Développement: Théorème des deux carrés

Adrien Fontaine

8 avril 2013

Référence : Daniel Perrin, Cours d'algèbre p56

1 Introduction

Le problème est de déterminer quels entiers $n \in \mathbb{N}$ sont somme de deux carrés : $n = a^2 + b^2$ avec $a, b \in \mathbb{N}$. On pose :

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

Remarquons tout d'abord que si $n \equiv 3[4]$, on a $n \notin \Sigma$. En effet, si a est pair, alors $a^2 \equiv 0[4]$ et si a est impair, $a^2 \equiv 1[4]$, donc $a^2 + b^2 \equiv 0, 1, 2[4]$.
L'idée que nous allons utiliser pour étudier Σ est de noter que si $n \in \Sigma$, $n = a^2 + b^2$, n s'écrit dans $\mathbb{C}$ $n = (a+ib)(a-ib)$, et que cette relation a lieu en fait, dans l'anneau $\mathbb{Z}[i]$ des entiers de Gauss :

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

En particulier, si $p \in \mathbb{N}$ est un nombre premier, qui est somme de deux carrés, p n'est plus irréductible dans $\mathbb{Z}[i]$. C'est le cas par exemple de

$$5 = (2 + i)(2 - i)$$

2 Étude de l'anneau $\mathbb{Z}[i]$

Tout d'abord $\mathbb{Z}[i]$ est un anneau intègre, puisqu'il est inclus dans $\mathbb{C}$. Définissons une "norme" sur $\mathbb{Z}[i]$ par :

$$\forall z = a + ib \in \mathbb{Z}[i], N(z) = z\bar{z} = a^2 + b^2 \in \mathbb{N}$$

Il est clair que la norme N est multiplicative. Cette propriété permet de calculer les inversibles de $\mathbb{Z}[i]$:

Proposition 1

On a $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

Démonstration : En effet, si $z \in \mathbb{Z}[i]^\times$, il existe $z' \in \mathbb{Z}[i]^\times$ tel que $zz' = 1$. D'où, $1 = N(1) = N(zz') = N(z)N(z')$. Donc, $N(z)$ est inversible dans $\mathbb{Z}$ et positif, donc $N(z) = 1$. Il ne reste plus qu'à résoudre dans $\mathbb{Z}^2$, l'équation $a^2 + b^2 = 1$. On trouve que les seules solutions sont $(\pm 1, 0)$ et $(0, \pm i)$. Donc,

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$$

■

Cette propriété permet également d'établir un résultat, qui, à la main, peut s'avérer particulièrement fastidieux à démontrer :

Proposition 2

L'ensemble Σ des entiers somme de deux carrés est stable par multiplication.

Démonstration : En effet, si a^2+b^2 et $c^2+d^2 \in \Sigma$. Posons $z_1 = a+ib$ et $z_2 = c+id \in \mathbb{Z}[i]$. On a :

$$N(z_1 z_2) = N((ac-bd)+i(ad+bc)) = (ac-bd)^2+(ad+bc)^2$$

Et

$$N(z_1 z_2) = N(z_1)N(z_2) = (a^2+b^2)(c^2+d^2)$$

On en déduit l'identité dite de Lagrange :

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2$$

■

Cette propriété permet de ramener essentiellement l'étude de Σ à la détermination des nombres premiers p de $\mathbb{N}$ qui sont dans Σ (grâce à la décomposition d'un entier en produit de facteurs premiers). Pour cela, il nous faut étudier la structure arithmétique de $\mathbb{Z}[i]$. On a la proposition suivante :

Proposition 3

L'anneau $\mathbb{Z}[i]$ est euclidien, avec pour stathme la "norme" N. En particulier, $\mathbb{Z}[i]$ est principal.

Démonstration : Soient $z_1, z_2 \in \mathbb{Z}[i]$ non nuls. On commence par faire la division de z_1 par z_2 dans le corps $\mathbb{C}$. Si on écrit $z_1 = a+ib$ et $z_2 = c+id$, alors a,b,c,d étant dans $\mathbb{Z}$, on peut écrire

$$\frac{z_1}{z_2} = P+iQ \text{ où } P,Q \in \mathbb{Q}$$

(plus précisément, on a $P = \frac{ac+bd}{c^2+d^2}$ et $Q = \frac{bc-ad}{c^2+d^2}$). Par ailleurs, il existe $x,y \in \mathbb{Z}$ et $\alpha,\beta \in \mathbb{Q}$ tels que

$$P = x+\alpha \text{ et } Q = y+\beta \text{ avec } |\alpha| \leq \frac{1}{2} \text{ et } |\beta| \leq \frac{1}{2}$$

Donc, on a :

$$\frac{z_1}{z_2} = (x+iy)+(\alpha+i\beta)$$

D'où,

$$z_1 = z_2(x+iy)+(\alpha+i\beta)z_2 = z_2 q + r \text{ où } q = x+iy \text{ et } r = (\alpha+i\beta)z_2$$

