L'équation d'Hurwitz

Christophe Rose

Mai 2006

Introduction

L'équation d'Hurwitz est ${x_1}^2 + \cdots + {x_n}^2 = kx_1 \cdots x_n$, pour n,$k \in \mathbb{N}^*$, avec $x_1 \ldots x_n \in \mathbb{N}^*$. Le but de cet article est de chercher — pour n donné — les valeurs de k pour lesquelles il existe au moins une solution. Nous commencerons par monter que k est compris entre 1 et n, puis nous verrons une méthode pour calculer les valeurs possibles pour k.

Lorsque $n = 3$ et $k = 3$, l'équation devient : ${x_1}^2 + {x_2}^2 + {x_3}^2 = 3x_1x_2x_3$, pour x_1, x_2, $x_3 \in \mathbb{N}^*$. On appelle ce cas particulier de l'équation d'Hurwitz, **l'équation de Markov**. L'ensemble de ses solutions a des propriétés particulières en théorie des nombres.

Table des matières

1 Étude générale

Avant de commencer à étudier cette équation, regardons pourquoi on ne prend pas $\mathbb{Z}$ au lieu de $\mathbb{N}^*$. La raison profonde est que le premier membre est toujours positif, et s'annule si et seulement si $x_1 = \cdots = x_n = 0$.

Si $(k,x_1 \dots x_n)$ est solution, $(|k|,|x_1| \dots |x_n|)$ aussi, et on obtient toutes les solutions dans $\mathbb{Z}$ à partir de celles dans $\mathbb{N}$ en multipliant un nombre pair de variables par (-1), et s'il y a un 0 parmi k, $x_1 \dots x_n$, alors $x_1 = \cdots = x_n = 0$.

Nous verrons plus tard que si — pour k fixé avec $n \geq 2$ — il y a au moins une solution, alors il y en a une infinité pour le même k. De fait, les seules choses intéressantes à chercher ne sont pas les solutions elles-mêmes mais les valeurs possibles de k pour lesquelles il existe au moins une solution ; et pour de telles valeurs, les solutions fondamentales, qui engendrent toutes les solutions. Nous verrons plus tard qu'il n'y a qu'un nombre fini de solutions fondamentales à k et n fixés, et comment engendrer toutes les solutions à partir des solutions fondamentales.

Tout d'abord, les cas $n = 1$ et $n = 2$ sont triviaux. Pour $n = 1$, l'équation devient : ${x_1}^2 = kx_1$, soit $x_1 = k$. Il existe donc une unique solution pour n'importe quel k fixé.

Pour $n = 2$, l'équation devient : ${x_1}^2 + {x_2}^2 = kx_1x_2$. Si on décompose $x_1 = ua$ et $x_2 = ub$ avec u le PGCD de x_1 et x_2 et a et b premiers entre eux, alors $a^2 + b^2 = kab$, donc a divise b^2, donc a divise 1, donc $a = 1$, et par le même raisonnement, $b = 1$. Donc $x_1 = x_2$, et l'équation devient $2{x_1}^2 = k{x_1}^2$, et k est forcément égal à 2.

Et si $k = 2$, alors ${x_1}^2 + {x_2}^2 = 2x_1x_2$ devient $(x_1 - x_2)^2 = 0$, qui a pour solutions les couples (u,u), quelque soit $u \in \mathbb{N}^*$. Conclusion : pour $n = 2$, il existe des solutions si et seulement si $k = 2$, et dans ce cas, il y a une infinité de solutions.

Supposons maintenant $n \geq 3$. Fixons $k \geq 1$ et considérons l'ensemble des solutions $(x_1 \dots x_n)$.

Par symétrie de l'équation, si $(x_1 \dots x_n)$ est une solution, $(x_{\sigma(1)} \dots x_{\sigma(n)})$ également pour n'importe quelle permutation $\sigma \in \mathfrak{S}_n$.

Une caractéristique fondamentale de l'équation, est que pour tout $i \in \{1 \dots n\}$, l'équation est du second degré en x_i. Mais comme la somme des deux racines du polynôme $X^2 + a_1X + a_0$ vaut $-a_1$, on en déduit que si $(x_1 \dots x_n)$ est une solution de l'équation de départ, alors c'est aussi le cas de :

$$(x_1 \dots x_{i-1},kx_1 \cdots \widehat{x_i} \cdots x_n - x_i,x_{i+1} \dots x_n)$$

La formule $\widehat{x_i}$ signifie qu'on omet le x_i. Ceci permet de créer une solution à partir d'une autre.

1.1 Solutions fondamentales

On suppose maintenant k et n fixés avec $n \geq 3$. On fera un abus de langage en disant que deux solutions sont les mêmes si l'une s'obtient par permutation de l'autre. On dira aussi que $(x_1 \dots x_n)$ est plus petite que $(y_1 \dots y_n)$ si en les ordonnant, la première est plus petite que la deuxième pour l'ordre lexicographique.

Soit $(x_1 \dots x_n)$ une solution. Pour tout $i \in \{1 \dots n\}$, les n-uplets de la forme $(x_1 \dots x_{i-1}, kx_1 \cdots \widehat{x_i} \cdots x_n - x_i, x_{i+1} \dots x_n)$ sont également des solutions, qu'on appellera les voisins. Une solution est dite fondamentale si elle est plus petite que tous ses voisins. Montrons qu'une solution a au plus un père, c'est-à-dire un voisin qui lui est plus petit.

