Théorème des deux carrés de Fermat

Mohamed NASSIRI

Références:

Cours d'Algèbre, Daniel Perrin p.56→58, p.74-75

Recasage :

• • • • • 126 : Exemples d'équations en arithmétique.
• • • • ○ 121 : Nombres premiers. Applications.
• • • • ○ 122 : Anneaux principaux. Applications.

Résumé:

Certains nombres premiers sont sommes de deux carrés, par exemple : $2 = 1^2 + 1^2$, $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$. En revanche, d'autres comme 3, 7, 11 et 19 ne se décomposent pas ainsi. Le théorème des deux carrés de Fermat nous fournit un critère général permettant de répondre à ce problème.

Prérequis:

Entiers de Gauss - Anneaux principaux - Carrés de $\mathbb{F}_p$ - Nombres premiers

---

Théorème : Soient $\Sigma = \{n \in \mathbb{N} \mid n = a^2 + b^2;\ a, b \in \mathbb{N}\}$ et p un nombre premier. On a l'équivalence suivante :

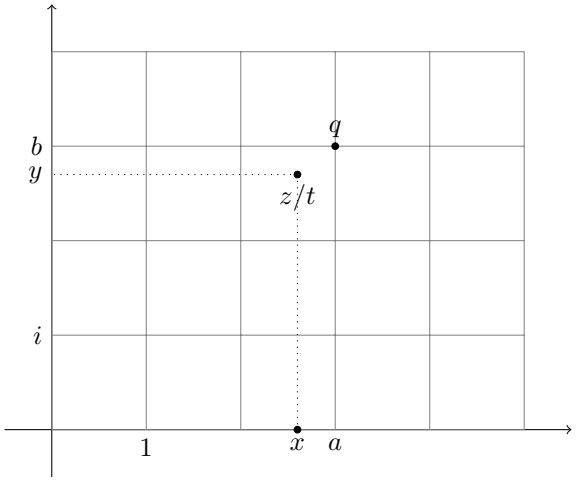
$$p \in \Sigma \Leftrightarrow p = 2 \text{ ou } p \equiv 1 \pmod 4$$

Démonstration. Richard Dedekind est l'auteur de la démonstration proposée ci-après. Elle utilise l'anneau euclidien des entiers de Gauss $\mathbb{Z}[i] = \{a + ib;\ a, b \in \mathbb{Z}\}$.

Etape 1 - Montrons que $\mathbb{Z}[i]$ est euclidien et $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$:

• Considérons la "norme" $N(z) = z\overline{z} = a^2 + b^2$ pour $z \in \mathbb{Z}[i]$.
Soient $z, t \in \mathbb{Z}[i]\backslash\{0\}$. On approxime $z/t = x + iy$ par un entier de Gauss $q = a + ib$ le plus proche de z/t.

Un dessin pour mieux comprendre tout ça



On a donc

$$|z/t - q| = |(x-a) + i(y-b)| = \sqrt{\underbrace{(x-a)^2}_{\leq \frac{1}{2}} + \underbrace{(y-b)^2}_{\leq \frac{1}{2}}} \leq \frac{\sqrt{2}}{2} < 1$$

Soit $r = z - qt \in \mathbb{Z}[i]$ et on a :

$$|r| = |t(z/t - q)| = |t|\ |z/t - q| < |t| \quad \Rightarrow \quad N(r) < N(t)$$

On a donc bien $z = qt + r$ avec $N(r) < N(t)$ et donc $\mathbb{Z}[i]$ est euclidien.

• On a $\{\pm 1, \pm i\} \subset \mathbb{Z}[i]^*$. Il reste donc à montrer l'inclusion réciproque.
Soit $z = a + ib \in \mathbb{Z}[i]^*$, alors il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$ d'où $1 = N(zz') = N(z)N(z')$ et donc $N(z) = 1$. Or $N(z) = a^2 + b^2$ donc $a^2 + b^2 = 1$ implique ($a = 0$ et $b = \pm 1$) ou ($a = \pm 1$ et $b = 0$). Donc $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Etape 2 - Montrons que ($p \in \Sigma$) $\Leftrightarrow$ (p n'est pas irréductible dans $\mathbb{Z}[i]$) :

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

Etape 3 - Montrons que (p n'est pas irréductible dans $\mathbb{Z}[i]$) $\Leftrightarrow$ ($-1 \in \mathbb{F}_p^{*2}$) :

