Le 05.12.20

Devoir surveillé n°4
CORRECTION

Problème - Equation de Pell-Fermat

On appelle équation de Pell-Fermat l'équation :

$$x^2 - dy^2 = m$$

où $d, m \in \mathbb{N}$ et où les inconnues x et y sont entières (on parle d'équation diophantienne dans ce cas).

$$A_d = \mathbb{Z}[\sqrt{d}] = \{a + \sqrt{d}b; a, b \in \mathbb{Z}\}$$

Partie A - Etude d'un couple de suites imbriquées

1. On considère deux suites numériques $(a_n)_n$ et $(b_n)_n$ telles que

$$\begin{cases} & a_0 = 1 \\ \forall\, n \in \mathbb{N}, & a_{n+1} = 2b_n + a_n \end{cases} \qquad \begin{cases} & b_0 = 0 \\ \forall\, n \in \mathbb{N}, & b_{n+1} = a_n + b_n \end{cases}$$

Piste de recherche...
Il faut prendre le temps de bien répondre à cette question. Elle est ouverte (on ne sait si les suites sont croissantes ou décroissantes ou autre chose), il faut donc « prendre ses responsabilités ».
Quelques calculs des premiers termes semblent indiquer que ces deux suites sont croissantes.
Ensuite, pour montrer la croissance, on calcule $a_{n+1} - a_n$ et $b_{n+1} - b_n$. Il faut donc commencer par démontrer un résultat intermédiaire (et non demandé) : la positivité des deux suites...

Montrons par récurrence : $\mathcal{P}_n$: « $a_n \geqslant 0$ et $b_n \geqslant 0$ ».
— Par hypothèse $a_0 \geqslant 0$ et $b_0 \geqslant 0$. Donc $\mathcal{P}_0$ est vraie.
— Supposons que $\mathcal{P}_n$ est vraie.
Alors par addition de nombres positifs : $a_{n+1} = 2b_n + a_n \geqslant 0$ et $b_{n+1} = a_n + b_n \geqslant 0$ /2

Donc pour tout $n \in \mathbb{N}$, $a_n \geqslant 0$ et $b_n \geqslant 0$.

Et donc pour tout $n \in \mathbb{N}$, $a_{n+1} - a_n = 2b_n \geqslant 0$ et $b_{n+1} - b_n = a_n \geqslant 0$. /1

Donc les suites (a_n) et (b_n) sont croissantes.

2. (a) On sait que pour tout $n \in \mathbb{N}$: $a_{n+1} = a_n + 2b_n$ et $b_{n+1} = a_n + b_n$.
Donc $b_n = \frac{1}{2}(a_{n+1} - a_n)$ et $a_n = b_{n+1} - b_n$.
Donc pour tout $n \in \mathbb{N}$:

$$a_{n+2} = a_{n+1} + 2b_{n+1} = a_{n+1} + 2(a_n + b_n) = a_{n+1} + 2a_n + 2b_n = a_{n+1} + 2a_n + a_{n+1} - a_n = 2a_{n+1} + a_n$$

$$b_{n+2} = a_{n+1} + b_{n+1} = a_n + 2b_n + b_{n+1} = b_{n+1} - b_n + 2b_n + b_{n+1} = 2b_{n+1} + b_n$$

/1,5

(a_n) et (b_n) vérifient $\begin{cases} & a_0 = 1 \\ & a_1 = 1 \\ \forall\, n \in \mathbb{N}, & a_{n+2} = 2a_{n+1} + a_n \end{cases}$ $\begin{cases} & b_0 = 0 \\ & b_1 = 1 \\ \forall\, n \in \mathbb{N}, & b_{n+2} = 2b_{n+1} + b_n \end{cases}$.

(b) (a_n) et (b_n) sont des suites récurrentes linéaires d'ordre 2 à coefficients constants, de même équation caractéristique :

$$x^2 - 2x - 1 = 0 \iff (x - 1 - \sqrt{2})(x - 1 + \sqrt{2}) = 0$$

Donc il existe A_1, A_2, B_1, B_2 tels que pour tout $n \in \mathbb{N}$,

$$a_n = A_1(1 + \sqrt{2})^n + A_2(1 - \sqrt{2})^n \qquad b_n = B_1(1 + \sqrt{2})^n + B_2(1 - \sqrt{2})^n$$

Or $a_0 = a_1 = 1$

$$\left\{\begin{array}{llll} A_1 & +A_2 & = 1 \\ A_1(1+\sqrt{2}) & +A_2(1-\sqrt{2}) & = 1 \end{array}\right. \iff \left\{\begin{array}{llll} A_1 & +A_2 & = 1 \\ A_1\sqrt{2} & -A_2\sqrt{2} & = 0 \end{array}\right. \iff \left\{\begin{array}{ll} A_1 & = \frac{1}{2} \\ A_2 & = \frac{1}{2} \end{array}\right.$$

Or $b_0 = b_1 = 1$

$$\left\{\begin{array}{llll} B_1 & +B_2 & = 0 \\ B_1(1+\sqrt{2}) & +B_2(1-\sqrt{2}) & = 1 \end{array}\right. \iff \left\{\begin{array}{llll} B_1 & +B_2 & = 0 \\ B_1\sqrt{2} & -B_2\sqrt{2} & = 1 \end{array}\right. \iff \left\{\begin{array}{ll} B_1 & = \frac{1}{2\sqrt{2}} \\ B_2 & = \frac{-1}{2\sqrt{2}} \end{array}\right.$$

/2

$$\boxed{\text{Pour tout } n \in \mathbb{N},\ a_n = \frac{1}{2}((1+\sqrt{2})^n + (1-\sqrt{2})^n) \text{ et } b_n = \frac{1}{2\sqrt{2}}((1+\sqrt{2})^n - (1-\sqrt{2})^n)}$$

(c) Comme $1-\sqrt{2} \in]-1, 0]$, alors $(1-\sqrt{2})^n \to 0$.
Et de même $1+\sqrt{2} > 1$, donc $(1+\sqrt{2})^n \to +\infty$.
Donc

$$(1-\sqrt{2})^n = o\left((1+\sqrt{2})^n\right)$$

Ainsi $(1+\sqrt{2})^n + (1-\sqrt{2})^n \sim (1+\sqrt{2})^n$ et $(1+\sqrt{2})^n - (1-\sqrt{2})^n \sim (1+\sqrt{2})^n$. /1,5

$$\boxed{a_n \sim \tfrac{1}{2}(1+\sqrt{2})^n \text{ et } b_n \sim \tfrac{1}{2\sqrt{2}}(1+\sqrt{2})^n.}$$

3. (a) Pour tout $n \in \mathbb{N}^*$, $a_n - b_n = a_{n-1} + 2b_{n-1} - a_{n-1} - b_{n-1} = b_{n-1} \geqslant 0$.
Donc si $a_n \leqslant k$, alors $b_n (\leqslant a_n) \leqslant k$.
Ainsi, si $a_n \leqslant k$, alors nécessairement $b_n \leqslant k$. La condition sur b_n dans la définition de r_k est inutile.
On en déduit donc que /1

$$\boxed{r_k = \text{card}\{n \in \mathbb{N} \mid a_n \leqslant k\}}$$

(b) Soit $k \in \mathbb{N}$ et $k \geqslant 2$.
$a_0 = 1$ et la suite $(a_n) \to +\infty$. Ainsi il existe $N \in \mathbb{N}$ tel que $a_N \leqslant k$ et $a_{N+1} > k$.
La suite (a_n) est croissante. Donc $a_n \leqslant k \iff n \leqslant N$. /1
On se concentre sur la recherche de N.
Comme $1-\sqrt{2} \in]-1, 0]$, pour tout $n \in \mathbb{N}$, $|(1-\sqrt{2})^n| < 1$ i.e. $-1 \leqslant -(1-\sqrt{2})^n \leqslant 1$.