Supposons par l'absurde qu'il existe une solution qui aie au moins deux pères. Alors on peut en prendre une qui est la plus petite pour l'ordre lexicographique, $(x_1 \dots x_n)$. Soit $(u_1 \dots u_n)$ l'un de ses pères. $(u_1 \dots u_n)$ est obtenu par permutation de $(x_1 \dots x_{i-1}, kx_1 \cdots \widehat{x_i} \cdots x_n - x_i, x_{i+1} \dots x_n)$, et on a forcément $kx_1 \cdots \widehat{x_i} \cdots x_n - x_i \leq x_i$, sinon $(u_1 \dots u_n)$ serait strictement plus grand que $(x_1 \dots x_n)$. Donc :

$$\begin{aligned} x_i &\geq kx_1 \cdots x_{i-1}x_{i+1} \cdots x_n - x_i \\ 2x_i &\geq kx_1 \cdots x_{i-1}x_{i+1} \cdots x_n \\ 2{x_i}^2 &\geq kx_1 \cdots x_n \\ 2{x_1}^2 &\geq {x_1}^2 + \cdots + {x_n}^2 \\ {x_i}^2 &\geq {x_1}^2 + \cdots + {x_{i-1}}^2 + {x_{i+1}}^2 + \cdots + {x_n}^2 \end{aligned}$$

On ne peut avoir que $i = n$. Donc $(u_1 \dots u_n)$ est une permutation du n-uplet $(x_1 \dots x_{n-1}, kx_1 \cdots \widehat{x_i} \cdots x_{n-1} - x_n)$. Contradiction.

On en déduit que toute solution est associée à une unique solution fondamentale. En effet, on prend une solution, et si elle n'est pas fondamentale, on prend son unique père, et on itère. Comme l'ordre lexicographique est un bon ordre, le procédé s'arrête.

1.2 Infinité des solutions à k fixé

On suppose maintenant qu'il existe au moins une solution à l'équation d'Hurwitz. Supposons par l'absurde qu'il n'y ait qu'un nombre fini de solutions. L'ordre lexicographique étant total, il existe une solution maximale $(x_n \dots x_1)$. Par maximalité de la solution, $x_1 \leq \dots \leq x_n$ et les calculs habituels montrent que :

$$\begin{aligned} x_1 &\geq kx_2 \cdots x_n - x_1 \\ 2x_1 &\geq kx_2 \cdots x_n \\ 2{x_1}^2 &\geq kx_1 \cdots x_n \\ 2{x_1}^2 &\geq {x_1}^2 + \cdots + {x_n}^2 \\ {x_1}^2 &\geq {x_2}^2 + \cdots + {x_n}^2 \end{aligned}$$

Ce qui est absurde vu que $n \geq 3$.

1.3 Étude analytique de l'équation d'Hurwitz

Quelles sont les valeurs possibles pour k ? En d'autres termes, quelles sont les valeurs entières prises par la fonction f, définie par :

$$\begin{array}{rccc} f & : & (\mathbb{N}^*)^n & \mapsto & \mathbb{R} \\ & & (x_1 \dots x_n) & \to & \frac{{x_1}^2 + \cdots + {x_n}^2}{x_1 \cdots x_n} \end{array}$$

Nous allons montrer que c'est un ensemble inclus dans $\{1 \dots n\}$. Une étude analytique directe n'aboutit pas à ce résultat, car lorsque $x_1 \dots x_{n-1}$ sont fixés, $\lim\limits_{x_n \to +\infty} f(x_1 \dots x_n) = +\infty$.

Considérons une solution minimale $(x_1 \dots x_n)$ pour l'ordre lexicographique. En effet, s'il existe une solution, alors il en existe une qui est minimale car l'ordre lexicographique est un bon ordre. Elle est en outre fondamentale. Comme le fait de permuter les x_i ne change pas le fait qu'on aie toujours une solution, cela implique que $x_1 \leq \dots \leq x_n$.

Cherchons donc à borner x_n quand k,$x_1 \dots x_{n-1}$ sont des entiers naturels non nuls. Pour cela, séparons deux cas :

1er cas : $x_1 = \dots = x_{n-1} = 1$. Alors l'équation devient $(n-1) + {x_n}^2 = kx_n$, soit $k = x_n + \frac{n-1}{x_n}$. L'équation est à solutions entières, donc x_n divise $(n-1)$, donc $1 \leq x_n \leq (n-1)$, et une simple étude de la fonction $\phi(x) = x + \frac{n-1}{x}$ qui atteint son maximum en 1 ou en $(n-1)$ montre que $k \leq n$.

2e cas : $x_{n-1} \geq 2$. La minimalité de la solution implique que $(x_1 \dots x_n) \preccurlyeq (x_1 \dots x_{n-1}, kx_1 \dots x_{n-1} - x_n)$, ce qui équivaut à :

$$\begin{array}{rcl} x_n & \leq & kx_1 \dots x_{n-1} - x_n \\ 2x_n & \leq & kx_1 \dots x_{n-1} \\ 2{x_n}^2 & \leq & kx_1 \dots x_n \\ 2{x_n}^2 & \leq & {x_1}^2 + \dots + {x_n}^2 \\ {x_n}^2 & \leq & {x_1}^2 + \dots + {x_{n-1}}^2 \end{array}$$

Les majorations $x_{n-1} \leq x_n$ et ${x_n}^2 \leq {x_1}^2 + \dots + {x_{n-1}}^2$ montrent que :

$$\begin{array}{rcl} k & = & \frac{{x_1}^2 + \dots + {x_n}^2}{x_1 \dots x_n} \\ k & \leq & \frac{2({x_1}^2 + \dots + {x_{n-1}}^2)}{x_1 \dots x_{n-1} x_{n-1}} \\ k & \leq & \frac{2}{x_1 \dots x_{n-2}} \left(\left(\frac{x_1}{x_{n-1}} \right)^2 + \dots + \left(\frac{x_{n-2}}{x_{n-1}} \right)^2 + 1 \right) \end{array}$$

Nous allons maintenant prouver que $k \leq n$.

