DÉCOMPOSITION D'UN NOMBRE PREMIER P≡1 (MOD 4) EN UNE SOMME DE DEUX CARRÉS

La démonstration du théorème de Bachet (A.P.M. 198) repose en partie sur la proposition suivante : Tout nombre premier $p \equiv 1 \bmod 4$ est égal à une somme de deux carrés. Voici une démonstration élémentaire assez peu connue de cette proposition.

Soit l'équation $x^2 + y^2 \equiv 0 \bmod p$ dans $\mathbf{Z}$ [p premier tel que $p \equiv 1 \bmod 4$] x et y premiers avec p. On peut trouver a tel que $x \equiv ay \bmod p$. En effet,

$$a^2y^2 + y^2 \equiv y^2(a^2 + 1) \equiv 0 \bmod p \Rightarrow a^2 + 1 \equiv 0 \bmod p \text{ car } (y, p) = 1.$$

Cette dernière congruence est possible puisque par hypothèse $\left(\frac{-1}{p}\right) = +1$.

Des solutions de $x^2 + y^2 \equiv 0 \bmod p$ sont donc de la forme $x = av + pu$ $y = v$, u et v entiers quelconques de Z.

Ce résultat peut s'interpréter dans un système orthonormé. M étant le point figuratif d'un couple-solution $\overrightarrow{OM} = v\vec{A} + u\vec{B}$ $\vec{A}(a, 1)$ $\vec{B}(p, 0)$.

Les points figuratifs des couples-solutions appartiennent donc à un réseau R construit sur les vecteurs $\vec{A}$ et $\vec{B}$.

Chaque parallélogramme du réseau R a une aire égale à p. Convenons d'associer à chaque parallélogramme un point de ce réseau, par exemple le sommet tel que $\begin{pmatrix} x \text{ minimum} \\ y \text{ minimum} \end{pmatrix}$

Soit un cercle [O, R] R assez grand contenant N sommets. Il existe un cercle de rayon $R + b > R$ aussi petit que possible et de centre O contenant les parallélogrammes dont les sommets sont intérieurs à [O, R].

Il existe aussi un cercle de rayon $R - a > R$ aussi grand que possible et de centre O complètement intérieur aux parallélogrammes coupés par [O, R] ; a et b majorés par $|\overrightarrow{OA} + \overrightarrow{OB}|$.

D'où
$$\pi(R - a)^2 \leqslant Np \leqslant \pi(R + b)^2,$$
$$\frac{\pi}{p}\left(1 - \frac{a}{R}\right)^2 \leqslant \frac{N}{R^2} \leqslant \frac{\pi}{p}\left(1 + \frac{b}{R}\right)^2$$
$$\lim_{R \to \infty} \frac{N}{R^2} = \frac{\pi}{p}.$$

Ceci posé, soit I $[x_0, y_0]$ le point du réseau le plus proche de l'origine, s sa distance à l'origine, c'est-à-dire la distance minimum entre deux points du réseau $s^2 = x_0^2 + y_0^2$.

Considérons les cercles centrés en chaque point du réseau et de rayon au plus égal à $\frac{s}{2}$. Cercles qui seront donc extérieurs les uns aux autres. Pour les cercles dont les centres sont intérieurs au cercle [O, R] on a

$$N\pi\left(\frac{s}{2}\right)^2 < \pi(R+b)^2 \Rightarrow s^2 < 4\frac{R^2}{N}\left(1 + \frac{b}{R}\right)^2$$

donc à la limite
$$s^2 < \frac{4p}{\pi} < 2p$$

et s^2 étant multiple de p on a nécessairement $s^2 = p = x_0^2 + y_0^2$.

J. Querré (*Brest*).