$$\begin{array}{rl} \frac{1}{2}((1+\sqrt{2})^N - 1) \quad \leqslant a_N = \frac{1}{2}((1+\sqrt{2})^N - (1-\sqrt{2})^N) & \\ a_{N+1} = \frac{1}{2}((1+\sqrt{2})^{N+1} - (1-\sqrt{2})^{N+1}) \quad \leqslant \frac{1}{2}((1+\sqrt{2})^{N+1} + 1) & \end{array}$$

Ainsi :

$$\left\{\begin{array}{l} a_N \leqslant k \\ a_{N+1} > k \end{array}\right. \implies \left\{\begin{array}{l} \frac{1}{2}((1+\sqrt{2})^N - 1) \leqslant k \\ k < \frac{1}{2}((1+\sqrt{2})^{N+1} + 1) \end{array}\right. \implies \left\{\begin{array}{l} (1+\sqrt{2})^N \leqslant 2k+1 \\ 2k-1 < (1+\sqrt{2})^{N+1} \end{array}\right.$$

$$\implies \left\{\begin{array}{l} N \leqslant \dfrac{\ln(2k+1)}{\ln(1+\sqrt{2})} \\ \dfrac{\ln(2k-1)}{\ln(1+\sqrt{2})} < N+1 \end{array}\right. \implies \left\{\begin{array}{l} N = \lfloor N \rfloor \leqslant \left\lfloor \dfrac{\ln(2k+1)}{\ln(1+\sqrt{2})} \right\rfloor \\ \left\lfloor \dfrac{\ln(2k-1)}{\ln(1+\sqrt{2})} \right\rfloor < \lfloor N+1 \rfloor = N+1 \end{array}\right.$$

Selon l'énoncé, notons donc $N_k = \left\lfloor \dfrac{\ln(2k)}{\ln(1+\sqrt{2})} \right\rfloor$
ainsi que $\epsilon_1 = \left\lfloor \frac{\ln(2k+1)}{\ln(1+\sqrt{2})} \right\rfloor - \left\lfloor \frac{\ln(2k)}{\ln(1+\sqrt{2})} \right\rfloor$ et $\epsilon_2 = \left\lfloor \frac{\ln(2k)}{\ln(1+\sqrt{2})} \right\rfloor - \left\lfloor \frac{\ln(2k-1)}{\ln(1+\sqrt{2})} \right\rfloor$ On a donc $N \leqslant N_k + \epsilon_1$ et $N_k - \epsilon_2 < N+1$, donc $N_k \in [\![N - \epsilon_1, N+1-\epsilon_2[\![$.
Or d'après l'énoncé, ϵ_1 et $\epsilon_2 \in [0, \frac{1}{2}[$.
Il y a donc un seul nombre entier dans l'intervalle $[\![N-\epsilon_1, N+1-\epsilon_2[\![$, c'est N. Donc $N_k = N$. /2

$$\boxed{\text{Avec } N_k = \left\lfloor \frac{\ln(2k)}{\ln(1+\sqrt{2})} \right\rfloor, \text{ on a } a_n \leqslant k \iff n \leqslant N_k.}$$

(c) Le carré $[\![0, k]\!]^2$ contient $(k+1)^2$ couple (a, b).
Parmi ceux-ci, r_k sont des couples de type (a_n, b_n).
Or ces couples sont exactement $(a_0, b_0), (a_1, b_1) \ldots (a_{N_k}, b_{N_k})$. Donc $r_k = N_k + 1$ /1

$$\boxed{\text{Donc la proportion des } (a_n, b_n) \text{ parmi les couples de } [\![0,k]\!]^2 \text{ est } s_k := \frac{1}{(k+1)^2}\left(\left\lfloor \frac{\ln(2k)}{\ln(1+\sqrt{2})} \right\rfloor + 1\right).}$$

(d) $\ln(2k) = \ln k + \ln 2 \sim \ln k$. De même $(k+1)^2 \sim (k)^2 = k^2$.

Puis pour tout suite $(u_n) \to +\infty$, $u_n - 1 < \lfloor u_n \rfloor \leqslant u_n$, donc $1 - \dfrac{1}{u_n} \leqslant \dfrac{\lfloor u_n \rfloor}{u_n} \leqslant 1$.

Et donc par encadrement, si $(u_n) \to \infty$: $\lfloor u_n \rfloor \sim u_n$.

On trouve donc /2

$$\boxed{s_k \underset{k\to+\infty}{\sim} \frac{1}{\ln(1+\sqrt{2})} \frac{\ln k}{k^2}}$$

Partie B - Structure algébrique

Soit $d \in \mathbb{N}$. On suppose que d n'est pas un carré parfait.
On note $A_d = \mathbb{Z}[\sqrt{d}]$

1. Unicité d'écriture.

(a) i. Si pour tout $p \in \mathcal{P}$, $v_p(d)$ est pair, alors $d = \left(\prod_{p\in\mathcal{P}} p^{v_p(d)/2}\right)^2$.

Et donc d est un carré parfait. Impossible. /1

$$\boxed{\text{Il existe } s \in \mathcal{P}, \text{ tel que } v_s(d) \text{ est impair.}}$$

ii. On suppose que $\sqrt{d} \in \mathbb{Q}$, et donc qu'il existe $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $\sqrt{d} = \dfrac{p}{q}$.

On a alors $p^2 = dq^2$, et donc $2v_s(p) = v_s(p^2) = 2v_s(p) = v_s(d) + v_s(q^2) = v_s(d) + 2v_s(q)$.
Ainsi $v_s(d) = 2(v_p(s) - v_q(s))$. Donc $v_s(d)$ est pair.
On a une contradiction. avec la question précédente. /2

$$\boxed{\sqrt{d} \text{ est irrationnel}}$$

(b) L'existence est donnée par la définition de A_d. Il faut et il suffit de démontrer l'unicité.
Soit $z = a + \sqrt{d}b = a' + \sqrt{d}b' \in A_d$ $(a, b, a', b' \in \mathbb{Z})$.
On a alors $(b - b')\sqrt{d} = a' - a$.
Si $b - b' \neq 0$, alors $\sqrt{d}$ s'écrirait sous forme d'une fraction. Impossible.
Donc $b - b'$ i.e. $b = b'$ et $a' - a = 0$ i.e. $a = a'$.
L'écriture est unique. /1,5

$$\boxed{\text{Pour tout } z \in A_d \text{ il existe un unique couple } (a,b) \in \mathbb{Z}^2 \text{ tel que } z = a + \sqrt{d}b.}$$

