CONCOURS GÉNÉRAL DES LYCÉES

SESSION DE 2001

COMPOSITION DE MATHÉMATIQUES

(Classe terminale S)

DURÉE : 5 heures

La calculatrice de poche est autorisée.
La clarté et la précision de la rédaction seront prises en compte dans l'appréciation des copies.

Les premières questions de chacune des quatre parties de ce problème sont indépendantes des autres parties. Il n'est donc pas obligatoire de commencer son étude dans l'ordre indiqué.

Les candidats peuvent admettre les résultats d'une question, à condition de l'indiquer clairement sur la copie.

On appelle **trio** tout triplet de nombres réels **(a,b,c)** non tous nuls et vérifiant la relation :

$$\mathbf{ab} + \mathbf{bc} + \mathbf{ca} = 0.$$

Lorsque $\mathbf{a} + \mathbf{b} + \mathbf{c} = 1$, on dit que le trio **(a,b,c)** est un trio **réduit**.

Les coordonnées sont rapportées à un repère orthonormal direct $(\mathbf{O}, \vec{\mathbf{I}}, \vec{\mathbf{J}}, \vec{\mathbf{K}})$ de l'espace.

Première partie

On note $\mathbf{C}$ l'ensemble des points de coordonnées **(a,b,c)** où **(a,b,c)** est un trio.
On note Γ l'ensemble des points de coordonnées **(a,b,c)** où **(a,b,c)** est un trio réduit.

On note $\mathcal{P}$ le plan d'équation $\mathbf{x}+\mathbf{y}+\mathbf{z}=1$.

1) Existe-t-il des trios **(a,b,c)** tels que $\mathbf{a}+\mathbf{b}+\mathbf{c}=0$?

2) Montrer que **C** est une réunion de droites passant par **O** et privées de ce point.

3) Montrer que Γ est l'intersection d'un plan et d'une sphère de centre **O**. Quelle est la nature géométrique de Γ ?

4) Donner la nature géométrique de **C** et l'illustrer par un croquis.

5) Soit **L** un point fixé de Γ. Montrer que le volume **V** du tétraèdre $\mathbf{O\,L\,L'\,L''}$, où $\mathbf{L'}$ et $\mathbf{L''}$ sont deux points distincts de Γ et différents de **L**, est maximal lorsque les arêtes issues de **O** sont deux à deux orthogonales et déterminer alors les coordonnées de $\mathbf{L'}$ et $\mathbf{L''}$ en fonction de celles de **L**.

6) Montrer que le produit **abc** admet un maximum et un minimum lorsque le point de coordonnées **(a,b,c)** décrit Γ. Préciser les trios réduits réalisant ces extrémums.

Deuxième partie

Dans cette partie et les suivantes, un trio **(a,b,c)** est dit **rationnel** lorsque **a**, **b** et **c** sont des nombres rationnels (éléments de l'ensemble $\mathbb{Q}$); il est dit **entier** lorsque **a**, **b** et **c** sont des nombres entiers relatifs (éléments de l'ensemble $\mathbb{Z}$) ; enfin un trio entier est dit **primitif** si **a**, **b** et **c** n'admettent que 1 et -1 comme diviseurs communs.

1) Déterminer la nature de l'ensemble $\mathbf{H}_1$ des points de coordonnées **(x,y,**1**)** tels que **(x,y,**1**)** soit un trio. Montrer que le point Ω_1 de coordonnées $(-1,-1,1)$ est un centre de symétrie de $\mathbf{H}_1$. Quels sont les points de $\mathbf{H}_1$ à coordonnées entières ?

2) Pour tout entier naturel non nul **h**, on note $\mathbf{Z}_h$ l'ensemble des trios entiers **(a,b,c)** tels que $\mathbf{c}=\mathbf{h}$. Déterminer $\mathbf{Z}_h$ pour $\mathbf{h}=1$ et $\mathbf{h}=2$.

3) Montrer que $\mathbf{Z}_h$ est un ensemble fini et exprimer le nombre $\mathbf{N(h)}$ de ses éléments en fonction de celui des diviseurs de $\mathbf{h}^2$ dans $\mathbb{Z}$. Montrer que 4 divise $\mathbf{N(h)}-2$.

4) Pour tout entier naturel non nul **h**, on note $\mathbf{N'(h)}$ le nombre de trios entiers **(a,b,c)** tels que l'un au moins des entiers **a**, **b** ou **c** soit égal à **h**. Exprimer $\mathbf{N'(h)}$ en fonction de $\mathbf{N(h)}$ selon la parité de **h**.

5) Montrer qu'à tout trio entier **(a,b,c)** on peut associer un triplet **(r,s,t)** d'entiers tels que **r** et **s** soient premiers entre eux, **s** positif ou nul, et tels que l'on ait :

$$\mathbf{a}=\mathbf{r}\,(\mathbf{r}+\mathbf{s})\,\mathbf{t}, \qquad \mathbf{b}=\mathbf{s}\,(\mathbf{r}+\mathbf{s})\,\mathbf{t}, \qquad \mathbf{c}=-\mathbf{r}\,\mathbf{s}\,\mathbf{t}.$$

Énoncer et démontrer une réciproque. Pour quels trios **(a,b,c)** le triplet **(r,s,t)** n'est-il pas unique ?

