Sur les sommes de carrés

Gilles Auriol
auriolg@free.fr — http ://auriolg.free.fr

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. L'ensemble est accessible à un élève de Terminale S.

1.1.1 Théorème de Wilson

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

Preuve. — $x^2 \equiv 1\,[p] \iff \exists k \in \mathbb{N}$ 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 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 $x \equiv -1\,[p]$.
Réciproquement, si $x = 1 + pk'$, alors $x^2 = 1 + 2pk' + p^2k'^2 \equiv 1\,[p]$. On vérifie de même la solution $x \equiv -1\,[p]$.
Si $p = 2$, on a $-1 \equiv 1\,[2]$, donc il n'y a qu'une solution, à savoir $x \equiv 1\,[p]$. ∎

1.2 Remarque. — 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 $x \equiv 7\,[8])$.

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

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

Preuve. — ($\Longrightarrow$) 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. Or $|y - y'| < p$ (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), 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 directement.

($\Longleftarrow$) Si n est un diviseur strict de p alors il est un facteur de $(p-1)!$ et $(p-1)! \equiv 0\,[n]$. Or si l'on suppose $(p-1)! \equiv -1\,[p]$, on a aussi $(p-1)! \equiv -1\,[n]$ d'où $0 \equiv -1\,[n]$, ce qui est faux car $n > 1$. Ainsi p est premier. ∎

1.1.2 Cas d'un nombre premier impair

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

Preuve. — 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 $\dfrac{1}{H}$.

- 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, $q < H$. ∎

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

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

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

■

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

Preuve. — ($\Longrightarrow$) 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 $p = a^2 + b^2 = 4(k^2 + k'^2 + k') + 1 \equiv 1\,[4]$.

($\Longleftarrow$) **Preuve 1**. Nous suivons [Des86], théorème 1.1.4 p. 13.
Si $p \equiv 1\,[4]$, il existe un m tel que $m^2+1 \equiv 0\,[p]$ d'après le lemme 1.6. Appliquons le théorème 1.5 en choisissant $\xi = \dfrac{m}{p}$ et $H = \sqrt{p}\,(> 1)$; il existe $(s,t) \in \mathbb{Z}\times\mathbb{N}^*$ tel que $t < \sqrt{p}$ et $\left| t\,\dfrac{m}{p} - s \right| \leqslant \dfrac{1}{\sqrt{p}}$.
Le choix $r = tm - sp$ donne, après multiplication de cette inégalité par $p > 0$, $|\,r\,| \leqslant \sqrt{p}$ ou $r^2 \leqslant p$ [**1**]. D'autre part $t < \sqrt{p} \Longrightarrow 0 < t^2 < p$ d'où $0 < t^2 + r^2 < 2p$ en ajoutant à [1].
Mais on a aussi $t^2 + r^2 \equiv t^2 + t^2m^2 = t^2(1+m^2) \equiv 0\,[p]$ et puisque $0 < t^2 + r^2 < 2p$, on arrive bien la conclusion voulue, $t^2 + r^2 = p$.

Preuve 2. Nous nous inspirons cette fois-ci du §20.4 p.300 de [HW60].
Soit $p \equiv 1\,[4]$. D'après le lemme 1.6, il existe x tel que $x^2 + 1 \equiv 0\,[p]$. On peut choisir x avec $|x| < \dfrac{p}{2}$ (l'égalité pouvant être strict car p est impair) de sorte que $0 < 1 + x^2 < p^2$, donc il existe k avec $0 < k < p$ tel que $x^2 + 1 = kp$. Il en résulte que l'ensemble

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

n'est pas vide (il suffit de faire $a = x$ et $b = 1$ pour voir qu'il contient au moins un élément), donc en tant que partie non vide de $\mathbb{N}$ il admet un plus petit élément noté m.

