

Le théorème d'Aubry

Dans le livre de Marc Guinot, *Les resveries de Fermat* (Arithmétique pour amateurs, tome 2), on trouve ce théorème, attribué à Aubry (1912) :

si un nombre entier peut s'écrire comme une somme de deux carrés de nombres rationnels, alors il peut aussi s'écrire comme une somme de deux carrés de nombres entiers.

Ce théorème peut être étendu à des sommes de trois ou même quatre carrés. . . On se limite dans ce document au cas de *deux carrés*.

Théorème 1. Le nombre entier $n > 0$ étant fixé, si l'équation $x^2 + y^2 = n$ admet une solution en nombres rationnels, alors elle admet aussi une solution en nombres entiers.

En voici la traduction géométrique, dans un repère *orthonormé*.

Théorème 2. Si le cercle $(\mathcal{C}) : x^2 + y^2 = n$ passe par un point à coordonnées rationnelles, alors il passe aussi par un point à coordonnées entières.

Démonstration du théorème 2. Soit un point $P(a/b ; c/d)$ à coordonnées rationnelles (non entières) sur le cercle (\mathcal{C}) et soit un point $P'(p ; q)$ à coordonnées entières tel que $PP' < 1$, c'est-à-dire

$$(1) \quad 0 < \left(p - \frac{a}{b}\right)^2 + \left(q - \frac{c}{d}\right)^2 < 1.$$

Il est clair qu'un tel point P' existe toujours. La droite (PP') coupe (\mathcal{C}) en P et Q . Déterminons les coordonnées de ce point Q . Le vecteur

$$(2) \quad \overrightarrow{PP'} \left(p - \frac{a}{b} ; q - \frac{c}{d}\right)$$

dirige la droite (PP') , d'où la caractérisation sous forme paramétrique d'un quelconque point M de celle-ci

$$(3) \quad M \left(p + t \left(p - \frac{a}{b}\right) ; q + t \left(q - \frac{c}{d}\right)\right), t \in \mathbb{R}.$$

En reportant ces expressions dans l'équation de (\mathcal{C}) , on obtient

$$(4) \quad \left[p + t \left(p - \frac{a}{b}\right)\right]^2 + \left[q + t \left(q - \frac{c}{d}\right)\right]^2 = n$$

c'est-à-dire, en ordonnant relativement au paramètre t ,

$$(5) \quad \left[\left(p - \frac{a}{b}\right)^2 + \left(q - \frac{c}{d}\right)^2\right] t^2 + 2 \left[p \left(p - \frac{a}{b}\right) + q \left(q - \frac{c}{d}\right)\right] t + p^2 + q^2 - n = 0.$$

C'est une équation du second degré en t , dont $t = 1$ est une solution, puisque P (correspondant à cette valeur du paramètre) est point d'intersection de la droite et du cercle. La seconde solution est donc donnée par

$$(6) \quad t = \frac{p^2 + q^2 - n}{\left(p - \frac{a}{b}\right)^2 + \left(q - \frac{c}{d}\right)^2}.$$

Observons que $\left(p - \frac{a}{b}\right)^2 + \left(q - \frac{c}{d}\right)^2 = PP'^2$; alors on a plus simplement

$$(7) \quad t = \frac{p^2 + q^2 - n}{PP'^2}.$$

On en déduit alors les coordonnées (rationnelles) du point cherché

$$(8) \quad Q \left(p + \frac{p^2 + q^2 - n}{PP'^2} \left(p - \frac{a}{b} \right); q + \frac{p^2 + q^2 - n}{PP'^2} \left(q - \frac{c}{d} \right) \right).$$

Or, on a

$$(9) \quad PP'^2 = \left(p - \frac{a}{b} \right)^2 + \left(q - \frac{c}{d} \right)^2$$

$$(10) \quad = p^2 + q^2 + \left(\frac{a}{b} \right)^2 + \left(\frac{c}{d} \right)^2 - 2 \left(\frac{pa}{b} + \frac{qc}{d} \right)$$

$$(11) \quad = p^2 + q^2 + n - 2 \left(\frac{pad + qcb}{bd} \right).$$

Ainsi, PP'^2 peut s'écrire comme un quotient d'entiers de la forme $\frac{e}{bd}$; et puisque le choix de P' est tel que $0 < PP'^2 < 1$, alors on en déduit l'inégalité $0 < e < bd$.

En revenant aux coordonnées du point Q , on a

$$(12) \quad Q \left(p + \frac{(p^2 + q^2 - n)bd}{e} \left(p - \frac{a}{b} \right); q + \frac{(p^2 + q^2 - n)bd}{e} \left(q - \frac{c}{d} \right) \right),$$

ce qui montre qu'elles peuvent s'écrire comme des quotients d'entiers dont le dénominateur e est tel que $0 < e < bd$.

Si les coordonnées de Q ne sont pas entières, alors on recommence le procédé, avec Q' point à coordonnées entières le plus proche : le droite (QQ') recoupe le cercle (\mathcal{C}) en R , dont les coordonées pourront se mettre sous la forme d'un quotient d'entiers de dénominateur f , avec $0 < f < e < bd$. Un tel procédé doit se terminer, sans quoi on produirait ainsi une suite strictement décroissante d'entiers positifs... Ainsi, on pourra trouver un point à coordonnées entières sur le cercle (\mathcal{C}) . \square

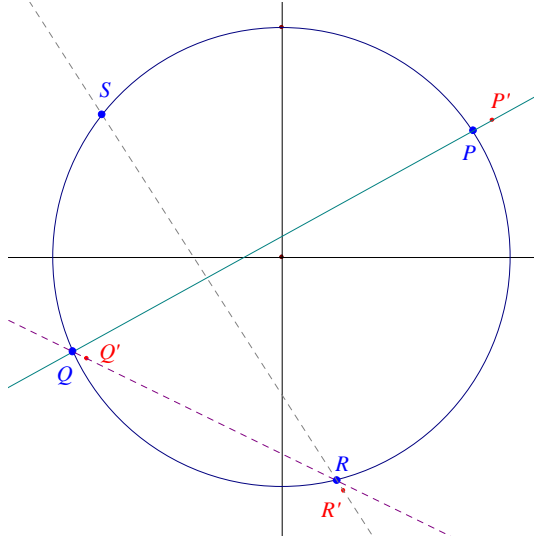


FIG. 1 – P point rationnel sur le cercle; P' point entier le plus proche, etc.