NAVELET NOUALHIER Maxime

Travaux d'initiative personnelle encadrés

L'équation de Pell-Fermat et autres équations diophantiennes

Réalisé avec M. Jerôme GERMONI

Table des matières

1 Un peu d'histoire

Historiquement, le type d'équations qu'on appelle équations diophantiennes est apparu au III$^{\text{ème}}$ siècle après Jésus-Christ, introduites par le mathématicien grec *Diophante d'Alexandrie*. Ce sont des équations entières, entendons par là que les solutions cherchées sont dans $\mathbb{Z}$, ainsi que les coefficients y apparaissant. De nombreux problèmes ont depuis lors vu le jour et ont pour certains mis longtemps avant d'être élucidés, comme par exemple le dernier théorème de Fermat caractérisant l'existence de solutions à l'équation $x^n + y^n = z^n$ en fonction du nombre n, n'a été résolu qu'en 1995 par *Andrew Wiles*[1] et *Richard Taylor*[2].

L'une de ces équations, attribuée aux mathématiciens *Pierre de Fermat* et suite à une confusion de *Leonhard Euler*, à *John Pell*, va nous intéresser dans la suite de ce document. C'est *Pierre de Fermat* qui remit cette équation au goût du jour au XVII$^{\text{ème}}$ siècle, celle-ci étant déjà connue du mathématicien *Brahmagupta* mille ans auparavant. Plusieurs méthodes de résolution existent, et nous n'allons en traiter que deux. Dans tous les cas, pour être capable de trouver toutes les solutions, il nous faudra connaître la "solution minimale", c'est celle-ci qui engendre le groupe des solutions. Pour cela, nous allons expliciter une méthode efficace qui utilise le développement en fraction continue des nombres quadratiques.

Nous allons aussi nous-même construire trois équations diophantiennes, l'une étant un problème de recherche de "triangles rectangles presque isocèles", l'autre caractérise dans quels cas il existe le même nombre de façons de tirer p boules parmi $n-1$ et $p-1$ parmi n. Et enfin, la dernière est une équation appelée "vol de canards", dont les solutions donnent des pyramides que l'on peut séparer en deux afin d'obtenir deux pyramides de même tailles mais plus petites que la première.
Dans la suite de document, d désignera un entier non carré.

[1] Professeur à l'université de Princeton.
[2] Professeur à l'université d'Harvard.

2 Approche géométrique

2.1 Le groupe $\mathcal{H}$

Dans cette partie $\mathcal{H}$ désignera l'ensemble des points situés sur l'hyperbole d'équation $XY = 1$ dans le repère $(\Omega, \vec{k}, \vec{\ell})$[3].
Nous allons voir dans cette partie comment l'hyperbole[4] $\mathcal{H}$ peut être munie d'une structure de groupe, grâce à une loi que nous noterons $*$.

Définition 2.1.1. *Soit A et B deux points de l'hyperbole $\mathcal{H}$ et M_0 le point de coordonnées $(1, 1)$. Notons Δ_{AB} la droite parallèle à (AB) et passant par M_0. On définit alors $A * B$ par :*
si Δ_{AB} n'est pas tangente à $\mathcal{H}$ en M_0, $A * B = (\Delta_{AB} \cap \mathcal{H}) \setminus \{M_0\}$;
sinon $A * B = M_0$

Remarque. *Par abus de notation, on ne distinguera pas le cas où $A = B$, nous considèrerons que, dans ce cas, (AA) est la tangente à $\mathcal{H}$ en A. Le cas $A = B$ est alors implicitement traité car l'équation de Δ_{AA} (la parallèle à la tangente à $\mathcal{H}$ en A passant par M_0) est :*

$$y = -\frac{1}{x_A^2}x + 1 + \frac{1}{x_A^2}$$

En fait, on peut dire que l'application qui à un couple (A, B) de $\mathcal{H}$, lui associe la droite Δ_{AB} est continue.

Lemme 2.1.2. *La loi $*$ définie ci-dessus est une loi interne sur l'ensemble $\mathcal{H}$.*

Démonstration. Les points d'intersections M de Δ_{AB} et $\mathcal{H}$ s'obtiennent en résolvant le système suivant,

$$\begin{cases} y = x^{-1} \\ (x, y) \in \Delta_{AB} \end{cases}$$

L'équation de la droite Δ_{AB} dans le repère $(\Omega, \vec{k}, \vec{\ell})$ est, en notant (x_A, x_A^{-1}) (resp. (x_B, x_B^{-1})) les coordonnées de A (resp. B) dans $(\Omega, \vec{k}, \vec{\ell})$:

$$\Delta_{AB} : y = -\frac{1}{x_A x_B}x + 1 + \frac{1}{x_A x_B}$$

.
En remplaçant y par x^{-1} dans la seconde équation, il vient l'équation polynomiale suivante,

$$\begin{aligned} & x^2 - (x_A x_B + 1)x + x_A x_B = 0 \\ \Leftrightarrow \quad & (x - x_A x_B)(x - 1) = 0 \end{aligned}$$

[3] Attention, le repère n'est pas nécessairement orthonormé, ni même orthogonal.
[4] Plus généralement toute conique.

Les deux solution cette équation sont donc $x = x_A x_B$ et $x = 1$, qui sont distinctes si $x_A \neq x_B^{-1}$. Dans le cas d'une racine double, on se retrouve en fait dans la situation où Δ_{AB} est la tangente à $\mathcal{H}$ en M_0.

On a ainsi traité les deux cas de figure et la proposition est ainsi démontrée.

□

Remarque. *On gardera en mémoire la relation* $(x, x^{-1}) \in \mathcal{H} \cap \Delta_{AB} \Rightarrow x \in \{1, x_A x_B\}$*, car elle nous sera utile pour démontrer la proposition suivante.*

Proposition 2.1.3. *(i) La loi* $*$ *munit l'ensemble* $\mathcal{H}$ *d'une structure de groupe commutatif.*
(ii) Le groupe $(\mathcal{H}, *)$ *est isomorphe au groupe multiplicatif des réels non nuls* $(\mathbb{R}^*, \cdot)$*.*
(iii) L'application $\Phi : \begin{array}{ccc} \mathcal{H} & \longrightarrow & \mathbb{R}^* \\ (x, \frac{1}{x}) & \longmapsto & x \end{array}$ *réalise cet isomorphisme.*

Démonstration. (i) • $\mathcal{H}$ est stable par $*$ par le lemme précédent.

- Montrons que l'ensemble $\mathcal{H}$ admet un élément neutre pour la loi $*$.
  $\forall A \in \mathcal{H}$, $\Delta_{AM_0} = (AM_0)$ donc $A * M_0 = A$.
- Montrons que tout élément de $\mathcal{H}$ admet un inverse par la loi $*$.
  Soit $A \in \mathcal{H}$. Notons Δ la droite parallèle à la tangente à $\mathcal{H}$ en M_0 et passant par A si $A \neq M_0$, la tangente à $\mathcal{H}$ en M_0 si $A = M_0$.
  On définit alors le point B comme étant le point d'intersection de Δ avec $\mathcal{H}$ autre que M_0 si $A \neq M_0$, ou par M_0 si $A = M_0$. Dans tous les cas, on a $\Delta_{AB} = (M_0 M_0)$.
  On a donc $A * B = M_0$ et $B = A^{-1}$.
- Montrons que la loi $*$ est commutative.
  En effet, il est évident que $\Delta_{AB} = \Delta_{BA}$, ce qui montre bien le point souhaité.

Pour que la loi $*$ munisse $\mathcal{H}$ d'une structure de groupe il faut encore que celle-ci soit associative, ce qui sera démontré en même temps que le second point[5].

(ii) Supposons pour l'instant que $*$ soit associative et donc que $\mathcal{H}$ soit un groupe.

- Soit A et B deux points de $\mathcal{H}$, montrons que $\Phi(A * B) = \Phi(A).\Phi(B)$.
  On a vu, lors de la preuve précédente, que l'équation cartésienne de la droite Δ_{AB} était : $y = -(x_A x_B)^{-1} x + 1 + (x_A x_B)^{-1}$.
  On sait de plus par la remarque précédente que si un point M est dans $\mathcal{H} \cap \Delta_{AB}$, alors son abscisse vaut $x_A x_B$ ou 1. Or, par définition $A * B$ est dans cette intersection, donc l'abscisse de $A * B$ est soit $x_A x_B$, soit 1. Si $x_A x_B \neq 1$, $\mathcal{H} \cap \Delta_{AB}$ contient M_0 et le point d'abscisse $x_A x_B$ qui est donc $A * B$. Sinon Δ_{AB} est la tangente à $\mathcal{H}$ en M_0 et $A * B = M_0$ qui est bien d'abscisse 1.
  D'où $\Phi(A * B) = x_A x_B = \Phi(A)\Phi(B)$.

[5] Une autre preuve sera donnée en annexe, utilisant le *théorème de Pascal*.

De plus soit $\Psi : \mathbb{R}^* \longrightarrow \mathcal{H}$ la fonction qui à un réel x non nul associe le couple (x, x^{-1}) de $\mathcal{H}$.
On vérifie aisément que $\Phi \circ \Psi = \Psi \circ \Phi = id$, donc $\Psi = \Phi^{-1}$, en particulier Φ est bijective.

- Montrons maintenant que $*$ est associative.
D'après les points précédents, Φ réalise un morphisme bijectif entre $\mathbb{R}^*$ et $\mathcal{H}$.
Donc $\forall (A, B, C) \in \mathcal{H}^3$,

$$\begin{aligned}
(A * B) * C &= \Phi^{-1} \circ \Phi((A * B) * C) \\
&= \Phi^{-1}(\Phi(A * B) \cdot \Phi(C)) \\
&= \Phi^{-1}((x_A \cdot x_B) \cdot x_C) \\
&= \Phi^{-1}(x_A \cdot (x_B \cdot x_C)) \\
&= \Phi^{-1}(\Phi(A) \cdot \Phi(B * C)) \\
&= \Phi^{-1} \circ \Phi(A * (B * C)) \\
&= A * (B * C)
\end{aligned}$$

Ainsi, on a montré que $(\mathcal{H}, *)$ était un groupe commutatif isomorphe au groupe des réels non nuls. □

La loi $*$ et le groupe $\mathcal{H}$ étant maintenant bien définis, nous allons voir trois applications des propriétés de ce groupe, la première étant la recherche de "triangles rectangles presque isocèles" (cf définition), la seconde concerne notre problème initial, à savoir la résolution de l'équation de *Pell-Fermat* , et enfin nous traiterons (de manière plus brève) une équation combinatoire. Pour cela nous devons encore montrer que n'importe quelle conique peut être munie de la loi $*$, ou encore qu'il existe un repère tel que cette conique ait une équation de la forme $XY = 1$ (pour une hyperbole) , $Y = X^2$ (pour une parabole) ou encore $X^2 + Y^2 = 1$ (pour une ellipse).

Proposition 2.1.4. *Soit $\mathcal{K}$ une conique. Alors il existe un repère de $\mathbb{R}^2$ tel que $\mathcal{K}$ ait une équation de la forme :*

- *$XY = 1$ si $\mathcal{K}$ est une hyperbole ;*
- *$X^2 + Y^2 = 1$ si $\mathcal{K}$ est une ellipse ;*
- *$Y = X^2$ si c'est une parabole,*

dans ce repère.

Démonstration. L'équation de $\mathcal{K}$ dans le repère $(\Omega, \vec{k}, \vec{\ell})$ est

$$(K) : ax^2 + by^2 + cxy + dx + ey + f = 0$$

Premier cas : Les deux carrés ne sont pas nuls.
On factorise l'équation de $\mathcal{K}$ comme suit :

$$\begin{aligned}
(K) : \quad a'x'^2 + b'y'^2 + d'x' + e'y' + f' &= 0 \\
\Leftrightarrow \quad a'\left(x' + \frac{d'}{2}\right)^2 + b'\left(y' + \frac{e'}{2}\right)^2 + f'' &= 0
\end{aligned}$$

Si $f'' = 0$ alors $\mathcal{K}$ est réduite à un point, sinon on raisonne sur le signe de a' et b'.
On suppose que $f'' = -1$ de sorte que l'équation de $\mathcal{K}$ soit de la forme

$$(K) : a'X^2 + b'Y^2 = 1$$

a', b' sont de même signe. Si il sont tous les deux négatifs, alors $\mathcal{K}$ n'existe pas. Supposons-les donc positifs. On a alors que l'équation de $\mathcal{K}$ s'écrit

$$(K) : \left(\sqrt{a'}X\right)^2 + \left(\sqrt{b'}Y\right)^2 = 1$$

Nous avons donc une ellipse, et si l'on pose $X' = \sqrt{a'}X$ et $Y' = \sqrt{b'}Y$, l'équation de $\mathcal{K}$ est bien de la forme voulue.

$a'b' < 0$ Supposons que $a' > 0$. Le même raisonnement que ci-dessus nous amène à

$$(K) : \left(\sqrt{a'}X\right)^2 - \left(\sqrt{-b'}Y\right)^2 = 1$$

En posant alors $X' = \sqrt{a'}X + \sqrt{-b'}Y$ et $Y' = \sqrt{a'}Y - \sqrt{-b'}Y$, on obtient $(K) : X'Y' = 1$.

