L'équation de Pell-Fermat $X^2 - 2Y^2 = -1$

`blogdemaths.wordpress.com`

Dans ce document, on se propose de trouver toutes les solutions de l'équation de Pell-Fermat $X^2 - 2Y^2 = -1$ ($X, Y \in \mathbb{Z}$).

1 Exemples de solutions et notation

1. Notation

Définition. *Pour dire que le couple (X, Y) est une solution de l'équation $X^2 - 2Y^2 = -1$, on dira que le nombre $X + Y\sqrt{2}$ est une solution de cette équation.*

La notation $X + Y\sqrt{2}$ ne peut représenter qu'une seule solution (on dit qu'elle est bien définie) comme le prouve la proposition suivante :

Proposition. *Soit $X, Y, X', Y' \in \mathbb{Z}$.*

$$X + Y\sqrt{2} = X' + Y'\sqrt{2} \iff X = X' \text{ et } Y = Y'$$

Démonstration. Montrons l'implication $\Rightarrow$ (l'autre étant évidente). On a :

$$X + Y\sqrt{2} = X' + Y'\sqrt{2} \iff (Y - Y')\sqrt{2} = X' - X$$

Si on avait $Y \neq Y'$ alors la condition précédente serait équivalente à $\sqrt{2} = \dfrac{X' - X}{Y - Y'}$ et cela impliquerait que $\sqrt{2}$ est un nombre rationnel, ce qui n'est pas le cas. On en déduit que nécessairement $Y = Y'$ et donc $0 \times \sqrt{2} = X' - X$ ce qui entraîne que $X = X'$. □

2. Quelques solutions

Cherchons quelques solutions de l'équation $X^2 - 2Y^2 = -1$ avec $X \geqslant 0$ et $Y \geqslant 0$:

- S'il existait une solution avec $X = 0$ alors on aurait $0^2 - 2Y^2 = -1 \iff Y^2 = \frac{1}{2}$, ce qui donnerait $Y = \sqrt{\frac{1}{2}}$, qui n'est pas entier. Il n'y a donc pas de solution avec $X = 0$.
- On remarque $X = 1$ et $Y = 1$ vérifient $1^2 - 2 \times 1^2 = 1 - 2 = -1$ donc $1 + \sqrt{2}$ est une solution qu'on appelle la solution *fondamentale*.
- On vérifie que pour $X = 2$, il n'y a pas de solution car $2^2 - 2 \times Y^2 = -1 \iff Y^2 = \frac{5}{2}$, ce qui donnerait un nombre Y qui n'est pas entier. De même, il n'y a pas de solution pour $X = 3, 4, 5, 6$.
- Les nombres $X = 7$ et $Y = 5$ vérifient bien l'équation donc $7 + 5\sqrt{2}$ est une solution.

2 Produit, inverse et opposé de solutions

1. L'identité de Brahmagupta

Lemme. *Pour tous nombres réels a, b, c et d,*

$$(a^2 - 2b^2)(c^2 - 2d^2) = (ac + 2bd)^2 - 2(ad + bc)^2$$

Démonstration. D'une part,

$$\begin{aligned}(a^2 - 2b^2)(c^2 - 2d^2) &= a^2c^2 - 2a^2d^2 - 2b^2c^2 + 4b^2d^2 \\ &= (ac)^2 + (2bd)^2 - 2(ad)^2 - 2(bc)^2\end{aligned}$$

D'autre part,

$$\begin{aligned}(ac + 2bd)^2 - 2(ad + bc)^2 &= (ac)^2 + 2ac \times 2bd + (2bc)^2 - 2\left[(ad)^2 + 2adbc + (bc)^2\right] \\ &= (ac)^2 + 4abcd + (2bd)^2 - 2(ad)^2 - 4adbc - 2(bc)^2 \\ &= (ac)^2 + (2bd)^2 - 2(ad)^2 - 2(bc)^2\end{aligned}$$

d'où l'égalité. □

2. Produit de deux solutions

Proposition. *Soit n et m deux entiers. On suppose que :*
- *$a + b\sqrt{2}$ est une solution de l'équation $X^2 - 2Y^2 = n$*
- *$c + d\sqrt{2}$ est une solution de l'équation $X^2 - Y^2 = m$*

alors le nombre $(a + b\sqrt{2})(c + d\sqrt{2})$ est une solution de l'équation $X^2 - 2Y^2 = n \times m$.

