Nombres premiers de forme $p = x^2 + 3y^2$

Geoffrey Deperle

Leçons associées :
— 121 : Nombres premiers. Applications.
— 122 : Anneaux principaux. Exemples et applications.
— 126 : Exemples d'équations en arithmétique.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Un nombre premier p se décompose sous la forme $p = x^2 + 3y^2$ avec $x, y \in \mathbb{Z}$ si et seulement si $p = 3$ ou $p \equiv 1[3]$*

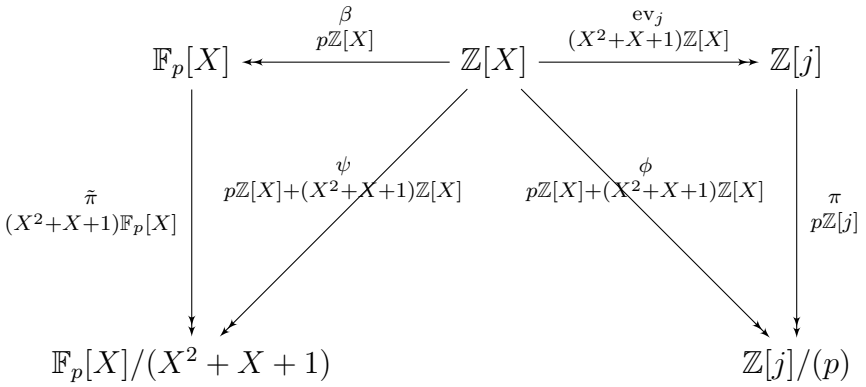
Preuve :
($\Longleftarrow$) Si $p = x^2 + 3y^2$ alors p est un carré modulo 3.
Or les carrés modulo 3 sont 0 et 1 donc $p \equiv 1[3]$ ou $3|p$ d'où $p = 3$ car p premier.

($\Longrightarrow$) Si $p = 3$, alors le couple $(0, 1)$ convient.
Supposons maintenant $p \equiv 1[3]$,

Étape 1 : Montrons que $X^3 - 1$ est scindé dans $\mathbb{F}_p \iff p = 3$ ou $p \equiv 1[3]$

Comme 0 n'est pas racine de X^3-1, on se ramène à l'équation dans $\mathbb{F}_p^*$ cyclique et donc isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$. Cela revient à résoudre l'équation $3x = 0$ dans $\mathbb{Z}/(p-1)\mathbb{Z}$. Or, comme $p \equiv 1[3]$, les entiers $0, \frac{p-1}{3}, \frac{2(p-1)}{3}$ sont trois solutions distinctes et il n'y a pas d'autre (question de degré).

Étape 2 : Montrons que l'on a $\mathbb{Z}[j]/(p) \simeq \mathbb{F}_p[X]/(X^2 + X + 1)$ avec $j = \frac{-1+i\sqrt{3}}{2}$



On construit les différents morphismes du diagramme (dont on note les noyaux respectifs en dessous)

Tous les morphismes sont surjectifs de noyau :

— $\mathrm{Ker}(\mathrm{ev}_j) = (X^2 + X + 1)$
— $\mathrm{Ker}(\pi) = p\mathbb{Z}[j]$

Calculons $\mathrm{Ker}(\phi)$,
Soit $P \in \mathbb{Z}[X]$, on effectue la division euclidienne de P par le polynôme unitaire $X^2 + X + 1$: il existe $A, B \in \mathbb{Z}[X]$ tel que $P = (X^2 + X + 1)A(X) + B(X)$.

$$\begin{aligned} P \in \mathrm{Ker}(\phi) &\iff \pi(\mathrm{ev}_j(P)) = 0 \\ &\iff \pi(B(j)) = 0 \\ &\iff p | B(j) \\ &\iff B \in p\mathbb{Z}[X] \end{aligned}$$

donc $\mathrm{Ker}(\phi) = p\mathbb{Z}[X] + (X^2 + X + 1)\mathbb{Z}[X]$.
De même,
— $\mathrm{Ker}(\beta) = p\mathbb{Z}[X]$
— $\mathrm{Ker}(\tilde{\pi}) = (X^2 + X + 1)\mathbb{F}_p[X]$

et de même $\mathrm{Ker}(\psi) = p\mathbb{Z}[X] + (X^2 + X + 1)\mathbb{Z}[X]$.
Comme ψ et ϕ sont surjectifs,

$$\mathbb{F}_p[X]/(X^2 + X + 1) \simeq \mathbb{Z}[X]/\mathrm{Ker}(\psi) = \mathbb{Z}[X]/\mathrm{Ker}(\phi) \simeq \mathbb{Z}[j]/(p)$$

Étape 3 : Montrons qu'il existe un élément $\alpha \in \mathbb{Z}[j]$ de norme p

Ainsi, comme $p \equiv 1[3]$, $X^3 - 1$ possède 3 racines sur $\mathbb{F}_p$ et donc $X^2 + X + 1$ possède deux racines sur $\mathbb{F}_p$ d'où $X^2 + X + 1$ n'est pas irréductible sur $\mathbb{F}_p$ et l'anneau $\mathbb{F}_p[X]/(X^2 + X + 1)$ n'est pas intègre donc l'anneau $\mathbb{Z}[j]/(p)$ n'est pas intègre et p n'est pas premier dans $\mathbb{Z}[j]$.
Comme $\mathbb{Z}[j]$ est factoriel, p est irréductible :
Il existe α, β non inversible (donc de norme > 1) dans $\mathbb{Z}[j]$ tels que $p = \alpha\beta$.
Ainsi, $p^2 = N(\alpha)N(\beta)$ et comme $N(\alpha) \in \mathbb{N}$, $N(\alpha) = p$.

Étape 4 : Montrons qu'en multipliant par un inversible, il existe un élément $\alpha \in \mathbb{Z}[\frac{-1+i\sqrt{3}}{2}]$ de norme p

Montrons qu'il existe un représentant de α modulo les inversibles de $\mathbb{Z}[j]$ se trouvant dans $\mathbb{Z}[i\sqrt{3}]$.
$\alpha \in \mathbb{Z}[j]$ donc $\exists a, b \in \mathbb{Z} / \alpha = a + bj$. Comme $j = \frac{-1+i\sqrt{3}}{2}$, on a $\alpha \in \mathbb{Z}[i\sqrt{3}]$ si et seulement si b est pair.
Or, si b est impair :
— Si a est impair, on a $j(a + bj) = aj - b(1 + j) = -b + (a - b)j \in \mathbb{Z}[i\sqrt{3}]$
— Si a est pair, $j^2(a + bj) = b - a(1 + j) = b - a - aj \in \mathbb{Z}[i\sqrt{3}]$

Ainsi, quitte à multiplier par un inversible (de norme 1), on a $\alpha \in \mathbb{Z}[i\sqrt{3}]$.
Donc avec ce $\alpha = x + iy\sqrt{3}$ et $p = N(\alpha) = x^2 + 3y^2$ donnant une décomposition de p sous la forme voulue. □

Références

[1] Philippe Caldero et Marie Peronnier. *Carnet de voyage en Algébrie*. Calvage Mounet, 2019.