# Sur les sommes de carrés

Gilles Auriol - auriolg@wanadoo.fr
http ://perso.wanadoo.fr/gilles.auriol/

18 août 2003

## Table des matières



# 1 Somme de deux carrés

## 1.1 Version élémentaire

Dans cette partie nous allons donner des caractérisations de nombres qui sont sommes de deux carrés avec des outils très élémentaires. Pas de corps, ni de $\mathbb{Z}[i]$, ni d'anneaux euclidiens. L'ensemble est accessible à un élève de Terminale S, le point difficile résidant dans la démonstration du théorème de Wilson (que l'on pourra admettre)

### 1.1.1 Théorème de Wilson

**Proposition 1.1.** *Soit $p$ un entier premier, alors $x^2 \equiv 1\,[p] \iff (x \equiv 1\,[p]$ ou $x \equiv -1\,[p])$.*

*Démonstration.* $x^2 \equiv 1\,[p] \iff \exists k \in \mathbb{N}$ t.q. $x^2 - 1 = kp \iff \exists k \in \mathbb{N}$ t.q. $(x-1)(x+1) = kp$ d'où l'on déduit, grâce au théorème de Gauss puisque $p$ est premier, que $p$ divise $x-1$ ou[1] que $p$ divise $x+1$. Dans le premier cas il existe $k' \in \mathbb{N}$ tel que $x - 1 = pk'$ d'où $x \equiv 1\,[p]$, dans le second il existe $k'' \in \mathbb{N}$ tel que $x + 1 = pk''$ d'où $x \equiv -1\,[p]$.

[1] c'est l'un ou l'autre, mais pas les deux en même temps ; il s'agit donc d'un ou exclusif.

Réciproquement, si $x = 1 + pk'$, alors $x^2 = 1 + 2pk' = p^2k'^2 \equiv 1\,[p]$. On vérifie de même la solution $x \equiv -1\,[p]$. □

**Remarque 1.2.** *L'équivalence de la proposition n'est pas une banalité. Par exemple pour* $p = 8$ *(qui n'est pas premier),* $x^2 \equiv 1\,[8] \iff (x \equiv 1\,[8]$ *ou* $x \equiv 3\,[8]$ *ou* $x \equiv 5\,[8]$ *ou* $x \equiv 7\,[8])$.

**Définition 1.3.** *L'entier* $x$ *et dit inversible modulo* $p$ *s'il existe un entier* $y$ *tel que* $xy \equiv 1\,[p]$.

**Théorème 1.4 (de Wilson).** $p$ *est premier* $\iff (p-1)! \equiv -1\,[p]$.

*Démonstration.* ($\Longrightarrow$) Soit $A = \{1, 2, \ldots, p-1\}$. Fixons $x$ dans $A$ et considérons l'application $f_x : A \to A$ qui à tout $y$ de $A$ associe le reste $r$ dans la division par $p$ de $xy$, qui n'est pas 0 puisque $p$ ne divise ni $x$ ni $y$.
L'application $f_x$ est bijective. Pour cela il suffit de montrer qu'elle est injective, car $f_x$ est une application entre ensemble de même cardinal. Si $f_x(y) = f_x(y') = r$ alors il existe $(k, k') \in \mathbb{Z}^2$ tel que $xy = pk + r$ et $xy' = pk' + r$, et par soustraction on obtient que $x(y - y')$ est divisible par $p$. L'entier $x$ n'étant pas divisible par $p$, c'est $|y - y'|$ qui l'est[2]. Or $|y - y'| < p$, donc $|y - y'| = 0$ et $y = y'$.
La bijectivité de $f_x$ est prouvée, en particulier il existe donc un seul $r \in A$ tel que $f(r) = 1$, c'est-à-dire tel qu'il existe $k \in \mathbb{Z}$ avec $xr = 1 + pk$ ou $xr \equiv 1\,[p]$.
Maintenant que nous savons que tous les éléments de $A$ sont inversibles modulo $p$ et que leur inverse est unique, cherchons quels sont ceux qui sont leur propre inverse. Ceci n'a lieu que si $p^2 \equiv 1\,[p]$ et d'après la proposition précédente cela n'a lieu que pour 1 et $p - 1$. Posons $A' = \{2, \ldots, p-2\}$ (et supposons $p \geqslant 5$), alors à chaque $a \in A'$, on peut associer l'unique $a' \in A'$ avec $a \neq a'$ tel que $aa' \equiv 1\,[p]$, on obtient ainsi $\dfrac{p-3}{2}$ paires $\{a, a'\}$ distinctes. Le produit des éléments de $A'$ vaut donc 1, d'où

$$(p-1)! = 1 \times (p-1) \times (a_1 a'_1) \times \cdots \times (a_{(p-3)/2} a'_{(p-3)/2}) \equiv p - 1 \equiv -1\,[p]$$

Les cas $p = 2$ ou $p = 3$ se vérifient à la main.

