Résolution de l'équation diophantienne: $(ED)\ a^2 + 2b^2 + 3c^2 = 6abc$. Au fil des maths N°539, ex 539-2 page 77.

Patrick David (david@ensea.fr), Julien Sautier (sautier.julien@orange.fr)

Mai 2021

I. Notations et propriétés générales.

I.1.Position du problème.

L'équation (ED) rappelle l'équation diophantienne de Markov : $(EDM)\ a^2 + b^2 + c^2 = 3abc$.
L'équation de Markow a l'avantage de présenter une symétrie entre les variables. Elle se généralise avec les équations d'Hurwitz : $(EDH)\ \sum_{i=1}^{n} x_i^2 = k\prod_{j=1}^{n} x_j$. Le choix des coefficients de (ED) est judicieux. 1,2 et 3 sont les diviseurs de 6 ce qui permettra de rester dans $\mathbb{N}^{*3}$. Leur somme fait encore 6 (6 est parfait) ce qui a pour conséquence simple que le triplet $(1, 1, 1)$ est une solution.

I.2.Polynôme associé à (ED).

Résoudre (ED), revient à déterminer les triplets d'entiers relatifs qui sont des racines du polynôme P à trois indéterminées :
Notation: $P(x, y, z) = x^2+2y^2+3z^2-6xyz$.
Le premier membre de (ED) est positif ou nul, donc une solution (a, b, c) doit contenir un nombre pair d'entiers strictement négatifs. De plus si un des a, b, c est nul, les deux autres sont aussi nuls. En changeant les signes des termes négatifs et en supprimant la solution nulle, on peut donc se limiter sans perte de généralité aux solutions de (ED) de triplets d'entiers naturels non nuls.
Notation: $\mathcal{S}$ est l'ensemble des solutions de (ED) formées d'entiers naturels non nuls. $(1, 1, 1) \in \mathcal{S}$.
$\mathcal{S}^* = \mathcal{S}\backslash\{(1, 1, 1)\}$.

II.Construction des solutions.

II.1.Racines associées.

Soit $(a, b, c) \in \mathcal{S}$. Considérons les trois polynômes partiels de P à une indéterminée :
Notation: $P_{b,c}(x) = P(x, b, c)$,
$P_{a,c}(y) = P(a, y, c)$,
$P_{a,b}(z) = P(a, b, z)$.
a, b, c sont respectivement une des racines de ces trois polynômes du second degré.

Proposition 1: Pour $(a, b, c) \in \mathcal{S}^*$, $P_{b,c}(x)$, $P_{a,c}(y)$ et $P_{a,b}(z)$ ont chacun deux racines entières et strictement positives.

Démonstration:
$P_{b,c}(x) = x^2 - 6bcx + 2b^2 + 3c^2$
$P_{a,c}(y) = 2y^2 - 6acy + a^2 + 3c^2$
$P_{a,b}(z) = 3x^2 - 6abz + a^2 + 2b^2$.
Les trois polynômes ont par définition, une racine entière strictement positive (respectivement a, b, c). Comme la somme des racines de chaque polynôme est entière, strictement positive, et que le produit des racines est strictement positif, la seconde racine est également entière et strictement positive.
Notation: $\tilde{a}, \tilde{b}$ et $\tilde{c}$ sont les racines associées respectivement à a, b et c.

Proposition 2: Deux racines associées sont distinctes sauf dans le cas $a = b = 1$ alors $c = \tilde{c} = 1$.

