Théorème des deux carrés

Lemme 1. L'anneau $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b,\ a, b \in \mathbb{Z}\}$ est euclidien, de stathme multiplicatif $N : a + \mathrm{i}b \mapsto a^2 + b^2$.

Démonstration. Soient $z \in \mathbb{Z}[\mathrm{i}]$ et $t \in \mathbb{Z}[\mathrm{i}]\backslash\{0\}$. Notons $z/t = x + \mathrm{i}y \in \mathbb{C}$. En choisissant a et b les entiers les plus proches de x et y respectivement et en notant $q = a + \mathrm{i}b$, il vient :

$$\left|\frac{z}{t} - q\right| \leq \frac{\sqrt{2}}{2} < 1.$$

Ainsi, en posant $r = z - qt = t(z/t - q)$, on conclut en observant que $N(r) < N(t)$ puisque $|r| < |t|$. $\square$

Lemme 2. Les inversibles de $\mathbb{Z}[\mathrm{i}]$ sont donnés par $\mathbb{Z}[\mathrm{i}]^\times = \{\pm 1, \pm \mathrm{i}\}$.

Démonstration. On a clairement l'inclusion $\{\pm 1, \pm \mathrm{i}\} \subset \mathbb{Z}[\mathrm{i}]^\times$. D'autre part, tout inversible de $\mathbb{Z}[\mathrm{i}]$ est de norme 1 (car de norme inversible dans $\mathbb{N}$), ce qui donne l'inclusion réciproque. $\square$

Lemme 3. Notons $\Sigma = \{n \in \mathbb{N} \mid \exists a, b \in \mathbb{N}, n = a^2 + b^2\}$. Un nombre premier impair p appartient à Σ si et seulement si p est réductible dans $\mathbb{Z}[\mathrm{i}]$.

Démonstration. Si $p = a^2 + b^2 = (a + \mathrm{i}b)(a - \mathrm{i}b)$, alors p est réductible dans $\mathbb{Z}[\mathrm{i}]$, en distinguant les cas où $a = 0$ ou $b = 0$. Réciproquement, si $p = zz'$ est une réduction non triviale de p, alors $N(p) = N(z)N(z') = p^2$, ce qui entraîne nécessairement que $p = N(z) \in \Sigma$. $\square$

Lemme 4. Un élément $x \in \mathbb{F}_p$ est un carré de $\mathbb{F}_p$ si et seulement si $x^{\frac{p-1}{2}} = 1$.

Démonstration. Notons $X = \{x \in \mathbb{F}_p,\ x^{\frac{p-1}{2}} = 1\}$. Tout d'abord, $|X| \leq \frac{p-1}{2}$. Si x est un carré dans $\mathbb{F}_p^\times$, alors $x \in X$. De plus, l'application $x \in \mathbb{F}_p^\times \mapsto x^2 \in \mathbb{F}_p^2\backslash\{0\} \subset X$ a pour noyau $\{\pm 1\}$, donc $|\mathbb{F}_p^2\backslash\{0\}| = \frac{p-1}{2}$. Ainsi, par cardinalité, X est l'ensemble des carrés non nuls de $\mathbb{F}_p$. $\square$

Théorème 5. Soit p premier impair. Avec les notations précédentes, $p \in \Sigma \iff p \equiv 1\ [4]$.

Démonstration. En reprenant le résultat d'un lemme précédent, $p \in \Sigma$ si et seulement si $\mathbb{Z}[\mathrm{i}]/(p)$ est non intègre. Or, $\mathbb{Z}[\mathrm{i}] \simeq \mathbb{Z}[X]/(X^2+1)$, donc $\mathbb{Z}[\mathrm{i}]/(p) \simeq \mathbb{F}_p[X]/(X^2+1)$ donc $p \in \Sigma$ si et seulement si $X^2 + 1$ est réductible dans $\mathbb{F}_p[X]$, i.e. si $X^2 + 1$ admet une racine dans $\mathbb{F}_p$. Ainsi, $p \in \Sigma$ si et seulement si -1 est un carré dans $\mathbb{F}_p$. D'apès un lemme précédent, -1 est un carré dans $\mathbb{F}_p$ si et seulement si $(-1)^{\frac{p-1}{2}} = 1$, i.e. si et seulement si $p \equiv 1\ [4]$. $\square$

Corollaire 6. En notant $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$, on a la caractérisation suivante :

$$n \in \Sigma \iff \big(\forall p \in \mathcal{P},\ p \equiv 3\ [4] \implies \nu_p(n) \equiv 0\ [2]\big).$$

Démonstration. Commençons par remaruqer que Σ est stable par multiplication, par propriété de N. Traitons d'abord le sens direct. Supposons $n = a^2 + b^2 \in \Sigma$. Soit $p \in \mathcal{P}$ tel que $p \equiv 3\ [4]$. Le théorème précédent assure que p est irréductible dans $\mathbb{Z}[\mathrm{i}]$. Si $\nu_p(n) = 0$, alors il n'y a rien à montrer. Sinon, puisque $p | n = a^2 + b^2 = (a + \mathrm{i}b)(a - \mathrm{i}b)$, par irréductibilité, $p | a + \mathrm{i}b$ ou $p | a - \mathrm{i}b$, ce qui entraîne (par conjugaison), que $p | a$ et $p | b$, donc $p^2 | n$. De là :

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

Par récurrence, on montre alors que $\nu_p(n)$ est pair. Pour la réciproque, il suffit d'écrire :

$$n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)} = \left(\prod_{p \equiv 3\ [4]} p^{\nu_p(n)/2}\right)^2 \left(\prod_{p \not\equiv 3\ [4]} p^{\nu_p(n)}\right)$$

qui est un produit d'un carré et d'une somme de deux carrés, ce qui suffit pour conclure $n \in \Sigma$. $\square$