□

Corollaire 2.1.5. *Le repère défini précédemment est déterminé de manière unique si l'on fixe un point M_0 de $\mathcal{K}$ dans $(O, \vec{i}, \vec{j})$, et que ses coordonnées soient $(1, 1)$ dans $(\Omega, \vec{k}, \vec{\ell})$.*

Remarque. *En réalité, le repère trouvé n'est pas exactement unique. En effet, relativement à $(\Omega, \vec{k}, \vec{\ell})$, $\mathcal{K}$ est symétrique, et on peut renverser le repère, c'est-à-dire poser $\vec{k} := \vec{\ell}$ et $\vec{\ell} := \vec{k}$.*

Démonstration. Nous allons ici faire la démonstration dans le cas où $\mathcal{K}$ est une hyperbole.
Il existe donc un repère de $\mathbb{R}^2$ tel que *mathcalK* ait une équation réduite $XY = 1$. Posons alors

$$\begin{cases} X' = K_1 X \\ Y' = K_2 Y \end{cases}$$

où K_1 et K_2 sont des constantes vérifiant $K_1 K_2 = 1$. Il reste alors à déterminer ces constantes.
Le point M_0 appartient à $\mathcal{K}$. On a donc :

$$\begin{cases} 1 = K_1 X_0 \\ 1 = K_2 Y_0 \end{cases}$$

$$\Leftrightarrow \quad \begin{cases} K_1 = X_0^{-1} \\ K_2 = Y_0^{-1} \end{cases}$$

En considérant l'autre possibilité qui est d'échanger K_1 et K_2, on a bien déterminer de manière quasi-unique[6] le repère adapté. □

[6] Nous en laissons la vérification au lecteur.

2.2 Application à la recherche des triangles rectangles presque isocèles

Définition 2.2.1. *Nous appellerons triangle rectangle presque isocèle, abrégé en TRPI, un triangle de cotés a, $a+1$ et b, où a et b sont des entiers naturels, tel que celui-ci soit rectangle.*

Si le triangle de cotés a , $a+1$, b est un TRPI, nous dirons que le couple $(a,b) \in \mathbb{N}^2$ définit un TRPI.

Le lemme suivant découle immédiatement de l'application du théorème de Pythagore.

Lemme 2.2.2. *Un couple $(a,b) \in \mathbb{N}^2$ définit un TRPI si et seulement si : $b^2 = 2a^2 + 2a + 1$.*

Proposition 2.2.3. *Le plus petit TRPI non aplati est celui défini par le couple $(3,5)$.*

Démonstration. En effet, le cas $a = 0$ fournit bien un TRPI mais celui-ci est aplatit, le cas $a = 1$ (resp. $a = 2$) nous donne $b = \sqrt{5}$ (resp. $b = \sqrt{13}$) $\notin \mathbb{N}$.
On voit ensuite que $5^2 = 2.3^2 + 2.3 + 1$ ce qui montre le point voulu. □

Nous devons dès lors chercher les points entiers de la conique (qui s'avère être une hyperbole) C d'équation $y^2 = 2x^2 + 2x + 1$.
Réécrivons cette équation sous une forme plus explicite :

$$\begin{aligned} & y^2 = 2x^2 + 2x + 1 \\ \Leftrightarrow \quad & 2y^2 - 4x^2 - 4x = 2 \\ \Leftrightarrow \quad & 2y^2 - (2x+1)^2 + 1 = 2 \\ \Leftrightarrow \quad & (2x + \sqrt{2}y + 1)(-2x + \sqrt{2}y - 1) = 1 \end{aligned}$$

Posons alors le changement de repère défini par :

$$\begin{cases} X = (\sqrt{2}-1)(2x + \sqrt{2}y + 1) \\ Y = (\sqrt{2}+1)(-2x + \sqrt{2}y - 1) \end{cases}$$

ce qui s'écrit encore matriciellement :

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 2\sqrt{2}-2 & 2-\sqrt{2} \\ -2\sqrt{2}-2 & \sqrt{2}+2 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} \sqrt{2}-1 \\ \sqrt{2}+1 \end{pmatrix}$$

Remarque. *Les termes $\sqrt{2} \pm 1$ nous assurent que le point M_0 soit l'élément neutre du groupe C, ie que ses coordonnées dans $(\Omega, \vec{k}, \vec{\ell})$ soient $(1,1)$.*

L'application réciproque est donnée par :

$$\begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{4} \cdot \begin{pmatrix} \sqrt{2}+1 & 1-\sqrt{2} \\ 2+\sqrt{2} & 2-\sqrt{2} \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} - \begin{pmatrix} 1/2 \\ 0 \end{pmatrix}$$

Soit encore :

$$\begin{cases} x &= \dfrac{\sqrt{2}+1}{4}X - \dfrac{\sqrt{2}-1}{4}Y - \dfrac{1}{2} \\ \\ y &= \dfrac{\sqrt{2}+2}{4}X + \dfrac{2-\sqrt{2}}{4}Y \end{cases}$$

Posons alors le nouveau repère $R' = (\Omega, \vec{k}, \vec{\ell})$ définit par :

$$\begin{cases} \Omega &= (-\dfrac{1}{2}, 0) \\ \\ \vec{k} &= \dfrac{1}{4}((\sqrt{2}+1)\vec{i} + (\sqrt{2}+2)\vec{j}) \\ \\ \vec{\ell} &= \dfrac{1}{4}((1-\sqrt{2})\vec{i} + (2-\sqrt{2})\vec{j}) \end{cases}$$

Ainsi nous pouvons munir C d'une structure de groupe grâce à la loi $*$, dans le changement de repère ci-dessus.

Remarque. – *Le repère R' apparaît en fait de manière naturelle, Ω étant le point d'intersection des deux asymptotes de C et les vecteurs $\vec{k}, \vec{\ell}$ en sont des vecteurs directeurs. On dit alors que le repère R' est adapté à l'hyperbole C.*

– *Nous noterons les coordonnées d'un point M en majuscules dans R' et en minuscules dans R.*

Calculons les coordonnées de M_0 et de M_1 dans R'.

$$\begin{aligned} \begin{pmatrix} X_0 \\ Y_0 \end{pmatrix} &= \begin{pmatrix} 2\sqrt{2}-2 & 2-\sqrt{2} \\ -2\sqrt{2}-2 & \sqrt{2}+2 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} \sqrt{2}-1 \\ \sqrt{2}+1 \end{pmatrix} \\ &= \begin{pmatrix} 1 \\ 1 \end{pmatrix} \end{aligned}$$

M_0 est donc l'élément neutre du groupe C
De même, les coordonnées de M_1 dans R' sont $(3+2\sqrt{2}, 3-2\sqrt{2})$.
On définit alors l'application φ comme suit :

$$\varphi : \begin{cases} C & \longrightarrow & C \\ M & \longmapsto & M_1 * M \end{cases}$$

Proposition 2.2.4. *$\forall M = (x, y) \in C$, les coordonnées de $\varphi(M)$ dans R sont :*

$$\varphi(M) : \begin{cases} x' &= 3x + 2y + 1 \\ y' &= 4x + 3y + 2 \end{cases}$$

Démonstration. On a : $\varphi(M) = \begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} (3 + 2\sqrt{2})(\sqrt{2} - 1)(2x + \sqrt{2}y + 1) \\ (3 - 2\sqrt{2})(\sqrt{2} + 1)(-2x + \sqrt{2}y - 1) \end{pmatrix}$

Finalement , $\varphi(M) = \begin{pmatrix} (2 + 2\sqrt{2})x + (2 + \sqrt{2})y + 1 + \sqrt{2} \\ (2 - 2\sqrt{2})x + (2 - \sqrt{2})y + 1 - \sqrt{2} \end{pmatrix}$

Et donc :

$$\begin{aligned} \begin{pmatrix} x' \\ y' \end{pmatrix} &= \frac{1}{4} \cdot \begin{pmatrix} \sqrt{2} + 1 & 1 - \sqrt{2} \\ 2 + \sqrt{2} & 2 - \sqrt{2} \end{pmatrix} \begin{pmatrix} X' \\ Y' \end{pmatrix} - \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix} \\ &= \frac{1}{4} \cdot \begin{pmatrix} \sqrt{2} + 1 & 1 - \sqrt{2} \\ 2 + \sqrt{2} & 2 - \sqrt{2} \end{pmatrix} \begin{pmatrix} (2 + 2\sqrt{2})x + (2 + \sqrt{2})y + 1 + \sqrt{2} \\ (2 - 2\sqrt{2})x + (2 - \sqrt{2})y + 1 - \sqrt{2} \end{pmatrix} - \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix} \\ &= \frac{1}{4} \begin{pmatrix} 12x + 8y + 4 \\ 16x + 12y + 8 \end{pmatrix} \\ &= \begin{pmatrix} 3x + 2y + 1 \\ 4x + 3y + 2 \end{pmatrix} \end{aligned}$$

□

Lemme 2.2.5. *φ est bijective.*

Démonstration. Grâce à la structure de groupe de C, on sait que M_1 admet un inverse.
Soit alors ψ l'application de C dans C définie par : $\forall M \in C, \psi(M) = M_1^{-1} * M$.
On a alors $\varphi(\psi(M)) = M_1^{-1} * (M_1 * M)$
Par associativité, on en déduit $\varphi \circ \psi(M) = M$ et $\psi = \varphi^{-1}$. □

Remarque. *Les coordonnées de $\varphi^{-1}(M)$ se trouvent en résolvant le système de la proposition 2.2.4 pour (x, y). On trouve alors :*

$$\begin{cases} x = 3x' - 2y' + 1 \\ y = 3y' - 4x' - 2 \end{cases}$$

Notons C^+ l'ensemble des points de C d'ordonnée positive, on obtient alors le lemme suivant.

Lemme 2.2.6. *On a : $\varphi(C^+) = C^+$.*

Démonstration. D'après la définition du changement de repère, C^+ est la partie de C située dans le premier quadrant relativement à R'. L'ordonnée de $\varphi(M)$ dans R' est alors $Y' = \underbrace{(3-2\sqrt{2})}_{\geqslant 0} Y \geqslant 0$. □

On définit alors une suite de points $(M_n)_{\mathbb{N}}$ de C de la manière suivante :

$$\forall n \geqslant 0, M_{n+1} = \varphi(M_n) = M_1 * M_n$$

Lemme 2.2.7. *$\forall n \in \mathbb{N}$, M_n définit un TRPI.*

Démonstration. D'après la proposition 2.2.4 , on a les formules de récurrences en notant $M_n = (u_n, v_n)$:

$$\begin{cases} u_{n+1} &= 3u_n + 2v_n + 1 \\ v_{n+1} &= 4u_n + 3v_n + 2 \end{cases}$$

En particulier, M_n est un point à coordonnées entières.
Or, vu la définition de la suite $(M_n)_{\mathbb{N}}$, $M_n \in C$, donc M_n définit bien un TRPI. □

Nous avons donc construit une suite de solutions à notre problème de recherche de TRPI, mais la question que nous devons encore nous poser est est-ce-que la suite $(M_n)_{\mathbb{N}}$ fournit toutes les solutions ? La réponse est oui et nous allons le montrer dans la fin de cette partie.

Définition 2.2.8. *On appelle arc de C^+ de bornes M_n et M_{n+1}, et on note $[M_nM_{n+1}]$, l'ensemble des points M de C^+ dont l'abscisse appartient à l'intervalle réel $[u_n; u_{n+1}]$.*

Lemme 2.2.9. *$\forall n \in \mathbb{N}$, $\varphi([M_nM_{n+1}]) \subseteq [M_{n+1}M_{n+2}]$*

Démonstration. Soit $M(x, y) \in [M_nM_{n+1}]$. Montrons que $\varphi(M) \in [M_{n+1}M_{n+2}]$
On a le système d'inéquation suivant :

$$\begin{cases} u_n \leqslant x \leqslant u_{n+1} \\ v_n \leqslant y \leqslant v_{n+1} \end{cases}$$

En multipliant la première inégalité par 3 et la seconde par 2, on obtient en sommant :

$$3u_n + 2v_n + 1 \leqslant 3x + 2y + 1 \leqslant 3u_{n+1} + 2v_{n+1} + 1$$

En utilisant le fait que $\varphi(C^+) = C^+$, on obtient $\varphi(M) \in [M_{n+1}M_{n+2}]$. □

Lemme 2.2.10. *L'ensemble des points M de C^+ tel que $\varphi(M)$ a une abscisse positive est :*

$$\bigcup_{n\in\mathbb{N}} [M_1^{-1}M_n]$$

Démonstration. Notons E cet ensemble.

$$\begin{aligned} E &= \{(x,y) \in C^+, \varphi(x,y) \text{ a une abscisse positive } \} \\ &= \{(x,y) \in C^+, 3x+2y+1 \geqslant 0, y \geqslant 0\} \\ &= \left\{(x,y) \in C^+, x \geqslant -\frac{2y+1}{3}, y \geqslant 0\right\} \end{aligned}$$

Or la droite (D) d'équation $3x+2y+1=0$ ne coupe C^+ qu'en un seul point qui est M_1^{-1}.
De plus tous les points M de C^+, tels que leur abscisse est plus petite que -1, sont en dessous de (D). On a donc :

$$E = \{(x,y) \in C^+, x \geqslant -1, y \geqslant 0\}$$

□

Remarque. *On a fait montré que, en notant C_+^+ l'ensemble des point de C^+ d'abscisse positive,*

$$\varphi^{-1}(C_+^+) = \left[M_1^{-1} + \infty\right[$$

Proposition 2.2.11. *Pour tout n de $\mathbb{N}$, $\varphi([M_nM_{n+1}]) = [M_{n+1}M_{n+2}]$.*

