Une variante de l'équation de Markov

Daniel PERRIN

Introduction

Le problème abordé ici est posé dans le numéro 539 de *Au fil des maths* (problème 539-2) :

Résoudre dans les nombres entiers naturels l'équation (E) *:*

$$a^2 + 2b^2 + 3c^2 = 6abc.$$

Le problème est passionnant, mais loin d'être évident, et ce texte n'épuise sans doute pas le sujet [1]. On peut au moins dire que cette équation admet une infinité de solutions.

Comme l'indiquait la question 539-2, l'équation est une variante de l'équation de Markov :

$$a^2 + b^2 + c^2 = 3abc, \text{ voir :}$$

`https://fr.wikipedia.org/wiki/Nombre_de_Markov`.

De fait, l'une des propriétés de l'équation de Markov (le fait que ses solutions sont invariantes par l'application $(a, b, c) \mapsto (a, b, 3ab - c)$) se généralise dans le cas présent et permet de montrer nombre de propriétés des solutions.

1 Remarques préliminaires

1.1 Des solutions avec l'ordinateur

Face à une question ouverte comme celle-ci, il est utile de disposer d'une liste de "petites" solutions (s'il y en a). Le programme suivant, sur SAGE, renvoie la liste des solutions de l'équation avec des nombres $a, b, c \leq n$:

```
def APM(n):
   for a in [0..n] :
         for b in [0..n] :
            for c in [0..n] :
               if a^2+2*b^2+3*c^2==6*a*b*c :
                  print(a,b,c)
```

Pour $n = 1000$, on trouve les 35 solutions suivantes :

$(0, 0, 0)$, $(1, 1, 1)$, $(1, 2, 1)$, $(1, 2, 3)$, $(1, 7, 3)$, $(1, 7, 11)$, $(1, 26, 11)$, $(1, 26, 41)$, $(1, 97, 41)$, $(1, 97, 153)$, $(1, 362, 153)$, $(1, 362, 571)$, $(5, 1, 1)$, $(5, 1, 9)$, $(5, 14, 1)$,

1. Outre qu'il n'est pas exclu qu'il comporte des erreurs.

$(5, 14, 139)$, $(5, 134, 9)$, $(11, 2, 1)$, $(11, 2, 43)$, $(11, 31, 1)$, $(11, 31, 681)$, $(35, 2, 3)$, $(35, 2, 137)$, $(35, 313, 3)$, $(49, 1, 9)$, $(49, 1, 89)$, $(79, 14, 1)$, $(79, 223, 1)$, $(125, 7, 3)$, $(175, 31, 1)$, $(175, 494, 1)$, $(461, 7, 11)$, $(485, 1, 89)$, $(485, 1, 881)$ et $(505, 2, 43)$.

1.2 Solutions nulles

1.1 Proposition. *L'unique solution de l'équation avec a, b ou c nul est $(0, 0, 0)$.*

Démonstration. C'est clair car si l'un est nul on a $abc = 0$ et il reste une somme de deux nombres positifs égale à 0, donc les autres sont nuls.

On suppose désormais $a, b, c > 0$. On note $\mathcal{S}$ l'ensemble des solutions de (E) dans $(\mathbf{N}^*)^3$.

1.3 Trois équations du second degré

L'équation (E) peut être vue comme une équation de degré 2 en a, b ou c. Comme ce point de vue joue un rôle essentiel dans ce qui suit, nous détaillons les résultats qui le concernent dans la proposition suivante.

1.2 Proposition. *1) Pour $b, c \in \mathbf{N}^*$ fixés, l'équation (E) peut être vue comme une équation en a : $a^2 - 6bca + 2b^2 + 3c^2 = 0$. Le discriminant réduit de cette équation est $\Delta_1' = 9b^2c^2 - 2b^2 - 3c^2$ et il est > 0. Les solutions a', a'' de cette équation sont réelles positives. Elles sont entières si et seulement si Δ_1' est le carré d'un entier δ_1 et on a alors $a', a'' = 3bc \pm \delta_1$. Elles vérifient $a'' = 6bc - a'$ et inversement.*

2) Pour $c, a \in \mathbf{N}^*$ fixés, l'équation (E) peut être vue comme une équation en b : $2b^2 - 6acb + 3c^2 + a^2 = 0$. Le discriminant réduit de cette équation est $\Delta_2' = 9a^2c^2 - 6c^2 - 2a^2$ et il est > 0. Les solutions b', b'' de cette équation sont réelles positives. Elles sont entières si et seulement si Δ_2' est le carré d'un entier δ_2 et on a $b', b'' = \dfrac{3ac \pm \delta_2}{2}$. Elles vérifient $b'' = 3ac - b'$ et inversement.

3) Pour $a, b \in \mathbf{N}^*$ fixés, l'équation (E) peut être vue comme une équation en c : $3c^2 - 6abc + a^2 + 2b^2 = 0$. Le discriminant réduit de cette équation est $\Delta_3' = 9a^2b^2 - 6b^2 - 3a^2$ et il est ≥ 0 et même > 0 sauf dans le cas $a = b = 1$. Les solutions c', c'' de cette équation sont réelles positives. Elles sont entières si et seulement si Δ_3' est le carré d'un entier δ_3 et on a $c', c'' = \dfrac{3ab \pm \delta_3}{3}$. Elles vérifient $c'' = 2ab - c'$ et inversement.

Démonstration. Les trois résultats se montrent de manière analogue. Traitons par exemple le point 3). On a $\Delta_3' = 6b^2(a^2 - 1) + 3a^2(b^2 - 1) \geq 0$ et Δ_3'

n'est nul que pour $a = b = 1$. Les solutions sont positives car leur somme et leur produit le sont. Si les solutions sont entières, $\pm\delta_3 = 3c - 3ab$ est entier. Inversement, si δ_3 est entier, il est multiple de 3 car Δ'_3 l'est, de sorte que c' et c'' sont entières. Enfin, la relation $c'' = 2ab - c'$ n'est autre que la formule donnant la somme des racines.

1.3 Corollaire. *Si (a, b, c) est une solution de (E), on a $a \neq b$ sauf dans le cas $(1, 1, 1)$, $a \neq c$ sauf dans les cas $(1, 1, 1)$ et $(1, 2, 1)$ et $b \neq c$ sauf dans les cas $(1, 1, 1)$ et $(5, 1, 1)$.*

Démonstration. Si $b = c$ (resp. $c = a$, resp. $a = b$) l'équation en a (resp. b, resp. c) a pour discriminant $b^2(9b^2 - 5)$ (resp. $a^2(9a^2 - 8)$, resp. $a^2(9a^2 - 9)$ et pour a ou $b \geq 2$, ces nombres ne sont pas des carrés (le plus grand carré $< 9a^2$ est $(3a-1)^2 = 9a^2-6a+1 \leq 9a^2-11$). On vérifie qu'il reste seulement les trois cas annoncés.

2 Les opérations markoviennes

Ce paragraphe est directement inspiré du cas originel de l'équation de Markov.

2.1 Les opérations et les solutions primitives

2.1 Proposition-Définition. *Soit $\mathcal{S}$ l'ensemble des solutions de (E) dans $(\mathbf{N}^*)^3$. Les applications suivantes (que l'on nommera opérations markoviennes) laissent stables $\mathcal{S}$ et sont involutives :*

1) $F_1 : (a, b, c) \mapsto (6bc - a, b, c)$,
2) $F_2 : (a, b, c) \mapsto (a, 3ac - b, c)$,
3) $F_3 : (a, b, c) \mapsto (a, b, 2ab - c)$.

Démonstration. Cela résulte essentiellement [2] de 1.2. Traitons le point 1). Si a, b, c est une solution, a est une des racines de l'équation du second degré vue en 1.2.1, disons a', et F_1 change simplement a' en l'autre racine a'' et (a'', b, c) est dans $\mathcal{S}$.

