

# 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 :

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

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

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

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  $f(b) = \sqrt{1 + 5b^2}$ .

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



Voici un script Haskell qui détermine des couples solution :

```
f b = sqrt (1 + 5 * b^2)

test_to n = [ (a, b) | b <- [1..n]
                , let a = f b
                , isNat a
                ]
```

On obtient :

$[(9, 4), (161, 72), (2889, 1292), (51841, 23184), (930249, 416020), (16692641, 7465176), (37325880, 16692641), (54018521, 24157817), (70711162, 31622993), \dots, (686478381, 307002465), (703171022, 314467641), (723804261, 323695106), \dots]$

La solution avec le plus petit  $b$  est la solution fondamentale  $(9, 4)$ , qui satisfait :  $9^2 - 5 \cdot 4^2 = 81 - 80 = 1$  **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 $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$

**1)** L'existence de cette écriture est assurée par la définition de  $\mathbb{Z}[\sqrt{5}]$ . 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 :

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

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  $x \in \mathbb{Z}[\sqrt{5}]$  est unique.

---

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

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

Et similairement :



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

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

**3)** Soient  $x, y \in \mathbb{Z}[\sqrt{5}]$

**a)** On a les égalités suivantes :  $N(xy) = xy\overline{xy} = x\overline{x}y\overline{y} = N(x)N(y)$

**b)** En développant pour  $x = a + b\sqrt{5}$ :

$$\begin{aligned}
N(x) &= (a + b\sqrt{5})(a - b\sqrt{5}) \\
&= a^2 - 5b^2
\end{aligned}$$

Ainsi  $x$  a pour norme  $N(x) = 1$  si et seulement si  $(a, b) \in \mathbb{Z}^2$  est solution de l'équation  $(E)$ .

**4) Groupe des unités**  $\mathbb{U} = \{x \in \mathbb{Z}[\sqrt{5}], N(x) = 1\}$

**a)** Soient  $x, y \in \mathbb{U}$ . Alors  $N(xy) = 1 \cdot 1 = 1$ , et  $\mathbb{U}$  est clos sous la multiplication héritée de  $\mathbb{Z}[\sqrt{5}]$ .

**b)** Soit  $x = a + b\sqrt{5} \in \mathbb{U}$ . Comme  $N(0) = N(0 + 0\sqrt{5}) = 0$ ,  $x \neq 0$ . En passant au conjugué :

$$\begin{aligned}
\frac{1}{x} &= \frac{N(a + b\sqrt{5})}{a + b\sqrt{5}} \\
&= \frac{a^2 - 5b^2}{a + b\sqrt{5}} \\
&= a - b\sqrt{5} = \overline{x}
\end{aligned}$$

Comme  $N(\overline{x}) = N(x) = 1$ ,  $\overline{x}$  et donc  $\frac{1}{x} \in \mathbb{U}$ . Donc  $\mathbb{U}$  est un groupe sous la multiplication héritée de  $\mathbb{Z}[\sqrt{5}]$  (l'associativité est héritée).

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

**1)** Posons  $\mathbb{E} = \mathbb{U} \cap ]1; +\infty[$ . Soit  $x = a + b\sqrt{5} \in \mathbb{E}$ .

**a)** D'une part,  $x + \frac{1}{x} > 0$  car  $x > 1$ . D'autre part,  $x + \frac{1}{x} = x + \overline{x} = 2a$ . Donc  $2a > 0$  et  $a > 0$ .

**b)** Comme  $x > 1$ ,  $x - \frac{1}{x} > 0$ . De plus  $x + \frac{1}{x} = x + \overline{x} = 2b$ . Donc  $2b > 0$  et  $b > 0$ .



**2)** Soit  $(a_0, b_0) \in \mathbb{N}^2$  la solution fondamentale de  $(E)$ . Comme  $b_0 \neq 0, b_0 > 0$  et  $a_0 = f(b_0) > 0$ . De plus, comme  $b_0$  est minimal et que  $f$  est croissante sur  $\mathbb{R}^+$ ,  $a_0$  doit aussi être minimal. Donc  $x_0 = a_0 + b_0\sqrt{5}$  est bien le plus petit élément de  $\mathbb{E}$ .

**3) a)** La suite  $(x_0^n)_{n \in \mathbb{N}^*}$  est strictement croissante et diverge vers  $+\infty$  car  $x_0 > 1$ . Ainsi, pour chaque  $y \in \mathbb{R}^+$ , il existe un unique  $n \in \mathbb{N}^*$  tel que  $x_0^n \leq y < x_0^{n+1}$  : en particulier, pour tout  $x \in \mathbb{E}$ , il existe  $n \in \mathbb{N}^*$  tel que  $x_0^n \leq x < x_0^{n+1}$ .

**b)** Soit  $n \in \mathbb{N}^*$  l'unique entier tel que  $x_0^n \leq x < x_0^{n+1}$ . Supposons que  $x \neq x_0$ , soit

$$x_0^n < x < x_0^{n+1}$$

En divisant par  $x_0^n > 0$ , on trouve l'inégalité :

$$1 < \frac{x}{x_0^n} < x_0$$

Comme  $\mathbb{U}$  est un groupe et  $x, x_0 \in \mathbb{U}$ ,  $\frac{x}{x_0^n} \in \mathbb{U}$ . De plus, le côté gauche assure que  $\frac{x}{x_0^n} \in \mathbb{E}$ . Mais le côté droit contredit la minimalité de  $x_0$  : on doit donc avoir  $x = x_0$ .

**4)** Par la question C.1,  $\mathbb{E}$  est l'ensemble des  $x = a + b\sqrt{5} \in \mathbb{U}$  pour  $a, b \in \mathbb{N}^*$ . Ainsi, comme on peut passer  $a$  et  $b$  au négatif en restant dans  $\mathbb{U}$ , déterminer les éléments de  $\mathbb{E}$  suffit à déterminer les éléments de  $\mathbb{U}$ , et donc ensuite les solutions dans  $\mathbb{Z}^2$  de  $(E)$ . Or tous les éléments de  $\mathbb{E}$  sont générés par les puissances de  $x_0$ .

On peut donc prendre  $x_0 = 9 + 4\sqrt{5}$  ( $(9, 4)$  est la solution fondamentale), et calculer les « coordonnées » de ses puissances successives, ce qui permet de trouver toutes les solutions de  $(E)$ .

## Partie D - Annexes

**1)** Afin de ne pas froisser les fans de python :

```
def f(b: int) -> float:
    return sqrt(1 + 5 * b**2)

def test_to(n: int):
    for b in range(1, n+1):
        a = f(b)
        if a.is_integer():
            yield a, b
```

**2)** Plus (+) de DMs d'arithmétique svp Madame<sup>1</sup>

<sup>1</sup>Un fan qui restera anonyme