Théorème des deux carrés (Fermat)

Recasage: 121, 122, (126 ?)

Réf: Perrin p 56 à 58.

On pose $\Sigma = \{a^2+b^2 : a,b \in \mathbb{N}\}$. On remarque rapidement que si $n \equiv 3 \ (4)$ alors $n \notin \Sigma$.

Idée: si $n = a^2+b^2$ alors $n = (a+ib)(a-ib)$ et cette relation a lieu dans l'anneau des entiers de Gauss $\mathbb{Z}[i] = \{a+ib : a,b \in \mathbb{Z}\}$.

En effet si un nombre premier est somme de deux carrés, il perd son irréductibilité dans $\mathbb{Z}[i]$.

$\mathbb{Z}[i]$ est intègre en tant que sous-anneau de $\mathbb{C}$, la conjugaison en est un automorphisme évident. Soit aussi $N : z = a+ib \in \mathbb{Z}[i] \mapsto z\bar{z} = a^2+b^2$. N est multiplicative et à valeurs dans $\mathbb{N}$.

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

Dém: $z \in \mathbb{Z}[i]^\times \iff N(z) = 1$: si $N(z) = 1 = |z|^2 = z\bar{z}$ alors $z \in \mathbb{Z}[i]^\times$ car $\bar{z} \in \mathbb{Z}[i]$.

si $z \in \mathbb{Z}[i]^\times$, $\exists z' \in \mathbb{Z}[i]$ tq $zz' = 1$ donc $N(zz') = N(z)N(z') = 1$ donc $N(z) = 1$.

Maintenant si $N(z = a+ib) = 1 = a^2+b^2$, cela impose $a = 0$ ou $b = 0$ ce qui donne $z = \pm 1$ ou $z = \pm i$. □

Prop: $\mathbb{Z}[i]$ est euclidien (donc principal).

Dém: Soient $z \in \mathbb{Z}[i]$, $t \in \mathbb{Z}[i] \setminus \{0\}$, on écrit $\frac{z}{t} = x+iy \in \mathbb{C}$

Il existe $a,b \in \mathbb{Z}$ tels que $|x-a| \leq \frac{1}{2}$ et $|y-b| \leq \frac{1}{2}$

On pose $q = a+ib$ de sorte que $\left|\frac{z}{t} - q\right| = (x-a)^2+(y-b)^2 \leq \frac{1}{2} < 1$

Avec $r = z - qt \in \mathbb{Z}[i]$, on a $|r| = |t| \cdot \left|\frac{z}{t} - q\right| < |t|$ donc en élevant au carré, $N(r) = |r|^2 < |t|^2 = N(t)$. Ainsi N est un stathme sur $\mathbb{Z}[i]$. □

Lemme : $p \in \Sigma \iff p$ n'est pas irréductible dans $\mathbb{Z}[i]$.

Dém : $\Rightarrow$ si $p = a^2+b^2$, on a $p = (a+ib)(a-ib)$ et $a, b \neq 0$ donc $a+ib,\ a-ib \notin \mathbb{Z}[i]^\times$ donc p n'est pas irréductible dans $\mathbb{Z}[i]$.

$\Leftarrow$ si $p = zz'$ avec $z, z' \notin \mathbb{Z}[i]^\times$, $N(p) = N(z)N(z') = p^2$ et comme $N(z), N(z') \neq 1$, on a $p = N(z) = N(z')$ et $p \in \Sigma$. □

Théorème : $p \in \Sigma \iff p = 2$ ou $p \equiv 1\ (4)$

Dém : La condition est clairement nécessaire via la remarque faite au début.

Maintenant comme $\mathbb{Z}[i]$ est principal, donc factoriel, p n'est pas irréductible dans $\mathbb{Z}[i] \iff$ l'idéal principal $(p) = p\mathbb{Z}[i]$ n'est pas premier $\iff \mathbb{Z}[i]/(p)$ n'est pas intègre

Lemme (admis) : si A anneau commutatif et $a, b \in A$, on a

$$(A/(a))/(\bar{b}) \simeq A/(a,b) \simeq (A/(b))/(\bar{a})$$

Dès lors, on a, en sachant que $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$ (morphisme d'évaluation + division euclidienne) et grâce au lemme :

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

Bref, $p \in \Sigma \iff \mathbb{F}_p[X]/(X^2+1)$ est non intègre ↔ car $\mathbb{F}_p[X]$ est principal (car $\mathbb{F}_p$ corps) cf. Perrin p 51

car de degré 2 ↑ $\iff X^2+1$ n'est pas irréductible sur $\mathbb{F}_p$

$\iff X^2+1$ admet une racine dans $\mathbb{F}_p$

$\iff -1$ est un carré dans $\mathbb{F}_p^*$

$\iff p = 2$ ou $p \equiv 1\ (4)$

Détails...

Démo lemme : Il suffit de montrer $A/(a,b) \simeq (A/(a))/(\bar{b})$, l'autre étant symétrique.

Soit $\pi_a : A \to A/(a)$ et $\pi_{ab} : A \to A/(a,b)$ les surjections canoniques de A dans ses quotients par les idéaux (a) et (a,b).
Comme $(a) \subset (a,b) = \ker \pi_{ab}$, d'après la propriété universelle des quotients, il existe un morphisme d'anneaux $\overline{\pi_{ab}} : A/(a) \to A/(a,b)$ tel que

$$\overline{\pi_{ab}} \circ \pi_a = \pi_{ab}.$$

D'après le premier théorème d'isomorphisme, $\operatorname{Im} \overline{\pi_{ab}} \simeq (A/(a))/\ker \overline{\pi_{ab}}$.