2.2 Définition. *On définit la* **hauteur** *d'une solution $(a, b, c) \in \mathcal{S}$ comme l'entier $h(s) = a + b + c$. On dit qu'une application markovienne F_i est* **croissante** *en (a, b, c) si elle augmente la hauteur : si $F_i(a, b, c) = (a', b', c')$ on a $a' + b' + c' \geq a + b + c$. On dit qu'une solution $(a, b, c) \in \mathcal{S}$ est* **primitive**

2. On peut aussi vérifier directement que $F_i(a, b, c)$ est une solution, mais il faut s'assurer que les nombres sont positifs.

si les trois opérations markoviennes sont croissantes en (a, b, c). Cela signifie qu'on a $3bc \geq a$, $3ac \geq 2b$ et $ab \geq c$.

2.3 *Remarques.* 1) Notons déjà que $(1, 1, 1)$ est primitive. En effet, on a $F_3(1, 1, 1) = (1, 1, 1)$, $F_2(1, 1, 1) = (1, 2, 1)$ et $F_1(1, 1, 1) = (5, 1, 1)$.

2) On vérifie aussitôt que, si a, b, c sont positifs, la hauteur ne peut être invariante par les trois transformations F_i. En effet, cela signifierait qu'on a $ab = c$, $3ac = 2b$ et $3bc = a$ dont la seule solution entière est $(0, 0, 0)$.

Le théorème principal est le suivant :

2.4 Théorème. *La seule solution primitive de (E) dans $(\mathbf{N}^*)^3$ est $(1, 1, 1)$.*

Démonstration. Soit (a, b, c) une solution primitive. Dans les équations du second degré de 1.2, cela signifie que a, b, c est la plus petite racine, les opérations markoviennes consistant à remplacer cette racine par l'autre.

Si $(a, b, c) \neq (1, 1, 1)$, c'est que l'un des nombres a, b, c est > 1. Supposons par exemple que c est le plus grand des trois, les autres cas sont analogues. Si l'on montre que c est la plus grande des racines de $f(c) = 3c^2 - 6abc + 2b^2 + a^2$, on aura la contradiction cherchée. Pour cela, on considère le plus grand parmi a et b. Si c'est a on a $f(a) = 4a^2 + 2b^2 - 6a^2b \leq 6a^2 - 6a^2b \leq 0$, ce qui montre que a est entre les racines de f, donc que c, qui est plus grand que a, est la plus grande racine. Si b est $\geq a$ on a $f(b) = 5b^2 + a^2 - 6ab^2 \leq 6b^2 - 6ab^2 \leq 0$ et, de même, c est la plus grande des racines.

2.2 Conséquences sur les solutions

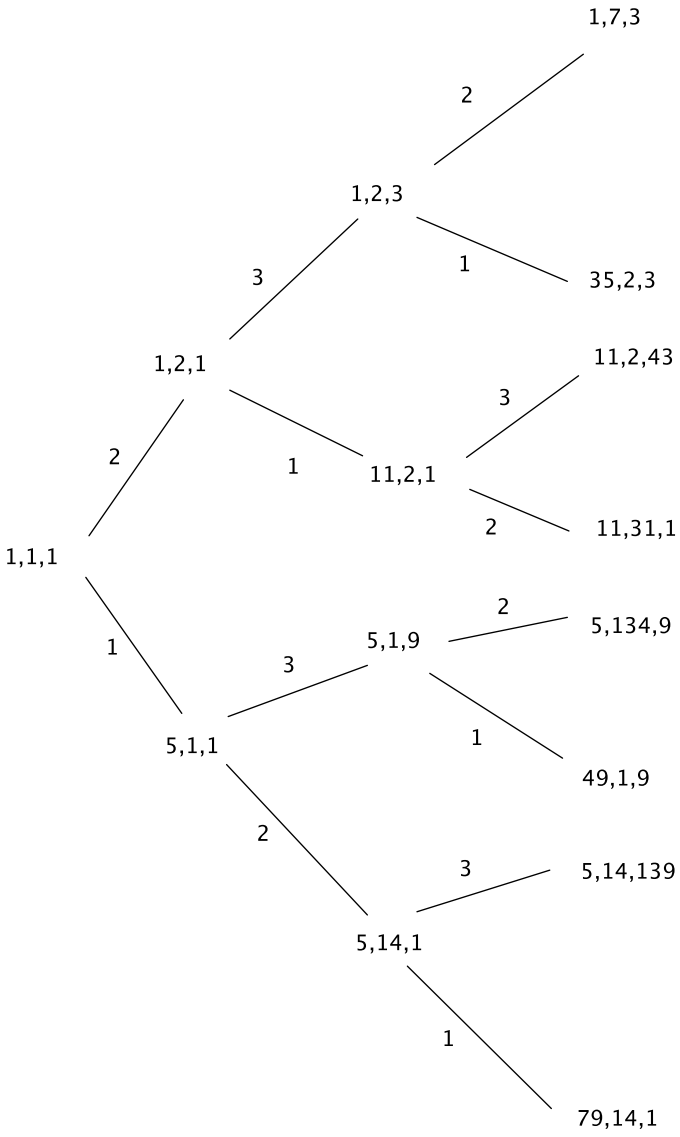
2.2.1 Le graphe des solutions

Le théorème montre déjà qu'on obtient toutes les solutions de (E) en composant les applications F_i :

2.5 Corollaire. *Toute solution de (E) s'obtient à partir de $(1, 1, 1)$ par un nombre fini d'opérations F_i, que l'on peut supposer croissantes.*

Démonstration. On raisonne par l'absurde. On considère une solution $s = (a, b, c)$ qui ne vérifie pas la propriété et sa hauteur $h(s) = a + b + c$ et on peut supposer que cette hauteur est minimum. On a $s \neq (1, 1, 1)$, de sorte que s n'est pas primitive. Il existe donc un indice i tel que $s' = F_i(s)$ soit de hauteur plus petite que s. L'hypothèse de minimalité montre que s' s'obtient à partir de $(1, 1, 1)$ en composant des opérations F_i croissantes, mais alors $s = F_i(s')$ aussi, ce qui est absurde.

On obtient ainsi, de proche en proche, le graphe des solutions (le nombre affiché près d'une arête est le i de l'opération F_i qui passe d'un sommet à l'autre) :



2.2.2 Infinitude des solutions

On a une infinité (multiple) de solutions de l'équation (E) :

2.6 Théorème. *1) Si pour a (resp. b, resp. c) fixé l'équation admet une solution (a, b, c) elle en a une infinité.*

2) Il y a une infinité de a (resp. b, resp. c) tels que l'équation admette une solution avec cette valeur.

Démonstration. 1) On utilise les opérations markoviennes grâce au lemme suivant :

2.7 Lemme. *Soit $s = (a, b, c) \in \mathcal{S}$, distincte de $(1, 1, 1)$. Alors, parmi les trois solutions $F_i(s)$, deux sont de hauteurs strictement plus grandes que $h(s)$ et la troisième de hauteur strictement plus petite.*

En particulier, la chaîne descendante issue de s en utilisant les opérations markoviennes est unique.

Démonstration. Le fait qu'il y ait une des transformées dont la hauteur est plus petite a été vu au corollaire 2.5. Si, par exemple, $F_2(s)$ et $F_3(s)$ sont de hauteurs strictement plus petites que $h(s)$, c'est qu'on a à la fois $3ac \leq 2b$ et $ab \leq c$ mais on en déduit $2b \geq 3a^2b$, donc $a^2 \leq 2/3$ et c'est absurde.

2.8 *Remarque.* Dans le cas de $s = (1, 1, 1)$ on a $F_1(s) = (5, 1, 1)$, $F_2(s) = (1, 2, 1)$, strictement plus grandes et $F_3(s) = s$.