($\Longleftarrow$) Supposons que $p$ soit composé : il existe deux entiers $a$ et $b$ avec $p = ab$ et $1 < a \leqslant b < m$.
- Si $a < b$, alors $p = ab$ divise $(p-1)!$ et $(p-1)! \equiv 0 \not\equiv -1\,[p]$ ;
- Si $a = b$, alors $m = a^2$.
  - Si $a = 2$, alors $(a^2 - 1)! = 3! = 6 \equiv 2 \not\equiv -1\,[4]$
  - Si $a > 2$, alors $a^2 > 2a$ et $a$ et $2a$ sont des facteurs de $(a^2 - 1)!$, donc $2a^2$ divise $(a^2 - 1)!$, donc $(a^2 - 1)! \equiv 0 \not\equiv -1\,[a^2]$.

□

### 1.1.2 Cas d'un nombre premier impair

**Théorème 1.5.** *(Théorème 1.1.1 p.12 de [Des86])*
*Pour tout réel* $\xi$ *et pour tout réel* $H > 1$*, il existe un couple* $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ *tel que* $q < H$ *et* $|\, q\xi - p \,| \leqslant \dfrac{1}{H}$.

*Démonstration.* Supposons d'abord $H$ entier. Le nombre 1 et les $H$ nombres $i\xi - [i\xi]$, où $i \in [\![0, H-1]\!]$ et où $[i\xi]$ désigne la partie entière de $i\xi$, appartiennent tous à $[0, 1]$. Deux au moins de ces $H + 1$ nombres ont donc une distance mutuelle inférieure ou égale à $\dfrac{1}{H}$.

[2]Pour ceux qui ne sont pas convaincus, on a facilement l'encadrement $-p + 2 \leqslant y - y' \leqslant p - 2$, équivalent à $|y - y'| \leqslant p - 2$ et si $a$ divise $b$, alors $-a$ divise $b$

– Si ces deux nombres sont $i\xi - [i\xi]$ et $i\xi' - [i'\xi]$ avec $i < i'$, le choix $q = i' - i$ et $p = i'\xi - [i\xi]$ conduit à $0 < q < H$ et $|\, q\xi - p\,| = |\, i'\xi - [i'\xi] - (i\xi - [i\xi])\,| \leqslant \dfrac{1}{H}$.

– Si ces deux nombres sont $i\xi - [i\xi]$ et 1, le choix $q = i < H$ et $p = [i\xi] + 1$ donne $|\, q\xi - p\,| \leqslant \dfrac{1}{H}$ et $q > 0$.

Supposons maintenant $H > 1$ non entier, et posons $H' = [H] + 1$. La première partie de la démonstration établit l'existence de $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $0 < q < H'$ et $|\, q\xi - p\,| \leqslant \dfrac{1}{H'} < \dfrac{1}{H}$ avec, puisque $q$ est un entier et que $H$ ne l'est pas, $q < H$. □

**Lemme 1.6.** *Soit $p$ un nombre premier congru à 1 modulo 4, alors* $\left(\left(\dfrac{p-1}{2}\right)!\right)^2 \equiv -1\,[p]$.

*Démonstration.* Soit $p$ un nombre premier. $p \equiv 1\,[4] \iff \dfrac{p-1}{2}$ est pair, donc d'après le théorème de Wilson,

$$\begin{aligned}
-1 \equiv (p-1)! &\equiv 1 \times 2 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(\frac{p+1}{2}\right) \times \cdots \times (p-2) \times (p-1) \\
&\equiv 1 \times 2 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(-\frac{p-1}{2}\right) \times \cdots \times (-2) \times (-1) \\
&\equiv (-1)^{(p-1)/2} \left(\frac{p-1}{2}\right)! \left(\frac{p-1}{2}\right)! \quad [p]
\end{aligned}$$

□

**Théorème 1.7.** *Un nombre premier impair est la somme de deux carrés d'entiers si et seulement s'il est congru à 1 modulo 4.*

*Démonstration.* ($\Longrightarrow$) Si $p = a^2 + b^2$, alors $a^2$ et $b^2$ sont de parités différentes (puisque "impair + impair = pair + pair = pair"). Par ailleurs un nombre et son carré ont même parité, puisque $(2k)^2 = 4k^2$ et $(2k+1)^2 = 2(2k^2 + 2k) + 1$. Donc $a$ et $b$ ont une parité différente et pour fixer les idées, disons $a$ pair et $b$ impair. Il existe donc $(k, k') \in \mathbb{N}^2$ tel que $a = 2k$ et $a = 2k' + 1$ d'où $p = a^2 + b^2 = 4(k^2 + k'^2 + k') + 1 \equiv 1\,[4]$.

