Eléments de Correction Concours Général 2001

Première Partie:

1. Remarquons que pour tout triplet de réels (a , b , c) on a :
   $(a + b + c)^2 = a^2 + b^2 + c^2 + 2(ab + bc + ca)$
   Donc, si ce triplet est un trio, en particulier, on doit avoir : $(a + b + c)^2 = a^2 + b^2 + c^2$.
   Comme a, b et c sont non tous nuls et réels, cela est donc impossible.
2. C'est évident si on remarque (a , b , c) est un trio si et seulement si pour tout réel non nul x, (xa , xb , xc) est aussi un trio.
   Donc, un point M(a , b , c) appartient à **C** si et seulement si la droite (OM) privée de O est dans **C**.
3. M(a , b , c) appartient à **Γ** si et seulement si on a :
   $\{a + b + c = 1$ et $ab + bc + ca = 0\}$.
   D'après l'égalité "$(a + b + c)^2 = a^2 + b^2 + c^2 + 2(ab + bc + ca)$", on a donc : $(a^2 + b^2 + c^2 = 1)$.
   Donc **Γ** est donc dans l'intersection du plan (P) d'équation $x + y + z = 1$ et de la sphère S d'équation:
   $x^2 + y^2 + z^2 = 1$.
   On vérifie sans peine la réciproque.
   Γ est donc l'intersection de (P) et de S, où S est la sphère unité. C'est donc un cercle situé dans un plan admettant le vecteur de coordonnées (1 ; 1 ; 1) comme vecteur normal.
4. D'après ce que l'on vient de dire, **C** est l'ensemble des points images de **Γ** par une homothétie h quelconque de rapport non nul. Autrement dit **,** comme **Γ** est un cercle, **C** est un cône de révolution de sommet O, mais privé de O, dont l'axe est une droite (D) passant par O et de vecteur directeur de coordonnées (1 ; 1 ; 1).
5. Il faut revenir au calcul du volume d'un tétraèdre.
   Si ABCD est un tétraèdre, alors le volume de celui-ci est : (1/6)||AB ^ AC||.DK où K est le projeté orthogonal de D sur le plan (ABC).
   Si L' et L" sont deux points distincts entre eux et de L de **G**, alors le volume du tétraèdre (OLL'L") est:
   Volume = (1/6)||OL' ^ OL"||LK où K est le projeté de orthogonal de L sur (OL'L").
   Mais comme L, L' et L" sont sur la sphère de centre O et de rayon 1, on voit alors que ce volume est $\leq$ (1/6).
   De plus, il ne peut être égal à (1/6) que si et seulement si ||OL' ^ OL"|| = 1 et LK = 1.
   Comme OL' = OL" = OL = 1, on obtient ces égalités que si OL' , OL" et OL sont orthogonales deux à deux.
6. On cherche les extrémums de abc sachant que (ab + bc + ca = 0 et a + b + c = 1).
   Or, on vérifie sans peine que $abc = a^3 - a^2$ dans ces conditions.
   Les variations de $(a^3 - a^2)$ sur l'intervalle [0 ; 1] montre alors que abc admet pour maximum 0 et pour minimum (-4/27).
   De plus, le maximum est atteint en (0 , 0 , 1) ou (0 , 1 , 0) ou (1 , 0 , 0)
   et le minimum est atteint en (2/3 , 2/3 , -1/3) ou (2/3 , -1/3 , 2/3) ou (-1/3 , 2/3 , 2/3).
   On obtient ces valeurs en revenant aux conditions portant sur (a , b , c) et se ramenant à une équation du second degré.