Par ailleurs, comme z_2, z_2 et $x+iy$ sont dans $\mathbb{Z}[i]$, on a ($\mathbb{Z}[i]$ étant bien sûr un anneau) $r \in \mathbb{Z}[i]$. Enfin, on a :

$$N(q) = N((\alpha+i\beta)z_2) = (\alpha^2+\beta^2)N(z_2) \leq (\frac{1}{4}+\frac{1}{4})N(z_2) < N(z_2)$$

Donc, N est bien un stathme pour $\mathbb{Z}[i]$. ■

On est maintenant en mesure de prouver le théorème principal de ce paragraphe. On a :

Théorème 1

Soit $p \in \mathbb{N}$ un nombre premier. On a l'équivalence :

$$p \in \Sigma \Leftrightarrow p = 2 ou p \equiv 1[4]$$

Démonstration : La condition est bien sûr nécessaire, car un nombre premier impair est congru soit à 1 soit à 3 modulo 4, et on a vu que si $p \equiv 3[4]$ alors $p \notin \Sigma$.
Pour la réciproque, on établit d'abord le lemme suivant :

Lemme 1

On a :

$$p \in \Sigma \Leftrightarrow p \text{ n'est pas irréductible dans } \mathbb{Z}[i]$$

Démonstration : Pour le sens direct, il suffit d'écrire $p = a^2 + b^2 = (a + ib)(a - ib)$ et de remarquer que a et b sont non nuls, de sorte que ni $a + ib$, ni $a - ib$ ne sont dans $\mathbb{Z}[i]^\times$. Donc, p n'est pas irréductible. Pour le sens indirect : si $p = zz'$ avec $z, z' \neq \pm 1, \pm i$. On a $N(p) = N(z)N(z') = p^2$. De plus, $N(z)$ et $N(z') \neq 1$, on a donc $N(z) = p$. Donc, $p \in \Sigma$. ■

Poursuivons maintenant la preuve du théorème. Comme $\mathbb{Z}[i]$ est principal, dire p est non irréductible, revient exactement à dire que l'idéal principal $(p) = p\mathbb{Z}[i]$ est non premier, donc que le quotient $\mathbb{Z}[i]/(p)$ est non intègre. Par ailleurs, on dispose de l'isomorphisme,

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

Donc,

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

On a donc les équivalences suivantes :

$$(p) \text{ non premier } \Leftrightarrow X^2 + 1 \text{ non irréductible dans } \mathbb{F}_p[X] \Leftrightarrow X^2 + 1 \text{ a une racine dans } \mathbb{F}_p$$

Grâce au lemme ci-dessus, on en déduit :

$$p \in \Sigma \Leftrightarrow -1 \text{ est un carré dans } \mathbb{F}_p$$

Il reste à montrer que -1 est un carré dans $\mathbb{F}_p$, si et seulement si, $p = 2$ ou $p \simeq 1[4]$.
Or, $p \equiv 1[4]$ revient à dire que le cardinal de $(\mathbb{F}_p^\times)^2$, i.e $\frac{p-1}{2}$ est pair. Or, un groupe d'ordre pair, contient des éléments d'ordre 2 (théorème de Sylow par exemple, ou voir le lemme en annexe). Un tel élément est un x tel que $x^2 = 1$ et $x \neq 1$, c'est donc nécessairement -1. On a donc bien $p \equiv 1[4] \Leftrightarrow -1 \in (\mathbb{F}_p^\times)^2$.
Ce qui achève la démonstration. ■

On peut maintenant achever l'étude de Σ.

Théorème 2

Soit $n \geq 2$. On décompose n en facteurs premiers :

$$n = \prod_{p \in P} p^{v_p(n)}$$

Alors, on a $n \in \Sigma \Leftrightarrow v_p(n)$ est pair pour $p \equiv 3[4]$.

Démonstration : Le sens indirect est clair, d'après la stabilité par multiplication de Σ et le théorème que l'on vient de démontrer.
Pour le sens direct, on suppose que $n \in \Sigma$. Soit $p \equiv 3[4]$. On montre par récurrence sur $v_p(n)$ que $v_p(n)$ est pair. Si $v_p(n) = 0$, c'est clair. Sinon, $p|(a^2 + b^2) = (a + ib)(a - ib)$, mais comme p est irréductible dans $\mathbb{Z}[i]$, p divise par exemple $a + ib$ (lemme d'Euclide). Mais alors, comme p est entier, on a $p|a$ et $p|b$. Donc $p^2|n$, et si on écrit $a = pa'$ et $b = pb'$, on a $\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma$. Mais, $v_p(\frac{n}{p^2}) = v_p(n) - 2$ est pair,d'après l'hypothèse de récurrence donc aussi $v_p(n)$. ■

3 Annexe

Montrons qu'un groupe d'ordre pair contient des éléments d'ordre 2.
Soit G un groupe d'ordre pair. Soit $X = \{g \in G, g^2 = 1\}$. X est non vide car il contient 1. De plus, les éléments de $G \setminus X$ peuvent être rangés par pair $\{g, g^{-1}\}$. On a donc, $|G| \equiv |X|[2]$. En pariculier, $|x| \geq 2$. Donc, G contient des éléments d'ordre 2.