6) Déterminer les triplets $\mathbf{(r,s,t)}$ ainsi associés aux trios primitifs. En déduire que si $\mathbf{(a,b,c)}$ est un trio primitif, alors $|\mathbf{abc}|$, $|\mathbf{a+b}|$, $|\mathbf{b+c}|$ et $|\mathbf{c+a}|$ sont des carrés d'entiers.

7) Pour tout entier naturel non nul $\mathbf{h}$, on note $\mathbf{P(h)}$ le nombre de trios primitifs $\mathbf{(a,b,c)}$ tels que $\mathbf{c=h}$. Montrer que $\mathbf{P(h)}$ est une puissance de 2. Pour quels entiers $\mathbf{h}$ a-t-on $\mathbf{P(h)=N(h)}$? Expliciter une suite d'entiers $(\mathbf{h}_n)$ telle que la suite $\big(\mathbf{P(h}_n\mathbf{)/N(h}_n\mathbf{)}\big)$ converge vers zéro.

8) Soit $\mathbf{(a,b,1)}$ un trio. Montrer qu'il existe deux suites $(\mathbf{x}_n)$ et $(\mathbf{y}_n)$ convergeant respectivement vers $\mathbf{a}$ et $\mathbf{b}$ et telles que, pour tout $\mathbf{n}$, $(\mathbf{x}_n\mathbf{,y}_n\mathbf{,1})$ soit un trio rationnel.

9) Soit $\mathbf{(a,b,c)}$ un trio réduit. Montrer qu'il existe trois suites $(\mathbf{x}_n)$, $(\mathbf{y}_n)$ et $(\mathbf{z}_n)$ convergeant respectivement vers $\mathbf{a}$, $\mathbf{b}$ et $\mathbf{c}$ et telles que, pour tout $\mathbf{n}$, $(\mathbf{x}_n\mathbf{,y}_n\mathbf{,z}_n)$ soit un trio rationnel réduit.

Troisième partie

On note j le nombre complexe $\mathrm{e}^{2\mathrm{i}\pi/3}$, c'est-à-dire $-\dfrac{1}{2}+\mathrm{i}\,\dfrac{\sqrt{3}}{2}$.

Pour tout trio $\mathbf{T=(a,b,c)}$ on note $\widehat{\mathbf{T}}=\mathbf{(a,c,b)}$, $\mathbf{S(T)=a+b+c}$ et $\mathbf{z(T)=a+b\,j+c\,j^2}$.

1) Calculer le module de $\mathbf{z(T)}$ en fonction de $\mathbf{S(T)}$. Peut-on avoir $\mathbf{z(T)}=0$? Calculer le cosinus et le sinus d'un argument θ de $\mathbf{z(T)}$ en fonction de $\mathbf{a}$, $\mathbf{b}$ et $\mathbf{c}$.

2) Soit $\mathbf{z}_0$ un nombre complexe non nul. Déterminer les trios $\mathbf{T=(a,b,c)}$ tels que $\mathbf{z(T)=z}_0$.

3) Étant donnés deux trios $\mathbf{T}_1$ et $\mathbf{T}_2$, montrer qu'il existe un unique trio, noté $\mathbf{T}_1*\mathbf{T}_2$, vérifiant $\mathbf{S(T}_1*\mathbf{T}_2\mathbf{)=S(T}_1\mathbf{)S(T}_2\mathbf{)}$ et $\mathbf{z(T}_1*\mathbf{T}_2\mathbf{)=z(T}_1\mathbf{)z(T}_2\mathbf{)}$. Calculer $\mathbf{T}_1*\mathbf{T}_2$ en fonction de $\mathbf{T}_1$ et $\mathbf{T}_2$. Que peut-on dire d'un argument de $\mathbf{z(T}_1*\mathbf{T}_2\mathbf{)}$? Que peut-on dire d'un argument de $\mathbf{z(T}_1*\widehat{\mathbf{T}}_1\mathbf{)}$?

4) Si $\mathbf{T}_1$ et $\mathbf{T}_2$ sont réduits, en est-il de même de $\mathbf{T}_1*\mathbf{T}_2$? Si $\mathbf{T}_1$ et $\mathbf{T}_2$ sont entiers, en est-il de même de $\mathbf{T}_1*\mathbf{T}_2$? Si $\mathbf{T}_1$ et $\mathbf{T}_2$ sont primitifs, en est-il de même de $\mathbf{T}_1*\mathbf{T}_2$?

5) Comparer les trios $\mathbf{T}_1*\mathbf{T}_2$ et $\mathbf{T}_2*\mathbf{T}_1$, $(\mathbf{T}_1*\mathbf{T}_2)*\mathbf{T}_3$ et $\mathbf{T}_1*(\mathbf{T}_2*\mathbf{T}_3)$, $\mathbf{T}_1$ et $\mathbf{T}_1*(1,0,0)$.

6) Étant donnés les trios $\mathbf{T}_1$ et $\mathbf{T}_2$, résoudre l'équation $\mathbf{T}_1*\mathbf{T}=\mathbf{T}_2$ où le trio $\mathbf{T}$ est l'inconnue.