Démonstration: Il suffit de montrer que les discriminants des trois polynômes sont strictement positifs. Notons $\Delta_{b,c}, \Delta_{a,c}$ et $\Delta_{a,b}$, les discriminants respectivement des polynômes $P_{b,c}, P_{a,c}$ et $P_{a,b}$.
Comme $a \geqslant 1, b \geqslant 1, c \geqslant 1$:

$\Delta_{b,c} = 4[9b^2c^2 - (2b^2 + 3c^2)]$
$\Delta_{b,c} = 4[2b^2(c^2 - 1) + 3c^2(b^2 - 1) + 4b^2c^2]$
$\Delta_{b,c} \geqslant 16.$
$\Delta_{a,c} = 4[9a^2c^2 - 2(a^2 + 3c^2)]$
$\Delta_{a,c} = 4[2a^2(c^2 - 1) + 6c^2(a^2 - 1) + a^2c^2]$
$\Delta_{a,c} \geqslant 4.$
$\Delta_{a,b} = 4[9a^2b^2 - 3(a^2 + 2b^2)]$
$\Delta_{a,b} = 4[3a^2(b^2 - 1) + 6b^2(a^2 - 1)]$
Si $a > 1$ ou $b > 1$,$\Delta_{a,b} \geqslant 4$
Si $a = 1$ et $b = 1$,$\Delta_{a,b} = 0$.

Corollaire 3: Si (a, b, c) est un élément de $\mathcal{S}^*$. $(\tilde{a}, b, c)$, $(a, \tilde{b}, c)$ et $(a, b, \tilde{c})$ sont trois autres solutions distinctes de (ED) et :
$\tilde{a} = 6bc - a$
$\tilde{b} = 3ac - b$
$\tilde{c} = 2ab - c.$

Démonstration: Ces relations proviennent de la somme des racines d'un polynôme du second degré.

II.2.Les opérateurs θ_i .

Définition: On définit trois opérateurs sur $\mathcal{S}$, notés θ_i, où $i \in [\![1, 3]\!]$, qui a un élément (a, b, c) de $\mathcal{S}$ associe le triplet obtenu en remplaçant la coordonnée à la position i par sa racine associée.

Proposition 4: Soit$(a, b, c) \in \mathcal{S}$, alors
$\theta_1[(a, b, c)] = (6bc - a, b, c)$
$\theta_2[(a, b, c)] = (a, 3ac - b, c)$
$\theta_3[(a, b, c)] = (a, b, 2ab - c).$

Démonstration: Déjà vu.

Théorème 5: Pour i et $j \in [\![1, 3]\!]$:
1. Les θ_i sont des applications de $\mathcal{S}$ dans $\mathcal{S}$.
2. Les opérateurs θ_i sont involutifs.
3. Pour $i \neq j$, $\theta_i \circ \theta_j \neq \theta_j \circ \theta_i$.
4. Si $s = (a, b, c) \in \mathcal{S}^*$, les quatre éléments $s, \theta_1(s), \theta_2(s)$ et $\theta_3(s)$ sont distincts.
5. $\theta_1[(1, 1, 1)] = (5, 1, 1)$,
$\theta_2[(1, 1, 1)] = (1, 2, 1)$ et
$\theta_3[(1, 1, 1)] = (1, 1, 1)$

Démonstration:
1.Par définition, les images sont aussi des éléments de $\mathcal{S}$.
2. Il est clair que par exemple $\tilde{\tilde{a}} = a$, d'où l'involution des opérateurs.
3. Par exemple :
$\theta_2 \circ \theta_1[(1, 2, 1)] = (11, 31, 1)$ et
$\theta_1 \circ \theta_2[(1, 2, 1)] = (5, 1, 1)$.
4. Dans ce cas, les racines et leurs racines associées sont distinctes.
5. Le calcul est évident.

Définition: Soit s une solution de (ED). On appellera $\theta_1(s), \theta_2(s), \theta_3(s)$ les solutions voisines de s.

II.3.Relation d'ordre sur $\mathcal{S}$.

L'ordre lexicographique induit sur $\mathcal{S}$ une structure d'ordre total. Cette relation d'ordre sera notée $\preccurlyeq$ et la relation d'ordre strict induite $\prec$.

Remarque:
1. $\forall s \in \mathcal{S}, (1, 1, 1) \preccurlyeq s$.
2. Si on remplace, dans $s = (a, b, c)$, a par a', avec $a < a'$, (resp. b par b', $b < b'$, c par c', $c < c'$) pour obtenir s' alors $s \prec s'$.

II.4.Solutions à composantes égales.