Eléments de Correction : Partie 2

1. $\mathbf{H_1}$ est l'ensemble des points M(a , b , 1) vérifiant ab + b + a = 0.
   Donc, b = -a/(a+1). (1)
   C'est donc une hyperbole (équilatère) dans le plan d'équation "z = 1".
   On sait que pour une hyperbole dans un plan, le point d'intersection des asymptotes est centre de symétrie.
   On voit sans problème que ce point est de coordonnées (-1 , -1 , 1).
   La relation (1) montre qu'un point de H1 est à coordonnées entières si et seulement si (a+1) divise a.
   Les seuls possibles pour a sont alors : a = 0 ou a = -2.
   Les points à coordonnées entières de $\mathbf{H_1}$ sont donc les points: A(0 , 0 , 1) ou B(-2 , 2 , 1).
2. L'ensemble $\mathbf{Z}_1$ est simplement l'ensemble **H1** étudié précédemment .
   L'ensemble $\mathbf{Z}_2$ est formé des trios de la forme (a , b , 2).
   On a donc : ab + 2b + 2a = 0 ce qui peut s'écrire (a+2)(b+2) = 4.
   Comme a et b sont entiers, et que la décomposition de 4 en facteurs premiers est : $4 = 2^2$, on peut alors dire que (a , b , 2) appartient à $\mathbf{Z}_2$ si et seulement si:
   {a+ 2 = 1 et b + 2 =4} ou {a+ 2 = -1 et b+2=-4 } ou {a+2 = 2 et b+2 = 2} ou
   {a+2 = -2 et b+2 = -2} ou {a+2 = 4 et b+2 = 1} ou {a+2 = -4 et b+2 = -1}
   Ce qui conduit alors aux trios appartenant à $\mathbf{Z}_2$:
   (1 , 2 , 2) ; (-3 , -6 , 2) ; (0 , 0 , 2) ; (-4 , -4 , 2) ; (2 , -1 , 2) ; (-6 , -3 , 2)
3. On peut généraliser ce qui vient d'être dit à un entier naturel h non nul en remarquant que:
   (ah + ba + ha = 0) si et seulement si $(a+h)(b+h) = h^2$.
   Donc, (a , b , h) appartient à $\mathbf{Z}_h$ si et seulement si (a+h) est un diviseur de h^2 et $b = h^2/(a+h) - h$.
   Comme h^2 a un nombre fini de diviseurs, on voit bien que $\mathbf{Z}_h$ est fini.
   De plus, à tout diviseur n de h^2 correspond un et un seul élément de $\mathbf{Z}_h$ qui est $(a = n-h , b = h^2/(a+h)-h , h)$.
   Il y a donc autant d'élément dans $\mathbf{Z}_h$ que de diviseurs (dans les entiers relatifs!) de h^2.
   Si on se place dans les diviseurs entiers naturels de h^2, on voit que:
   $\mathbf{N}(h) = \text{Cardinal}(\mathbf{Z}_h) = 2$ fois le nombre de diviseurs naturels de h^2.
   On connaît le nombre de diviseurs entiers naturels d'un entier quelconque positif en fonction de sa décomposition en facteurs premiers.
   Si $n = \Pi p_i^{ai}$, p_i parcourt l'ensemble des nombres premiers >0, alors
   n admet $\Pi(a_i+1)$ diviseurs dans IN.
   Or, la décomposition en facteurs premiers de h^2 est de la forme :
   $h^2 = \Pi p_i^{ai}$ où les ai sont des entiers pairs donc de la forme 2bi.
   Le nombre de diviseurs naturels de h^2 est alors: $\Pi(2b_i + 1)$
   On a donc , d'après le résultat précédent:
   $\mathbf{N}(h) = 2\,\Pi(2b_i + 1)$.
   Si on passe aux congruences modulo 4 , en développant $\Pi(2b_i + 1)$, on obtient :
   $\mathbf{N}(h) = 2(2b_1 + 2b_2 + \ldots + 2b_k + 1)$ modulo 4 ou encore $\mathbf{N}(h) = 2$ modulo 4
   On a bien alors $\mathbf{N}(h) - 2 = 0$ modulo 4 ou encore $\mathbf{N}(h) - 2$ divisible par 4.
4. Le cas (h , h , h) est exclu car on ne peut avoir h = 0.
   On étudie alors les deux cas suivants: "une seule valeur est égale à h" et "deux valeurs sont égales à h"
   Le cas (a , h , h) conduit à 2a = -h. Donc si h est impair, pas de solution, et si h et pair, 3 solutions possibles de la forme (a , h ,h) ; (h , a , h) ; (h , h , a).
   Le cas (a , b , h) a été traité dans sa généralité dans la question précédente.
   On en déduit alors que **N'(h) = 3N(h) ,** si h est impair: et **N'(h) = 3N(h) - 3 ,** si h est pair.
5. Un trio (a, b , c) vérifiant, par définition, la relation ab + bc + ca = 0 , comme
   $(a + c)(b + c) = ab + bc + ca + c^2$, (a , b , c) est un trio si et seulement si on a:
   $(a + c)(b + c) = c^2$. (relation 1)
   Remarquons aussi que ab + bc + ca = 0 implique que l'un au moins des entiers a , b , et c soit < 0.
   Disons que c'est c.
   Si (a , b , c) est un trio entier, posons alors t = PGCD(a , b , c). On vérifie alors sans peine que
   (a' , b' , c') où a = ta' , b = tb' et c = tc' est un trio primitif .
   De la relation (1) , on voit alors que $(c')^2 = (a' + c')(b' + c')$. Les entiers c' , (a' + c') et (b' + c') sont bien sur premiers entre eux. Posons alors R = (a' + c') et S = (b' + c').
   De $(c')^2 = R.S$, on en déduit que R et S sont de même signe. Quitte à changer les signes de a , b et c , on peut supposer que R et S sont > 0. Considérons alors r et s (entiers > 0) tels que $R = r^2$ et $S = s^2$.
   On obtient alors les relations:
   * $(a' + c') = r^2$ et $(b' + c') = s^2$ et $c' = -rs$ (c' est < 0)

   ou encore:
   * $(a + c) = tr^2$ et $(b + c) = ts^2$ et $c = -trs$

   d'où les relations : a = r(r+s)t ; b = s(r+s)t ; c = -rst
   On vérifie sans peine que si (a , b , c) est la forme précédente, on a bien à faire à un trio.
6. Le trio (a , b , c) est primitif si et seulement si t = 1. Les triplets (r , s , t) associés aux trios primitifs.
   Dans ce cas , on a :$|abc| = r^2s^2(r+s)^2$, $|a+b| = (r+s)^2$, $|b+c| = r^2$ et $|c+a| = s^2$
7. Si c = h > 0 , le trio associé (r , s , t) à (a , b , c) est unique. Comme le trio est primitif, on a t = 1.
   Les relations obtenues dans 5. montre alors que si N est le nombre de nombres premiers (1 inclus) intervenant dans la décomposition en facteurs premiers de h (ou de c) alors le nombre de choix pour le couple (r,s) est 2^N . Cela se voit en passant au nombre de parties d'un ensemble à N éléments.
   On a donc P(h) qui est bien une puissance de 2.
   De plus , on a P(h) = N(h) si h > 1.
   En prenant $h_n = 2^n$, on a $P(h_n) = 4$, $N(h_n) = 4n+ 2$. On obtient alors la limite demandée.

8. Remarquons que si (a , b , 1) est un trio alors a et b sont différents de -1.
Soit *x* un rationnel quelconque. Posons *y* = -x/(x+1) , qui est aussi un rationnel .
On vérifie que (x , y , 1) est aussi un trio.
De la relation (a+1)(b+1) = 1 , ou encore , b = -a/(a+1) , on en déduit que si une suite (xn) converge vers a alors la suite (yn = -xn(xn+1)) converge vers b. Comme tout réel a peut s'écrire somme limite d'une de rationnels, on en déduit qu'il existe bien deux suites (xn) et (yn) de rationnels convergeant respectivement vers a et b, et telles que (xn , yn , 1) soit un trio rationnel.
9. Si c = 0 , alors on a (a = 0 et b = 1) ou (a = 1 et b = 0). Dans ce cas, on choisit xn = a , yn = b.
Sinon , on divise a, b et c par c , en on obtient un trio (a' , b' , 1).
La question précédente permet alors de répondre à la question.

Troisième partie

On rappelle que $j^2 = \frac{1}{j} = \bar{j}$ et que $1 + j + j^2 = 0$.