2. Structure algébrique de A_d.

(a) Pour tout $a, b \in \mathbb{Z}$, $a + \sqrt{d}b \in \mathbb{R}$, donc $A_d \subset \mathbb{R}$.
Et $1_{\mathbb{R}} = 1_{\mathbb{Z}} + \sqrt{d} \times 0_{\mathbb{Z}} \in A_d$. /0,5

$$\boxed{A_d \subset \mathbb{R} \qquad \text{et} \qquad 1 \in A_d}$$

(b) Notons $z_1 = a_1 + \sqrt{d}b_1$ et $z_2 = a_2 + \sqrt{d}b_2$.
Alors $z_1 - z_2 = (a_1 - a_2) + \sqrt{d}(b_1 - b_2) \in A_d$ /1

$$\boxed{\text{Pour tout } z_1, z_2 \in A_d,\ z_1 - z_2 \in A_d.}$$

(c) Notons $z_1 = a_1 + \sqrt{d}b_1$ et $z_2 = a_2 + \sqrt{d}b_2$.
Alors $z_1 \times z_2 = (a_1a_2 + db_1b_2) + \sqrt{d}(a_1b_2 + a_2b_1) \in A_d$ /1

$$\boxed{\text{Pour tout } z_1, z_2 \in A_d,\ z_1 \times z_2 \in A_d.}$$

(d) On a démontré que A_d est un sous-anneau de $\mathbb{R}$. /1

$$\boxed{A_d \text{ est un anneau.}}$$

3. Morphisme c_d.
On note pour tout $z = a + \sqrt{n}b \in A_d$, $c_d(z) = a - \sqrt{n}b$ et $N_d(z) = z \times c(z)$.

(a) Clairement, /0,5

$$\boxed{\text{pour tout } z \in A_d,\ c_d(z) \in A_d \text{ et } c_d(1) = 1.}$$

(b) Notons $z_1 = a_1 + \sqrt{d}b_1$ et $z_2 = a_2 + \sqrt{d}b_2$.

$c_d(z_1+z_2) = c_d\big((a_1+a_2)+\sqrt{d}(b_1+b_2)\big) = (a_1+a_2)-\sqrt{d}(b_1+b_2) = (a_1-\sqrt{d}b_1)+(a_2-\sqrt{d}b_2) = c_d(z_1)+c_d(z_2)$

Et par ailleurs :

$$c_d(z_1 \times z_2) = c_d\big((a_1a_2 + db_1b_2) + \sqrt{d}(a_1b_2 + a_2b_1)\big) = (a_1a_2 + db_1b_2) - \sqrt{d}(a_1b_2 + a_2b_1)$$

alors que

$$c_d(z_1) \times c_d(z_2) = (a_1 - \sqrt{d}b_1) \times (a_2 - \sqrt{d}b_2) = (a_1a_2 + db_1b_2) - \sqrt{d}(a_1b_2 + a_2b_1)$$

Pour tout $z_1, z_2 \in A$, $c_d(z_1 + z_2) = c_d(z_1) + c_d(z_2)$ et $c_d(z_1 \times c_2) = c_d(z_1) \times c_d(z_2)$.

/1,5

c_d est un morphisme d'anneaux $(A_d, +, \times)$ sur $(A_d, +, \times)$.

(c) Soit $z = a + \sqrt{d}b \in A_d$.

$$N_d(z) = z \times c_d(z) = ((a)(a) + d(b)(-b)) + \sqrt{d}((a)(-b) + (a)(b)) = a^2 - db^2 \in \mathbb{Z}$$

/1

Pour tout $z \in A_d$, $N_d(z) \in \mathbb{Z}$.

(d) Soient $z_1, z_2 \in A_d$.

$$\begin{array}{lll} N_d(z_1z_2) & = (z_1z_2)c_d(z_1z_2) = z_1 \times z_2 \times c(z_1) \times c(z_2) & \text{Morphisme } c_d \\ & = z_1c_d(z_1) \times z_2c_d(z_2) & \text{Commutativé de } \mathbb{R} \\ & = N_d(c_1) \times N_d(z_2) & \end{array}$$

/1

$\forall\ z_1, z_2 \in A_d$, $N_d(z_1 \times z_2) = N_d(z_1)N_d(z_2)$

4. Inverses de A_d.

(a) Supposons que z admet un inverse $z' \in A_d$, alors $z \times z' = 1$.

$$N_d(1) = 1 = N_d(z \times z') = N_d(z) \times N_d(z')$$

Or $N_d(z), N_d(z') \in \mathbb{Z}$, donc $N_d(z)$ est inversible dans $\mathbb{Z}$.
Ainsi $N_d(z) \in \mathbb{Z}^\times = \{-1, 1\}$ /2

Si z admet un inverse $z' \in A_d$, alors $N_d(z) = 1$ ou $N_d(z) = -1$.

(b) Supposons que $|N_d(z)| = 1$.
On a donc $N_d(z) = z \times c_d(z) \in \{-1, 1\}$.
• Si $N_d(z) = 1$, alors z est inversible d'inverse $c_d(z)$.
• Si $N_d(z) = -1$, alors z est inversible d'inverse $-c_d(z)$. /2

Si $|N_d(z)| = 1$, alors z est inversible et $z^{-1} = N_d(z) \times c_d(z)$.

Remarques !
On a démontré que z est inversible dans l'anneau $\mathbb{Z}[\sqrt{d}]$ si et seulement si $N_d(z) = \pm 1$

Partie C - Cas particulier $n = 2$

On considère ici $A_2 = \mathbb{Z} + \sqrt{2}\mathbb{Z} = \{z \in \mathbb{R} \mid \exists\ (a, b) \in \mathbb{Z}^2, z = a + \sqrt{2}b\}$.
On rappelle que $a + \sqrt{2}b$ est inversible dans A_2 ssi $N_2(z) = \pm 1$, ie ssi $|a^2 - 2b^2| = 1$

1. On cherche à résoudre ici l'équation de Pell-Fermat pour $d = 2$ et m quelconque.
On considère alors l'ensemble $I = \{m \in \mathbb{Z} \mid \exists\ (a, b) \in \mathbb{Z}^2, m = a^2 - 2b^2\}$.

(a) Soient $m_1, m_2 \in I$.
Alors il existe $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ tels que $m_1 = a_1^2 - 2b_1^2 = N_2(z_1)$ et $m_2 = a_2^2 - 2b_2^2 = N_2(z_2)$.
Alors d'après A.3.(d) :

$$m_1m_2 = N_2(z_1) \times N_2(z_2) = N_2(z_1 \times z_2) = (a_1a_2 + b_1b_2)^2 - 2(a_1b_2 - a_2b_1)^2$$

Comme $a_1a_2 + b_1b_2 \in \mathbb{Z}$ et $a_1b_2 - a_2b_1 \in \mathbb{Z}$, alors $m_1m_2 \in I$ /1,5

Donc I est stable par produit.

(b) Les nombres modulo 8 se résument à leurs représentant pris entre 0 et 7, on élève au carré : /2

a	0	1	2	3	4	$5(=-3)$	$6(=-2)$	$7(=-1)$
a^2	0	1	4	$9=1$	0	1	4	1

(c) Les valeurs prises par a^2, modulo 8 sont réduites à $0, 1, 4$.
On a alors pour $a^2 - 2b^2$, au plus 9 valeurs possibles $x - 2y$ avec $x, y \in \{0, 1, 4\}$.

$$a^2 - 2b^2 = m \equiv K[8] \text{ avec } K \in \{0, -2 = 6, -8 = 0, 1, -1 = 7, 1, 4, 2, 4\} = \{0, 1, 2, 4, 6, 7\}$$

Donc, nécessairement 3 n'appartient pas à I.