L'assertion 1) résulte du lemme. Traitons par exemple le cas de a. S'il n'y a qu'un nombre fini (non nul) de solutions avec a fixé on en choisit une de hauteur maximum. Mais le lemme montre que l'une des solutions $F_2(s)$ ou $F_3(s)$ est de hauteur plus grande que s, ce qui est absurde.

2) Fixons un b tel qu'il existe une solution a, b, c. En vertu de 1), il y a une infinité de solutions a_n, b, c_n. De plus, pour b, c fixés il y a au plus deux solutions (les racines de l'équation du second degré), de sorte qu'il y a une infinité de a_n donnant des solutions.

2.9 *Remarques.* 1) Le lemme 2.7 montre qu'il y a 2^n solutions "au niveau n" c'est-à-dire obtenues par application de n opérations markoviennes.

2) Nous verrons au paragraphe suivant une autre méthode, plus globale, pour trouver les solutions avec a fixé.

2.2.3 D'autres propriétés : taille, divisibilité

Le théorème 2.4 permet de montrer que pour a, b ou c fixé, si l'on a des solutions, on en a de hauteur assez petite :

2.10 Corollaire. *S'il existe une solution (a, b, c) de (E) avec $a > 1$ (resp. $b > 1$, resp. $c > 1$) fixé, il en existe une avec le même a (resp. b, resp. c) et $bc < a/3$ (resp. $ac < 2b/3$, resp. $ab < c$). En particulier, il existe une solution avec $b, c < a$ (resp. $a, c < b$, resp. $a, b < c$).*

Démonstration. Traitons le cas de a, les autres sont analogues. Choisissons parmi les solutions avec a fixé, celle qui admet la somme $b+c$ minimale. Comme a est plus grand que 1, la solution n'est pas primitive, de sorte qu'elle s'écrit $(a,b,c) = F_i(a',b',c')$ avec $a'+b'+c' < a+b+c$. Dans les cas $i = 2,3$ on a $a' = a$ et cela contredit l'hypothèse de minimalité. Il reste le cas $i = 1$ et on a donc $a' = 6bc - a < a$, d'où le résultat.

2.11 *Remarque.* Du point de vue du calcul, par exemple avec une machine, il suffit donc, pour savoir s'il existe une solution avec une valeur a, b ou c fixée, d'essayer les triplets (a,b,c) avec les autres valeurs plus petites. On constate ainsi que les valeurs $a < 1000$ qui donnent des solutions sont exactement $1, 5, 11, 35, 49, 79, 125, 175, 461, 485$ et 505.

Le théorème 2.4 permet aussi de préciser les facteurs communs des solutions :

2.12 Corollaire. *Soit* $(a,b,c) \in \mathcal{S}$.

1) Deux quelconques des nombres a, b, c *n'ont pas de facteur premier* p *en commun.*

2) Les nombres a *et* c *sont impairs et* b *n'est pas multiple de* 4.

3) Les nombres a, b *ne sont pas multiples de* 3.

Démonstration. On note d'abord que si un nombre premier p divise deux des nombres il divise le troisième. (C'est évident pour $p \geq 5$ et pour $p = 2,3$ il suffit de raisonner modulo 4 ou 9.)

Supposons que le point 1) est faux et prenons un contre-exemple (a,b,c) de hauteur $a+b+c$ minimum. Le nombre premier p divise donc a, b, c. Comme (a,b,c) n'est pas égal à $(1,1,1)$, il s'écrit $(a,b,c) = F_i(a',b',c')$ avec (a',b',c') de hauteur plus petite et on a aussi $(a',b',c') = F_i(a,b,c)$ car F_i est involutive. Les formules donnant les F_i montrent que p divise a', b', c', de sorte que (a',b',c') est aussi un contre-exemple contrairement à l'hypothèse de minimalité.

Pour 2) et 3), on note que si l'un des nombres a ou c est pair l'autre l'est aussi (donc a, b, c sont pairs et c'est absurde) et que si a ou b est multiple de 3 l'autre l'est aussi (et donc les trois le sont et c'est absurde).

Enfin, pour le fait que b n'est pas multiple de 4, on raisonne modulo 8 en notant que le carré d'un nombre impair est congru à 1 modulo 8.

2.13 *Remarque.* Il est relativement facile de montrer le point 1) sans recours au théorème. Pour les autres, je ne sais pas faire sans cela.

Terminons ce paragraphe par une conjecture, qui semble bien naturelle, mais qui n'est manifestement pas si facile :

2.14 Conjecture. *Si $s = (a, b, c)$ et $s' = (a', b', c')$ sont deux solutions avec le même a (resp. même b, resp. même c), il existe une suite d'opérations de Markov F_2, F_3 (resp. F_3, F_1, resp. F_1, F_2) qui font passer de s à s'.*

Cette conjecture sera établie au paragraphe suivant.

3 L'approche *via* l'équation de Pell-Fermat

Le fait que l'équation (E) se ramène à des équations du second degré dont il s'agit de dire si le discriminant est un carré conduit à introduire des anneaux d'entiers quadratiques qui vont permettre de relier le problème à celui, bien mieux connu, de Pell-Fermat.

Rappelons que si D est un entier > 0, l'anneau $\mathbf{Z}[\sqrt{D}]$ est l'ensemble des réels de la forme $z = x + y\sqrt{D}$ avec $x, y \in \mathbf{Z}$. Le conjugué de z est l'élément $\overline{z} = x - y\sqrt{D}$ et la norme de z est l'entier $N(z) = z\,\overline{z} = x^2 - Dy^2$. On sait qu'un élément $u + v\sqrt{D}$ de $\mathbf{Z}[\sqrt{D}]$ est inversible si et seulement si il est de norme ± 1 et on sait aussi que ces éléments (les "unités") sont en nombre infini et qu'ils s'obtiennent à partir de l'un d'eux (l'unité fondamentale) w, de norme ± 1, comme les $\pm w^n$, $n \in \mathbf{Z}$ (on notera qu'on a $\overline{w} = \pm w^{-1}$ si w est une unité). On renvoie à [3] ou [1] pour toutes précisions sur ces questions [3]. Dans les cas qui nous intéressent (on verra qu'ils sont donnés par $D = 9a^2 - 6$ ou $D = 9b^2 - 3$ ou $D = 9c^2 - 2$), on a $D \equiv -1 \pmod 4$ ou D multiple de 3 et il n'y a pas d'unités de norme -1 comme le montre le lemme suivant :

3.1 Lemme. *Soit D un entier congru à -1 modulo 4 ou congru à 0 modulo 3. L'équation $x^2 - Dy^2 = -1$ n'a pas de solutions dans $\mathbf{Z}$.*

Démonstration. Il suffit d'examiner les congruences de x et y modulo 4 ou modulo 3.

3.2 *Remarque.* Qu'il n'y ait pas d'unité de norme -1 est équivalent au fait que longueur de la période du développement en fraction continuée de $\sqrt{D}$ est paire, ce que nous constaterons ci-dessous.

3.1 Les solutions avec a fixé : la voie des unités

3.1.1 Le principe

3.3 Notations. Soit $s = (a, b, c) \in (\mathbf{N}^*)^3$. On pose $D_a(s) = 9a^2 - 6$ (on écrira simplement D s'il n'y a pas de risque de confusion), on définit $\delta = \delta(s) = 3c - 3ab$ et $z = z(s) = \delta(s) + b\sqrt{D}$.

3. Le lecteur est averti que ce paragraphe utilise des notions plus avancées que les précédents.

On a le lemme suivant :

3.4 Lemme. *Soit $a \in \mathbf{N}^*$. L'élément $s = (a, b, c) \in (\mathbf{N}^*)^3$ est une solution de (E) si et seulement si le couple $(\delta(s), b)$ est solution de l'équation*[4] *:*

$$N(z(s)) = \delta(s)^2 - Db^2 = -3a^2 \quad \textit{(notée } (PF_a)\textit{).}$$

L'application qui à $s = (a, b, c)$ associe $(\delta(s), b)$ est une bijection de l'ensemble des solutions de (E) de première coordonnée a sur l'ensemble des solutions de l'équation de Pell-Fermat dans $\mathbf{Z} \times \mathbf{N}^*$, de réciproque donnée par $(\delta, b) \mapsto (a, b, c)$ avec $c = \dfrac{3ab + \delta}{3}$.

