Théorème des deux carrés de Fermat

Théorème : Soit $\mathcal{A}_2 := \{x^2 + y^2 : x, y \in \mathbb{Z}\}$ et $n \in \mathbb{N}$. Alors $n \in \mathcal{A}_2$ si et seulement si pour tout nombre premier p, $p \equiv 3[4] \Rightarrow v_p(n) \equiv 0[2]$.

Lemme 0 : Si p est un nombre premier impair, -1 est un carré de $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1[4]$.

Lemme 1 : $X, Y \in \mathcal{A}_2 \Rightarrow XY \in \mathcal{A}_2$.

Lemme 2 : Si p est premier, $p \equiv 1[4] \Rightarrow p \in \mathcal{A}_2$.

Preuve lemme 0 : Admis.

Preuve lemme 1 : Soit $X = x_1^2 + x_2^2$ et $Y = y_1^2 + y_2^2$. On remarque alors que $X = |x_1 + ix_2|^2$ et $Y = |y_1 + iy_2|^2$ donc $XY = |(x_1y_1 - x_2y_2) + i(x_1y_2 + y_1x_2)|^2 = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + y_1x_2)^2$ d'où $XY \in \mathcal{A}_2$. $\square$

Preuve lemme 2 : Soit p premier impair tel que $p \equiv 1[4]$. Par le lemme 0 il existe $\bar{x} \in \mathbb{Z}/p\mathbb{Z}$ tel que $\bar{x}^2 = -1$. Ainsi, $x^2 + 1 \equiv 0[p]$ donc il existe $m \in \mathbb{Z}$ tel que $mp \in \mathcal{A}_2$. Quitte à prendre un relevé de $\bar{x}$ entre 0 et $p - 1$ on peut supposer que $0 \leq m < p$.

Soit $m_0 = \min\{m \in \mathbb{N} : mp \in \mathcal{A}_2\}$. On va montrer que $m_0 = 1$. Si $m_0 = 1$, c'est bon. Sinon on écrit $m_0 p = x^2 + y^2$.
On a alors ($m_0 \not| x$ ou $m_0 \not| y$) (sinon on aurait $m_0^2 | m_0 p$ donc $m_0 | p$, absurde car $1 < m_0 < p$).

Soit c, d les entiers les plus proches de $\dfrac{x}{m_0}$ et $\dfrac{y}{m_0}$. On note alors $x_1 = x - cm_0$ et $y_1 = y - cm_0$. On a alors

$$\begin{cases} |x_1| \leq \dfrac{m_0}{2},\ |y_1| \leq \dfrac{m_0}{2} \\ x_1^2 + y_1^2 > 0 \end{cases}$$

mais $x_1^2 + y_1^2 \equiv 0[m_0]$ donc il existe $m_1 > 0$ tel que $x_1^2 + y_1^2 = m_1 m_0$. Par ailleurs, $x_1^2 + y_1^2 \leq \dfrac{m_0^2}{2}$ donc $m_1 < \dfrac{m_0}{2} < m_0$.

On a alors $m_0^2 m_1 p = (x^2 + y^2)(x_1^2 + y_1^2) = (xx_1 + yy_1)^2 + (xy_1 - yx_1)^2$, les deux derniers termes étant divisibles par m_0. En effet, $xx_1 + yy_1 = x^2 + y^2 - m_0(c + d)$ et comme $x^2 + y^2$ est divisible par m_0, le tout est bien divisible par m_0. C'est la même chose pour le deuxième terme. On peut alors écrire

$$m_1 p = \left(\frac{xx_1 + yy_1}{m_0}\right)^2 + \left(\frac{(xy_1 - yx_1)}{m_0}\right)^2$$

et donc $m_1 p \in \mathcal{A}_2$, ce qui est absurde car m_0 était censé être minimal. On a alors $m_0 = 1$ et donc $p \in \mathcal{A}_2$.□

Preuve du théorème :

Condition Nécessaire : Soit $n = x^2 + y^2$ et p premier divisant n tel que $v_p(n) \equiv 1[2]$. On note $d = x \wedge y$ et $X = \frac{x}{d}$, $Y = \frac{y}{d}$. Ainsi, $n = d^2(X^2 + Y^2)$ et $p|X^2 + Y^2$ car $v_p(d^2)$ est forcément paire. On en déduit alors que $p \not| X$, sinon $p^2|X^2$ et donc $p|Y$, ce qui est absurde car X et Y sont premiers entre eux. On en déduit que $\bar{X}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$ et donc en multipliant par $(\bar{X}^{-1})^2$ on a la relation $\bar{1} + (\bar{Y}\bar{X}^{-1})2 = \bar{0}$ donc -1 est un carré modulo p donc $p \equiv 1[4]$ par le lemme 2 (on vient de montrer la contraposée de l'implication du théorème).

Condition suffisante : Soit $n \in \mathbb{N}$ et $p_1, ..., p_k$ les nombres premiers divisant n ayant une valuation impaire. On peut alors écrire $n = m^2 p_1 ... p_k$. Avec les hypothèses on sait que $p_i = 2$ ou $p_i \equiv 1[4]$ donc $p_i \in \mathcal{A}_2$ par le lemme 2 (il est clair que $2 \in \mathcal{A}_2$). Comme $m^2 = m^2 + 0^2$, n est produit d'élément de $\mathcal{A}_2$ donc par le lemme 1 n est dans $\mathcal{A}_2$.□

Remarques importantes :

- Il faut savoir démontrer le lemme 0 je pense.
- Il y a peut-être des flous sur quelques affirmations (notamment sur des divisibilités, écrivez bien tout au moins une fois).