/2

Plus généralement, $\{(a^2 - 2b^2)\%8; a, b \in \mathbb{Z}\} = \{0, 1, 2, 4, 6, 7\}$.

2. Densité de A_2 dans $\mathbb{R}$.

(a) Soit $p \in \mathbb{Z}$, alors $p = p + 0\sqrt{2} \in A_2$. Et $(\sqrt{2} - 1) \in A_2$.
Par récurrence, comme A_2 est stable par produit, $(\sqrt{2} - 1)^n \in A_2$.
Et à nouveau par stabilité par produit : $p(\sqrt{2} - 1)^n \in A_2$ /1

Pour tout $p \in \mathbb{Z}$, et pour tout $n \in \mathbb{N}$, $p(\sqrt{2} - 1)^n \in A_2$.

(b) Soit $x < y$, deux éléments de $\mathbb{R}$.
On va montrer qu'il existe $(p, n) \in \mathbb{Z} \times \mathbb{N}$ tel que $x < p(\sqrt{2} - 1)^n < y$.
En effet :

$$x < p(\sqrt{2} - 1)^n < y \iff \frac{x}{(\sqrt{2} - 1)^n} < p < \frac{y}{(\sqrt{2} - 1)^n}$$

Or $\sqrt{2} - 1 \in [0, 1[$, donc la suite géométrique $(\sqrt{2} - 1)^n \longrightarrow 0$.
Prenons $\epsilon = y - x$.
Il existe $N \in \mathbb{N}$ tel que $\forall\ n \in \mathbb{N}$, $0 < (\sqrt{2} - 1)^n < \epsilon$., Donc

$$0 < (\sqrt{2}-1)^N < y-x \Longrightarrow 0 < 1 < \frac{y}{(\sqrt{2} - 1)^N} - \frac{x}{(\sqrt{2} - 1)^N} \Longrightarrow \frac{x}{(\sqrt{2} - 1)^N} + 1 < \frac{y}{(\sqrt{2} - 1)^N}$$

Notons $p = \left\lfloor \frac{x}{(\sqrt{2} - 1)^N} \right\rfloor + 1$, on a donc

$$\left\lfloor \frac{x}{(\sqrt{2} - 1)^N} \right\rfloor \leqslant \frac{x}{(\sqrt{2} - 1)^N} < \underbrace{\left\lfloor \frac{x}{(\sqrt{2} - 1)^N} \right\rfloor + 1}_{=p} \leqslant \frac{x}{(\sqrt{2} - 1)^N} + 1 < \frac{y}{(\sqrt{2} - 1)^N}$$

Donc

$$\frac{x}{(\sqrt{2} - 1)^n} < p < \frac{y}{(\sqrt{2} - 1)^n}$$

Ainsi, pour tout $x < y \in \mathbb{R}$, il existe $z(= p(\sqrt{2} - 1)^N) \in A_2$ tel que $x < z < y$. /2,5

A_2 est dense dans $\mathbb{R}$.

On également $\mathcal{H} = \{(x, y) \in \mathbb{R}^2 \mid |x^2 - 2y^2| = 1\}$.
Géométriquement, il s'agit d'une réunion de deux hyperboles de $\mathbb{R}^2$.

3. On note $\omega = 1 + \sqrt{2}$, un élément particulier de A_2.

(a) Plusieurs stratégies, par récurrence ou binôme de Newton.
Soit $n \in \mathbb{N}$. On note $P = \{k \in [\![0, n]\!] \mid k \text{ pair}\}$ et $I = \{k \in [\![0, n]\!] \mid k \text{ impair}\}$.
Comme $P \uplus I = [\![0, n]\!]$:

$$\begin{aligned}(1 + \sqrt{2})^n &= \sum_{k=0}^{n} \binom{n}{k} \sqrt{2}^k = \sum_{k \in P} \binom{n}{k} \sqrt{2}^k + \sum_{k \in I} \binom{n}{k} \sqrt{2}^k \\ &= \underbrace{\sum_{k \in P} \binom{n}{k} 2^{k/2}}_{\in \mathbb{N}} + \sqrt{2} \underbrace{\sum_{k \in I} \binom{n}{k} 2^{(k-1)/2}}_{\in \mathbb{N}} \in A_2\end{aligned}$$

Ce qui assure l'existence de a_n, b_n. L'unicité est donnée par la réponse à la question A.1.(b). /2

Pour tout $n \in \mathbb{N}$, il existe un unique couple noté $(a_n, b_n) \in \mathbb{N}^2$ tel que $\omega^n = a_n + \sqrt{2} b_n$.

(b) Notons d'abord l'équivalence :

$$(a,b) \in \mathcal{H} \iff |a^2 - 2b^2| = 1 \iff |N_2(a + \sqrt{2}b)| = 1$$

Démontrons le par récurrence. Posons $\mathcal{P}_n$: « $(a_n, b_n) \in \mathcal{H}$ ».
— $a_0 + \sqrt{2}b_0 = \omega^0 = 1$, donc $a_0 = 1$ et $b_0 = 0$.
Donc $|a_0^2 - 2b_0^2| = |1| = 1$. Donc $(a_0, b_0 \in \mathcal{H}$. Et $\mathcal{P}_0$ est vraie.
— Soit $n \in \mathbb{N}$. Supposons que $\mathcal{P}_n$ est vraie.

$$(a_{n+1}, b_{n+1}) \in \mathcal{H} \iff |N_2(a_{n+1} + \sqrt{2}b_{n+1})| = 1 \iff |N_2(\omega^{n+1})| = 1$$

Or, on a vu par morphisme :

$$N_2(\omega^{n+1}) = N_2(\omega^n \times \omega) = N_2(\omega^n)N_2(\omega)$$

Et $N_2(\omega) = 1^2 - 2(1)^2 = 1 - 2 = -1$ et $|N_2(\omega^n)| = 1$ d'après $\mathcal{P}_n$.
Donc

$$\left|N_2(\omega^{n+1})\right| = |(-1)| \times |N_2(\omega)| = 1$$

Donc $\mathcal{P}_{n+1}$ est vraie. /2

$$\boxed{\text{Pour tout } n \in \mathbb{N},\ (a_n, b_n) \in \mathcal{H}.}$$

(c) On considère l'application $\varphi : \mathbb{Z}^2 \to \mathbb{Z}^2$, $(x,y) \mapsto (x + 2y, x + y)$.
• φ est bien à valeurs dans $\mathbb{Z}^2$.
• $\varphi(x,y) = \varphi(x',y') \iff \left\{ \begin{array}{rcl} x+2y & = & x'+2y' \\ x+y & = & x'+y' \end{array} \right. \iff \left\{ \begin{array}{l|r} x = x' & -L_1 + 2L_2 \\ y = y' & L_1 - L_2 \end{array} \right.$
Donc φ est injective.
• $\forall\ a, b \in \mathbb{Z}$, $\varphi(x,y) = (a,b) \iff \left\{ \begin{array}{rcl} x+2y & = & a \\ x+y & = & b \end{array} \right. \iff \left\{ \begin{array}{rcl|r} x = & & 2b-a & -L_1 + 2L_2 \\ y = & & a-b & L_1 - L_2 \end{array} \right.$
Donc φ est surjective ($\exists\ (x,y) \in \mathbb{Z}^2 \mid \varphi(x,y) = (a,b)$). /2

$$\boxed{\varphi \text{ est bijective et } \varphi^{-1} : \mathbb{Z} \to \mathbb{Z},\ (a,b) \mapsto (2b - a, a - b).}$$

Remarques !
On aurait pu craindre que $x, y \in \mathbb{Q}$, s'il avait fallut diviser par 2 par exemple lors de la résolution du système...