Démonstration. Comme $a^2 - 2b^2 = n$ et $c^2 - 2d^2 = m$, en multipliant ces deux équations on obtient :

$$(a^2 - 2b^2)(c^2 - 2d^2) = n \times m$$

D'après le lemme précédent, on en déduit que :

$$(ac + 2bd)^2 - 2(ad + bc)^2 = n \times m$$

donc $X = ac + 2bc$ et $Y = ad + bc$ est une solution de l'équation $X^2 - 2Y^2 = n \times m$. Il reste à voir que cette solution correspond bien au nombre $(a + b\sqrt{2})(c + d\sqrt{2})$. En développant ce nombre, on obtient :

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2}$$

Ainsi, $(a + b\sqrt{2})(c + d\sqrt{2})$ est bien une solution de l'équation $X^2 - 2Y^2 = n \times m$. □

3. Inverse d'une solution

On peut aussi prouver que l'inverse d'une solution reste une solution :

Proposition. *Si $a + b\sqrt{2}$ est une solution de l'équation $X^2 - 2Y^2 = -1$ alors $(a + b\sqrt{2})^{-1}$ est aussi une solution de cette équation.*

Démonstration. On a :

$$(a+b\sqrt{2})^{-1}=\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a-b\sqrt{2}}{-1}=-a+b\sqrt{2}$$

et donc $(a+b\sqrt{2})^{-1}=-a+b\sqrt{2}$ est aussi une solution de l'équation $X^2-2Y^2=-1$ car

$$(-a)^2-2b^2=a^2-2b^2=-1$$

□

4. Opposé d'une solution

Proposition. *Si $a+b\sqrt{2}$ est une solution de l'équation $X^2-2Y^2=-1$ alors $-(a+b\sqrt{2})$ est aussi une solution.*

Démonstration. On suppose que $a^2-2b^2=-1$. Puisque $-(a+b\sqrt{2})=(-a)+(-b)\sqrt{2}$ et que $(-a)^2-2(-b)^2=a^2-2b^2=-1$, alors $-(a+b\sqrt{2})$ est bien une solution. □

3 Une famille de solutions

Proposition. *Pour tout entier relatif n, le nombre $(1+\sqrt{2})^{2n+1}$ est une solution de l'équation $X^2-2Y^2=-1$.*

Démonstration. Commençons par montrer par récurrence que la proposition est vraie pour tout entier *naturel*.

- Si $n=0$ alors $(1+\sqrt{2})^{2\times 0+1}=1+\sqrt{2}$ qui, comme nous l'avons vu, est bien une solution.
- Soit $n\in\mathbb{N}$. On suppose que $(1+\sqrt{2})^{2n+1}$ est une solution de l'équation $X^2-2Y^2=-1$.
  Comme $(1+\sqrt{2})^2=3+2\sqrt{2}$ est une solution de l'équation $X^2-2Y^2=1$ (car $3^2-2\times 2^1=1$), on sait alors que $(1+\sqrt{2})^{2n+1}\times(1+\sqrt{2})^2=(1+\sqrt{2})^{2(n+1)+1}$ est une solution de l'équation $X^2-2Y^2=(-1)\times 1$. Cela prouve que la propriété est vraie au rang $n+1$.

Considérons à présent $n\in\mathbb{Z}$ un entier strictement négatif.
On remarque que $(1+\sqrt{2})^{2n+1}=\left((1+\sqrt{2})^{2(-n-1)+1}\right)^{-1}$. Or, $-n-1$ est un entier naturel donc on sait que $(1+\sqrt{2})^{2(-n-1)+1}$ est une solution de l'équation. Comme l'inverse d'une solution est une solution, on en déduit finalement que $\left((1+\sqrt{2})^{2(-n-1)+1}\right)^{-1}=(1+\sqrt{2})^{2n+1}$ est aussi une solution de l'équation $X^2-2Y^2=-1$. □

4 Toutes les solutions

Théorème. *Soit $X,Y\in\mathbb{Z}$.*
Le nombre $X+Y\sqrt{2}$ est une solution de l'équation $X^2-2Y^2=-1$ si, et seulement s'il existe $n\in\mathbb{Z}$ tel que

$$\boxed{X+Y\sqrt{2}=\pm(1+\sqrt{2})^{2n+1}}$$

Démonstration. Nous avons déjà prouvé que si $X+Y\sqrt{2}=(1+\sqrt{2})^{2n+1}$ alors c'est une solution. De plus, si $X+Y\sqrt{2}=-(1+\sqrt{2})^{2n+1}$ alors $X+Y\sqrt{2}$ est l'opposé d'une solution, donc c'est aussi une solution.
Réciproquement, soit $X+Y\sqrt{2}$ une solution et supposons dans un premier temps que $X\geqslant 0$ et $Y\geqslant 0$ (on peut même suppose $X>0$ car nous avons vu qu'il n'y a pas de solution pour $X=0$). La suite $(1+\sqrt{2})^{2n+1}$ est strictement croissante et tend vers $+\infty$ quand n tend vers $+\infty$ donc il existe un unique $n\in\mathbb{N}$ tel que