Démonstration. Soit M un point de $[M_{n+1}M_{n+2}]$. On sait qu'il existe un seul point N dans $[M_1^{-1} + \infty]$ tel que $M = \varphi(N)$. Or si N était d'abscisse supérieure à u_{n+1} , on aurait, par le lemme 2.2.9, que M aurait une abscisse supérieure à u_{n+2}, ce qui est absurde. Il faut donc chercher N dans $[M_1^{-1}M_{n+1}]$. A partir de là, on raisonne par récurrence sur n.
Au rang 0. Soit $M \in [M_1M_2]$. Il existe donc un seul N dans $[M_1^{-1}M_1]$ tel que $M = \varphi(N)$. Supposons $N \in [M_1^{-1}M_0]$. Alors $\varphi(N) \in [M_0M_1]$ et dans ce cas $N = M_0$. Sinon $\varphi(N) \in [M_1M_2]$. La propriété est donc vraie au rang 0.
Supposons-la vraie à un certain rang n, ie : $\varphi([M_{n-1}M_n]) \supseteq [M_nM_{n+1}]$.
Soit $M \in [M_{n+1}M_{n+2}]$. Alors il existe $N \in [M_1^{-1}M_{n+1}]$ tel que $M = \varphi(N)$.
Si $N \in [M_1^{-1}M_n]$, alors $\varphi(N)$ est un point de C^+, d'abscisse comprise entre u_0 et u_{n+1}. Donc le seul point possible est $N = M_n$.
Donc $N \in [M_nM_{n+1}]$. Ce qu'il fallait démontrer. □

Proposition 2.2.12. *Soit (a,b) un couple d'entiers naturels définissant un TRPI. Alors il existe un entier n tel que $(a,b) = M_n$.*

Démonstration. En effet, si (a,b) est un tel couple, alors il appartient à la partie de C^+ formée des points d'abscisse positive.
Il existe donc un entier n tel que (a,b) soit sur l'arc $[M_nM_{n+1}]$. Il suffit alors de montrer que les seuls point à coordonnées entières d'un tel arc sont les points M_n et M_{n+1}.
Supposons que (a,b) soit strictement dans $[M_nM_{n+1}]$ (ie : il ne vaut ni M_n, ni M_{n+1}). On sait par ce qui précède, que (a,b) provient de n application de φ sur M_0.

Or si (a, b) n'est ni M_n, ni M_{n+1}, alors $\varphi^{-n}(a, b)$ n'est ni M_0 ni M_1. Absurde.
Il existe donc un entier n tel que $(a, b) = M_n$.

□

Cette dernière proposition montre bien que la méthode décrite plus haut permet de trouver tous les TRPI existant.
Voici un schéma récapitulatif.

$$\begin{array}{ccc} (M_1)_R & \xrightarrow[P]{} & (M_1)_{R'} \\ & & \downarrow \varphi^n \\ (M_n)_R & \xleftarrow{P^{-1}} & (M_n)_{R'} \end{array}$$

Où P désigne l'application qui permet de passer des coordonnées de R à celle de R'.

Calcul des premiers TRPI

n	u_n	v_n
1	3	5
2	20	29
3	119	169
4	696	985
5	4059	5741

2.3 Application à l'équation de *Pell-Fermat*

Reprenons l'équation, que nous noterons (P) durant la suite de cette partie, $x^2 - dy^2 = 1$. Comme dans la partie précédente, on voit bien que résoudre cette équation revient à trouver les points à coordonnées entières de l'hyperbole, que nous noterons de nouveau C, d'équation $x^2 - dy^2 = 1$ dans le repère $(O, \vec{i}, \vec{j})$, ce que l'on va faire grâce à un changement de repère. Réécrivons (P) sous la forme $(x - \sqrt{d}y)(x + \sqrt{d}y) = 1$. Ainsi le changement de repère apparaît de manière naturelle, posons alors $X = x - \sqrt{d}y$ et $Y = x + \sqrt{d}y$.

Remarque. *Normalement, il faudrait multiplier X et Y par des constantes afin que le point $(1, 0)$ soit bien l'élément neutre, mais c'est déjà le cas ici.*

Durant la suite de cette partie nous noterons R le repère $(O, \vec{i}, \vec{j})$ et R' le nouveau repère $(\Omega, \vec{k}, \vec{\ell})$ où $\Omega = O$, $\vec{k} = \vec{i} - \sqrt{d}\vec{j}$ et $\vec{\ell} = \vec{i} + \sqrt{d}\vec{j}$.

Remarque. *Comme dans la partie précédente, nous noterons en majuscules les coordonnées dans R' et en minuscules celles dans R*

On obtient donc la matrice de passage de R à R' qui est : $P = \begin{pmatrix} 1 & -\sqrt{d} \\ 1 & \sqrt{d} \end{pmatrix}$ et la matrice de passage de R' à R est donc $P^{-1} = \begin{pmatrix} 1/2 & 1/2 \\ \sqrt{d}/2d & -\sqrt{d}/2d \end{pmatrix}$.
Ainsi dans le repère R', C a pour équation $XY = 1$ et possède donc une structure de groupe via la loi $*$ définie dans la partie précédente, avec pour élément neutre le point M_0 de coordonnées $(1, 1)$ dans R' qui a aussi pour coordonnées $(1, 0)$ dans R.

Définition 2.3.1. *On appelle solution minimale de (P), le couple $(x, y) \in \mathbb{N}^2$, vérifiant (P), tel qu'il n'existe aucune autre solution (x', y') de (P) vérifiant $x' \leqslant x$.*

Notons (x_1, y_1) la solution minimale de l'équation de *Pell-Fermat* et M_1 le point de coordonnées (x_1, y_1) dans R de sorte que $M_1 \in C$. Par abus de langage on dira que un point M est solution de l'équation de *Pell-Fermat* si ses coordonnées le sont.
Reprenons l'application[7] φ définie par $\varphi(M) = M_1 * M$.

Lemme 2.3.2. *Les coordonnées de $\varphi(M)$ dans R sont :*

$$\begin{cases} x' = xx_1 + dyy_1 \\ y' = xy_1 + yx_1 \end{cases}$$

[7] φ est bijective du fait de la structure de groupe de C. cf partie 2.2.

Démonstration. Les coordonnées de M_1 dans R' sont $\begin{pmatrix} x_1 + \sqrt{d}y_1 \\ x_1 - \sqrt{d}y_1 \end{pmatrix}$
Les coordonnées de $\varphi(M)$ dans R' sont donc :
$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} (x_1 + \sqrt{d}y_1)(x + \sqrt{d}y) \\ (x_1 - \sqrt{d}y_1)(x - \sqrt{d}y) \end{pmatrix}$$
Les coordonnées de $\varphi(M)$ dans R sont alors données par :
$$\begin{pmatrix} x' \\ y' \end{pmatrix} = P^{-1}\begin{pmatrix} X' \\ Y' \end{pmatrix}$$
$$= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ d^{-1/2} & -d^{-1/2} \end{pmatrix}\begin{pmatrix} (x_1 + \sqrt{d}y_1)(x + \sqrt{d}y) \\ (x_1 - \sqrt{d}y_1)(x - \sqrt{d}y) \end{pmatrix}$$
$$= \begin{pmatrix} xx_1 + dyy_1 + \sqrt{d}(xy_1 + yx_1) + xx_1 + yy_1 - \sqrt{d}(xy_1 + yx_1) \\ d^{-1/2}(xx_1 + dyy_1 + \sqrt{d}(xy_1 + yx_1) - xx_1 + yy_1 + \sqrt{d}(xy_1 + yx_1)) \end{pmatrix}$$
$$= \begin{pmatrix} xx_1 + dyy_1 \\ xy_1 + yx_1 \end{pmatrix}$$
□

Définissons alors la suite $(M_n)_{\mathbb{N}}$ de points de C par :
$$\forall n \in \mathbb{N}, M_{n+1} = M_1 * M_n$$

Proposition 2.3.3. *Pour tout n entier, M_n est solution de (P)*

Démonstration. M_n est à coordonnées entières dans R car M_0 l'est, il appartient de plus à l'hyperbole C. M_n est donc solution de (P). □

Nous avons donc une méthode permettant d'engendrer une infinité de solutions de (P), mais il reste à montrer que la suite $(M_n)_{\mathbb{N}}$ définit bien toutes les solutions.
Notons C_+ la partie de C formée des points d'abscisse positive.

Lemme 2.3.4. $\varphi(C^+) = C^+$

Démonstration. C^+ est la partie de C située dans le premier quadrant, relativement à R'. De plus les coordonnées de $\varphi(M)$ dans R' sont :
$$\begin{cases} X' = X_1 X \\ Y' = Y_1 Y \end{cases}$$
avec $X_1 = x_1 - \sqrt{d}y_1$, $Y_1 = x_1 + \sqrt{d}y_1$.
On a forcément $x_1 \geqslant sqrtdy_1$ car dans le cas contraire, $X_1 Y_1$ serait négatif et ne serait pas sur C
On a donc $X' \geqslant 0$ et $Y' \geqslant 0$, donc $\varphi(M)$ est bien dans le premier quadrant de R'. □

Définition 2.3.5. *On appelle arc de C^+ de bornes M et N, l'ensemble des points de C^+ dont l'ordonnée est comprise entre celle de M et celle de N.*

Lemme 2.3.6. *Pour tout entier n,*

$$\varphi([M_nM_{n+1}]) \subseteq [M_{n+1}M_{n+2}]$$

Démonstration. La preuve est identique à celle donnée dans la partie sur les TRPI, si ce n'est que c'est y qu'il faut encadrer. □

Proposition 2.3.7. *L'ensemble des points M de C^+, tel que $\varphi(M)$ à une ordonnée positive est*

$$\bigcup_{n\in\mathbb{N}} [M_1^{-1}M_n]$$

Démonstration. Notons E cet ensemble. On a alors :

$$\begin{aligned} E &= \{(x,y) \in C^+, x \geqslant 0, \geqslant 0\} \\ &= \left\{(x,y) \in C^+, x \geqslant 0, y \geqslant -\frac{y_1}{x_1}x\right\} \end{aligned}$$

Or la droite (D) d'équation $xy_1 + yx_1 = 0$ ne coupe C^+ qu'en M_1^{-1}. A droite (en restant sur la branche d'ordonnées positives) de ce point, C^+ est au-dessous de (D), et à gauche (sur la branche d'ordonnées négatives ainsi que sur la branche d'ordonnées positives), C^+ est au-dessus de (D). Cela prouve bien l'assertion voulue.

□

Proposition 2.3.8. *Pour tout n entier,*

$$\varphi([M_nM_{n+1}]) = [M_{n+1}M_{n+2}]$$

Démonstration. Là encore, la démonstration est identique à celle de la proposition 2.2.11. □

Proposition 2.3.9. *Soit $(x,y) \in \mathbb{N}^2$. Si (x,y) est solution de (P), alors il existe un entier n tel que $(x,y) = M_n$.*

Démonstration. De la même manière que pour les TRPI, on montre que si (x,y) est sur l'arc $[M_nM_{n+1}]$, mais n'est ni M_n, in M_{n+1}, alors il existe une solution sur l'arc $[M_0M_1]$ distincte de M_0 et M_1. □

Nous avons donc un moyen de trouver toutes les solutions (positives) de (P) (modulo la connaissance de (x_1, y_1)).

d	n	x_n	y_n	d	n	x_n	y_n
3	0	1	0	7	0	1	0
	1	2	1		1	8	3
	1	7	4		1	127	48
	2	26	15		2	2 024	705
	3	97	56		3	32 257	12 192
	4	362	209		4	514 088	194 307
	5	1 351	780		5	81 913 151	3 096 720
	6	5 042	2 911		6	130 576 328	49 353 213
	7	1 881	10 864		7	2 081 028 097	786 554 688
5	0	1	0	11	0	1	0
	1	9	4		1	10	3
	1	161	72		1	199	60
	2	2 889	1 292		2	3 970	1 197
	3	51 841	23 184		3	79 201	23 880
	4	930 249	416 020		4	1 580 050	476 403
	5	16 692 641	7 465 176		5	31 521 799	9 504 180
	6	259 537 289	133 957 148		6	628 855 930	189 607 197
	7	5 374 978 561	2 403 763 488		7	12 545 596 801	3 782 639 760

FIG. 1 – Quelques solutions

2.4 Étude d'une équation combinatoire

Nous allons ici étudier une autre équation, de manière beaucoup plus brève afin de ne pas être trop répétitif, que nous noterons (E) et qui est :

$$\binom{n-1}{p} = \binom{n}{p-1}$$

Où $\binom{n}{p}$ désigne le coefficient binomial $C_n^p = \dfrac{n!}{p!(n-p)!}$.