($\Longleftarrow$) Nous suivons [Des86], théorème 1.1.4 p. 13.
Si $n \equiv 1\,[4]$, il existe un $m$ tel que $m^2 + 1 \equiv 0\,[n]$ d'après le lemme 1.6. Appliquons le théorème 1.5 en choisissant $\xi = \dfrac{m}{n}$ et $H = \sqrt{n}$ $(> 1)$ ; il existe $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $q < \sqrt{n}$ et $\left|\, q\dfrac{m}{n} - p\,\right| \leqslant \dfrac{1}{\sqrt{n}}$. Le choix $r = qm - pn$ donne, après multiplication de cette inégalité par $n > 0$, $|\, r\,| \leqslant \sqrt{n}$ où $r^2 \leqslant n$ [**1**]. D'autre part $q < \sqrt{n} \Longrightarrow 0 < q^2 < n$ d'où $0 < q^2 + r^2 < 2n$ en ajoutant à [1].
Mais on a aussi $q^2 + r^2 \equiv q^2 + q^2m^2 = q^2(1 + m^2) \equiv 0\,[n]$ et puisque $0 < q^2 + r^2 < 2n$, on arrive bien la conclusion voulue, $q^2 + r^2 = n$. □

## 1.2 Version licence

Maintenant nous allons redémontrer le théorème 1.7 en utilisant l'algèbre enseignée en licence. Nous pourrons ensuite caractériser tous les nombres qui sont sommes de deux carrés.

### 1.2.1 Théorème de Wilson

Redémontrons le théorème 1.4 en utilisant les corps finis.
Soit $p$ en entier premier.

*Démonstration.* ($\Longrightarrow$) L'ensemble $G = \mathbb{F}_p^*$ est un groupe pour la multiplication. Étant donné que $\text{Card}(G) = p-1$, le théorème de Lagrange permet d'écrire $\forall x \in G, x^{p-1} = 1$, c'est-à-dire que le polynôme $P(X) = X^{p-1} - 1$ admet comme racines $1, 2, \ldots, p-1$. Son degré étant $p-1$ il admet au plus $p-1$ racines. Donc les racines de $P$ sont exactement les éléments de $G$. Ainsi

$$P(X) = X^{p-1} - 1 = (X-1)(X-2)\ldots(X-(p-1))$$

d'où en développant et en comparant les termes constants

$$-1 = (-1)^{p-1} \times 1 \times 2 \times \cdots \times (p-1) = (-1)^{p-1}(p-1)!$$

Si $p = 2$, l'égalité est évidemment vraie. Si $p > 2$, alors $p-1$ est pair, et on a $-1 = (p-1)!$.

($\Longleftarrow$) Soit $C \in \mathbb{F}_p^*$, $a$ un élément de $\mathbb{Z}$ représentant de $C$. On peut supposer que $1 \leqslant a \leqslant p-1$, quitte à remplacer $a$ par son reste dans la division euclidienne par $p$. Par hypothèse

$$\prod_{i=1}^{p-1} i = -1 \quad \text{d'où} \quad -a \prod_{\substack{i=1 \\ i \neq a}}^{p-1} i = 1$$

ce qui prouve que $C$ est inversible dans $\mathbb{F}_p$, d'inverse $-\prod\limits_{\substack{i=1 \\ i \neq a}}^{p-1} i$, donc $\mathbb{F}_p$ est un corps, donc $p$ est premier. □

### 1.2.2 Caractérisation des carrés dans $\mathbb{F}_p$

Soit $p$ un nombre premier impair, on note $\mathbb{F}_p$ le corps à $p$ éléments, $\mathbb{F}_p^2 = \{x^2, x \in \mathbb{F}_p\}$ et $\mathbb{F}_p^{*2} = \mathbb{F}_p^* \cap \mathbb{F}_p^2$.

**Proposition 1.8.** *(Il s'agit de la proposition VII.52 de [Goz97] p.93)*
▶ $\mathbb{F}_p^{*2}$ *est un sous-groupe d'indice 2 de* $\mathbb{F}_p^*$ *; donc Card*$(\mathbb{F}_p^{*2}) = \dfrac{p-1}{2}$.
▶ $\mathbb{F}_p^{*2}$ *est le noyau de l'endormorphisme* $x \mapsto x^{\frac{p-1}{2}}$ *de* $\mathbb{F}_p^*$.