En effet, fixons $c = x_{n-1} \geq 2$ et considérons la fonction g définie par :

$$\begin{array}{rccc} g & : & [1;c]^{n-2} & \to & \mathbb{R} \\ & & (x_1 \dots x_{n-2}) & \mapsto & \frac{2}{x_1 \dots x_{n-2}} \left(\left(\frac{x_1}{c} \right)^2 + \dots + \left(\frac{x_{n-2}}{c} \right)^2 + 1 \right) \end{array}$$

C'est une fonction continue sur un domaine compact $[1;c]^{n-2}$, elle possède donc un maximum m en $(\xi_1 \dots \xi_n)$. Par symétrie de la fonction, on peut supposer $\xi_1 \leq \dots \leq \xi_{n-2}$. Parmi ces $n-2$ valeurs, il y en a α égales à 1, β dans $]1;c[$ et γ égales à c. Montrons par l'absurde que $\beta = 0$, et donc que $\alpha + \gamma = n - 2$.

Supposons par l'absurde que $\beta > 0$. La fonction h définie par :

$$\begin{array}{rccc} h & : & [1;c]^{\beta} & \to & \mathbb{R} \\ & & (y_1 \dots y_{\beta}) & \mapsto & \frac{2}{y_1 \dots y_{\beta} c^{\gamma}} \left(\alpha \left(\frac{1}{c} \right)^2 + \left(\frac{y_1}{c} \right)^2 + \dots + \left(\frac{y_{\beta}}{c} \right)^2 + (\gamma + 1) \right) \end{array}$$

possède un maximum dans $]1;c[^{\beta}$ en $(\eta_1 \dots \eta_{\beta})$ et donc pour tout $i \in \{1 \dots \beta\}$,

$$\frac{\partial h}{\partial y_i}(\eta_1 \dots \eta_{\beta}) = 0$$

Comme la fonction h est un quotient, cela équivaut à dire que les dérivées logarithmiques du numérateur et du dénominateur sont égales.

$$\frac{\eta_1 \cdots \eta_{i-1}\eta_{i+1} \cdots \eta_\beta}{\eta_1 \cdots \eta_i \cdots \eta_\beta} = \frac{2\eta_i \left(\frac{1}{c}\right)^2}{\alpha\left(\frac{1}{c}\right)^2 + \left(\frac{\eta_1}{c}\right)^2 + \cdots + \left(\frac{\eta_\beta}{c}\right)^2 + (\gamma+1)}$$

donc

$$\begin{array}{rcl} 2\left(\frac{\eta_i}{c}\right)^2 & = & \alpha\left(\frac{1}{c}\right)^2 + \left(\frac{\eta_1}{c}\right)^2 + \cdots + \left(\frac{\eta_\beta}{c}\right)^2 + (\gamma+1) \\ 2\left(\frac{\eta_i}{c}\right)^2 & \geq & \left(\frac{\eta_i}{c}\right)^2 + 1 \\ \left(\frac{\eta_i}{c}\right)^2 & \geq & 1 \\ \eta_i & \geq & c \end{array}$$

Contradiction. Cela prouve $\beta = 0$, et par conséquent $\alpha + \gamma = n - 2$.

Donc $m = \frac{2}{c^\gamma}\left(\alpha\left(\frac{1}{c}\right)^2 + \gamma + 1\right) \leq \frac{2}{2^\gamma}\left(\frac{\alpha}{4} + \gamma + 1\right)$.
Si $\gamma \geq 1$, alors $m \leq \frac{2}{2}(\alpha + \gamma + 1) = n - 1 < n$.
Si $\gamma = 0$, alors $m \leq 2\left(\frac{n-2}{4} + 1\right) = \frac{n+2}{2} < n$.
Conclusion : $k < n$.

Donc l'équation ${x_1}^2 + \cdots + {x_n}^2 = kx_1 \cdots x_n$ a des solutions uniquement lorsque k appartient à un certain ensemble inclus dans $\{1 \ldots n\}$. De plus, n est toujours présent dans cet ensemble pour la solution $(1 \ldots 1)$ quand $k = n$.

1.4 Les valeurs possibles de k pour $n = 3$

$k = 1$: On réduit l'équation modulo 3. Si $\overline{x_1}$, $\overline{x_2}$ et $\overline{x_3}$ sont tous non-nuls, alors $\overline{x_1 x_2 x_3} = \overline{{x_1}^2} + \overline{{x_2}^2} + \overline{{x_3}^2} = \overline{1} + \overline{1} + \overline{1} = \overline{0}$. Contradiction car $\mathbb{Z}/3\mathbb{Z}$ est un corps. Donc on peut supposer $\overline{x_1} = 0$, et les seules valeurs possibles pour $\overline{x_2}$ et $\overline{x_3}$ sont 0. Donc x_1, x_2 et x_3 sont divisibles par 3, et $\left(\frac{x_1}{3}\right)^2 + \left(\frac{x_2}{3}\right)^2 + \left(\frac{x_3}{3}\right)^2 = 3\left(\frac{x_1}{3}\right)\left(\frac{x_2}{3}\right)\left(\frac{x_3}{3}\right)$. On est ramené au cas $k = 3$.

$k = 2$: x_1, x_2 et x_3 ne peuvent pas être pairs en même temps, sinon on obtient une solution pour $k = 4$. En réduisant modulo 2, il y a deux variables impaires et une paire. On peut supposer x_1 et x_2 impairs et x_3 pair. En réduisant $2x_1x_2x_3 - {x_3}^2 = {x_1}^2 + {x_2}^2$ modulo 4, on obtient $\overline{0} = \overline{2}$, contradiction.

