Un problème vache

AR2 2011-12

Vous avez peut-être entendu parler du "Théorème de Fermat" qui affirme que, dès que n est supérieur ou égal à 3, l'équation $x^n + y^n = z^n$ n'admet pas de solution en entiers non nuls. Ce résultat énoncé par Fermat a dû attendre presque 350 ans pour avoir enfin une démonstration par A. Wiles, en 1995.

Nous allons faire (presque) aussi fort : montrer le théorème de Fermat pour les polynômes.

> *Dès que $n \geq 3$, il n'existe pas de polynômes non constants $P, Q, R \in \mathbb{C}[X]$ tels que $P^n + Q^n = R^n$.*

1) Pouvez vous trouver des polynômes non constants P, Q, R tels que $P^2 + Q^2 = R^2$?

On suppose maintenant $n \geq 3$. On va montrer un résultat plus fort que le théorème de Fermat pour les polynômes.

> (*) *Il n'existe pas de polynômes non constants P, Q, R de $\mathbb{C}[X]$ et de complexes non nuls a, b, c tels que $aP^n + bQ^n + cR^n = 0$.*

2) Montrer (*) entraîne Fermat-polynômes.

Pour montrer (*), on va raisonner par l'absurde en supposant l'existence de P, Q, R, a, b, c comme ci-dessus vérifiant $aP^n + bQ^n + cR^n = 0$. On peut alors choisir une telle solution avec $\deg P \leq \deg Q \leq \deg R$ qui soit minimale du point de vue des degrés, dans le sens suivant : toute autre solution fait intervenir un polynôme de degré $\geq \deg R$.

3) Montrer que la condition de minimalité du point de vue des degrés entraîne que P, Q, R sont premiers entre eux deux à deux. (Indication : s'ils ne le sont pas, montrer qu'ils ont un facteur commun non constant et qu'on obtiendrait une solution avec des degrés plus petits en divisant pas ce facteur).

4) Soit u un nombre complexe tel que $u^n = -c/b$ et soit $\omega = e^{2i\pi/n}$. Montrer que

$$Q^n + \frac{c}{b} R^n = \prod_{k=0}^{n-1} (Q - u\omega^k R) \, .$$

(On pourra vérifier que $\prod_{k=0}^{n-1}(X - u\omega^k) = X^n + (c/b)$).

Dans ce qui suit, on pose $A_k = Q - u\omega^k R$ pour $k = 0, \ldots, n-1$.

5) Montrez que les A_k sont premiers entre eux deux à deux.

6) En déduire qu'il existe des polynômes $B_k \in \mathbb{C}[X]$ pour $k = 0, \ldots, n-1$ tels que $A_k = B_k^n$. (Utiliser $Q^n + \frac{c}{b} R^n = (-a/b)P^n$, et faire intervenir une décomposition en produit de facteurs irréductibles de P).

7) Montrer que $(\omega^2 - \omega)B_0^n + (1 - \omega^2)B_1^n + (\omega - 1)B_2^n = 0$.

8) Conclure.