*Démonstration.* ▶ Clairement $f : x \mapsto x^2$ est un endomorphisme de groupe de $\mathbb{F}_p^*$, donc $\mathbb{F}_p^{*2} = \text{Im}(f)$ est un sous-groupe de $\mathbb{F}_p$, et est par décomposition canonique isomorphe à $\mathbb{F}_p^*/\ker(f)$. Or $\ker(f) = \{x \in \mathbb{F}_p / x^2 = 1\} = \{-1, 1\}$ et $-1 \neq 1$ car $p \neq 2$. Donc $\mathbb{F}_p^{*2}$ est un sous-groupe d'incide 2 de $\mathbb{F}_p^*$. D'où $\text{Card}(\mathbb{F}_p^{*2}) = \dfrac{\text{Card}(\mathbb{F}_p^*)}{2} = \dfrac{q-1}{2}$.
▶ Clairement $u : x \mapsto x^{\frac{p-1}{2}}$ est un endormorphisme de groupe de $\mathbb{F}_p^*$. Du théorème de Lagrange, il résulte que $\forall x \in \mathbb{F}_p^*, (u(x))^2 = x^{q-1} = 1$, donc $\text{Im}(u) \subseteq \{-1, 1\}$. Si $\text{Im}(u) = \{1\}$, on aurait $\forall x \in \mathbb{F}_p^*, u(x) = x^{\frac{q-1}{2}} = 1$ et le polynôme $X^{\frac{p-1}{2}} - 1$ de $\mathbb{F}_p[X]$ aurait $q-1$ racines : impossible. Donc $\text{Im}(u) = \{-1, 1\}$. D'où $\text{Card}(\ker(u)) = \dfrac{p-1}{2}$. Comme $\mathbb{F}_p^{*2} \subseteq \ker(u)$ et comme $\text{Card}(\mathbb{F}_p^{*2}) = \dfrac{p-1}{2}$, il vient $\mathbb{F}_p^{*2} = \ker(u)$. □

**Corollaire 1.9.** *-1 est un carré dans $\mathbb{F}_p \iff p \equiv 1\,[4]$.*

*Démonstration.* D'après la proposition, $-1$ est un carré dans $\mathbb{F}_p \iff (-1)^{\frac{p-1}{2}} = 1 \iff \dfrac{p-1}{2}$ est pair $\iff p \equiv 1\,[4]$. □

### 1.2.3 Quelques rappels sur les anneaux

**Définition 1.10.** *Un anneau $A$ est dit principal s'il est intègre et si tous ses idéaux sont principaux, c'est-à-dire que pour chaque idéal $I$, il existe $b \in I$ tel que $I = bA = \{ba, a \in A\}$.*

**Définition 1.11.** *Un anneau est dit euclidien s'il est intègre et s'il est muni d'un stathme euclidien, c'est-à-dire une application $f : A - \{0\}$ telle que*

$$\forall (a,b) \in A \times (A - \{0\}), \exists (a,b) \in A^2, a = bq + r \text{ et } (r = 0 \text{ ou } f(r) < f(b)).$$

Par exemple $\mathbb{Z}$ est euclidien en prenant $x \mapsto |x|$.

**Théorème 1.12.** *Tout anneau euclidien est principal.*

*Démonstration.* Soient $A$ un anneau euclidien, $f$ la division euclidienne associée et $I$ un idéal de $A$. Si $I$ est l'idéal nul, alors 0 engendre $I$ qui est donc principal. Sinon il existe $x_0 \in A$ non nul tel que $x_0 \in I$. En posant $\{E = f(x)\,;\, x \in I - \{0\}\}$ on constate que $E$ est une partie non vide $\mathbb{N}$ donc admet un plus petit élément $f(a)$ où $a \in I - \{0\}$. Considérons $b \in$. Il existe donc $(a,b) \in A^2$ tel que $b = aq + r$ avec $r = 0$ ou $f(r) < f(a)$. Or $r = b - aq \in I$, donc le caractère minimal de $f(a)$ impose que $r = 0$ c'est-à-dire que $b = aq$. Ainsi $I \subseteq aA$. L'inclusion inverse étant évidente, $I = aA$. □

**Définition 1.13.** *Un anneau $A$ est dit factoriel s'il est intègre, si tout élément $a$ non nul de $A$ s'écrit $a = up_1 \dots p_r$, avec $u$ inversible et $p_1 \dots p_r$ irréductibles et si cette décomposition est unique au sens suivant : si $a = up_1 \dots p_r = vq_1 \dots q_s$, on a $r = s$ et il existe $\sigma \in \mathfrak{S}_r$ tel que $p_i$ et $q_{\sigma(i)}$ soient associés.*