Démonstration. C'est essentiellement le point 3) de 1.2 : on considère l'équation de degré 2 en c : $3c^2 - 6abc + 2b^2 + a^2 = 0$, de discriminant réduit $\Delta' = 9a^2b^2 - 6b^2 - 3a^2 = Db^2 - 3a^2$. Si δ est une racine de Δ' on a $\delta^2 - Db^2 = -3a^2$ et $c = \dfrac{3ab \pm \delta}{3}$. On choisit ici la racine δ qui correspond au signe + : $\delta = 3c - 3ab$.

3.5 Corollaire. *Si (a, b, c) est une solution de (E), (b, δ), avec $\delta = 3c - 3ab$, est une solution de (PF_a), correspondant à $z = \delta + b\sqrt{D}$ et on obtient une infinité de solutions de (PF_a) en remplaçant z par $zw^n := \delta_n + b_n\sqrt{D}$ où $w = u + v\sqrt{D}$ est une unité de norme 1 de $\mathbf{Z}[\sqrt{D}]$. Quitte à changer $u + v\sqrt{D}$ en $\pm(u \pm v\sqrt{D})$, on peut supposer $b_n > 0$. On obtient alors une infinité de solutions de (E), (a, b_n, c_n) avec $c_n = \dfrac{3ab_n \pm \delta_n}{3}$.*

On voit qu'on sait calculer une infinité de solutions de (E) à partir de l'une d'elles dès qu'on dispose d'une unité de $\mathbf{Z}[\sqrt{D}]$.

3.1.2 Les unités correspondant aux opérations de Markov

Les opérations de Markov fournissent des unités :

3.6 Lemme. *On reprend les notations de 3.3 et on pose $w = (3a^2 - 1) - a\sqrt{D}$. Si $s = (a, b, c)$ est une solution de (E) et $z = z(s)$, on a les formules :*
1) $z(F_3(s)) = -\overline{z}$,
2) $z(F_2(s)) = -\overline{z}\, w$,

Démonstration. Le cas de F_3 est évident. Pour F_2 on a les formules :

$$b(F_2(s)) = 3ac - b = (3a^2 - 1)b + a\delta \text{ et}$$

4. Que l'on dira de Pell-Fermat, avec beaucoup de réticences.

$$\delta(F_2(s)) = 3ab + 3c - 9a^2c = -(9a^2 - 6)ab - (3a^2 - 1)\delta$$

et, si l'on ne voit pas aussitôt w, on le cherche sous la forme $u + v\sqrt{D}$ en résolvant un système de deux équations linéaires.

3.7 *Remarque.* On notera les formules $z(F_3 \circ F_2(s)) = z\overline{w}$ et $z(F_2 \circ F_3(s)) = zw$.

3.8 *Remarque.* Le travail effectué ci-dessus en prenant c comme inconnue peut être fait de la même manière avec b et l'anneau à considérer est le même : $\mathbf{Z}[\sqrt{D}]$ avec $D = 9a^2 - 6$.

3.1.3 Calcul de l'unité fondamentale

La proposition suivante montre que les unités "de Markov" sont des unités fondamentales :

3.9 Proposition. *Avec les notations de 3.3, l'unité* $w = (3a^2 - 1) - a\sqrt{D}$ *est une unité fondamentale de* $\mathbf{Z}[\sqrt{D}]$.

Démonstration. Ici, on entre dans la théorie de l'équation de Pell-Fermat, et son lien avec les fractions continuées, classique, mais pas si facile, pour laquelle on renvoie à [1] ou [2] par exemple [5].

Il faut déterminer le développement $[a_0, a_1, \ldots, a_n]$ en fraction continuée de $x_0 = \sqrt{9a^2 - 6}$. Le lecteur montrera que, dans le cas $a = 1$, le développement de $\sqrt{3}$ est $[1, \overline{1, 2}]$ et en déduira que l'unité fondamentale est $2 \pm \sqrt{3}$. Traitons le cas $a \geq 2$. On commence par montrer qu'on a $[x_0] = 3a - 1$, c'est-à-dire $3a - 1 \leq x_0 < 3a$, c'est évident par élévation au carré en tenant compte de $a \geq 2$. On considère ensuite $x_0 - [x_0]$, son inverse $x_1 = \dfrac{1}{\sqrt{9a^2 - 6} - 3a + 1} = \dfrac{\sqrt{D} + 3a - 1}{6a - 7}$, et on montre que l'on a $[x_1] = 1$ pour $a \geq 2$. En effet, les inégalités $1 \leq x_1 < 2$ s'écrivent :

$$3a - 6 \leq \sqrt{9a^2 - 6} < 9a - 13,$$

qui sont acquises pour $a \geq 2$.

On continue en montrant que la partie entière de x_2, inverse de $x_1 - [x_1]$, vaut $a - 2$. On a $x_2 = \dfrac{\sqrt{9a^2 - 6} + 3a - 6}{6}$ et les inégalités à montrer sont $3a - 6 \leq \sqrt{D} < 3a$.

5. J'ai écrit ce texte pendant le troisième confinement et je n'avais pas accès à une bibliothèque universitaire. Heureusement l'excellent papier de Lionel Ponton ([2]) m'a permis de répondre à bon nombre des questions que je me posais.

Ensuite, on calcule x_3, inverse de $x_2 - [x_2]$, on a $x_3 = \dfrac{\sqrt{D} + 3(a-2)}{6a-7}$ et on vérifie qu'on a $[x_3] = 1$.

On passe à x_4, inverse de $x_3 - [x_3]$ et, ô merveille, on trouve $x_4 = \sqrt{D} + 3a - 1 = x_0 + [x_0]$, d'où $[x_4] = 2[x_0] = 2(3a-1)$ et $x_4 - [x_4] = x_0 - [x_0]$, de sorte qu'on a $x_5 = x_1$. On vérifie ainsi que la fraction continuée est périodique (c'est bien connu) et on a son expression : $[3a-1, \overline{1, a-2, 1, 6a-2}]$. Comme la période est paire, la théorie de l'équation de Pell-Fermat assure alors que, si l'on pose :

$$\frac{p_3}{q_3} = 3a - 1 + \frac{1}{1 + \frac{1}{a-2+1}} = \frac{3a^2-1}{a}$$

une unité fondamentale est $p_3 + q_3\sqrt{D} = 3a^2 - 1 + a\sqrt{D} = \overline{w}$ (de norme 1) comme annoncé.

Au passage on a prouvé :

3.10 Corollaire. *On pose $D = 9a^2-6$. Les réduites p_n/q_n du développement en fraction continuée de $\sqrt{D}$ sont données (pour $n \geq 0$) par les formules suivantes : $p_{-2} = 0$, $p_{-1} = 1$, $p_0 = 3a-1$, $p_1 = 3a$, $p_2 = 3a^2 - 3a - 1$, $p_3 = 3a^2 - 1$; $q_{-2} = 1$, $q_{-1} = 0$, $q_0 = 1$, $q_1 = 1$, $q_2 = a-1$, $q_3 = a$.*

On en déduit le résultat suivant :

3.11 Corollaire. *On pose $D = 9a^2-6$. Les seuls entiers m tels que l'équation $x^2 - Dy^2 = m$ admette une solution avec x, y entiers premiers entre eux et $m < \sqrt{D}$ sont $m = 1$, $m = -6a + 7$ et $m = 6$.*

Démonstration. C'est le théorème 14 de [2]. Avec ses notations, on a $v_0 = 1$, $v_1 = 6a - 7$, $v_2 = 6$, $v_3 = 6a - 7$, $v_4 = 1$.

