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 :

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

Ce qu'il fallait démontrer.

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

l'identité de Brahmagupta assure que :

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

Autrement dit, $(a^2 + 5b^2, 2ab)$ 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.

e) Soit (a, b) une solution de (E) avec $a, b \in \mathbb{N}^*$. On a donc :

$$
\begin{aligned}
(E) : a^2 - 5b^2 &= 1 \\
\Leftrightarrow a^2 &= 1 + 5b^2 \\
\Leftrightarrow a &= \sqrt{1 + 5b^2}
\end{aligned}
$$

car $a \in \mathbb{N}, b \in \mathbb{N}$ donc $a \geq 0, 1 + 5b^2 \geq 0$.

Une telle fonction est donc

$$
\begin{aligned}
f : \mathbb{N} &\to \mathbb{R}_+ \\
b &\mapsto \sqrt{1 + 5b^2}
\end{aligned}
$$

La solution est valide si et seulement si $f(b) \in \mathbb{N}$.

Voici un script Haskell qui détermine des couples solution :

```haskell
f :: Double -> Double
f b = sqrt (1 + 5 * b^2)

test_to :: Double -> [Double]
test_to n = filter (isNat . f) [1..n]
```

On obtient :

```
[4, 72, 1292, 23184, 416020, 7465176, 16692641, 24157817, 31622993, 48315634,
55780810, 63245986, 79938627, 87403803, 94868979, 111561620, 119026796,
126491972, 133957148, ..., 3077073806,3077489826, 3078836095, ...]
```

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

1) L'existence de cette écriture est assurée par la définition de $\mathbb{Z}\left[\sqrt{5}\right]$. Supposons que $x = a + b\sqrt{5} = c + d\sqrt{5}$ pour $(a, b), (c, d) \in \mathbb{Z}^2$. Si $b \neq d$, alors :

$$
\begin{aligned}
a + b\sqrt{5} &= c + d\sqrt{5} \\
\Longleftrightarrow \sqrt{5} &= \frac{c - a}{b - d}
\end{aligned}
$$

Ce qui contredit l'irrationalité de $\sqrt{5}$. Donc $b = d$, et $a + b\sqrt{5} = c + b\sqrt{5}$, d'où $a = c$. Donc l'écriture $x = a + b\sqrt{5}$ de chaque $x \in \mathbb{Z}\left[\sqrt{5}\right]$ est unique.

---

2) Posons $x = a + b\sqrt{5}, y = c + d\sqrt{5}$. Alors :

$$
\begin{aligned}
\overline{x + y} &= \overline{(a + c) + (b + d)\sqrt{5}} \\
&= (a + c) - (b + d)\sqrt{5} \\
&= \left(a - b\sqrt{5}\right) + \left(c - d\sqrt{5}\right) \\
&= \overline{x} + \overline{y}
\end{aligned}
$$

Et similairement :

$$\begin{aligned}
\overline{xy} &= \overline{(ac+5bd)+(ad+bc)\sqrt{5}} \\
&= ac+5bd-(ad+bc)\sqrt{5} \\
\overline{x}\cdot\overline{y} &= \left(a-b\sqrt{5}\right)\cdot\left(c-d\sqrt{5}\right) \\
&= (ac+5bd)-(ad+bc)\sqrt{5}
\end{aligned}$$

D'où $\overline{xy} = \overline{x}\cdot\overline{y}$.

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