L'équation (E) s'écrit donc aussi :

$$\begin{aligned} \frac{(n-1)!}{p!(n-p-1)!} &= \frac{n!}{(p-1)!(n-p+1)!} \\ \Leftrightarrow \quad n^2 - 3np + p^2 + n - p &= 0 \end{aligned}$$

On note alors Q la conique d'équation $P(x,y) = x^2 - 3xy + y^2 + x - y = 0$.

$$\begin{aligned} P(x,y) &= x^2 - 3xy + y^2 + x - y \\ &= \left(x - \frac{3}{2}y + \frac{1}{2}\right)^2 - \frac{5}{4}y^2 + \frac{1}{2}y - \frac{1}{4} \\ &= \left(x - \frac{3}{2}y + \frac{1}{2}\right)^2 - \frac{5}{4}\left(y - \frac{1}{5}\right)^2 - \frac{1}{5} \end{aligned}$$

Q est alors décrit par $P(x,y) = 0$, ce qui est équivalent à

$$\begin{aligned} 5\left(x - \frac{3}{2}y + \frac{1}{2}\right)^2 - \frac{25}{4}\left(y - \frac{1}{5}\right)^2 &= 1 \\ \Leftrightarrow \quad \frac{5}{4}(2x - 3y + 1)^2 - \frac{1}{4}(5y - 1)^2 &= 1 \end{aligned}$$

On pose alors :

$$\begin{cases} X = K_1\left[2\sqrt{5}x + \left(5 - 3\sqrt{5}\right)y + \sqrt{5} - 1\right] \\ Y = K_2\left[2\sqrt{5}x - \left(3\sqrt{5} + 5\right)y + \sqrt{5} + 1\right] \end{cases}$$

Où K_1 et K_2 sont des constantes à déterminer, vérifiant $K_1K_2 = 1$. Observons le tableau suivant :

On voit alors que deux solutions apparaissent : $(n,p) = (2,1)$ et $(n,p) = (15,6)$.
On aimerait que le point M_0 de coordonnées $(2,1)$ dans $(O,\vec{i},\vec{j})$ soit l'élément neutre de la conique Q. Il faut pour cela déterminer les constantes K_1 et K_2 de telle sorte que l'on ait bien M_0 de coordonnées $(1,1)$ dans le repère adapté à Q. On trouve ainsi :

$$\begin{cases} K_1 = \dfrac{1}{\sqrt{5} + 2} \\ K_2 = \dfrac{1}{\sqrt{5} - 2} \end{cases}$$

Nous avons encore besoin des coordonnées du point M_1 qui représente la solution mini-

n\p	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1																
1	1	1															
2	1	2	1														
3	1	3	3	1													
4	1	4	6	4	1												
5	1	5	10	10	5	1											
6	1	6	15	20	15	6	1										
7	1	7	21	35	35	21	7	1									
8	1	8	28	56	70	56	28	8	1								
9	1	9	36	84	126	126	84	36	9	1							
10	1	10	45	120	210	252	210	120	45	10	1						
11	1	11	55	165	330	462	462	330	165	55	11	1					
12	1	12	66	220	495	792	924	792	495	220	66	12	1				
13	1	13	78	286	715	1287	1716	1716	1287	715	286	78	13	1			
14	1	14	91	364	1001	2002	3003	3432	3003	2002	1001	364	91	14	1		
15	1	15	105	455	1365	3003	5005	6435	6435	5005	3003	1365	455	105	15	1	
16	1	16	120	560	1820	4368	8008	11440	12870	11440	8008	4368	1820	560	120	16	1

http://nte-serveur.univ-lyon1.fr/nte/immediato/recurrence/chap07/chap07a.htm

FIG. 2 – Triangle de Pascal

male $(15, 6)$.

$$M_1 : \begin{cases} X_1 &= \dfrac{7+3\sqrt{5}}{2} \\ \\ Y_1 &= \dfrac{7-3\sqrt{5}}{2} \end{cases}$$

On définit de nouveau la fonction φ par $\varphi(M) = M_1 * M$, et la suite $(M_n)_{\mathbb{N}}$ par $M_{n+1} = M_1 * M_n$. Nous aurons besoin de pouvoir passer des coordonnées dans $(O, \vec{i}, \vec{j})$ à celles dans $(\Omega, \vec{k}, \vec{\ell})$, ce qui se fait comme suit :

$$(*) \begin{cases} x &= \dfrac{1}{10}\left[\left(5\sqrt{5}+11\right)X + \left(11-5\sqrt{5}\right)Y - 2\right] \\ \\ y &= \dfrac{1}{5}\left[\left(2+\sqrt{5}\right)X + \left(2-\sqrt{5}\right)Y + 1\right] \end{cases}$$

Les coordonnées de $\varphi(M)$ dans $(\Omega, \vec{k}, \vec{\ell})$ sont alors données par :

$$\varphi(M) : \begin{cases} X' &= X_1 X \\ Y' &= Y_1 Y \end{cases}$$

$$\Leftrightarrow \quad \varphi(M) : \begin{cases} X' &= \frac{1}{2}\left[\left(5+\sqrt{5}\right)x - \left(5-\sqrt{5}\right)y + 2\right] \\ Y' &= \frac{1}{2}\left[\left(5-\sqrt{5}\right)x - \left(5+\sqrt{5}\right)y + 2\right] \end{cases}$$

On remplace alors X (resp Y) par X' (resp Y') dans $(*)$ et on trouve :

$$\begin{cases} x' &= 8x - 3y + 2 \\ y' &= 3x - y + 1 \end{cases}$$

Comme dans les autres parties, on a en fait trouvé toutes les solutions de l'équation (E).

n	p	C_{n-1}^{p}
2	1	1
15	6	3003
104	40	$\mathcal{O}(10^{28})$
714	273	$\mathcal{O}(10^{204})$
4895	1870	$\mathcal{O}(10^{1411})$
33552	12816	$\mathcal{O}(10^{9687})$

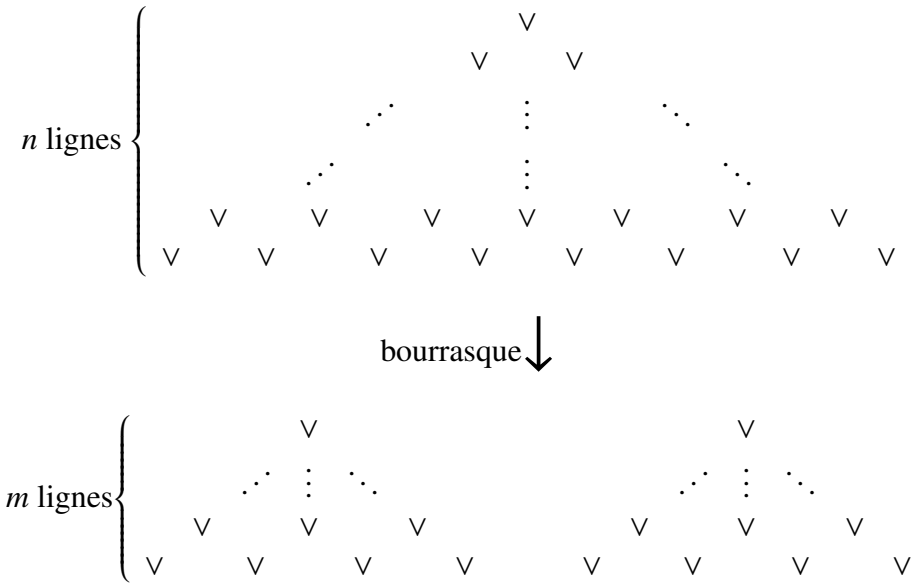
FIG. 3 – Les premières solutions.

Remarque. *La notation $\mathcal{O}$ désigne ici que si $n = \mathcal{O}(p)$ alors n et p ont le même nombre de chiffres.*

2.5 Le vol de canards

Notre problème est ici le suivant : étant donné un groupe de canards constitué de n lignes où chaque ligne compte 1 canard de moins que la précédente, une bourrasque sépare notre groupe de canards en deux autre groupe de m lignes chacun. Dans quels cas aucun canard n'est perdu ?

Schématisons :



Avant la bourrasque, nous avons $n(n+1)/2$ canards, alors qu'après nous en avons $m(m+1)$. Si aucun canard ne s'est perdu, alors l'égalité suivante est vérifiée

$$n^2 + n = 2m^2 + 2m.$$

Nous laissons alors en exercice au lecteur la résolution de cette équation[8].

[8] Il faut multiplier par 4 l'équation.

3 Une approche algébrique

Comme nous l'avons vu dans la partie précédente, l'équation de *Pell-Fermat* (P) peut s'écrire $(x - \sqrt{d}y)(x + \sqrt{d}y) = 1$, ce qui nous amène naturellement à nous demander à quelle condition un élément de $\mathbb{Q}[\sqrt{d}]$ est inversible dans $\mathbb{Z}[\sqrt{d}]$ afin de garder des solutions entières.

3.1 Le corps $\mathbb{Q}[\sqrt{d}]$

Lemme 3.1.1. *L'ensemble $\mathbb{Q}[\sqrt{d}]$ (où d est un entier non carré) munit des lois $\cdot$ et $+$ est un corps commutatif.*

Démonstration. La commutativité et la distributivité sont des conséquences triviales du fait que $\mathbb{Q}[\sqrt{d}]$ est un sous-ensemble de $\mathbb{R}$. De plus 1 et 0 sont dans $\mathbb{Q}[\sqrt{d}]$, donc celui-ci possède bien une unité et l'élément nul.
$\forall (x, y) \in \mathbb{Q}[\sqrt{d}]$, en notant $x = x_1 + \sqrt{d}x_2$ et $y = y_1 + \sqrt{d}y_2$, on a :

- $x + y = (x_1 + y_1) + \sqrt{d}(x_2 + y_2) \in \mathbb{Q}[\sqrt{d}]$
- $xy = (x_1y_1 + dx_2y_2) + \sqrt{d}(x_1y_2 + x_2y_1) \in \mathbb{Q}[\sqrt{d}]$
- Pour $x \neq 0$, c'est-à-dire[9] $(x_1, x_2) \neq 0)$,

$$\frac{1}{x} = \frac{x_1 - \sqrt{d}x_2}{x_1^2 - dx_2^2}$$

$$= \frac{x_1}{x_1^2 - dx_2^2} - \sqrt{d}\frac{x_2}{x_1^2 - dx_2^2} \in \mathbb{Q}[\sqrt{d}]$$

Ainsi x est inversible dans $\mathbb{Q}[\sqrt{d}]$ et $x^{-1} = \frac{x_1}{x_1^2 - dx_2^2} - \sqrt{d}\frac{x_2}{x_1^2 - dx_2^2}$

□

Définition 3.1.2. *(i) Soit $x = x_1 + \sqrt{d}y_1 \in \mathbb{Q}[\sqrt{d}]$. On appelle conjugué de x et on note $\overline{x} = x_1 - \sqrt{d}y_1$.*
(ii) On appelle norme de x et on note $N(x)$, le nombre rationnel $N(x) = x\overline{x}$.

Remarque. *Nous laissons au lecteur le soin de vérifier que $N(x)$ est bien un élément de $\mathbb{Q}$.*

Lemme 3.1.3. *L'application σ définie par $\sigma(x) = \overline{x}$ est un automorphisme involutif de $\mathbb{Q}[\sqrt{d}]$.*

Démonstration. – Il est évident que σ est involutive, c'est à dire que l'on a : $\sigma \circ \sigma = id_{\mathbb{Q}[\sqrt{d}]}$ et que $\sigma(1) = 1$.

Par suite σ est bijective et $\sigma^{-1} = \sigma$

[9] Voir 4.1.5 pour une preuve.

– Une autre chose évidente est que étant donnée la définition de l'addition dans $\mathbb{Q}[\sqrt{d}]$, $x + x' = (x_1 + x'_1) + \sqrt{d}(y_1 + y'_1)$, d'où $\forall (x, y) \in \mathbb{Q}[\sqrt{d}]^2, \sigma(x + y) = \sigma(x) + \sigma(y)$

De plus $\forall (x, x') \in \mathbb{Q}[\sqrt{d}]^2, xx' = x_1x'_1 + dx_2x'_2 + \sqrt{d}(x_1x'_2 + x_2x'_1)$
D'où :

$$\begin{aligned} \sigma(xx') &= x_1x'_1 + dx_2x'_2 - \sqrt{d}(x_1x'_2 + x_2x'_1) \\ &= (x_1 - \sqrt{d}x_2).(x'_1 - \sqrt{d}x'_2) \\ &= \sigma(x).\sigma(x') \end{aligned}$$

□

Corollaire 3.1.4. *Soit $x, y \in \mathbb{Q}[\sqrt{d}]$*
(i) $N(xy) = N(x)N(y)$
(i) Pour x non nul, $N(x^{-1}) = N(x)^{-1}$.

Démonstration. (i) $N(xy) = xy\overline{xy} = x\bar{x}y\bar{y} = N(x)N(y)$.
(ii) Soit x non nul. $N(xx^{-1}) = 1 = N(x)N(x^{-1})$. Donc $N(x^{-1}) = N(x)^{-1}$

□

Corollaire 3.1.5. *Soit $x \in \mathbb{Q}[\sqrt{d}]$. $\forall k \in \mathbb{Z}, \overline{x^k} = (\bar{x})^k$ et $N(x^k) = N(x)^k$.*

Démonstration. Ce resultat découle d'une récurrence immédiate sur le morphisme multiplicatif que réalise σ. □

Proposition 3.1.6. *Les éléments inversibles de $\mathbb{Z}[\sqrt{d}]$ sont exactement les éléments de norme ± 1.*

Démonstration. Soit $x \in \mathbb{Z}[\sqrt{d}]$. Si $N(x) = \pm 1$, alors $x\bar{x} = \pm 1$ et $x^{-1} = \pm\bar{x}$
Si x est inversible, on a alors d'une part

$$N(xx^{-1}) = N(1) = 1$$

D'autre part,

$$N(xx^{-1}) = N(x)N(x^{-1}) = N(x)N(x)^{-1}$$

$N(x)$ est alors un élément inversible de $\mathbb{Z}$ donc $N(x) = \pm 1$ □

Définition 3.1.7. *Soit $z = x + \sqrt{d}y$ un élément de $\mathbb{Q}[\sqrt{d}]$.*
On appelle partie rationnelle (resp. partie irrationelle) du nombre z et on note $R(z)$ (resp. $I(z)$) le nombre rationnel x (resp. y).