1) $|z(T)|^2 = (a + bj + cj^2)\overline{(a + bj + cj^2)} = (a + bj + cj^2)(a + bj^2 + cj)$

$= a^2 + b^2 + c^2 + (ab + bc + ca)j^2 + (ab + bc + ca)j = a^2 + b^2 + c^2 = (a + b + c)^2$

d'où : $|z(T)| = |a + b + c| = |S(T)|$.

$z(T) = 0$ puisque cela entraînerait $S(T) = 0$ qui est impossible d'après la question 1) de la première partie.

$$\cos\theta = \frac{z(T) + \overline{z(T)}}{2|z(T)|} = \frac{2a + b(j + j^2) + c(j + j^2)}{2|z(T)|} = \frac{2a - b - c}{2|a + b + c|}$$

$$\sin\theta = \frac{z(T) - \overline{z(T)}}{2i|z(T)|} = \frac{b(i\sqrt{3}) - c(i\sqrt{3})}{2i|z(T)|} = \frac{(b - c)\sqrt{3}}{2|a + b + c|}.$$

2) Soit $z_0 = x_0 + iy_0$ un complexe non nul. Cherchons s'il existe des trios $T = (a\,;b\,;c)$ tels que $z(T) = z_0$.

Il faut donc que *a*, *b* et *c* vérifient $a + bj + cj^2 = z_0$ et donc aussi $a + bj^2 + cj = \overline{z_0}$ et $|z_0| = |a + b + c|$.

Par addition et soustraction des deux premières égalités, on obtient : $2a - b - c = 2x_0$ et $(b - c)\sqrt{3} = 2y_0$.

Supposons d'abord que $|z_0| = a + b + c$. En combinant les trois équations obtenues, on obtient

$a = \frac{|z_0| + 2x_0}{3}$, $b = \frac{|z_0| - x_0 + y_0\sqrt{3}}{3}$ et $c = \frac{|z_0| - x_0 - y_0\sqrt{3}}{3}$.

Pour vérifier qu'il s'agit bien d'un trio, il suffit de remarquer que $z_0 = a + bj + cj^2$ est bien vérifiée et donc les nombres *a*, *b* et *c* ne sont pas tous nuls puisque $z_0 \neq 0$ et d'autre part $|z_0| = a + b + c$ donc

$|z_0|^2 = (a + b + c)^2 = a^2 + b^2 + c^2 + 2(ab + bc + ca)$ mais aussi

$|z_0|^2 = a^2 + b^2 + c^2 + (ab + bc + ca)(j + j^2)$ d'où par soustraction $ab + bc + ca = 0$.

Supposons maintenant que $|z_0| = -a - b - c$.

On obtient ainsi une deuxième solution : $a = \frac{-|z_0| + 2x_0}{3}$, $b = \frac{-|z_0| - x_0 + y_0\sqrt{3}}{3}$ et

$c = \frac{-|z_0| - x_0 - y_0\sqrt{3}}{3}$.

Chaque nombre complexe non nul est donc ainsi associé à deux trios différents T' et T''.

On aura remarqué que $S(T')$ et $S(T'')$ sont opposés.

Si le trio T' est $(a\,;b\,;c)$, on peut éventuellement vérifier que

$$T'' = \left(\frac{a - 2b - 2c}{3}\,;\frac{-2a + b - 2c}{3}\,;\frac{-2a - 2b + c}{3}\right).$$

3) Soit $T_1 = (a_1\,;b_1\,;c_1)$ et $T_2 = (a_2\,;b_2\,;c_2)$ deux trios.

Formons le nombre complexe $z(T_1)z(T_2)$. Il est non nul comme produit de deux complexes non nuls. Il existe donc, d'après 2), deux trios T' et T'' tels que $z(T') = z(T_1)z(T_2)$ et $z(T'') = z(T_1)z(T_2)$.

On a donc $|z(T')| = |S(T')| = |z(T_1)z(T_2)| = |z(T_1)||z(T_2)| = |S(T_1)||S(T_2)| = |S(T_1)S(T_2)|$.

Les réels $S(T')$ et $S(T_1)S(T_2)$ ont la même valeur absolue : s'ils sont égaux, le seul trio vérifiant les deux égalités demandées est donc $T_1 * T_2 = T'$. Sinon, on aura $S(T_1)S(T_2) = -S(T') = S(T'')$ et donc $T_1 * T_2 = T''$.

$z(T_1) = a_1 + b_1 j + c_1 j^2$, $z(T_2) = a_2 + b_2 j + c_2 j^2$ d'où

$z(T_1)z(T_2) = (a_1 + b_1 j + c_1 j^2)(a_2 + b_2 j + c_2 j^2)$

$= (a_1a_2 + b_1c_2 + b_2c_1) + (a_1b_2 + b_1a_2 + c_1c_2)j + (a_1c_2 + c_1a_2 + b_1b_2)j^2$

Appelons T le triplet $\left(A = a_1a_2 + b_1c_2 + b_2c_1\ ; B = \left(a_1b_2 + b_1a_2 + c_1c_2\right); C = \left(a_1c_2 + c_1a_2 + b_1b_2\right)\right)$
On vérifie en développant que
$S(T_1)S(T_2) = \left(a_1 + b_1 + c_1\right)\left(a_2 + b_2 + c_2\right) = A + B + C$.
On a aussi :
$\left|\, z(T_1)z(T_2)\,\right| = \left|\, z(T_1)\,\right|\left|\, z(T_2)\,\right| = \left|\, S(T_1)\,\right|\left|\, S(T_2)\,\right| = \left|\, a_1 + b_1 + c_1\,\right|\left|\, a_2 + b_2 + c_2\,\right| = \left|\, A + B + C\,\right|$.
En procédant exactement comme dans la question 2), on prouve alors que T est bien un trio qui vérifie donc à la fois $S(T_1)S(T_2) = S(T)$ et $z(T_1)z(T_2) = z(T)$.
On en déduit que $T = T_1 * T_2$.

$z(T_1)z(T_2) = z(T_1 * T_2)$ donc un argument de $z(T_1 * T_2)$ s'obtient, à $2p$ près, en ajoutant un argument de $z(T_1)$ avec un argument de $z(T_2)$.
$z(T_1 * \hat{T}_1) = z(T_1)z(\hat{T}_1) = z(T_1)\overline{z(T_1)} = \left|\, z(T_1)\,\right|^2$ est un réel positif ; un de ses arguments est 0.

