

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 $\mathbb{Z}[\sqrt{d}]$ l'ensemble $\{a + b\sqrt{d}\}_{a, b \in \mathbb{Z}}$.

- 1) Montrer que $\mathbb{Z}[\sqrt{d}]$, muni de l'addition et de la multiplication des réels, est un anneau.
- 2) a) Montrer l'irrationalité de \sqrt{d} .
 b) Montrer que pour tout $x \in \mathbb{Z}[\sqrt{d}]$, 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 \bar{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 pour tous $x, x' \in \mathbb{Z}[\sqrt{d}]$: $\overline{x + x'} = \bar{x} + \bar{x}'$ et $\overline{xx'} = \bar{x} \bar{x}'$.
- 3) Pour tout $x \in \mathbb{Z}[\sqrt{d}]$, on appelle *norme de x* et on note $N(x)$ le réel $x\bar{x}$.
 a) Montrer que pour tous $x, x' \in \mathbb{Z}[\sqrt{d}]$: $N(xx') = N(x)N(x')$.
 b) Montrer que pour tout $x \in \mathbb{Z}[\sqrt{d}]$: $N(x) \in \mathbb{Z}$.
 c) Montrer que l'ensemble G des éléments de norme 1 de $\mathbb{Z}[\sqrt{d}]$ est un sous-groupe de $U(\mathbb{Z}[\sqrt{d}])$.
 d) Expliquer en quoi la résolution de l'équation de Pell-Fermat : $x^2 - dy^2 = 1$ d'inconnue $(x, y) \in \mathbb{Z}^2$ est équivalente à la détermination de G .
- 4) Soit $x = a + b\sqrt{d} \in G \cap]1, +\infty[$.
 a) Simplifier $x + \bar{x}$. En déduire 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 : $b \geq 2$, puis que : $a \geq 3$.
 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 pour un certain $n \in \mathbb{Z}$: $\xi^n \leq x < \xi^{n+1}$.
 b) Déduire de la minimalité de ξ l'égalité : $x = \xi^n$.
- 7) a) Montrer que : $-1 \in G$, puis que : $G = \{\varepsilon \xi^n\}_{n \in \mathbb{Z}, \varepsilon = \pm 1}$.
 b) Compléter pour tout $n \in \mathbb{N}$: $\xi^n = \underbrace{\sum_{\dots \in \mathbb{Z}} \binom{n}{\dots} \alpha^{\dots} \beta^{\dots} d^{\dots}}_{\in \mathbb{Z}} + \sqrt{d} \underbrace{\sum_{\dots \in \mathbb{Z}} \binom{n}{\dots} \alpha^{\dots} \beta^{\dots} d^{\dots}}_{\in \mathbb{Z}}$.
 c) Comment obtenir une expression analogue de ξ^n dans le cas où n est négatif?

On démontre à présent l'existence de la solution ξ . Les questions qui suivent sont plus déroutantes, donc facultatives.

- 8) a) Soit $n \in \mathbb{N}^*$ fixé. On pose pour tout $k \in \llbracket 0, n \rrbracket$: $\delta_k = k\sqrt{d} - \lfloor k\sqrt{d} \rfloor$. Montrer l'existence de deux entiers $k, k' \in \llbracket 0, n \rrbracket$ pour lesquels : $|\delta_k - \delta_{k'}| < \frac{1}{n}$.
 b) En déduire pour tout $n \in \mathbb{N}^*$ l'existence d'un couple $(p, q) \in \mathbb{Z} \times \llbracket 1, n \rrbracket$ pour lequel : $|p - q\sqrt{d}| < \frac{1}{n}$.

- c) En déduire l'existence d'une infinité de couples $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ pour lesquels : $|p - q\sqrt{d}| < \frac{1}{q}$.
- d) Montrer que pour tout couple (p, q) de la question c) : $|p^2 - dq^2| < 1 + 2\sqrt{d}$.
- 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 :

$$p_0 \equiv p_1 \pmod{|r|} \quad \text{et} \quad q_0 \equiv q_1 \pmod{|r|}.$$

- 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 que : $z_0 > z_1$.
Montrer que : $\frac{z_0 z_1}{r} \in \mathbb{Z}[\sqrt{d}]$, puis que : $\frac{z_0 z_1}{r} \in G \cap]1, +\infty[$.
- 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.