Théorème des deux carrés de Fermat

Leçons concernées

* **121 :** Nombres premiers. Applications.
* **122 :** Anneaux principaux. Applications.
* **126** Exemples d'équations en arithmétique.

Réference

* *Perrin - Cours d'algèbre*

Le but de ce développement est de donner une condition nécessaire et suffisante pour qu'un entier n soit somme de deux carrés. Notons Σ l'ensemble de tels entiers.

Pour cela, nous allons travailler avec $\mathbb{Z}[i]$ des entiers de Gauss. On commence par un premier lemme :

Lemme. *L'anneau $\mathbb{Z}[i]$ est un anneau euclidien. Il est donc en particulier principal. Un élément z de cet ensemble est inversible si et seulement si $N(z) = z\overline{z} = 1$.*

Démonstration. Soient x et y deux entiers de Gauss. On écrit $\frac{x}{y} = \alpha + i\beta$ dans $\mathbb{C}$ et on prends $q_1, q_2 \in \mathbb{Z}$ tels que $|q_1 - \alpha| \leq \frac{1}{2}$ et $|q_2 - \beta| \leq \frac{1}{2}$. Soient alors $q = q_1 + iq_2 \in \mathbb{Z}[i]$ et $r = x - yq \in \mathbb{Z}[i]$. Alors $x = yq + r$ et si $r \neq 0$, $N(r) = N(y)N(\frac{x}{y} - q) \leq \frac{1}{2}N(y) < N(y)$ car $N(y) \neq 0$ sans que $r = 0$. L'anneau est ainsi euclidien, de stathme N.

Maintenant, un entier de Gauss $z \neq 0$ est inversible si et seulement si $z^{-1} \in \mathbb{Z}[i]$. Or, si $N(z) = 1$, $z\overline{z} = 1$ donc $z^{-1} = \overline{z} \in \mathbb{Z}[i]$. Réciproquement, si $z^{-1} \in \mathbb{Z}[i]$, $zz^{-1} = 1$ donc en passant à la norme on trouve $N(z) = 1$ puisque c'est un entier positif diviseur de 1. □

Ceci étant démontré, on prouve un deuxième lemme :

Lemme. *Soit p un nombre premier. Alors $p \in \Sigma$ si et seulement si p est réductible dans $\mathbb{Z}[i]$.*

Démonstration. Si $p = a^2 + b^2$ est dans Σ, alors $p = (a + ib)(a - ib)$. Or, les normes de chacun de ces deux éléments sont égaux à p qui est distinct de 1. Donc, d'après le lemme, p s'écrit comme produit de deux éléments non inversibles dans l'anneau des entiers de Gauss, il est donc réductible.
Réciproquement, écrivons $p = (x + iy)(a + ib)$ comme produit de deux entiers de Gauss non inversibles. En passant à la norme, on trouve $p^2 = (a^2 + b^2)(x^2 + y^2)$. Le premier terme est donc un diviseur de p^2, mais distinct de 1, car $a + ib$ n'est pas inversible, et distinct de p^2, sinon $x + iy$ serait inversible. En conséquence, $p = a^2 + b^2$.

□

On peut enfin passer au premier théorème :

Théorème. *Un entier premier p est somme de deux carrés si et seulement si $p = 2$ ou $p = 1[4]$.*

Démonstration. On sait que $\mathbb{Z}[i]$ est un anneau principal. Donc, p est réductible si et seulement si $\dfrac{\mathbb{Z}[i]}{(p)}$ n'est pas un corps. Or, on a les isomorphismes, issu du théorème d'isomorphisme :

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

On en déduit que p est somme de deux carrés si et seulement si -1 est un carré modulo p. Et il est connu alors que -1 est un carré si et seulement si $p = 2$ (tous les éléments de $\mathbb{F}_2$ sont des carrés) ou $p = 1[4]$ car il faudrait $(-1)^{\frac{p-1}{2}} = 1$, ce qui montre le théorème.