Pour la suite, il est nécessaire de déterminer les éléments de $\mathcal{S}$ ayant plusieurs composantes égales.

Proposition 6: Soient a, b, c trois entiers naturels non nuls distincts :
1. Si $(a, a, a) \in \mathcal{S}$, alors $(a, a, a) = (1, 1, 1)$.
2. Il n'existe pas d'élément de $\mathcal{S}$ de la forme (a, a, c).
3. Si $(a, b, b) \in \mathcal{S}$, alors $(a, b, b) = (5, 1, 1)$.
4. Si $(a, b, a) \in \mathcal{S}$, alors $(a, b, a) = (1, 2, 1)$.
5. Tous les autres éléments de $\mathcal{S}$, sont de la forme (a, b, c) avec a, b, c trois entiers naturels non nuls distincts.

Démonstration:
Nous notons $\mathbb{P}$ l'ensemble des nombres premiers.

Lemme: Soient x et y deux entiers naturels non nuls tels que $x^2 = y^2[(p + 1)x - p]$ où $p \in \mathbb{P} \cup \{1\}$ alors $y = 1$ et $x = 1$ ou $x = p$.
la démonstration de ce lemme est proposée dans l'Annexe mathématique de l'article.
1. $\forall a \in \mathbb{N}^*$, $P(a, a, a) = 6a^2(1 - a) = 0 \Rightarrow a = 1$.
2. $P(a, a, c) = 3a^2 + 3c^2 - 6a^2c$
$P(a, a, c) = 3a^2(1 - 2c) + 3c^2 = 0$
$\Leftrightarrow$ $c^2 = a^2(2c - 1)$.
D'après le lemme, nous en déduisons que $a = 1$ et $c = 1$.
3. $P(a, b, b) = a^2 + b^2(5 - 6a) = 0$

$\Leftrightarrow \; a^2 = b^2(6a-5)$.
D'après le lemme, nous en déduisons que $b=1$ et $a=1$ ou $a=5$
4. $P(a,b,a) = 2a^2(2-3b) + 2b^2 = 0$
$\Leftrightarrow b^2 = a^2(3b-2)$.
D'après le lemme, nous en déduisons que $a=1$ et $b=1$ ou $b=2$.
Nous vérifions que les triplets obtenus sont bien des solutions de (ED).

II.5.Solutions aux composantes distinctes.

Notation: Considérons une solution (a,b,c) dont les composantes sont distinctes 2 à 2. Nous notons : $u = \mathrm{Min}(a,b,c), w = \mathrm{Max}(a,b,c)$ et v le terme médian. Nous avons donc :
$\{a,b,c\} = \{u,v,w\}$, avec $u < v < w$.
Notons $\alpha_u, \alpha_v, \alpha_w$ les coefficients des termes u, v, w dans le polynôme P associé à (ED). Nous avons : $\{\alpha_u, \alpha_v, \alpha_w\} = \{1,2,3\}$.
Avec ces notations, $\alpha_u + \alpha_v + \alpha_w = \sigma = 6$ et $P(a,b,c) = \alpha_u u^2 + \alpha_v v^2 + \alpha_w w^2 - \sigma uvw$.
Nous considérons les opérateurs ψ_u, ψ_v, ψ_w. Par exemple, ψ_u est égal à l'opérateur θ_i où i est le rang de $u = \mathrm{Min}(a,b,c)$. Cette définition des opérateurs ψ est ambigüe si des composantes de la solution sont égales, ici, nous excluons ce cas. Enfin, toujours à partir du polynôme P de (ED), nous construisons trois polynômes à une indéterminée, $P_{v,w}$, $P_{u,w}$ et $P_{u,v}$, obtenus en remplaçant respectivement u, v, w par l'indéterminée x. Par exemple :
$P_{v,w}(x) = \alpha_u x^2 - \sigma vwx + \alpha_v v^2 + \alpha_w w^2$.
Les racines de $P_{v,w}$ sont u et $\tilde{u}$.

