble $\mathfrak{O}_\mathbf{C}$ des entiers algébriques de $\mathbf{C}$ est un sous-anneau de $\mathbf{C}$.

Indication : On pourra utiliser sans démonstration qu'un sous-groupe d'un groupe abélien de type fini est de type fini.

7. Montrer que $\mathfrak{O}_\mathbf{C} \cap \mathbf{Q} = \mathbf{Z}$.

☛*Dans la suite, on considère le corps $\boldsymbol{K} = \boldsymbol{Q}(\zeta)$ où $\zeta = e^{\frac{2i\pi}{p}}$ avec p premier impair, et on note $\mathfrak{O}_{\boldsymbol{K}}$ l'ensemble des entiers algébriques de $\boldsymbol{K}$. On pose $\lambda = 1 - \zeta$.*
On définit la norme *et la* trace *de tout élément $\theta \in \boldsymbol{K} = \boldsymbol{Q}(\zeta)$ par*

$$\mathrm{N}(\theta) = \prod_{k=1}^{p-1} \sigma_k(\theta) \ \textit{et}\ \mathrm{Tr}(\theta) = \sum_{k=1}^{p-1} \sigma_k(\theta),$$

où les σ_k sont les morphismes de $\boldsymbol{Q}$-algèbre de $Q(\zeta)$ définis dans la question 2 de cette partie. ☚

III Le corps $Q(\zeta)$ et son anneau d'entiers

1. (a) Montrer que les morphismes de $\mathbf{Q}$-algèbre de $\mathbf{Q}(\zeta)$ sont les σ_k tels que $\sigma_k(\zeta) = \zeta^k$, avec $k \in \{1, ..., p-1\}$.

(b) i. Montrer que $\mathrm{N}(\zeta) = 1$ et $\mathrm{Tr}(\zeta) = -1$.

ii. Montrer que $\mathrm{N}(1-\zeta) = p$ et $\mathrm{N}(1+\zeta) = 1$.

2. Montrer l'inclusion $\mathbf{Z}[\zeta] \subseteq \mathfrak{O}_\mathbf{K}$.

3. Soit $z \in \mathbf{Z}[\zeta]$.

(a) Montrer que $z \in \mathbf{Z}[\zeta]^\times$ si et seulement si $\mathrm{N}(z) \in \{-1, +1\}$.

(b) Montrer que si $\mathrm{N}(z)$ est un nombre premier, alors z est irréductible.

4. Le but de cette question est de montrer que l'ensemble G des racines de l'unité contenues dans $\mathbf{K}$ est formé exactement des éléments de la forme $\pm\zeta^k$, $k \in \{0, \ldots, p-1\}$.

(a) Justifier que G est un groupe fini cyclique, dont on notera n le cardinal.

(b) Soit ω un générateur de G. Justifier que $2p \mid n$ et que $\mathbf{Q}(\zeta) = \mathbf{Q}(\omega)$.

(c) En déduire que $n = 2p$ et conclure.