4) Si T_1 et T_2 sont réduits, alors $S(T_1) = 1$ et $S(T_2) = 1$ d'où $S(T_1 * T_2) = S(T_1)S(T_2) = 1$ et $T_1 * T_2$ est bien réduit.
Si T_1 et T_2 sont entiers, il est clair, d'après l'expression donnée en 3) de $T_1 * T_2$, que $T_1 * T_2$ est lui aussi entier.
Si T_1 et T_2 sont primitifs, $T_1 * T_2$ ne l'est pas forcément comme le montre le contre-exemple suivant :
$T_1 = T_2 = (2\ ;\ 2\ ;\ -1)$, $T_1 * T_2 = (0\ ;\ 9\ ;\ 0)$.

5) On vérifie directement sur la formule établie plus haut donnant $T_1 * T_2$:
$T_1 * T_2 = \left(A = a_1a_2 + b_1c_2 + b_2c_1\ ; B = \left(a_1b_2 + b_1a_2 + c_1c_2\right); C = \left(a_1c_2 + c_1a_2 + b_1b_2\right)\right)$ que
$T_1 * T_2 = T_2 * T_1$, ainsi que $T_1 * (1\ ;\ 0\ ;\ 0) = T_1$.
Pour établir l'égalité $(T_1 * T_2) * T_3 = T_1 * (T_2 * T_3)$, on utilise encore 2).
$z((T_1 * T_2) * T_3) = z(T_1 * T_2)z(T_3) = z(T_1)z(T_2)z(T_3)$ et de même $z(T_1 * (T_2 * T_3)) = z(T_1)z(T_2)z(T_3)$
et encore $S((T_1 * T_2) * T_3) = S(T_1 * T_2)S(T_3) = S(T_1)S(T_2)S(T_3)$ et
$S(T_1 * (T_2 * T_3)) = S(T_1)S(T_2)S(T_3)$. Comme on l'a vu dans 2), deux trios qui ont la même image par les applications z et S sont égaux : $(T_1 * T_2) * T_3 = T_1 * (T_2 * T_3)$.

6) L'équation $T_1 * T = T_2$ est équivalente aux deux équations $z(T_1 * T) = z(T_2)$ et $S(T_1 * T) = S(T_2)$, c'est -à-dire $z(T_1)z(T) = z(T_2)$ et $S(T_1)S(T) = S(T_2)$.
$z(T_1)$ n'étant pas nul d'après 1), $z(T) = \dfrac{z(T_2)}{z(T_1)}$. D'après 2), on sait qu'il y a exactement deux trios vérifiant cette égalité, puisque $\dfrac{z(T_2)}{z(T_1)}$ est un complexe non nul. De $z(T) = \dfrac{z(T_2)}{z(T_1)}$, on déduit $\left|\, z(T)\,\right| = \dfrac{\left|\, z(T_2)\,\right|}{\left|\, z(T_1)\,\right|}$ c'est-à-dire $\left|\, S(T)\,\right| = \dfrac{\left|\, S(T_2)\,\right|}{\left|\, S(T_1)\,\right|}$ ou $\left|\, S(T_1)S(T)\,\right| = \left|\, S(T_2)\,\right|$.
Les deux trios T concernés ont leur images par S opposées ce qui signifie que l'un d'eux vérifie bien $S(T_1)S(T) = S(T_2)$ mais que l'autre vérifie $S(T_1)S(T) = -S(T_2)$.
Nous venons de montrer que l'équation donnée admet toujours un trio solution unique.

Soit $T_1 = (a_1\ ;\ b_1\ ;\ c_1)$ et $T_2 = (a_2\ ;\ b_2\ ;\ c_2)$ deux trios.
Passons au calcul explicite du trio T solution unique de l'équation $T_1 * T = T_2$.
Il faut que :

$$z(T) = \frac{z(T_2)}{z(T_1)} = \frac{a_2 + b_2 j + c_2 j^2}{a_1 + b_1 j + c_1 j^2} = \frac{\left(a_2 + b_2 j + c_2 j^2\right)\left(a_1 + b_1 j^2 + c_1 j\right)}{\left(a_1 + b_1 j + c_1 j^2\right)\left(a_1 + b_1 j^2 + c_1 j\right)}$$

$$z(T) = \frac{a_1a_2 + b_1b_2 + c_1c_2}{a_1^{\ 2} + b_1^{\ 2} + c_1^{\ 2}} + \frac{a_1b_2 + b_1c_2 + c_1a_2}{a_1^{\ 2} + b_1^{\ 2} + c_1^{\ 2}}\, j + \frac{a_1c_2 + b_1a_2 + c_1b_2}{a_1^{\ 2} + b_1^{\ 2} + c_1^{\ 2}}\, j^2.$$

Il faut ensuite vérifier si le trio :
$T = \left(\dfrac{a_1a_2 + b_1b_2 + c_1c_2}{a_1^{\ 2} + b_1^{\ 2} + c_1^{\ 2}}\ ;\ \dfrac{a_1b_2 + b_1c_2 + c_1a_2}{a_1^{\ 2} + b_1^{\ 2} + c_1^{\ 2}}\ ;\ \dfrac{a_1c_2 + b_1a_2 + c_1b_2}{a_1^{\ 2} + b_1^{\ 2} + c_1^{\ 2}}\right)$ est bien celui cherché parmi les deux trios possibles qui correspondant à ce nombre complexe.

Pour ce faire, on doit examiner si l'égalité $S(T_1)S(T)=S(T_2)$ est vraie.
Or effectivement :

$$S(T_1)S(T)=(a_1+b_1+c_1)\left(\frac{a_1a_2+b_1b_2+c_1c_2+a_1b_2+b_1c_2+c_1a_2+a_1c_2+b_1a_2+c_1b_2}{a_1^{\ 2}+b_1^{\ 2}+c_1^{\ 2}}\right)$$

$$=(a_1+b_1+c_1)\frac{(a_1+b_1+c_1)(a_2+b_2+c_2)}{(a_1+b_1+c_1)^2}=a_2+b_2+c_2=S(T_2)$$

T est bien la solution cherchée.

