Développement : Théorèmes des deux carrés de Fermat.

RM

2022-2023

Référence :

1. Oral à l'agreg

Énoncé :

Théorème 1 : Soit Σ l'ensemble des entiers qui sont somme de deux carrés. Alors $n \in \mathbb{N}^*$ est dans Σ si et seulement si $v_p(n)$ est pair pour tout p premier tel que $p = 3[4]$.

Il convient d'abords de remarquer que si l'on considère l'anneau $\mathbb{Z}[i]$ des entiers de Gauss, alors avec la norme $N(z) = z\overline{z} = a^2 + b^2$ ou $z = a + ib$, on remarque que

$$n \in \Sigma \Leftrightarrow \exists z \in \mathbb{Z}[i], N(z) = n$$

Proposition 2 : Soit $p > 2$ un nombre premier. Alors $x \in \mathbb{F}_p^*$ est un carré de $\mathbb{F}_p$ si et seulement si $x^{\frac{p-1}{2}} = 1$.

Démonstration : On pose $X = \{x \in \mathbb{F}_p | x^{\frac{p-1}{2}} = 1\}$, et on note S l'ensemble des carrés non nuls de $\mathbb{F}_p$. Comme un polynôme de degré d sur $\mathbb{F}_p$ possède au plus d racines, on a $|X| \leq \frac{p-1}{2}$. D'autre part, si $x \in S$, il existe $y \in \mathbb{F}_p^*$ tel que $x = y^2$ et on a donc $x^{\frac{p-1}{2}} = y^{p-1} = 1$. On a donc $S \subset X$ et il nous reste à calculer $|S|$ pour conclure par cardinalité. Pour ce faire, il suffit de remarquer que l'on a $x^2 = y^2$ si et seulement si $x = y$ ou $x = -y$. Ainsi, comme $\mathbb{F}_p$ est de caractéristique différente de 2, chaque élément de S est l'image d'exactement deux éléments distinct de $\mathbb{F}_p^*$ via l'application $x \mapsto x^2$, on en déduit qu'il y a donc $\frac{p-1}{2}$ carrés non nuls dans $\mathbb{F}_p$ et donc $|S| = \frac{p-1}{2}$ et donc $S = X$. □

Corollaire 3 : Soit p un nombre premier. Alors -1 est un carré de $\mathbb{F}_p$ si et seulement si $p \equiv 1[4]$ ou $p = 2$.

Démonstration : Pour $p = 2$, l'élément -1 est bien un carré de $\mathbb{F}_2$ puisqu'on a $-1 \equiv 1 \equiv 1^2[2]$. Pour $p > 2$, on a que -1 est un carré de $\mathbb{F}_p$ si et seulement si $(-1)^{\frac{p-1}{2}} = 1$, c'est-à-dire si et seulement si $\frac{p-1}{2}$ est pair, i.e si on a $p \equiv 1[4]$. □

Résolution :

Lemme 4 : L'ensemble Σ est stable par multiplication.

Démonstration : Soient $n, n' \in \Sigma$: il existe z et z' dans $\mathbb{Z}[i]$ tels que $n = N(z)$ et $n' = N(z')$. Alors par multiplicativité de N, on a $nn' = N(z)N(z') = N(zz')$ et donc $nn' \in \Sigma$.
Ce résultat est équivalent à l'égalité suivante, souvent appelée identité de Diophante : $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$. □

Lemme 5 : Soit p premier congru à 3[4]. Alors $p \notin \Sigma$.

Démonstration : Supposons par l'absurde que $p \in \Sigma$: il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$. Or si $a = 2k$, alors $a^2 = 4k^2$ et donc $a^2 \equiv 0[4]$ et si $a = 2k+1$, alors $a^2 = 4k^2 + 4k + 1$ et donc $a^2 \equiv 1[0]$, de même pour b. Donc on a nécessairement $a^2 \equiv 0[4]$ ou $a^2 \equiv 1[4]$, de même pur b^2. Il est donc impossible que $p = a^2 + b^2 \equiv 3[4]$, d'où $p \notin \Sigma$. □

Lemme 6 : Les éléments inversibles de $\mathbb{Z}[i]$ sont $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

Démonstration : Soit $z \in \mathbb{Z}[i]$ inversible : il existe $u \in \mathbb{Z}[i]$ tel que $zu = 1$. On a $N(zu) = N(z)N(u) = 1$, donc $N(z) = 1$ car $N(z)$ et $N(u)$ sont des entiers naturels. Si on note $z = a + ib$ avec $a, b \in \mathbb{Z}$, alors, comme $a^2 + b^2 = 1$, on a nécessairement a ou b qui est nul avec l'autre qui est égale à 1, d'où $z = \pm 1$ ou $\pm i$. Réciproquement ces éléments sont bien inversibles. □

Lemme 7 : L'anneau $\mathbb{Z}[i]$ est euclidien.