3.12 *Remarque.* Pour $m = 1$ on a la solution $x = 3a^2 - 1$, $y = a$, pour $m = -6a + 7$, $x = 3a - 1$, $y = 1$ et pour $m = 6$, $x = 3a$, $y = 1$.

3.2 Les solutions pour a fixé : ubiquité de la voie des unités

3.2.1 L'équivalence

Ce paragraphe a un double but : revenir sur la conjecture 2.14 et montrer que la voie des unités donne toutes les solutions avec a fixé. La convergence de ces deux préoccupations réside dans la proposition suivante :

3.13 Proposition. *Soit a un entier positif et $D = 9a^2 - 6$. Les propriétés suivantes sont équivalentes :*

1) Si $s = (a, b, c)$ et $s' = (a, b', c')$ sont deux solutions de (E), de première coordonnée a, il existe une suite d'opérations de Markov F_2, F_3 qui font passer de s à s'.

2) Il y a une unique solution $s = (a, b, c)$ minimale[6]*, au sens où $h(F_1(s)) > h(s)$.*

3) Si $s = (a, b, c)$ et $s' = (a, b', c')$ sont deux solutions de (E), de première coordonnée a, il existe w, unité de $\mathbf{Z}[\sqrt{D}]$ telle que l'on ait, avec les notations de 3.3, $z(s') = wz(s)$ ou $z(s') = w\overline{z}(s)$.

Démonstration. L'équivalence de 1) et 3) vient de 3.6. Montrons que 2) implique 1). Si s n'est pas minimale c'est que l'unique F_i qui diminue s est F_2 ou F_3 et on continue ainsi jusqu'à trouver une solution minimale en conservant le même a. On procède de même avec s' et on conclut par l'unicité de la solution minimale. Inversement, si l'on a deux solutions minimales, par 1) on peut les joindre par des opérations F_2, F_3, et il y a dans la chaîne ainsi obtenue une solution de hauteur plus grande que s et s'. On prend alors une telle solution t de hauteur maximale et $F_2(t)$ et $F_3(t)$ sont toutes deux de hauteur plus petite, mais c'est absurde en vertu de 2.7.

3.2.2 Le théorème, énoncé et premières approches

3.14 Théorème. *Les trois assertions de 3.13 sont vraies.*

Avant de prouver cette assertion dans le cas général, commençons par examiner quelques cas particuliers.

3.2.3 Approche par la condition 2) : le cas a petit

Pour a fixé, il est facile de vérifier la condition 2). En effet une solution a-minimale est telle que l'unique opération de Markov décroissante est F_1 et elle vérifie donc $3bc < a$ ce qui contraint fortement les solutions, notamment parce que b et c sont plus petits que a. Ainsi, pour $a = 1$ la seule solution minimale est $(1, 1, 1)$, pour $a = 5$ c'est $(5, 1, 1)$, pour $a = 11$, c'est $(11, 2, 1)$, pour 35, $(35, 2, 3)$, etc. On vérifie ainsi le théorème sur la liste des solutions de taille ≤ 1000.

Un programme un peu plus sérieux[7] qui limite les essais aux b, c tels que $3bc < a$ et qui ne prend en compte que les bonnes congruences de a

6. On précisera a-minimale, si besoin est.
7. Mais dont l'exécution a tout de même pris quelques heures.

et b (voir 3.21 et 3.24) fournit l'ensemble des 30 solutions a-minimales pour $a < 100000$: $(1,1,1)$; $(5,1,1)$; $(11,2,1)$; $(35,2,3)$; $(49,1,9)$; $(79,14,1)$; $(125,7,3)$; $(175,31,1)$; $(461,7,11)$; $(485,1,89)$; $(505,2,43)$; $(1259,223,1)$; $(1609,2,137)$; $(1715,26,11)$; $(2789,494,1)$; $(4801,1,881)$; $(5599,313,3)$; $(6395,26,41)$; $(7231,134,9)$; $(11671,14,139)$; $(19999,1118,3)$; $(20065,3554,1)$; $(23219,2,1977)$; $(23861,97,41)$; $(44449,7873,1)$; $(47525,1,8721)$; $(71339,1322,9)$; $(73249,7,1747)$; $(73979,2,6299)$; $(89045,97,153)$.

Sur cette liste on voit que le théorème 3.14 est vérifié puisqu'aucune valeur de a n'apparaît deux fois. On note dans la liste des nombres a premiers, ou produit de deux nombres premiers (éventuellement avec des puissances), voire de trois : $23219 = 7 \times 31 \times 107$ ou $89045 = 5 \times 11 \times 1619$.

3.2.4 Approche par la condition 3) : le cas a premier

Montrons la condition 3) de la proposition 3.13 dans le cas où a est premier. En vertu de 3.4 on a $z\,\overline{z} = z'\,\overline{z}' = -3a^2$. On utilise ici le fait que $\mathbf{Z}[\sqrt{D}]$ est un anneau de Dedekind [8] (car $D \equiv 3 \pmod 4$) et on a donc une décomposition unique des idéaux en produits d'idéaux premiers. On commence par décomposer l'idéal (3). On a les isomorphismes $\mathbf{Z}[\sqrt{D}]/(3) \simeq \mathbf{Z}[T](3, T^2 - D) \simeq (\mathbf{Z}/3\mathbf{Z})[T]/(T^2)$ car 3 divise D. L'idéal (3) est donc le carré de l'idéal premier $\mathfrak{m} = (3, \sqrt{D})$. En revanche, comme a est premier avec 6 et que -6 est un carré modulo a (voir ci-dessous 3.21), on a $(a) = \mathfrak{p}\,\overline{\mathfrak{p}}$ avec $\mathfrak{p} = (a, \sqrt{D} - u)$ et $\overline{\mathfrak{p}} = (a, \sqrt{D} + u)$ où u et $-u$ sont les racines de $D = -6$ modulo a. On note que l'on a $\mathfrak{p} + \overline{\mathfrak{p}} = (1)$ car cet idéal contient a et -6 et on a vu en 2.12 que ces entiers sont premiers entre eux.

En définitive, on a $(z\,\overline{z}) = (z'\,\overline{z}') = \mathfrak{m}^2\mathfrak{p}^2\overline{\mathfrak{p}}^2$. L'idéal $\mathfrak{m}$ divise (z) ou $(\overline{z})$ et, comme il est égal à son conjugué, il divise les deux, et de même pour (z'). L'idéal $\mathfrak{p}$ divise (z) ou $(\overline{z})$ et de même avec z'. Supposons par exemple que $\mathfrak{p}$ divise (z) et (z'). Alors $\mathfrak{p}$ ne divise pas $(\overline{z})$, sinon $\overline{\mathfrak{p}}$ diviserait (z) et c'est impossible car $\mathfrak{p}$ et $\overline{\mathfrak{p}}$ engendrent l'idéal unité. On a donc $(z) = \mathfrak{m}\mathfrak{p}^2$ et $(\overline{z}) = \mathfrak{m}\overline{\mathfrak{p}}^2$ et, de même, $(z') = \mathfrak{m}\mathfrak{p}^2$. On en déduit $(z) = (z')$ ce qui signifie que ces éléments sont associés, comme annoncé.

3.15 *Remarques.* 1) La même démonstration vaut pour a puissance d'un nombre premier. Le cas difficile est celui où a admet plusieurs facteurs premiers distincts (par exemple $a = 35$). En effet, si l'on décompose $(5) = \mathfrak{p}\,\overline{\mathfrak{p}}$ et $(7) = \mathfrak{q}\,\overline{\mathfrak{q}}$, il faut expliquer pourquoi, si $\mathfrak{p}$ divise (z) et (z'), $\mathfrak{q}$ ne peut diviser (z) et $(\overline{z}')$, voir ci-dessous.

