UNE EQUATION DE MORDELL

On propose de montrer que si les entiers x, y vérifient

$$y^2 + 4 = x^3,$$

alors $(x, y) = (5, \pm 11)$ ou $(2, \pm 2)$.

On travaille sur l'anneau euclidien (donc factoriel) $\mathbb{Z}[i]$.

$$x^3 = (y + 2i)(y - 2i). \ (*)$$

Nous allons montrer que ceci implique que les deux facteurs du membre de droite sont des cubes de $\mathbb{Z}[i]$. Montrons tout d'abord que ceci nous mènera avec puissance et élégance à la solution de l'énoncé. Supposons donc

$$y + 2i = (m + ni)^3, \ m, n \in \mathbb{Z}.$$

On obtient alors $y = m(m^2 - 3n^2)$, $2 = n(3m^2 - n^2)$. La seconde équation donne $n = \pm 1$ ou $n = \pm 2$.
On obtient cas par cas les solutions suivantes $(n, m) = (1, \pm 1)$, ou $(-2, \pm 1)$. Le premier cas donne $(x, y) = (2, \pm 2)$ et le second $(5, \pm 11)$.

Reste à montrer que $y + 2i$ et $y - 2i$ sont des cubes. En fait, par (*), il suffit de le montrer pour un des deux.
L'équation $y^2 + 4 = x^3$ quotientée dans $\mathbb{Z}/2\mathbb{Z}$ montre que x et y sont de même parité.

1er Cas. x et y sont impairs. Montrons que $y + 2i$ et $y - 2i$ sont premiers entre eux dans $\mathbb{Z}[i]$.
Soit d un diviseur commun à $(y+2i)$ et $(y-2i)$. Alors d divise $4i$. Donc, dans $\mathbb{Z}$, $N(d)$ divise 16 et $N(y+2i) = y^2+4$ qui est impair et ainsi $N(d) = 1$, ce qui fait de d une unité.
Il vient que $y+2i$ et $y-2i$ sont bien premiers entre eux et donc l'équation (*) montre que ce sont des cubes à unité près dans $\mathbb{Z}[i]$. Mais les unités de $\mathbb{Z}[i]$ sont elles-mêmes des cubes (ce sont les racines quatrièmes de l'unité et 3 est inversible dans $\mathbb{Z}/4\mathbb{Z}$), et donc notre assertion est vérifiée dans ce cas.

2ème cas. On suppose maintenant que x et y sont tous deux pairs. On pose $x = 2t$ et $y = 2z$, de sorte que

$$z^2 + 1 = 2t^3.$$

ce qui donne que z est impair en regardant cette équation modulo 2 et t est impair, en la regardant modulo 4. Le nombre z étant impair, on a facilement que $z + i$ est divisible par $(1 + i)$ dans $\mathbb{Z}[i]$ et de même, $z - i$ est divisible par $(1 + i)$. D'où

$$-it^3 = \left(\frac{z + i}{1 + i}\right)\left(\frac{z - i}{1 + i}\right).$$

Ces deux facteurs sont de plus premiers entre eux dans $\mathbb{Z}[i]$, puisque si d est un diviseur commun, alors, d divise leur différence $\frac{2i}{1+i}$. Ce qui donne $N(d)$ divise $N(\frac{2i}{1+i}) = 2$. Or, comme d divise t^3, $N(d)$ divise aussi $N(t^3) = t^6$ qui est impair. Donc d est une unité et on conclut comme dans le premier cas que $\frac{z+i}{1+i}$ est un cube, puis que $y + 2i = 2(z + i) = i^3(1 + i)^3 \frac{z+i}{1+i}$ en est un aussi.