ÉQUATIONS DE PELL-FERMAT

On appelle *équation de Pell-Fermat* toute équation de la forme $x^2 - dy^2 = 1$ d'inconnue $(x,y) \in \mathbb{Z}^2$ dans laquelle l'entier $d \in \mathbb{N}$ est fixé. On suppose seulement que d N'EST PAS un carré parfait.

On note $\mathbb{Z}\left[\sqrt{d}\right]$ l'ensemble $\left\{a + b\sqrt{d} \mid \quad a,b \in \mathbb{Z}\right\}$.

1) Montrer que $\mathbb{Z}\left[\sqrt{d}\right]$, muni de l'addition et de la multiplication des réels, est un anneau.

2) a) Montrer l'irrationnalité de $\sqrt{d}$.

b) Montrer que pour tout $x \in \mathbb{Z}\left[\sqrt{d}\right]$, il existe un et un seul couple $(a,b) \in \mathbb{Z}^2$ pour lequel $x = a + b\sqrt{d}$.

L'élément $a - b\sqrt{d}$ est appelé le *conjugué de* x et noté $\overline{x}$. Cette définition ne pose aucun problème d'ambiguïté vis-à-vis du choix de a et b car le couple (a,b) est unique. On ne confondra pas cette nouvelle notion de conjugaison avec la conjugaison complexe usuelle.

c) Montrer que l'application $x \longmapsto \overline{x}$ est un automorphisme d'anneau de $\mathbb{Z}\left[\sqrt{d}\right]$.

3) Pour tout $x \in \mathbb{Z}\left[\sqrt{d}\right]$, on appelle *norme de* x et on note $N(x)$ le réel $x\overline{x}$.

a) Montrer que pour tous $x, x' \in \mathbb{Z}\left[\sqrt{d}\right]$: $\quad N(xx') = N(x)N(x')$.

b) Montrer que $N(x) \in \mathbb{Z}$ pour tout $x \in \mathbb{Z}\left[\sqrt{d}\right]$.

c) Montrer que l'ensemble G des éléments de norme 1 de $\mathbb{Z}\left[\sqrt{d}\right]$ est un sous-groupe de $\mathrm{U}\left(\mathbb{Z}\left[\sqrt{d}\right]\right)$.

d) Exhiber une bijection de l'ensemble des solutions de l'équation de Pell-Fermat $x^2 - dy^2 = 1$ d'inconnue $(x,y) \in \mathbb{Z}^2$ sur le groupe G.

4) Soit $x = a + b\sqrt{d} \in G \cap]1, +\infty[$.

a) Montrer que $a > 0$.

b) Montrer que $x^2 = 1 + 2bx\sqrt{d}$, puis que $b > 0$.

5) On conserve les notations de la question **4)**, mais en supposant cette fois que $d = 2$.

a) Montrer que $b \geqslant 2$, puis que $a \geqslant 3$.

b) En déduire que l'ensemble $G \cap]1, +\infty[$ admet $3 + 2\sqrt{2}$ pour plus petit élément.

Dans les questions **6)** et **7)**, on revient au cas général d'un entier d quelconque et on ADMET momentanément que l'ensemble $G \cap]1, +\infty[$ possède un plus petit élément $\xi = \alpha + \beta\sqrt{d}$ avec $\alpha, \beta \in \mathbb{N}^*$.

6) Soit $x \in G \cap \mathbb{R}_+^*$.

a) Montrer que $\xi^n \leqslant x < \xi^{n+1}$ pour un certain $n \in \mathbb{Z}$ à préciser.

b) En déduire que $x = \xi^n$.

7) a) Montrer que G contient -1, puis que : $\quad G = \left\{\xi^n \mid \quad n \in \mathbb{Z}\right\} \cup \left\{-\xi^n \mid \quad n \in \mathbb{Z}\right\}$. En déduire que les groupes G et $\mathbb{Z} \times \left\{\pm 1\right\}$ sont isomorphes.

b) Compléter pour tout $n \in \mathbb{N}$: $\quad \xi^n = \overbrace{\sum_{\cdots} \binom{n}{\cdots} \alpha^{\cdots} \beta^{\cdots} d^{\cdots}}^{\in \mathbb{Z}} + \sqrt{d} \overbrace{\sum_{\cdots} \binom{n}{\cdots} \alpha^{\cdots} \beta^{\cdots} d^{\cdots}}^{\in \mathbb{Z}}$.

c) Comment obtenir très simplement une expression analogue de ξ^n dans le cas où n est négatif ?

La fin de ce devoir est subtile et facultative. On y démontre l'existence de la solution ξ en exploitant massivement le *principe des tiroirs*.

Théorème **(Principe des tiroirs)** Quand on range $n+1$ chaussettes dans n tiroirs, deux chaussettes au moins se retrouvent dans le même tiroir.

8) a) Soit $n \in \mathbb{N}^*$ fixé. On pose pour tout $k \in [\![0,n]\!]$: $\delta_k = k\sqrt{d} - \lfloor k\sqrt{d} \rfloor$. Montrer l'existence de deux entiers $k, k' \in [\![0,n]\!]$ distincts pour lesquels $|\delta_k - \delta_{k'}| < \dfrac{1}{n}$.

b) En déduire pour tout $n \in \mathbb{N}^*$ l'existence d'un couple $(p,q) \in \mathbb{Z} \times [\![1,n]\!]$ pour lequel $\left|p - q\sqrt{d}\right| < \dfrac{1}{n}$.

c) En déduire l'existence d'une infinité de couples $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ pour lesquels $\left|p - q\sqrt{d}\right| < \dfrac{1}{q}$.

d) Montrer que pour tout couple (p,q) de la question **c)** : $\left|p^2 - dq^2\right| < 1 + 2\sqrt{d}$.

e) En déduire que pour un certain $r \in \mathbb{Z}$ non nul, l'équation $x^2 - dy^2 = r$ d'inconnue $(x,y) \in \mathbb{N}^2$ possède une infinité de solutions.

f) En déduire que l'équation de la question **e)** possède deux solutions (p_0,q_0) et (p_1,q_1) distinctes pour lesquelles : $p_0 \equiv p_1 \left[|r|\right]$ et $q_0 \equiv q_1 \left[|r|\right]$.

9) On pose $z_0 = p_0 + q_0\sqrt{d}$ et $z_1 = p_1 + q_1\sqrt{d}$. On peut supposer sans perte de généralité $z_0 > z_1$.
Montrer que $\dfrac{z_0\overline{z_1}}{r} \in \mathbb{Z}\left[\sqrt{d}\right]$, puis que $\dfrac{z_0\overline{z_1}}{r} \in G \cap]1,+\infty[$.

10) a) Montrer que pour tous $x = a + b\sqrt{d}, x' = a' + b'\sqrt{d} \in G \cap]1,+\infty[$: $a > a' \implies x > x'$.

b) En déduire que l'ensemble $G \cap]1,+\infty[$ possède un plus petit élément.