7) Étant donné un trio $\mathbf{T}$, on définit une suite de trios $(\mathbf{T}_n)$ par $\mathbf{T}_0=(1,0,0)$ et $\mathbf{T}_{n+1}=\mathbf{T}*\mathbf{T}_n$. Calculer $\mathbf{S(T}_n\mathbf{)}$. Étant donné un entier $\mathbf{p}$, résoudre l'équation $\mathbf{T}_p=\mathbf{T}_0$ où le trio $\mathbf{T}$ est l'inconnue.

Quatrième partie

On note $\mathbf{A}$ l'ensemble des entiers $\mathbf{m}$ non nuls tels qu'il existe deux entiers $\mathbf{u,v}$ tels que $\mathbf{m}=\mathbf{u}^2+3\,\mathbf{v}^2$.
On note $\mathbf{A}'$ l'ensemble des nombres complexes $\mathbf{z}$ non nuls tels qu'il existe deux entiers $\mathbf{u,v}$ tels que $\mathbf{z}=\mathbf{u}+\mathrm{i}\,\mathbf{v}\sqrt{3}$ (on remarquera que $|\mathbf{z}|^2=\mathbf{u}^2+3\,\mathbf{v}^2$).

On note $\mathbf{B}$ l'ensemble des entiers $\mathbf{n}$ non nuls tels qu'il existe deux entiers $\mathbf{r,s}$ tels que $\mathbf{n}=\mathbf{r}^2+\mathbf{rs}+\mathbf{s}^2$.

1) Montrer que le produit de deux éléments de $\mathbf{A}'$ appartient à $\mathbf{A}'$, puis que le produit de deux éléments de $\mathbf{A}$ appartient à $\mathbf{A}$.

2) Montrer que, si $\mathbf{p}$ est un nombre premier élément de $\mathbf{A}$, alors $\mathbf{p}=3$ ou 3 divise $\mathbf{p}-1$.

3) Montrer que $\mathbf{A}=\mathbf{B}$ (on pourra notamment remarquer que $\mathbf{r}^2+\mathbf{rs}+\mathbf{s}^2=(\mathbf{r}+\mathbf{s})^2-(\mathbf{r}+\mathbf{s})\,\mathbf{s}+\mathbf{s}^2$).

4) Montrer que 4 divise les éléments pairs de $\mathbf{A}$ et que les quotients appartiennent à $\mathbf{A}$, puis que tout élément de $\mathbf{A}$ est produit d'un élément impair de $\mathbf{A}$ par une puissance de 4.

5) **a**) Soit, s'il en existe, un entier impair $\mathbf{m}=\mathbf{u}^2+3\,\mathbf{v}^2$ tel que les entiers $\mathbf{u}$ et $\mathbf{v}$ soient premiers entre eux et qui admet un diviseur premier $\mathbf{p}$ n'appartenant pas à $\mathbf{A}$. Montrer qu'il existe alors un plus petit entier strictement positif $\mathbf{n}_0$ tel que $\mathbf{n}_0\,\mathbf{p}$ appartienne à $\mathbf{A}$. Montrer que $\mathbf{n}_0$ est impair.

b) Établir l'existence de deux entiers $\mathbf{u}'$ et $\mathbf{v}'$ inférieurs en valeur absolue à $\mathbf{p}/2$ tels que $\mathbf{p}$ divise $\mathbf{u}'-\mathbf{u}$ et $\mathbf{v}'-\mathbf{v}$. Montrer que $\mathbf{p}$ divise l'entier non nul $\mathbf{u}'^2+3\,\mathbf{v}'^2$ et que $\mathbf{n}_0<\mathbf{p}$.

c) Établir l'existence de deux entiers non nuls premiers entre eux $\mathbf{u}_0$ et $\mathbf{v}_0$ tels que $\mathbf{n}_0\,\mathbf{p}=\mathbf{u}_0^2+3\,\mathbf{v}_0^2$.

d) Établir l'existence de deux entiers $\mathbf{u}_1$ et $\mathbf{v}_1$ inférieurs en valeur absolue à $\mathbf{n}_0/2$ tels que $\mathbf{n}_0$ divise $\mathbf{u}_1-\mathbf{u}_0$ et $\mathbf{v}_1-\mathbf{v}_0$. Montrer que $\mathbf{n}_0$ divise l'entier non nul $\mathbf{u}_1^2+3\,\mathbf{v}_1^2$ que l'on notera $\mathbf{n}_0\,\mathbf{n}_1$.

e) En déduire qu'un tel entier $\mathbf{m}$ ne peut pas exister (on pourra considérer l'entier $\mathbf{n}_0^2\,\mathbf{n}_1\,\mathbf{p}$).

6) Montrer que tout élément de $\mathbf{A}$ s'écrit $\mathbf{m}=\mathrm{C}^2\ \mathbf{p}_1\ldots\mathbf{p}_k$ où C est un entier naturel non nul et les $\mathbf{p}_i$ des nombres premiers distincts éléments de $\mathbf{A}$.

