DVP Théorème des deux carrés de Fermat par les entiers de Gauss

Antoine Dequay

21 septembre 2022

Notes

— Prof : Lionel Fourquaux.

— Leçons : 121, 126.

— Références :

  — Isenmann.

Rappel 1 Soit $p \in \mathcal{P}$, $p > 2$. Alors $x \in \mathbb{F}_p^*$ est un carré modulo $\mathbb{F}_p$ si et seulement si $x^{\frac{p-1}{2}} = 1$.

Rappel 2 Soit $p \in \mathcal{P}$. Alors -1 est un carré de $\mathbb{F}_p$ si et seulement si $p = 2$ ou $p \equiv 1 \ (mod\ 4)$.

Notation On note $\Sigma := \left\{x^2 + y^2, (x, y) \in \mathbb{N}^2\right\}$ et $N(z) = z\overline{z} = a^2 + b^2$ pour $z = a + \imath b \in \mathbb{Z}[\imath]$.

Théorème 3 Soit $n \in \mathbb{N}^*$. Alors $n \in \Sigma$ si et seulement si $v_p(n)$ est pair pour tout $p \in \mathcal{P}$ tel que $p \equiv 3 \ (mod\ 4)$.

Preuve. **Lemme 4** L'ensemble Σ est stable par multiplication et on a $p \equiv 3 \ (mod\ 4) \implies p \notin \Sigma$.

Preuve. Soient $(n, n') \in \Sigma^2$, il existe donc $(z, z') \in \mathbb{Z}[\imath]^2$ tel que $n = N(z)$ et $n' = N(z')$. Alors $nn' = N(z)N(z') = N(zz')$ par multiplicativité de N, d'où le premier résultat.

Remarque On a la formule explicite, dite *identité de* DIOPHANTE :

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

Pour le second résultat, comme $0^2 \equiv 2^2 \ (mod\ 4) \equiv 0 \ (mod\ 4)$ et $1^2 \equiv 3^2 \ (mod\ 4) \equiv 1 \ (mod\ 4)$, on a : $N(z) \equiv 0, 1, 2 \ (mod\ 4)$ pour $z \in \mathbb{Z}[\imath]$, d'où le résultat par son équivalence avec sa contraposée.

□

Lemme 5 On a $\mathbb{Z}[\imath]^* = \{1, -1, \imath, -\imath\}$ et $\mathbb{Z}[\imath]$ est euclidien.

Preuve. Soit $u \in \mathbb{Z}[\imath]^*$ et v son inverse. Alors on a $N(uv) = \underbrace{N(u)}_{\in\mathbb{N}}\underbrace{N(v)}_{\in\mathbb{N}} = 1$. Donc $N(u) = a^2+b^2$, ce qui prouve l'inclusion directe. L'inclusion réciproque est immédiate.

Il reste à prouver que N est un stathme euclidien de $\mathbb{Z}[\imath]$. Soit donc $(z, t) \in \mathbb{Z}[\imath]^2$ avec $t \neq 0$. On cherche $(q, r) \in \mathbb{Z}[\imath]^2$ tels que $z = qt + r$ et $N(r) < N(t)$. Posons $\dfrac{z}{t} = x + \imath y$ et $q = a + \imath b$ avec $(a, b) \in \mathbb{Z}^2$ tels que $|x - a| \leq \dfrac{1}{2}$ et $|y - b| \leq \dfrac{1}{2}$. Alors $\left|\dfrac{z}{t} - q\right|^2 = (x - a)^2 + (y - b)^2 \leq \dfrac{1}{2}$. Alors, avec $r = z - qt$, on a bien vérifié toutes les conditions, car alors $N(r) = |t|^2\left|\dfrac{z}{t} - q\right|^2 < |t|^2 = N(t)$.

□

Proposition 6 Soit $p \in \mathcal{P}$. Alors $p \in \Sigma \iff p$ n'est pas irréductible dans $\mathbb{Z}[\imath]$.

Preuve. Soit $p \in \Sigma$. Alors il existe $(a, b) \in \mathbb{Z}^2$, tel que $p = (a + \imath b)(a - \imath b)$. Comme a et b sont non-nuls, les deux facteurs ne sont pas inversibles par le lemme 5, donc p n'est pas irréductible dans $\mathbb{Z}[\imath]$.

Réciproquement, si $p = uv$ avec u et v non inversibles dans $\mathbb{Z}[\imath]$, alors $N(p) = p^2 = \underbrace{N(u)}_{\neq 1}\underbrace{N(v)}_{\neq 1}$ car u et v ne sont pas inversibles, donc $N(u) = N(v) = p$ par primalité de p. D'où $p \in \Sigma$.

□

Supposons $v_p(n)$ pair pour tout p premier tel que $p \equiv 3 \ (mod\ 4)$. Montrons que $p^{v_p(n)} \in \Sigma$, pour $p \in \mathcal{P}$. Par stabilité par multiplication de Σ (lemme 4), on aura bien $n \in \Sigma$.

Si $p \equiv 3 \ (mod\ 4)$, alors $p^{v_p(n)} = \left(p^{\frac{v_p(n)}{2}}\right)^2 \in \Sigma$.

Si $p \equiv 1, 2 \ (mod\ 4)$, alors, d'après le rappel, -1 est admet une racine a dans $\mathbb{F}_p$. Donc p divise $a^2 + 1 = (a + \imath)(a - \imath)$, mais pas $a \pm \imath$, donc p n'est pas premier dans $\mathbb{Z}[\imath]$ qui est euclidien par le lemme 5. Donc p n'est pas irréductible. La proposition permet de conclure ce sens.

Réciproquement, supposons $n \in \Sigma$. Soit $p \in \mathcal{P}$ un diviseur de n tel que $p \equiv 3 \ (mod\ 4)$. Par le lemme 4, $p \notin \Sigma$, donc par la proposition 6, p est irréductible, donc premier, dans $\mathbb{Z}[\imath]$. Comme p divise $n := (a + \imath b)(a - \imath b)$, il divise $a \pm \imath b$, donc a et b. Donc $\dfrac{n}{p^2} = \left(\dfrac{a}{p}\right)^2 + \left(\dfrac{b}{p}\right)^2$, d'où p^2 divise n et $\dfrac{n}{p^2} \in \Sigma$. En itérant le processus jusqu'à ce que p ne divise plus $\dfrac{n}{p^{2k}}$, il vient $v_p(n) = 2k$, d'où le résultat.

□