

Solution du problème sur l'équation de Pell-Fermat

Partie I: Résolution géométrique de $x^2 - 3y^2 = 1$.

1. Etude d'une application du plan

1.a. Considérons la courbe $\mathcal{H}$ d'équation $x^2 - 3y^2 = 1$. Alors (x, y) sont solutions de $\mathcal{H}$ ssi ce couple vérifie $\left(\frac{x}{a}\right)^2 - \left(\frac{y}{b}\right)^2 = 1$ avec $a = 1$ et $b = \frac{1}{\sqrt{3}}$; nous reconnaissons alors l'équation d'une hyperbole de distance focale $c = \sqrt{a^2 + b^2} = \frac{2\sqrt{3}}{3}$. Les foyers de l'hyperbole sont donnés par $F(\frac{2\sqrt{3}}{3})$ et $F'(\frac{-2\sqrt{3}}{3})$. Enfin, les directrices sont les droites d'équations $x = \mp \frac{a^2}{c}$, donc $\mathcal{D} : x = \frac{\sqrt{3}}{2}$ et $\mathcal{D}' : x = -\frac{\sqrt{3}}{2}$. L'excentricité vaut $e = \frac{c}{a} = \frac{2\sqrt{3}}{2}$. Enfin, les asymptotes sont les droites d'équation $x - \sqrt{3}y = 0$ et $x + \sqrt{3}y = 0$.

b. Soit M un point du plan $\mathcal{P}$ dont l'affixe dans le repère $\mathcal{R}$ est $z = x + iy$. Alors $F(M)$ a pour affixe z' vérifiant $z' = f(z)$, soit $z' = f(z) = (2 - i)z + 2i\bar{z} = (2 - i)(x + iy) + 2i(x - iy) = (2 + i)x + (3 + 2i)y$. Ainsi, $M' = F(M)$ est le point de coordonnées $(2x + 3y; x + 2y)$.

Méthode Pour montrer qu'une fonction est une bijection, soit on montre qu'elle est injective et surjective (en deux temps), soit on montre directement qu'elle est bijective par exemple en exhibant sa fonction réciproque. Généralement, il est bon de chercher (au moins au brouillon) via la méthode d'Analyse-Synthèse (à moins que l'énoncé ne vous donne des indications dans les questions précédentes).

Montrons à présent que F est bijective: considérons $M'(x', y') \in \mathcal{P}$ et montrons qu'il existe un unique point M vérifiant $F(M) = M'$. Pour cela, on résoud le système

$$\begin{cases} x' = 2x + 3y \\ y' = x + 2y \end{cases} \quad \text{ce qui implique} \quad \begin{cases} x = 2x' - 3y' \\ y = -x' + 2y' \end{cases}$$

Ainsi en déduisons-nous que la fonction réciproque de f est donnée par: $f^{-1}(x, y) = (2x - 3y; -x + 2y)$.

Montrons l'équivalence (i): $M \in \mathcal{H} \Leftrightarrow F(M) \in \mathcal{H}$.

Soit $M(x, y)$ un point du plan $\mathcal{P}$ et $M'(x'; y')$ son image par F . Nous avons alors:

$M \in \mathcal{H} \Leftrightarrow x^2 - 3y^2 = 1 \Leftrightarrow (2x' - 3y')^2 - 3(-x' + 2y')^2 = 1 \Leftrightarrow x'^2 - 3y'^2 = 1 \Leftrightarrow M' \in \mathcal{H}$. Nous en déduisons bien l'équivalence i.

Montrons à présent l'équivalence (ii): $M \in \mathcal{H}' \Leftrightarrow F(M) \in \mathcal{H}'$. Partons de l'équivalence précédente. Si $(x, y) \in \mathbb{Z}^2$, alors $(2x + 3y; x + 2y) \in \mathbb{Z}^2$ (et réciproquement). Ainsi en déduisons-nous que $M \in \mathcal{H}' \Leftrightarrow F(M) \in \mathcal{H}'$.

c.i. De $A_0(1; 0)$, nous utilisons la formule $f(x; y) = (2x + 3y; x + 2y)$ pour obtenir les points $A_1(2; 1)$ et $A_2(7; 4)$.

c.ii. Nous raisonnons par récurrence sur n . Au rang initial, $A_0 \in \mathcal{H}'$. Soit à présent $n \in \mathbb{N}$. Par la question 1.b, si $A_n \in \mathcal{H}'$ alors $A_{n+1} \in \mathcal{H}'$. Il résulte alors du théorème de la récurrence que $\forall n \in \mathbb{N}, A_n \in \mathcal{H}'$.

c.iii. Tout point $M(x, y)$ appartenant à l'arc $\widehat{A_0 A_1}$ de $\mathcal{H}$ vérifie $1 \leq x \leq 2$. Ainsi, puisque les points de $\mathcal{H}'$ sont à coordonnées entières, il y a deux possibilités: soit $x = 1$ et il s'agit du point A_0 soit $x = 2$ et il s'agit du point A_1 . Ainsi, les seuls éléments de $\mathcal{H}'$ situés sur l'arc $\widehat{A_0 A_1}$ de $\mathcal{H}$ sont les points A_0 et A_1 .

2. Structure de groupe sur $\mathcal{H}$.

2.a.i. Calculons $\det(\vec{e}_1; \vec{e}_2) = \begin{vmatrix} \frac{1}{2} & \frac{1}{6} \\ -\frac{\sqrt{3}}{6} & \frac{\sqrt{3}}{6} \end{vmatrix} = \frac{\sqrt{3}}{6} > 0$. Nous en déduisons alors qu'il s'agit bien d'une base du plan $\mathcal{P}$ puisque les vecteurs ne sont pas colinéaires. De plus, puisque $\det(\vec{e}_1; \vec{e}_2) > 0$, nous en déduisons que le repère est orienté dans le sens direct. Ce repère n'est pas orthonormé puisque les vecteurs ne sont ni normés, ni orthogonaux. Par contre, nous reconnaissons dans ces axes les deux asymptotes de $\mathcal{H}$.