$$(1+\sqrt{2})^{2n+1}\leqslant X+Y\sqrt{2}<(1+\sqrt{2})^{2(n+1)+1}$$

Cela est équivalent à

$$1\leqslant(1+\sqrt{2})^{-(2n+1)}(X+Y\sqrt{2})<(1+\sqrt{2})^2$$

c'est-à-dire

$$1\leqslant(1+\sqrt{2})^{-(2n+1)}(X+Y\sqrt{2})<3+2\sqrt{2}$$

Les nombres $(1+\sqrt{2})^{-(2n+1)}$ et $X+Y\sqrt{2}$ sont tous deux solutions de l'équation $X^2-2Y^2=-1$ donc leur produit $(1+\sqrt{2})^{-(2n+1)}(X+Y\sqrt{2})$ est solution de l'équation $X^2-2Y^2=(-1)\times(-1)=1$. Or, la plus petite solution positive différente de 1 de l'équation $X^2-2Y^2=1$ est $3+2\sqrt{2}$. Comme $(1+\sqrt{2})^{-(2n+1)}(X+Y\sqrt{2})<3+2\sqrt{2}$, cela implique que $(1+\sqrt{2})^{-(2n+1)}(X+Y\sqrt{2})$ est nécessairement la solution triviale, c'est-à-dire :

$$(1+\sqrt{2})^{-(2n+1)}(X+Y\sqrt{2})=1$$

Cela prouve donc que $X+Y\sqrt{2}=(1+\sqrt{2})^{2n+1}$.

Pour finir, il reste trois cas à étudier. Avant cela, remarquons que si $X+Y\sqrt{2}$ est une solution, alors $-X+Y\sqrt{2}$, $X-Y\sqrt{2}$ et $-X-Y\sqrt{2}$ sont aussi des solutions.

• Si $X<0$ et $Y<0$:
Dans ce cas, $-X>0$ et $-Y>0$ donc, d'après ce que nous venons de voir, il existe un entier naturel n tel que, $(-X)+(-Y)\sqrt{2}=(1+\sqrt{2})^{2n+1}$. Autrement dit, $-(X+Y\sqrt{2})=(1+\sqrt{2})^{2n+1}$ donc $X+Y\sqrt{2}=-(1+\sqrt{2})^{2n+1}$.
• Si $X<0$ et $Y\geqslant 0$:
On a :

$$X+Y\sqrt{2}=\frac{(X+Y\sqrt{2})(-X+Y\sqrt{2})}{-X+Y\sqrt{2}}=\frac{2Y^2-X^2}{-X+Y\sqrt{2}}=\frac{1}{-X+Y\sqrt{2}}$$

Par suite, $X+Y\sqrt{2}=(-X+Y\sqrt{2})^{-1}$. Vu que $-X>0$ et $Y\geqslant 0$, on sait qu'il existe un entier n tel que $-X+Y\sqrt{2}=(1+\sqrt{2})^{2n+1}$ et on en déduit que

$$X+Y\sqrt{2}=\left((1+\sqrt{2})^{2n+1}\right)^{-1}=(1+\sqrt{2})^{-2n-1}=(1+\sqrt{2})^{2(-n-1)+1}=(1+\sqrt{2})^{2k+1}(k\in\mathbb{Z})$$

• Si $X\geqslant 0$ et $Y<0$:
De la même façon que précédemment, on peut prouver que

$$X+Y\sqrt{2}=\frac{-1}{X-Y\sqrt{2}}$$

ce qui entraîne que $X+Y\sqrt{2}=-\left(X-Y\sqrt{2}\right)^{-1}$. Comme $X\geqslant 0$ et $-Y>0$, il existe un entier n tel que $X-Y\sqrt{2}=(1+\sqrt{2})^{2n+1}$. D'où l'égalité

$$X+Y\sqrt{2}=-\left((1+\sqrt{2})^{2n+1}\right)^{-1}=-(1+\sqrt{2})^{2(-n-1)+1}=-(1+\sqrt{2})^{2k+1}(k\in\mathbb{Z})$$

□