$k = 3$: Il y a une solution évidente (1,1,1), et à partir de là, une infinité de solutions. Nous verrons plus loin que c'est la seule solution fondamentale, et donc que toutes les solutions proviennent de (1,1,1).

Conclusion : les valeurs possibles de k pour $n = 3$ sont 1 et 3. De plus, le cas $k = 1$ n'est pas intéressant car les solutions sont exactement les solutions du cas $k = 3$ multipliées par 3. Le plus petit cas particulier de l'équation d'Hurwitz dont l'étude présente un certain intérêt est le cas $n = 3$ et $k = 3$, c'est l'équation de Markov.

Pour trouver les valeurs possibles de k pour n quelconque, il existe une méthode algorithmique, décrite dans la section suivante.

2 Calcul des solutions fondamentales

Nous avons vu, pour $n \geq 3$ et $k \in \mathbb{N}^*$, que toute solution est associée à une unique solution fondamentale. Ainsi, l'équation d'Hurwitz a une solution si et seulement si elle a au moins une solution fondamentale.

Il est possible de trouver algorithmiquement l'ensemble des solutions fondamentales à k et n fixés, donc comme on sait que $k \leq n$, il est possible de trouver les valeurs possibles de k pour n quelconque fixé.

Nous allons chercher une majoration de $x_1 \dots x_n$ pour une solution fondamentale, puis calculer si l'équation est vérifiée pour toutes les valeurs possibles de $x_1 \dots x_n$. Prenons une solution fondamentale $(x_1 \dots x_n)$.

$$kx_1 \cdots x_{n-2}{x_{n-1}}^2 \leq {x_1}^2 + \cdots + {x_n}^2 \leq 2\left({x_1}^2 + \cdots + {x_{n-1}}^2\right) \leq 2(n-1){x_{n-1}}^2$$

donc pour $i \in \{1 \dots n-2\}$:

$$k{x_i}^{n-i-1} \leq kx_1 \cdots x_{n-2} \leq 2(n-1)$$

$$x_i \leq \sqrt[n-i-1]{\frac{2(n-1)}{k}}$$

On est donc revenu à des équations du type $X + a^2 + b^2 = Yab$ où X et Y sont des entiers naturels fixés, et a et b les inconnues.

On cherche à nouveau une solution fondamentale.

$$\begin{array}{rcl} b & \leq & Ya - b \\ 2b & \leq & Ya \\ 2b^2 & \leq & Yab \\ 2b^2 & \leq & X + a^2 + b^2 \\ b^2 & \leq & X + a^2 \end{array}$$

Donc $a \leq b \leq \sqrt{X + a^2}$. On peut alors séparer en deux cas :

1er cas : Si $a = b$, il n'y a qu'une valeur possible, c'est $a = b = \sqrt{\frac{X}{Y-2}}$, sous réserve d'existence.

2e cas : Sinon, $a < b$, donc $a + 1 \leq \sqrt{X + a^2}$ soit $2a + 1 \leq X$, ou encore $a \leq \frac{X-1}{2}$, et cela implique $b \leq \sqrt{X + \frac{(X-1)^2}{4}} = \frac{X+1}{2}$.

On a donc un nombre fini de solutions à tester. On peut donc chercher les valeurs possibles de k à n fixé en temps fini.

2.1 Complexité de l'algorithme

Il reste à savoir si la complexité de cet algorithme n'est pas trop grande. Soit $p = \lceil \ln n \rceil$. Alors le nombre de valeurs posibles pour $(x_1 \dots x_{n-2})$ est inférieur à

$$\prod_{i=1}^{n-2} \sqrt[n-i-1]{\frac{2(n-1)}{k}} \leq \exp\left(\ln 2(n-1) \sum_{i=1}^{n-2} \frac{1}{n-i-1}\right) = \exp\left(\ln 2(n-1) \sum_{i=1}^{n-2} \frac{1}{i}\right)$$

donc à $\exp(\ln 2n \ln n)$.

De plus, $\forall i \in \{1 \dots n-2\}$, $x_i \leq 2n$ donc $X \leq (n-2)(2n)^2 \leq 4n^3$. Il y a donc au plus $4n^6$ choix possibles pour a et b, donc au plus
$\exp(\ln 2n \ln n + \ln 4 + 6 \ln n)$ équations possibles. Or le calcul des deux membres se fait en $O(np)$ donc la vérification de l'équation également. La complexité de l'algorithme est donc inférieure à :

$$\begin{array}{rcl} C(n) & \leq & Knp \exp(\ln 2n \ln n + \ln 4 + 6 \ln n) \\ & \leq & \exp(\ln K + \ln n + \ln p + \ln 2n \ln n + \ln 4 + 6 \ln n) \\ & \leq & \exp(\ln K + p + \ln p + (p + \ln 2)p + \ln 4 + 6p) \\ & \leq & \exp\left(p^2 + (7 + \ln 2)p + \ln p + (\ln K + \ln 4)\right) \end{array}$$

où K est une constante telle que l'équation se vérifie en Knp.

L'algorithme ainsi indiqué est exponentiel en p. On peut donc espérer faire le calcul en temps raisonnable pour $n \leq 30$.

2.2 Implémentation de l'algorithme et résultats

On peut implémenter l'algorithme en Caml Light. On commence par implémenter quelques fonctions utiles.

```
let rec map f = function
 []  -> []
|t::q-> (f t)::(map f q) ;;

let rec concat l = function
 []  -> l
|t::q-> t::concat l q ;;

let rec puissance a = function
  0  -> 1
| b  -> a*(puissance a (b-1)) ;;

let racine x =  let i = ref 0 in
                while (!i * !i) <= x do
                incr i
                done ;
                !i-1 ;;

let max (a,b) = if a < b then b else a ;;
```

On peut alors écrire l'algorithme, où la fonction `equation X Y Qmin n` renvoie pour $n \geq 2$ les solutions fondamentales de l'équation :

$$X + {x_1}^2 + \cdots + {x_n}^2 = Y x_1 \cdots x_n$$

telles que $x_i \geq Q_{\min}$ pour tout $i \in \{1 \dots n\}$.