Lemme 3.1.8. *Soit $z \in \mathbb{Q}[\sqrt{d}]$.On a les formules suivantes :*

$$\begin{cases} R(z) = \dfrac{1}{2}(z + \bar{z}) \\ I(z) = \dfrac{1}{2\sqrt{d}}(z - \bar{z}) \end{cases}.$$

Démonstration. Notons $z = x + \sqrt{d}y$.

- $z + \overline{z} = x + x + \sqrt{d}y - \sqrt{d}y = 2x = 2R(z)$.
- $z - \overline{z} = \sqrt{d}y + \sqrt{d}y + x - x = 2\sqrt{d}y = 2\sqrt{d}I(z)$.

□

3.2 Résolution de l'équation de *Pell-Fermat*

Maintenant que nous avons établis les propriétés nous intéressant de l'anneau $\mathbb{Q}[\sqrt{d}]$, nous allons pouvoir nous pencher sur notre problème initial, l'équation de *Pell-Fermat* . On définit alors les suites $(u_n)_{\mathbb{N}}$ et $(v_n)_{\mathbb{N}}$ par :

$$u_n + \sqrt{d}v_n = \left(u_1 + \sqrt{d}v_1\right)^n$$

D'après ce qui précède, le couple (u_n, v_n) est solution de (P) si et seulement si $N(u_n + \sqrt{d}v_n) = 1$, ce qui est bien le cas étant donné que $N(x_1 + \sqrt{d}y_1) = 1$.
Il faut alors montrer que toute solution de (P) est caractérisée par un terme de la suite $(u_n + \sqrt{d}v_n)_{\mathbb{N}}$, ce que nous allons faire en "algébrisant" les arguments géométriques des parties précédentes, c'est-à-dire faire correspondre la conique C d'équation $x^2 - dy^2 = 1$ avec le corps $\mathbb{Q}[\sqrt{d}]$. On sait que, l'application φ qui à un point $M = (x, y)$ de C lui associe $M_1 * M$ est bijective et que les coordonnées de $\varphi(M)$ dans le repère $(O, \vec{i}, \vec{j})$ sont données par

$$\begin{cases} x' = xx_1 + dyy_1 \\ y' = xy_1 + yx_1 \end{cases}.$$

Remarquons alors que le produit $z_1 z = \left(x_1 + \sqrt{d}y_1\right)\left(x + \sqrt{d}y\right)$ nous donne

$$\begin{cases} x' = R(z_1 z) \\ y' = I(z_1 z) \end{cases}.$$

La définition suivante est alors motivée.

Définition 3.2.1. *On appelle affixe d'un point $M = (x, y)$ de $\mathbb{Q}^2$, l'élément $z = x + \sqrt{d}y$ de $\mathbb{Q}[\sqrt{d}]$.*

Proposition 3.2.2. *Soit $M \in C$ un point d'affixe $z \in \mathbb{Q}[\sqrt{d}]$. Alors l'affixe de M^{-1} est $\overline{z}$.*

Démonstration. M^{-1} est par définition le point d'intersection de la tangente à C en M_0 passant par M et de C.
Or cette tangente est verticale, c'est-à-dire que les points M et M^{-1} ont la même ordonnée. Par symétrie de C, on conclut que les point M et M^{-1} ont leur ordonnée de signe opposé. D'où $z_{M^{-1}} = \overline{z_M}$. □

Lemme 3.2.3. *Notons M_{-1} l'inverse du point de coordonnées (x_1, y_1) pour la loi $*$.Soit $M = (x, y) \in C_{\mathbb{Z}}$ tel que $x, y > 0$. Notons $M' = (x', y')$ le point $M_{-1} * M$. On a alors*

$$\begin{cases} 0 \leqslant x' < x \\ 0 \leqslant y' < y \end{cases}.$$

Démonstration. L'affixe de $M_{-1} * M$ est $z' = (x_1 - \sqrt{d}y_1)(x + \sqrt{d}y) = \overline{z_1}z$.
D'où

$$x' = R(z\bar{z}) = \frac{1}{2}\left[\left(x_1 - \sqrt{d}y_1\right)\left(x + \sqrt{d}y\right) + \left(x_1 + \sqrt{d}y_1\right)\left(x - \sqrt{d}y\right)\right]$$

On a x et y positifs donc $x + \sqrt{d}y > 0$. De l'égalité $x^2 - dy^2 = 1 > 0$, on en déduit $x - \sqrt{d}y > 0$.
De même pour $x_1 \pm \sqrt{d}y_1$.
Donc $x' \geqslant 0$.
Le point $M_1 * M' = M$ est d'ordonnée supérieure à celle de M' (cf. 2.3.6), de plus, par croissance de la fonction $y \mapsto \sqrt{1 + dy^2}$, il vient les deux inégalités

$$x' < x \text{ et } y' < y.$$

Reste à montrer que $y' \geqslant 0$.
On a :

$$y' = I(z\bar{z}) = \frac{1}{2\sqrt{d}}\left[\left(x_1 - \sqrt{d}y_1\right)\left(x + \sqrt{d}y\right) - \left(x_1 + \sqrt{d}y_1\right)\left(x - \sqrt{d}y\right)\right]$$

Montrons que $\left(x_1 - \sqrt{d}y_1\right)\left(x + \sqrt{d}y\right) \geqslant \left(x_1 + \sqrt{d}y_1\right)\left(x - \sqrt{d}y\right)$.
En effet, on a bien que

$$\frac{x + \sqrt{d}y}{x - \sqrt{d}y} \geqslant \frac{x_1 + \sqrt{d}y_1}{x_1 - \sqrt{d}y_1}$$

$$\Leftarrow \quad \underbrace{\frac{\left(x + \sqrt{d}y\right)^2}{N(x + \sqrt{d}y)}}_{=1} \geqslant \underbrace{\frac{\left(x_1 + \sqrt{d}y_1\right)^2}{N(x_1 + \sqrt{d}y_1)}}_{=1}$$

Ce qui est bien le cas car (x_1, y_1) est la solution minimale, donc $y \geqslant y_1$, ce qui implique aussi que $x = \sqrt{1 + dy^2} \geqslant \sqrt{1 + dy_1^2} = x_1$. On a donc bien les inégalités souhaitées.

□

Ce lemme nous sert en fait à pouvoir définir une suite de points de $C_{\mathbb{Z}}$ (pris dans le premier quadrant).
Fixons un point M de coordonnées positives (x, y) dans $C_{\mathbb{Z}}$. On définit la suite $(N_n)_{\mathbb{N}}$ par :

- $N_0 = M$.

- Pour $n \in \mathbb{N}$ tel que $N_0, \ldots, N_n$ soient bien définis, si$x_{N_n}, y_{N_n} > 0$, on pose $N_{n+1} = M_{-1} * N_n$, sinon c'est que $y_{N_n} = 0$ et dans ce cas la suite est finie.

Justifions que cette suite s'arrête forcément.
C'est en fait un argument de descente de *Fermat* qui nous permet d'affirmer qui ce suite s'arrête à un certain rang n. En effet, d'après le lemme précédent, on a l'encadrement suivant :

$$0 \leqslant y_{N_{n+1}} \leqslant y_{N_n}$$

ce qui nous fournit deux résultats :

– Premièrement, la suite $(y_{N_n})_{\mathbb{N}}$ est strictement décroissante.
– Deuxièmement, cette suite est minorée par 0.

Donc la suite $(y_{N_n})_{\mathbb{N}}$ converge, et même mieux dans notre cas on peut dire qu'elle devient "stationnaire" à partir du rang n tel que $N_n = M_0$.

En conclusion, il existe forcément un certain n entier tel que $(M_{-1})^{*n} * M = M_0$, c'est-à-dire que $M = M_1^{*n}$.
Or l'affixe du point M_1^{*n} est donnée par $z_1^n = \left(x_1 + \sqrt{d}y_1\right)^n$, donc toutes les solutions sont caractérisées par une puissance n-ième de la solution minimale.

4 Recherche de la soultion minimale

4.1 Le développement en fraction continue

Soit ζ un nombre réél, nous allons expliciter de manière simple l'algorithme qui permet de trouver le développement en fraction continue de ζ.
Si ζ est entier on s'arrête, sinon on écrit ζ sous la forme :
$\zeta = \underbrace{\lfloor\zeta\rfloor}_{a_0} + \underbrace{(\zeta - \lfloor\zeta\rfloor)}_{\epsilon_1}$

On a ainsi $\epsilon_1 < 1$ et donc $\exists\zeta_1 > 1$ tel que $\epsilon_1 = \dfrac{1}{\zeta_1}$

Ainsi $\zeta = a_0 + \dfrac{1}{\zeta_1}$
Et on recommence le procédé avec ζ_1.

Remarque. *Le développement en fraction continue de ζ peut être fini ou infini.*

On a alors, avec une notation un peu abusive si le développement en fraction continue de ζ est infini :

$$\zeta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \cfrac{1}{a_n}}}$$

- Si le développement en fraction continue de ζ est fini, nous noterons $\zeta = [a_0, a_1, \cdots, a_n]$
- Si il est k-péridique à partir du rang p nous noterons :
  $\zeta = [a_0, a_1, \cdots, \overline{a_p, \cdots, a_{p+k-1}}]$

Exemple : développement en fraction continue de $\sqrt{3}$:
Posons $\zeta = \sqrt{3}$
On a donc $\lfloor\zeta\rfloor = a_0 = 1$ et $\epsilon_0 = \zeta - \lfloor\zeta\rfloor = \sqrt{3} - 1$

$\zeta_1 = \dfrac{1}{\epsilon_0} = \dfrac{\sqrt{3}+1}{2}$

Donc $\sqrt{3} = 1 + \cfrac{1}{\cfrac{\sqrt{3}+1}{2}}$ On recommence avec $\zeta_1 = \dfrac{\sqrt{3}+1}{2}$

$a_1 = \lfloor\zeta_1\rfloor = 1$

$$\begin{aligned}\epsilon_1 &= \zeta_1 - \lfloor\zeta_1\rfloor \\ &= \frac{\sqrt{3}+1}{2} - 1 \\ &= \frac{\sqrt{3}-1}{2}\end{aligned}$$

$$\zeta_2 = \frac{1}{\epsilon_1} = \sqrt{3} + 1 = 1 + \zeta$$
Donc $\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \sqrt{3}}}$
Le développement en fraction continue de $\sqrt{3}$ est donc périodique : $\sqrt{3} = [1, \overline{1, 2}]$

Définition 4.1.1. *On appelle réduite de rang n du nombre $\zeta \in \mathbb{R}$ le rationnel $\frac{p_n}{q_n} = [a_0, \cdots, a_n]$*

Par exemple la réduite de rang 2 de $\sqrt{3}$ est :

$$\frac{p_2}{q_2} = 1 + \cfrac{1}{1 + \cfrac{1}{2}} = \frac{5}{3}$$

Pour une étude plus précise du développement en fraction continue , nous renvoyons le lecteur vers les documents de *Marc Hindry*[10], ou de *Antoine Chambert-Loir*[11] .

4.1.2 Développement des entiers quadratiques

Nous nous intéressons ici au développement des nombres quadratiques (voir définition ci-dessous) et aux propriétés qu'il peut avoir.

Définition 4.1.3. *Soit $x \in \mathbb{R}$. On dit que x est un entier quadratique si il existe un polynôme P de degré 2, non nul et à coefficients entiers, tel que $P(x) = 0$.*

Lemme 4.1.4. *Tout nombre quadratique x s'écrit sous la forme $a + b\sqrt{d}$, où a et b sont des nombres rationnels et d est un entier.*

Démonstration. Soit $P(X) = a_0 + a_1X + a_2X^2 \in \mathbb{Z}[X]$ tel que $P(x) = 0$
Le discriminant de P est $\Delta = a_1^2 - 4a_0a_2 \in \mathbb{Z}$ (a priori). Δ est nécessairement positif car x est réel et racine de P donc $\Delta \in \mathbb{N}$. D'où $x = \frac{-a_1 \pm \sqrt{\Delta}}{2a_2}$
CQFD □

Ce qui nous intéresse ici, c'est le développement en fraction continue de $\sqrt{d}$, nous verrons plus loin que celui-ci est périodique à partir d'un certain rang, mais pour l'instant nous avons besoin de plusieurs résultats.