2.a.ii. Il suffit pour cela d'inverser le système:

$$\begin{cases} \vec{e}_1 = \frac{1}{2}\vec{e}_1 - \frac{\sqrt{3}}{6}\vec{e}_2 \\ \vec{e}_2 = \frac{1}{2}\vec{e}_1 + \frac{\sqrt{3}}{6}\vec{e}_2 \end{cases} \quad \text{d'où} \quad \begin{cases} \vec{e}_1 = \vec{e}_1 + \vec{e}_2 \\ \vec{e}_2 = -\sqrt{3}\vec{e}_1 + \sqrt{3}\vec{e}_2 \end{cases}$$

Ainsi le point M de coordonnées (x, y) dans le repère a-t-il pour coordonnées $(x - \sqrt{3}y; x + \sqrt{3}y)$ dans le nouveau repère $\mathcal{R}'$. Ainsi, le point A_0 a-t-il $(1, 1)$ pour coordonnées dans $\mathcal{R}'$.

2.a.iii. Soit $M \in \mathcal{H}$ un point de coordonnées (x, y) dans $\mathcal{R}$ et de coordonnées (x', y') dans $\mathcal{R}'$. Alors $x'y' = (x - \sqrt{3}y)(x + \sqrt{3}y) = x^2 - 3y^2 = 1$ (par identité remarquable et car $M \in \mathcal{H}$). Ainsi en déduisons-nous que $M \in \mathcal{H} \Rightarrow x'y' = 1$. L'implication réciproque résulte du fait que le changement de repère est une bijection.

2.b.i. Dans le repère $\mathcal{R}'$, les coordonnées de M et N sont $M(m; \frac{1}{m})$ et $N(n; \frac{1}{n})$ (car M et N sont des points de $\mathcal{H}$). Le point $P(x', y')$ appartient à la droite (MN) si et seulement si les vecteurs $\overrightarrow{MN}$ et $\overrightarrow{MP}$ sont colinéaires, c'est-à-dire ssi $\det(\overrightarrow{MN}; \overrightarrow{MP}) = 0$.

$\det(\overrightarrow{MN}; \overrightarrow{MP}) = \begin{vmatrix} x' - m & n - m \\ y' - \frac{1}{m} & \frac{1}{n} - \frac{1}{m} \end{vmatrix} = (\frac{1}{m} - \frac{1}{n})x' + (m - n)y' + \frac{n}{m} - \frac{m}{n} = 0$. Nous en déduisons alors que (x', y') vérifient $x' + mny' = m + n$. Ainsi, l'équation cartésienne de la droite (MN) dans le repère $\mathcal{R}'$ est $x' + mny' = m + n$.

2.b.ii. La droite $\Delta(M; N)$ étant parallèle à la droite (M, N) , elles ont même coefficient directeur. Ainsi, l'équation de $\Delta(M, N)$ est de la forme $x' + mny' = k$ où k est une constante réelle. Pour la déterminer, nous utilisons le fait que $A_0 \in \Delta(M; N)$. Ainsi obtenons-nous $1 + mn = k$ et donc l'équation cartésienne de la droite $\Delta(M, N)$ (dans le cas $M \neq N$) est $x' + mny' = 1 + mn$. 2

2.b.iii. Soit (x', y') les coordonnées de $M \star N$ dans $\mathcal{R}'$. Nous savons que $M \star N \in \mathcal{H} \cap \Delta(M; N)$. Ainsi, nous avons: $M \star N \in \mathcal{H}$ donc $x'y' = 1$ et $M \star N \in \Delta(M; N)$ donc $x' + mny' = 1 + mn$. En résolvant ce système par substitution ($x' = \frac{1}{y'}$), nous obtenons: $y' = 1$ ou $y' = \frac{1}{mn}$, ce qui implique que les couples $(1; 1)$ et $(mn; \frac{1}{mn})$ sont solutions de ce système. Le premier couple correspond au point A_0 et le second correspond aux coordonnées du point $M \star N$.

2.c.i. On note $(m; \frac{1}{m})$ les coordonnées de M dans le repère $\mathcal{R}'$. Considérons la représentation paramétrique de $\mathcal{H}$ donnée par $g : \mathbb{R}^* \rightarrow \mathbb{R}^2, g : t \mapsto \begin{pmatrix} t \\ \frac{1}{t} \end{pmatrix}$. Alors la tangente à cette courbe en $M(f(m))$ est dirigée par

$\overrightarrow{g'(m)} = \begin{pmatrix} 1 \\ -\frac{1}{m^2} \end{pmatrix}$. Ainsi, si $P(x', y')$ est un point de cette tangente, alors les vecteurs $\overrightarrow{MP}$ et $\overrightarrow{g'(m)}$ sont colinéaires, donc $\det \begin{vmatrix} x' - m & 1 \\ y' - \frac{1}{m} & -\frac{1}{m^2} \end{vmatrix} = 0$ ce qui donne $x' + m^2y' = 2m$.

2.c.ii. De la même manière que précédemment, l'équation de $\Delta(M; M)$ est de la forme $x' + m^2y' = k$ où k est une constante que l'on détermine grâce à $A_0 \in \Delta(M; M)$. Ainsi $k = 1 + m^2$.

2.c.iii. Si $P(x'; y')$ est un point de $\Delta(M; M)$ alors (x', y') vérifie l'équation $\mathcal{H}$ ainsi que de celle de $\Delta(M; M)$. Il s'ensuit alors que $x'y' = 1$ et $x' + m^2y' = 1 + m^2$ ce qui implique que les coordonnées de $M \star M$ sont $(m^2; \frac{1}{m^2})$.

2.d.

Méthode Généralement, pour montrer que $(G; \times)$ est un groupe, il suffit de montrer que c'est un sous-groupe d'un groupe connu. Ici, ce n'est pas possible, car nous ne connaissons aucun groupe contenant ce type d'ensemble... Il faut alors revenir à la définition de groupe, et montrer que $\star$ est une loi de composition interne, que $\mathcal{H}$ possède un neutre pour $\star$, que $\star$ est associative et que tout élément possède un inverse dans $\mathcal{H}$.