(d) Par unicité d'écriture, nous pourrons identifier : /1

$$a_{n+1} + \sqrt{2}b_{n+1} = \omega^{n+1} = (a_n + \sqrt{2}b_n)(1 + \sqrt{2}) = (a_n + 2b_n) + \sqrt{2}(a_n + b_n)$$

$$\boxed{\text{Donc pour tout } n \in \mathbb{N},\ (a_{n+1}, b_{n+1}) = (a_n + 2b_n, a_n + b_n) = \varphi((a_n, b_n)).}$$

(e) On a déjà vu que $\omega^n = a_n + \sqrt{2}b_n$ vérifie :
• $1 = |N_2(\omega^n)| = a_n^2 - 2b_n^2$
• Et par récurrence : $a_n, b_n \in \mathbb{N}$.
En effet : si $x, y \in \mathbb{N}$, alors $\varphi(x,y) = (x + 2y, x + y) \in \mathbb{N}^2$.
Donc $(a_{n+1}, b_{n+1}) = \varphi(a_n, b_n) \in \mathbb{N}^2$.
Donc on a l'inclusion /1

$$\boxed{\{\omega^n, n \in \mathbb{N}\} \subset \{(a + \sqrt{2}b \text{ tel que } |a^2 - 2b^2| = 1 \ \&\ a, b \in \mathbb{N}\} = \mathcal{H} \cap \mathbb{N}^2}$$

4. Réciproquement, on considère $(x,y) \in \mathbb{N}^2 \cap \mathcal{H}$

(a) On suppose que $(x,y) \neq (1,0)$. Et évidemment $x^2 - 2y^2 = \pm 1$ avec $x, y \in \mathbb{N}$.
• Si $x < y$, alors $0 \leqslant x \leqslant y - 1$ puisque ce sont des nombres entiers naturels,
donc $x^2 \leqslant y^2 - 2y + 1$ et donc $x^2 - 2y^2 \leqslant 1 - 2y - y^2 = 1 - y(2 + y) < 1$ car $y > 0$.
On ne peut donc pas avoir $x^2 - 2y^2 = 1$, donc $x^2 - 2y^2 = -1$.
Et pourtant $-1 = x^2 - 2y^2 \leqslant 1 - 2y - y^2$, donc $(y+1)^2 - 3 = y^2 + 2y - 2 \leqslant 0$.
On trouve donc $(y+1)^2 \leqslant 3$.
Mais $y - 1 \geqslant 0$, donc $y + 1 \geqslant 2$ et $(y+1)^2 \geqslant 4$. Contradiction.
Donc on ne peut pas avoir $x < y$, i.e. $y \leqslant x$. /1
• Si $x \geqslant 2y \geqslant 0$, alors $x^2 \geqslant 4y^2 (\geqslant 0)$ alors $x^2 - 2y^2 \geqslant 2y^2 \geqslant 0$.
Or $x^2 - 2y^2 = \pm 1$. Nécessairement, cela ne peut être -1, donc $x^2 - 2y^2 = 1 \geqslant 2y^2$.

Comme $y \in \mathbb{N}$, il y a une seule possibilité : $y = 0$ et donc $x = 1$.
Or par hypothèse, $(x, y) \neq (1, 0)$. Ainsi nécessairement : $x < 2y$. /1

$$\boxed{\text{Nécessairement : } 0 \leqslant y \leqslant x < 2y.}$$

On a donc $2y - x > 0$ et $x - y \geqslant 0$, donc $(2y - x, x - y) \in (\mathbb{Z} \cap \mathbb{R}_+)^2 = \mathbb{N}^2$.
Et par ailleurs, $(2y - x)^2 - 2(x - y)^2 = 4y^2 - 4yx + x^2 - 2x^2 + 4xy - 2y^2 = -(x^2 - 2y^2)$
Or $(x, y) \in \mathcal{H}$, donc $|x^2 - 2y^2| = 1$ et donc $|(2y - x)^2 - 2(x - y)^2| = 1$.
Donc $(2y - x, x - y) \in \mathcal{H}$. /1

$$\boxed{\text{Si } (x, y) \in \mathbb{N} \cap \mathcal{H} \text{ avec } (x, y) \neq (1, 0), \text{ alors } (2y - x, x - y) \in \mathbb{N}^2 \cap \mathcal{H}.}$$

(b) On définit la suite $((x_n), (y_n))_{n\in\mathbb{N}}$ par $\begin{cases} (x_0, y_0) = (a, b) \\ \forall\ n \in \mathbb{N},\ (x_{n+1}, y_{n+1}) = (2y_n - x_n, x_n - y_n) \end{cases}$.
Pour tout $n \in \mathbb{N}$, si $(x_n, y_n) \neq (1, 0)$: $y_{n+1} = x_n - y_n < y_n$ car $x_n < 2y_n$.
Donc la suite $(y_n)_n$ est une suite d'entiers strictement décroissantes,
elle s'annule donc à partir d'un certain rang $n(< b)$.
On a alors $x_n^2 - 2y_n^2 = \pm 1$, donc une seule possibilité : $x_n = 1$ $(x_n > 0)$. /2

$$\boxed{\text{Donc il existe } n \in \mathbb{N} \text{ tel que } (x_n, y_n) = (1, 0).}$$

(c) On peut faire une récurrence ou trouver un invariant.

Piste de recherche...
On a alors $(1, 0) = (x_n, y_n) = (\varphi^{-1} \circ \cdots \circ \varphi^{-1})(x_0, y_0)$.
Et donc $(a, b) = (x_0, y_0) = (\varphi \circ \cdots \circ \varphi)(1, 0)$ *(en composant* n *fois par* φ*).*

Notons, pour tout $k \leqslant n$, $\mathcal{P}_k$: « $\omega^k = x_{n-k} + \sqrt{2}y_{n-k}$ »
— $\omega^0 = 1 = x_n + \sqrt{2}y_n$. Donc $\mathcal{P}_0$ est vraie.
— Soit $k \leqslant n - 1$. Supposons que $\mathcal{P}_k$ est vraie.
Alors $\omega^k = x_{n-k} + \sqrt{2}y_{n-k}$. Puis par définition de la suite (x_n, y_n),

$$(x_{n-k}, y_{n-k}) = \varphi^{-1}(x_{n-k-1}, y_{n-k-1}) \Longleftrightarrow (x_{n-(k+1)}, y_{n-(k+1)}) = \varphi(x_{n-k}, y_{n-k})$$