[10] www.math.jussieu.fr/ hindry/Cours-arith.pdf
[11] http ://perso.univ-rennes1.fr/antoine.chambert-loir/2005-06/h4/

Lemme 4.1.5. *Soit p_0, q_0 deux entiers.*

$$|p_0^2 - dq_0^2| = 0 \Rightarrow p_0 = q_0 = 0$$

Démonstration. Nous allons étudier l'équation $(*)$ $x^2 - d = 0$ et montrer qu'elle n'a pas de solution dans $\mathbb{Q}$.
En se rappelant que d n'est pas un carré, on voit que $(*)$ n'a pas de solution dans $\mathbb{Z}$ car sinon d serait un carré.
Par l'absurde supposons que $(*)$ admet des solutions rationnelles.
Soit $\frac{p}{q}$ une de ces solutions, écrite sous forme irréductible.
On a alors $\frac{p^2}{q^2} = d$ et donc $q^2|p^2$ mais $p^2 = dq^2$ et $q|dq^2$.
On a donc $q|p^2$. Par hypothèse $p \wedge q = 1$ donc d'après le lemme de Gauss, $q|p$ donc $q = 1$ et $(*)$ admet une solution entière. Absurde.
Il n'existe donc aucune solution rationnelle non triviale de $|p_0^2 - dq_0^2| = 0$, a fortiori il n'en existe aucune entière différente de $(0, 0)$. □

On définit alors la suite $(x_n)_{\mathbb{N}}$ par :

$$\begin{cases} x_0 &= \sqrt{d} \\ x_{n+1} &= \dfrac{1}{x_n - \lfloor x_n \rfloor} \end{cases}$$

Prouvons que cette suite est bien définie.

Lemme 4.1.6. $\forall n \in \mathbb{N}, x_n \in \mathbb{R}\backslash\mathbb{Q}$

Démonstration. Par récurrence sur $n \in \mathbb{N}$.
Au rang 0, $x_0 = \sqrt{d} \notin \mathbb{Q}$ (car d est non carré).
Supposons alors que x_n soit irrationnel.
On a alors

$$x_{n+1} = \frac{1}{x_n - \lfloor x_n \rfloor}$$

Si x_{n+1} était rationnel, alors on aurait nécessairement $x_n - \lfloor x_n \rfloor \in \mathbb{Q}$, ce qui est absurde. □

La suite $(x_n)_{\mathbb{N}}$ existe donc bien.

Proposition 4.1.7. *Pour tout $n \in \mathbb{N}$, il existe des entiers $\alpha_n, \beta_n, \gamma_n$ et δ_n vérifiant $\alpha_n\delta_n - \beta_n\gamma_n = (-1)^n$ tels que :*

$$x_n = \frac{\alpha_n \sqrt{d} + \beta_n}{\gamma_n \sqrt{d} + \delta_n}$$

Nous noterons aussi[12] *:* $x_n = \begin{pmatrix} \alpha_n & \beta_n \\ \gamma_n & \delta_n \end{pmatrix} \cdot \sqrt{d}$

Démonstration. Par récurrence sur n.
Au rang 0 on a : $x_0 = Id \cdot x_0$ et $\det Id = 1$
Supposons que la formule soit vraie au rang n.
On a alors :

$$\begin{aligned} x_{n+1} &= \frac{1}{x_n - \underbrace{\lfloor x_n \rfloor}_{k_n}} \\ &= \frac{1}{\begin{pmatrix} \alpha_n & \beta_n \\ \gamma_n & \delta_n \end{pmatrix} \cdot x_n - k_n} \\ &= \begin{pmatrix} \gamma_n & \delta_n \\ \alpha_n - k_n\gamma_n & \beta_n - k_n\delta_n \end{pmatrix} \cdot x_n \end{aligned}$$

Posons alors : $\begin{pmatrix} \gamma_n & \delta_n \\ \alpha_n - k_n\gamma_n & \beta_n - k_n\delta_n \end{pmatrix} = \begin{pmatrix} \alpha_{n+1} & \beta_{n+1} \\ \gamma_{n+1} & \delta_{n+1} \end{pmatrix}$
On a de plus :

$$\begin{aligned} \alpha_{n+1}\gamma_{n+1} - \beta_{n+1}\delta_{n+1} &= \gamma_n\beta_n - k_n\gamma_n\delta_n - \alpha_n\delta_n + k_n\gamma_n\delta_n \\ &= -(\alpha_n\gamma_n - \beta_n\delta_n) \\ &= (-1)^{n+1} \end{aligned}$$

La propostion est ainsi démontrée. □

Remarque. *Notons au passage les formules de récurrence suivantes qui nous seront utiles plus tard :*

$$\begin{cases} \alpha_{n+1} &= \gamma_n \\ \beta_{n+1} &= \delta_n \\ \gamma_{n+1} &= \alpha_n - k_n\gamma_n \\ \delta_{n+1} &= \beta_n - k_n\delta_n \end{cases}$$

Nous obtenons donc la matrice de l'homographie

$$\begin{pmatrix} \alpha_n & \beta_n \\ \alpha_{n+1} & \beta_{n+1} \end{pmatrix}$$

Proposition 4.1.8. *Pour tout n entier, il existe des coefficients entiers A_n, B_n et C_n tels que*

$$A_n x_n^2 + B_n x_n + C_n = 0$$

[12] Voir annexe page 38.

De plus, les entiers A_n, B_n et C_n vérifient

$$|B_n^2 - 4A_nC_n| = 4d$$

Démonstration. On a l'égalité

$$x_n = \begin{pmatrix} \alpha_n & \beta_n \\ \gamma_n & \delta_n \end{pmatrix} \cdot x_0$$

On en déduit alors

$$x_0 = (-1)^n \begin{pmatrix} \delta_n & -\beta_n \\ -\gamma_n & \delta_n \end{pmatrix} \cdot x_n$$

Or $x_0^2 = d$, d'où

$$d = \frac{\delta_n^2 - 2\beta_n\gamma_n x_n + \beta_n^2}{\gamma_n^2 x_n^2 - 2\alpha_n\gamma_n x_n + \alpha_n^2}$$

x_n est alors racine du polynôme de $\mathbb{Z}[X]$

$$\underbrace{\left(\delta_n^2 - d\gamma_n^2\right)}_{A_n} X^2 - 2\underbrace{\left(\beta_n\delta_n - d\alpha_n\gamma_n\right)}_{B_n/2} X + \underbrace{\beta_n^2 - d\alpha_n^2}_{C_n}$$

De plus, le discriminant réduit de ce polynôme est

$$\begin{aligned} B_n^2 - A_nC_n &= \left[-2\alpha_n\beta_n\gamma_n\delta_n + \beta_n^2\gamma_n^2 + \alpha_n^2\delta_n^2\right] \\ &= (\alpha_n\delta_n - \beta_n\gamma_n)^2 d \\ &= d \end{aligned}$$

Cela montre bien que le discriminant (en particulier sa valeur absolue) est égale à $4d$. □

Lemme 4.1.9. *Soient A_n, B_n et C_n les nombres définis plus tôt. Pour tout n de $\mathbb{N}$ on a :*

$$A_nC_n < 0$$

Démonstration. L'application σ qui envoie x sur son conjugué (cf 3.1.2) fournit une seconde racine du $A_nX^2 + B_nX + C_n$, en effet on sait que x_n est une racine. On a alors

$$\begin{aligned} & \sigma(A_nx_n^2 + B_nx_n + C_n) = \sigma(0) \\ \Leftrightarrow\ & \sigma(A_n)\sigma(x_n^2) + \sigma(B_n)\sigma(x_n) + \sigma(C_n) = 0 \\ \Leftrightarrow\ & A_n\sigma(x_n)^2 + B_n\sigma(x_n) + C_n = 0 \end{aligned}$$

A_nC_n est alors du même signe que $x_n\sigma(x_n) = N(x_n)$. Reste alors à montrer que x_n et $\sigma(x_n)$ sont de signes contraires, plus précisément que $\sigma(x_n) < 0$ ce que l'on va faire par récurrence sur n.
Au rang 0 , $\sigma(x_0) = -\sqrt{d} < 0$.
Supposons alors que $\sigma(x_n) < 0$. Alors

$$\sigma(x_{n+1}) = \frac{1}{\sigma(x_n) - \lfloor x_n \rfloor} < 0$$

A_n et C_n sont donc des signes contraires. □

Corollaire 4.1.10. *Les suites $(A_n)_{\mathbb{N}}$, $(B_n)_{\mathbb{N}}$ et $(C_n)_{\mathbb{N}}$ sont bornées.*

Démonstration. Comme A_n et C_n sont de signe contraires, on a alors pour tout n entier

$$\left|B_n^2 - 4A_nC_n\right| = B_n^2 - 4A_nC_n + 4d$$

D'où la majoration suivante :

$$|B_n| \leqslant 2\sqrt{d}$$

De plus, en considérant le fait que C_n ne peut être nul,

$$A_n = \frac{4d - B_n^2}{Cn}$$

Et donc :

$$|A_n| \leqslant |4d|$$

Un raisonnement analogue pour C_n conduit aussi au résultat voulu.

□

Proposition 4.1.11. *Il existe deux entiers distincts n_0 et n_1 tels que $x_{n_0} = x_{n_1}$.*

Démonstration. On a vu que $(A_n, B_n, C_n) \in [\![-4d, 4d]\!] \times [\![-\lfloor 2\sqrt{d} \rfloor, \lfloor 2\sqrt{d} \rfloor]\!] \times [\![-4d, 4d]\!]$. On peut donc trouver deux entiers n_0 et n_1 tels que $(A_{n_0}, B_{n_0}, C_{n_0}) = (A_{n_1}, B_{n_1}, C_{n_1})$. Mais alors x_{n_0} est la racine positive du polynôme

$$A_{n_0}X^2 + B_{n_0}X + C_{n_0}$$

De même, x_{n_1} est racine de

$$A_{n_1}X^2 + B_{n_1}X + C_{n_1}$$

Or, ces deux polynômes sont égaux et ont donc les même racines, de plus $x_{n_1}, x_{n_0} > 0$. Donc $x_{n_0} = x_{n_1}$.

□

Proposition 4.1.12. *Il existe un quadruplet $(\alpha, \beta, \gamma, \delta) \in \mathbb{Z}^4$ différent de $\pm(1,0,0,1)$ tel que*

$$\sqrt{d} = \frac{\alpha\sqrt{d} + \beta}{\gamma\sqrt{d} + \delta}$$

Remarque. *On voit en fait que $\sqrt{d}$ est un point fixe d'une homographie non triviale.*

$$\sqrt{d} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot \sqrt{d}$$

Démonstration. L'existence d'un tel quadruplet découle des points 4.1.7 et 4.1.11, en effet : notons M_n la matrice $\begin{pmatrix} \alpha_n & \beta_n \\ \gamma_n & \delta_n \end{pmatrix}$. Il existe $n_0 \neq 0$ tel que

$$M_{n_0} \cdot x_0 = x_{n_0} = x_{n_1} = M_{n_1} \cdot x_0$$

On a donc

$$x_0 = M_{n_0}^{-1} M_{n_1} \cdot x_0$$

Notons alors P_n la matrice $\begin{pmatrix} 0 & 1 \\ 1 & -\lfloor x_n \rfloor \end{pmatrix}$. On voit que son déterminant est (-1), P_n est donc inversible et

$$P_n^{-1} = \begin{pmatrix} \lfloor x_n \rfloor & 1 \\ 1 & 0 \end{pmatrix}$$

Or $M_{n+1} = P_n M_n$ d'où

$$M_{n+1}^{-1} = M_n^{-1} P_n^{-1}$$

Mais on a

$$M_n^{-1} = (-1)^n \begin{pmatrix} \delta_n & -\beta_n \\ -\gamma_n & \alpha_n \end{pmatrix}$$

On définit alors les suites $(\tilde{\alpha}_n)_{\mathbb{N}}$, $\left(\tilde{\beta}_n\right)_{\mathbb{N}}$, $(\tilde{\gamma}_n)_{\mathbb{N}}$ et $\left(\tilde{\delta}_n\right)_{\mathbb{N}}$ par

$$\begin{pmatrix} \tilde{\delta}_n & \tilde{\beta}_n \\ \tilde{\gamma}_n & \tilde{\alpha}_n \end{pmatrix} = M_n^{-1}$$

Il vient les formules de récurrences suivantes :

$$\begin{cases} \tilde{\delta}_{n+1} &= \lfloor x_n \rfloor \tilde{\delta}_n + \tilde{\beta}_n \\ \tilde{\beta}_{n+1} &= \tilde{\delta}_n \\ \tilde{\gamma}_{n+1} &= \lfloor x_n \rfloor \tilde{\gamma}_n + \tilde{\alpha}_n \\ \tilde{\alpha}_{n+1} &= \tilde{\gamma}_n \end{cases}$$

Deux autres formules de degré deux nous intéressant en découlent :

$$\begin{cases} \tilde{\delta}_{n+2} = \lfloor x_n \rfloor \tilde{\delta}_{n+1} + \tilde{\delta}_n \\ \\ \tilde{\gamma}_{n+2} = \lfloor x_n \rfloor \tilde{\gamma}_{n+1} + \tilde{\gamma}_n \end{cases}$$

On a de plus $\tilde{\delta}_0 = 1$ et $\tilde{\gamma}_0 = 0$, il est donc évident que les suites $(\tilde{\delta}_n)_{\mathbb{N}}$ et $(\tilde{\gamma}_n)_{\mathbb{N}}$ sont positives et strictement croissantes à partir du rang 1.
Mais on sait qu'il existe deux entiers distincts n_0 et n_1 (on supposera $n_0 < n_1$) tels que

$$\begin{cases} x_{n_0} = M_{n_0} \cdot x_0 = h_{M_{n_0}}(x_0) \\ \\ x_{n_1} = M_{n_1} \cdot x_0 = h_{M_{n_1}}(x_0) \end{cases}$$

Il vient alors :

$$h^{-1}_{M_{n_1}} \left(h_{M_{n_0}}(x_0) \right) = x_0$$

$$\Leftrightarrow \qquad h_{M^{-1}_{n_1} M_{n_0}}(x_0) = x_0$$

Deux cas se présentent alors :
- soit la matrice $M^{-1}_{n_1} M_{n_0}$ est dans $Id\mathbb{R}^*$,
- soit cette matrice n'est pas triviale (au sens des homographies) et x_0 est un point fixe (ce que l'on souhaite).