Note: Démontrer que c'est un sous-groupe évite de démontrer que la loi est associative. Fort heureusement, ici cela n'est pas fastidieux!

Montrons que $(\mathcal{H}; \star)$ est un groupe (on considère ici le repère $\mathcal{R}'$). Ainsi, les éléments de $\mathcal{H}$ ont pour coordonnées $(x; \frac{1}{x})$ avec $x \in \mathbb{R}^*$. Nous savons déjà que c'est bien une loi de composition interne, c'est-à-dire que si $(M; N) \in \mathcal{H}^2$, alors $M \star N \in \mathcal{H}$.

Le point $A_0(1; 1)$ est un élément neutre pour cette loi puisque si $M(x; \frac{1}{x}) \in \mathcal{H}$, alors $A_0 \star M = M$ (par 2.b.iii.)

Cette loi est associative car si $M(m; \frac{1}{m})$, $N(n; \frac{1}{n})$ et $P(p; \frac{1}{p})$ sont des éléments de $\mathcal{H}$, alors: $(M \star N) \star P = M \star (N \star P)$ car nous obtenons dans les deux cas le point de coordonnées $(mnp; \frac{1}{mnp})$.

Enfin, à tout élément $M(m; \frac{1}{m}) \in \mathcal{H}$, nous considère $M'(\frac{1}{m}; m) \in \mathcal{H}$. Alors $M \star M' = A_0$ et donc tout élément admet un inverse dans $\mathcal{H}$ pour la loi $\star$.

Enfin, pour obtenir le fait que ce groupe soit isomorphe à $(\mathbb{R}^*; \times)$, nous pouvons considérer l'application $\phi : \mathbb{R}^* \rightarrow \mathcal{H}, \phi(x) = (x; \frac{1}{x})$. Puisque $\phi(x \times y) = \phi(x) \star \phi(y)$, nous en déduisons que c'est bien un isomorphisme de groupes.

3. Résolution de l'équation de Pell-Fermat dans le cas $d = 3$

3.a Soit respectivement (x, y) et (x', y') les coordonnées de M dans le repère $\mathcal{R}$ et $\mathcal{R}'$ et (X, Y) , $(X'; Y')$ celles du point $F(M)$. La formule de changement de repère (2.a.ii) est donc: $\begin{cases} X &= x - \sqrt{3}y \\ Y &= x + \sqrt{3}y \end{cases}$ La formule donnant les coordonnées de l'image de M par F dans le repère $\mathcal{R}$ sont: $\begin{cases} x' &= 2x + 3y \\ y' &= x + 2y \end{cases}$

Ainsi avons-nous:

$$\begin{cases} X' &= x' - \sqrt{3}y' = (2x + 3y) - \sqrt{3}(x + 2y) = (2 - \sqrt{3})x + (3 - 2\sqrt{3})y \\ Y' &= x' + \sqrt{3}y' = (2x + 3y) + \sqrt{3}(x + 2y) = (2 + \sqrt{3})x + (3 + 2\sqrt{3})y \end{cases}$$

Nous pouvons inverser ces formules, ce qui nous donne:

$$\begin{cases} X' &= (2 - \sqrt{3})x + (3 - 2\sqrt{3})y = (2 - \sqrt{3})\frac{1}{2}(X + Y) + (3 - 2\sqrt{3})\frac{\sqrt{3}}{6}(-X + Y) \\ Y' &= (2 + \sqrt{3})x + (3 + 2\sqrt{3})y = (2 + \sqrt{3})\frac{1}{2}(X + Y) + (3 + 2\sqrt{3})\frac{\sqrt{3}}{6}(-X + Y) \end{cases}$$

Nous en déduisons alors finalement: $\begin{cases} X' &= (2 - \sqrt{3})X \\ Y' &= (2 + \sqrt{3})Y \end{cases}$

3.b. Le point A_1 a $(2; 1)$ pour coordonnées dans $\mathcal{R}$. Ainsi, ses coordonnées dans $\mathcal{R}'$ sont $(2 - \sqrt{3}; 2 + \sqrt{3})$. Soit $M(m, \frac{m}{m})$ un point de $\mathcal{H}$ (repère dans $\mathcal{R}'$). Alors $A_1 \star M$ est le point de coordonnées $((2 - \sqrt{3})m; (2 + \sqrt{3})\frac{1}{m})$. Ainsi, le produit des coordonnées donne: $(2 - \sqrt{3})m \times (2 + \sqrt{3})\frac{1}{m} = (2 - \sqrt{3})(2 + \sqrt{3}) = 4 - 3 = 1$ et donc ce point vérifie bien l'équation de $\mathcal{H}$ (dans le repère $\mathcal{R}'$).

3.c. Par 3.b. nous savons que $\forall n \in \mathbb{N}^*, A_{n+1} = A_1 \star A_n$ donc nous obtenons par récurrence $A_{n+1} ((2 - \sqrt{3})^n; (2 + \sqrt{3})^n)$ (dans le repère $\mathcal{R}'$).

3.d. Soit $M(m; \frac{1}{m}) \in \mathcal{H}$ (on repère toujours dans $\mathcal{R}'$). Alors $M \in A_n \widehat{A_{n+1}}$ si et seulement si $(2 - \sqrt{3})^n \leq m \leq (2 - \sqrt{3})^{n-1}$, soit encore si et seulement si $(2 - \sqrt{3})^{n+1} \leq (2 - \sqrt{3})m \leq (2 - \sqrt{3})^n$. Or, $(2 - \sqrt{3})m$ est l'abscisse de $A_1 \star M$ donc l'inégalité implique $A_1 \star M \in A_{n+1} \widehat{A_{n+2}}$.