**Théorème 1.14.** *Tout anneau principal est factoriel.*

*Démonstration.* Admis. Voir l'excellent [Per96] corollaire 3.21 p.49. □

### 1.2.4 Présentation de $\mathbb{Z}[i]$

**Définition 1.15.** *Le sous-anneau commutatif de $\mathbb{C}$ formé des éléments $a + ib$ avec $(a,b) \in \mathbb{Z}^2$ est appelé l'anneau des entiers de Gauss et est noté $\mathbb{Z}[i]$.*

*Démonstration.* C'est évident. Associativité, commutativité et distributivité résultent de ce que $\mathbb{Z}[i] \subset \mathbb{C}$. □

**Proposition 1.16.** *L'anneau $\mathbb{Z}[i]$ est factoriel.*

*Démonstration.* Il suffit de prouver qu'il est euclidien d'après les théorèmes 1.12 et 1.14. L'intégrité est assurée par $\mathbb{Z}[i] \subset \mathbb{C}$. Soit $z = x + iy \in \mathbb{C}$, $(x,y) \in \mathbb{R}^2$. Il est clair qu'il existe $(x_0, y_0) \in \mathbb{Z}^2$ tel que $|x - x_0| \leqslant \dfrac{1}{2}$ et $|y - y_0| \leqslant \dfrac{1}{2}$. Posons alors $z_0 = x_0 + iy_0 \in \mathbb{Z}[i]$. On constate que :

$$|z - z_0|^2 = |(x - x_0) + i(y - y_0)|^2 = |x - x_0|^2 + |y - y_0|^2 \leqslant \frac{1}{2} + \frac{1}{2} < 1$$

En résumé, $\forall z \in \mathbb{C}, \exists z_0 \in \mathbb{Z}[i] \,/\, |z - z_0| < 1$.
Soit $(a, b) \in \mathbb{Z} \times (\mathbb{Z}[i] - \{0\})$. D'après ce qui vient d'être prouvé, il existe $z_0 \in \mathbb{Z}[i]$ tel que $\left|\frac{a}{b} - z_0\right| < 1$ soit $|a - bz_0| < |b|$. on constate alors que pour $q = z_0$ et $r = a - bz_0$,

$$\exists (q, r) \in \mathbb{Z}[i]^2 \,/\, a = bq + r \text{ où } |r| < |b|$$

En posant $f : \mathbb{Z}[i] - \{0\} \to \mathbb{N}$, $z \mapsto |z|^2$, on en déduit que $f$ est un stathme euclidien sur l'anneau intègre $\mathbb{Z}[i]$. $\square$

**Définition 1.17.** *L'application $f : z = a + ib \mapsto |z|^2 = a^2 + b^2$ ainsi définie vérifie $N(zz') = N(z)N(z')$. On l'appelle norme.*

**Proposition 1.18.** *On note $\mathbb{Z}[i]^*$ l'ensemble des éléments inversibles de $\mathbb{Z}[i]$. On dispose de l'équivalence $z \in \mathbb{Z}[i]^* \iff N(z) = 1$.*

*Démonstration.* ($\Longrightarrow$) Si $a \in \mathbb{Z}[i]^*$, il existe $b \in \mathbb{Z}[i]$ tel que $ab = 1$ d'où en prenant les normes, $N(a)N(b) = 1$. On en déduit que $N(a) = 1$.
($\Longleftarrow$) $N(a) = 1 \iff x^2 + y^2 = 1$, $(x, y) \in \mathbb{Z}^2$ en écrivant $a = x + iy$. Finalement les seules possibilités sont ($x^2 = 1$ et $y^2 = 0$) et ($x^2 = 0$ et $y^2 = 1$), ce qui conduit à $a \in \{i, -i, 1, -1\}$, éléments inversibles comme on le vérifie immédiatement. $\square$

### 1.2.5 Cas d'un nombre premier impair

On établit maintenant la condition suffisante du théorème 1.7.

**Proposition 1.19.** *Soit $p$ un entier premier impair, alors $p \equiv 1\,[4] \Longrightarrow p$ est une somme de deux carrés.*

*Démonstration.* Supposons $p$ premier $\equiv 1\,[4]$, alors $-1 \in \mathbb{F}_p^{*2}$ d'après le corollaire 1.9, donc il existe $x \in \mathbb{Z}$ tel que $x^2 + 1 \equiv 0\,[p]$ autrement dit il existe $x \in \mathbb{Z}$ tel que $p$ divise $x^2 + 1$.

