Équation de Bachet

Samuel Rochetin

Jeudi 1er juin 2017

Problème. *Soit* $A := \mathbb{Z}\left[i\sqrt{2}\right]$.

On peut munir l'anneau euclidien $\mathbb{Z}\left[i\sqrt{2}\right] = \left\{a + i\sqrt{2}b, (a,b) \in (\mathbb{Z})^2\right\}$ *d'une norme* $N : \mathbb{Z}\left[i\sqrt{2}\right] \to \mathbb{Z}, z \mapsto N(z) = N\left(a + i\sqrt{2}b\right) = a^2 + 2b^2$.

On considère, pour $(x,y) \in \mathbb{Z}^2$, *l'équation*

$$x^2 + 2 = y^3 \tag{$*$}$$

1. *Quels sont les inversibles de* A *?*
2. *Montrer que* $i\sqrt{2}$ *est irréductible dans* A.
3. *Soit* (x,y) *solution de l'équation* $(*)$.
   (a) *Montrer que* x *est impair.*
   (b) *Soit* $\alpha \in A$ *un diviseur irréductible commun à* $x + i\sqrt{2}$ *et* $x - i\sqrt{2}$. *Montrer que* α *divise* $2i\sqrt{2}$ *et que* α *est associé à* $i\sqrt{2}$.
   (c) *En déduire que* $x + i\sqrt{2}$ *et* $x - i\sqrt{2}$ *sont premiers entre eux.*
   (d) *Montrer qu'il existe* $(a,b) \in \mathbb{Z}^2$ *tels que* $x + i\sqrt{2} = \left(a + bi\sqrt{2}\right)^3$.
   (e) *En déduire que* $a = \pm 1$ *et* $b = 1$.
4. *Résoudre l'équation* $(*)$.

Corrigé.

1. Les inversibles de A sont les éléments $\varepsilon = a + bi\sqrt{2}$ tels que $|N(z)| = 1$, c'est-à-dire tels que $a^2 + 2b^2 = 1$. Cela impose $b = 0$ (sinon $a^2 + 2b^2 \geq 2 > 1$), donc il vient $\varepsilon = \pm 1$. Réciproquement, 1 et -1 sont bien inversibles.
2. $N\left(i\sqrt{2}\right) = 2$ et 2 est un nombre premier, donc $i\sqrt{2}$ est irréductible dans A.
3. (a) Supposons que x soit pair. Alors, d'une part, 4 divise x^2 et d'autre part, $x^2 + 2$ est pair donc y^3 est pair, donc y est pair, donc 4 divise y^3. Donc 4 divise $y^3 - x^2 = 2$. Impossible. Donc x est impair.
   (b) α divise les deux éléments $x + i\sqrt{2}$ et $x - i\sqrt{2}$ donc α divise leur différence $2i\sqrt{2}$. Remarquons que $2i\sqrt{2} = -\left(i\sqrt{2}\right)^3$. L'irréductible α divise donc l'irréductible $i\sqrt{2}$. Donc α est associé à $i\sqrt{2}$.

(c) Supposons que $x+i\sqrt{2}$ et $x-i\sqrt{2}$ ne soient pas premiers entre eux : il existe un irréductible α qui divise ces deux éléments. D'après la question précédente, α est associé à $i\sqrt{2}$ donc $i\sqrt{2}$ divise ces deux éléments, en particulier $i\sqrt{2}$ divise $x+i\sqrt{2}$ donc $i\sqrt{2}$ divise x. Il existe donc des entiers relatifs m, n tels que $x = i\sqrt{2}\left(m+ni\sqrt{2}\right) = -2n + mi\sqrt{2}$. Or, x est un entier relatif, donc $m = 0$ et $x = -2n$ donc x est pair. Contradiction. Donc $x+i\sqrt{2}$ et $x-i\sqrt{2}$ sont premiers entre eux.

(d) $x^2+2 = y^3 \iff \left(x+i\sqrt{2}\right)\left(x-i\sqrt{2}\right) = y^3$. Les éléments $x+i\sqrt{2}$ et $x-i\sqrt{2}$ sont premiers entre eux, donc d'après le corollaire du théorème de décomposition en produit d'irréductibles, il existe un élément $z = a+bi\sqrt{2} \in A$ et un inversible $\varepsilon \in A$ tels que $x+i\sqrt{2} = \varepsilon\left(a+bi\sqrt{2}\right)^3$. Or, les inversibles de A sont 1 et -1, et vérifient $1 = 1^3$ et $-1 = (-1)^3$, ce qui répond à la question.

(e) En développant l'expression démontrée à la question précédente et en identifiant parties réelle et imaginaire, il vient $x = a\left(a^2-6b^2\right)$ et $1 = b\left(3a^2-2b^2\right)$, où a, b sont des entiers relatifs. Cette dernière égalité implique que $b = \pm 1$. Si $b = -1$, alors $3a^2 = 1$. Impossible. Donc $b = 1$ et il vient $a = \pm 1$.

4. Soit (x, y) solution de $(*)$. D'après la question précédente, nous avons nécessairement $x = a\left(a^2-6b^2\right), a = \pm 1, b = 1$, donc $x = \pm 5$ et $y^3 = 27$ donc $y = 3$. Réciproquement, $(5, 3)$ et $(-5, 3)$ sont solutions de $(*)$. Ce sont donc les seules.

□