2) Attention, pour un entier positif D quelconque, si l'on a deux éléments $z, z' \in \mathbf{Z}[\sqrt{D}]$ de même norme, il n'est pas vrai en général que z'/z ou $z'/\overline{z}$

8. Voir par exemple [3].

est dans $\mathbf{Z}[\sqrt{D}]$ (ce qui donnerait aussitôt l'assertion 3). Par exemple, pour $D = 3$ on a un contre-exemple : $z = 1+9\sqrt{3}$ et $z' = 11+11\sqrt{3}$ sont tous deux de norme -242, mais les quotients ne sont pas dans l'anneau ! L'explication est dans la décomposition en produits d'idéaux premiers : on a $(z) = \mathfrak{p}^2\mathfrak{m}$ et $(z') = \mathfrak{p}\overline{\mathfrak{p}}\mathfrak{m}$ avec $\mathfrak{p} = (11, 5 + \sqrt{3})$ et $\mathfrak{m} = (1 + \sqrt{3})$.

3.2.5 La preuve de 3.14

Nous passons [9] à la preuve du théorème 3.14.

On suppose que a s'écrit $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec des p_i premiers distincts. On pose $D = 9a^2 - 6$. Soient z, z' deux éléments de $A := \mathbf{Z}[\sqrt{D}]$ tels que $N(z) = z\overline{z} = N(z') = z'\overline{z'} = -3a^2$. Si $\mathfrak{m}$ est l'idéal $(3, \sqrt{D})$, on a vu ci-dessus qu'il divise à la fois (z) et (z'). Comme a est premier avec 6 les nombres premiers p_i sont non ramifiés dans A, et comme -6 est un carré modulo a (voir ci-dessous 3.21) ils sont décomposés en $(p_i) = \mathfrak{p}_i\overline{\mathfrak{p}_i}$ et $\mathfrak{p}_i$ et $\overline{\mathfrak{p}_i}$ sont étrangers (voir 3.2.4). Cela implique qu'un seul des idéaux $\mathfrak{p}$, $\overline{\mathfrak{p}}$ divise z (et de même pour z'). Sinon, comme ils sont premiers entre eux, $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ diviserait (z), donc p diviserait b et comme il divise a c'est impossible en vertu de 2.12.

Quitte à renommer les idéaux on peut supposer qu'on a $(z) = \mathfrak{m}\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$, $(z') = \mathfrak{m}\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_s^{\alpha_s}\overline{\mathfrak{p}_{s+1}}^{\alpha_{s+1}} \cdots \overline{\mathfrak{p}_r}^{\alpha_r}$ et $(\overline{z'}) = \mathfrak{m}\overline{\mathfrak{p}_1}^{\alpha_1} \cdots \overline{\mathfrak{p}_s}^{\alpha_s}\mathfrak{p}_{s+1}{}^{\alpha_{s+1}} \cdots \mathfrak{p}_r{}^{\alpha_r}$. Si l'on a $s = 0$ ou $s = r$, (z) est associé à $(\overline{z'})$ ou (z') et on a le résultat. Sinon, si l'on pose $I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_s^{\alpha_s}$ et $J = \mathfrak{p}_{s+1}{}^{\alpha_{s+1}} \cdots \mathfrak{p}_r{}^{\alpha_r}$, on a $(z) = \mathfrak{m}IJ$, $(\overline{z'}) = \mathfrak{m}\overline{I}J$. Dans le groupe des classes d'idéaux $C(A)$ (modulo les idéaux principaux) on a donc $I = \overline{I}$. Comme $I\overline{I}$ est égal à $(p_1^{\alpha_1} \cdots p_s^{\alpha_s})$ donc principal, il en est de même de I^2 et de J^2. Supposons par exemple que I^2 est celui des deux de plus petite norme et posons $I^2 = (w)$ avec $w = x + y\sqrt{D}$. On a $N(I) = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \leq \sqrt{a}$, donc $N(w) = N(I^2) = N(I)^2 \leq a \leq \sqrt{D}$. De plus, x et y sont premiers entre eux. En effet, si un nombre premier p les divise, il divise aussi la norme de I^2 et c'est donc l'un des p_i. Mais alors, $(p_i) = \mathfrak{p}_i\overline{\mathfrak{p}}_i$ divise I^2, donc $\mathfrak{p}_i$ et $\overline{\mathfrak{p}}_i$ divisent I et, vu la construction, c'est absurde car un seul des idéaux $\mathfrak{p}_i$ et $\overline{\mathfrak{p}}_i$ le divise.

On peut donc appliquer 3.11 et on a $N(w) = 1$, 6 ou $-6a + 7$. Comme les facteurs premiers de $N(w)$ sont ceux de a, qu'il est plus petit que $\sqrt{D}$ et que a est premier avec 6, il ne reste que le cas $N(w) = 1$. Cela signifie que I^2 est l'idéal unité, mais comme s est positif, c'est absurde car I^2 est inclus dans $\mathfrak{p}_1$.

9. Cette preuve est plus délicate que le reste du texte et elle utilise un peu plus la théorie des anneaux de Dedekind. L'auteur espère qu'il ne s'y est pas fourvoyé.

3.3 Les solutions avec b ou c fixés

Les résultats sont analogues avec b (resp. c) fixé [10] : on utilise l'équation en a (resp. en b) et il s'agit de résoudre en c et δ (resp. en a et δ) l'équation diophantienne $\delta^2 - Dc^2 = -2b^2$ avec $D = 9b^2 - 3$ (resp. $\delta^2 - Da^2 = -6c^2$ avec $D = 9c^2 - 2$). Si on a une solution on en a une infinité en utilisant les unités de $\mathbf{Z}[\sqrt{D}]$. De plus on a les analogues de 3.6 :

3.16 Lemme. *Soit $s = (a, b, c)$ une solution de (E). On pose $D = 9b^2 - 3$, $\delta = a - 3bc$, $z = \delta + c\sqrt{D}$. On a les formules :*
1) $z(F_1(s)) = -\overline{z}$,
2) $z(F_3(s)) = \overline{z}w$ avec $w = 1 - 6b^2 + 2b\sqrt{D}$.

3.17 Lemme. *Soit $s = (a, b, c)$ une solution de (E). On pose $D = 9c^2 - 2$, $\delta = 2b - 3ac$, $z = \delta + a\sqrt{D}$. On a les formules :*
1) $z(F_2(s)) = -\overline{z}$,
2) $z(F_1(s)) = \overline{z}w$ avec $w = 1 - 9c^2 + 3c\sqrt{D}$.

3.4 Exemples

3.4.1 Le cas $a = 1$

Dans ce cas, avec les notations précédentes, on a $D = 9a^2 - 6 = 3$, l'unité fondamentale de $\mathbf{Z}[\sqrt{3}]$ est $w = 2 + \sqrt{3}$, l'équation (PF_a) est $\delta^2 - 3b^2 = -3$, la plus petite solution (qui correspond à la solution $(1, 1, 1)$ de (E)) est $\delta = 0$, $b = 1$, donc $z = \sqrt{3}$ et on obtient une infinité de solutions en prenant les $z_n = \sqrt{3}(2 + \sqrt{3})^n = \delta_n + b_n\sqrt{3}$. On en déduit une infinité de solutions de l'équation de Markov $(1, b_n, c_n)$ avec $c_n = \dfrac{3b_n \pm \delta_n}{3}$.

Voici les premières valeurs : $n = 0$, $b = 1$, $\delta = 0$, $c = 1$; $n = 1$, $b = 2$, $\delta = 3$, $c = 1$ ou $c = 3$; $n = 2$, $b = 7$, $\delta = 12$, $c = 3$ ou $c = 11$; $n = 3$, $b = 26$, $\delta = 45$, $c = 11$ ou $c = 41$; $n = 4$, $b = 97$, $\delta = 168$, $c = 41$ ou $c = 153$; $n = 5$, $b = 362$, $\delta = 627$, $c = 153$ ou $c = 571$; $n = 6$, $b = 1351$, $\delta = 2340$, $c = 571$ ou $c = 2131$, etc.