7) Montrons par récurrence que : $S(T_n)=S(T)^n$ pour tout entier *n*.

$S(T_0)=1+0+0=1$; l'égalité est vraie pour $n=0$.

Supposons que l'égalité soit vraie pour un certain entier *n*

$S(T_{n+1})=S(T)S(T_n)=S(T)S(T)^n=S(T)^{n+1}$: l'égalité est donc vraie pour $n+1$.

D'après le principe de récurrence, l'égalité est vraie pour tous les entiers.

On obtient de façon similaire $z(T_n)=z(T)^n$.

Considérons maintenant l'équation : $T_p=T_0$. Elle équivaut à $S(T_p)=S(T_0)$ et à $z(T_p)=z(T_0)$, c'est-à-dire à $S(T)^p=1$ et $z(T)^p=1$.

<u>1er cas</u> : *p* est pair. Dans ce cas $z(T)^p=1$ entraînera $|z(T)|^p=|S(T)|^p=S(T)^p=1$ et donc tout trio pour lequel $z(T)$ est une racine p-ième de l'unité conviendra.

Il y a *p* racines p-ièmes de l'unité et chacune d'entre elles est l'image par *z* de deux trios.

Notre équation aura donc $2p$ solutions.

Plus précisément les racines p-ièmes de l'unité sont les complexes $z_k=\cos\left(\frac{2k\pi}{p}\right)+i\sin\left(\frac{2k\pi}{p}\right)$,

$0\le k<p$ et à chacune d'elles correspond les deux trios $(a_k\ ;b_k\ ;c_k)$: $a_k=\frac{1+2x_k}{3}$,

$b_k=\frac{1-x_k+y_k\sqrt{3}}{3}$ et $c_k=\frac{1-x_k-y_k\sqrt{3}}{3}$

et $\left(a_k'\ ;b_k'\ ;c_k'\right)$: $a_k'=\frac{-1+2x_k}{3}$, $b_k'=\frac{1-x_k+y_k\sqrt{3}}{3}$ et $c_k'=\frac{1-x_k-y_k\sqrt{3}}{3}$.

A titre d'exemple les trios solutions de l'équation $T_4=T_0$ sont $(1\ ;0\ ;0)$, $(-1\ ;0\ ;0)$, $\left(-\frac{1}{3}\ ;\frac{2}{3}\ ;\frac{2}{3}\right)$ et $\left(\frac{1}{3}\ ;-\frac{2}{3}\ ;-\frac{2}{3}\right)$.

<u>2ème cas</u> : *p* est impair. Dans ce cas $z(T)^p=1$ est nécessaire ainsi que $S(T)=1$.

Notre équation aura *p* solutions, à savoir les trios $(a_k\ ;b_k\ ;c_k)$: $a_k=\frac{1+2x_k}{3}$, $b_k=\frac{1-x_k+y_k\sqrt{3}}{3}$ et $c_k=\frac{1-x_k-y_k\sqrt{3}}{3}$ avec $x_k=\cos\left(\frac{2k\pi}{p}\right)$ et $y_k=\sin\left(\frac{2k\pi}{p}\right)$, $0\le k<p$.

A titre d'exemple les trios solutions de l'équation $T_3=T_0$ sont $(1\ ;0\ ;0)$, $(0\ ;1\ ;0)$ et $(0\ ;0\ ;1)$.

Quatrième partie

1) Soit $z = u + iv\sqrt{3}$ et $z' = u' + iv'\sqrt{3}$ deux éléments de A'.
Ils sont non nuls donc leur produit l'est également.
$zz' = \left(u + iv\sqrt{3}\right)\left(u' + iv'\sqrt{3}\right) = \left(uu' - 3vv'\right) + i\left(uv' + u'v\right)$. *u*, *v*, u' et v' étant des entiers, $uu' - 3vv'$ et $uv' + u'v$ sont bien des entiers.
Soit maintenant $m = u^2 + 3v^2$ et $m' = u'^2 + 3v'^2$ deux éléments de *A*.
En prenant les carrés des modules dans l'égalité précédente, on obtient
$mm' = \left(u^2 + 3v^2\right)\left(u'^2 + 3v'^2\right) = \left(uu' - 3vv'\right)^2 + 3\left(uv' + u'v\right)^2$ ce qui montre que mm' est un élément de *A*.

2) Soit *p* un nombre premier de *A*, donc de la forme $p = u^2 + 3v^2$, et supposons que *p* ne soit pas égal à 3.
u ne peut être un multiple de 3 sinon *p* serait un multiple de 3 autre que 3 et ne serait pas premier.
u peut donc être de la forme $u = 3q + 1$ ou $u = 3q + 2$.
Dans le premier cas, on obtient : $p - 1 = 3\left(3q^2 + 2q + v^2\right)$ et dans le deuxième :
$p - 1 = 3\left(3q^2 + 4q + 1 + v^2\right)$ ce qui termine la preuve.

3) Soit *m* un élément quelconque de *A*.
m s'écrit sous la forme $m = u^2 + 3v^2$, où *u* et *v* sont des entiers.
m peut aussi s'écrire $m = (u - v)^2 + (u - v)(2v) + (2v)^2$ ce qui montre que *m* est dans *B* puisqu'il s'écrit sous la forme $n = r^2 + rs + s^2$, où *r* et *s* sont les entiers $r = u - v$ et $s = 2v$.

Réciproquement soit *n* un élément quelconque de *B*.
n s'écrit sous la forme $n = r^2 + rs + s^2$, où *r* et *s* sont des entiers.
Si *s* est pair l'identité $r^2 + rs + s^2 = \left(r + \frac{s}{2}\right)^2 + 3\left(\frac{s}{2}\right)^2$ montre que *n* est bien dans *A*.

Si *r* est pair on utilisera l'identité : $r^2 + rs + s^2 = \left(r + \frac{s}{2}\right)^2 + 3\left(\frac{s}{2}\right)^2$.

