Représentations de nombres premiers sous la forme $p = x^2 + 3y^2$.

Leçon : 121, 122, 126

Rqs : CVA, calculs, récurrence

Théorème

Un nombre premier (positif) p se décompose en $x^2 + 3y^2$, avec $x, y \in \mathbb{Z}$ ssi $p = 3$ ou $p \equiv 1 [3]$.

Preuve

$\Rightarrow$ Si $p = x^2 + 3y^2$, $x, y \in \mathbb{Z}$. Alors $p = x^2$ dans $\mathbb{Z}/3\mathbb{Z}$. Donc p est un carré modulo 3. Or les carrés de $\mathbb{F}_3$ sont 0 ou 1.

x	0	1	2
x^2	0	1	1

. Si $p = 0$ dans $\mathbb{F}_3$, alors $3 | p$ donc $\boxed{p = 3}$ car p est premier.

. Si $p = 1$ dans $\mathbb{F}_3$, $\boxed{p \equiv 1 [3].}$

$\Leftarrow$ Stratégie : étudier $\mathbb{Z}[j] \to$ euclidien $\Rightarrow$ factoriel

Pq ? on veut étudier $\mathbb{Z}[i\sqrt{3}]$ mais il n'est pas factoriel

(par analogie avec le théorème des 2 carrés).

On va voir que si $\alpha \in \mathbb{Z}[j]$, alors il existe un représentant de α modulo $\mathbb{Z}[j]^\times$ dans $\mathbb{Z}[i\sqrt{3}]$.

On pose $A = \mathbb{Z}[j] := \{P(j) : P \in \mathbb{Z}[X]\}$, $j = \frac{-1+i\sqrt{3}}{2}$.

~~Si $p = 3$, alors $p = 0^2 + 3 \times 1^2$, donc c'est réglé. On suppose que $p \equiv 1 [3]$~~

1) Pq $X^3 - 1$ scindé sur $\mathbb{F}_p \Leftrightarrow p = 3$ ou $p \equiv 1 [3]$.

⇐ Si $p = 3$ ou $p \equiv 1 [3]$.

Si $p = 3$, alors dans $\mathbb{F}_3$, $X^3 - 1 = X^3 - 1^3 = (X-1)^3$ (Frobenius).

Si $p \equiv 1[3]$. On résout $x^3 = 1$.

On n'est pas satisfait, car on se ramène à résoudre l'équat° dans $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. On peut donc résoudre de manière additive : $3x = 0$ dans $\mathbb{Z}/p-1\mathbb{Z}$.

On $p - 1 \equiv 0[3]$, car a donc 3 solut° distinctes :

$$0, \quad \frac{p-1}{3}, \quad \frac{2}{3}(p-1).$$

Il n'y en a pas plus car $d^\circ(X^3 - 1) = 3$ (sur le corps $\mathbb{F}_q$).

⇒ Si $X^3 - 1$ est scindé. On distingue deux cas.

→ Si 1 est racine triple de $X^3 - 1$, alors $X^3 - 1 = (X-1)^3$

donc $3 = 0$ dans $\mathbb{F}_p$ (par coeffs binomiaux s'annulent).

Donc $3 | p$ et p 1ère $\Rightarrow$ $\boxed{p = 3}$

→ Si il existe une racine de $X^3 - 1 \neq 1$. Alors cet élément est d'ordre 3, donc par le théorème de Lagrange dans $\mathbb{F}_p^\times$, $3 | p-1$, donc $\boxed{p \equiv 1[3]}$.

2) Trq $A/(p)$ et $\mathbb{F}_p[X]/(X^2+X+1)$ sont isomorphes.

On note | $ev_j : \mathbb{Z}[X] \to \mathbb{Z}[j]$ l'évaluat° en j
$P \mapsto P(j)$

et la projection | $\pi : \mathbb{Z}[j] \to \mathbb{Z}[j]/(p)$
$P \mapsto \pi(P) = P \bmod p$.

ev_j et π sont surjectifs, donc si $\varphi : \mathbb{Z}[X] \to \mathbb{Z}[j]/(P)$, $P \mapsto \pi \circ ev_j(P)$

est aussi surjectif. Par passage au quotient on a

$$\operatorname{Im}\varphi = \mathbb{Z}[j]/(P) \simeq \mathbb{Z}[X]/(\operatorname{Ker}\varphi)$$

Déterminons $\operatorname{Ker}\varphi$. On commence par montrer $\operatorname{Ker}(ev_j) = (X^2+X+1)$.