7) **a**) Soient $\mathbf{p}$ un nombre premier tel que 3 divise $\mathbf{p}-1$, et $\mathbf{K}$ l'ensemble des triplets $(\mathbf{x,y,z})$ où les entiers $\mathbf{x}$, $\mathbf{y}$ et $\mathbf{z}$ sont strictement compris entre 0 et $\mathbf{p}$, et tels que $\mathbf{p}$ divise $(\mathbf{xyz}-1)$. Montrer que $\mathbf{K}$ possède $(\mathbf{p}-1)^2$ éléments, et que 3 divise le nombre d'éléments de $\mathbf{K}$ ne vérifiant pas $\mathbf{x}=\mathbf{y}=\mathbf{z}$.

b) En déduire qu'il existe un entier $\mathbf{x}$ strictement compris entre 1 et $\mathbf{p}$ tel que $\mathbf{p}$ divise $\mathbf{x}^2+\mathbf{x}+1$, puis que $\mathbf{p}$ appartient à $\mathbf{A}$. Décrire les éléments de $\mathbf{A}$.

8) Soit **D** l'ensemble des entiers **d** tels qu'il existe un trio entier **(a,b,c)** vérifiant $\mathbf{a}+\mathbf{b}+\mathbf{c}=\mathbf{d}$ et $\mathbf{abc}\neq 0$. Montrer, grâce à la question 5) de la deuxième partie, que tout élément de **D** possède un diviseur premier élément de **A**. Réciproquement, que peut-on dire d'un entier non nul admettant un diviseur premier élément de **A** ?

9) En déduire les éléments de **D** compris au sens large entre 2001 et 2010.

Corrigé abrégé

Première Partie

1) L'égalité $(a+b+c)^2 = a^2+b^2+c^2$ si $ab+bc+ca = 0$ montre que non.

2) C'est clair par homogénéité.

3) D'après la remarque du 1), la sphère annoncée est la sphère unité. Donc Γ est un cercle dans un plan perpendiculaire à la droite $x = y = z$.

4) En transformant Γ par toutes les homothéties possibles de centre O, on voit que C est un cône de révolution à deux nappes de sommet O, engendré par une droite passant par (et privée de) O et rencontrant Γ, d'axe la droite $x = y = z$, cône naturellement privé de son sommet O.

5) Les arêtes sont de longueur 1 d'après le 3). La formule donnant le volume V en fonction de l'aire A de la base $OL'L''$ et de la hauteur associée LH montre que le double de A et la hauteur étant toutes deux inférieures ou égales à 1, le volume ne peut dépasser $1/6$, ce maximum étant obtenu lorsque OL' et OL'' sont orthogonales et $H = O$, c'est-à-dire quand le tetraèdre $OLL'L''$ est formé de trois triangles rectangles isocèles et d'un triangle équilatéral. Si (a, b, c) sont les coordonnées de OL, celles de OL' et OL'' sont, au signe près, (b, c, a) et (c, a, b).

6) On veut $b + c = 1 - a$ et $bc = -a(b + c)$. Se donnant a, on voit que b et c sont racines de l'équation $x^2 - sx + p = 0$ avec $s^2 - 4p \geqslant 0$, ce qui impose la relation nécessaire et suffisante $(1-a)(1+3a) \geqslant 0$. Alors le produit abc vaut $a^3 - a^2$, dont les extremums valent 0 et $-4/27$. La valeur nulle 0 est obtenue pour les trois triplets analogues à $(0, 0, 1)$, alors que le maximum est obtenu pour les trois triplets analogues à $(-1/3, 2/3, 2/3)$.

Deuxième Partie

1) Il s'agit d'une hyperbole équilatère d'équation $(x+1)(y+1) = 1$; on peut aussi la reconnaître en mettant cette relation sous la forme $y = f(x)$. Il y a deux points à coordonnées entières, avec $x = y \in \{0, -2\}$.

2) D'après la première partie, $Z_1 = \{(0, 0, 1), (-2, -2, 1)\}$. Pour l'autre cas, on écrit la relation sous la forme $(x + 2)(y + 2) = 4$ et l'on cherche les diviseurs de 4 dans $\mathbb{Z}$ ce qui donne $Z_2 = \{(-1, 2, 2), (0, 0, 2), (2, -1, 2), (-3, -6, 2), (-4, -4, 2), (-6, -3, 2)\}$.

3) Par extension l'égalité $(x + h)(y + h) = h^2$ montre qu'il y a autant de couples (x, y) que de couples $(x + h), (y + h)$, donc que de diviseurs de h^2 dans $\mathbb{Z}$, et le double de ce nombre dans $\mathbb{N}$ puisque $h > 0$. Pour un diviseur d de h^2 dans $\mathbb{N}$, on peut lui associer le diviseur d' tel que $dd' = h^2$; en général d et d' sont distincts, sauf dans l'unique cas $d = d' = h$, ce qui montre que $N(h)/2$ est impair. (On peut aussi recourir à une expression explicite de $N(h)$ en fonction des exposants des diviseurs premiers de h^2, sur laquelle la propriété est évidente.)

4) Puisque (h,h,h) n'est pas un trio, on peut écarter ce triplet. Étudions le nombre ε de trios du type (x,h,h). Il est clair que $\varepsilon = 1$ si h est pair et 0 sinon : cela donne 3ε solutions en variant la place de h. Restent les cas où x et y sont tous les deux différents de h : le dénombrement donne facilement $3(N(h) - 2\varepsilon)$, ce qui donne finalement $N'(h) = 3N(h) - 3\varepsilon$, donc $3N(h) - 3$ si h est pair, $3N(h)$ sinon.