5. On note $\langle\lambda\rangle = \lambda\mathbf{Z}[\zeta]$, l'idéal de $\mathbf{Z}[\zeta]$ engendré par λ.
   (a) Montrer que $\langle\lambda\rangle \cap \mathbf{Z} = p\mathbf{Z}$.
   (b) Montrer que pour tout $k \in \{1, \ldots, p-1\}$, on a $\dfrac{1-\zeta}{1-\zeta^k} \in \mathbf{Z}[\zeta]^\times$ et en déduire que
   $$\lambda^{p-1}\mathbf{Z}[\zeta] = p\mathbf{Z}[\zeta].$$
   (c) Soit ψ le morphisme d'anneaux de $\mathbf{Z}[X]$ dans $\mathbf{Z}[\zeta]/\langle\lambda\rangle$, qui à $P \in \mathbf{Z}[X]$ associe $P(\zeta) \pmod{\langle\lambda\rangle}$. Déterminer l'image de ψ et montrer que $\ker\psi$ est l'ensemble des polynômes $P \in \mathbf{Z}[X]$ tels que $P(1) = 0 \pmod{p\mathbf{Z}}$.
   (d) En déduire que $\mathbf{Z}[\zeta]/\langle\lambda\rangle$ est isomorphe à $\mathbf{F}_p$.
   (e) Que peut-on en déduire pour l'idéal $\langle\lambda\rangle$?
6. On détermine ici la structure de $\mathbf{Z}[\zeta]^\times$. Le but est de démontrer que les éléments de $\mathbf{Z}[\zeta]^\times$ sont les $\zeta^r\varepsilon$, où $r \in \mathbf{Z}$ et ε est un réel inversible de $\mathbf{Z}[\zeta]$.
   Soit $u \in \mathbf{Z}[\zeta]^\times$.
   (a) Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbf{Z}[X]$ un polynôme unitaire de degré d, dont on note $\alpha_1, \ldots, \alpha_d$ les racines complexes comptées avec leur multiplicité. On suppose que pour tout $k \in \{1, \ldots, d\}$, α_k est de module 1.
      i. Montrer que pour tout $k \in \{0, \ldots, d\}$, on a $|a_k| \leqslant \binom{d}{k}$.
      En déduire qu'il n'existe qu'un nombre fini d'entiers algébriques de degré d dont tous les conjugués sont de module 1.
      ii. En déduire également que les racines de P sont des racines de l'unité.
      Indication : On pourra considérer les polynômes $P_n = \prod_{k=1}^{d}(X - \alpha_k^n)$, $n \in \boldsymbol{N}$, *dont on montrera qu'ils sont dans* $\boldsymbol{Z}[X]$.
   (b) Soit $P \in \mathbf{Z}[X]$ tel que $u = P(\zeta)$. Montrer que, pour tout $k \in \{1, \ldots, p-1\}$, $u_k = P(\zeta^k)$ est un conjugué de u, et que c'est un élément de $\mathbf{Z}[\zeta]^\times$.
   (c) Justifier que $\dfrac{u_1}{u_{p-1}}$ est un entier algébrique dont tous les conjugués sont de module 1.
   (d) En déduire qu'il existe $m \in \mathbf{Z}$ tel que $\dfrac{u_1}{u_{p-1}} = \pm\zeta^m$.
   (e) i. Soit $\theta \in \mathbf{Z}[\zeta]$. Justifier qu'il existe un entier $a \in \mathbf{Z}$ tel que $\theta = a \pmod{\langle\lambda\rangle}$. En déduire que deux éléments conjugués de $\mathbf{Z}[\zeta]$ sont égaux modulo $\langle\lambda\rangle$.
      ii. Démontrer que $\dfrac{u_1}{u_{p-1}} = \zeta^m$.
   (f) Justifier l'existence de $r \in \mathbf{Z}$ tel que $2r = m \pmod{p\mathbf{Z}}$. On pose $\varepsilon = \zeta^{-r}u$. Montrer que $\varepsilon \in \mathbf{R}$ et conclure.
7. Le but de ce qui suit est de montrer que $\mathfrak{O}_\mathbf{K} = \mathbf{Z}[\zeta]$.
   (a) Montrer que pour tout $\theta \in \mathfrak{O}_\mathbf{K}$, on a $\mathrm{N}(\theta) \in \mathbf{Z}$ et $\mathrm{Tr}(\theta) \in \mathbf{Z}$.
   (b) Soit $\theta \in \mathbf{K} = \mathbf{Q}(\zeta)$ un entier algébrique. Il existe des rationnels $a_0, \ldots, a_{p-2}$ tels que
   $$\theta = \sum_{k=0}^{p-2} a_k\zeta^k.$$
      i. Pour $k \in \{0, \ldots, p-2\}$, calculer $b_k = \mathrm{Tr}(\theta\zeta^{-k} - \theta\zeta)$ et justifier que $b_k \in \mathbf{Z}$.

ii. Montrer qu'il existe des entiers $c_0, c_1, \ldots, c_{p-2}$, que l'on exprimera en fonction des b_k, tels que $p\theta = \sum_{k=0}^{p-2} c_k \lambda^k$. Justifier ensuite que pour tout $k \in \{0, \ldots, p-2\}$

$$b_k = \sum_{\ell=k}^{p-2} (-1)^\ell \binom{\ell}{k} c_\ell.$$

iii. Montrer qu'il existe $\beta \in \mathbf{Z}[\zeta]$ tel que $p = \lambda^{p-1}\beta$. En déduire que $p \mid c_0$, puis que pour tout $k \in \{0, \ldots, p-2\}$, on a $p \mid c_k$. Conclure.

IV Le théorème de Fermat pour $p = 3$

On cherche à démontrer dans cette partie que l'équation

$$x^3 + y^3 + z^3 = 0 \tag{1}$$

n'a pas de solution entières non triviales, *i. e.*, telles que $xyz \neq 0$.

Soient x, y et z trois entiers relatifs tels que $x^3 + y^3 + z^3 = 0$.