$\supseteq$: c'est clair, si $P = (X^2+X+1)Q$, alors

$$P(j) = ev_j(P) = (j^2+j+1)Q(j) = 0.$$

$\subseteq$ Soit $P \in \mathbb{Z}[X]$, tq $P(j) = 0$. Le polynôme X^2+X+1 est unitaire, donc par DE, il existe $Q \in \mathbb{Z}[X]$ et $a, b \in \mathbb{Z}$ tq

$$P = (X^2+X+1)Q + aX + b.$$

On $P(j) = 0$, donc $aj + b = 0$

$$\Rightarrow a = b = 0.$$

Donc $P = (X^2+X+1)Q$ et on a bien

$\operatorname{Ker}(ev_j) = (X^2+X+1)$.

Ainsi $\operatorname{Ker}\varphi = \varphi^{-1}(0) = ev_j^{-1}(\pi^{-1}(0)) = ev_j^{-1}(p\mathbb{Z}[j])$

$$\overset{(*)}{=} p\mathbb{Z}[X] + (X^2+X+1)\mathbb{Z}[X].$$

$(*)$ par double inclusion.

Ainsi $\mathbb{Z}[j]/(P) \simeq \mathbb{Z}[X]/(p\mathbb{Z}[X] + (X^2+X+1)\mathbb{Z}[X])$.

On construit $\varphi : \mathbb{Z}[X] \to \mathbb{F}_p[X]/(X^2+X+1)$

via $\beta : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ ou $\pi : \mathbb{F}_p[X] \to \mathbb{F}_p[X]/(X^2+X+1)$

$P \mapsto P \bmod p$ $\quad$ $P \mapsto \pi(P)$

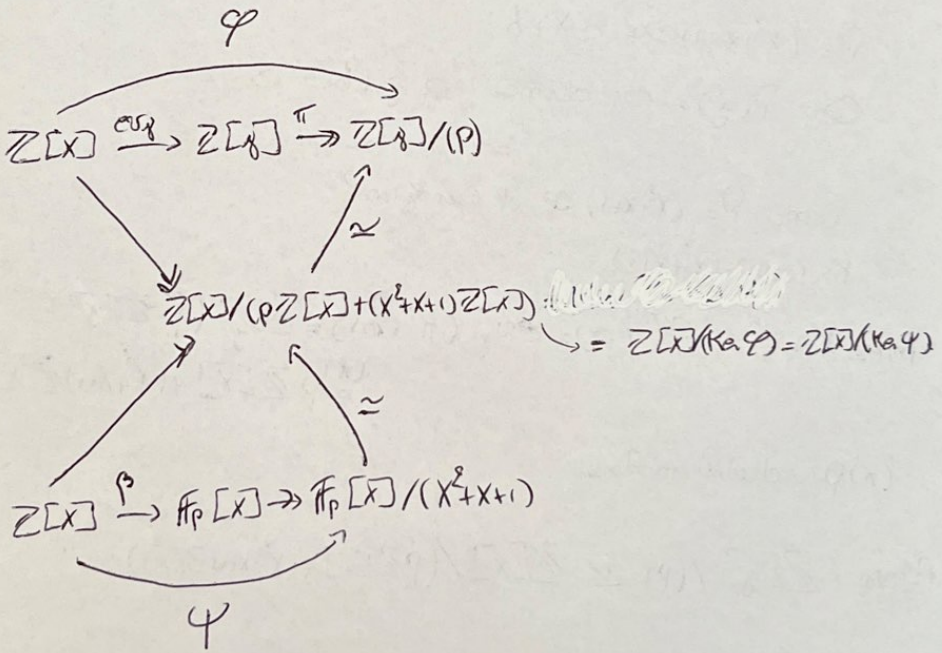
Par propriété : clairement φ est surjective.

$\ker \beta = p\mathbb{Z}[X]$, donc comme précédemment,

$\ker \varphi = p\mathbb{Z}[X] + (X^2+X+1)\mathbb{Z}[X]$.

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

ce qui prouve l'unicité.



3) Lien entre $\mathbb{Z}[i\sqrt{3}]$ et A. $\quad \hookrightarrow = \{\pm 1, \pm j, \pm j^2\}$.

Soit $\alpha \in A$. Mq qu'il existe $x \in A^\times$ tq $\alpha x \in \mathbb{Z}[i\sqrt{3}]$.

On a vu que $\alpha \in A = \mathbb{Z}[j]$ peut s'écrire $a+jb$, $a,b \in \mathbb{Z}$.

On a $j = \frac{1+i\sqrt{3}}{2}$, donc $\alpha = a+jb = \frac{2a+b}{2} + i\sqrt{3}\frac{b}{2}$

est dans $\mathbb{Z}[i\sqrt{3}]$ ssi b est pair.