Puisque $\mathbb{Z}[i]$ est factoriel, on en déduit que $p$ divise $x^2 + 1 = (x - i)(x + i)$. Par le théorème de Gauss, si $p$ est premier dans $\mathbb{Z}[i]$, alors $p$ divise $x + i$ ou $p$ divise $x - i$. Par exemple si $p$ divise $x + i$, alors il existe $(x_0, y_0) \in \mathbb{Z}^2$ tel que $x + i = px_0 + ipy_0$. On en déduit que $py_0 = 1$, c'est-à-dire que $p$ divise 1, ce qui est absurde... Aussi, $p$ n'est pas premier dans $\mathbb{Z}[i]$.

Il en résulte qu'il existe $(z_1, z_2) \in \mathbb{Z}[i]^2$ tel que $p = z_1 z_2$ avec $z_1$ et $z_2$ non inversibles dans $\mathbb{Z}[i]$. En passant aux normes, on en déduit que $p^2 = N(z_1)N(z_2)$, mais ni $N(z_1)$, ni $N(z_2)$ ne valent 1. Donc $N(z_1) = N(z_2) = p$ et il existe bien $(x_1, y_1) \in \mathbb{Z}^2$ tel que $p = x_1^2 + y_1^2$. $\square$

### 1.2.6 Cas général

**Théorème 1.20.** ▶ *Un entier naturel est une somme de deux carrés si et seulement si les facteurs premiers congrus à -1 modulo 4 de sa décomposition en produit de facteurs premiers y figurent avec un exposant pair (éventuellement nul).*
▶ *Pour que la décomposition soit unique, il faut et il suffit qu'en outre, $m$ n'admette qu'un seul facteur premier congru à 1 modulo 4 et que celui-ci figure dans la décomposition de $m$ avec l'exposant 1.*

*Démonstration.* ▶ Nous suivons [Duv98] p.62.
($\Longrightarrow$) Supposons que $n$ somme deux carrés, $n = a^2 + b^2$. Soit $\delta = PGCD(a, b)$ ; on a $n = \delta^2(c^2 + d^2)$, avec $c$ et $d$ premiers entre eux.

Soit $p$ un diviseur premier impair de $c^2+d^2$ ; alors $p|(c+id)(c-i)$ dans $\mathbb{Z}[i]$. Si $p$ était premier dans $\mathbb{Z}[i]$, il diviserait $c+id$ dans $\mathbb{Z}[i]$, donc aussi $c-id$ (en prenant les conjugués[3]), ainsi que la somme et la différence de ces nombres. Donc $p|2c$ et $p|2id$ dans $\mathbb{Z}[i]$ ; en prenant les normes $p^2|4c^2$ et $p^2|4d^2$ dans $\mathbb{Z}$ et puisque $p$ est premier impair, $p|c$ et $p|d$, contradiction avec l'hypothèse $c$ et $d$ premiers entre eux. Donc $p$ n'est pas premier dans $\mathbb{Z}[i]$ et $p=xy$, $x$ et $y$ non inversible dans $\mathbb{Z}[i]$.
Le même argument que dans la démonstration de la proposition 1.19 montre qu'en prenant les normes, il existe $(\alpha,\beta)\in\mathbb{Z}^2$ tel que $p=\alpha^2+\beta^2$, donc $p\equiv 1\,[4]$. Les seuls diviseurs premiers possibles de $c^2+d^2$ sont donc 2 et les nombres premiers congru à 1 modulo 4. Les nombres premiers congrus à $-1$ modulo 4 figurant éventuellement dans la décomposition de $n$ sont dans le $\delta^2$, donc ils y figurent avec un exposant pair.

($\Longleftarrow$) Si les nombres premiers $p_i$ congrus à $-1$ modulo 4 figurant dans la décomposition de $n$ y figurent avec un exposant pair, on a $n=2^\delta\left(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}\right)^2\cdot q_1^{\beta_1}q_2^{\beta_2}\dots q_m^{\beta_m}$. Les $q_i$ (qui sont donc congrus à 1 modulo 4) sont des sommes de deux carrés d'après la proposition 1.19. Donc en vertu de l'identité

$$(a^2+b^2)(c^2+d^2)=(ad+bc)^2+(ac-bd)^2 \tag{1}$$

l'entier $q_1^{\beta_1}q_2^{\beta_2}\dots q_m^{\beta_m}$ est somme de deux carrés ; posons $q_1^{\beta_1}q_2^{\beta_2}\dots q_m^{\beta_m}=a^2+b^2$. Il en résulte que $n=2^\delta\left((\gamma a)^2+(\gamma b)^2\right)$, où $\gamma=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$. Mais $2=1^2+1^2$, donc d'après l'identité (1), $n$ s'exprime bien comme une somme de deux carrés.