Démonstration : La norme N jouera le rôle de stathme euclidien de $\mathbb{Z}[i]$. Soient $z, t \in \mathbb{Z}[i]$ tels que $t \neq 0$. On cherche $q, r \in \mathbb{Z}[i]$ tels que $z = qt + r$ et $N(r) < N(t)$. On pose $\frac{z}{t} = x + iy \in \mathbb{C}$ avec $x, y \in \mathbb{R}$, et $q = a + ib$ où a et b sont des entiers tels que $|x - a| \leq 1/2$ et $|y - b| \leq 1/2$. Alors $|\frac{z}{t} - q|^2 = (x-a)^2 + (y-b)^2 \leq 1/4 + 1/4 = 1/2$. On pose alors $r = z - qt$. Or $N(r) = |r|^2 = |t|^2 |\frac{z}{t} - q|^2 < |t|^2 = N(t)$. Donc N est bien un stathme euclidien et $\mathbb{Z}[i]$ est euclidien. □

Lemme 8 : Soit p un nombre premier. Alors $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.

Démonstration : Supposons qu'il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$. Alors p se factorise $p = (a + ib)(a - ib)$ dans $\mathbb{Z}[i]$. De plus a et $b$sont non nuls car sinon p ne serait pas premier. Donc $a + ib$ et $a - ib$ ne sont pas inversibles d'après le Lemme 5 et donc p n'est pas irréductible.
Supposons que p ne soit pas irréductible : il existe $z, u \in \mathbb{Z}[i]$ non inversible tels que $p = zu$. Ainsi on a $N(p) = p^2$ et $N(p) = N(zu) = N(z)N(u)$. Comme z et u sont non inversibles, on a $N(z) \neq 1$ et $N(u) \neq 1$, d'où $p = N(z) = N(u)$ car le seul diviseur de p^2 est p et 1 et on a donc exclus 1. Finalement $p \in \Sigma$. □

Démonstration (Théorème 1) : Supposons que $v_p(n)$ est pair pour tout p premier tel que $p \equiv 3[4]$. On va montrer que $p^{v_p(n)} \in \Sigma$ pour tout premier p, et on en déduira que $m \in \Sigma$ par stabilité par multiplication de Σ. Soit p premier tel que $p \equiv 3[4]$, alors $p^{v_p(n)} = \left(p^{\frac{v_p(n)}{2}}\right)^2 + 0^2$ et donc appartient à Σ. Si $p = 2$ ou $p \equiv 1[4]$, alors il existe $a \in \mathbb{Z}$ telle que $-1 = a^2[p]$ d'après le corollaire 3, donc p divise $a^2 + 1 = (a - i)(a + i)$. Or p ne divise pas $a - i$ ni $a + i$, donc p n'est pas premier dans $\mathbb{Z}[i]$, et, comme $\mathbb{Z}[i]$ est euclidien, il n'est donc pas irréductible. D'après le lemme 8, on a que $p \in \Sigma$. Si p premier, alors $p = 2$,$p \equiv 1[4]$ ou $p \equiv 3[4]$ (le reste 0 et 2 n'est pas possible car p est premier). On a prouvé que peu importe le nombre premier p, $p^{v_p(n)} \in \Sigma$ par stabilité par multiplication pour $p = 2$ et $p \equiv 1[4]$, et donc $n \in \Sigma$ finalement.
Supposons que $n \in \Sigma$: il existe $a, b \in \mathbb{Z}$ telles que $n = a^2 + b^2$. Soit p un diviseur premier de n tel que $p \equiv 3[4]$. D'après le Lemme 5, p n'appartient pas à Σ et donc d'après le Lemme 8, p est irréductible et donc premier dans l'anneau $\mathbb{Z}[i]$. Comme p divise $n = (a + ib)(a - ib)$, il divise donc $a + ib$ ou $a - ib$ dans $\mathbb{Z}[i]$, et donc il divise a et b (par unique décomposition $x + iy$ d'un nombre complexe). On a donc $n/p^2 = (a/p)^2 + (b/p)^2$, d'où $p^2 | n$ et $\frac{n}{p^2} \in \Sigma$. On itère donc le processus jusqu'à ce que p ne divise plus n/p^{2k}. On a alors $n = p^{2k}u$ avec u qui n'est pas divisible par p, d'où $v_p(n) = 2k$ est pair.