Comme $\mathbb{Z}[i]$ est principal, donc factoriel, dire que p est non irréductible est équivalent à dire que l'idéal (p) est non premier et donc que le quotient $\mathbb{Z}[i]/(p)$ est non intègre. Or on a :

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

Par suite,

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

Etape 4 - Montrons que $(-1 \in \mathbb{F}_p^{*2}) \Leftrightarrow (p = 2 \text{ ou } p \equiv 1 \pmod 4)$:

- $p = 2$, $-1 = 1 = 1^2$
- $p > 2$, $x \in \mathbb{F}_p^{*2} \Leftrightarrow x^{\frac{p-1}{2}} = 1$. En effet :

Posons $X = \{x \in \mathbb{F}_p \mid x^{\frac{p-1}{2}} = 1\}$. On a $|X| \leq \frac{p-1}{2}$. D'autre part, si $x \in \mathbb{F}_p^{*2}$, il existe $y \in \mathbb{F}_p^*$ tel que $x = y^2$ donc $x^{\frac{p-1}{2}} = y^{p-1} = 1$ et ainsi $\mathbb{F}_p^{*2} \subset X$, et comme $|\mathbb{F}_p^{*2}| = \frac{p-1}{2}$, on a $X = \mathbb{F}_p^{*2}$. Finalement,

$$-1 \in \mathbb{F}_p^{*2} \Leftrightarrow \frac{p-1}{2} \text{ est pair } \Leftrightarrow p \equiv 1 \pmod 4$$

□

Remarques :

- Dans la démonstration, on a utilisé le lemme suivant :

> **Lemme :**
> Soit A un anneau principal. Les conditions équivalentes suivantes :
> 1. p est premier,
> 2. p est irréductible.

Démonstration : 1 ⇒ 2 : (en fait, cette implication est vraie pour un anneau intègre) Soient p premier et $a, b \in A$ tels que $p = ab$. Alors

$$\begin{aligned} ab = p &\Rightarrow p|a \text{ ou } p|b \\ &\Rightarrow \exists\, a', b' \in A \text{ tel que } a = a'p \text{ ou } b = b'p \\ &\Rightarrow \exists\, a', b' \in A \text{ tel que } p = a'bp \text{ ou } p = ab'p \\ &\Rightarrow \exists\, a', b' \in A \text{ tel que } (1 - a'b)p = 0 \text{ ou } (1 - ab')p = 0 \\ &\Rightarrow \exists\, a', b' \in A \text{ tel que } a'b = 1 \text{ ou } ab' = 1 \text{ car } A \text{ est intègre et } p \neq 0 \\ &\Rightarrow b \text{ est inversible ou } a \text{ est inversible} \\ &\Rightarrow p \text{ est irréductible} \end{aligned}$$

2 ⇐ 1 : Soient $\mathcal{P}$ l'ensemble des irréductibles de A, $p, a, b \in A$ avec p irréductible et $p|ab$. Alors en écrivant les factorisations en irréductibles de a et b, on obtient

$$a = u \prod_{q \in \mathcal{P}} q^{v_q(a)} \quad \text{et} \quad b = v \prod_{q \in \mathcal{P}} q^{v_q(b)} \quad \Rightarrow \quad p|ab = uv \prod_{q \in \mathcal{P}} q^{v_q(a)+v_q(b)}$$

avec u, v des éléments inversibles.
Comme l'écriture est unique (et que p est irréductible), p est nécessairement un facteur irréductible de a ou de b, donc $p|a$ ou $p|b$. Par conséquent, a est premier.

□

- Plus technique, on a utilisé les isomorphismes suivants :

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

Soyons professionels, et donnons au moins une justification à l'isomorphisme :

$$(\mathbb{Z}[X]/(X^2+1))/(p) \xleftarrow{\sim} \mathbb{Z}[X]/(X^2+1, p)$$

Considérons le très appétissant diagramme suivant :

$$\begin{array}{ccc} \mathbb{Z}[X] & \xrightarrow{\pi_1} & \mathbb{Z}[X]/(X^2+1,p) \\ \downarrow{\scriptstyle \pi_2} & \overset{\varphi}{\nearrow} & \uparrow{\scriptstyle \psi} \\ \mathbb{Z}[X]/(X^2+1) & \xrightarrow[\pi_3]{} & (\mathbb{Z}[X]/(X^2+1))/(p) \end{array}$$