3.e. Soit $(x, y) \in \mathbb{N}^2$ vérifiant $x^2 - 3y^2 = 1$. Nous considérons donc la demi-branche de l'hyperbole $\mathcal{H}$ appartenant au quart de plan supérieur. Par 3.d. si $M \in \mathcal{H}'$ et $M \in A_n \widehat{A_{n+1}}$ alors $F^{-1}(M) \in A_{n-1} \widehat{A_n}$. Par récurrence descendante, nous obtenons $F^{-n}(M) \in A_0 \widehat{A_1}$ et par 1.c.iii. nous avons $F^{-n}(M) = A_0$ ou $F^{-n}(M) = A_1$. Ainsi, il s'ensuit que $M = F^n(A_0) = A_n$ ou $M = F^n(A_1) = A_{n+1}$, et nous obtenons donc les points de $\mathcal{H}'$ appartenant au quart de plan supérieur.

3.f. Les autres points de $\mathcal{H}'$ sont obtenus par les symétries selon l'axe des abscisses ou par celle selon l'axe des ordonnées (ainsi que par leur composée: la symétrie centrale). Cela nous permet d'obtenir tous les points de $\mathcal{H}'$.

Partie 2: Etude des cas $d = 2$ et $d = 3$

1. On cherche donc les couples $(x; y)$ d'entiers naturels solutions de (E_2) , donc vérifiant $x^2 - 2y^2 = 1$, soit encore $x^2 = 1 + 2y^2$. Déjà $(1; 0)$ est un premier couple de solutions (évident). Ensuite, testons: pour $y = 1$, nous obtenons $x^2 = 3$ équation n'ayant pas de solutions de $\mathbb{N}$. Pour $y = 2$, nous obtenons $x^2 = 9$ qui admet bien une solution dans $\mathbb{N}$; ainsi, nous obtenons le second couple solution: $(3; 2)$. Ensuite on poursuit ... jusqu'à trouver un y tel que $1 + 2y^2$ soit un carré, ce qui arrive pour $y = 12$, donnant le couple $(17; 12)$ pour solutions de (E_2) .

2. Déjà, nous constatons que H est bien un sous-ensemble de $\mathbb{R}_+^*$.

Ensuite, l'élément neutre de $(\mathbb{R}_+^*; \times)$ est $1 = 1 + 0\sqrt{2}$, donc $1 \in H$.

Soient $(g, h) \in H^2$. Ainsi, il existe $(a, b, c, d) \in \mathbb{Z}^4$ tels que $g = a + b\sqrt{2}$ et $h = c + d\sqrt{2}$. De plus $a^2 - 2b^2 = c^2 - 2d^2 = 1$. Montrons alors que le $gh = (ac + 2bd) + (ad + bc)\sqrt{2}$ est un élément de H . Déjà $(ac + 2bd)$ et $(ad + bc)$ sont des entiers comme somme / produit d'entiers (plus formellement, $(\mathbb{Z}; +; \times)$ est un anneau). $gh > 0$ comme produit de deux éléments strictement positifs. Montrons à présent que gh est aussi un élément de H , c'est-à-dire que $(ac + 2bd)^2 - 2(ad + bc)^2 = 0$.

$$\begin{aligned} (ac + 2bd)^2 - 2(ad + bc)^2 &= a^2c^2 + 4abcd + 4b^2d^2 - 2a^2d^2 - 4abcd - 2b^2c^2 \\ &= a^2(c^2 - 2d^2) + 2b^2(2d^2 - c^2) \\ &= a^2 - 2b^2 \quad \text{car } c^2 - 2d^2 = 1 \\ &= 1 \end{aligned}$$

Nous en déduisons donc que H est stable par $\times$.

Soit $h \in H$; ainsi, il existe des entiers a et b tels que $h = a + b\sqrt{2}$, et $a^2 - 2b^2 = 1$. Montrons que h possède un inverse en raisonnant par analyse-synthèse.

Supposons donc que $g = c + d\sqrt{2}$ vérifiant $c^2 - 2d^2 = 1$ est l'inverse de h . Ainsi, $h \times g = 1$, donc $(a + b\sqrt{2})(c + d\sqrt{2}) = 1$, ce qui nous donne le système:

$$\begin{cases} ac + 2bd = 1 \\ ad + bc = 0 \end{cases} \quad \text{d'où} \quad \begin{cases} abc + 2ab^2d = b \\ a^2d + abc = 0 \end{cases} \quad \text{et par soustraction } d = -b.$$

Il s'ensuit alors que $c = a$ (on substitue d par $-b$ dans la première équation; on obtient $ac - 2b^2 = 1$ et nous savons que $a^2 - 2b^2 = 1$).

Phase de synthèse: Considérons $g = a - b\sqrt{2}$. Déjà, cet élément appartient clairement à H puisque $a^2 - 2b^2 = 1$. De plus, $g \times h = (a - b\sqrt{2})(a + b\sqrt{2}) = a^2 - 2b^2 = 1$ car $h \in H$. Ainsi en déduisons-nous que g possède bien un inverse dans H .

On pouvait trouver l'inverse de $h = a + b\sqrt{2}$ sans faire la phase d'analyse. En ce cas, il est tout à fait possible de n'écrire que la phase de synthèse; i.e. posons $g = a - b\sqrt{2}$. On vérifie déjà que $g \in H$ puis que $gh = 1$ et on conclut que h possède un inverse dans H .

Néanmoins, quand on a pas d'idée, on raisonne bien souvent par Analyse-synthèse ou par absurde: ces deux raisonnements permettent de débiter notre recherche de solution avec un hypothèse en plus!

3.i. D'après la question précédente, si $h = a + b\sqrt{2}$, alors $h^{-1} = a - 2\sqrt{2}$ (inverse dans H). Ainsi $a + b\sqrt{2} > 0$ et $a - b\sqrt{2} > 0$. Nous en déduisons donc que $2a = h + h^{-1} > 2$ (l'inégalité est stricte car le cas d'égalité correspond

uniquement à $h = 1$, ce qui est exclu car $h \in H \cap]1; +\infty[$. Nous en déduisons donc que $a > 1$. Or, puisque $a^2 = 1 + 2b^2$, nous en déduisons que a^2 est impaire, donc que a lui-même l'est. Ainsi, $a \geq 3$ (premier nombre impaire strictement supérieur à 1).

