Sandrine CARUSO

Entiers de Gauss et somme de deux carrés

Référence(s) : Oraux X-ENS, Francinou-Ginanella-Nicolas, algèbre 1, p 98
Perrin ?

Théorème. *Soit p un nombre premier. Alors p est somme de deux carrés (dans $\mathbb{Z}$) si et seulement si $p = 2$ ou $p \equiv 1 \pmod 4$.*

On considère l'anneau des entiers de Gauss $\mathbb{Z}[i] = \{u + iv, u, v \in \mathbb{Z}\}$. Soit

$$\begin{array}{rccc} N : & \mathbb{Z}[i] & \to & \mathbb{N} \\ & z & \mapsto & z\bar{z} = |z|^2 \end{array} .$$

Les éléments inversibles de $\mathbb{Z}[i]$ sont les z tels que $N(z) = 1$, c'est-à-dire $\pm 1, \pm i$. En effet, si $z \in \mathbb{Z}[i]$ est inversible, $1 = N(zz^{-1}) = N(z)N(z^{-1})$, donc $N(z)$ est inversible dans $\mathbb{Z}$, donc $N(z) = 1$. Inversement, si $N(z) = 1$, alors $z\bar{z} = 1$ et z est inversible d'inverse $\bar{z}$.

Montrons que l'anneau $\mathbb{Z}[i]$ est euclidien pour N. Soient $a, b \in \mathbb{Z}[i]$, $b \neq 0$. Le nombre $\frac{a}{b}$ est un nombre complexe, soit x sa partie réelle et y sa partie imaginaire. Soit u l'entier le plus proche de x, v l'entier le plus proche de y. On pose $q = u + iv$, et $r = a - qb$. Alors on a :

$$\begin{aligned} N(r) &= N(a - qb) = N(b) \times \left|\frac{a}{b} - q\right|^2 = N(b) \times \left((x-u)^2 + (y-v)^2\right) \\ &\leqslant N(b)\left(\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2\right) < N(b), \end{aligned}$$

et bien entendu, $a = qb + r$.

Montrons maintenant que p est somme de deux carrés si et seulement si il n'est plus irréductible dans $\mathbb{Z}[i]$.

☞ Si $p = u^2 + v^2$, $u, v \in \mathbb{Z}$, alors $p = (u + iv)(u - iv)$. De plus, $u \pm iv$ sont non inversibles car $N(u \pm iv) = p \neq 1$. Donc p n'est pas irréductible dans $\mathbb{Z}[i]$.

☞ Si $p = zz'$ avec z et z' non inversibles, alors $p^2 = N(p) = N(z)N(z')$, mais comme $N(z)$ et $N(z')$ sont différents de 1 et que p est premier, on a nécessairement $N(z) = N(z') = p$. Ainsi, si $z = u + iv$, $p = u^2 + v^2$ est somme de deux carrés.

Essayons donc de caractériser les premiers de $\mathbb{Z}$ qui restent irréductibles dans $\mathbb{Z}[i]$. Le nombre p est irréductible dans $\mathbb{Z}[i]$ si et seulement s'il est premier, car $\mathbb{Z}[i]$ est euclidien donc factoriel, *ie* si et seulement si l'anneau $\mathbb{Z}[i]/(p)$ est intègre. On a

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

et $\mathbb{F}_p[X]/(X^2+1)$ est intègre si et seulement si X^2+1 est irréductible dans $\mathbb{F}_p[X]$, donc si et seulement si il n'a pas de racine puisqu'il est de degré 2, c'est-à-dire si et seulement si -1 n'est pas un carré dans $\mathbb{F}_p$.

Cherchons une condition nécessaire et suffisante sur p pour que -1 soit un carré dans $\mathbb{F}_p$. Si $p=2$, alors $-1=1=1^2$. Supposons maintenant $p \equiv 1 \pmod 4$, et soit k tel que $p=4k+1$. L'équation $x^{\frac{p-1}{2}}=1$ a au plus $\frac{p-1}{2}$ solutions dans $\mathbb{F}_p^*$; or, $p-1>\frac{p-1}{2}$ donc il existe $y \in \mathbb{F}_p^*$ tel que $y^{\frac{p-1}{2}} \neq 1$. Mais comme de plus, $y^{p-1}=1$ par le petit théorème de Fermat, on en déduit que $y^{\frac{p-1}{2}}=-1$. Cela donne $y^{2k}=-1$ et donc y^k est une racine carré de -1.

Inversement, si $-1=x^2$ avec $x \in \mathbb{F}_p$, alors soit $p=2$, soit $(-1)^{\frac{(p-1)}{2}}=x^{p-1}=1$ (petit théorème de Fermat). Si $p \neq 2$, $1 \neq -1$ et donc le fait que $(-1)^{\frac{(p-1)}{2}}=1$ implique que $\frac{p-1}{2}$ est pair, c'est-à-dire que $p \equiv 1 \pmod 4$.

Au final, on a montré les équivalences suivantes : p est somme de deux carrés si et seulement si il n'est pas irréductible dans $\mathbb{Z}[i]$, si et seulement si -1 a une racine carrée dans $\mathbb{F}_p$, si et seulement si $p=2$ ou $p \equiv 1 \pmod 4$. C'est bien ce que l'on voulait.

Remarque. On aurait pu montrer plus directement le sens direct : si p est somme de deux carrés, comme il carré est congru à 0 ou 1 modulo 4, p est congru à 0, 1 ou 2 modulo 4. Le premier cas est exclus car p est premier donc pas multiple de 4. Le dernier cas donne p pair donc $p=2$.