Donc

$$x_{n-(k+1)} + \sqrt{2}y_{n-(k+1)} = \omega \times \omega^k = \omega^{k+1}$$

Donc $\mathcal{P}_{k+1}$ est vraie.
La récurrence est démontré, et en particulier pour $k = n$: /2

$$a + \sqrt{2}b = x_0 + \sqrt{2}y_0 = w^n$$

Ainsi, pour tout $(a, b) \in \mathbb{N}^2 \cap \mathcal{H}$, i.e. $|a^2 - 2b^2| = 1$ et $a, b \in \mathbb{N}$,
il existe $n \in \mathbb{N}$ tel que $\pi(a, b) = a + \sqrt{2}b = \omega^n = a_n\sqrt{2}b_n$ avec les notations de 3.
Et par unicité d'écriture dans A_2, on a $(a, b) = (a_n, b_n)$. /1

$$\boxed{\text{Les } (x, y) \in \mathbb{N}^2 \text{ vérifiant l'équation } |x^2 - 2y^2| = 1 \text{ sont les couples } (a_n, b_n) \text{ avec } n \in \mathbb{N}.}$$

(d) On a donc l'inclusion : $\{(a, b) \mid |a^2 - 2b^2| = 1, a, b \in \mathbb{N}\} \subset \{(a_n, b_n), n \in \mathbb{N}\}$.
Si l'on applique π :

$$\pi(\mathbb{N}^2 \cap \mathcal{H}) = \{a + \sqrt{2}b \text{ tel que } |a^2 - 2b^2| = 1 \& a, b \in \mathbb{N}\} \subset \{\omega^n, n \in \mathbb{N}\}$$

Avec l'inclusion réciproque montrée en 3.(e), on peut affirmer : /2

$$\boxed{\pi\left(\{\mathbb{N}^2 \cap \mathcal{H}\}\right) = \{\omega^n; n \in \mathbb{N}\}}$$

5. On cherche une approximation du nombre de solutions $(a, b) \in \mathbb{Z}^2$ tel que $|a^2 - 2b^2| = 1$, ou plutôt une certaine fréquence.
On note $R_k = \{(a, b) \in \mathbb{Z}^2 \text{ tel que } |a^2 - 2b^2| = 1 \ \&|a| \leqslant k, |b| \leqslant k\}$
et $R_k^+ = \{(a, b) \in \mathbb{N}^2 \text{ tel que } |a^2 - 2b^2| = 1 \ \& a \leqslant k, b \leqslant k\}$.

(a) On note $R_k^{+,-} = R_k \cap (\mathbb{N}\times\mathbb{Z}^-) = \{(a,b) \in \mathbb{Z}^2 \text{ tel que } |a^2-2b^2| = 1 \;\&0 \leqslant a \leqslant k, -k \leqslant b \leqslant 0\}$.
De même, on définit $R_k^{-,-}$ et $R_k^{-,+}$.
On considère $\theta_{+,-} : R_k^+ \to R_k^{+,-}$, $(a,b) \mapsto (a,-b)$.
Clairement si $(a,b) \in \mathbb{R}_k^+$, alors $0 \leqslant a \leqslant k$, $-k \leqslant -b \leqslant 0$ et $|a^2-2(-b^2)| = |a^2-2b^2| = 1$.
Donc θ est bien à valeurs dans $R_k^{+,-}$.
θ est bijective, l'application réciproque est $(c,d) \mapsto (c,-d)$.
Donc $\text{card}(R_k^+) = \text{card}(R_k^{+,-})$.
Et de même : $\text{card}(R_k^+) = \text{card}(R_k^{-,-}) = \text{card}(R_k^{-,+})$.
Malheureusement, on n'a pas $R_k = R_k^+ \uplus R_k^{+,-} \uplus R_k^{-,-} \uplus R_k^{-,+}$
Car les ensembles ne sont pas disjoints.
En effet : $R_k^+ \cap R_k^{+,-} = \{(a,b) \mid a^2-2b^1 = \pm 1, a \in \mathbb{N} \& b = 0\} = \{(1,0)\}$
et $R_k^{-,+} \cap R_k^{-,-} = \{(a,b) \mid a^2-2b^1 = \pm 1, a \leqslant 0 \& b = 0\} = \{(-1,0)\}$.
Les autres intersections sont vides (aucune solution avec $a = 0$). /2

$$\boxed{\text{card}(R_k) = \text{card}(R_k^+) + \text{card}(R_k^{+,-}) + \text{card}(R_k^{-,-}) + \text{card}(R_k^{-,+}) - 2 = 4 \times \text{card}(R_k^+) - 2}$$

(b) On reprend la notation de 3.(a).
$(a_0 + \sqrt{2}b_0) = \omega^0 = 1$. Par unicité d'écriture : $a_0 = 1$ et $b_0 = 0$.
$(a_1 + \sqrt{2}b_1) = \omega^1 = 1+\sqrt{2}$. Par unicité d'écriture : $a_0 = 1$ et $b_0 = 1$.
On sait que pour tout $n \in \mathbb{N}$: $(a_{n+1}, b_{n+1}) = \varphi(a_n, b_n) = (a_n + 2b_n, a_n + b_n)$. /1

$$\boxed{\text{les suites } (a_n) \text{ et } (b_n) \text{ sont les mêmes suites que celles définies en partie } A.}$$

(c) Puisque $\text{card}(R_k^+) = r_k$ (défini en A), on trouve donc

$$\frac{\text{card}(R_k)}{(2k+1)^2} = \frac{4r_k - 2}{(2k+1)^2} = \frac{4(k+1)^2 s_k - 2}{(2k+1)^2} \sim 4\left(\frac{k+1}{2k+1}\right)^2 s_k$$

car $\frac{2}{(2k+1)^2} \to 0$.
En reprenant la dernière réponse de la partie A, ainsi que le fait que $\left(\frac{k+1}{2k+1}\right)^2 \to 4$ /2

$$\boxed{\frac{\text{card}(R_k)}{(2k+1)^2} \sim s_k \sim \frac{1}{\ln(1+\sqrt{2})}\frac{\ln k}{k^2}}$$

Partie Partie D - Générateur de A_d

On considère de nouveau d, un entier naturel non carré quelconque.

1. (a) $\sqrt{d} > 1$ n'est pas rationnel. On note $N = \lfloor \sqrt{d} \rfloor$. Donc $N < \sqrt{d} < N+1$ ($\sqrt{d}$ est irrationnel).
Soit $D = \mathbb{Q} \cap]N, N+1[$. D est infini (il possède tous les $\frac{aN+b(N+1)}{a+b}$ avec $a,b \in \mathbb{N}$).
Soit $\frac{x}{y} \in D$ avec $y > 1$, nécessairement (sinon $y = 1$, $\frac{x}{y} \in \mathbb{N}\ldots$).
On a donc $N^2 < \frac{x^2}{y^2} < (N+1)^2$ et de même $N^2 < d < (N+1)^2$.
Donc comme $y^2 > 0$: $\quad N^2y^2 < x^2 < (N+1)^2y^2$ et $N^2y^2 < dy^2 < (N+1)^2y^2$.
Donc $[N^2 - (N+1)^2]y^2 < x^2 - dy^2 < [(N+1)^2 - N^2]y^2$
Et par conséquent $|x^2 - dy^2| < (2N+1)y^2$.
Or $y^2 > 1$, donc $|x^2 - dy^2| < 2N + 1 < 2\sqrt{d} + 1$ car $N < \sqrt{d}$. /2

$$\boxed{\text{Il existe une infinité de couples } (x,y) \in \mathbb{N}^2 \text{ tels que } 0 < |x^2 - dy^2| \leqslant 1 + 2\sqrt{d}.}$$

(Au moins tous les couples obtenus à partir de l'ensemble D).