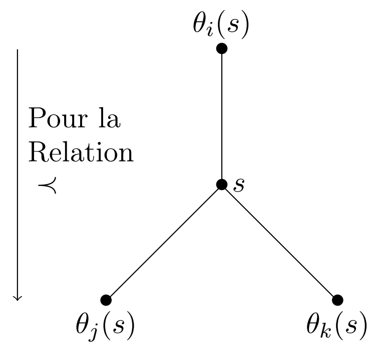
Théorème 7: Soit $s \in \mathcal{S}$ ayant ses trois composantes distinctes :
1. $s \prec \psi_u(s)$.
2. $s \prec \psi_v(s)$.
3. $\psi_w(s) \prec s$.

Démonstration: Un polynôme du second degré de concavité positive qui possède deux racines réelles a des valeurs négatives si et seulement si le polynôme est calculé pour une valeur comprise strictement entre ses racines.
1.$P_{v,w}(w) = \alpha_u w^2 - \sigma v w^2 + \alpha_v v^2 + \alpha_w w^2$.
Majorons strictement $\alpha_v v^2$ par $\alpha_v w^2$:
$P_{v,w}(w) < \alpha_u w^2 - \sigma v w^2 + \alpha_v w^2 + \alpha_w w^2$
$P_{v,w}(w) < \sigma w^2(1-v) < 0$. On en déduit que w est strictement compris entre les deux racines de $P_{v,w}$, u et $\tilde{u}$. Par définition, $u < w$, nécessairement $u < w < \tilde{u}$ et $s \prec \psi_u(s)$.
On procède de la même façon pour établir les propriétés (2) et (3).
2.$P_{u,w}(w) = \alpha_v w^2 - \sigma u w^2 + \alpha_u u^2 + \alpha_w w^2$.
Majorons strictement $\alpha_u u^2$ par $\alpha_u w^2$:
$P_{u,w}(w) < \alpha_v w^2 - \sigma u w^2 + \alpha_u w^2 + \alpha_w w^2$
$P_{u,w}(w) < \sigma w^2(1-u) \leqslant 0$. On en déduit que w est strictement compris entre les deux racines de $P_{u,w}$, v et $\tilde{v}$. Par définition, $v < w$, nécessairement $v < w < \tilde{v}$ et $s \prec \psi_v(s)$.
3. $P_{u,v}(v) = \alpha_w v^2 - \sigma u v^2 + \alpha_u u^2 + \alpha_v v^2$.
Majorons strictement $\alpha_u u^2$ par $\alpha_u v^2$:
$P_{u,v}(v) < \sigma v^2(1-u) \leqslant 0$.
Nous en déduisons que v est strictement compris entre les deux racines de $P_{u,v}$, w et $\tilde{w}$. Par définition, $v < w$, nécessairement $\tilde{w} < v < w$ et $\psi_w(s) \prec s$.

Remarque: La définition de ψ_u n'est pas possible pour les deux éléments $(1,2,1)$ et $(5,1,1)$ de $\mathcal{S}^*$ qui ont deux composantes égales. Néanmoins par un calcul direct on a aussi :
$s = (1,2,1)$,
$\theta_1(s) = (11,2,1)$, on a bien $s \prec \theta_1(s)$.
$\theta_3(s) = (1,2,3)$, on a bien $s \prec \theta_3(s)$.
$\theta_2(s) = (1,1,1)$, on a bien $\theta_2(s) \prec s$.
De même : $s = (5,1,1)$,
$\theta_2(s) = (5,14,1)$, on a bien $s \prec \theta_2(s)$.
$\theta_3(s) = (5,1,9)$, on a bien $s \prec \theta_3(s)$.
$\theta_1(s) = (1,1,1)$, on a bien $\theta_1(s) \prec s$.
$s = (1,1,1)$,
nous allons voir que s n'a pas de prédécesseur :
$\theta_1(s) = (5,1,1)$, on a bien $s \prec \theta_1(s)$.
$\theta_2(s) = (1,2,1)$, on a bien $s \prec \theta_2(s)$.
Mais exceptionnellement :
$\theta_3(s) = (1,1,1)$, on a bien $\theta_3(s) = s$.
Démonstration: Il suffit d'appliquer les définitions de θ_i :
$\theta_1((a,b,c)) = (6bc - a, b, c)$,
$\theta_2((a,b,c)) = (a, 3ac - b, c)$,
$\theta_3((a,b,c)) = (a, b, 2ab - c)$.

