Théorème des deux carrés (Fermat)

Recasages : 122, 127, ~~121~~, ~~123~~, ~~120~~

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

- Si $n \equiv 3 \bmod 4$, on a $n \notin \Sigma$. En effet, si a est pair, on a $a^2 \equiv 0$ [4] ; si a est impair, $a^2 \equiv 1 \bmod 4$ donc $a^2 + b^2 \equiv 0, 1$ ou 2 [4].

Proposition 1 : On pose $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} / (a, b) \in \mathbb{Z}^2\}$
$\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ (donc intègre) dont les inversibles sont $\{-1 ; 1 ; -i ; i\}$.

Preuve : On introduit $N : \mathbb{Z}[i] \to \mathbb{N}$, $a+ib \mapsto a^2+b^2$. N est une application multiplicative.
- Si $z \in \mathbb{Z}[i]^*$, alors $\exists z' \in \mathbb{Z}[i]$, $zz' = 1$ donc $N(zz') = N(1) = 1$ donc $N(z)N(z') = 1$. Or, $N(z)$ et $N(z') \in \mathbb{N}$, donc $N(z) = N(z') = 1$. Ainsi, si $z = a + ib$, on a donc $a^2 + b^2 = 1$, de sorte que $a \neq 0$ et $b = 0$ ou $a = 0$ et $b = \pm 1$, d'où le résultat.

Proposition 2 : Σ est stable par multiplication.

Preuve : $n \in \Sigma \Leftrightarrow \exists z \in \mathbb{Z}[i]$, $n = N(z)$. D'où si $n = N(z)$, $n' = N(z')$ on a donc $nn' = N(zz') \in \Sigma$.

Proposition 3 : $\mathbb{Z}[i]$ est euclidien pour le stathme N, donc principal.

Preuve : Soient $(z, t) \in \mathbb{Z}[i] \setminus \{0\}$. Approximons $\frac{z}{t} \in \mathbb{C}$ par un entier de la forme q : si $\frac{z}{t} = x + iy \in \mathbb{C}$, on prend $a \in \mathbb{N}$ tq $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$, $b \in \mathbb{N}$
Posons $q = a + ib$, $\left|\frac{z}{t} - q\right| \leq \frac{\sqrt{2}}{2} < 1$
Posons $r = z - bq$, $r \in \mathbb{Z}[i]$ et $r = t\left(\frac{z}{t} - q\right)$ d'où $|r| = |t| \left|\frac{z}{t} - q\right| < |t|$
On a donc $N(r) < N(t)$ d'où $z = qt + r$ et $N(r) < N(t)$.

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

Preuve: "$\Rightarrow$" $p = a^2 + b^2 = (a+ib)(a-ib)$ $a, b \neq 0$ donc $a+ib, a-ib \notin \mathbb{Z}[i]^\times$ donc p n'est pas irréductible.
"$\Leftarrow$" Si $p = zz'$, $z, z' \neq 1, \pm i$, $N(p) = N(z)N(z') = p^2$ et comme $N(z), N(z') \neq 1$ on a alors $p = N(z)$ donc $p \in \Sigma$.

Théorème: $p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1 \bmod 4$ premier "$p \neq 0 \bmod 4$ sinon $4 \mid p$ et pas premier

Preuve: "$\Rightarrow$" On a vu que si $p \equiv 3 \bmod 4$, $p \notin \Sigma$ si $p = 2$, ok, on suppose $p \neq 2$.
"$\Leftarrow$" $\mathbb{Z}[i]$ est principal donc factoriel donc dire que p n'est pas irréductible dans $\mathbb{Z}[i]$ équivaut à : (p) non premier i.e $\mathbb{Z}[i]/(p)$ n'est pas intègre.
On $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$ via $\varphi : \mathbb{Z}[X] \to \mathbb{Z}[i]$, $P \mapsto P(i)$ surjectif de noyau (X^2+1)

