Théorème. *Soit $d > 1$ un entier sans facteurs carrés, alors il existe un unique $(x_1, y_1) \in \mathbb{N}^{*2}$ tel que les solutions de l'équation*

$$x^2 - dy^2 = 1$$

sont exactement les $(\pm x_n, \pm y_n)$ où $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n$.

Démonstration. Soit $K = \mathbb{Q}(\sqrt{d})$. Comme d n'as pas de facteurs carrés, K est une extension quadratique de $\mathbb{Q}$. Pour tout $a \in K$, on note m_a l'endomorphisme de K donné par la multiplication par a. La matrice de m_a dans la base $(1, \sqrt{d})$ est $\begin{bmatrix} x & dy \\ y & x \end{bmatrix}$ où $a = x + \sqrt{d}y$. On pose $N(a) = \det(m_a) = x^2 - dy^2$ et $t(a) = tr(m_a) = 2x$. Comme $m_a \circ m_b = m_{ab}$ et le déterminant est multiplicatif, alors N est multiplicatif.
Si $a = x+\sqrt{d}y$, on note $\bar{a} = x-\sqrt{d}y (= N(a)/a$ pour $a \neq 0)$; $a \mapsto \bar{a}$ est aussi multiplicatif.
Voici quelques propriétés des objets introduits :
- Si $a \in \mathbb{Z}[\sqrt{d}]$, alors $N(a)$ et $t(a)$ sont dans $\mathbb{Z}$.
- $a^2 - t(a)a + N(a) = 0$ (Polynôme annulateur de m_a).
- $\forall a \in \mathbb{Z}[\sqrt{d}]$, on a $a \in \mathbb{Z}[\sqrt{d}]^*$ si et seulement si $N(a) = \pm 1$.

Existence d'une solution : Selon un lemme classique d'approximation rationnelle, il existe une infinité de couples d'entiers (x, y) tels que $|\frac{x}{y} - \sqrt{d}| \leq \frac{1}{y^2}$. Un tel couple (x, y) vérifie alors $|x^2 - dy^2| \leq |x - \sqrt{d}y|(|x - \sqrt{d}y| + 2\sqrt{d}|y|) \leq 1 + 2\sqrt{d}$. Comme il existe une infinité de tels couples, il existe $k \in \mathbb{N}$ tel que $x^2 - dy^2 = k$ a une infinité de solutions. Soient (x_0, y_0) et (x_1, y_1) deux tels couples congrus modulo k.
Soit $u + \sqrt{d}v = \frac{x_0+\sqrt{d}y_0}{x_1+\sqrt{d}y_1}$. On a $N(u + \sqrt{d}v) = \frac{k}{k} = 1$.
De plus, $\frac{x_0+\sqrt{d}y_0}{x_1+\sqrt{d}y_1} = \frac{x_0x_1-dy_0y_1}{k} + \sqrt{d}\frac{x_1y_0-x_0y_1}{k}$ est bien dans $\mathbb{Z}[\sqrt{d}]$; on a bien une solution, non triviale car $x_0y_1 \neq x_1y_0$ (sinon (x_0, y_0) et (x_1, y_1) sont proportionnels).

Description de l'ensemble des solutions : On définit le morphisme :

$$L : \begin{cases} \mathbb{Z}[\sqrt{d}]^* \to \mathbb{R} \\ a \mapsto \log|a| \end{cases}$$

$Im(L)$ est discret ; en effet, si $R > 0$, $a \in L^{-1}(B_R)$, alors $|a| \leq e^R$ et $|\bar{a}| = |a|^-1 \leq e^R$, donc a est solution de $X^2 - t(a)X \pm 1$ où $t(a) \in \mathbb{Z}$ et $|t(a)| \leq 2e^R$; il y a donc un nombre fini d'éléments dans $L^{-1}(B_R)$.
$\ker(L) = \{\pm 1\}$; en effet, -1 est bien dans $\ker(L)$ et réciproquement, selon les considérations précédentes, $\ker(L)$ est un sous-groupe **fini** de $\mathbb{R}^*$, d'où ce résultat.
$\mathbb{Z}[\sqrt{d}]^*/\ker(L)$ est donc isomorphe à un sous-groupe discret de $\mathbb{R}$, et est donc monogène, non réduit à $\{0\}$ grâce à l'existence d'une solution non triviale ; il existe donc $a_1 \in \mathbb{Z}[\sqrt{d}]^*$ tel que $Im(L) = \mathbb{Z}L(a_1)$ et donc $\mathbb{Z}[\sqrt{d}]^* = \pm a_1^{\mathbb{Z}}$. □

Remarque. *Il y a un lien entre les solutions de l'équation de Pell-Fermat et les approximation diophantienne de $\sqrt{d}$; en effet, si $x^2 - dy^2 = 1$, alors*

$$\begin{aligned} 0 < \frac{x}{y} - \sqrt{d} &= \frac{x - \sqrt{d}y}{y} \\ &= \frac{1}{(x + \sqrt{d}y)y} \\ &= \frac{1}{\left(\frac{x}{y} + \sqrt{d}\right) y^2} \\ &< \frac{1}{2\sqrt{d}y^2} \end{aligned}$$

Réciproquement, si $0 < \frac{x}{y} - \sqrt{d} < \frac{1}{2\sqrt{d}y^2}$, alors

$$\begin{aligned} 0 < x^2 - dy^2 = y^2 \left(\frac{x}{y} - \sqrt{d}\right) \left(\frac{x}{y} + \sqrt{d}\right) &< \frac{1}{2\sqrt{d}} \left(2\sqrt{d} + \frac{1}{\sqrt{d}y^2}\right) \\ &\leq 2 \end{aligned}$$

D'où le résultat.

Référence : Hindry