5) Écrivons toujours la relation fondamentale sous la forme $(a+c)(b+c) = c^2$. Puisque le triplet (a,b,c) n'est pas $(0,0,0)$, on peut introduire le PGCD $t \neq 0$ de a, b et c de façon que leurs quotients par t soient premiers entre eux. La relation de base s'écrit maintenant $\dfrac{c}{t}^2 = \dfrac{a+c}{t}\dfrac{b+c}{t}$. Or l'on prouve aussitôt que $\dfrac{a+c}{t}$ et $\dfrac{b+c}{t}$ sont également premiers entre eux; quitte à changer t en $-t$ pour que ces deux rationnels soient positifs, on montre facilement qu'il existe alors une décomposition $\dfrac{c}{t} = -rs$, avec r et s premiers entre eux avec $s \geqslant 0$ par exemple, telle que $\dfrac{a+c}{t} = r^2$ et $\dfrac{b+c}{t} = s^2$, soit enfin $a = r(r+s)t$, $b = s(r+s)t$ et $c = -rst$. L'existence est maintenant établie. De plus, les expressions données vérifient évidemment la relation de départ, ce qui fournit une réciproque simple sous forme de condition nécessaire et suffisante en y ajoutant naturellement la condition $t \neq 0$ pour éviter le triplet $(0,0,0)$.

Une autre façon de faire consiste à remarquer que les rationnels $1/a$, $1/b$ et $1/c$ ont une somme nulle, et sont donc proportionnels à des entiers premiers entre eux s, r et $-r-s$.

En ce qui concerne l'unicité, si $b \neq 0$, le couple (r,s) est évidemment unique, car $\dfrac{r}{s}$ n'est autre que la forme réduite du rationnel $\dfrac{a}{b}$ (c'est ici que $s > 0$ intervient) et t s'en déduit également de façon unique. Enfin si $b = 0$, on a $ac = 0$: si $c \neq 0$, il y a encore unicité du triplet (r,s,t) car alors $s = -r$ d'où $s = 1$ et $r = -1$; si $b = c = 0$, il y a par contre deux solutions en (r,s,t), à savoir $(1,0,a)$ et $(-1,0,a)$: l'unicité de (r,s,t) est donc "presque" générale, avec juste un contre-exemple dans un tout petit coin : celui des trios $(a,0,0)$.

6) Pour que le trio soit primitif, il est clair qu'il faut et suffit que $t^2 = 1$. Dès lors les quatre valeurs absolues concernées s'écrivent $r^2s^2(r+s)^2$, $(r+s)^2$, r^2 et s^2, et sont clairement des carrés.

N.B. Ainsi l'équation diophantienne $xy + yz + zx = 0$ est-elle très facile à résoudre avec des moyens élémentaires, et peut donc désormais rejoindre dans le panier des exercices "incoutournables" sa collègue très classique $x^2+y^2 = z^2$, remontant à la plus haute antiquité, et dont l'intérêt est historiquement insurpassable.

7) Ici l'unicité de (r,s,t) est vérifiée car $c \geqslant 0$. On veut $rx = \pm h$ avec r et s premiers entre eux et $s \geqslant 0$. La décomposition de h en facteurs premiers montre aussitôt que $P(h) = 2^{k+1}$ où k est le nombre de diviseurs premiers de h (même si $h = 1$). On n'a $P(h) = N(h)$ que pour $h > 1$ puisqu'alors $(0,0,h)$ est un trio non primitif. Enfin la suite $h_n = 2^n$ est telle que $P(h_n) = 4$ alors que $N(h_n) = 4n+2$ et répond visiblement à la demande.

8) Notons x_n une suite de rationnels distincts de -1 tendant vers a, lui-même distinct de -1 car $(a+1)(b+1) = 1$. Alors la suite de rationnels $y_n = -\dfrac{x_n}{1+x_n}$ est bien définie et converge vers $-\dfrac{a}{1+a} = b$ et est telle que $(x_n, y_n, 1)$ est un trio qui répond à la demande. Notons - cela sera utile pour le 9) - que $x_n + y_n + 1 = \dfrac{x_n^2 + x_n + 1}{1+x_n}$ n'est jamais nul.

9) Si $c = 0$ il suffit de prendre la suite constante $(a,b,0)$. Sinon, en considérant le trio $(a',b',1)$ et ses suites associées (x'_n, y'_n) par la question précédente, on constate que les suites définies

par $x_n = \dfrac{x'_n}{x_n+y_n+1}$, $y_n = \dfrac{y'_n}{x_n+y_n+1}$ et $z_n = \dfrac{1}{x_n+y_n+1}$ conviennent visiblement puisque $a'+b'+1 = \dfrac{1}{c}$.

Troisième partie

1) On a $2z(T) = (2a-b-c)+(b-c)\sqrt{3}$, d'où $|z(T)|^2 = a^2+b^2+c^2 > 0$. On retrouve ainsi que $|z(T)| = |S(T)| \neq 0$. On trouve $\cos\theta = \dfrac{2a-b-c}{2|a+b+c|}$ et $\sin\theta = \dfrac{(b-c)\sqrt{3}}{2|a+b+c|}$.

2) En posant traditionnellement $z_0 = x+iy$ et $s = S(T)$ il vient $3(a,b,c) = (s+2x, s-x+y\sqrt{3}, s-x-y\sqrt{3})$; puisqu'il s'agit d'un trio, on en déduit que $s^2 = x^2+y^2$ ce qui donne exactement deux choix possibles pour s et deux trios distincts solutions.