► Il s'agit de la proposition 3.6 p.63 de [Gob01]. □

# 2 Somme de trois carrés

**Théorème 2.1.** *Pour qu'un entier naturel $n$ soit somme de trois carrés, il faut et il suffit qu'il ne soit pas de la forme $4^h(8k+7)$ avec $(h,k)\in\mathbb{N}^2$.*

*Démonstration.* Ceci est au-dessus de mes moyens. Voir [Ser70] p.79 ou [Des86] p.136. □

# 3 Somme de quatre carrés

**Théorème 3.1.** *Tout entier naturel est somme de quatre carrés.*

Quand on a démontré le théorème des trois carrés, ceci n'est qu'une simple formalité.

*Démonstration.* En effet, si $a\in\mathbb{N}$ est la somme de de trois carrés, la conclusion est atteinte en ajoutant à cette somme un quatrième carré nul. Sinon $a$ est de la forme $4^h(8k+7)$ et $b=4^h(8k+6)$ est la somme de trois carrés, donc $a=b+4^h=b+\left(2^h\right)^2$ est la somme de quatre carrés. □

Pour démontrer le théorème 3.1, nous suivons [Mon03] p.128 et [Duv98] p.73. Nous aurons besoin du lemme suivant.

**Lemme 3.2.** *Soit $p$ un entier naturel premier impair. Alors il existe $(x,y)\in\left\{0,\dots,\dfrac{p-1}{2}\right\}^2$ tel que $1+x^2+y^2\equiv 0\,[p]$.*

[3] si $c+id=kp$ alors $c-id=\overline{kp}=\overline{k}p$ d'où $p|c-id$.

*Démonstration.* Considérons $f : X \mapsto X^2$ et $g : Y \mapsto -Y^2 - 1$, applications de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, on a

$$\forall (X_1, X_2) \in (\mathbb{Z}/p\mathbb{Z})^2, \quad f(X_1) = f(X_2) \Longleftrightarrow X_2 = -X_1 \text{ ou } X_2 = X_1.$$

Ainsi $f(\mathbb{Z}/p\mathbb{Z})$ a exactement $\dfrac{p+1}{2}$ éléments qui sont $f(0), f(1), \dots f\left(\dfrac{p-1}{2}\right)$.
Pour les mêmes raisons, $g(\mathbb{Z}/p\mathbb{Z})$ a exactement $\dfrac{p-1}{2}$ éléments ; on déduit

$$\mathrm{Card}(f(\mathbb{Z}/p\mathbb{Z})) + \mathrm{Card}(g(\mathbb{Z}/p\mathbb{Z})) = p + 1 > p = \mathrm{Card}(\mathbb{Z}/p\mathbb{Z})$$

donc $f(\mathbb{Z}/p\mathbb{Z}) \cap g(\mathbb{Z}/p\mathbb{Z}) \neq \emptyset$ et il existe $(a, b) \in \left\{0, \dots, \dfrac{p-1}{2}\right\}^2$ tel que $a^2 \equiv -b^2 - 1\,[p]$. □

Passons à la démonstration du théorème.

*Démonstration.* Elle est basée sur l'identité

$$\begin{aligned}(x^2 + y^2 + z^2 + t^2)&(x'^2 + y'^2 + z'^2 + t'^2)\\ &= (xx' + yy' + zz' + tt')^2 + (xy' - yx' + tz' - zt')^2\\ &+ (xz' - zx' + yt' - ty')^2 + (xt' - tx' + zy' - yz')^2 \qquad (2)\end{aligned}$$

liée à la théorie des quaternions, mais qui peut se vérifier directement[4].
Comme tout entier naturel peut se décomposer en un produit de facteurs premiers, il suffit de montrer, d'après l'identité (2), que tout entier premier impair est somme de quatre carrés (pour 2, on a immédiatement $2 = 1^2 + 1^2 + 0^2 + 0^2$).

Considérons donc $p$ premier impair. D'après le lemme 3.2, il existe $x$ et $y$ tels que $1 + x^2 + y^2 \equiv 0\,[p]$ avec $|x| < \dfrac{p}{2}$ et $|y| < \dfrac{p}{2}$, ainsi $1 < 1 + x^2 + y^2 < p^2$, et il existe $k$ tel que $1 + x^2 + y^2 = kp$, avec $1 \leqslant k \leqslant p - 1$. Il en résulte que l'ensemble

$$\{k \in [\![1, p-1]\!] ; \exists (a, b, c, d) \in \mathbb{N}^4 ; a^2 + b^2 + c^2 + d^2 = kp\}$$

est une partie non vide de $\mathbb{N}^*$ (il suffit de prendre $a = x$, $b = y$, $c = 1$ et $d = 0$ pour s'en convaincre) et admet un plus petit élément noté $m$.
L'entier $m$ est impair. En effet si $m$ était pair, 0, 2 ou 4 des nombres $a, b, c, d$ seraient pairs. Quitte à permuter $a, b, c, d$, on aurait :

$$(a, b, c, d \text{ pairs}) \quad \text{ou} \quad (a, b \text{ pairs et } c, d \text{ impairs}) \quad \text{ou} \quad (a, b, c, d \text{ impairs})$$