1. On suppose que $3 \nmid xyz$. Montrer que x^3 vaut $+1$ ou $-1 \pmod 9$ et conclure à une impossibilité.

☛*On traite à présent le cas $3 \mid xyz$. Dans la suite de cette partie, on note $\lambda = 1 - j$ avec toujours $j = e^{\frac{2i\pi}{3}}$ et on suppose que les entiers x, y et z sont premiers entre eux dans $\boldsymbol{Z}[j]$ (et pas seulement dans $\boldsymbol{Z}$), cas auquel on peut se ramener en divisant par leur* `pgcd` *dans $\boldsymbol{Z}[j]$.* ☚

2. Montrer que 3 et λ^2 sont associés dans $\mathbf{Z}[j]$, ce que l'on a noté $3 \sim \lambda^2$.
3. Soit $s \in \mathbf{Z}[j]$ tel que $s \not\equiv 0 \pmod{\langle\lambda\rangle}$. Montrer qu'il existe $\varepsilon \in \{-1, +1\}$ tel que $s^3 = \varepsilon \pmod{\langle\lambda^4\rangle}$.
   Indication : On pourra remarquer que tout élément $s \in \boldsymbol{Z}[j]$ est congru à $-1, 0$ ou $1 \pmod{\langle\lambda\rangle}$.

☛*Par symétrie des rôles de x, y et z, on peut supposer que $3 \mid z$ (et donc $3 \nmid x$, $3 \nmid y$ puisqu'ils sont premiers entre eux). En particulier, on a $\lambda \mid z$, $\lambda \nmid x$ et $\lambda \nmid y$ dans $\boldsymbol{Z}[j]$.*
On note n la valuation en λ de z ; il existe donc $\mu \in \boldsymbol{Z}[j]$ premier avec λ tel que $z = \mu\lambda^n$, et par hypothèse $n \geqslant 1$. On a donc $x^3 + y^3 + \mu^3\lambda^{3n} = 0$.
La propriété suivante (qui pourra être utilisée sans plus de justification) est donc vérifiée :

$$(P_n) : \text{il existe } \alpha, \beta, \delta \in \mathbf{Z}[j] \text{ et } \omega \in \mathbf{Z}[j]^\times \text{ tels que } \begin{cases} \lambda \nmid \alpha\beta\delta, \\ \alpha \text{ et } \beta \text{ premiers entre eux,} \\ \alpha^3 + \beta^3 + \omega\lambda^{3n}\delta^3 = 0. \end{cases}$$

Nous allons montrer que si (P_n) est vérifiée, alors $n \geqslant 2$ et (P_{n-1}) est également vérifiée. ☚

4. Supposons (P_n) vérifiée pour un quadruplet $(\alpha, \beta, \delta, \omega)$. En considérant les valeurs de α^3, β^3 et $\omega\lambda^{3n}\delta^3 \pmod{\langle\lambda^4\rangle}$, montrer que $n \geqslant 2$.
5. Supposons (P_n) vérifiée pour un quadruplet $(\alpha, \beta, \delta, \omega)$. On montre dans cette question que (P_{n-1}) est également vérifiée.
   (a) Montrer que
   $$-\omega\lambda^{3n}\delta^3 = (\alpha + \beta)(\alpha + j\beta)(\alpha + j^2\beta).$$

(b) En déduire que λ divise chacun des facteurs $\alpha+\beta$, $\alpha+j\beta$ et $\alpha+j^2\beta$.

(c) Démontrer que λ est un `pgcd` de $\alpha+\beta$ et $\alpha+j\beta$. En déduire que λ^2 divise exactement l'un des éléments $\alpha+\beta$, $\alpha+j\beta$ ou $\alpha+j^2\beta$.

Quitte à remplacer β par $j\beta$ ou $j^2\beta$, on peut supposer que λ^2 divise $\alpha+\beta$. Il existe donc des éléments κ_1,κ_2 et κ_3 de $\boldsymbol{Z}[j]$ tels que $\lambda\nmid\kappa_1\kappa_2\kappa_3$ et

$$\begin{cases}\alpha+\beta=\lambda^{3n-2}\kappa_1,\\ \alpha+j\beta=\lambda\kappa_2,\\ \alpha+j^2\beta=\lambda\kappa_3.\end{cases}$$

(d) Montrer que $-\omega\delta^3=\kappa_1\kappa_2\kappa_3$ et en déduire qu'il existe des éléments γ_1,γ_2 et γ_3 de $\mathbf{Z}[j]$ tels que pour tout $\ell\in\{1,2,3\}$, $\kappa_\ell\sim\gamma_\ell^3$.

(e) Démontrer qu'il existe deux inversibles τ et τ' de $\mathbf{Z}[j]^\times$ tels que

$$\gamma_2^3+\tau\gamma_3^3+\tau'\lambda^{3(n-1)}\gamma_1^3=0.$$

(f) Montrer que si $\tau=\pm1$, alors (P_{n-1}) est vérifiée.

(g) Montrer que $\tau=\pm1\pmod{\langle\lambda^3\rangle}$, puis que $\tau\notin\{j,-j,j^2,-j^2\}$.