3) La question précédente montre qu'il existe deux trios T tels que $z(T) = z(T_1)z(T_2)$; nécessairement $|z(T)| = |z(T_1)||z(T_2)| = |S(T_1)||S(T_2)| = \varepsilon S(T_1)S(T_2)$. Il suffit de poser $T_1 * T_2 = \varepsilon T$ pour répondre à la question et cette solution est clairement unique. Le calcul explicite de $(a_1+b_1j+c_1j^2)(a_2+b_2j+c_2j^2)$ avec la simplification usuelle sur j et j^2 (à savoir $j^3=1$) donne les valeurs les plus "vraisemblables" de (a,b,c), à savoir $(a,b,c) = (a_1a_2+b_1c_2+c_1b_2, a_1b_2+b_1a_2+c_1c_2, a_1c_2+b_1b_2+c_1a_2)$ en considérant les coefficients de 1, j et j^2. Le calcul de vérification de la relation $S(a,b,c) = S(T_1)S(T_2) = (a_1+b_1+c_1)(a_2+b_2+c_2)$ est trivial. La somme, calculée modulo 2π par exemple, de deux arguments de T_1 et T_2 est un argument de $T_1 * T_2$ à cause de la relation $z(T) = z(T_1)z(T_2)$. Enfin un argument de $T_1 * \hat{T}_1$ est une différence de ceux de T_1 et T_1, donc 0 par exemple, puisque le passage de T_1 à $\hat{T}_1$ correspond à un passage au complémentaire pour $z(T_1)$. On peut en déduire par exemple que $T_1 * \hat{T}_1$ est de la forme $(a,0,0)$ ce qui se vérifie instantanément avec $a = s(T_1)^2 = a_1^2+b_1^2+c_1^2$.

4) Les formules explicites montrent que les deux premières réponses sont évidemment positives; pour la troisième, c'est non bien que trouver un contre-exemple demande un peu plus de travail; le plus simple d'entre eux est sans aucun doute le "carré" $(-1,2,2)*(-1,2,2) = (9,0,0)$ qui est non primitif.

5) Il s'agit chaque fois d'une égalité.

6) On trouve $T = \dfrac{1}{|z(T_1)|^2}\hat{T}_1 * T_2$.

7) On trouve $S(T_n) = S(T)^n$. Si $T_p = T_0$, nécessairement $S(T)^p = 1$. Si p est impair, il vient $S(T) = z(T)^p = 1$, soient p solutions avec $z(T) = \exp(2ik\pi/p)$; si p est pair, il en existe $2p$ avec cette fois-ci la possibilité supplémentaire $S(T) = -1$ qui introduit p nouvelles solutions opposées des précédentes.

N.B. Le lecteur curieux peut vérifier que cette loi $*$ munit le cône épointé C d'une structure de groupe commutatif, dont la restriction à Γ est tout simplement le groupe $O(2)$ des rotations de ce cercle (à cause de la propriété de sommation des arguments). On peut par exemple chercher dans le cas général la limite éventuelle de la suite (T_n) ou bâtir un modèle simple du groupe C à partir de $O(2)$ et $\mathbb{R}_+^*$.

On peut également obtenir d'autres lois de groupe intéressantes sur C ou une partie de C, par exemple en associant aux trios (a,b,c) et $(a',b'c')$ avec $cc' \neq 0$ le trio $(aa'+ac'+a'c, bb'+bc'+b'c, cc')$, pour laquelle une interprétation géométrique est également possible mais moins évidente. Par exemple, on peut dans ce cas

raccrocher cette loi à celle que l'on définit sur l'hyperbole H_1 d'équation $xy+x+y=0$, incluse dans C, en associant au couple $\big((x,y),(x',y')\big)$ le couple $(x",y")$ avec $x"+1=(x+1)(x'+1)$, $y"+1=(y+1)(y'+1)$, susceptible de nombreuses interprétations géométriques; on peut notamment vérifier ici que l'associativité de cette loi, un peu laborieuse à prouver à la main, est tout simplement une application du théorème de Pascal sur l'"hexagramme mystique" appliqué à l'hyperbole.

Quatrième partie

1) C'est clair puisque $zz' = (uu'-3vv')+i(uv'+u'v)\sqrt{3}$. Il suffit de passer aux carrés des modules pour obtenir que A est aussi fermé par rapport à la multiplication.

2) On a $3 = 0^2+3.1^2$. Si $p=u^2+3v^2$ avec $p=3n+2$, l'entier 2 peut alors s'écrire comme résidu d'un carré modulo 3, ce qui est exclu. Ou encore : si 3 ne divise pas u, il divise $u+1$ ou $u-1$, donc u^2-1 puis $p-1=u^2-1+3v^2$.

3) Tout $m\in A$ s'écrit $u^2+3v^2=(u+v)^2-2v(u+v)+(-2v)^2\in B$. Réciproquement, si $m=r^2+rs+s^2$, le cas r pair donne $m=\left(s+\frac{r}{2}\right)^2+3\left(\frac{r}{2}\right)^2\in A$; le cas s pair est analogue; enfin le cas r et s impairs convient également puisque l'égalité $m=(r+s)^2-s(r+s)+s^2=r'^2+r's'+s'^2$ est du type r' pair ce qui ramène au cas précédent.