Suppons $m > 1$ (c'est-à-dire $1 < m \leqslant p-1$).
Soient x et y les entiers congrus modulo m à a et b respectivement, tels que $|x| \leqslant \dfrac{m}{2}$ et $|y| \leqslant \dfrac{m}{2}$ (cette fois-ci on ne peut pas prendre une inégalité stricte car m peut être pair). On a alors $x^2 + y^2 \equiv a^2 + b^2 \equiv 0\,[m]$ et $x^2 + y^2 \leqslant 2 \times \left(\dfrac{m}{2}\right)^2 < m^2$. En outre x et y ne peuvent pas être nuls, car cela traduirait que m divise a et b et dans ce cas m^2 diviserait $a^2 + b^2 = pm$, donc m^2 diviserait pm ou encore m diviserait p, ce qui est impossible car $1 < m \leqslant p-1$ d'après l'hypothèse. Finalement de $0 < x^2 + y^2 < m^2$ et $x^2 + y^2 \equiv 0\,[m]$ on déduit que

$$x^2 + y^2 = um \quad \text{avec} \quad 0 < u < m.$$

Comme $a^2+b^2=mp$ et $x^2+y^2=um$, une multiplication membre à membre donne

$$m^2up=(a^2+b^2)(x^2+y^2)=A^2+B^2$$

avec, en vertu de l'identité de Euler[1]

$$\left\{\begin{array}{rcl} A & = & ax+by \\ B & = & ay-bx \end{array}\right.$$

Or modulo m, les entiers A et B deviennent

$$\left\{\begin{array}{rcl} A & \equiv & x^2+y^2\equiv 0\,[m] \\ B & \equiv & xy-yx=0\,[m] \end{array}\right.$$

Il existe donc $(\alpha,\beta)\in\mathbb{Z}^2$ tel que $A=m\alpha$ et $B=m\beta$ d'où

$$m^2up=m^2\alpha^2+m^2\beta^2$$

ou encore $up=\alpha^2+\beta^2$ après simplification par m^2, ce qui contredit le caractère minimal de m, puisque $0<u<m$. Ainsi $m=1$. ∎

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 un entier premier. On note $\mathbb{F}_p$ le corps à p éléments.

Preuve. — ($\Longrightarrow$) L'ensemble $G=\mathbb{F}_p^*$ est un groupe pour la multiplication. Etant donné que $\mathrm{card}(G)=p-1$, 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 $p=2$, un calcul direct montre que l'énoncé est vrai. Si $p\geqslant 3$, alors $p-1$ est pair, et on a $-1=(p-1)!$.

($\Longleftarrow$) Soit $C\in(\mathbb{Z}/p\mathbb{Z})-\{0\}$, 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 $(\mathbb{Z}/p\mathbb{Z})$, d'inverse $-\prod_{\substack{i=1\\ i\neq a}}^{p-1} i$, donc $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc p est premier. ∎

[1]Pour tout entier a,b,c,d, on a $(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2$, voir remarque 1.18

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

On note $\mathbb{F}_p^2 = \{x^2, x \in \mathbb{F}_p\}$ et $\mathbb{F}_p^{*2} = \mathbb{F}_p^* \cap \mathbb{F}_p^2$.

1.8 Proposition. — *(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* $\mathbb{F}_p^*$.

Preuve. — ▶ Clairement $f : x \mapsto x^2$ est un endomorphisme de groupe de $\mathbb{F}_p^*$, donc $\mathbb{F}_p^{*2} = \mathrm{Im}(f)$ 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'indice 2 de $\mathbb{F}_p^*$. D'où $\mathrm{Card}(\mathbb{F}_p^{*2}) = \dfrac{\mathrm{Card}(\mathbb{F}_p^*)}{2} = \dfrac{p-1}{2}$.
▶ 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 $\mathrm{Im}(u) \subseteq \{-1, 1\}$. Si $\mathrm{Im}(u) = \{1\}$, on aurait $\forall x \in \mathbb{F}_p^*, u(x) = x^{\frac{p-1}{2}} = 1$ et le polynôme $X^{\frac{p-1}{2}} - 1$ de $\mathbb{F}_p[X]$ aurait $p-1$ racines : impossible. Donc $\mathrm{Im}(u) = \{-1, 1\}$. D'où $\mathrm{Card}(\ker(u)) = \dfrac{p-1}{2}$. Comme $\mathbb{F}_p^{*2} \subseteq \ker(u)$ et comme $\mathrm{Card}(\mathbb{F}_p^{*2}) = \dfrac{p-1}{2}$, il vient $\mathbb{F}_p^{*2} = \ker(u)$. ∎

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

Preuve. — 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 $\iff p \equiv 1\,[4]$. ∎

1.10 Remarque. — Ceci généralise le lemme 1.6 qui ne démontre que ($\Longleftarrow$) mais qui explicite une solution de $x^2 = -1$, ce qui n'est pas le cas ici. De toutes façons, pour ce qu'on veut faire, il suffit de savoir qu'une solution existe.