Dans tous les cas, $(a + b), (a - b), (c + d), (c - d)$ seraient pairs, et

$$\left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{m}{2}\,p$$

ce qui contredirait le caractère minimal de $m$.

Ainsi $m$ est impair ; supposons que $m \geqslant 3$. Soit $x, y, z, t$ les éléments de $\left\{-\dfrac{m-1}{2}, \dots, \dfrac{m-1}{2}\right\}$ congrus modulo $m$ à $a, b, c, d$ respectivement. Posons

$$n = x^2 + y^2 + z^2 + t^2.$$

[4] et ce n'est pas une partie de plaisir...

On a $n \equiv a^2 + b^2 + c^2 + d^2 \equiv 0\,[m]$ et $n > 0$ car

$$\begin{array}{rcl} n = 0 & \Longrightarrow & x = y = z = t = 0 \\ & \Longrightarrow & a \equiv 0 \text{ et } b \equiv 0 \text{ et } c \equiv 0 \text{ et } d \equiv 0\,[m] \\ & \Longrightarrow & a^2 + b^2 + c^2 + d^2 \equiv 0\,[m^2] \\ & \Longrightarrow & m^2 | a^2 + b^2 + c^2 + d^2 = mp \\ & \Longrightarrow & m | p \end{array}$$

impossible car $1 < m \leqslant p - 1$ et $p$ premier.
Comme $|x| \leqslant \dfrac{m-1}{2}, \dots, |t| \leqslant \dfrac{m-1}{2}$, on a $0 < n \leqslant 4 \times \left(\dfrac{m-1}{2}\right)^2 \leqslant (m-1)^2$. Ajouté au fait que $n \equiv 0\,[m]$, on en déduit que $n = um$, avec $1 \leqslant u \leqslant m - 1$. Puisque

$$um = x^2 + y^2 + z^2 + t^2 \qquad \text{et} \qquad mp = a^2 + b^2 + c^2 + d^2$$

on a, d'après l'identité (2),

$$(um)(mp) = A^2 + B^2 + C^2 + D^2$$

où

$$\left\{ \begin{array}{rcl} A & = & ax + by + cz + dt \\ B & = & ay - bx + ct - dz \\ C & = & az - bt - cx + dy \\ D & = & at + bz - cy - dx \end{array} \right.$$

D'autre part modulo $m$ :

$$\left\{ \begin{array}{rcl} A & \equiv & x^2 + y^2 + z^2 + t^2 \equiv 0\,[m] \\ B & \equiv & xy - yx + zt - tz = 0\,[m] \\ C & \equiv & xz - yt - zx + ty = 0\,[m] \\ D & \equiv & xt + yz - zy - tx = 0\,[m] \end{array} \right.$$

donc il existe $(\alpha, \beta, \gamma, \delta) \in \mathbb{Z}^4$ tels que $A = m\alpha$, $B = m\beta$, $C = m\gamma$ et $D = m\delta$. Par suite,

$$(um)(mp) = A^2 + B^2 + C^2 + D^2 = m^2\alpha^2 + m^2\beta^2 + m^2\gamma^2 + m^2\delta^2$$

ce qui donne, après simplification par $m^2$,

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = up$$

avec, rappelons-le, $1 \leqslant u \leqslant m - 1$. Ceci contredit donc la caractère minimal de $m$ et par conséquent $m = 1$. Le théorème de Lagrange est démontré. □

# Références


[Des86] Descombes, R., *Élements de théorie des nombres*. PUF, 1986.

[Duv98] Duverney, D., *Théorie des nombres*. Dunod, 1998.

[Gob01] Goblot, R., *Algèbre commutative*. Dunod, 2001.

[Goz97] Gozard, Y., *Théorie de Galois*. Ellipses, 1997.

[Mon03] Monier, J.-M., *Algèbre MPSI*. Dunod, 2003.

[Per96] Perrin, D., *Cours d'algèbre*. Ellipses, 1996.

[Ser70] Serre, J.-P., *Cours d'arithmétique*. PUF, 1970.