□

On passe maintenant au résultat central de ce développement :

Théorème. *Soit $n = \prod_{k=1}^{r} p_k^{n_k}$ un entier écrit dans sa décomposition en produit de facteurs premiers. Alors $n \in \Sigma$ si et seulement si pour tout $k \in [\![1; r]\!]$, si $p_k = 3[4]$ alors n_k est pair.*

Démonstration. Faisons plusieurs remarques avant de démontrer ce théorème. Tout d'abord, Σ contient les nombres carrés. Ensuite, Σ est stable par produit. En effet, cela vient du fait que si z_1, z_2 sont des entiers de Gauss, alors $N(z_1)N(z_2) = N(z_1 z_2)$. Ainsi, puisque tout entier de Σ s'écrit comme étant la norme N d'un certain entier de Gauss, on a effectivement la stabilité par produit.
Ces deux remarques permettent alors de montrer le sens réciproque du théorème, d'après le lemme précédent. En effet, si $p_k = 2$ ou $p_k = 1[4]$, c'est un élément de Σ d'après le théorème précédent, et donc $p_k^{n_k} \in \Sigma$ par stabilité par produit. Si jamais par hasard $p_k = 3[4]$, fort heureusement, n_k est pair et $p_k^{n_k}$ est alors un carré, et donc un élément de Σ. Ainsi, au final, $n \in \Sigma$.

Pour le sens direct, écrivons $n = a^2 + b^2$ et supposons par l'absurde que, pour un certain k, $p_k = 3[4]$ et que n_k soit impair. D'après le théorème précédent, p_k est irréductible dans l'anneau des entiers de Gauss (sinon il serait un carré, ce qui est exclut d'après l'égalité qu'il vérifie). Or, p_k divise $n = (a - ib)(a + ib)$. Puisqu'il est irréductible, il est premier, donc p_k divise l'un ou l'autre des facteurs. Mais puisque c'est un entier (tout court), en écrivant la définition cela équivaut à dire que p_k divise a et b. Donc p_k^2 divise $a^2 + b^2 = n$, et le quotient vérifie $\dfrac{n}{p_k^2} = \left(\dfrac{a}{p_k}\right)^2 + \left(\dfrac{b}{p_k}\right)^2 \in \Sigma$ et on a baissé la valuation de p_k de 2.

On voit alors que dès qu'il y a encore un facteur p_k, il y en a automatiquement un deuxième, et le quotient par p_k^2 est encore dans Σ. Donc, peut réitérer ce raisonnement si il y a encore un p_k en facteur. Ce processus se terminant, puisque la valuation est finie, cette dernière doit nécessairement être pair puisque nous ne faisons que de baisser la valuation de 2 à chaque étape.

□

Remarque : Détaillons un peu les deux isomorphismes qu'on a utilisé. Puisque $\mathbb{Z}[i] \simeq \dfrac{\mathbb{Z}[X]}{(X^2+1)}$, il suffit de prouver l'isomorphisme en remplaçant $\mathbb{Z}[i]$ par ce quotient. Posons : $\forall P \in \mathbb{Z}[X], \varphi(P) = \overline{\overline{P(X)}} \in \dfrac{\frac{\mathbb{Z}[X]}{(X^2+1)}}{(p)}$ (on vérifie bien sûr aisément que cette application est bien définie). Cette application, linéaire, est bien une surjection. Ce qui reste compliqué, c'est l'injectivité. Si $P \in \operatorname{Ker} \varphi$, alors $\overline{P(X)} \in (p)$. Donc il existe un élément $\overline{Q(X)} \in \dfrac{\mathbb{Z}[X]}{(X^2+1)}, P(X) = p\overline{Q(x)}$. Donc, il existe $R(X) \in \mathbb{Z}$ tel que $P(X) = pQ(X) + R(X)(X^2+1)$. Donc

$P \in (p, X^2 + 1)$. Réciproquement, tout élément de cet idéal est dans le noyau, et on conclut par théorème d'isomorphisme.
On déduit l'autre isomorphisme de la même manière.