Sur l'équation de Pell-Fermat

Soit $\omega \in \mathbb{N}^*$ qui n'est pas un carré parfait. On s'intéresse à l'équation de Pell-Fermat (P_ω) :

$$x^2 - \omega y^2 = 1,$$

d'inconnues $x, y \in \mathbb{Z}$, et dont on note $\mathscr{E}_\omega^+$ l'ensemble des solutions. On va montrer que des solutions non triviales existent toujours et préciser la structure des solutions.

1 L'anneau $\mathbb{Z}[\sqrt{\omega}]$

On définit $\mathbb{Z}[\omega] = \left\{a + \sqrt{\omega} b, (a, b) \in \mathbb{Z}^2\right\}$.

1. Montrer que $\mathbb{Z}[\sqrt{\omega}]$ est un sous-anneau de $\mathbb{R}$.
2. Montrer que l'écriture $s = a + \sqrt{\omega} b$, avec $a, b \in \mathbb{Z}$, d'un élément s de $\mathbb{Z}[\sqrt{\omega}]$ est unique.

Si $s \in \mathbb{Z}[\sqrt{\omega}]$ s'écrit $s = a + \sqrt{\omega} b$, on définit sa norme par $N(s) = a^2 - \omega b^2$.

3. Montrer que pour $s, t \in \mathbb{Z}[\sqrt{\omega}]$, on a $N(st) = N(s)N(t)$.
4. Montrer que $s \in \mathbb{Z}[\sqrt{\omega}]$ est inversible ssi $N(s) = \pm 1$.

On note $\mathscr{U}$ le groupe des inversibles de $\mathbb{Z}[\sqrt{\omega}]$ et $\mathscr{E}_\omega^\pm$ l'ensemble des couples $(x, y) \in \mathbb{Z}^2$ tels que $x^2 - \omega y^2 = \pm 1$. On note aussi $\mathscr{U}^+$ le sous-groupe de $\mathscr{U}$ formé des éléments de norme 1. L'application $(x, y) \mapsto x + \sqrt{\omega} y$ définit ainsi une bijection de $\mathscr{E}_\omega^\pm$ dans $\mathscr{U}$; elle induit une bijection de $\mathscr{E}_\omega^+$ dans $\mathscr{U}^+$.

5. Montrer que si $\mathscr{U}$ n'est pas réduit à $\{\pm 1\}$, alors $\mathscr{E}_\omega^+$ est infini.

2 Existence d'une solution non triviale

Dans cette partie, on appliquera plusieurs fois le principe des tiroirs de Dirichlet.

Si E et F sont des ensembles, si F est fini de cardinal n et si E est infini ou fini de cardinal $m > n$, alors une fonction $f : E \to F$ n'est pas injective.

De façon informelle, si on doit répartir dans des tiroirs des paires de chaussettes et qu'il y a strictement plus de paires de chaussettes que de tiroirs, alors un tiroir contiendra au moins deux paires de chaussettes.

6. Soit $n \in \mathbb{N}^*$. En considérant les valeurs $a + \sqrt{\omega} b$ pour $a, b \in [\![0, n]\!]$, montrer qu'il existe deux entiers relatifs A_n et B_n, non tous les deux nuls, tels que
$|A_n| \leq n, |B_n| \leq n$ et $|A_n + \sqrt{\omega} B_n| \leq \dfrac{1}{n}(1 + \sqrt{\omega})$.

7. Montrer que l'ensemble des couples (A_n, B_n), pour $n \in \mathbb{N}^*$, est infini.

8. Montrer que pour tout $n \in \mathbb{N}^*$, $|A_n^2 - \omega B_n^2| \leq (1 + \sqrt{\omega})^2$.

9. En déduire qu'il existe $c \in \mathbb{Z}$ tel que l'équation $x^2 - \omega y^2 = c$ admette une infinité de solutions $(x, y) \in \mathbb{Z}^2$.

10. Montrer qu'on peut trouver deux couples distincts (x, y) et (x', y') dans $\mathbb{N}^* \times \mathbb{Z}$, solutions de l'équation ci-dessus tels que $x \equiv y\,[c]$ et $x' \equiv y'\,[c]$.

11. Avec ces notations, on pose $\eta = x + \sqrt{\omega} y$, $\eta' = x' + \sqrt{\omega} y'$ et $\xi = \dfrac{\eta}{\eta'}$.
Montrer que $\xi \in \mathbb{Z}[\omega] \setminus \{\pm 1\}$ et qu'il est de norme 1.

3 Structure des solutions

On note $\mathscr{A}$ l'ensemble des réels $s = a + \sqrt{\omega} b \in \mathscr{U}^+$ tels que $a \geq 0$ et $s > 1$.

12. Montrer que si $s = a + \sqrt{\omega} b \in \mathscr{A}$, alors $b \geq 1$.

13. Démontrer que $\mathscr{A}$ est non vide et qu'il admet un plus petit élément ε.

14. En utilisant la structure des sous-groupes additifs de $\mathbb{R}$, montrer que $\mathscr{U}^+$ est l'ensemble des réels de la forme $\pm\varepsilon^k$, pour $k \in \mathbb{Z}$. A quel groupe $\mathscr{U}^+$ est-il isomorphe ?

15. **Application.** Déterminer ε pour $\omega = 2, 3, 5$. Déterminer dans chaque cas *les trois premiers* couples, qui sont des solutions non triviales de l'équation de Pell-Fermat.