Enfin si *r* et *s* sont tous deux impairs, fera : $r^2 + rs + s^2 = \left(\frac{s - r}{2}\right)^2 + 3\left(\frac{r + s}{2}\right)^2$.

4) Soit $m = u^2 + 3v^2$ un élément quelconque de *A*.
Si *m* est pair, il est impossible que *u* soit pair et *v* impair, ou que *u* soit impair et *v* pair.
Il reste à examiner deux cas.
Si *u* et *v* sont tous les deux pairs : $u = 2u'$, $v = 2v'$ et $m = 4\left(u'^2 + 3v'^2\right)$.
Si *u* et *v* sont tous les deux impairs : $u = 2u' + 1$, $v = 2v' + 1$ et $m = 4\left(u'^2 + 3v'^2 + u' + 3v' + 1\right)$.
Dans les deux cas, on a obtenu un multiple de 4.

Montrons par récurrence pour tous les entiers naturels non nuls la propriété $p(n)$ suivante :

Si *n* appartient à *A*, *n* s'écrit sous la forme $n = 4^k(2q + 1)$.
$p(1)$ est vérifié : 1 est dans *A*, mais s'écrit bien sous la forme demandée avec $q = k = 0$.
Supposons que pour un certain entier *n* la propriété soit vraie pour tous les entiers strictement inférieurs à *n* (hypothèse de récurrence) et examinons si la propriété reste vraie pour *n*.
Si *n* n'est pas dans *A*, il n'y a rien à démontrer, la propriété est vraie pour *n*.
Si *n* est dans *A* et *n* est impair, *n* s'écrit $n = 4^k(2q + 1)$ avec $k = 0$.
Si *n* est dans *A* et *n* est pair : $n = u^2 + 3v^2$ avec *u* et *v* de même parité.
En reprenant l'égalité $n = (u - v)^2 + (u - v)(2v) + (2v)^2$ écrivons : $\frac{n}{4} = \left(\frac{u - v}{2}\right)^2 + \left(\frac{u - v}{2}\right)v + v^2$. Cela montre que $\frac{n}{4}$ est un élément de *A*. Comme il est strictement inférieur à *n*, l'hypothèse de récurrence indique qu'il s'écrit sous la forme $\frac{n}{4} = 4^k(2q + 1)$, d'où $n = 4^{k+1}(2q + 1)$. Ceci termine la preuve par récurrence annoncée.

5) a) Supposons qu'il existe un entier *m* comme décrit dans l'énoncé. *m* est donc de la forme $m = kp$, k désignant un entier naturel non nul. L'ensemble *E* des entiers naturels non nuls *n* pour lesquels $np \in A$ n'est pas vide, puisque cet ensemble contient *k*. Soit n_0 le plus petit élément de *E*. (Tout ensemble non vide ne contenant que des entiers naturels a toujours un plus petit élément).

Supposons que n_0 soit pair. $n_0 p$ est donc pair et élément de *A*. D'après 4) $n_0 p$ est divisible par 4. Puisque *m* est impair, *p* est différent de 2 et, étant premier, est premier avec 4.

Le théorème de Gauss permet alors d'affirmer que n_0 est divisible par 4. De plus, il a été montré dans 4) que, dans ces conditions $\frac{n_0 p}{4} = \left(\frac{n_0}{4}\right)p$ appartient à *A*. La contradiction est que $\frac{n_0}{4}$ ne peut cependant appartenir à *E* puisque n_0 (> 0) est le plus petit élément de *E*.

On en déduit, par l'absurde, que n_0 est impair. Remarquons que $n_0 \neq 1$.

b) Soit $u = qp + r$, $0 \leq r < p$ la division euclidienne de *u* par *p*.

Si $0 \leq r < \frac{p}{2}$, on prendra $u' = r$ et $u' - u = -qp$ est bien un multiple de *p*.

Si $\frac{p}{2} \leq r < p$, on prendra $u' = r - p$ et $u' - u = -(q+1)p$ est bien un multiple de *p*.

Notons que *p* étant impair, $r = \frac{p}{2}$ est impossible et on a dans les deux cas $|u'| < \frac{p}{2}$.

On procède de manière similaire pour *v*.

L'égalité $u'^2 + 3v'^2 = (u'^2 - u^2) + 3(v'^2 - v^2) + (u^2 + 3v^2) = (u' - u)(u' + u) + 3(v' - v)(v' + v) + m$ montre que $u'^2 + 3v'^2$ est un multiple de *p* puisque les trois termes du membre de droite le sont.

$u'^2 + 3v'^2$ est un élément de *A* multiple de *p*, donc de la forme $u'^2 + 3v'^2 = kp$, *k* étant un élément de *E*.

De $|u'| < \frac{p}{2}$ et $|v'| < \frac{p}{2}$ on tire $kp = u'^2 + 3v'^2 < \frac{p^2}{4} + 3\frac{p^2}{4} = p^2$, d'où $k < p$.

Comme *k* est dans *E* et n_0 le plus petit entier de *E* : $n_0 \leq k < p$.

c) $n_0 p$ est un élément de *A* : il existe deux entiers u_0 et v_0 tels que $n_0 p = u_0{}^2 + 3v_0{}^2$.

Montrons par l'absurde que u_0 et v_0 sont premiers entre eux. S'ils ne l'étaient pas, ils seraient tous deux divisibles par un même nombre premier p'.

En reprenant l'égalité $n_0 p = (u_0 - v_0)^2 + (u_0 - v_0)(2v_0) + (2v_0)^2$ écrivons :

$$\frac{n_0 p}{p'^2} = \left(\frac{u_0}{p'} - \frac{v_0}{p'}\right)^2 + \left(\frac{u_0}{p'} - \frac{v_0}{p'}\right)\left(\frac{2v_0}{p'}\right) + \left(\frac{2v_0}{p'}\right)^2$$ qui est donc un entier de *A*.

Si $p' = p$, $\frac{n_0 p}{p'^2} = \frac{n_0}{p}$ serait un entier or $n_0 < p$ d'après 5)b) et ce cas est donc exclu.

Sinon *p* et p'^2 sont premiers entre eux. D'après le théorème de Gauss, puisque p'^2 divise $n_0 p$ et est premier avec *p* alors p'^2 divise n_0.