où les π_i désignent les morphismes de projection.
Le premier théorème d'isomorphisme appliqué à π_1 donne d'une part :
comme $(X^2+1) \subset \mathrm{Ker}\pi_1 = (X^2+1,p)$, alors π_1 se factorise par $\mathbb{Z}[X]/(X^2+1)$: il existe un morphisme $\varphi : \mathbb{Z}[X]/(X^2+1) \to \mathbb{Z}[X]/(X^2+1,p)$ tel que $\pi_1 = \varphi \circ \pi_2$.
Le même premier théorème d'isomorphisme appliqué à φ donne d'autre part :
comme $(p) \subset \mathrm{Ker}\varphi = \pi_2(\mathrm{Ker}\pi_1) = (p)$, alors φ se factorise par $(\mathbb{Z}[X]/(X^2+1))/(p)$: il existe un morphisme $\psi : (\mathbb{Z}[X]/(X^2+1))/(p) \to \mathbb{Z}[X]/(X^2+1,p)$ tel que $\varphi = \psi \circ \pi_3$.
Finalement, comme π_1 est surjectif, alors φ puis ψ le sont également; par ailleurs, $\mathrm{Ker}\psi = \pi_3(\mathrm{Ker}\varphi) = (0)$: ψ est par conséquent un isomorphisme, ce qui prouve que $(\mathbb{Z}[X]/(X^2+1))/(p) \xleftarrow{\sim} \mathbb{Z}[X]/(X^2+1,p)$.

- On peut généraliser ce théorème aux entiers. Si, dans un premier temps, on écrit les entiers inférieurs à 50 sur quatre lignes, en fonction du reste de leur division par quatre, on obtient :

	4	8	12	16	20	24	28	32	36	40	44	48
1	5	9	13	17	21	25	29	33	37	41	45	49
2	6	10	14	18	22	26	30	34	38	42	46	50
3	7	11	15	19	23	27	31	35	39	43	47	

Les entiers entourés sont ceux qui peuvent s'écrire comme somme de deux carrés, et les autres sont ceux pour lesquels une telle écriture est impossible. On constate que la quatrième ligne ne contient pas de solution. Le théorème suivant nous fournit une réponse :

Corollaire : Un entier est somme de deux carrés si et seulement si chacun de ses facteurs premiers de la forme $4k+3$ intervient à une puissance paire.

Démonstration :

□

Ainsi $30 = 2 \times 3 \times 5$ n'est pas somme de carrés car dans sa décomposition en facteurs premiers, 3 intervient avec un exposant 1. En revanche, $45 = 32 \times 5$ est somme de carrés, car 3 intervient à la puissance 2 (on trouve bien que $45 = 6^2 + 3^2$).

- Irréductibles de $\mathbb{Z}[i]$
- Résultats connexes Wikip
- L'identité de Diophante dit que le produit de deux nombres, égaux chacun à une somme de deux carrés, est lui-même une somme de deux carrés :

$$\forall a,b,c,d \in A \quad (a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2,$$

où A désigne un anneau commutatif.

Si $u = a+ib$ et $v = c+id$ avec $a,b,c,d \in \mathbb{R}$, l'identité de Diophante devient $|u|^2|v|^2 = |uv|^2$ qui n'est rien d'autre que la multiplicativité du module d'un nombre complexe.

Encore plus fort, encore plus loin, l'identité des quatre carrés d'Euler (qui dit que le produit de deux nombres, chacun étant la somme de quatre carrés, est lui-même une somme de quatre carrés) peut être vue comme une généralisation de l'identité de Diophante, utilisant la norme des quaternions.

L'identité des quatre carrés d'Euler :

$$\begin{aligned}(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2) =&(ap+bq+cr+ds)^2+\\ &(aq-bp-\varepsilon cs+\varepsilon dr)^2+\\ &(ar+\varepsilon bs-cp-\varepsilon dq)^2+\\ &(as-\varepsilon br+\varepsilon cq-dp)^2, \quad \text{pour} \quad \varepsilon=\pm 1.\end{aligned}$$

- Si une somme de trois carrés est divisible par 4 alors les trois carrés le sont.
- Condition nécessaire pour que p soit somme de deux carrés :

Proposition : Un entier de la forme $4k-1$ n'est jamais somme de deux carrés de rationnels.

Démonstration :

□