Corollaire 8: Tous les éléments s de $\mathcal{S}^*$ ont trois voisins distincts et distincts de

s. Un de ces voisins est un prédécesseur strict de s pour l'ordre lexicographique, et les deux autres sont des successeurs stricts de s. Le prédécesseur est $\theta_i(s)$, i est le rang de Max(s), les deux successeurs sont les deux autres $\theta_j(s)$ et $\theta_k(s)$.



Corollaire 9: Tout élément de $\mathcal{S}^*$ est l'image de $(1,1,1)$ par une succession d'opérateurs θ_i.

Démonstration: Soit une solution $(a,b,c) = s \in \mathcal{S}^*$. D'après le corollaire 8, il a un unique voisin qui est un prédécesseur strict pour l'ordre lexicographique et dont la somme des composantes est strictement inférieure à $a+b+c$. Nous sommes en présence d'une suite strictement décroissante d'éléments de $\mathcal{S}^*$ avec un nombre de termes inférieur à $a+b+c$. Cela s'arrête sur le dernier terme qui est $(1,1,1)$ et qui n'a pas de prédécesseur. Cette suite est unique car tout élément de $\mathcal{S}^*$ a un prédécesseur unique. On a donc :
$(1,1,1) = \theta_{i_n} \circ \theta_{i_{n-1}} \circ \cdots \circ \theta_{i_2} \circ \theta_{i_1}(s)$.
Comme les θ_i sont involutifs,
$s = \theta_{i_1} \circ \theta_{i_2} \circ \cdots \circ \theta_{i_{n-1}} \circ \theta_{i_n}((1,1,1))$.

Corollaire 10:
1. L'ensemble $\mathcal{S}$ est de cardinal infini.
2. Tout élément de $\mathcal{S}^*$ est en bijection avec une suite finie $(i_1, i_2, \cdots, i_n)$ telle que :
a) $i \in \{1,2\}$.
b) $\forall k \in [\![2,n]\!]$, $i_k \in \{1,2,3\}$.
c) $\forall k \in [\![2,n]\!]$, $i_{k-1} \neq i_k$.

Démonstration:
1.Soit une solution s dont les trois termes sont distincts deux à deux. Nous construisons la suite $s_{n+1} = \psi_u(s_n)$ et $s_0 = s$. D'après le théorème précédent la suite est strictement croissante.
2. Ceci résulte de la démonstration du Corollaire 9.

II.6.Une suite récurrente de $\mathcal{S}$.

Nous pouvons aussi montrer que le cardinal de $\mathcal{S}$ est infini en construisant dans $\mathcal{S}$ des suites à récurrence linéaires strictement croissantes. Soit $s = (a,b,c)$ un élément de $\mathcal{S}$, tel que l'une des deux composantes b ou c n'est pas égale à Max(a,b,c). Si c'est b, nous commençons par appliquer l'opérateur θ_2 à s. Si c'est c, nous commençons par θ_3. Dans ce qui suit, nous faisons l'hypothèse que la composante b n'est pas égale à Max(a,b,c), nous commençons par appliquer l'opérateur θ_2.
Nous considérons la suite récurrente (s_n) définie par :
$s_0 = (a,b,c)$,
$s_1 = \theta_2((a,b,c)) = (a,\tilde{b},c) = (a,-b+3ac,c)$
Nous avons vu que au théorème 7 que $s_0 \prec s$ et aussi que $\tilde{b} > \mathrm{Max}(a,b,c)$, donc nous composons s_1 par θ_3.
$s_2 = \theta_3((a,\tilde{b},c)) = (a,\tilde{b},\tilde{c})$
$s_2 = (a,-b+3ac,2a\tilde{b}-c)$
$s_2 = (a,3ac-b,2a(3ac-b)-c)$
$s_2 = (a,3ac-b,(6a^2-1)c-2ab)$.
Le même théorème permet d'affirmer que $s_1 \prec s_2$. Il en résulte que la suite définie par :
$s_0 = (a,b,c)$ et
$s_n = \theta_3 \circ \theta_2(s_{n-1})$ est strictement croissante.
La transformation est linéaire car a reste constant. La matrice de cette transformation linéaire est

