Devoir maison n°11 : Équation de Pell-Fermat

Jules Charlier, Thomas Diot, Pierre Gallois, Jim Garnier
1E1

Partie A - Premières propriétés

$$(E) : x^2 - 5y^2 = 1$$

1) Symétries : Les variables x et y sont mises au carré dans (E) et donc toujours positives. Donner un nombre négatif présent dans $\mathbb{Z}$ est équivalent à donner son opposé qui est dans $\mathbb{N}$. Il suffit donc de chercher toutes les solutions (x, y) positives qui sont dans $\mathbb{N}^2$ pour obtenir toutes les solutions dans $\mathbb{Z}^2$ de (E).

---

2) Nombre de solutions

a) Soient $a, b \in \mathbb{N}$. L'identité de Brahmagupta est équivalente à :

$$\left(a^2 + 5b^2\right)^2 - \left(a^2 - 5b^2\right)^2 = 5(2ab)^2$$

En factorisant le côté gauche de l'équation, on trouve :

$$\begin{aligned}\left(a^2 + 5b^2\right)^2 - \left(a^2 - 5b^2\right)^2 &= \left(a^2 + a^2 + 5b^2 - 5b^2\right)\left(a^2 - a^2 + 5b^2 + 5b^2\right) \\ &= \left(2a^2\right)\left(2 \cdot 5b^2\right) \\ &= 5(2ab)^2\end{aligned}$$

Ce qu'il fallait démontrer.

b) Soient $(x, y) \in \mathbb{N}^2$, tel que $(x, y) \neq (1, 0)$ et (x, y) solution de $(E) : x^2 - 5y^2 = 1$.

l'identité de Brahmagupta assure que :

$$1 = \left(a^2 + 5b^2\right) - 5(2ab)^2$$

Autrement dit, $\left(a^2 + 5b^2, 2ab\right)$ est également une solution de (E). Comme $a^2 + 5b^2 > a$ et $2ab > b$, cette solution est également différente de (a, b) et de tout autre solution (x, y) où $x < a$, $y < b$. Il existe donc, en itérant ce procédé, une infinité de solutions de (E) dans $\mathbb{N}^2$.

c) $(a, b) \in \mathbb{N}^2$ est solution de (E) si et seulement si $a^2 = 1 + 5b^2$. Comme $b^2 \geq 0$ et $a \geq 0$, on trouve que (a, b) est solution si et seulement si $a = \sqrt{1 + 5b^2}$. On pose donc $f(b) = \sqrt{1 + 5b^2}$.

TODO : script

d) Supposons que (a, b) et (a', b) soient solutions. Alors $a = f(b) = a'$ et $a = a'$. On peut donc bien choisir un ‹ couple minimal › comme le couple avec le b minimal.

Partie B - L'ensemble $\mathbb{Z}\left[\sqrt{5}\right] = \left\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$

Partie C - Détermination d'un élément générateur de $\mathbb{U}$.