3.ii. Les mêmes inégalités impliquent $2\sqrt{2}b > 0$. Or, $b \in \mathbb{Z}$, donc $g \geq 1$. Pour la valeur $b = 1$, alors l'équation $a^2 - 2 = 1$ n'admet pas de solution dans $\mathbb{Z}$. Ainsi en déduit-on que $b \geq 2$.

3.iii. Finalement le premier couple possible est $a \geq 3$ et $b \geq 2$. Or, $(3 + 2\sqrt{2}) \in H$, d'où nous en déduisons qu'il s'agit de la plus petite valeur possible pour $H \cap]1; +\infty[$. Ainsi $\delta = 3 + 2\sqrt{2}$.

4. Puisque H est stable par produit, nous en déduisons que $\forall n \in \mathbb{N}$, $\delta^n \in H$ (pour $n = 0$, cela résulte du fait que $\delta^0 = 1$ qui est le neutre de H). De plus, puisque $\delta^{-1} = \frac{1}{\delta}$, nous en déduisons que les puissances négatives de δ sont aussi dans H .

A présent, montrons l'inclusion réciproque. Soit $h \in H$. Puisque $h > 0$, nous pouvons en prendre le logarithme. Soit alors $k = \left\lceil \frac{\ln(h)}{\ln(\delta)} \right\rceil$. Nous avons donc $k \leq \frac{\ln(h)}{\ln(\delta)} \leq k + 1$ d'où $k \ln(\delta) \leq \ln(h) \leq \ln(\delta)(k + 1)$ (la dernière inégalité étant justifiée par $\delta > 1$ donc $\ln(\delta) > 0$). Ainsi: $1 \leq \frac{h}{\delta^k} < \delta$. Comme δ est le minimum de $H \cap]1; +\infty[$, nous en déduisons que $\frac{h}{\delta^k} = 1$, donc $h = \delta^k$. Nous en déduisons donc que $H \subset \{\delta^n; n \in \mathbb{Z}\}$.

5. Nous cherchons donc tous les k tels que $(3 + 2\sqrt{2})^k \leq 100(1 + \sqrt{2})$. Nous avons $\delta^1 = 3 + 2\sqrt{2}$, $\delta^2 = 17 + 12\sqrt{2}$ et $\delta^3 = 99 + 70\sqrt{2}$ qui est le dernier élément de H vérifiant cette condition.

6.i. Si nous avons toutes les solutions de (E_2) dans $\mathbb{N}^2$, alors nous déduisons toutes les solutions de (E_2) dans $\mathbb{Z}^2$ en utilisant la parité de l'équation $x^2 - dy^2 = 1$. En l'occurrence, si (x, y) est solution, alors $(-x, y)$, $(x, -y)$ et $(-x, -y)$ le sont aussi.

6.ii. Toute solution de (E_2) dans $\mathbb{N}^2$ est de la forme δ^k (pour un certain $k \in \mathbb{N}$. Ainsi, notons $(3 + 2\sqrt{2})^n = x_n + y_n\sqrt{2}$. Nous définissons ainsi deux suites. La suite double $(x_n; y_n)$ vérifie: $(x_0; y_0) = \delta^0 = 1$ et $\forall n \in \mathbb{N}$,

$$\begin{aligned} (x_{n+1}; y_{n+1}) &= \delta^{n+1} = \delta^n \times \delta \\ &= (x_n + y_n\sqrt{2})(3 + 2\sqrt{2}) \\ &= (3x_n + 4y_n) + (2x_n + 3y_n)\sqrt{2}. \end{aligned}$$

Ainsi la suite double $(x_n; y_n)$ est définie par les relations de récurrences:
$$\begin{cases} x_0 = 1; & y_0 = 0 \\ x_{n+1} &= 3x_n + 4y_n \\ y_{n+1} &= 2x_n + 3y_n \end{cases}$$

Attention ici, nous identifions $(x_{n+1}; y_{n+1}) \in \mathbb{Z}^2$ à partir de la relation $x_{n+1} + y_{n+1}\sqrt{2} = (3x_n + 4y_n) + (2x_n + 3y_n)\sqrt{2}$, car $\sqrt{2}$ est irrationnel (qui repose sur le fait que 2 n'est pas un carré). A titre d'exemple, on ne peut rien conclure à partir de la relation suivante: $x_{n+1} + y_{n+1}\sqrt{4} = (3x_n + 4y_n) + (2x_n + 3y_n)\sqrt{4}$ (idem si $(x_n; y_n) \in \mathbb{R}^2$).

6.iii. En appliquant cette relation de récurrence, nous obtenons:

$$\delta_0 = (1); \delta^1 = (3 + 2\sqrt{2}); \delta^2 = 17 + 12\sqrt{2}; \delta^3 = 99 + 70\sqrt{2}...$$

Nous retrouvons alors bien les résultats de la question II.5.

7. Nous procédons de la même manière que précédemment (en remarquant que 3 n'est pas un carré). Déjà, recherchons le plus petit élément δ . Si $h = a + b\sqrt{3}$, alors son inverse est l'élément $h^{-1} = a - b\sqrt{3}$. Il s'ensuit alors que, de $h > 0$ et $\frac{1}{h} > 0$, nous obtenons: $a \geq 1$. Le cas $a = 1$ correspond à la solution triviale $(1; 0)$. Considérons donc $a \geq 2$. Cela implique alors $b \geq 1$. On montre alors que $\delta = 2 + \sqrt{3}$ est le générateur de l'ensemble H des solutions de (E_3) . Nous pouvons à présent rechercher les relations de récurrences permettant de définir les suites $(x_n; y_n)$ telles que $x_n + y_n\sqrt{3} = \delta^n$. Nous obtenons alors: $x_{n+1} = 2x_n + 3y_n$ et $y_{n+1} = x_n + 2y_n$, avec comme condition initiale $x_0 = 1$ et $y_0 = 0$.