$$T(a) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 3a \\ 0 & -2a & 6a^2-1 \end{pmatrix}.$$

Cette matrice a comme valeurs propres 1 et deux réels inverses l'un de l'autre. En particulier pour $(a,b,c) = (1,1,1)$, la matrice de l' application linéaire est :

$$T(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 3 \\ 0 & -2 & 5 \end{pmatrix}.$$

Ses valeurs propres sont : $\left(1, 2+\sqrt{3}, 2-\sqrt{3}\right)$.
Notons : $s_n = (a_n, b_n, c_n)$.

Proposition 11:
1. $S_{n+1} = TS_n$.
2. $\begin{cases} a_{n+1} &= a_n \\ b_{n+1} &= -b_n + 3c_n \\ c_{n+1} &= -2b_n + 5c_n \end{cases}$

(s_n) est une suite à récurrence linéaire. Les premiers termes de la suite sont $(1,1,1), (1,2,3), (1,7,11), (1,26,41)\ldots$ On a donc une infinité d'éléments de $\mathcal{S}$ comportant 1 en première position. On peut facilement généraliser pour avoir des suites ayant une infinité de 1 en deuxième ou troisième position. Si $(a,b,c) \in \mathcal{S}$, nous pouvons de même montrer qu'il existe des suites d'éléments de $\mathcal{S}$ ayant a constant en première position (respectivement b en deuxième position, ou c en troisième position).

III.Propriétés arithmétiques des solutions.

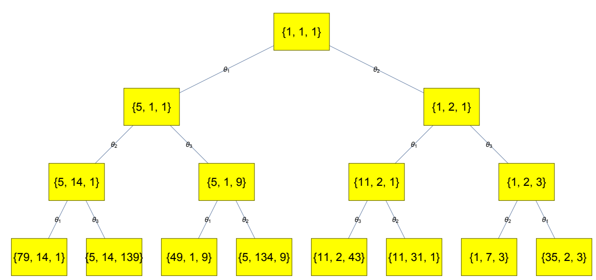
Proposition 12: Soit $(a,b,c) \in \mathcal{S}$,
(1) a est congru à $\pm 1 \mod 6$.
(2) b est congru à $\pm 1 \mod 3$. b n'est pas multiple de 3.
(3) c est congru à $1 \mod 2$. c est impair.

Démonstration:
D'abord l'élément $(1,1,1)$ possède les propriétés (1),(2) et (3).
Nous savons que toute solution est l'image par une suite finie d'opérateurs θ_i,
$i \in [\![1,3]\!]$, de $(1,1,1)$. On a donc une suite :
$s_0 = (1,1,1), s_1 = (a_1, b_1, c_1), \cdots,$
$s_n = (a_n, b_n, c_n) = (a,b,c)$.
1. On a vu au corollaire 3 que $\tilde{a} = 6bc - a$. Si $(a_{k+1}, b_{k+1}, c_{k+1}) = \theta_1((a_k, b_k, c_k))$, $a_{k+1} \equiv -a_k \mod 6$. Dans le cas contraire $a_{k+1} \equiv a_k \mod 6$. Nous avons donc un changement de signe « modulo 6 » à chaque usage de θ_1. Donc si $a \equiv 1 \mod 6$, il y a un nombre pair de θ_1 utilisés, et si $a \equiv -1 \mod 6$, il y a un nombre impair de θ_1 utilisés.
2.De même comme $\tilde{b} = 3ac - b$,
$b \equiv 1 \mod 3$ si un nombre pair de θ_2 est utilisé, et $b \equiv -1 \equiv 2 \mod 3$ si un nombre impair de θ_2 est utilisé.
3.Comme $\tilde{c} = 2ab - c$, $c \equiv 1 \mod 2$, c'est à dire c est impair.