$\frac{n_0 p}{p'^2} = \left(\frac{n_0}{p'^2}\right)p \in A$ ce qui signifie que $\frac{n_0}{p'^2} \in E$, contredisant le caractère minimal de n_0 dans *E*.

u_0 et v_0 sont donc bien premiers entre eux.

Si l'un d'entre eux était nul, l'autre devrait valoir 1 (ou -1) ce qui donnerait $n_0 p = 1$ ou $n_0 p = 3$. Les deux sont impossibles car n_0 est un entier non nul et *p* un nombre premier qui n'est pas dans *A* (et qui donc est différent de 3).

d) La preuve est en tout point semblable à celle faite en 5) b).

e) De $|u_1| < \frac{n_0}{2}$ et $|v_1| < \frac{n_0}{2}$ on tire $n_0 n_1 = u_1{}^2 + 3v_1{}^2 < \frac{n_0{}^2}{4} + 3\frac{n_0{}^2}{4} = n_0{}^2$, d'où $n_1 < n_0$.

Remarquons ici que n_1 n'est pas nul car sinon on aurait $u_1 = v_1 = 0$ et u_0 et v_0 seraient tous les deux divisibles par n_0 (>1) ce qui est contradictoire avec le fait qu'ils sont premiers entre eux.

Considérons l'entier $n_0{}^2 n_1 p = \left(u_0{}^2 + 3v_0{}^2\right)\left(u_1{}^2 + 3v_1{}^2\right) = \left(u_0u_1 + 3v_0v_1\right)^2 + 3\left(u_0v_1 - v_0u_1\right)^2$.
Rappelons que $u_0 \equiv u_1 \ [\text{mod}.n_0]$ et $v_0 \equiv v_1 \ [\text{mod}.n_0]$ et donc que
$u_0u_1 + 3v_0v_1 \equiv u_0{}^2 + 3v_0{}^2 \equiv 0 \ [\text{mod}.n_0]$ et aussi que $u_0v_1 - v_0u_1 \equiv u_0v_0 - v_0u_0 \equiv 0 \ [\text{mod}.n_0]$.
Ces deux entiers étant divisibles par n_0, on pourrait donc écrire :
$n_1 p = \left(\dfrac{u_0u_1 + 3v_0v_1}{n_0}\right)^2 + 3\left(\dfrac{u_0v_1 - v_0u_1}{n_0}\right)^2 \in A$. Ceci signifie que $n_1 \in E$ constitue une contradiction avec l'inégalité $n_1 < n_0$ puisque n_0 est le plus petit entier de *E*.

6) On sait déjà qu'un élément *m* quelconque de *A* s'écrit sous la forme $m = 4^k(2q+1)$ avec $2q+1$ élément impair de *A*, qui peut donc lui-même s'écrire $2q+1 = U^2 + 3V^2$. Soit *D* le *PGCD* de *U* et de *V*. $U = Du$, $V = Dv$, *u* et *v* sont premiers entre eux.
$m = 4^r(2q+1) = 4^r D^2\left(u^2 + 3v^2\right) = \left(2^r D\right)^2\left(u^2 + 3v^2\right)$.
$u^2 + 3v^2$ est donc impair, u et v sont premiers entre eux et d'après 5), tous les facteurs de la décomposition de $u^2 + 3v^2$ en produit de facteurs premiers sont dans *A*.
En isolant les facteurs premiers qui interviennent avec un exposant impair dans la décomposition de $u^2 + 3v^2$ et en les nommant $p_1, p_2, \ldots p_k$, on peut alors écrire *m* sous la forme annoncée.

7) a) Choisissons pour *x* et pour *y* deux entiers quelconques strictement compris entre 0 et *p* et considérons l'équation $xyz - 1 = kp$ d'inconnues *k* et *z*. *p* est premier avec *x* et avec *y* donc avec leur produit. Le théorème de Bézout indique que cette équation admet au moins une solution $(z_0 \ ; k_0)$. On écrit alors
$xy(z - z_0) = (k - k_0)p$ et l'utilisation classique du théorème de Gauss montre que la solution générale de l'équation est $(z_0 + hp \ ; k_0 - hxy)$ où *h* désigne un entier quelconque. Il existe donc une solution $(z \ ; k)$ unique tel que $0 \le z < p$ (le reste de la division euclidienne de z_0 par p). On voit de plus d'après l'équation que *z* ne peut être nul.
Il y a donc autant de triplets $(x \ ; y \ ; z)$ solutions qu'il y a de choix pour $(x \ ; y)$, puisque à chaque couple $(x \ ; y)$ peut être complété par une valeur *z* unique.
Il y a donc $(p-1)^2$ solutions possibles. ($p-1$ choix possibles pour *x* et $p-1$ choix possibles pour *y*).
Le nombre total de solutions $(x \ ; y \ ; z)$ est donc $(p-1)^2$: $p-1$ étant un multiple de 3, $(p-1)^2$ est un multiple de 9.
Le nombre de solutions $(x \ ; y \ ; z)$ formées de trois entiers distincts est un multiple de 6.
En effet elles peuvent être regroupées par paquets de 6, $(x \ ; y \ ; z)$ se regroupant avec $(x \ ; z \ ; y)$, $(y \ ; z \ ; x)$, $(y \ ; x \ ; z)$, $(z \ ; x \ ; y)$ et $(z \ ; y \ ; x)$.
Les solutions formées de deux entiers distincts peuvent être regroupées par paquets de 3, comme $(x \ ; x \ ; y)$, $(x \ ; y \ ; x)$ et $(y \ ; x \ ; x)$.
Par soustraction le nombre des solutions restantes, qui sont celles de la forme $(x \ ; x \ ; x)$ est un multiple de 3.

b) Le nombre d'entiers *x* compris entre 1 et $p-1$ pour lesquels *p* divise $x^3 - 1 = (x-1)(x^2 + x + 1)$ est donc un multiple de 3. Un de ces entiers *x* est 1. Il y a au moins deux autres solutions. Mais si *x* est différent de 1, $0 < x - 1 < p - 2$ et $x - 1$ est premier avec p. D'après le théorème de Gauss *p* divise donc $x^2 + x + 1$.
Remarquons que $x^2 + x + 1 = x^2 + x1 + 1^2$ est un élément de *A*. De l'égalité $x < p - 1$, on déduit
$x^2 + x + 1 < (p-1)^2 + (p-1) + 1 < (p-1)^2 + 2(p-1) + 1 = p^2$.
p^2 ne divise donc pas $x^2 + x + 1$. D'après 6) *p* fait donc partie, dans l'écriture de $x^2 + x + 1$ sous la forme $C^2 p_1 p_2 \ldots p_k$, des nombres premiers $p_1, p_2, \ldots p_k$ qui interviennent dans cette écriture avec un exposant impair (en fait égal à 1) et qui sont tous dans *A*.