Partie 3: Etude du cas général

1. Lemme d'approximation de Dirichlet

a. Considérons les $(n + 1)$ réels $\{k\xi\}$ pour $k \in \{0, \dots, n\}$. Tous ces réels appartiennent à l'intervalle $[0; 1[$ par définition de la partie fractionnaire d'un réel. Aussi, considérons la subdivision régulière de $[0; 1[$: $\{I_r = [\frac{r}{n}; \frac{r+1}{n}]\}$ avec $r \in \{0, \dots, n - 1\}$.

Par le lemme des tiroirs, nous en déduisons qu'au moins l'un des intervalles I_r contient 2 éléments: c'est-à-dire il existe $r \in \{0, \dots, n - 1\}$ et deux entiers naturels $0 \leq p < q \leq n$ tel que $\{q\xi\} \in I_r$ et $\{p\xi\} \in I_r$, ce qui implique $0 \leq \{q\xi\} - \{p\xi\} < \frac{1}{n}$.

Nous avons donc: $0 \leq \{q\xi\} - \{p\xi\} < \frac{1}{n}$. Par définition de la partie fractionnaire, nous avons: $0 \leq q\xi - [q\xi] - p\xi + [p\xi] < \frac{1}{n}$ donc $0 \leq (q - p)\xi - ([q\xi] - [p\xi]) < \frac{1}{n}$. On pose alors $x = q - p \in \mathbb{Z}$ et $y = [q\xi] - [p\xi] \in \mathbb{Z}^*$ ce qui implique alors la relation: $1 \leq y \leq n$ et $\left| \xi - \frac{x}{y} \right| < \frac{1}{ny}$. Il suffit alors de considérer la fraction irréductible pour obtenir la condition de l'énoncé.

b. Pour $N_0 \in \mathbb{N}^*$, on a par a. l'existence d'une fraction irréductible $\frac{x_0}{y_0}$ telle que $0 \leq \xi - \frac{x_0}{y_0} \leq \frac{1}{N_0 y_0} \leq \frac{1}{y_0^2}$. Comme ξ est irrationnel, $\xi - \frac{x_0}{y_0} \neq 0$. Ainsi, il existe un entier naturel N_1 tel que $N_1 > \frac{1}{|\xi - \frac{x_0}{y_0}|}$. Par la question a. il existe alors une fraction irréductible $\frac{x_1}{y_1}$ telle que $|\xi - \frac{x_1}{y_1}| \leq \frac{1}{y_1^2}$. En réitérant ce processus, nous obtenons une suite de fractions irréductibles $\left(\frac{x_n}{y_n}\right)$ telle que: $\forall n \in \mathbb{N}$, $|\xi - \frac{x_n}{y_n}| < \frac{1}{y_n^2}$. De plus, les $(x_n; y_n)$ sont tous différents car: $\forall n \in \mathbb{N}$, $|\xi - \frac{x_{n+1}}{y_{n+1}}| < \frac{1}{N_n y_{n+1}} < \frac{1}{N_n} < |\xi - \frac{x_n}{y_n}|$. Nous en déduisons alors le lemme d'approximation de Dirichlet.

2. Existence d'une solution non triviale de (E_d) .

a. Si $a \equiv b \pmod{m}$ et $c \equiv d \pmod{m}$ alors il existe des entiers $(k; l) \in \mathbb{Z}^2$ tels que $a = b + km$ et $c = d + lm$. Ainsi, $ac = bd + (kd + bl + klm)m \equiv ab \pmod{m}$.

b. Supposons par l'absurde que $\sqrt{d} \in \mathbb{Q}$. Ainsi, il existe $(x, y) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $\sqrt{d} = \frac{x}{y}$ et $x \wedge y = 1$ (i.e. x et y sont premiers entre eux). Il s'ensuit alors que $by^2 = x^2$. Soit p un nombre premier divisant x . Alors p^2 est un diviseur de x^2 . Alors $p^2 | (dy^2)$. Or, par le théorème de Gauss, puisque x et y sont premiers entre eux, nous en déduisons que $p^2 | d$, ce qui contredit le fait que d soit sans facteurs carrés. Ainsi, nous montrons bien que $\sqrt{d}$ est irrationnel.

c. Soient $(m, n, p, q) \in \mathbb{Z}^4$ tels que $m + n\sqrt{d} = p + q\sqrt{d}$. Alors $(m - p) = (q - n)\sqrt{d}$. Si $q \neq n$, cela implique $\sqrt{d} = \frac{m-p}{q-n}$, et par la question b. nous en déduisons que c'est absurde. Aussi, nous avons nécessairement $q = n$ et par suite $p = m$.

d. $\sqrt{d}$ est donc irrationnel: nous pouvons donc utiliser le lemme d'approximation de Dirichlet. Aussi il existe une infinité de fractions irréductibles $\frac{x}{y}$ telles que $|\sqrt{d} - \frac{x}{y}| < \frac{1}{y^2}$. Il s'ensuit alors que $|x - y\sqrt{d}| < \frac{1}{y}$ soit $|x| < \sqrt{d}y + \frac{1}{y}$. Ainsi, nous en déduisons que $|x + y\sqrt{y}| \leq |x| + y\sqrt{d} < 2y\sqrt{d} + \frac{1}{y}$. En multipliant cette inégalité par $|x - y\sqrt{d}| < \frac{1}{y}$ nous en déduisons

$$|x^2 - dy^2| = |x - \sqrt{d}y| \times |x + \sqrt{d}y| < 2\sqrt{d} + \frac{1}{y^2} \leq 2\sqrt{d} + 1.$$

