<u>Au fil des problèmes</u> <u>Jean-Claude Carréga (Lyon)</u>

<u>Solution N° 537-3</u>

A) <u>Equation $x^2 + y^2 = 31 z^2$</u> (3)

Soit (x, y, z) une solution de l'équation avec x, y, z dans **N**. Si z = 0, alors $x^2 + y^2 = 0$ entraine x = y = 0. Si x = 0, on a $y^2 = 31 z^2$. Si y et z sont non nuls on obtient une contradiction car l'exposant de 31 dans la décomposition en facteurs premiers du premier membre est pair et cet exposant est impair dans la décomposition du second membre. Ainsi si x = 0 on a nécessairement y = z = 0. On a un résultat analogue en supposant y = 0. Il en résulte x, y, et z sont non nuls. Après division par pgcd(x, y, z), on peut supposer x, y, z premiers entre eux dans leur ensemble.
Modulo 31 on a $\bar{x}^2 + \bar{y}^2 = \bar{0}$. Si $\bar{y} = \bar{0}$, alors 31 divise y et d'après (3) 31 divise aussi x, d'où il résulte que 31^2 divise $x^2 + y^2$, donc 31^2 divise $31z^2$, d'où 31 divise z. Ceci est contradictoire avec x, y, z premiers entre eux dans leur ensemble, donc $\bar{y} \neq \bar{0}$. Ainsi $\bar{y}$ est inversible dans le corps **Z**/31**Z** et à partir de $\bar{x}^2 + \bar{y}^2 = \bar{0}$, on obtient $(\bar{x}\bar{y}^{-1})^2 = -\bar{1}$.
Or, nous savons que, si p est un nombre premier impair, $-\bar{1}$ est un carré dans le corps **Z**/p**Z** si et seulement si $p \equiv 1 \pmod 4$. Ici nous avons p = 31 et $31 \equiv 3 \pmod 4$. Ceci est donc contradictoire avec $(\bar{x}\bar{y}^{-1})^2 = -\bar{1}$. Il en résulte que l'équation (3) n'a pas de solutions autres que la solution triviale (0,0,0).

B) <u>Sur l'équation $x^2 + y^2 = 29 z^2$</u> (4)

1) On a $29 \equiv 1$ (Mod 4), on n'a pas ici l'impossibilité trouvée pour l'équation (3).
En fait, on trouve aussitôt une solution non triviale. A partir de $29 = 5^2 + 2^2$, on obtient la solution (5, 2, 1) et par homogénéité de l'équation, on obtient une infinité de solutions (5 k, 2k, k) avec k entier k ≥ 1. On a aussi les solutions obtenues en permutant x et y, soit (2k, 5k, k) avec k entier k ≥ 1.

2) Dans la suite, on cherche des solutions (x, y, z) avec x, y, z entiers ≥ 1. Les solutions dans $\mathbf{Z}^3$ s'obtiendraient alors par (± x, ± y, ± z).
Nous donnons une méthode permettant d'obtenir une infinité de solutions de la façon suivante :
a) On résout l'équation $x_1^2 + y_1^2 = z^2$
b) l'équation (4) permet d'obtenir $x^2 + y^2 = (5^2 + 2^2)(x_1^2 + y_1^2)$
c) On sait que les sommes de 2 carrés sont stables par produit d'où, par l'identité de Lagrange, $x^2 + y^2 = = (5x_1 - 2\varepsilon y_1)^2 + (5y_1 + 2\varepsilon x_1)^2$, avec $\varepsilon = \pm 1$. Cela permet d'obtenir des solutions de l'équation (4) : $(5x_1 - 2\varepsilon y_1, 5y_1 + 2\varepsilon x_1, z)$ et $(5y_1 + 2\varepsilon x_1, 5x_1 - 2\varepsilon y_1, z)$.