1.2.3 Quelques rappels sur les anneaux

1.11 Définition. — *Un anneau* A *est dit principal s'il est intègre et si tous ses idéaux sont principaux, c'est-à-dire que chaque idéal est de la forme* $\{ba, a \in A\}$ *avec* $b \in A$.

1.12 Définition. — *Un anneau est dit euclidien s'il est intègre et s'il est muni d'un stathme euclidien, c'est-à-dire une application* $f : A - \{0\} \to \mathbb{N}$ *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 pour f le stathme $x \mapsto |x|$.

1.13 Théorème. — *Tout anneau euclidien est principal.*

Preuve. — Soient A un anneau euclidien, f le stathme euclidien associé 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 $b \in I$. 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, $I = aA$. ∎

1.14 Définition. — *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.*

1.15 Théorème. — *Tout anneau principal est factoriel.*

Preuve. — Voir par exemple [Per96] corollaire 3.21 p.49. ∎

1.2.4 Présentation de $\mathbb{Z}[i]$

1.16 Définition. — *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 $\mathbb{Z}[i]$.*

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

1.17 Définition. — *L'application $N : z = a + ib \mapsto |z|^2 = a^2 + b^2$ de $\mathbb{Z}[i]$ dans $\mathbb{N}$ vérifie $N(zz') = N(z)N(z')$. Cette application est appelée norme.*

Preuve. — $N(z) = |z|^2 = z\overline{z}$, donc en utilisant le fait que la conjugaison est un automorphisme de corps de $\mathbb{C}$, on obtient $N(zz') = zz'\overline{zz'} = zz'\overline{z}\overline{z'} = z\overline{z}z'\overline{z'} = N(z)N(z')$. ∎

1.18 Remarque. — On a $(a+ib)(c+id) = (ac-bd)+(ad+bc)i$, donc en passant aux normes $(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2$. Cette identité est attribuée à Euler ; elle montre en particulier que l'ensemble des nombres qui s'écrivent comme une somme de deux carrés est stable par multiplication.

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

Preuve. — Il suffit de prouver qu'il est euclidien d'après les théorèmes 1.13 et 1.15. 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 $|y - y_0| \leqslant \dfrac{1}{2}$ (x_0 et y_0 sont les entiers "les plus proches" de x et y). Posons alors $z_0 = x_0 + iy_0 \in \mathbb{Z}[i]$. On constate que :

$$|z - z_0|^2 = |(x - x_0) + i(y - y_0)|^2 = (x - x_0)^2 + (y - y_0)^2 \leqslant \frac{1}{4} + \frac{1}{4} < 1$$

En résumé, $\forall z \in \mathbb{C}, \exists z_0 \in \mathbb{Z}[i] \,/\, |z - z_0| < 1$.

Soit $(a,b) \in \mathbb{Z} \times (\mathbb{Z}[i] - \{0\})$, et effectuons la division euclidienne de a par b. D'après ce qui vient d'être prouvé, il existe $z_0 \in \mathbb{Z}[i]$ tel que $\left|\dfrac{a}{b} - z_0\right| < 1$ soit $|a - bz_0| < |b|$ ou encore en élevant au carré $N(a - bz_0) < N(b)$. On constate alors que pour $q = z_0$ et $r = a - bz_0$,

$$\exists (q,r) \in \mathbb{Z}[i]^2 \,/\, a = bq + r \text{ où } (N(r) < N(b) \text{ ou } r = 0)$$

le cas $r = 0$ ayant lieu si $\dfrac{a}{b} \in \mathbb{Z}[i]$. Donc N est un stathme euclidien sur l'anneau intègre $\mathbb{Z}[i]$. ∎

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

Preuve. — ($\Longrightarrow$) 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 $y^2 = 0$) ou ($x^2 = 0$ et $y^2 = 1$), ce qui conduit à $a \in \{i, -i, 1, -1\}$, éléments inversibles comme on le vérifie immédiatement. ∎

1.2.5 Cas d'un nombre premier impair

On établit maintenant la condition suffisante du théorème 1.7.