Considérons le premier cas et montrons qu'il est absurde.
Soit donc $a \in \mathbb{Z}$ tel que $aM_{n_1} = M_{n_0}$. On a alors, par un calcul de déterminant, que $a = \pm 1$.
On a alors $M_{n_1} = \pm M_{n_0}$, mais nous avons vu plus haut que les coefficients des matrices (pris en valeur absolue) M_{n_0} et M_{n_1} sont des termes de suites strictement croissantes. Ainsi on doit avoir $|\alpha_{n_0}| = |\pm \alpha_{n_1}| < |\pm \alpha_{n_1}|$ (de même pour les autres termes) ce qui est absurde.
Le nombre x_0 est donc un point fixe d'une homographie non triviale, et la proposition est ainsi démontrée.

□

Lemme 4.1.13. *Les nombres α, β, γ et δ définis plus tôt vérifient*

$$\begin{cases} \delta = \alpha \\ \beta = \gamma d \end{cases}$$

Démonstration. De l'égalité $\sqrt{d} = \dfrac{\alpha\sqrt{d} + \beta}{\gamma\sqrt{d} + \delta}$, on déduit :

$$d\gamma + \delta\sqrt{d} = \alpha\sqrt{d} + \beta \quad \in \mathbb{Z}[\sqrt{d}]$$

Or $\sqrt{d} \notin \mathbb{Q}$ d'où, en identifiant terme à terme dans $\mathbb{Z}[\sqrt{d}]$:

$$\begin{cases} \delta = \alpha \\ \beta = \gamma d \end{cases}$$

□

Corollaire 4.1.14. *On a l'égalité suivante :*

$$\alpha^2 - d\gamma^2 = \pm 1$$

Démonstration. On a :

$$\begin{aligned} \det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} &= \det \begin{pmatrix} \alpha & \gamma d \\ \gamma & \alpha \end{pmatrix} \\ &= \det M_{n_1}^{-1} M_{n_0} \\ &= \frac{\det M_{n_0}}{\det M_{n_1}} \\ &= \pm 1 \end{aligned}$$

□

Remarque. *Tous les résultats définis dans cette partie peuvent être adaptés afin d'être vrais pour tout nombre irrationnel quadratique grâce au lemme 4.1.4.*

Proposition 4.1.15. *La suite* $\left(\left|\frac{\alpha_n}{\gamma_n}\right|\right)_{\mathbb{N}}$ *est la suite des réduites de* $\sqrt{d}$.

Démonstration. Nous redirigeons le lecteur à la page de *Antoine Chambert-Loir*, plus précisément à la page 2 de l'article *Compléments de théorie algébrique des nombres*. Le résultat, numéroté (5), correspond bien à l'assertion que nous voulons prouver. □

Récapitulons. Le développement en fraction continue de $\sqrt{d}$ est donné par

$$\sqrt{d} = [\lfloor x_0 \rfloor, \lfloor x_1 \rfloor, \cdots, \lfloor x_n \rfloor, \cdots].$$

On a vu que celui-ci était périodique à partir d'un certain rang, et que la suite des ses réduites donnait des solutions de l'équation de *Pell-Fermat*, plus précisément, on trouve ces solutions au rang auquel la suite $(x_n)_{\mathbb{N}}$ boucle.

5 Annexes

5.1 Graphiques : La loi $*$ et le théorème de *Pascal*

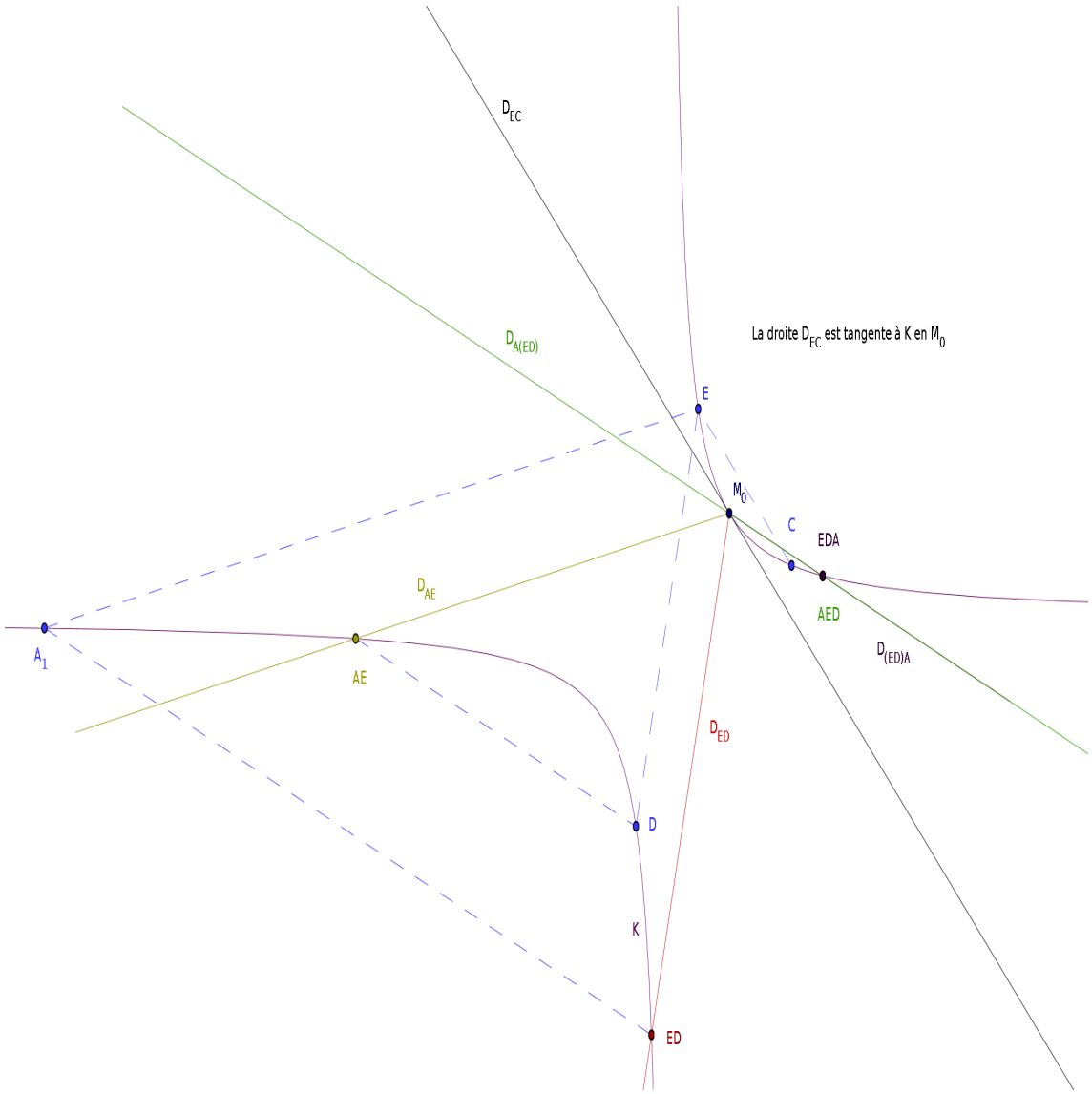


FIG. 4 – La loi $*$

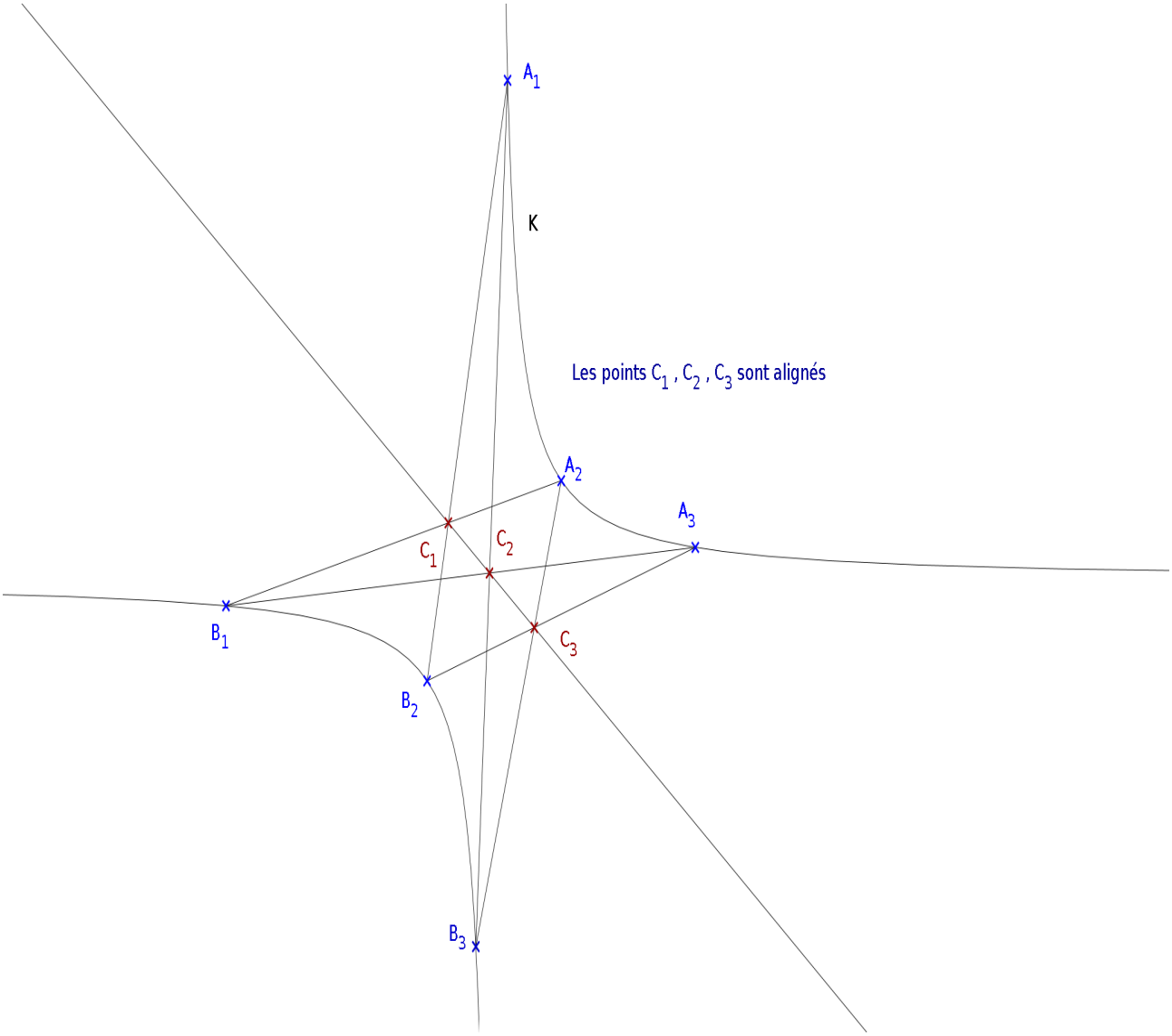


FIG. 5 – Le théorème de Pascal

5.2 Preuve de l'associativité de la loi $*$ grâce au théorème de *Pascal*

Nous nous plaçons dans un plan projectif, afin de pouvoir dire que des points sont alignés sur la droite de l'infini.

Théorème 5.2.0.1. *[Théorème de* Pascal*] Soit A_1, A_2, A_3 et B_1, B_2, B_3 six points, distincts deux à deux, d'une conique $\mathcal{K}$.*
On définit trois points C_1, C_2, C_3 par :

- *C_1 est l'intersection des droites (A_2B_3) et (A_3B_2).*
- *C_2 est l'intersection des droites (A_1B_3) et (A_3B_1).*

– *C_3 est l'intersection des droites (A_2B_1) et (A_1B_2).*

Alors les points C_i sont alignés.

Démontrons maintenant l'associativité de $*$.

Preuve : (Associativité de $*$). On se donne trois points, distincts deux à deux, A, B, C de l'hyperbole $\mathcal{H}$. On note M_0 le point de coordonnées $(1, 1)$. On obtient alors deux autres points de $\mathcal{H}$ qui sont : $A * B$ et $B * C$.
Pour montrer que $A * (B * C) = (A * B) * C$, il suffit de montrer que les deux droites $\Delta_{A(B*C)}$ et $\Delta_{(A*B)C}$ sont confondues, ou encore, de manière équivalente, que les droites $(A(B * C))$ et $((A * B)C)$ sont parallèles.
Prenos la configuration de *Pascal* suivante :

$$\left|\begin{array}{ll} A_1 = A & B * A = B_1 \\ A_2 = M_0 & B = B_2 \\ A_3 = C & C * B = B_3 \end{array}\right.$$

Par définition de la loi $*$, on a :
– $(M_0(C * B)) \,/\!/\, (CB)$. Donc l'intersection I de ces deux droites se situe à l'infini.
– $(M_0(A * B)) \,/\!/\, (AB)$. Donc l'intersection J de ces deux droites se situe aussi à l'infini.
D'après le théorème de *Pascal*, l 'intersection K de $(A(C * B))$ et de $(C(B * A))$, est sur la droite (IJ), elle se situe donc sur la droite de l'infini, et les deux droites $(A(C * B))$ et $(C(A * B))$ sont donc parallèles. □

5.3 Homographies

Dans toute cette partie, on supposera que les matrices utilisées ne sont pas de déterminant nul.

