FEUILLE DE TRAVAUX DIRIGÉS 6

ARITHMÉTIQUE DES ANNEAUX

Exercice 1 (Un autre théorème de Fermat)**.**

Montrer que les solutions de l'équation diophantienne $y^2 + 4 = z^3$ sont $(\pm 11, 5)$ et $(\pm 2, 2)$.
Indication : Travailler dans l'anneau euclidien $\mathbb{Z}[i]$ et séparer les deux cas : y impair puis y pair.

• Traitons d'abord le cas y impair. On se place dans l'anneau des entiers de Gauss $\mathbb{Z}[i]$, où l'équation s'écrit

$$y^2 + 4 = (y + 2i)(y - 2i) = z^3.$$

Soit $a+ib$ un facteur commun à $y+2i$ et à $y-2i$, alors il divise aussi leur somme $2y$ et leur différence $4i$. D'où la norme $a^2 + b^2$ divise $4y^2$ et 16. Donc $a^2 + b^2$ est une puissance de 2 et comme y est impair, on a que $a^2 + b^2$ divise 4. Les seules possibilités sont alors $a = \pm 1$, $b = 0$ et $a = 0$, $b = \pm 1$, qui sont des unités, et $a = \pm 1$, $b = \pm 1$, mais ce dernier cas est impossible car y est impair. Donc $y + 2i$ et $y - 2i$ est premiers entre eux dans $\mathbb{Z}[i]$. Comme $\mathbb{Z}[i]$ est un anneau euclidien, il est principal puis factoriel. En appliquant le lemme d'Euclide, on a que $y + 2i$ et $y - 2i$ sont des cubes. On a ainsi $y + 2i = (a + ib)^3$, ce qui donne par identification

$$y = a(a^2 - 3b^2) \quad \text{et} \quad 2 = b(3a^2 - b^2).$$

Les seuls valeurs possibles de a et de b donnent $y = \pm 11$ et $z = 5$ et $y = \pm 2$ et $z = 2$, qui sont bien solutions de l'équation de départ.

• Si maintenant y est pair. On peut l'écrire $y = 2Y$. L'équation devient alors $4Y^2+4 = 4(Y^2+1) = z^3$. Donc z est pair, et on l'écrit aussi $z = 2Z$. Il faut alors résoudre $Y^2 + 1 = 2Z^3$, qui devient

$$Y^2 + 1 = (Y + i)(Y - 1) = 2Z^3$$

dans $\mathbb{Z}[i]$. Remarquons que Y est impair. Soit $a + ib$ un diviseur commun de $Y + i$ et de $Y - 1$, de la même manière que précédement, on a que $a = \pm 1$, $b = 0$ et $a = 0$, $b = \pm 1$, qui sont des unités, et $a = \pm 1$, $b = \pm 1$. Donc le plus grand diviseur commun de $Y + i$ et de $Y - 1$ est $1 + i$. Comme $-i.(1 + i) = 1 - i$ et que $-i$ est une unité, on a que $1 - i$ divise $Y - i$. Et comme $(1 + i)(1 - i) = 2$, on a $Y + i = (1 + i)(a + ib)^3$. On montre alors qu'il n'a aucune solution possible.