IV.Représentation de $\mathcal{S}$ comme graphe.

IV.1.Définition du graphe.

On considère $\mathcal{S}$ comme l'ensemble des sommets d'un graphe simple non orienté. Deux éléments s et s' de $\mathcal{S}$ sont reliés par une arrête s'ils sont voisins. Autrement dit, deux éléments de $\mathcal{S}$ ont une arrête commune si et seulement s'il existe $i \in [\![1,3]\!]$ tel que $\theta_i(s) = s'$. On a ainsi un graphe simple $\mathcal{G}$. Nous allons montrer plus loin que $\mathcal{G}$ est un arbre binaire infini de racine $(1,1,1)$. Avec des calculs simples, on peut construire le début de ce graphe.



IV.2.Propriétés du graphe.

Proposition 13:
1. $\mathcal{G}$ est connexe.
2. $\mathcal{G}$ ne possède pas de cycle, c'est un arbre.
3. Tous les sommets sont de degré 3, sauf $(1,1,1)$ qui est de degré 2.
4. Le graphe $\mathcal{G}$ est un arbre binaire à racine unique $(1,1,1)$.

Démonstration:
1. Tout élément de $\mathcal{G}$ est relié à $(1,1,1)$ par une suite finie d'arrêtes. Deux sommets quelconques sont donc reliés. D'où la propriété de connexité du graphe.
2. Si un cycle existe, alors il admet au moins un sommet s qui est supérieur ou égal aux autres sommets du cycle pour la relation d'ordre lexicographique $\preccurlyeq$. Il doit être en particulier supérieur ou égal à ses deux voisins. Or nous avons vu au théorème 7 que tout sommet a au plus 3 voisins dont 2 sont strictement supérieurs à s. **3.** De même, ce

résultat a été obtenu dans la théorème 7.
4. Nous avons aussi démontré que tout sommet différent de $(1,1,1)$ a trois sommets voisins : deux qui lui sont plus grands et un qui lui est plus petit. Autrement dit, un sommet a exactement deux fils, les sommets voisins plus grands, et un père, unique, le sommet voisin plus petit.
$(1,1,1)$ est la racine de l'arbre binaire.

V.Généralisations possibles.

V.1.Le problème général.

Le problème traité est un cas particulier du problème plus général, trouver les solutions de l'équation diophantienne :

$$\sum_{i=1}^{n} \alpha_i x_i^2 = k \prod_{i=1}^{n} x_i.$$

Le cas traité concerne la situation :
(1) $n = 3$
(2) $(\alpha_1, \alpha_2, \alpha_3) = (1, 2, 3)$
(3) $\alpha_1 + \alpha_2 + \alpha_3 = 6 = \sigma = k$
(4) $\forall i \in [\![1, n]\!]\ , \alpha_i | k$
On peut envisager différents types de généralisations.

V.2.Généralisations semblables au cas étudié.

Le problème général avec n , α_i et k quelconques, semble assez difficile. On peut dans ce cas chercher des conditions sur k pour qu'il y ait au moins une solution. Les généralisations qui semblent suivre les méthodes vues précédemments sont de prendre :
(1) n quelconque
(2) Les α_i distincts et premiers entre eux
(3) $\sum_{i=1}^{n} \alpha_i = \sigma = k$
(4) $\forall i \in [\![1, n]\!]\ , \alpha_i | k$
Avec ces hypothèses, il semble qu'il n'y a rien de très intéressant pour $n = 2$ ou $n = 3$ autre que le cas étudié. Pour $n = 4$, l'équation diophantienne $a^2 + 2b^2 + 3c^2 + 6d^2 = 12abcd$ semble avoir des propriétés qui ressemblent à celle déjà étudiée. Pour $n = 5$, le fait que 28 soit un nombre parfait comme 6 pourrait faire que l'équation diophantienne
$a^2 + 2b^2 + 4c^2 + 7d^2 + 14e^2 = 28abcde$
ait aussi des propriétés qui ressemblent à l'équation déjà étudiée.