3.18 *Remarque.* Le théorème 3.14 montre qu'on obtient toutes les solutions de (E) avec $a = 1$ par cette procédure. Dans ce cas, on peut le retrouver directement. En effet, si l'on a $\delta + b\sqrt{3}$ de norme -3, donc avec $\delta^2 - 3b^2 = -3$, on voit que δ est multiple de 3. Si l'on divise par $\sqrt{3}$, on trouve que $b + (\delta/3)\sqrt{3}$ est dans A et de norme 1, donc un inversible. On voit que toutes les solutions z de norme -3 sont de la forme $\sqrt{3}w$ où w est une unité. Dans le cas $a = 1$, comme le conjugué de $\sqrt{3}$ est $-\sqrt{3}$, $z'_n = \sqrt{3}\,\overline{w}^n = \sqrt{3}(2 - \sqrt{3})^n = -\overline{z_n} = -\delta_n + b_n\sqrt{3}$ ne donne pas de nouvelle solution.

10. Le lecteur se chargera des détails.

3.4.2 Le cas $a = 5$

Cette fois, on a $D = 219$, une unité fondamentale est $w = 74 + 5\sqrt{219}$, l'équation (PF_a) est $\delta^2 - 219b^2 = -75$ et on a la solution $b = 1$, $\delta = -12$ qui correspond à la solution $(5, 1, 1)$ de (E). On pose $z_0 = -12 + \sqrt{219}$ et on obtient une double infinité de solutions en prenant les $z_n = z_0 w^n = \delta_n + b_n\sqrt{219}$ et les $z'_n = z_0\overline{w}^n = \delta'_n + b'_n\sqrt{219}$. On en déduit une quadruple infinité de solutions de l'équation de Markov $(5, b_n, c_n)$ et $(5, b'_n, c'_n)$ avec $c_n = \dfrac{15b_n \pm \delta_n}{3}$ et de même pour c'_n.

3.19 *Exemple.* Avec $n = 0$ on a les solutions $(5, 1, 1)$ et $(5, 1, 9)$. Avec $n = 1$ on a $b = 14$, $\delta = 207$ et les solutions $(5, 14, 1)$ et $(5, 14, 139)$ ou $b' = 134$, $\delta' = -1983$ et les solutions $(5, 134, 9)$ et $(5, 134, 1331)$. Avec $n = 2$, on a $\delta = 30648$ et $b = 2071$ et les solutions $(5, 2071, 139)$ et $(5, 2071, 20571)$ ou $b' = 19831$ et $\delta' = -293472$ et les solutions $(5, 2071, 1331)$ et $(5, 2071, 196979)$. On peut ainsi trouver des solutions arbitrairement grandes, par exemple, avec $n = 8$, on trouve :

$$(5, 208351166167830721, 13983933906256721).$$

3.20 *Remarque.* En vertu de 3.14 la procédure ci-dessus fournit toutes les solutions de (E) avec $a = 5$.

3.4.3 Le cas $b = 1$

On a $D = 6$, une unité fondamentale est $w = 5+2\sqrt{6}$, l'équation (PF_b) est $\delta^2-6c^2 = -2$. La solution $(1, 1, 1)$ donne $c = 1, \delta = -2$ donc $z = -2+\sqrt{6}$. On obtient les solutions $\delta_n + c_n\sqrt{6} = (-2 + \sqrt{6})(5 + 2\sqrt{6})^n = zw^n$ de l'équation de Pell-Fermat et on en déduit les solutions de (E) en posant $a_n = 3c_n \pm \delta_n$. Avec $n = 1$ on trouve $(5, 1, 1)$, avec $n = 2$, $(5, 1, 9)$ et $(49, 1, 9)$, avec $n = 3$, $(49, 1, 89)$ et $(485, 1, 89)$, avec $n = 4$, $(485, 1, 881)$ et $(4801, 1, 881)$, etc.

On notera que les produits de z par les $\overline{w}^n$ ne donnent rien de plus à cause de la formule $\overline{zw} = -z$.

3.5 Facteurs premiers de a

Il reste une question délicate : une valeur de a (par exemple) étant donnée, comment savoir s'il existe une solution $(a, b, c) \in \mathcal{S}$? La réponse n'est pas évidente. On a vu que cette existence est équivalente à celle d'une solution de $\delta^2 - Db^2 = m$ avec $D = 9a^2 - 6$ et $m = -3a^2$. Mais comme $|m|$ est plus grand que $\sqrt{D}$ les résultats de [2] ne s'appliquent pas. Cependant, on dispose de conditions nécessaires en termes de congruences.

3.21 Proposition. *Soit a, b, c une solution de l'équation. Alors, a est congru à $1, 5, 7$ ou 11 modulo 24 ainsi que tous ses facteurs premiers.*

Démonstration. On utilise ici librement le symbole de Legendre et la loi de réciprocité quadratique pour lesquels on renvoie à [4].

Le premier point résulte du second car $\{1, 5, 7, 11\}$ est un sous-groupe de $(\mathbf{Z}/24\mathbf{Z})^*$. Soit donc p un diviseur premier de a, qui est ≥ 5 en vertu de 2.12. Comme p divise a^2 et $6abc$, il divise $2b^2 + 3c^2$ et on a donc $4b^2 = -6c^2$ modulo p. Comme p ne divise pas c (toujours 2.12), on voit que -6 est un carré modulo p, c'est-à-dire que le symbole de Legendre $\left(\frac{-6}{p}\right)$ est égal à 1. Comme on a $-6 = (-1) \times 2 \times 3$, il y a quatre cas.

1) On a $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{2}{p}\right) = 1$ et $\left(\frac{3}{p}\right) = 1$.

2) On a $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{2}{p}\right) = -1$ et $\left(\frac{3}{p}\right) = -1$.

3) On a $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{2}{p}\right) = 1$ et $\left(\frac{3}{p}\right) = -1$.

4) On a $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{2}{p}\right) = -1$ et $\left(\frac{3}{p}\right) = 1$.

En utilisant les critères usuels pour dire que -1 et 2 sont des carrés et la loi de réciprocité quadratique (voir [4]), on voit que ces cas correspondent respectivement à $p \equiv 1 \pmod 8$ et $p \equiv 1 \pmod 3$ donc $p \equiv 1 \pmod{24}$, ou à $p \equiv 5 \pmod 8$ et $p \equiv -1 \pmod 3$ donc $p \equiv 5 \pmod{24}$ ou à $p \equiv -1 \pmod 8$ et $p \equiv 1 \pmod 3$ donc $p \equiv 7 \pmod{24}$ ou enfin à $p \equiv 3 \pmod 8$ et $p \equiv -1 \pmod 3$ donc $p \equiv 11 \pmod{24}$.

3.22 *Exemples.* La liste donnée en 1.1 permet de trouver des solutions (a, b, c) telles que a admette un diviseur premier p avec $p \equiv 1, 5, 7, 11$. Voici quatre exemples : $(5, 1, 1)$, $(11, 2, 1)$, $(79, 14, 1)$, $(485, 1, 89)$ ($485 = 5 \times 97$ et $97 \equiv 1 \pmod{24}$). On a aussi obtenu une solution [11] avec a premier, $a \equiv 1 \pmod{24}$ avec $(4801, 1, 881)$ en 3.4.3.

3.23 *Remarque.* Il y a beaucoup de nombres a avec les bonnes congruences qui ne donnent pas de solutions de l'équation. Pour en trouver, il suffit d'utiliser la liste des solutions (a, b, c) avec des nombres < 1000 vue en 1.1. Les a avec les bonnes congruences qui ne figurent pas dans les résultats n'y figureront jamais en vertu de 2.10. C'est le cas de 25, 29, 31, 53, 55, 59, 73, 77, 83, etc.