Or, π_{ab} est surjective donc $\overline{\pi_{ab}}$ aussi si bien que $\operatorname{Im} \overline{\pi_{ab}} = A/(a,b)$.

Ensuite $\bar{x} \in \ker \overline{\pi_{ab}} \iff x \in \ker \pi_{ab} \iff x \in (a,b) \iff \bar{x} \in (\bar{b})$.
($\bar{x} = \pi_a(x)$)

$x = au + bv \implies \pi_a(x) = \bar{x} = \bar{b}\bar{v} \in (\bar{b})$
$\bar{x} = \bar{b}\bar{v} \implies \bar{x} = bv + (a) \implies \exists u \in A,\ x = au + bv$

On obtient bien $A/(a,b) = \operatorname{Im} \overline{\pi_{ab}} \simeq (A/(a))/\ker \overline{\pi_{ab}} \simeq (A/(a))/(\bar{b})$. □

$-1 \in \mathbb{F}_p^{*2}$: Perrin p75

$x \in \mathbb{F}_p^{*2} \iff x^{\frac{p-1}{2}} = 1$: en effet si x est un carré, $\exists y \in \mathbb{F}_p^*$ tq $x = y^2$ donc $x^{\frac{p-1}{2}} = y^{p-1} = 1$ par le théorème de Lagrange. Comme il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$ et que $X^{\frac{p-1}{2}} - 1$ a au plus $\frac{p-1}{2}$ racines dans le corps $\mathbb{F}_p$, on les a toutes.

Ainsi $-1 \in \mathbb{F}_p^{*2} \iff (-1)^{\frac{p-1}{2}} = 1 \iff \frac{p-1}{2}$ est pair $\iff p \equiv 1 \ (4)$

Perrin p56

Σ est stable par multiplication : en effet, $n \in \Sigma \iff \exists z \in \mathbb{Z}[i],\ n = N(z)$ donc si $n = N(z)$, $n' = N(z') \in \Sigma$, par multiplicativité de N, on a $nn' = N(z)N(z') = N(zz') \in \Sigma$.

On ramène ainsi l'étude de Σ à la détermination des premiers qui sont dedans.

Théorème : $n \in \mathbb{N}^*$ qu'on écrit $n = \prod_{p \in P} p^{v_p(n)}$. Alors $n \in \Sigma \iff v_p(n)$ est pair pour $p \equiv 3\ (4)$.

Perrin p58

Dém : $\Leftarrow$ $p = 2 \in \Sigma$, $p \equiv 1\ (4) \iff p \in \Sigma$ et par hypothèse $p^{v_p(n)}$ est un carré lorsque $p \equiv 3\ (4)$ donc est dans Σ, et Σ est stable par multi$^{\text{e}}$.

$\Rightarrow$ soit $p \equiv 3\ (4)$, on montre par récurrence sur $v_p(n)$ que $v_p(n)$ est pair. Si $v_p(n) = 0$: ok. Sinon, p divise $n = a^2 + b^2 = (a+ib)(a-ib)$ mais p étant irréductible dans $\mathbb{Z}[i]$, p divise par exemple $a+ib$ ce qui impose $p \mid a$ et $p \mid b$ donc $p^2 \mid n$ et si on écrit $a = pa'$, $b = pb'$ on a $\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma$. Mais $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2$ est pair par hypothèse de récurrence donc idem pour $v_p(n)$. □

Théorème : Les irréductibles de $\mathbb{Z}[i]$ sont, aux éléments inversibles près :

- les entiers premiers $p \in \mathbb{N}$ avec $p \equiv 3\ (4)$
- les entiers de Gauss $a+ib$ dont la norme a^2+b^2 est un nb. premier.

Perrin p58

Dém : Les premiers $\equiv 3\ (4)$ sont bien irréductibles dans $\mathbb{Z}[i]$ comme vu plus tôt. Si $a+ib \in \mathbb{Z}[i]$ avec $N(z) = a^2+b^2 = p$ premier est réductible, $\exists z' \in \mathbb{Z}[i]$ tq $zz' = 1$ et donc $N(z)N(z') = 1$ donc $p \mid 1$: impossible.

Réciproquement, soit z irréductible de norme $N(z) = z\bar{z} \in \mathbb{N}$.
Soit p un nombre premier divisant $N(z)$. Si $p \equiv 3\ (4)$, p est premier dans $\mathbb{Z}[i]$ donc divise z ou $\bar{z}$ et on a $z = p$ à $\pm 1, \pm i$ près.
Si $p \in \Sigma$, $p = a^2+b^2$ et l'entier de Gauss $t = a+ib$ est irréductible dans $\mathbb{Z}[i]$ donc divise z ou $\bar{z}$ et on a $z = t$ ou $\bar{t}$ à $\pm 1, \pm i$ près. □

Rmq initiale : $n \equiv 3\ (4) \Rightarrow n \notin \Sigma$: en effet, on vérifie que $a^2+b^2 \equiv 0, 1, 2\ (4)$.

Perrin p56