Introduction et notations

On désigne par $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ l'anneau des nombres entiers relatifs, le corps des nombres rationnels, le corps des nombres réels et le corps des nombres complexes.

Soit A un anneau commutatif intègre. On dit que deux éléments α et β de A sont *premiers entre eux* s'ils n'ont pas d'autre diviseur commun que les éléments inversibles de A. Soit α un élément non nul, et non inversible de A ; on dit que α est un élément *irréductible* de A si une égalité $\alpha = \beta\gamma$ dans A implique que β ou γ est inversible dans A.

Rappelons que dans un anneau principal A, si un élément irréductible divise un produit, il divise un facteur. De plus, tout élément non nul et non inversible a de A est produit d'éléments irréductibles. L'écriture de a comme produit d'éléments irréductibles de A a la propriété suivante : si $a = p_1 p_2 \dots p_n$ et $a = q_1 q_2 \dots q_m$ sont deux écritures de a comme produit d'éléments irréductibles de A, alors $m = n$ et il existe une permutation σ de l'ensemble des entiers $\{1, \dots, n\}$, et des éléments inversibles ϵ_i, $1 \leqslant i \leqslant n$, de A tels que l'on ait $q_i = \epsilon_i p_{\sigma(i)}$ pour $1 \leqslant i \leqslant n$.

L'objectif de ce problème est d'étudier les solutions entières de quelques équations algébriques.

I . La relation $a^2 + b^2 = c^2$

1) Soit $M = (x, y)$ un point de $\mathbf{R}^2$. On suppose que l'on a $x^2 + y^2 = 1$, $x \geqslant 0$, $y \geqslant 0$. Soit $\theta \in [0, \pi/2]$ le nombre réel tel que

$$x = \cos\theta, \qquad y = \sin\theta.$$

On pose

$$t = \tan(\theta/2).$$

a) Exprimer x et y en fonction de t. En déduire que, si t est un nombre rationnel, x et y sont aussi des nombres rationnels.

b) Inversement, démontrer que, si x et y sont des nombres rationnels, t est aussi un nombre rationnel.

2) Soient a, b, c des nombres entiers > 0 et tels que

$$a^2 + b^2 = c^2.$$

On pose $x = a/c$, $y = b/c$; les nombres x et y sont rationnels et satisfont à l'égalité $x^2 + y^2 = 1$. Soit t le nombre défini dans la question (I.1). Le nombre t est rationnel et l'on a $0 < t < 1$.

a) On pose $t = v/u$, où u et v sont des nombres entiers positifs, premiers entre eux. Exprimer a/c et b/c en fonction de u et v.

b) Supposons que u et v aient des parités différentes. Démontrer que les nombres $2uv$, $u^2 + v^2$, $u^2 - v^2$ sont premiers entre eux deux à deux.

c) En déduire qu'il existe dans ce cas un entier w tel que

$$a = (u^2 - v^2)\,w, \qquad b = 2\,u\,v\,w, \qquad c = (u^2 + v^2)\,w.$$

d) Supposons maintenant que les nombres u et v soient tous deux impairs. Démontrer qu'il existe alors un entier w tel que

$$a = \frac{u^2 - v^2}{2}\, w, \qquad b = u\, v\, w, \qquad c = \frac{u^2 + v^2}{2}\, w.$$

e) En déduire qu'il existe dans ce cas des entiers u' et v', premiers entre eux et de parités dstinctes, tels que l'on ait

$$a = 2\, u'\, v'\, w, \qquad b = (u'^2 - v'^2)\, w, \qquad c = (u'^2 + v'^2)\, w.$$

3) Soient a, b, c des nombres entiers > 0 et tels que

$$a^2 + b^2 = c^2.$$

a) Démontrer que si les nombres a, b et c sont premiers entre eux dans leur ensemble, ils sont premiers entre eux deux à deux.

b) Supposons dans la suite que a et b sont premiers entre eux. Démontrer que a et b ne peuvent avoir la même parité. [On pourra remarquer que, si n est un entier impair, alors $n^2 \equiv 1 \pmod 4$].

