UNE ARITHMÉTIQUE NOUVELLE AU SERVICE DE MORDELL

On s'intéresse dans ce devoir à l'*équation de Mordell* : $y^2 = x^3 - 2$ d'inconnue $(x,y) \in \mathbb{Z}^2$. Nous avons résolu deux équations de ce type dans un devoir précédent par des considérations de pure arithmétique dans $\mathbb{Z}$, et c'est au fond de la même manière que nous allons résoudre cette nouvelle équation. Nous devrons cependant ici dépasser l'anneau $\mathbb{Z}$ et explorer l'arithmétique inattendue de l'anneau $\mathbb{Z}\big[\mathrm{i}\sqrt{2}\big] = \Big\{a + \mathrm{i}b\sqrt{2}\Big\}_{a,b\in\mathbb{Z}}$. Vous comprendrez mieux après ce devoir, en principe, en quoi les structures algébriques sont riches de sens en dépit de leur apparente gratuité et susceptibles de révéler de nombreux phénomènes mathématiques qui nous resteraient cachés sans.

Une fois pour toutes, on pose : $A = \mathbb{Z}\big[\mathrm{i}\sqrt{2}\big]$.

1) a) Représenter A dans le plan complexe, puis montrer que A est un sous-anneau de $\mathbb{C}$.

b) Montrer que pour tout $x \in A$: $|x|^2 \in \mathbb{N}$. À quelle condition a-t-on : $|x|^2 = 1$?

c) Déterminer le groupe $U(A)$ des inversibles de A.

À partir de la définition qui suit, le vocabulaire de l'arithmétique dans $\mathbb{Z}$ va se trouver progressivement transcrit dans l'anneau A. Prenez bien garde de ne pas confondre une idée que vous avez dans $\mathbb{Z}$ et une idée que vous avez dans A, les mots coïncident mais pas les objets.

Définition (Divisibilité et association dans A) Soient $x, y \in A$.

- On dit que x *divise* y ou que x est un *diviseur de* y s'il existe un élément $k \in A$ pour lequel : $y = kx$.
- On dit que y est *associé à* x s'il existe un élément $u \in U(A)$ pour lequel : $y = ux$.

2) a) Expliquer l'assertion suivante : « $U(A)$ est un groupe, donc la relation d'association est une relation d'équivalence sur A. »

b) Montrer que pour tous $x, y \in A$, x et y sont associés si et seulement si x et y se divisent mutuellement.

3) a) Montrer que pour tous $x, y \in A$ avec $y \neq 0$, il existe un couple $(q,r) \in A^2$ pour lequel : $x = qy + r$ et $|r|^2 < |y|^2$ — *théorème de la division euclidienne*. On pourra chercher à approximer $\dfrac{x}{y}$ par un élément de A.

b) Montrer que le couple (q,r) de la question **a)** n'est pas forcément unique.

Définition (Couple d'éléments premiers entre eux dans A) Soient $x, y \in A$. On dit que x et y sont *premiers entre eux* si leurs seuls diviseurs communs sont les éléments de $U(A)$.

4) Soient $x, y \in A$ premiers entre eux. On note $Ax + Ay$ l'ensemble : $Ax + Ay = \big\{ux + vy\big\}_{u,v\in A}$.

a) Justifier l'existence de : $m = \min\limits_{\substack{z\in Ax+Ay \\ z\neq 0}} |z|^2$.

On peut dès lors se donner un élément $d \in Ax + Ay$ non nul pour lequel : $|d|^2 = m$.

b) Montrer que d divise x.

c) En déduire l'existence de deux éléments $u, v \in A$ pour lesquels : $ux + vy = 1$ — *théorème de Bézout*.

5) Soient $x, y, z \in A$. On suppose que x divise yz et que x et y sont premiers entre eux. Montrer qu'alors x divise z — *théorème de Gauss*.

Définition (Irréductibles de A) Soit $x \in A$. On dit que x est *irréductible* si x n'est pas inversible et si ses seuls diviseurs sont 1, x et leurs associés.

On se donne à présent arbitrairement un *ensemble P de représentants des classes d'équivalence des irréductibles de A pour la relation d'association*. Cette expression signifie que P est une partie de A satisfaisant les trois conditions suivantes :

— tout élément de P est irréductible,

— tout irréductible de A est associé à un élement de P,

— les éléments de P sont deux à deux non associés.

6) Montrer que pour tout $x \in A$ non nul, il existe un élément $u \in U(A)$ et une famille presque nulle $(\alpha_p)_{p\in P}$ d'entiers naturels pour lesquels : $x = u\prod_{p\in P} p^{\alpha_p}$ — existence d'une *factorisation irréductible*.

7) Soit $p \in P$.

a) Justifier l'existence, pour tout $x \in A$ non nul, de : $v_p(x) = \max\left\{n \in \mathbb{N} / \quad p^n \text{ divise } x\right\}$ — *valuation p-adique de x*.

b) Montrer que pour tous $x, y \in A$ non nuls : $v_p(xy) = v_p(x) + v_p(y)$.

c) Que valent $v_p(u)$ pour tout $u \in U(A)$ et $v_p(q)$ pour tout $q \in P$?

8) Montrer l'unicité de la factorisation irréductible à l'ordre des facteurs près.

9) Montrer que pour tous $x, y \in A$ premiers entre eux, si xy est le cube d'un élément de A, alors x et y en sont aussi.

On résout enfin dans la dernière partie de ce devoir l'équation de Mordell : $y^2 = x^3 - 2$ d'inconnue $(x, y) \in \mathbb{Z}^2$.

10) Soit $(x, y) \in \mathbb{Z}^2$. On suppose que : $y^2 = x^3 - 2$. Soit $d \in A$ un diviseur commun de $y + \mathrm{i}\sqrt{2}$ et $y - \mathrm{i}\sqrt{2}$.

a) Montrer que dans $\mathbb{Z}$, $|d|^2$ divise à la fois 8 et x^3.

b) Montrer, en raisonnant modulo 4, que x est impair.

c) En déduire que : $d \in U(A)$.

11) Montrer finalement que les solutions de l'équation de Mordell : $y^2 = x^3 - 2$ d'inconnue $(x, y) \in \mathbb{Z}^2$ sont exactement les couples $(3, 5)$ et $(3, -5)$.