Thème : équation de Pell-Fermat

Introduction

Soit d un entier naturel qui **n'est pas** un carré[1]. Ce problème propose une méthode permettant de déterminer tous les couples (x, y) d'entiers relatifs vérifiant l'équation de Pell-Fermat

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

Nous allons résoudre cette équation pour $d = 5$ mais la méthode se généralise pour n'importe quelle valeur de d.

I Premières constatations et expérimentation en Python

1. Quelques symétries : expliquer pourquoi il suffit de chercher les couples solutions (x, y) avec x et y dans $\mathbb{N}$ pour obtenir toutes les solutions de l'équation de Pell-Fermat.

Quelles symétries peut-on en déduire pour l'hyperbole[2] d'équation $x^2 - 5y^2 = 1$?

2. Soit (a, b) une solution de $x^2 - 5y^2 = 1$ avec a et b dans $\mathbb{N}^*$. Déterminer une fonction f telle que $a = f(b)$.

3. En déduire un script Python qui détermine des couples solutions de $\mathbb{N}^* \times \mathbb{N}^*$ (on pourra faire varier b de 1 à 2000).

4. Justifier que si (a, b) et (a', b) sont deux couples de $(\mathbb{N}^*)^2$ solutions, alors nécessairement $a = a'$.

On note ainsi légitimement (a_0, b_0) **le** couple solution de $\mathbb{N}^* \times \mathbb{N}^*$ obtenu avec Python, avec b minimal. On l'appellera *la solution fondamentale*.

II Utilisation de l'anneau $\mathbb{Z}[\sqrt{5}]$

On note $\mathbb{Z}[\sqrt{5}]$ l'ensemble des nombres réels de la forme $a+b\sqrt{5}$ avec a et b des entiers (relatifs).

1. *Une remarque instructive* : développer $(a_0 + b_0\sqrt{5})^2$ et $(a_0 + b_0\sqrt{5})^3$. Que remarque-t-on ?

2. Démontrer que tout élément x de $\mathbb{Z}[\sqrt{5}]$ admet une écriture unique de la forme $x = a+b\sqrt{5}$ avec a et b des entiers (relatifs).

Le nombre $\overline{x} = a - b\sqrt{5}$ est alors appelé «conjugué[3]» de x. C'est un élément de $\mathbb{Z}[\sqrt{5}]$.

---

1. Et si d est un carré ? On prend par exemple $d = 9$. Déterminer les entiers x et y tels que $x^2 - 9y^2 = 1$
2. Au fait savez-vous tracer cette hyperbole ?
3. Pourquoi ne pourrait-on pas écrire cette nouvelle définition sans l'unicité de la question précédente ?

3. Démontrer que l'application conjugaison est multiplicative, c'est-à-dire

$$\forall (x,y) \in \mathbb{Z}[\sqrt{5}]^2, \quad \overline{xy} = \overline{x}\ \overline{y}.$$

4. Pour $x = a + b\sqrt{5}$ de $\mathbb{Z}[\sqrt{5}]$, on pose $N(x) = x\overline{x}$. On dit que c'est la norme de x.

(a) Déduire de la question précédente que l'application norme est multiplicative, *i.e.*

$$\forall (x,y) \in \mathbb{Z}[\sqrt{5}]^2, \quad N(xy) = N(x)N(y).$$

(b) Si $x = a + b\sqrt{5}$ est dans $\mathbb{Z}[\sqrt{5}]$, donner l'expression de $N(x)$. En déduire une condition nécessaire et suffisante sur $N(x)$ pour que le couple (a,b) soit solution de l'équation de Pell-Fermat.

On considère l'ensemble

$$G = \{x \in \mathbb{Z}[\sqrt{5}] \mid \quad N(x) = 1\}.$$

5. Soit $a+b\sqrt{5}$ un élément de $\mathbb{Z}[\sqrt{5}]$. Démontrer que le réel $a+b\sqrt{5}$ est dans G si et seulement si le couple (a,b) est solution de l'équation de Pell-Fermat.

6. Démontrer que l'ensemble G est stable par multiplication, c'est-à-dire que si x et x' sont dans G alors xx' est encore dans G.

7. Soit $x \in G$, justifier que x est non nul et montrer que $\frac{1}{x} \in G$.

On vient d'établir une «correspondance bijective» entre les solutions de l'équation de Pell-Fermat $x^2 - 5y^2 = 1$ et les éléments du groupe G. Il reste à établir que tous les éléments du groupe G sont engendrés par l'élément $x_0 = a_0 + b_0\sqrt{5}$, ce qui prouvera que l'on peut déterminer toutes les solutions de l'équation de Pell-Fermat à l'aide de la solution fondamentale.

III Détermination d'un élément générateur de G

1. *Une correspondance* :

Soit $x = a + b\sqrt{5} \in G \cap]1, +\infty[$.

(a) Calculer $x + x^{-1}$ et en déduire que $a > 0$.

(b) Justifier que $x - \frac{1}{x} > 0$ en déduire que $b > 0$.

Ce résultat montre qu'un élément $x = a + b\sqrt{5}$ de G vérifie $x > 1$ ssi ($a > 0$ et $b > 0$).

2. *Un élément minimal du groupe*

On pose $x_0 = a_0 + b_0\sqrt{5}$ l'élément de $\mathbb{Z}[\sqrt{5}]$ où (a_0, b_0) est la solution fondamentale. Démontrer que x_0 est le plus petit élement de $G \cap]1, +\infty[$.

(on pourra remarquer que l'application $f : y \mapsto \sqrt{1 + 5y^2}$ est croissante sur $[1, +\infty[$).

3. Soit $x \in G \cap]1, +\infty[$.

(a) Déterminer un entier $n \in \mathbb{N}^*$ tel que $x_0^n \leqslant x < x_0^{n+1}$.

(b) En déduire que $x = x_0^n$ (on pourra raisonner par l'absurde et diviser l'inégalité précédente par un élément de G bien choisi).

4. Conclure que
$$G\cap]1,+\infty[=\{x_0^n \mid \quad n \in \mathbb{N}^*\}.$$

5. Déterminer enfin toutes les solutions de l'équation $x^2 - 5y^2 = 1$.