c) Supposons toujours a et b premiers entre eux et supposons que b est pair. Démontrer qu'il existe des nombres entiers u et v, strictement positifs, premiers entre eux et de parités distinctes, satisfaisant aux relations

$$a = u^2 - v^2, \qquad b = 2\, u\, v, \qquad c = u^2 + v^2. \tag{A}$$

4) Dans cette question, on suppose donnés trois nombres entiers a, b, c, strictement positifs, premiers entre eux deux à deux et tels que

$$a^4 + b^4 = c^2.$$

Compte tenu de la question précédente, a et b ont des parités distinctes. De plus, en supposant que b est pair, il existe des nombres entiers u et v, strictement positifs, premiers entre eux et de parités distinctes, tels que

$$a^2 = u^2 - v^2, \qquad b^2 = 2uv, \qquad c = u^2 + v^2.$$

a) Démontrer que v est pair.

b) Démontrer l'existence de deux entiers x et y, strictement positifs, premiers entre eux, tels que $u = x^2$, $v = 2\, y^2$.

c) Établir la relation $a^2 + (2y^2)^2 = x^4$. En déduire l'existence de deux nombres entiers s et t strictement positifs, premiers entre eux, tels que $y^2 = st$, $x^2 = s^2 + t^2$.

d) Démontrer que s et t sont les carrés de nombres entiers > 0, $s = m^2$, $t = n^2$.

e) Vérifier que l'on a $m^4 + n^4 = x^2$ et $0 < x < c$.

f) En utilisant les résultats précédents, donner une démonstration de l'impossibilité de trouver trois nombres entiers a, b, c, strictement positifs, tels que $a^4 + b^4 = c^2$.

II . L'anneau $\mathbf{Z}[\mathrm{i}\sqrt{2}]$

On note $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ l'ensemble des nombres complexes $a+\mathrm{i}b\sqrt{2}$, où $a\in\mathbf{Z}$ et $b\in\mathbf{Z}$.

Pour tout nombre complexe z, on pose $\mathrm{N}(z)=z\overline{z}=|z|^2$.

Pour tous z et $z'\in\mathbf{C}$, on a $\mathrm{N}(zz')=\mathrm{N}(z)\,\mathrm{N}(z')$.

1) Démontrer que $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ est un sous-anneau de $\mathbf{C}$, commutatif et intègre.

2) a) Vérifier que pour tout élément α de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$, le nombre $\mathrm{N}(\alpha)$ est entier.

b) Démontrer que les éléments inversibles de l'anneau $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ sont les éléments α tels que $\mathrm{N}(\alpha)=1$.

c) Déterminer les éléments inversibles de l'anneau $\mathbf{Z}[\mathrm{i}\sqrt{2}]$.

3) Étant donnés deux éléments α et β, $\beta\neq 0$, de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$, démontrer qu'il existe γ et $\delta\in\mathbf{Z}[\mathrm{i}\sqrt{2}]$ tels que

$$\alpha=\beta\,\gamma+\delta \quad \text{et} \quad |\delta|<|\beta|.$$

[On pourra prouver l'existence de $\gamma\in\mathbf{Z}[\mathrm{i}\sqrt{2}]$ tel que $|\gamma-\frac{\alpha}{\beta}|<1$].

4) Démontrer que l'anneau $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ est principal.

5) Déterminer les diviseurs irréductibles de 2 dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$.

III . Somme et différence de deux carrés

Dans cette partie on utilise les résultats de la deuxième partie.

1) Soient m et n des entiers >0 et *premiers entre eux* dans $\mathbf{Z}$. On suppose que m^2+n^2 et m^2-n^2 sont des carrés dans $\mathbf{Z}$. Soient p et q des entiers $\geqslant 0$ tels que

$$m^2+n^2=p^2, \qquad m^2-n^2=q^2. \tag{B}$$

On a donc

$$2\,m^2=p^2+q^2, \qquad 2\,n^2=p^2-q^2. \tag{C}$$

a) En utilisant la question (I.3), démontrer que les parités de m et n sont distinctes et que p et q sont des nombres impairs.

b) Démontrer que q et n sont premiers entre eux.

c) Démontrer que n est pair et que m est impair.

