Théorème des deux carrés

Florian BOUGUET

Référence : PERRIN : Cours d'algèbre

On cherche à caractériser les nombres s'écrivant comme une somme de deux carrés :

$$\Sigma = \left\{ n \in \mathbb{N} / n = a^2 + b^2 ; a, b \in \mathbb{N} \right\}$$

On notera $\mathbb{P}$ l'ensemble des nombres premiers de $\mathbb{N}$.

Theorème 1

Soit $n \in \mathbb{N}, n = \sum_{p \in \mathbb{P}} p^{\nu_p(n)}$
Alors

$$n \in \Sigma \Leftrightarrow \nu_p(n) \text{ est pair quand } p \equiv 3[4]$$

Avant de chercher à démontrer ce théorème, introduisons un lemme qui va s'avérer utile à la fin de la preuve :

Lemme 1

Soit $p \in \mathbb{P}, p > 2$. *Alors*

(i) x *est un carré modulo p si, et seulement si,* $x^{(p-1)/2} = 1$.

(ii) (-1) est un carré modulo p si, et seulement si, $p \equiv 1[4]$.

Preuve du lemme :

Remarquons d'abord que le cas $p = 2$ est évident, tous les éléments de $\mathbb{F}^2$ étant des carrés. Soit donc $p \in \mathbb{P}, p > 2$. Les nombres premiers différents de 2 sont évidemment impairs, on a donc $p \equiv 1$ ou $3[4]$. Remarquons enfin que :

$$(\star) \qquad \frac{(p-1)}{2} \text{ est pair } \Leftrightarrow p \equiv 1[4]$$

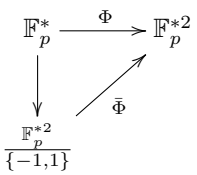
Notons $\mathbb{F}_p^{*2}$ l'ensemble des carrés de $\mathbb{F}_p^*$, c'est-à-dire des éléments inversibles de $\mathbb{F}_p$ s'écrivant comme carré d'un élément de $\mathbb{F}_p$. On va montrer que

$$x \in \mathbb{F}_p^{*2} \Leftrightarrow x^{(p-1)/2} = 1$$

Notons $A = \{x \in \mathbb{F}_p^* / x^{(p-1)/2} = 1\}$. Le polynôme $X^{(p-1)/2} - 1$ possède au plus $\frac{(p-1)}{2}$ racines, donc $|A| \leq \frac{(p-1)}{2}$. De plus, notons

$$\begin{array}{rccc} \Phi : & \mathbb{F}_p^* & \to & \mathbb{F}_p^{*2} \\ & x & \mapsto & x^2 \end{array}$$

Φ est évidemment surjectif, $\ker \Phi = \{\pm 1\}$ d'où la factorisation



$\bar{\Phi}$ est un isomorphisme, d'où $|\mathbb{F}_p^{*2}| = \frac{(p-1)}{2}$. Si $x \in \mathbb{F}_p^{*2}$, $x = y^2$

$$x^{(p-1)/2} = (y^2)^{(p-1)/2} = y^{p-1} = 1$$

Donc $\mathbb{F}_p^{*2} \subseteq A$, et donc $\mathbb{F}_p^{*2} = A$ par argument de cardinalité, ce qui démontre (i).

On déduit tout de suite (ii) de (i) par $(\star)$.

□

Preuve du théorème :
La fait important à remarquer à propos de Σ est que $a^2+b^2 = (a+ib)(a-ib)$. Cela nous invite donc naturellement à travailler dans l'anneau des entiers de GAUSS

$$\mathbb{Z}[i] = \{a + ib / a, b \in \mathbb{Z}\}$$

Cet anneau est euclidien grâce au stathme

$$N(a + ib) = (a + ib)(a - ib) = a^2 + b^2$$

Il est bon de savoir redémontrer que :
– $N(zz') = N(z)N(z')$ (immédiat)
– les éléments inversibles de $\mathbb{Z}[i]$ sont exactement les éléments de norme 1 : $1, -1, i, -i$.
On a donc la caractérisation suivante de Σ :

$$n \in \Sigma \Leftrightarrow \exists z \in \mathbb{Z}[i] \text{ tel que } n = N(z)$$

Notons que si $n = N(z), n' = N(z')$ alors $nn' = N\left(z\bar{z'}\right)$. Σ est donc stable par multiplication, ce qui nous invite à nous pencher sur $\mathbb{P} \cap \Sigma$. Démontrons l'équivalence suivante pour $p \in \mathbb{P}$:

$$p \in \Sigma \Leftrightarrow p \text{ est réductible dans } \mathbb{Z}[i]$$

En effet, si $p \in \Sigma, p = N(z) = z\bar{z}$. De plus $p = N(z) > 1$ donc z et $\bar{z}$ ne sont pas inversibles, donc p est réductible. Dans l'autre sens, si $p = zz'$ alors $N(p) = p^2 = N(z)N(z')$. Cette égalité a lieu dans $\mathbb{N}$ et $N(z), N(z') \neq 1$ donc $N(z) = N(z') = p$, donc $p \in \Sigma$, CQFD. Rappelons que

$$\frac{\mathbb{Z}[i]}{(p)} \simeq \frac{\mathbb{Z}[X]/(X^2+1)}{(p)} \simeq \frac{\mathbb{Z}[X]/(p)}{(X^2+1)} \simeq \frac{\mathbb{F}_p[X]}{(X^2+1)}$$

On a maintenant la suite d'équivalences suivante :

$$\begin{aligned}
p \text{ irréductible dans } \mathbb{Z}[i] &\Leftrightarrow (p) \text{ premier de } \mathbb{Z}[i] \\
&\Leftrightarrow \mathbb{Z}[i]/(p) \text{ intègre} \\
&\Leftrightarrow \frac{\mathbb{F}_p[X]}{(X^2+1)} \text{ intègre} \\
&\Leftrightarrow X^2+1 \text{ irréductible sur } \mathbb{F}_p \\
&\Leftrightarrow X^2+1 \text{ n'a pas de racine dans } \mathbb{F}_p \\
&\Leftrightarrow (-1) \text{ n'est pas un carré dans } \mathbb{F}_p
\end{aligned}$$

Autrement dit

$$p \in \Sigma \Leftrightarrow p \text{ est réductible dans } \mathbb{Z}[i] \Leftrightarrow (-1) \text{ est un carré modulo } p$$

En utilisant le lemme, en notant la stabilité par multiplication de Σ et en remarquant que les entiers au carré sont trivialement des éléments de Σ on pourra conclure la réciproque dans le théorème (ce qui n'est déjà pas mal).

Il nous reste donc à démontrer l'implication, ce qui sera rapide compte tenu du travail préalablement fourni. En effet, soit $n = a^2+b^2 \in \Sigma$ et soit $p \in \mathbb{P}, p \equiv 3[4]$. Si $\nu_p(n) = 0$, le résultat est vrai. Sinon, cela signifie que p divise n. Remarquons alors que, puisque $p \equiv 3[4]$, p est irréductible dans $\mathbb{Z}[i]$. p divise $(a+ib)(a-ib)$ donc p divise (par

exemple) $a+ib$. p étant réel, p divise a et b. On peut noter $a = pa'$ et $b = pb'$. Alors $n = a^2 + b^2 = p^2(a'^2 + b'^2)$ donc

$$\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma \text{ et } \nu_p\left(n/p^2\right) = \nu_p(n) - 2$$

Par récurrence, on peut donc montrer que $\nu_p(n)$ est paire, ce qui conclut le théorème.

□