La fonction `hurwitz k n` renvoie la liste des solutions fondamentales à k et n fixés (à condition que $n \geq 3$ et $k \geq 1$).

```
let rec equation x y qmin = function
 2->let resultat = ref [] in
    if y > 2 then
    (   let j = racine (x/(y-2)) in
        if (j*j*(y-2) = x && j >= qmin) then
        resultat := [[j;j]]  );
    for i = qmin to ((x-1)/2) do
        let j = ref (i+1) in let somme_provisoire = i*i+x in
        while (!j * !j) <= somme_provisoire do
            if (somme_provisoire+ !j * !j = y * i * !j) then
                resultat := [i; !j] :: !resultat ;
            incr j
        done ;
    done ;
    !resultat
|n->let majorant = ((2*(n-1+x))/y) in
    let resultat = ref [] in
    let i = ref qmin in
    while (puissance !i (n-2)) <= majorant do
        let l = equation (x+ !i* !i) (y* !i) (max(qmin,!i)) (n-1) in
        resultat := concat (map (function a -> !i::a) l) !resultat ;
        incr i
    done ;
    !resultat ;;

let hurwitz k n = equation 0 k 1 n ;;
```

On trouve pour $n = 3$ qu'il n'y a des solutions que si $k = 1$, et alors (3,3,3) est l'unique solution fondamentale, ou alors si $k = 3$, et alors (1,1,1) est l'unique solution fondamentale.

Si $n = 4$, il n'y a des solutions que si $k \in \{1,4\}$, les solutions fondamentales respectives étant (2,2,2,2), et (1,1,1,1). Si $n = 5$, il n'y a des solutions que si $k \in \{1,4,5\}$, les solutions fondamentales respectives étant (1,1,3,3,4), (1,1,1,1,2), et (1,1,1,1,1).

Voici un tableau qui récapitule les valeurs possibles de k pour n donné.

3	1,3
4	1,4
5	1,4,5
6	3,6
7	1,2,3,5,7
8	1,8
9	6,9
10	1,2,4,6,10
11	2,3,7,11

12	12
13	1,3,4,7,8,13
14	1,4,5,14
15	3,9,15
16	8,16
17	1,2,8,10,17
18	3,6,18
19	1,5,9,11,19
20	2,4,20

21	3,9,12,21
22	1,2,3,5,7,10,22
23	1,4,5,13,23
24	24
25	1,2,4,6,10,11,14,25
26	1,2,8,10,26
27	1,3,15,27
28	1,4,12,28
29	4,5,11,16,29

2.3 Taille de l'ensemble des solutions fondamentales

Nous avons vu pour $n = 3,4,5$ et les valeurs de k correspondantes qu'il n'y a qu'une seule solution fondamentale, et donc que toutes les solutions proviennent de cette solution fondamentale. On pourrait penser qu'il n'y a toujours qu'une unique solution fondamentale. Mais c'est faux. En effet, pour $n = 14$ et $k = 1$, les solutions $(1 \dots 1,3,4,6)$ et $(1 \dots 1,2,2,3,3)$ sont fondamentales et engendrent deux ensembles distincts de solutions.

Pour $n = 19$ et $k = 1$ il y a trois solutions fondamentales $(1 \dots 1,3,5,5)$, $(1 \dots 1,4,4,4)$ et $(1 \dots 1,2,2,3,4)$. Et en fait, on peut trouver des couples (n,k) avec un nombre arbitrairement grand de solutions fondamentales.

Soit $r \in \mathbb{N}^*$. Nous allons voir qu'il existe (k,n) tel qu'il y a au moins r solutions fondamentales. En fait nous allons démontrer un résultat plus fort : à r et k fixés, il existe n tel qu'il y a au moins $r + 1$ solutions fondamentales. Il suffira alors de poser $k = 1$.

Une solution de l'équation d'Hurwitz est fondamentale si et seulement si $(x_1 \dots x_n)$ est plus petit que son plus petit voisin, le n-uplet qui doit alors s'écrire $(x_1 \dots x_{n-1}, kx_1 \cdots x_{n-1} - x_n)$.

Ou encore :

$$\begin{array}{rcl} x_n & \leq & kx_1 \cdots x_{n-1} - x_n \\ 2x_n & \leq & kx_1 \cdots x_{n-1} \\ 2{x_n}^2 & \leq & kx_1 \cdots x_n \\ 2{x_n}^2 & \leq & x_1 + \cdots x_n \\ {x_n}^2 & \leq & {x_1}^2 + \cdots {x_{n-1}}^2 \end{array}$$

Nous allons créer des solutions qui ne comporte que les nombres $i = 1$, 2, 4, 3, 9, qui apparaissent chacun λ_i fois dans la solution. Soit encore les solutions du type $(\underbrace{1 \dots 1}_{\lambda_1 \text{ fois}}, \underbrace{2 \dots 2}_{\lambda_2 \text{ fois}} \dots \underbrace{9 \dots 9}_{\lambda_9 \text{ fois}})$.

Prenons maintenant $\mu_2 = 0$, $\mu_4 \geq 62r$, $\mu_3 = 14r$, $\mu_9 = 0$, et $\mu_1 = k \cdot 2^{\mu_2} 3^{\mu_3} 4^{\mu_4} 9^{\mu_9} - 4\mu_2 - 9\mu_3 - 16\mu_4 - 81\mu_9$, avec μ_4 suffisament grand pour que $\mu_1 \geq \max(55r,82)$. On pose alors $n = \mu_1 + \mu_2 + \mu_4 + \mu_3 + \mu_9 = k \cdot 2^{\mu_2} 3^{\mu_3} 4^{\mu_4} 9^{\mu_9}$.