→ Si b est pair : $\alpha \in \mathbb{Z}[i\sqrt{3}]$

→ Si b est impair :

→ Si a est pair : $j^2(a+bj) = -(1+j)a + b$
$= b - a - ja \in \mathbb{Z}[i\sqrt{3}]$

→ Si a est impair : $j(a+bj) = aj + b(-1-j)$
$= -b + (b-a)j \in \mathbb{Z}[i\sqrt{3}]$

car $a-b$ est pair.

4) Conclusion. Si $p=3$, $p = 0^2 + 3\times 1^2$: V.

Si $p \equiv 1[3]$. Alors $X^3 - 1$ possède 3 racines sur $\mathbb{F}_p$, et donc X^2+X+1 en a 2 (car $X^2+X+1 \mid X^3-1$) sur $\mathbb{F}_p$.

comme X^2+X+1 n'est pas irréductible sur $\mathbb{F}_p$.

$\Rightarrow \mathbb{F}_p[X]/(X^2+X+1)$ non intègre

$\Rightarrow \mathbb{Z}[j]/(p)$ n'est pas intègre

$\Rightarrow p$ n'est pas 1er dans $\mathbb{Z}[j]$.

On $A = \mathbb{Z}[j]$ est factoriel (car euclidien) donc p est réductible

Sur $\mathbb{Z}[j]$: s'il existe $\alpha, \beta \in \mathbb{Z}[j]$ non inversibles tq $p = \alpha\beta$. (de $N(\alpha), N(\beta) > 1$).

On a alors $p^2 = N(p) = N(\alpha) N(\beta)$, N morphisme sur $\mathbb{Z}[j]$

$\Rightarrow N(\alpha) = p$.

Quitte à multiplier par un inversible de $\mathbb{Z}[j]^\times$ (de norme 1) on peut supposer que $\alpha \in \mathbb{Z}[i\sqrt{3}]$.

Donc $\alpha = x + i\sqrt{3}y$ et $N(\alpha) = p$

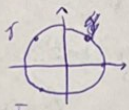
$\Leftrightarrow p = x^2 + 3y^2$.

□

- $\mathbb{Z}[i]$ et l'un des deux anneaux est le simple car $\mathbb{Z}[i]$ euclidien.
- $p \equiv 1 [3]$, $p = x^2 + 3y^2$ → les sont uniques !
- $N : \mathbb{Z}[j] \to \mathbb{Z}[j]$ ($\mathbb{N}$)

  $a + jb \mapsto (a+jb)(\overline{a+jb})$

On a $\overline{j} = -1 - j$



($\overline{j} = \overline{\frac{-1+i\sqrt{3}}{2}} = -\frac{1-i\sqrt{3}}{2} = \frac{1+i\sqrt{3}}{2} - 1 = -j - 1$).

Donc $N(a+jb) = (a+jb)(a-b-jb)$

$= a^2(a-b) - j^2 b^2 + jb(a-b) - jab$

$= a^2 - ab + (1+j)b^2 + jab - jb^2 - jab$

$= a^2 - ab + b^2$

$u \in \mathbb{Z}[j]$ inversible $\Leftrightarrow \exists v \in \mathbb{Z}[j]$, $uv = 1$

$\Leftrightarrow \dots$

$\Leftrightarrow N(u) = 1$.

N est multiplicative.

• $\mathbb{Z}[i\sqrt{3}]$ n'est factoriel :

$$4 = 2 \times 2 = (1 - i\sqrt{3})(1 + i\sqrt{3}).$$

• Rappel : I idéal de A est premier si A/I intègre

$$\Leftrightarrow \begin{cases} A \neq I \\ \forall a, b \in A,\ ab \in I \Rightarrow a \in I \text{ ou } b \in I. \end{cases}$$

* $p \in A$ est premier si (p) est premier.

* p irréductible : $\begin{cases} p \notin A^* \\ p = ab \Rightarrow a \in A^* \text{ ou } b \in A^* \end{cases}$

On a toujours : p 1er $\Rightarrow p$ irréductible

Dans les anneaux factoriels : irréductible $\Leftrightarrow$ 1er.
- principaux
- euclidiens

→ On a unicité du couple (x, y).

Si $x^2 + 3y^2 = p = x'^2 + 3y'^2$, on pose $\begin{cases} \pi = x + iy\sqrt{3} \\ \pi' = x' + iy'\sqrt{3} \end{cases}$

On a $N(\pi) = N(\pi') = p$.

Norme sur A et $N(\cdot) \in \mathbb{N} \Rightarrow$ dans p sur $\mathbb{Z} \Rightarrow$ dans π, π' A.

Donc $\overline{\pi}, \overline{\pi'}$ sont aussi irréductibles.

Donc, A factoriel, $\pi' = u\pi$ ou $\pi' = u\overline{\pi}$, $u \in A^*$

$A^* = \{\pm 1, \pm j, \pm j^2\}$

→ calcul ($\pi = a + bj$, $\pi' = a' + b'j$).