V.3.Généralisations avec k non nécessairement multiple ni somme des α_i.

Dans ce cas, $(1, 1 \cdots 1, 1)$ n'est pas nécessairement solution fondamentale, et une solution n'a pas nécessairement n voisins entiers.
Pour $n = 3$, on a :

Proposition 14:
Soit k entier naturel non nul, $(*)\ \sum_{i=1}^{3} \alpha_i x_i^2 = k \prod_{i=1}^{3} x_i$ admet pour solution (a, b, c) si et seulement si (ka, kb, kc) est solution de $(**)\ \sum_{i=1}^{3} \alpha_i x_i^2 = \prod_{i=1}^{3} x_i$.

Démonstration:
Il suffit de multiplier les deux membres de $(*)$ par k^2.

Corollaire 15:
Soit k entier naturel non nul tel que $(*)\ \sum_{i=1}^{3} \alpha_i x_i^2 = k \prod_{i=1}^{3} x_i$ n'admet aucune solution dans $\mathbb{N}^{*3}$, alors pour tout multiple k' de k, l'équation $\sum_{i=1}^{3} \alpha_i x_i^2 = k' \prod_{i=1}^{3} x_i$ n'a aucune solution dans $\mathbb{N}^{*3}$. .

Par exemple, on a trouvé par programme que l'équation
$x^2 + 2y^2 + 3z^2 = kxyz$ a des solutions pour $k \in \{1, 2, 3, 5, 6, 7, 9, 10, 11, 13, 14, 15, 17, 19, 22, 23, 25, 26, 29, 34, 38, 46, 50, 73\}$.
On peut conjecturer que pour $k \in \{4, 8, 12, 16, 18, 20, 21, 24, 27, 28, 30, 31, 32, 33, 35, 36, 37, 39, 40, 41, 42, 43, 44, 45, 47, 48, 49...\}$ l'équation $(*)$ n'a pas de solution. La recherche des k ne donnant pas de solution s'apparente au crible d'Erathostène et devrait donc avoir une répartition semblable à celle des nombres premiers.

Annexe mathématique.

Démonstration du lemme utilisé en II.4.

Lemme: Soient x et y deux entiers naturels non nuls tels que $(i)\ x^2 = y^2[(p + 1)x - p]$ où
$p \in \mathbb{P} \cup \{1\}$ alors $y = 1$ et $x = 1$ ou $x = p$.
Démonstration: Nous notons

$q=(p+1)x-p$. Avec cette notation :
(i) $x^2 = qy^2$
pgcd(x,q) = pgcd$(x,p) = \delta$. Comme p est un entier premier, $\delta = 1$ ou p.

- Si $\delta = 1$.

  .pgcd$(x,q) = 1$ donc pgcd$(x^2,q) = 1$ alors x^2 divise y^2, et $x \leqslant y$.

  .$x \geqslant 1$, alors $q \geqslant p$ et $qy^2 \geqslant py^2 \Rightarrow x \geqslant py$, d'où $x \geqslant y$.

  Les deux résultats précédents donnent $x = y = 1$.

- Si $\delta = p$. On pose $x = px'$, (i) se transforme en :

(ii) $px'^2 = y^2[(p+1)x'-1]$.
Posons $q' = [(p+1)x'-1]$.
(ii) $px'^2 = q'y^2$.

  .pgcd$(x',q') = 1$ d'où pgcd$(x'^2,q') = 1$ alors x'^2 divise y^2, et $x' \leqslant y$.

  .$x' \geqslant 1$, alors $q' \geqslant p$ et $q'y^2 \geqslant py^2$, $x' \geqslant py$ d'où $x' \geqslant y$.

  Les deux résultats précédents donnent $x' = y = 1$ et $x = p$.