e. Par la question précédente, nous savons qu'il existe une infinité de fractions irréductibles $\frac{x_n}{y_n}$ telles que $|x^2 - dy^2| \leq 2\sqrt{d} + 1$. Aussi existe un entier naturel $m \in \{1, \dots, \lfloor \sqrt{2d} + 1 \rfloor\}$ tel qu'il y ait une infinité de couples $(x, y) \in \mathbb{Z}^2$ avec $x \wedge y = 1$ et $x^2 - dy^2 = m$. Considérons alors la restriction de l'application $\phi : (x, y) \in \mathbb{Z}^2 \mapsto (x \pmod{m}; y \pmod{m}) \in \{0, \dots, m-1\}^2$ à cet ensemble de solutions. L'ensemble d'arrivée étant fini, nous en déduisons que ϕ n'est pas injective: il existe donc $(x_1; y_1)$ et $(x_2; y_2)$ vérifiant $|x^2 - dy^2| = m$ tels que $x_1 \equiv x_2 \pmod{m}$ et $y_1 \equiv y_2 \pmod{m}$.

f. Le calcul de $\gamma = \alpha \times \beta$ montre que $\gamma = (x_1 x_2 - d y_1 y_2) + (x_2 y_1 - x_1 y_2)\sqrt{d} = p + q\sqrt{d}$ (avec $(p, q) \in \mathbb{Z}^2$). Par les relations de congruences, nous déduisons: $p \equiv x_1 x_2 - d y_1 y_2 \equiv x_1^2 - d y_1^2 \equiv 0 \pmod{m}$. De même, $q \equiv x_2 y_1 - x_1 y_2 \equiv x_1 y_1 - x_1 y_1 \equiv 0 \pmod{m}$.

Montrons à présent que $p^2 - dq^2 = m^2$. Partons de $(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = (x_1 x_2 - d y_1 y_2) - (x_2 y_1 - x_1 y_2)\sqrt{d} = p - q\sqrt{d}$. Nous avons donc:

$$\begin{aligned} p^2 - dq^2 &= (p + q\sqrt{d})(p - q\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d})(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) \\ &= (x_1^2 - d y_1^2)(x_2^2 - d y_2^2) \\ &= m^2. \end{aligned}$$

g. Les solutions $(1; 0)$ et $(-1; 0)$ sont triviales. Soit $\omega = \frac{\gamma}{m} = a + b\sqrt{d}$ avec $a = \frac{p}{m}$ et $b = \frac{q}{m}$ vérifiant $a^2 - db^2 = \left(\frac{p}{m}\right)^2 - d\left(\frac{q}{m}\right)^2 = \frac{p^2 - dq^2}{m^2} = 1$. Cette solution (a, b) n'est pas triviale. En effet, si $a = 1$ et $b = 0$ alors $\gamma = \alpha\beta = m$. Nous en déduisons alors l'égalité $x_1 + y_1\sqrt{d} = x_2 + y_2\sqrt{d}$, ce qui implique ($\sqrt{d}$ étant irrationnel) $x_1 = x_2$ et $y_1 = y_2$: cela contredit la définition des couples $(x_1; y_1)$ et $(x_2; y_2)$.

3. Description des solutions de l'équation (E_d)

On considère à présent l'ensemble $H_d = \{a + b\sqrt{d} \in \mathbb{R}_+^* / (a, b) \in \mathbb{Z}^2, a^2 - db^2 = 1\}$.

a. Nous allons montrer que $(H_d; \times)$ est un sous-groupe de $(\mathbb{R}_+^*; \times)$. Déjà, les éléments de H_d sont bien des réels positifs.

$1 = 1 + 0\sqrt{d}$ donc H_d est non vide.

Si $h = a + b\sqrt{d}$ et $g = x + y\sqrt{d}$ sont des éléments de H_d , alors le produit $gh = (a + b\sqrt{d})(x + y\sqrt{d}) = (ax + bdy) + (ay + bx)\sqrt{d}$ est aussi un élément de H_d puisque $(ax + bdy)^2 - d(ay + bx)^2 = a^2x^2 + 2abxyd + d^2b^2y^2 - da^2y^2 - 2abxyd + db^2x^2 = a^2(x^2 - dy^2) + db^2(dy^2 - x^2) = a^2 - db^2 = 1$.

Enfin, H_d est stable par passage à l'inverse puisque si $h = a + b\sqrt{d}$, alors on vérifie que $h^{-1} = a - b\sqrt{d}$ est bien un élément de H_d et qu'il est l'inverse de h .

b. Considérons $H_d \cap]1; +\infty[$. Puisque H_d n'est pas réduit à 1, il existe $h \in H_d \setminus \{1\}$. Mais alors $h^{-1} \in H_d$ et donc l'un des deux éléments $\{h; h^{-1}\}$ appartient à l'ensemble $H_d \cap]1; +\infty[$. Il s'ensuit alors que $H_d \cap]1; +\infty[$ est une partie non vide et minorée de $\mathbb{R}$: aussi, elle admet une borne inférieure: soit δ celle-ci.

Montrons que $\delta \in H_d$. Si $h = a + b\sqrt{d}$, alors $h^{-1} = a - b\sqrt{d}$. Ainsi, nous avons: $2a = h + h^{-1}$ et $2bd > 0$. a et b étant des entiers, nous en déduisons $a \geq 1$ et $b \geq 1$; ainsi, $h \geq 1 + \sqrt{d} > 1$.