Définition 5.3.1. *Soit A la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.*
On appelle homographie de paramètres A, l'application :

$$\begin{array}{rccc} h_A : & \mathbb{R} \cup \{\infty\} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \dfrac{ax+b}{cx+d} \\ & \infty & \longmapsto & \dfrac{a}{c} \\ & -\dfrac{d}{c} & \longmapsto & \infty \end{array}$$

On notera H l'ensemble des homographies.

Proposition 5.3.2. *$(H, \circ)$ est un groupe.*

Démonstration. Soient h_1 et h_2 les homographies de paramètres respectifs $A_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ et $A_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$.

-Stabilité- Montrons que $h_1 \circ h_2 \in H$.
$\forall x \in \mathbb{R} \cup \{\infty\}$,

$$\begin{aligned} (h_1 \circ h_2)(x) &= \frac{a_1 \dfrac{b_1 x + b_2}{b_3 x + b_4} + a_2}{a_3 \dfrac{b_1 x + b_2}{b_3 x + b_4} + a_4} \\ &= \frac{(a_1 b_1 + a_2 b_3)x + a_1 b_2 + a_2 b_4}{(a_3 b_1 + a_4 b_3)x + a_3 b_2 + a_4 b_4} \end{aligned}$$

Donc $h_1 \circ h_2 \in H$.

-Neutre- L'application identité est dans H, c'est l'homographie de paramètres $1, 0, 0, 1$ et on a évidemment $h_1 \circ Id = Id \circ h_1 = h_1$.

-Inverse- Les homographies représentent des hyperboles qui sont sont des translatées de l'hyperbole d'équation $y = 1/x$, ce sont donc sont des bijections, en particulier elles

admettent une fonction réciproque. Reste à montrer que celle-ci est bien une homographie.

Cette application est : $h^{-1} : \mathbb{R}\backslash\{\frac{a}{c}\} \longrightarrow \mathbb{R} \in H.$

$$y \longmapsto \frac{-dy+b}{cy-a}$$

-Associativité- La loi $\circ$ est associative pour l'ensemble des applications pour lesquelles la composition est définie, elle l'est donc dans H.

□

Lemme 5.3.3. *On a un morphisme entre le groupe linéaire $GL_2(\mathbb{R})$ et H.*

$$\Psi : \quad GL_2(\mathbb{R}) \longrightarrow H$$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto h_A$$

De plus : $\ker(\Psi) = \{aI_2, a \in \mathbb{R}^*\}$.

Remarque. *On peut donc s'autoriser la notation matricielle pour décrire une homographie.*

Démonstration. Lors de la démonstration précédente , on a vu que $h_1 \circ h_2$ est l'homographie :

$$h_1 \circ h_2 : \mathbb{R} \cup \{\infty\} \longrightarrow \mathbb{R}$$

$$x \longmapsto \frac{(a_1b_1 + a_2b_3)x + a_1b_2 + a_2b_4}{(a_3b_1 + a_4b_3)x + a_3b_2 + a_4b_4}$$

D'autre part,

$$\Psi\left(\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}\right) = \Psi\left(\begin{pmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{pmatrix}\right)$$

$$= h_1 \circ h_2$$

$\ker \Psi = \{M \in GL_2(\mathbb{R}), \Psi(M) = Id\}$

Montrons que $\ker \Psi = I_2\mathbb{R}^*$ Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \ker \Psi$.

On a : $\forall x \in \mathbb{R} \cup \{\infty\}, M.x = x$

D'où :

$$M.x = x$$

$$\Leftrightarrow \quad \frac{ax+b}{cx+d} = x$$

$$\Leftrightarrow \quad cx^2 + (d-a)x - b = 0$$

Donc $c = b = 0$ et $a = d$. □

Proposition 5.3.4. *(i)* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot x + k = \begin{pmatrix} a+kc & b+kd \\ c & d \end{pmatrix} . x$

(ii) $\dfrac{1}{\begin{pmatrix} a & b \\ c & d \end{pmatrix} . x} = \begin{pmatrix} c & d \\ a & b \end{pmatrix} \cdot x$

Démonstration. (i)
$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot x + k &= \frac{ax+b}{cx+d} + k \\ &= \frac{ax+b+kcx+kd}{cx+d} \\ &= \begin{pmatrix} a+kc & b+kd \\ c & d \end{pmatrix} \cdot x \end{aligned}$$

(ii) Trivial.

□

5.4 Algorithmes

5.4.1 Solution minimale de *Pell-Fermat*

En Maple :

```
solmin :=
proc(d)
local x,y   ;
y := 1 ;
x := sqrt(1 + d*y^2)
while true
do
if x = floor(x)
then return (x ,y) ;
else x := x + 1 ;
     y := sqrt(1 + d*x^2)
fi ;
od ;
end ;
```

Remarque. *Cet algorithme est extrêmement naïf, il teste tous les nombres* 1 *par* 1 *jusqu'à trouver une solution. Il ne convient absolument pas pour certaines valeurs de d dépassant* 25 *(même si les "grandes" solutions minimales n'apparaissent que presque aléatoirement)* .

Remarque. *On voit que, mis à part quelques points, le nuage s'agglutine vers une droite linéaire, ce qui montre l'efficacité de l'algorithme.*

```
solminDFC :=
proc (d)
local dev, lg, reduites;
with(numtheory);
dev := cfrac(sqrt(d), 'periodic', 'quotients');
lg := nops(dev[2]);
dev := cfrac(sqrt(d), 'reduites');
if evalb(`mod`(lg, 2) = 0)
then return [numer(reduites[lg]), denom(reduites[lg])] ;
else return [numer(reduites[2*lg]), denom(reduites[2*lg])]
fi ;
end ;
```

Remarque. *Cet algorithme ne trouve la solution minimale que dans le cas où le second terme est égal à* 1.
Il est tout de même beaucoup plus performant que la procédure `solmin`*, ce que l'on voit bien sur les graphiques suivants. Un autre exemple est le calcul de la solution minimale pou* $d = 1512154$ *(qui n'est pas un nombre gigantesque) : la procédure* `solminDFC` *met un temps de* $63s$ *environ, alors que il est absolument impensable de calculer cette solution avec la procédure* `solmin`.

5.4.2 Calcul des solutions

```
#_____________________________________________________________________#
x2X := (x, y, d) -> (x+sqrt(d)*y, x-sqrt(d)*y ) :
# Changement de repère

#_____________________________________________________________________#
X2x := (X, Y, d) -> ((1/2)*X+(1/2)*Y, (1/2)*(X-Y)/sqrt(d)) :
# Changement de repère inverse

#_____________________________________________________________________#
with(numtheory) : # Chargement de cfrac

solminDFC := proc (d)
local dev, lg, reduites;

dev := cfrac(sqrt(d), 'periodic', 'quotients');
# dev contient la liste des coefficients entiers

lg := nops(dev[2]);
# on récupère la longueur de la liste

dev := cfrac(sqrt(d), 2*lg+1, reduites);
# reduites contient la liste des 2lg +1 premières réduites

if evalb(`mod`(lg, 2) = 0)  # Si la longueur est paire

then return numer(reduites[lg]), denom(reduites[lg])
# On renvoie la "réduite" de rang lg

else return numer(reduites[2*lg]), denom(reduites[2*lg])
# Sinon on renvoie celle de rang 2lg + 1
fi :
```

```
end :

#_____________________________________________________________________#
solSuiv := proc (xn, yn, d)
# On se donne une solution (xn , yn)

local X, Y, X1, Y1, XX1, YY1;
X, Y := x2X(xn, yn, d);
# Les coordonnées de (xn , yn) dans R'

X1, Y1 := x2X(solminDFC(d), d);
# Celles de (x1 , y1)

XX1, YY1 := X*X1, Y*Y1;
# Les coordonnées de (x1 , y1) * (xn , yn)

return
simplify(expand(X2x(XX1, YY1, d)[1])), simplify(expand(X2x(XX1, YY1, d)[2])) ;
# On renvoie le résultat simplifié du changement de repère inverse

end :

#_____________________________________________________________________#
solNieme := proc (d, n)
local i, xtemp, ytemp;
i := 0;
xtemp, ytemp := solminDFC(d);
# On initialise les valeurs

while i < n
# Tant que on n'atteint pas la valeur entrée en paramètre

do
xtemp, ytemp := solSuiv(xtemp, ytemp, d);
# On récupère la solution de rang i + 1

i := i+1 # On incrémente
od :
return xtemp, ytemp
# Renvoie de la n-ième solution
```

```
end :

#_____________________________________________________________________#
affNsol := proc (d, n)
local i, xn, yn;
i := 0;
while i <= n
# Tant que on atteint pas la valeur limite

do
print(" n = ", i, " xn , yn = ", solNieme(d, i));
# On affiche la solution de rang i

i := i+1
# On incrémente
od :
end :

#_____________________________________________________________________#
```

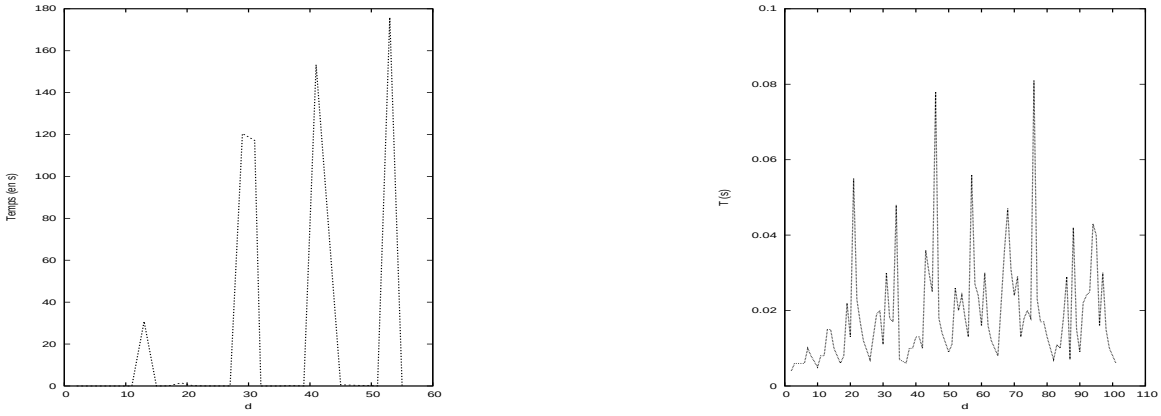


FIG. 7 – solmin (à gauche) et solminDFC (à droite)

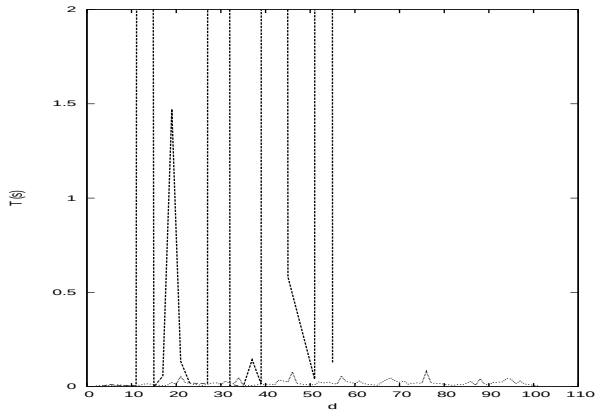


FIG. 8 – Comparaison

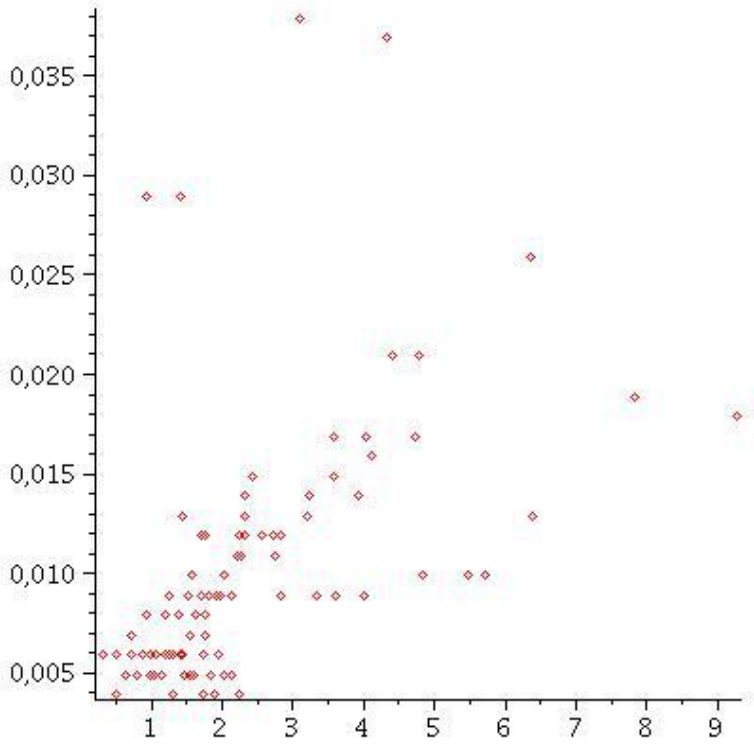


FIG. 9 – Nuage de $(log_{10}(x_1), T)$ (T : temps de calcul) pour d allant de 2 à 1000 de solminDFC