2) Dans l'anneau $\mathbf{Z}[\mathrm{i}\sqrt{2}]$, on a $p^2=(q+\mathrm{i}\,n\sqrt{2})(q-\mathrm{i}\,n\sqrt{2})$. Dans cette question, on va démontrer que les deux facteurs sont premiers entre eux dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$. Pour cela, on raisonne par l'absurde en supposant qu'un élément irréductible π de $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ divise les deux facteurs.

a) Démontrer que π divise $2q$ et $2\mathrm{i}\,n\sqrt{2}$.

b) Démontrer que π ne peut être un diviseur commun à q et n dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$.

c) Démontrer que π ne divise pas 2 dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$. [On pourra utiliser la connaissance des diviseurs irréductibles de 2, question (II.5)].

d) Conclure.

3) a) Déduire de la question précédente que $q+\mathrm{i}\,n\sqrt{2}$ ou $-q+\mathrm{i}\,n\sqrt{2}$ est un carré dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$.

Dans le premier cas, on pose $q' = q$, dans le deuxième, on pose $q' = -q$.

b) On pose $q' + \mathrm{i}\, n\sqrt{2} = (f + \mathrm{i}\, g\sqrt{2})^2$, où f et g appartiennent à $\mathbf{Z}$. Démontrer que les entiers f et g sont premiers entre eux dans $\mathbf{Z}$ et que f est impair.

c) En remarquant que $m^2 = q^2 + n^2 = f^4 + 4\,g^4$, et en utilisant la question (I.3), démontrer l'existence de nombres entiers u et v, positifs, premiers entre eux, de parités distinctes, tels que

$$f^2 = u^2 - v^2, \qquad g^2 = uv.$$

d) Démontrer que u et v sont des carrés dans $\mathbf{Z}$.

e) Démontrer que $u + v$ et $u - v$ sont premiers entre eux dans $\mathbf{Z}$.

f) En posant $u = a^2$ et $v = b^2$, en déduire que $a^2 + b^2$ et $a^2 - b^2$ sont des carrés dans $\mathbf{Z}$.

g) Démontrer l'inégalité $a^2 + b^2 < m^2 + n^2$.

h) En utilisant ce qui précède, démontrer que la somme et la différence de deux carrés $\neq 0$ ne peuvent être toutes deux des carrés dans $\mathbf{Z}$.

5) Soit ABC un triangle rectangle en A dans un plan affine euclidien. On suppose que les longueurs de ses trois côtés sont des nombres entiers. Démontrer que l'aire du triangle ABC ne peut être égale au carré d'un nombre entier.

6) Démontrer que l'équation $x^4 - y^4 = z^2$ n'a pas de solution en nombres entiers tous $\neq 0$.

IV . La relation $x^3 - y^2 = 2$

On considère, dans le plan $\mathbf{R}^2$, la courbe C d'équation $x^3 - y^2 - 2 = 0$.

1) a) Soit $\mathrm{M}_0 = (x_0, y_0)$ un point de C. Écrire des équations paramétriques de la tangente T_0 à C au point M_0.

b) Déterminer les coordonnées des points communs à T_0 et à C.

c) Déterminer les points d'inflexion de la courbe C.

d) Déterminer les symétries éventuelles de C, ses branches à l'infini et les points d'intersection avec les axes de coordonnées.

e) Dessiner la courbe C dans la bande $0 \leqslant x \leqslant 4$ (prendre pour unité le centimètre, ou deux carreaux si la copie est quadrillée).

2) Déterminer les points à coordonnées entières de C situés dans la bande $0 \leqslant x \leqslant 4$.

3) On se propose de démontrer que les points trouvés dans la question (IV.2) sont les seuls points à coordonnées entières de la courbe C. Pour cela, on raisonne dans l'anneau $\mathbf{Z}[\mathrm{i}\sqrt{2}]$ introduit dans la partie II du problème.

On suppose que le point M, de coordonnées entières (x, y), appartient à la courbe C. On a donc

$$x^3 = (y - \mathrm{i}\,\sqrt{2})(y + \mathrm{i}\,\sqrt{2}).$$

a) Démontrer que les deux facteurs sont premiers entre eux dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$. [Procéder comme dans la question (III.2)].

b) En déduire que $y + \mathrm{i}\,\sqrt{2}$ est un cube dans $\mathbf{Z}[\mathrm{i}\sqrt{2}]$.

c) En écrivant $y + \mathrm{i}\sqrt{2} = (a + \mathrm{i}\, b\sqrt{2})^3$, discuter les valeurs possibles de a et b et conclure.