Considérons maintenant les solutions telles que

$$\begin{array}{rcl} \lambda_1 & = & \mu_1 - 55a \\ \lambda_2 & = & \mu_2 + 124a \\ \lambda_4 & = & \mu_4 - 62a \\ \lambda_3 & = & \mu_3 - 14a \\ \lambda_9 & = & \mu_1 + 7a \end{array}$$

pour a entre 0 et r.

Premièrement, on a choisi les μ_i tels que les λ_i soient toujours des entiers positifs.

Deuxièmement, on a choisi les coefficients tels que

$$\lambda_1 + \lambda_2 + \lambda_4 + \lambda_3 + \lambda_9 = \mu_1 + \mu_2 + \mu_4 + \mu_3 + \mu_9 = n \geq 82$$

et

$$\sum_{i\in\{1,2,3,4,9\}} i^2\cdot\lambda_i = \lambda_1+4\lambda_2+16\lambda_4+9\lambda_3+81\lambda_9 = \mu_1+4\mu_2+16\mu_4+9\mu_3+81\mu_9$$

En effet,

$$a\left((-62+7)+124-62-14+7\right)=0$$

et

$$a\left(1\cdot(-8\cdot 62+63\cdot 7)+4\cdot 124-16\cdot 62-9\cdot 14+81\cdot 7\right)=0$$

Troisièmement,

$$\begin{array}{rl} & \prod_{i\in\{1,2,3,4,9\}} i^{\lambda_i} \\ = & 2^{\lambda_2+2\lambda_4}3^{\lambda_3+2\lambda_9} \\ = & 2^{\mu_2+2\mu_4}3^{\mu_3+2\mu_9}\left(2^{124-2\cdot 62}3^{-14+2\cdot 7}\right)^a \\ = & 2^{\mu_2+2\mu_4}3^{\mu_3+2\mu_9} \end{array}$$

Par construction de μ_1, les deux membres de l'équation ne varient pas en fonction de a. L'équation est donc vraie pour tout a entre 0 et r. Les solutions sont fondamentales, car ${x_n}^2 \leq 9^2 = 81 \leq n-1 \leq {x_1}^2+\cdots+{x_{n-1}}^2$.

On a donc trouvé pour $k=1$ et $n=\mu_1+\mu_2+\mu_4+\mu_3+\mu_9$ au moins $r+1$ solutions fondamentales.

3 Étude des nombres de Markov

Nous pouvons maintenant revenir à l'équation de Markov proprement dite : $x^2 + y^2 + z^2 = 3xyz$, pour x, y, z dans $\mathbb{N}^*$.

3.1 L'arbre des solutions

Une étude préalable nous a montré que (1,1,1) est l'unique solution fondamentale. La solution (1,1,2) a un père (1,1,1) et un fils (1,2,5). Nous allons montrer que toute autre solution a exactement un père et deux fils.

Montrons d'abord que toute autre solution est un triplet de trois entiers distincts. En effet, si (x,x,y) est une solution (pas forcément ordonnée), alors $2x^2+y^2 = 3x^2y$, donc x^2 divise y^2, donc x divise y, et $1+1+\left(\frac{y}{x}\right)^2 = (3x)\cdot 1\cdot 1\cdot\left(\frac{y}{x}\right)$. $3x$ ne peut prendre que les valeurs 1 ou 3, donc $x = 1$ et $2 + y^2 = 3y$, donc y divise 2, et on n'a que les possibilités (1,1,1) ou (1,1,2).

Prenons (x,y,z) une solution ordonnée avec $x < y < z$. Avec les inégalités suivantes, $3xz - y = \frac{x^2+z^2}{y} > \frac{z^2}{z} = z$, et $3yz - x > 3xz - y$, on trouve que $(x,z,3xz-y)$ et $(y,z,3yz-x)$ sont deux fils de (x,y,z), et donc $(x,y,3xy-z)$ — mis à part l'ordre du triplet — est son père.

Maintenant qu'on a prouvé que toute solution formée d'entiers distincts a exactement deux fils, on va pouvoir créer un arbre infini de la manière suivante : (1,1,1) est la racine, qui a pour unique fils (1,1,2), qui lui même a pour unique fils (1,2,5), qui a deux fils (1,5,13) et (2,5,29), et ainsi de suite chaque nœud (x,y,z) a exactement deux fils $(x,z,3xz-y)$ et $(y,z,3yz-x)$.

Cet arbre énumère toutes les solutions de l'équation de Markov. De plus, les définitions de père et de fils des solutions coincident avec celles des arbres.