(b) Notons $F := \{(x,y) \mid |x^2 - dy^2| < 1 + \sqrt{d}\}$. Nous savons que F est infini.
Pour simplifier les expressions, notons $M_d = \lfloor 1 + \sqrt{d} \rfloor$.
Soit $\Phi : F \to \mathbb{R}$, par construction $\Phi(F) \subset \mathbb{Z} \cap [-M_d - 1, M_d + 1]$.
Donc $\Phi(F)$ est fini, il est inclus dans $\{-M_d, \ldots 0, 1, \ldots M_d\rfloor\}$.
Considérons $\overline{\Phi} : F \to [\![-M, M]\!] \times [\![0, M_d]\!]^2$, $(x,y) \mapsto \big(x^2 - dy^2, x\%(x^2-dy^2), y\%(x^2-dy^2)\big)$
(où $a\%b$ est le reste dans la division euclidienne de a par b).
Alors $\overline{\Phi}$ a pour image un ensemble fini, donc elle n'est nécessairement pas injective.
Ainsi, il existe (x,y) et $(x',y') \in F$ tel que $\overline{\Phi}(x,y) = \overline{\Phi}(x',y')$.
En notant $k = \Phi(x,y)$, on a . /3

$$\boxed{x^2 - dy^2 = (x')^2 - d(y')^2 = k \qquad x \equiv x' \equiv x\%p[p] \qquad y \equiv y' \equiv y\%p[p]}$$

(c) Le calcul donne

$$(x' - \sqrt{d}y')(x + \sqrt{d}y) = \overbrace{(xx' - dyy')}^{=:\, a\in\mathbb{Z}} + \sqrt{d}\overbrace{(-xy' + x'y)}^{=:\, b\in\mathbb{Z}} = a + \sqrt{d}b$$

Alors

$$(x' + \sqrt{d}y')(x - \sqrt{d}y) = \overbrace{(xx' - dyy')}^{=a\in\mathbb{Z}} - \sqrt{d}\overbrace{(-xy' + x'y)}^{=b\in\mathbb{Z}} = a - \sqrt{d}b$$

Enfin, en multipliant ces deux nombres :

$$\begin{aligned} k^2 &= k \times k = (x^2 - dy^2)((x')^2 - d(y')^2) = (x + \sqrt{d}y)(x - \sqrt{d}y)(x' + \sqrt{d}y')(x' - \sqrt{d}y') \\ &= (x' - \sqrt{d}y')(x + \sqrt{d}y)(x' + \sqrt{d}y')(x - \sqrt{d}y) = (x^2 - dy^2)((x')^2 - d(y')^2) = a^2 - db^2 \end{aligned}$$

Donc $k^2 = a^2 - db^2$.
Mais par ailleurs, en notant $x' = x + kr$ et $y' = y + ks$:

$$u = (x + kr)x - d(y + ks)y = x^2 - dy^2 + k(rx + sy) = k(rx + sy + 1)$$

$$v = (x + kr)y - (y + ks)x = k(ry - sx)$$

Et ainsi

$$k^2 = a^2 - db^2 = k^2\left[(rx + sy + 1)^2 - d(ry - sx)\right]$$

. /3

Donc avec $u = rx + sy + 1$ et $v = ry - sx$, on trouve $u^2 - dv^2 = 1$.

2. On note $A_d = \{x + \sqrt{d}y \in \mathbb{R} \mid x, y \in \mathbb{Z} \text{ et } x^2 - dy^2 = 1\}$.

(a) On pose $G = A_d \cap \mathbb{R}_+^*$.

- Soient $z_1 = x_1 + \sqrt{d}y_1$,$z_2 = x_2 + \sqrt{d}y_2 \in G$. $z_1 > 0, z_2 > 0 \Longrightarrow z_1 z_2 > 0 \Longrightarrow z_1 z_2 \in \mathbb{R}_+^*$ et $z_1 \times z_2 \in A_d$ d'après A.2.(c). Donc $z_1 z_2 \in G$.
- $\frac{1}{z_1} > 0 \Longrightarrow \frac{1}{z_1} \in \mathbb{R}_+^*$.
  Et d'après A.4., comme $N_d(z_1) = 1$, alors z_1 est inversible dans A_d, i.e. $\frac{1}{z_1} \in .A_d$.
  Donc $\frac{1}{z_1} \in G$.. /1,5

G est stable par produit et par passage à l'inverse.

(b) Soit $z = x + \sqrt{d}y \in G$, alors $\frac{1}{z} = x - \sqrt{d}y \in G$.
Supposons que $z > 1$, alors $\frac{1}{z} < 1$.
On trouve donc $x + \sqrt{d}y > 1 > x - \sqrt{d}y$, donc $y > 0$ donc $y \geqslant 1$.
Puis $\frac{1}{z} = x - \sqrt{d}y > 0$, donc $x > \sqrt{d}y > 0$ donc $x \geqslant 1$.
Ainsi $x + \sqrt{d}y \geqslant 1 + 1\sqrt{d}$. /2

Tout élément $z \in G$ qui est strictement supérieur à 1 est supérieur ou égal à $1 + \sqrt{d}$.

(c) On note $H = G \cap]1, +\infty[$.
$H \subset \mathbb{R}_+^*$, H est non vide,
car G est non vide et si $z \in G$, alors z ou $\frac{1}{z} \in H$.
H est minoré par 1.
Donc H admet une borne inférieure notée $\omega \geqslant 1$.
Alors, pour tout $\epsilon > 0$, il existe $z \in H$ tel que $\omega \leqslant z < \omega + \epsilon$.
Si il existe $z_1, z_2 \in H$ tel que $\omega \leqslant z_1 < z_2 < \omega + \epsilon$,
alors $\frac{z_2}{z_1} > 1$, et par stabilité de A_d, $\frac{z_2}{z_1} \in A_d$.
Donc d'après la question précédente : $\frac{z_2}{z_1} \geqslant 1 + \sqrt{d}$, donc $z_2 - z_1 \geqslant \sqrt{d}z_1 > \sqrt{d}$ $(z_1 > 1)$.
Avec $\epsilon = \frac{\sqrt{d}}{2} > 0$, nous avons une contradiction :

$$\epsilon < \sqrt{d} \leqslant z_2 - z_1 \leqslant (\omega + \epsilon) - \omega = \epsilon$$

. /2

Donc $H \cap [\omega, \omega + \frac{\sqrt{d}}{2}]$ ne contient qu'un seul élément.

Sa borne inférieure est donc égale à cet élément qui est minimal. . /0,5

Donc $\omega \in H$.