4) Soit P_0 l'un des points à coordonnées entières de la courbe C. On note P_1 le point où la tangente en P_0 à la courbe C recoupe la courbe C. Puis, pour tout entier $n \geqslant 1$, on note P_{n+1} le point où la tangente en P_n à la courbe C recoupe la courbe C.

a) Démontrer que les coordonnées x_n, y_n des points P_n sont rationnelles.

b) Démontrer que les points P_n sont tous distincts, de sorte que la courbe C possède une infinité de points à coordonnées rationnelles. [Pour cela, on pourra étudier l'exposant du facteur 2 dans la factorisation de l'un des nombres rationnels x_n ou y_n.]

V . L'équation $x^3 + y^3 = z^3$

On note j le nombre complexe $j = \frac{1}{2}(-1 + \mathrm{i}\sqrt{3})$.

On note $\mathbf{Z}[j]$ l'ensemble des nombres complexes $a + j\, b$, où a et b appartiennent à $\mathbf{Z}$.

On note π l'élément $1 - j$ de $\mathbf{Z}[j]$.

1) a) Démontrer que $\mathbf{Z}[j]$ est un sous-anneau de $\mathbf{C}$, commutatif et intègre.

b) Démontrer que, pour tout élément α de $\mathbf{Z}[j]$, le nombre $\mathrm{N}(\alpha)$ est entier.

c) Déterminer les éléments inversibles de $\mathbf{Z}[j]$.

d) Indiquer comment démontrer que $\mathbf{Z}[j]$ est un anneau principal.

e) Démontrer que l'élément $\pi = 1 - j$ est irréductible dans $\mathbf{Z}[j]$.

2) Soit α un élément de $\mathbf{Z}[j]$. Démontrer que deux cas seulement peuvent se présenter :

- ou bien π divise α,
- ou bien l'on a $\alpha^3 \equiv \pm 1 \pmod{\pi^4}$.

[On utilisera la division euclidienne de α par π et on pourra s'aider d'un dessin].

3) Soient α, β et γ des éléments de $\mathbf{Z}[j]$ tels que

$$\alpha^3 + \beta^3 + \gamma^3 = 0.$$

Démontrer que π divise l'un des éléments α, β ou γ.

4) Soient maintenant α, β, γ et ϵ des éléments de $\mathbf{Z}[j]$. On suppose que ϵ est inversible, que α, β et γ sont premiers entre eux deux à deux dans $\mathbf{Z}[j]$ et que π divise γ. On suppose enfin satisfaite l'égalité

$$\alpha^3 + \beta^3 + \epsilon\gamma^3 = 0.$$

a) Démontrer que π^2 divise γ.

b) On définit l'entier n en supposant que π^n divise γ mais que π^{n+1} ne divise pas γ. On a donc $n \geqslant 2$ d'après a). En écrivant l'égalité

$$-\epsilon\gamma^3 = (\alpha + \beta)(\alpha + j\beta)(\alpha + j^2\beta),$$

démontrer que π divise les trois facteurs, mais qu'un seul est divisible par π^2.

c) Démontrer que π est un PGCD des trois facteurs.

d) En déduire qu'il existe des éléments λ, μ, ν de $\mathbf{Z}[j]$, premiers entre eux deux à deux, non divisibles par π, et des éléments inversibles ϵ_1, ϵ_2, ϵ_3 tels que l'on ait

$$\alpha + \beta' = \epsilon_1 \, \pi \, \lambda^3, \qquad \alpha + j \, \beta' = \epsilon_2 \, \pi \, \mu^3, \qquad \alpha + j^2 \, \beta' = \epsilon_3 \, \pi^{3n-2} \, \nu^3,$$

où β' désigne l'une des racines cubiques de β^3, c'est-à-dire β, $j\beta$ ou $j^2\beta$.

e) En déduire qu'il existe des éléments inversibles η_1 et η_2 de $\mathbf{Z}[j]$ tels que l'on ait

$$\lambda^3 + \eta_1 \, \mu^3 + \eta_2 \, \pi^{3n-3} \, \nu^3 = 0.$$

f) Démontrer l'égalité $\eta_1 = \pm 1$.

5) En utilisant la question précédente, rédiger une démonstration du fait que l'équation $x^3 + y^3 = z^3$, où x, y, z sont tous $\neq 0$, n'a pas de solution dans $\mathbf{Z}$.