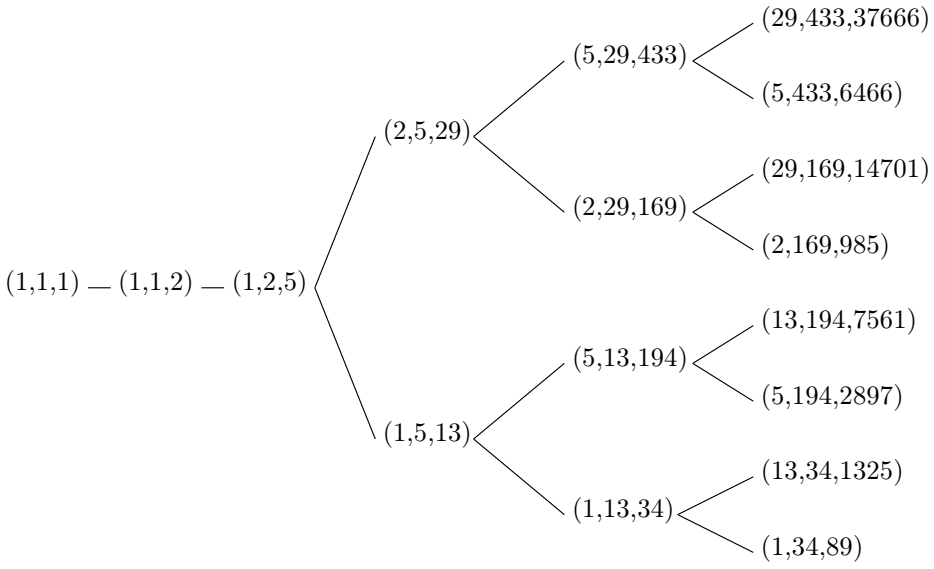

FIG. 1 – *Arbre des solutions de l'équation de Markov*

On appelle nombres de Markov les nombres qui apparaissent dans les triplets de solutions de l'équation de Markov. Chaque nombre apparaît donc dans l'arbre

des solutions, et quand il apparaît, on peut en déduire une infinité de solutions qui le contiennent. En effet, il apparaît comme z dans un triplet (x,y,z), et à partir de là, on obtient les solutions (z,x_n,x_{n+1}) avec $x_{n+2} = 3zx_{n+1} - x_n$, et $x_0 = x$, $x_1 = y$.

C'est pour cela que la branche gauche de l'arbre contient des nombres de Fibonacci. En effet, $F_0 = 1$ et $F_2 = 2$, et :

$$\begin{aligned} F_{n+2} &= F_{n+1} + F_n \\ &= (F_n + F_{n-1}) + F_n \\ &= 3F_n - (F_{n-1} + F_{n-2}) + (F_{n-1}) \\ &= 3F_n - F_{n-2} \end{aligned}$$

Comme avec $z = 1$, on a $x_0 = 1 = F_0$, $x_1 = 2 = F_2$ et $x_{n+2} = 3x_{n+1} - x_n$, cela explique que $x_n = F_{2n}$.

Une conjecture affirme qu'un nombre de Markov z n'apparaît qu'une seule fois dans l'arbre, c'est-à-dire que s'il apparaît dans une solution, la solution descend directement d'une unique plus petite solution (x,y,z) où $x \leq y \leq z$. En d'autres termes, l'équation $x^2 + y^2 + z^2 = 3xyz$ en (x,y) admet une unique solution fondamentale. Ou bien, comme on sait qu'il y a une solution telle que $x \leq y \leq z$, que tout triplet de Markov (x,y,z) est déterminé par son élément maximal.

3.2 Le théorème d'approximation d'Hurwitz

Dans cette section, nous nous contenterons de donner les résultats. Pour une preuve complète du théorème, voir les deux premiers chapitres de [Cas].

On commence par une définition préliminaire. Deux irrationnels θ et θ' sont dits **équivalents** si $\theta' = \dfrac{a\theta + b}{c\theta + d}$, où a, b, c et d sont des entiers relatifs et $|ad - bc| = 1$. On a bien une relation d'équivalence car $\theta = (ad - bc)\dfrac{d\theta' - b}{-c\theta' + a}$.

Il est facile de voir, en utilisant le principe des tiroirs, que pour tout irrationnel θ, il existe une infinité d'approximations rationnelles $\frac{p}{q}$ de θ telles que $\left|\theta - \frac{p}{q}\right| \leq \frac{1}{q^2}$.

Lagrange a amélioré ce résulat en montrant qu'il existe une infinité d'approximations $\frac{p}{q}$ de θ telles que $\left|\theta - \frac{p}{q}\right| \leq \frac{1}{\sqrt{5}q^2}$, et qu'on ne peut pas augmenter le $\sqrt{5}$ pour les irrationnels équivalents à $\theta = \frac{1+\sqrt{5}}{2}$. Pour tous les autres irrationnels, $\left|\theta - \frac{p}{q}\right| \leq \frac{1}{\sqrt{8}q^2}$.

Pour chaque θ irrationnel, on note $v = v(\theta) = \liminf q||q\theta||$, où $||q\theta||$ est la distance entre $q\theta$ et l'ensemble $\mathbb{Z}$ des entiers relatifs, ou encore la plus petite valeur prise par $|q\theta - p|$ lorsque p décrit $\mathbb{Z}$. Par définition, s'il existe une infinité d'approximations $\frac{p}{q}$ de θ telles que $\left|\theta - \frac{p}{q}\right| \leq w\frac{1}{q^2}$, alors $v \leq w$, et v est le plus grand nombre qui vérifie cette inégalité.

Pour $\theta = \frac{1+\sqrt{5}}{2}$, $v = \frac{1}{\sqrt{5}}$.
Pour $\theta = \sum_{n=0}^{+\infty} \frac{1}{a^{3^n}}$ avec $a > 1$ entier, $v = 0$. Donc pour tout $\varepsilon > 0$, il existe une infinité d'approximations telles que $\left|\theta - \frac{p}{q}\right| \leq \varepsilon \frac{1}{q^2}$.

On peut reformuler le résultat de Lagrange comme ceci : pour tout irrationnel θ équivalent à $\frac{1+\sqrt{5}}{2}$, $v(\theta) = \frac{1}{\sqrt{5}}$, et pour tous les autres, $v(\theta) = \frac{1}{\sqrt{8}}$.