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

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

Montrons que $x \in \mathbb{F}_q^{\times 2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$.
Posons $A = \{x \in \mathbb{F}_q \mid x^{\frac{q-1}{2}} = 1\}$, on a $\#A \leq \frac{q-1}{2}$. Le polynôme $X^{\frac{q-1}{2}} - 1$ a au plus $\frac{q-1}{2}$ racines
D'autre part, si $x \in (\mathbb{F}_q^\times)^2$, on a $x = y^2$ avec $y \in \mathbb{F}_q^{\times 2}$ donc $x^{\frac{q-1}{2}} = y^{q-1} = 1$ (Lagrange) donc $\mathbb{F}_q^{\times 2} \subset A$ ... inclusion

On, $\#(\mathbb{F}_q^\times)^2 = \frac{q-1}{2}$ (si $p \neq 2$) car $\mathbb{F}_q^\times \to (\mathbb{F}_q^\times)^2$, $x \mapsto x^2$ est un morphisme surjectif de noyau $\{\pm 1\}$

donc $(\mathbb{F}_q^\times)^2 = A$ par cardinal.

Ainsi, $-1 \in (\mathbb{F}_p^\times)^2 \Leftrightarrow p \equiv 1 \bmod 4$:

$$-1 \in (\mathbb{F}_p^\times)^2 \Leftrightarrow (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2} \text{ est pair} \Leftrightarrow p \equiv 1 \bmod 4.$$

$\mathbb{Z}[X] \to \mathbb{F}_p[X]$, $P \mapsto \bar{P}$ surjectif et de noyau (p)

$(X^2+1, p) \to (p)$, $(X^2+1)R + pR \mapsto pQ$ morphisme surjectif de noyau (X^2+1)

Théorème : Soit $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$ un entier non nul et différent de 1.
$n \in \Sigma \iff v_p(n)$ est pair pour $p \equiv 3 \bmod 4$.

Preuve : $\Leftarrow$ Par le théorème précédent, et en utilisant le fait que Σ est stable par multiplication, si $v_p(n)$ est pair pour $p \equiv 3 \bmod 4$, alors pour tout p dans la décomposition de n, $p \in \Sigma$ et donc $n \in \Sigma$.
↳ Soit $p \mid n$. - Si $p = 2 \to p \in \Sigma$ - Si $p \equiv 1 \bmod 4 \to p \in \Sigma$ - Si $p \equiv 3 \bmod 4$ et $v_p(n)$ pair $p^{v_p(n)} \in \Sigma \Rightarrow \Sigma$ stable par $\times \Rightarrow n \in \Sigma$.

$\Rightarrow$ Par récurrence sur n. P_n : "Pour tout $p \equiv 3 \bmod 4$, $v_p(n)$ est pair"

- Si $n = 2$, $v_p(n) = 0$ est pair (pour tout $p \equiv 3 \bmod 4$)
- Soit $n \in \mathbb{N}^*$. On suppose que pour tout $m \in [\![1; n-1]\!]$, $v_p(m)$ est pair pour $p \equiv 3 [4]$. Soit $p \equiv 3 \bmod 4$.
  - → Cas 1 : $v_p(n) = 0$, alors $v_p(n)$ est paire
  - → Cas 2 : $p \mid n$; comme $n \in \Sigma$, il existe $k \in \mathbb{N}$ tel que $n = (a+ib)(a-ib) = kp$ donc par le lemme d'Euclide, $p \mid a+ib$ ou $p \mid a-ib$. Disons $p \mid a+ib$. Alors, comme p est entier, $p \mid a$ et $p \mid b$ i.e. : $\exists a' \in \mathbb{N}, \exists b' \in \mathbb{N}, a = pa', b = pb'$. Ainsi, $\frac{n}{p^2} = a'^2 + b'^2$
  Donc $\frac{n}{p^2} \in \Sigma$. Par HR, $v_p\left(\frac{n}{p^2}\right)$ est paire

On a $v_p(n) = v_p\left(\frac{n}{p^2}\right) + 2$ donc $v_p(n)$ est paire.
↳ $n = \frac{n}{p^2} \times p^2 \to v_p(n) = v_p\left(\frac{n}{p^2}\right) + v_p(p^2) = v_p\left(\frac{n}{p^2}\right) + 2$

Par le principe de récurrence, ~~pour tout $n \in \mathbb{N}^*$~~, $v_p(n)$ est paire pour $p \equiv 3 [4]$
$\forall n \in \mathbb{N}^*$