Nous appliquons maintenant cette méthode :
Nous connaissons la forme générale des solutions non triviales de l'équation classique : $x_1^2 + y_1^2 = z^2$, elles sont données par $x_1 = k(u^2 - v^2)$, $y_1 = 2k\,u\,v$, $z = k(u^2 + v^2)$, avec u et v premiers entre eux v < u et k entier ≥ 1, avec aussi les solutions obtenues en permutant x_1 et y_1. On obtient alors $5x_1 - 2\varepsilon y_1 = 5k(u^2 - v^2) - 4k\varepsilon\,u\,v$, $5y_1 + 2\varepsilon x_1 = 10k\,u\,v + 2k\varepsilon(u^2 - v^2)$,

Il en résulte, pour l'équation (4),

les solutions (x, y, z) avec $x = k [5 (u^2 - v^2) - 4\varepsilon u v]$, $y = k [10 u v + 2\varepsilon (u^2 - v^2)]$, $z = k (u^2 + v^2)$ avec u et v entiers premiers entre eux vérifiant $v < u$ et k entier ≥ 1, $\varepsilon = \pm 1$ et avec la possibilité de permuter les valeurs de x et y.
Donnons 2 exemples : En prenant $u = 3$, $v = 1$, $k = 1$, $\varepsilon = 1$, on obtient $x = 28$, $y = 46$, $z = 10$.
On vérifie que $x^2 + y^2 = 784 + 2116 = 2900 = 29 \times (10)^2$, donc $x^2 + y^2 = 29 z^2$.
Avec $u = 3$, $v = 1$, $k = 1$ et $\varepsilon = -1$, on obtient $x = 52$, $y = 14$, $z = 10$.
On a alors $x^2 + y^2 = 2704 + 196 = 2900 = 29 z^2$.

3) Essai de résolution de l'équation (4) :
Nous avons obtenu, en 1) et 2), 2 familles infinies de solutions de l'équation (4), mais nous n'avons pas établi que ce sont les seules solutions de l'équation (4). Pour établir cela nous allons utiliser l'anneau des entiers de Gauss $A = \mathbf{Z}[i] = \{ a + i b \ / \ a \text{ et } b \text{ dans } \mathbf{Z}\}$.
C'est un anneau principal sur lequel est définie la fonction N à valeurs entières par $N(a + i b) = a^2 + b^2$. Cette fonction vérifie la propriété : $N(t t') = N(t) N(t')$ et les éléments inversibles t de l'anneau sont caractérisés par $N(t) = 1$.
Nous supposons que (x, y, z) est une solution non triviale de l'équation (4), on a donc $x^2 + y^2 = 29 z^2$. Dans l'anneau A, cette égalité peut s'écrire :
$(x + i y) (x - i y) = (5 + 2 i) (5 - 2 i) z^2$.
Montrons que l'élément $5 + 2 i$ est irréductible dans l'anneau A.
Si $5 + 2 i$ n'est pas irréductible, il existe t et t' dans A , non inversibles tels que $5 + 2 i = t t'$.
D'où $N(5 + 2 i) = N(t t')$, qui s'écrit $29 = N(t) N(t')$. Puisque 29 est un nombre premier, on obtient $N(t) = 1$ ou $N(t') = 1$, ce qui contredit que t et t' sont non inversibles.
Ainsi, $5 + 2 i$ est irréductible, donc aussi premier, dans l'anneau principal A. Cet élément premier divise $(x + i y) (x - i y)$, donc il divise l'un des 2 facteurs.
On peut supposer que $5 + 2 i$ divise $x + i y$, le raisonnement qui suit serait le même si $5 + 2 i$ divisait $x - i y$. Il existe donc t dans A tel que $x + i y = (5 + 2 i) t$. En prenant les images par la fonction N, on obtient $x^2 + y^2 = 29 N(t)$. En comparant avec $x^2 + y^2 = 29 z^2$, on obtient $z^2 = N(t)$.
En notant $t = x_1 + i y_1$, on a $z^2 = x_1^2 + y_1^2$.
– Si $x_1 = 0$ ou $y_1 = 0$, on obtient comme en 1) les solutions évidentes de l'équation (4) , les $(5k, 2k, k)$ ou $(2k, 5k, k)$ avec k entier ≥ 1.
– Si x_1 et y_1 sont non nuls, on est dans la situation 2) où nous avons obtenu les solutions (x, y, z) avec $x = k [5 (u^2 - v^2) - 4\varepsilon u v]$, $y = k [10 u v + 2\varepsilon (u^2 - v^2)]$, $z = k (u^2 + v^2)$, où u et v sont des entiers premiers entre eux vérifiant $v < u$ et k entier ≥ 1, $\varepsilon = \pm 1$ et avec la possibilité de permuter les valeurs de x et y.