Le **théorème d'approximation d'Hurwitz** est un résultat beaucoup plus fort : les valeurs prises par v qui sont strictement supérieures à $\frac{1}{3}$ sont toutes de la forme $\frac{m}{\sqrt{9m^2-4}}$ où m est un nombre de Markov.
$v = \frac{1}{\sqrt{5}}$ si et seulement si θ est équivalent à $\frac{1+\sqrt{5}}{2}$;
$v = \frac{1}{\sqrt{8}}$ si et seulement si θ est équivalent à $\sqrt{2}$;
$v = \frac{5}{\sqrt{221}}$ si et seulement si θ est équivalent à une racine de $5X^2 + 11X - 5$, etc.

Plus précisément, si $v > \frac{1}{3}$, alors θ est équivalent à une racine d'un polynôme $mX^2 + (3m - 2q)X + (r - 3q)$, où m est un nombre de Markov, q l'entier [1] tel que m divise $q^2 + 1$ et $0 < q < \frac{m}{2}$, et $r = \frac{q^2+1}{m}$.

3.3 Lien avec les sommes de Dedekind

Dans cette section également, nous nous contenterons de donner les résultats.

On note $((\cdot))$ la fonction telle que $((x)) = x - \frac{1}{2}$ pour $x \in]0;1[$, $((0)) = 0$, et $((x)) = ((x+1))$ pour tout x réel. Remarquons que cette fonction est impaire.

On appelle **somme de Dedekind** (généralisée) une somme de la forme $S(a,b,c) = \sum_{h=1}^{c-1} \left(\left(\frac{ah}{c}\right)\right)\left(\left(\frac{bh}{c}\right)\right)$ avec a et b tous deux premiers à c.

Il est important de remarquer qu'on peut sommer les h modulo c, et donc qu'en remplaçant dans la formule les h par des hk — où k est premier à c, la somme ne varie pas. En effet, modulo c, $\{1 \dots c-1\} = \{k \dots k(c-1)\}$. C'est-à-dire que $S(a,b,c) = S(ak,bk,c)$. En particulier $S(a,b,c) = S(a\overline{b},1,c)$, où $b\overline{b} \equiv 1 \mod c$.
Également en remarquant que modulo c, $\{1 \dots c-1\} = \left\{\overline{1} \dots \overline{c-1}\right\}$, on obtient l'égalité suivante : $S(x,1,c) = S(\overline{x},1,c)$. Cela montre que $S(a,b,c) = S(b,a,c)$.

Le **théorème de réciprocité de Rademacher** dit la chose suivante :
Soient a, b, c trois entiers deux à deux premiers entre eux. Alors on a :

$$S(a,b,c) + S(b,c,a) + S(c,a,b) = \frac{a^2 + b^2 + c^2 - 3abc}{12abc}.$$

1. Sauf pour $m = 1$ ou 2, et alors on prend respectivement $(q,r) = (0,1)$ et $(q,r) = (1,1)$.

Pour la démonstration, on se ramène à [Hir]. Il y a clairement un lien avec l'équation de Markov : en effet, (a,b,c) est un triplet de Markov si et seulement si $S(a,b,c) + S(b,c,a) + S(c,a,b) = 0$.

Cela va nous permettre de montrer d'une autre manière que les seules valeurs admissibles pour k avec $n = 3$ sont 1 et 3, et seulement 3 si on se réduit aux triplets (a,b,c) d'entiers deux à deux premiers entre eux. Commençons par un lemme.

Si c divise $a^2 + b^2$, alors $S(a,b,c) = 0$.

En effet, comme c et premier avec a ainsi qu'avec b, on peut prendre $\overline{b}$ tel que $b\overline{b} \equiv 1 \mod c$, et donc c divise $\left(a\overline{b}\right)^2 + 1$, et il en découle les égalités suivantes :

$$\begin{aligned} S(a\overline{b},1,c) &= S(\left(a\overline{b}\right)^2, a\overline{b}, c) \\ &= S(-1, a\overline{b}, c) \\ &= S(a\overline{b}, -1, c) \\ &= -S(a\overline{b}, 1, c) \end{aligned}$$

Donc $S(a\overline{b},1,c) = 0$, d'où le lemme.

Cela va nous permettre de démontrer un théorème qui montre le lien entre les sommes de Dedekind et l'équation de Markov.

Soient a, b, c trois entiers premiers entre eux. Les assertions suivantes sont équivalentes :

(i) Il existe $n \in \mathbb{Z}$ tel que $a^2 + b^2 + c^2 = nabc$.
(ii) $a|b^2 + c^2$, $b|a^2 + c^2$ et $c|a^2 + b^2$.
(iii) $S(a,b,c) = S(b,c,a) = S(c,a,b) = 0$.
(iv) $S(a,b,c) + S(b,c,a) + S(c,a,b) = 0$.
(v) $a^2 + b^2 + c^2 = 3abc$.

Ce théorème se prouve circulairement en faisant $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (v) \Rightarrow (i)$. Les seules implications non-triviales sont $(iv) \Rightarrow (v)$, qui est une conséquence du théorème de réciprocité, et $(ii) \Rightarrow (iii)$, qui est une conséquence du lemme précédent.

L'implication $(i) \Rightarrow (v)$ donne ce qu'on avait trouvé dans la section 1.4, c'est-à-dire que si un triplet (a,b,c) vérifie $a^2 + b^2 + c^2 = nabc$ avec a, b, et c deux à deux premiers, alors $n = 3$.

Références

[Sen] Volker Senkel, *Markoffzahlen*, Universität Bielefeld Fakultät für Mathematik, 1997. Diplomarbeit (`http://www.mathematik.uni-bielefeld.de/~senkel/DIP/dip.ps.gz`).

[Cas] John Cassels, *Introduction to diophantine approximation*, Cambridge : Cambridge University Press, 1957.

[Hir] Friedrich Hirzebruch, *The Atiyah-Singer theorem and elementary number theory*, Boston MA : Publish or Perish, 1974. Chap. 2.