Ce qui précède montre que les nombres premiers de *A* sont exactement 3 et tous les nombres premiers de la forme $3q+1$.
Les éléments de *A* sont exactement les entiers naturels non nuls qui, dans leur décomposition en produit de facteurs premiers, ne font éventuellement intervenir des nombres premiers avec un exposant impair qui si ces nombres premiers sont de la forme $3q+1$ ou 3.

8) Soit un trio $(a\,;b\,;c)$ vérifiant $a+b+c=d$ et $abc\neq 0$.

D'après la question 5) de la deuxième partie, il existe un unique triplet $(r\,;s\,;t)$ d'entiers non nuls tels que *r* et *s* sont premiers entre eux, *s* est positif et tels que $a=r(r+s)t$, $b=s(r+s)t$ et $c=-rst$.

$a+b+c=(r^2+rs+s^2)t=d$; r^2+rs+s^2 est donc un élément de *A*.

On a vu dans 3) comment écrire r^2+rs+s^2 sous la forme u^2+3v^2 suivant la parité de *r* et de *s* : $r^2+rs+s^2=\left(r+\frac{s}{2}\right)^2+3\left(\frac{s}{2}\right)^2$, $r^2+rs+s^2=\left(s+\frac{r}{2}\right)^2+3\left(\frac{r}{2}\right)^2$ ou $r^2+rs+s^2=\left(\frac{s-r}{2}\right)^2+3\left(\frac{r+s}{2}\right)^2$.

Montrons que dans les trois cas les nombres *u* et *v* utilisés sont des entiers premiers entre eux. Examinons le premier cas : si un entier *k* divise $\frac{s}{2}$ et $r+\frac{s}{2}$, il divise aussi leur différence *r* et aussi $s=2\left(\frac{s}{2}\right)$ donc il ne peut valoir que 1 ou -1 puisque *r* et *s* sont premiers entre eux. $\frac{s}{2}$ et $r+\frac{s}{2}$ sont donc premiers entre eux.

Le deuxième cas étant semblable au premier, examinons le troisième : si un entier *k* divise $\frac{s-r}{2}$ et $\frac{r+s}{2}$, il divise aussi leur somme et leur différence, donc *r* et *s* ; il ne peut valoir que 1 ou -1 puisque *r* et *s* sont premiers entre eux. $\frac{s-r}{2}$ et $\frac{r+s}{2}$ sont donc premiers entre eux.

Remarquons aussi dans les trois cas : *r* impair et *s* pair, *r* pair et *s* impair ou *r* impair et *s* impair l'entier r^2+rs+s^2 est toujours impair. *r* et *s* ne sont pas simultanément pairs puisqu'ils sont premiers entre eux.

Finalement $r^2+rs+s^2=u^2+3v^2$ est un entier (positif) impair de *A* . Il ne peut être égal à 1 car la condition $abc\neq 0$ entraîne que $r\neq 0$, $s\neq 0$ et $r+s\neq 0$: aucune des expressions $\left(r+\frac{s}{2}\right)^2+3\left(\frac{s}{2}\right)^2$, $\left(s+\frac{r}{2}\right)^2+3\left(\frac{r}{2}\right)^2$ ou $\left(\frac{s-r}{2}\right)^2+3\left(\frac{r+s}{2}\right)^2$ ne peut valoir 1.

$r^2+rs+s^2=u^2+3v^2$ admet donc un diviseur premier *p* : le résultat de la question 5 montre que *p* est un élément de *A*.

p divise donc aussi $(r^2+rs+s^2)t=d$.

Réciproquement, si *d* $(\neq 0)$ a un diviseur premier *p* dans *A* : $d=d'p$, *p* peut donc s'écrire sous la forme $p=r^2+rs+s^2$. Les entiers *r* et *s* sont premiers entre eux car s'ils avaient un diviseur premier commun, $p=r^2+rs+s^2$ serait divisible par le carré de ce nombre premier, ce qui est impossible.

Quitte à remplacer l'égalité $p=r^2+rs+s^2$ par $p=(r+s)^2+(r+s)(-s)+(-s)^2$, on peut supposer que *s* est bien positif. Enfin d' est non nul (sinon *d* le serait).

Toutes les conditions sont donc réunies pour affirmer que le triplet $(a\,;b\,;c)$: $a=r(r+s)d'$, $b=s(r+s)d'$ et $c=-rsd'$ est un trio.

En résumé les éléments de *D* sont exactement les entiers non nuls divisibles par au moins un nombre premier de *A*. (On rappelle les nombres premiers de *A* sont exactement les nombres premiers de la forme $3q+1$ réunis avec le nombre 3).

9) La décomposition en facteurs premiers de ces nombres est :

$2001=3\times 23\times 29$, $2002=2\times 7\times 11\times 13$, 2003, $2004=2^2\times 3\times 167$, $2005=5\times 401$, $2006=2\times 17\times 59$, $2007=3^2\times 223$, $2008=2^3\times 251$, $2009=7^2\times 41$ et $2010=2\times 3\times 5\times 67$.

Les nombres de *D* parmi ces nombres sont 2001, 2002, 2004, 2007, 2009 et 2010 car ils sont divisibles par un nombre premier de *A* (3 ou 7). 2003, 2005, 2006 et 2008 en revanche ne sont pas dans *D* car tous leurs diviseurs premiers sont de la forme $3q+2$.