4) Si m est un élément pair de $A=B$, il est facile de vérifier qu'il s'écrit $m=r^2+rs+s^2$ avec r et s également pairs, ce qui montre que $\frac{m}{4}\in B=A$. La seconde proposition s'en déduit aussitôt en considérant des divisions successives par 4 jusqu'à obtenir un non multiple de 4, qui est donc impair et élément de A (ce raisonnement pourrait être formalisé en recourant à la décomposition en facteurs premiers de m). La réciproque est claire puisque $4=2^2+3.0^2$ et que A est fermé pour la multiplication.

5) a) Il est généralement admis, comme étant intuitif, le fait que tout ensemble non vide d'entiers non nuls contient un élément minimum non nul n_0 (*une démonstration de ce fait ne peut être possible que dans le cadre d'une axiomatique comme celle de Dedekind, qui est clairement étrangère au contenu actuel des programmes de l'enseignement secondaire*). L'ensemble à considérer ici est celui des n tels que $np\in A$ qui contient $\frac{m}{p}$ mais non 1. (Pour être plus précis, il "suffit" ici de considérer les $\frac{m}{p}-2$ entiers de la forme $\frac{m}{p}-k>1$ et d'examiner - au moins théoriquement - si leurs produits par p appartiennent à A, ce qui permet d'échapper *(seulement en apparence)* à l'application explicite de la proposition ci-dessus tout en restant au niveau de la classe de Terminale.) Si n_0 était pair, 4 diviserait n_0p donc n_0 et $\frac{n_0}{4}$ appartiendrait à A, ce qui contredirait le caractère minimal de n_0.

b) Soit u' le plus petit (en valeur absolue) des nombres $u-kp$ où k décrit $\mathbb{Z}$: c'est soit le reste dans la division euclidienne de u par p, soit ce reste diminué de p. On a facilement $|u'|\leqslant\frac{p}{2}$, puis $|u'|<\frac{p}{2}$ puisque p est impair. Soit de même v'; p divise u^2+3v^2, donc $u'^2+3v'^2$, d'où $n_0\leqslant\frac{u'^2+3v'^2}{p}<\frac{4}{p}\left(\frac{p}{2}\right)^2=p$.

c) Puisque $n_0p\in A$ on peut écrire $n_0p=u_0^2+3v_0^2$ avec (u_0,v_0) entiers. Tout diviseur premier d commun à u_0 et v_0, s'il en existe, est tel que d^2 divise n_0p; ce ne peut être p puisque $n_0<p$;

donc d^2 divise n_0, mais c'est impossible puisqu'alors $\frac{n_0}{d^2}p = \left(\frac{u_0}{d}\right)^2 + 3\left(\frac{v_0}{d}\right)^2 \in A$. Donc u_0 et v_0 sont premiers entre eux.

d) On construit (u_1, v_1) comme u' et v' au b), en notant que n_0 est impair. Alors n_0 divise $u_1^2 + 3v_1^2$, nombre non nul puisque sinon n_0 diviserait u_0 et v_0 premiers entre eux, soit $n_0 = 1$ et $p \in A$ ce qui n'est pas.

e) Soit $0 < n_1 = \frac{u_1^2 + 3v_1^2}{n_0} < \frac{4}{n_0}\left(\frac{n_0}{2}\right)^2 = n_0$. On a $n_0^2 n_1 p = (u_0^2 + 3v_0^2)(u_1^2 + 3v_1)^2 = (u_0u_1 + 3v_0v_1)^2 + 3(u_0v_1 - u_1v_0)^2$ où n_0 divise $u_0v_1 - u_1v_0$ et $u_0u_1 + 3v_0v_1$, respectivement congrus modulo n_0 à $u_0v_0 - u_0v_0$ et $u_0^2 + 3v_0^2$ (a est dit congru à b modulo n si n divise $a - b$). Par suite $n_1 p = \left(\frac{u_0u_1 + 3v_0v_1}{n_0}\right)^2 + 3\left(\frac{u_0v_1 - u_1v_0}{n_0}\right)^2 \in A$, ce qui contredit enfin le caractère minimal de n_0 et ruine l'hypothèse ouvrant ce 5). Tout diviseur premier (et donc tout diviseur autre que 1) d'un nombre impair $u^2 + 3v^2 > 1$ où u et v sont premiers entre eux est aussi élément de A.

6) Par décomposition en facteurs premiers, tout entier est produit d'un carré et de k nombres premiers deux à deux distincts (k pouvant être nul). Si cet entier est dans A, ces nombres premiers sont impairs par le 4) et dans A par le 5). La réciproque est évidente par le 1).

7) a) Soit (x, y) l'un des $(p-1)^2$ couples d'entiers strictement compris entre 0 et p. Lorsque z décrit l'ensemble $\{1, 2, \ldots, p-1\}$, les restes des entiers $xyz - 1$ par division par p sont deux à deux distincts et différents de $p-1$ car p est premier et ne divise pas xy : chacune des valeurs entre 0 et $p-2$ est donc prise une fois et une seule. Il en résulte qu'il existe exactement un tel nombre z tel que p divise $xyz - 1$, ce qui donne bien $(p-1)^2 = 3q$ comme cardinal de K.