11. La plus petite solution avec a premier congru à 1 modulo 24 est $(1609, 2, 137)$.

3.6 Facteurs premiers de b

3.24 Proposition. *Soit a, b, c une solution de l'équation. Les facteurs premiers impairs p de b sont congrus à 1 modulo 3. Le nombre b est congru à 1 ou 2 modulo 6.*

Démonstration. Il suffit d'écrire que -3 est un carré modulo p. La congruence modulo 6 vient du fait que b n'est pas multiple de 4 (voir 2.12).

3.7 Facteurs premiers de c

3.25 Proposition. *Soit a, b, c une solution de l'équation. Alors, c est congru à 1 ou 3 modulo 8 ainsi que tous ses facteurs premiers.*

Démonstration. Cette fois c'est -2 qui est un carré modulo p.

3.26 *Remarque.* Avec ces conditions, il est facile de décider si un nombre a (par exemple) correspond à une solution. Prenons l'exemple de $a = 29$. S'il existe une solution $(29, b, c)$ il en existe une avec $bc < 29/3$ en vertu de 2.10, donc $bc \leq 9$. Comme b est congru à 1 ou 2 modulo 6 et non multiple de 4, cela ne laisse que les possibilités $b = 1, 2, 7$. Comme c est congru à 1 ou 3 modulo 8, les seuls couples (b, c) possibles sont $(1, 1)$, $(1, 3)$, $(1, 9)$, $(2, 1)$, $(2, 3)$ et $(7, 1)$ dont on vérifie qu'ils ne donnent pas de solutions.

3.27 *Remarque.* Par analogie avec l'équation de Markov ordinaire, on peut appeler nombres de Markov de types a, b, c les nombres qui interviennent dans les solutions de (E) aux places a, b, c. Une question non évidente est de savoir s'il y a d'autres nombres que 1 qui soient à la fois de Markov pour les trois types. Il est clair qu'ils devraient être congrus à 1 modulo 24 ainsi que tous leurs diviseurs. L'examen des premiers cas semble indiquer qu'il n'existe pas de tels nombres.

4 Généralisation

On peut s'intéresser, plus généralement, aux équations $E_{a,b,c,k}$ de la forme suivante :

$$ax^2 + by^2 + cz^2 = kxyz$$

avec $a, b, c, k \in \mathbf{N}^*$ et dont on cherche les solutions [12] $x, y, z \in \mathbf{N}^*$.

Dans ce qui suit nous montrons seulement deux choses : le fait qu'il n'y a pas toujours de solutions (voir ci-dessous 4.1) et, au moins conjecturalement, que s'il y en a une [13] il y en a une infinité (voir 4.2).

12. Le lecteur aura noté le changement de notations.
13. Par exemple si l'on prend $k = a + b + c$ il y a la solution $(1, 1, 1)$.

4.1 Un exemple sans solution

4.1 Proposition. *L'équation $x^2 + y^2 + z^2 = 2xyz$ n'a pas de solution dans* $\mathbf{N}^*$.

Démonstration. C'est essentiellement une question de parité, voire de congruences modulo 4. Déjà, il est évident que si x, y, z sont impairs ou si un seul l'est, il n'y a pas de solution, car le premier membre est impair et le second est pair.

Si deux des nombres x, y, z sont impairs, disons x, y et le dernier, z, pair, le premier membre est congru à 2 modulo 4 (car les carrés des nombres impairs sont congrus à 1 modulo 4) et le second à 0 et c'est absurde. Il reste le cas où x, y, z sont tous pairs. On peut supposer qu'ils s'écrivent $x = 2^\alpha x'$, $y = 2^{\alpha+\beta} y'$ et $z = 2^{\alpha+\gamma} z'$ avec x', y', z' impairs, $\alpha > 0$ et $0 \leq \beta \leq \gamma$. Après simplification par $2^{2\alpha}$, il reste :

$$x'^2 + 2^{2\beta} y'^2 + 2^{2\gamma} z'^2 = 2^{\alpha+\beta+\gamma+1} x' y' z'.$$

Si β est positif c'est absurde car le premier membre est impair et le second pair. Si $\beta = 0$, mais $\gamma > 0$, le premier membre, modulo 4, est congru à $x'^2 + y'^2$, donc à 2, et le second est nul et c'est encore absurde. Enfin, si $\beta = \gamma = 0$ on a, modulo 4, $x'^2 + y'^2 + z'^2 \equiv 0$ et c'est toujours absurde.

4.2 Une implique l'infini ?

4.2 Conjecture. *Si l'équation $E_{a,b,c,k}$ admet une solution dans* $\mathbf{N}^*$ *elle en a une infinité.*

Démonstration. Nous montrons la conjecture dans le cas où l'un des nombres a, b, c, disons c, vaut 1 ou est premier. On considère l'équation en Z :

$$cZ^2 - (kxy)Z + ax^2 + by^2 = 0.$$

Son discriminant est $\Delta(x, y) = k^2x^2y^2 - 4cax^2 - 4cby^2$ et on a le lemme suivant :

4.3 Lemme. *On suppose c premier ou égal à 1. Soient $x, y \in \mathbf{N}^*$. L'équation $E_{a,b,c,k}$ admet une solution (x, y, z) dans* $\mathbf{N}^*$ *si et seulement si $\Delta = \Delta(x, y)$ est un carré de* $\mathbf{N}$.

Démonstration. Si l'équation a une solution (x, y, z), on a $z = \dfrac{kxy \pm \sqrt{\Delta}}{2c}$, donc $\Delta = (2cz - kxy)^2$. Inversement, si Δ est un carré, $\Delta = \delta^2$, il suffit de montrer que $2c$ divise $kxy - \delta$ ou $kxy + \delta$. Déjà, il est clair que kxy et δ sont

de même parité, de sorte que 2 divise leur somme et leur différence, ce qui conclut le cas $c = 1$. Si c est premier impair, on a $\delta^2 \equiv k^2x^2y^2 \pmod{c}$ et, comme c est premier, cela implique $kxy \equiv \pm\delta \pmod{c}$ et on a le résultat. Enfin, si $c = 2$ on conclut en notant que $k^2x^2y^2 \equiv \delta^2 \pmod{8}$ et cela implique $kxy \equiv \pm\delta \pmod{4}$.

Si l'équation admet une solution (x, y, z), le lemme montre que $\Delta(x, y)$ est un carré. Fixons x et considérons l'équation $\Delta(x, y) = \delta^2$ comme une équation de Pell-Fermat en δ, y : $\delta^2 - Dy^2 = -4acx^2$ avec $D = k^2x^2 - 4bc$. On obtient alors de nouvelles solutions de l'équation de Pell-Fermat, donc aussi de $E_{a,b,c,k}$ en vertu du lemme, en multipliant $\delta + y\sqrt{D}$ par une unité de $\mathbf{Z}[\sqrt{D}]$. Comme on sait qu'il y a une infinité d'unités dans $\mathbf{Z}[\sqrt{D}]$, on a le résultat.

4.4 *Remarque.* Si aucun des coefficients n'est premier le résultat est moins clair. Par exemple, avec $(a, b, c, k) = (15, 21, 35, 71)$ on a la solution évidente $(1, 1, 1)$ mais aussi $(1, 25, 9)$. Ici on a $D = 2101$, $\Delta = 1 = \delta$, $w = 1 + \sqrt{2101}$, $w' = 1145 \pm 25\sqrt{2101}$. On notera que, dans ce cas, l'analogue du théorème 3.14 est en défaut car ni w'/w si $w'/\overline{w}$ ne sont entiers !

Références

[1] Hardy G.H. & Wright E.M., *An Introduction to the Theory of Numbers*, Oxford University Press, 1938.

[2] Ponton Lionel, *L'équation diophantienne* $ax^2 - by^2 = 1$, arXiv : 1707.07154

[3] Samuel Pierre, *Théorie algébrique des nombres*, Hermann, 1967.

[4] Serre Jean-Pierre, *Cours d'arithmétique*, PUF, 1970.