(d) Notons, que par stabilité de G, pour tout $k \in \mathbb{N}$, $\omega^k \in G$.
Puis comme $\omega > 1$, alors $\omega^k > 1$, également donc $\{\omega^n, n \in \mathbb{N}\} \subset H$.
Et de même comme $\{\omega^n, n \in \mathbb{Z}\}$ est un groupe : . /1,5

$$\boxed{\{\omega^n, n \in \mathbb{Z}\} \subset G}$$

(e) Réciproquement. Soit $z \in G$, alors $z > 0$.
Soit $k = \left\lfloor \dfrac{\ln z}{\ln \omega} \right\rfloor$.
Alors $k \ln \omega \leqslant \ln z < (k+1) \ln \omega$ donc en composant par exp, croissante :

$$\omega^k \leqslant z < \omega^{k+1}$$

Ainsi comme $\omega^k \in G$, $z \in G$, alors $\dfrac{z}{\omega^k} \in G$ (groupe).
Et également $1 \leqslant \dfrac{z}{\omega^k} < \omega$.
Si $\dfrac{z}{\omega^k} \neq 1$, alors $\dfrac{z}{\omega^k} \in H$, donc $\dfrac{z}{\omega^k} \geqslant \omega$. Absurde.
Donc $\dfrac{z}{\omega^k} = 1$. Donc il existe $k \in \mathbb{Z}$ tel que $z = \omega^k$.
Ainsi $G \subset \{\omega^n; n \in \mathbb{Z}\}$.. /2,5

$$\boxed{\text{Il existe } \omega > 1 \text{ tel que } G \subset \{\omega^n, n \in \mathbb{Z}\} \text{ (égalité).}}$$

Remarques !
En fait on a montré que $\{\ln z, z \in G\}$ est un sous-groupe de $\mathbb{Z}$ donc de la forme $\ln(\omega) \cdot \mathbb{Z}$.
La division euclidienne est ici transformée en expliotation de la fonction partie entière.

(f) Il reste à montrer l'unicté de ω.
Supposons que ω et ω' vérifient les mêmes conditions (engendré G et > 1).
Comme $\omega \in G = \{(\omega')^n; n \in \mathbb{Z}\}$, il existe $n \in \mathbb{Z}$ tel que $(\omega')^n = \omega$.
Comme $\omega' \in G = \{(\omega)^n; n \in \mathbb{Z}\}$, il existe $m \in \mathbb{Z}$ tel que $(\omega)^m = \omega'$.
Donc $\omega^{nm} = (\omega^m)^n = (\omega')^n = \omega$.
Donc $\omega^{nm-1} = 1$, i.e. $(nm-1)\ln \omega = \ln 1 = 0$.
Or $\omega > 1$, donc $\ln(\omega) > 0$ donc $nm - 1 = 0$, donc $m \in \mathbb{Z}^* = \{+1, -1\}$.
Enfin, $\omega^m = \omega' > 1$, donc $m \in \mathbb{N}$. Ainsi, $m = 1$ et $\omega' = \omega$.. /1,5

$$\boxed{\text{Le réel } \omega \in G \in]1, +\infty[\text{ qui engendre } G \text{ est unique (il existe aussi } \omega' = \tfrac{1}{\omega} < 1).}.$$

(g) G est un groupe monogène : $G = <\omega>$.
Par ailleurs, $G = A_d \cap \mathbb{R}_+^*$.
Notons d'abord que $0 \notin A_d$ car $0^2 - d0^2 = 0$.
Si $z \in A_d$ et $z > 0$, alors il existe $n \in Z$ tel $z = \omega^n$.
Si $z \in A_d$ et $z < 0$, alors $-z \in A_d$, car $(-x)^2 - d(-y)^2 = x^2 - dy^2 = 1$ et que $-x, -y \in \mathbb{Z}$.
Ainsi, il existe $n \in \mathbb{Z}$ tel que $-z = \omega^n$, donc $z = -\omega^n$. /2

$$\boxed{A_d = \{\pm\omega^n; n \in \mathbb{Z}\}}$$

3. Applications

(a) Pour $d = 2$, on $\omega = 3 + 2\sqrt{2}$
En effet, $3^2 - 2 \times 2^2 = 9 - 8 = 1$ et il n'a pas de solution pour $a = 0$, $a = 1$ et $a = 2$.
et pour $d = 3$, on $\omega = 2 + \sqrt{3}$
En effet, $2^2 - 3 \times 1^2 = 4 - 3 = 1$ t il n'a pas de solution pour $a = 0$, $a = 1$.. /2

$$\boxed{\omega_2 = 3 + 2\sqrt{2} \text{ et } \omega_3 = 2 + \sqrt{3}}$$

(b) Il s'agit donc des couples issus des puissances de $2 + \sqrt{3}$.
Or si $a_n + \sqrt{3}b_n = \omega^n$ alors

$$a_{n+1} + \sqrt{3}b_{n+1} = \omega^n \times \omega = (2a_n + 3b_n) + \sqrt{3}(a_n + 2b_n)$$

Donc $a_{n+1} = 2a_n + 3b_n$ et $b_{n+1} = a_n + 2b_n$.
Ainsi, on trouve $b_{n+1} - 2b_n = a_n$, donc

$$(a_{n+2} - 2a_{n+1}) - (2a_{n+1} - 4a_n) = 3b_{n+1} - 6b_n = 3a_n$$

$$a_{n+2} - 4a_{n+1} + a_n = 0$$

Et de même : $b_{n+2} - 4b_{n+1} + b_n = 0$, pour tout entier n.
L'équation caractéristique est

$$x^2 - 4x + 1 = (x-2)^2 - 3 = (x - 2 - \sqrt{3})(x - 2 + \sqrt{3}) = 0$$

Il existe $A_1, A_2 \in \mathbb{R}$ tels que pour tout $n \in \mathbb{N}$, $a_n = A_1(2+\sqrt{3})^n + A_2(2-\sqrt{3})^n$.

Comme $\omega^0 = 1$, $\omega = 2 + \sqrt{3}$, alors $a_0 = 1$ et $a_1 = 2$.

On résout le système ce qui donne : $A_1 = A_2 = \frac{1}{2}$, donc $a_n = \dfrac{1}{2}\big((2+\sqrt{3})^n + (2-\sqrt{3})^n\big)$.

Et de même comme $b_0 = 0$ et $b_1 = 1$.

On résout le système, et on trouve $b_n = \dfrac{1}{2\sqrt{3}}\big((2+\sqrt{3})^n - (2-\sqrt{3})^n\big)$.

On admet que le résultat est vrai encore pour $n \in \mathbb{Z}$, pour récupérer les ω^n, $n < 0$!!

On trouve donc le groupe G, engendré par ω, puis on considère les opposées également pour obtenir toutes les solutions. /3

$$\{(x,y) \in \mathbb{Z}^2 \text{ tels que } x^2 - 3y^2 = 1\} = \left\{ \pm \left(\tfrac{1}{2}\big((2+\sqrt{3})^n + (2-\sqrt{3})^n\big); \tfrac{1}{2\sqrt{3}}\big((2+\sqrt{3})^n - (2-\sqrt{3})^n\big) \right); n \in \mathbb{Z} \right\}$$

Remarques !

On pourrait se demander pourquoi on n'a pas les nombres $(x,-y)$ ou $(-x,y)$ lorsque (x,y) est solution.

En fait ils y sont pour $n < 0$, dans ce cas y peut être négatif et on retrouve le nombre $(x,-y)$.

Son opposé y figure nécessairement également.