L'ensemble des triplets (x, y, z) de K ne vérifiant pas $x = y = z$ est formé de deux parties, celles pour lesquelles les ensembles $\{x, y, z\}$ sont de cardinal trois, et celles pour lesquelles il est de cardinal 2, les cardinaux de ces deux parties étant tout deux multiples de 3. Il en résulte que 3 divise également le cardinal de l'ensemble des triplets $(x, x, x) \in K$, ensemble non vide puisque contenant $(1, 1, 1)$.

b) Il en résulte qu'il existe un $x \in \{2, 3, \ldots, p-1\}$ tel que p divise $x^3 - 1 = (x-1)(x^2 + x + 1)$, donc tel que p, premier avec $x - 1 < p$, divise $x^2 + x + 1$ (c'est un cas particulier d'un théorème dû à Cauchy). Comme $x^2 + x + 1 \in B = A$, il en résulte que ses diviseurs premiers impairs sont dans A, et donc que $p \in A$. Finalement, les éléments de A sont exactement les nombres dont les diviseurs premiers impairs sont égaux à 3 ou de la forme $3n + 1$, et où l'exposant éventuel de 2 est pair.

N.B. Fermat écrivait le 25 septembre 1652 à Blaise Pascal : "Tout nombre premier, qui surpasse de l'unité un multiple de 3, est composé d'un quarré et du triple d'un autre quarré, comme 7, 13, 19, 41, 43 etc..." (41 est évidemment un lapsus calami *pour 37). Il écrira encore un peu plus tard, le 19 juin 1958, à Sir Kenelm Digby : "Omnis numerus primus qui unitate superat ternarii multiplicam, est compositus ex quadrato et triplo alterius quadrati. Tales sunt 4, 13, 19, 31, 37, 43, etc.". Cette proposition sera reprise en 1801 par Gauss : "Tout nombre premier de la forme $3n+1$, peut se décomposer en un quarré et le triple d'un quarré, et cela d'une seule manière" avec les décompositions explicites de 1, 7, 13, 19, 31, 37, 43, 61, 67 et 73 (l'unicité, non traitée ici, est facile); il la prouve, et cite Euler, premier mathématicien à en avoir proposé une démonstration en 1760, au fond peu éloignée de celle de ce problème, dont le point crucial - notre 5) - repose sur la célèbre méthode de descente infinie de Fermat.*

8) Nous savons que l'on peut alors écrire :

$$d = a + b + c = r(r+s)t + s(r+s)t - rst = (r^2 + rs + s^2)t = mt$$

avec $m = r^2 + rs + s^2$ où r et s sont premiers entre eux et tels que $rs(r+s)t \neq 0$. Puisque r et s ne peuvent être pairs ensemble, on peut supposer par exemple s impair et il en résulte que m est impair (étudier les deux restes possibles de r par division par 2) et que $m > 1$, car sinon on aurait $r^2 + rs + s^2 = 1$, soit $r = 0$ et $s = \pm 1$ ou $r = -s = \pm 1$, d'où $r(r+s) = 0$ ce qui n'est pas. De plus $4m = (2r+s)^2 + 3s^2 = u^2 + 3v^2 \in A$ avec u et v premiers entre eux, comme r et s car le PGCD de ces nombres ne peut qu'être 1 ou 2 et s est impair. Il résulte alors du 5) que $4m$, et par suite m lui-même, admet au moins au moins un diviseur premier impair p, donc de la forme $p = u^2 + 3v^2 \in A$.

Tout élément d de D admet donc au moins un diviseur premier $p \in A$, c'est-à-dire égal à 3 ou de la forme $3n+1$. Inversement, tout entier d admettant au moins un diviseur premier de ce type est élément de D, car le triplet :

$$(a,b,c) = \frac{d}{p}\big(2v(u+v), 2v(v-u), (u-v)(u+v)\big)$$

est alors un trio T vérifiant $S(T) = a+b+c = d$. Par exemple, 2001 est divisible par $p = 3 = 0^2 + 3.1^2$ et l'équation $a+b+c = 2001$ admet comme solution le trio $(1334, 1334, -667)$.

9) Les six entiers $\{2001, 2002, 2004, 2007, 2009, 2010\}$ sont dans D car chacun d'entre eux possède un diviseur premier appartenant à A, en l'occurence 3 ou 7; ce n'est pas le cas des quatre entiers $\{2003, 2005, 2006, 2008\}$ dont les diviseurs premiers impairs sont tous de la forme $3n+2$ (en l'occurence 17, 59, 251, 401 et 2003). Par exemple nous connaissons un trio $T = (a,b,c)$ tel que $a+b+c = S(T) = 2001$, alors qu'il n'en existe pas pour $a+b+c = 2003$. Déterminer tous les trios convenables relèverait d'un emploi intelligent de la calculette (l'application de la théorie précédente à de tels cas particuliers serait beaucoup plus longue).

N.B. Les questions formant cette quatrième partie explicitent donc un point de départ "élémentaire" vers les résolutions des équations diophantiennes équivalentes $x^2+3y^2 = n$ et $x^2+xy+y^2 = m$, déjà essentiellement connues de Fermat comme le prouvent ses Observations sur les remarques de Bachet concernant Diophante IV 11 et 12.