A présent, raisonnons par l'absurde en supposant que $\delta \notin H_d \cap]1; +\infty[$. Alors, $r = \delta^2 > \delta > 1$ (car $\delta > 1$). Aussi, puisque $\delta < r$ est la borne inférieure de $H_d \cap]1; +\infty[$, nous en déduisons l'existence d'un élément $h \in H_d \cap]1; +\infty[$ tel que $\delta < h < \delta^2$. Soit $\varepsilon > 0$ tel que $\delta < h - \varepsilon$. Alors, il existe un second élément, $g \in H_d \cap]1; +\infty[$ tel que $\delta < g < h - \varepsilon < h < \delta^2$. Nous en déduisons alors: $1 < \frac{h}{g} < \delta$ ce qui contredit le fait que δ soit le minorant de $H_d \cap]1; +\infty[$ (puisque $\frac{h}{g} \in H_d$). Aussi, $\delta \in H_d \cap]1; +\infty[$ et est donc le minimum de cet ensemble.

c. Soit $h \in H_d$. Puisque $\delta > 1$, nous en déduisons que $\lim_{k \rightarrow +\infty} \delta^k = +\infty$ et $\lim_{k \rightarrow -\infty} \delta^k = 0$. Ainsi, il existe $k \in \mathbb{Z}$ tel que $\delta^k \leq h < \delta^{k+1}$. Donc $1 \leq \frac{h}{\delta^k} \delta$, et comme δ est le plus petit élément de $H_d \cap]1; +\infty[$, nous en déduisons que $h = \delta^k$. Ainsi, $H_d = \{\delta^n / n \in \mathbb{Z}\}$.

d. En repassant dans le repère $\mathcal{R}$, nous en déduisons que les solutions de (E_d) sont de la forme $\left(\pm \frac{1}{2}(\delta^n + \delta^{-n}); \pm \frac{1}{2\sqrt{d}}(\delta^n - \delta^{-n})\right)$ avec $n \in \mathbb{Z}$.

4. Algorithme des Anglais pour rechercher δ .

a. $k_0 = 1$ donc est un diviseur de tout élément. Ainsi, les seules conditions sur l sont $l \in \mathbb{Z}$ et $l \leq [\sqrt{d}]$. L'ensemble considéré est alors non vide et est majoré. Nous en déduisons qu'il possède un plus grand élément, qui est $[\sqrt{d}]$.

b. On a $p_1 = r_0 = [\sqrt{d}]$, $q_1 = 1$ et $k_1 = r_0^2 - d$ donc $p_1^2 - dq_1^2 = k_1$.

c. On a: $p_{n-1}q_n - p_nq_{n-1} = p_{n-1} \left(\frac{p_{n-1} + q_{n-1}r_{n-1}}{k_{n-1}} \right) - \left(\frac{p_{n-1}r_{n-1} + dq_{n-1}}{k_{n-1}} \right) q_{n-1} = \frac{p_{n-1}^2 - dq_{n-1}^2}{k_{n-1}} = 1$. On en déduit alors, d'après le théorème de Bezout, que $p_n \wedge q_n = 1$.

d. On a $p_n^2 - dq_n^2 = k_n^2$, soit $p_n^2 = k_n^2 + dq_n^2$. Si p est un nombre premier divisant à la fois k_n et q_n , alors p divise p_n et donc $p_n \wedge q_n = p$, ce qui contredit $p_n \wedge q_n = 1$. Ainsi, $k_n \wedge q_n = 1$.

e. ($\star\star\star$). Procédons en deux temps: on montre déjà que l'ensemble $\{l \in \mathbb{Z} / k_n | (p_n + lq_n)\}$ est non vide. Pour ce faire, on considère l'application $\Psi : \{0, \dots, k_n - 1\} \rightarrow \{0, \dots, k_n - 1\}$ définie par $\Psi(l) = p_n + lq_n \pmod{k_n}$ (i.e. le reste de la division euclidienne de $p_n + lq_n$ par k_n).

Cette application est injective car si $\Psi(l) = \Psi(l')$, alors $p_n + lq_n \equiv p_n + l'q_n \pmod{k_n}$ soit $(l - l')q_n \equiv 0 \pmod{k_n}$. Ainsi, $k_n | (l - l')q_n$ et comme $k_n \wedge q_n = 1$, le lemme de Gauss implique $k_n | (l - l')$. Or, $0 \leq |l - l'| \leq k_n - 1$, donc $l - l' = 0$.

Ψ étant une injection entre deux ensembles de mêmes cardinaux, c'est une bijection. Ainsi, 0 admet un antécédent par Ψ , don il existe $\ell \in \{0, 1, \dots, (k_n - 1)\}$ tel que $k_n | (p_n + \ell q_n)$.

Montrons à présent que l'ensemble $\{l \in \mathbb{Z} / k_n | (p_n + lq_n) \text{ et } l \leq [\sqrt{d}]\}$ est non vide. $\forall j \in \mathbb{N}$, $l_j = \ell - jk_n$. Pour j assez grand, $l_j < [\sqrt{d}]$. De plus, $k_n | (p_n + \ell q_n - jk_n q_n) = p_n + l_j q_n$. Ainsi, l'ensemble considéré est non vide et est majoré. Nous en déduisons alors qu'il possède un plus grand élément: r_n .

f. Par définition de r_n , k_n divise $p_n + r_n q_n$ donc divise $p_n(p_n + r_n q_n) = p_n^2 + p_n q_n r_n$. Or, $p_n^2 = k_n + dq_n^2$ donc k_n divise $p_n q_n r_n + dq_n^2 + k_n$ et donc divise $q_n(p_n r_n + dq_n)$.

g. Comme $k_n \wedge q_n = 1$, nous déduisons de f. et du théorème de Gauss que $k_n | p_n r_n + dq_n$. Ainsi k_{n+1} est un entier. Enfin:

$$p_{n+1}^2 - dq_{n+1}^2 = \frac{1}{k_n^2} (p_n^2 r_n^2 + q_n^2 d^2 + 2dp_n q_n r_n - dp_n^2 - dq_n^2 r_n^3 - 2dp_n q_n r_n)$$

d'où $p_{n+1}^2 - dq_{n+1}^2 = \frac{1}{k_n^2} (r_n^2 - d)(p_n^2 - dq_n^2)$. Comme $p_n^2 - dq_n^2 = k_n$, on en déduit $p_{n+1}^2 - dq_{n+1}^2 = \frac{1}{k_n} (r_n^2 - d) = k_{n+1}$.

Cette algorithme permet d'obtenir δ , qui permet à son tour d'obtenir toutes les solutions de (E_d) .