6. Conclure que l'équation (1) n'a pas de solution (x,y,z) dans le cas $3\mid xyz$.

V Le théorème de Fermat pour p régulier et $p\nmid xyz$

☛*On admet dans la suite que pour tout corps $\boldsymbol{K}$ de degré fini sur $\boldsymbol{Q}$, son anneau des entiers $\mathfrak{O}_{\boldsymbol{K}}$ vérifie la propriété suivante : tout idéal non nul de $\mathfrak{O}_{\boldsymbol{K}}$ s'écrit comme produit d'idéaux premiers, de manière unique à l'ordre près des facteurs.*
Dans ce contexte, on dit que deux idéaux I et J sont premiers entre eux *s'ils n'ont pas d'idéal premier en commun dans leur décomposition en produit d'idéaux premiers.*
*L'anneau $\boldsymbol{Z}[\zeta]$ qui est, d'après les résultats de la Partie **III**, l'anneau des entiers de $\boldsymbol{K}=\boldsymbol{Q}(\zeta)$ vérifie donc cette propriété de factorisation de ses idéaux.*
On suppose dans cette partie que $p>3$ est un nombre premier régulier*, ce qui signifie que si I est un idéal de $\boldsymbol{Z}[\zeta]$ tel que I^p est principal, alors I est lui même principal. On rappelle que l'on a noté $\lambda=1-\zeta$ et que certaines propriétés de l'idéal $\langle\lambda\rangle$ ont été étudiées en Partie **III**, question 5.*
On démontre dans cette partie que l'équation

$$x^p+y^p+z^p=0 \tag{2}$$

n'admet pas de solutions entières non triviales dans le cas où $p\nmid xyz$.
Par l'absurde, on se donne trois entiers $x,y,z\in\boldsymbol{Z}$ deux à deux premiers entre eux dans $\boldsymbol{Z}$, tels que $p\nmid xyz$ et qui vérifient l'équation (2). ☚

1. Montrer l'égalité d'idéaux
$$\prod_{k=0}^{p-1}\langle x+\zeta^k y\rangle=\langle z^p\rangle.$$

2. Soit deux entiers k et ℓ tels que $0\leqslant k<\ell\leqslant p-1$. On montre dans cette question que les idéaux $\langle x+\zeta^k y\rangle$ et $\langle x+\zeta^\ell y\rangle$ de $\mathbf{Z}[\zeta]$ sont premiers entre eux. Par l'absurde, soit $\mathfrak{P}$ un idéal premier divisant $\langle x+\zeta^k y\rangle$ et $\langle x+\zeta^\ell y\rangle$.

(a) En considérant $(x+\zeta^\ell y)-(x+\zeta^k y)$, montrer que $\lambda y\in\mathfrak{P}$.

(b) Montrer que $y\notin\mathfrak{P}$, en déduire que $x+y\in\langle\lambda\rangle\cap\mathbf{Z}$ et conclure à une absurdité.

3. Justifier l'existence d'un idéal I tel que $\langle x+\zeta y\rangle = I^p$.
4. Montrer qu'il existe $r \in \mathbf{Z}$, ε réel inversible de $\mathbf{Z}[\zeta]$ et $\alpha \in \mathbf{Z}[\zeta]$ tels que $x+\zeta y = \zeta^r \varepsilon \alpha^p$.
5. Montrer qu'il existe $a \in \mathbf{Z}$ tel que $\alpha^p = a \pmod{\langle p\rangle}$ (attention, ici $\langle p\rangle = p\mathbf{Z}[\zeta]$ et non $p\mathbf{Z}$) et en déduire que
$$x\zeta^{-r} + y\zeta^{1-r} - x\zeta^r - y\zeta^{r-1} = 0 \pmod{\langle p\rangle}.$$
6. Supposons que $r = 0 \pmod{p\mathbf{Z}}$. Montrer alors que $p \mid y$ dans $\mathbf{Z}$, ce qui est contraire à l'hypothèse.

On montrerait de même que l'on ne peut avoir $r = 1 \pmod{p\mathbf{Z}}$, ce que l'on admet.

7. D'après la question 5, il existe $\beta \in \mathbf{Z}[\zeta]$ tel que
$$x\zeta^{-r} + y\zeta^{1-r} - x\zeta^r - y\zeta^{r-1} = \beta p.$$
Montrer que deux des entiers $\pm r, \pm(1-r)$ sont égaux modulo p ; en déduire que $2r = 1 \pmod{p\mathbf{Z}}$.
8. Montrer que $\beta p\zeta^r = (x-y)\lambda$, puis que $x = y \pmod{p\mathbf{Z}}$.
9. Conclure à une absurdité.