1.21 Proposition. — *Soit p un entier premier impair tel que $p \equiv 1\,[4]$. Alors p est une somme de deux carrés.*

Preuve. — 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. Ainsi 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 d'après 1.20. Donc $N(z_1) = N(z_2) = p$ et il existe bien $(x_1, y_1) \in \mathbb{Z}^2$ tel que $p = x_1^2 + y_1^2$. ∎

1.2.6 Cas général

1.22 Théorème. — ▶ *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, cet entier n'admette qu'un seul facteur premier congru à 1 modulo 4 et que celui-ci figure dans sa décomposition avec l'exposant 1.*

Preuve. — ▶ 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 $p|(c + id)(c - id)$ 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[2]), 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 $p = xy$, avec x et y non inversible dans $\mathbb{Z}[i]$.
Le même argument que dans la démonstration de la proposition 1.21 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 δ^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 $n = (p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k})^2 \cdot 2^\delta \cdot q_1^{\beta_1} q_2^{\beta_2} \dots q_m^{\beta_m}$. Les q_i (qui sont congrus à 1 modulo 4) sont des sommes de deux carrés d'après la proposition 1.21 et $2 = 1^2 + 1^2$, donc en vertu de la remarque 1.18 (l'ensemble des nombres sommes de deux carrés est stable par multiplication), l'entier $2^\delta \cdot q_1^{\beta_1} q_2^{\beta_2} \dots q_m^{\beta_m}$ est somme de deux carrés ; posons $2^\delta \cdot q_1^{\beta_1} q_2^{\beta_2} \dots q_m^{\beta_m} = a^2 + b^2$.

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

Il en résulte que $n = (\gamma a)^2 + (\gamma b)^2$, où $\gamma = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, donc n est une somme de deux carrés.

▶ Il s'agit de la proposition 3.6 p.63 de [Gob01]. ∎

1.3 Compléments

On note $r(n)$ le nombre de décompositions de l'entier n en somme de deux carrés. Quelques exemples pour voir quand deux décompositions sont dites distinctes :
- $0 = 0^2 + 0^2$ donc $r(0) = 1$;
- $1 = (\pm 1)^2 + 0^2 = 0^2 + (\pm 1)^2$ donc $r(1) = 4$;
- $5 = (\pm 1)^2 + (\pm 2)^2 = (\pm 2)^2 + (\pm 1)^2$ donc $r(5) = 8$.

1.23 Théorème. — *On a* $\lim\limits_{n\to\infty} \dfrac{r(1) + \dots + r(n)}{n} = \pi$.

Preuve. — Voir [HW60] §16.9 p.241 et théorème 339 p.270. ∎

2 Somme de trois carrés

2.1 Théorème. — *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 $(h,k) \in \mathbb{N}^2$.*

Preuve. — ($\Longrightarrow$) On raisonne par contraposition : montrons que les nombres de la forme $4^h(8k+7)$ ne peuvent pas s'écrire comme une somme de trois carrés en utilisant une récurrence sur $h \geqslant 0$.

Pour $h = 0$ la propriété est vraie car pour tout entier naturel x, on a $x^2 \equiv 0, 1$ ou $4\,[8]$, d'où pour $(x,y,z) \in \mathbb{N}^3$, $x^2 + y^2 + z^2 \equiv 0, 1, 2, 3, 4, 5$ ou $6\,[8]$ (essayer tous les cas), mais jamais 7. On a donc $x^2 + y^2 + z^2 \not\equiv 7$, c'est-à-dire $x^2 + y^2 + z^2 \neq 8k + 7$.

Supposons que l'entier $4^h(8k+7)$ ne soit pas somme de trois carrés. Comme $0^2 \equiv 2^2 \equiv 0\,[4]$ et $1^2 \equiv 3^2 \equiv 1\,[4]$, la congruence $x^2 + y^2 + z^2 \equiv 0\,[4]$ ne peut avoir lieu que si $x^2 \equiv y^2 \equiv z^2 \equiv 0\,[4]$, c'est-à-dire si x, y, z sont pairs. Alors si $4^{h+1}(8k+7) = x^2 + y^2 + z^2$ les entiers x, y et z sont pairs et en divisant par 4,

$$4^h(8k+7) = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2$$

ce qui est contraire à l'hypothèse de récurrence. Ainsi $4^{h+1}(8k+7)$ n'est pas une somme et trois carré et la condition nécessaire du théorème est démontrée.

($\Longleftarrow$) La démonstration de la condition suffisante dépasse le cadre de cet article[3]. Voir [Ser70] p.79 ou [Des86] p.136.

[3] Les outils mis en œuvre sont les formes quadratiques (sur $\mathbb{Q}$).

3 Somme de quatre carrés

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

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

Preuve. — 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 $4^h(8k+7)$, alors $b = 4^h(8k+6)$ 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 directement le théorème 3.1, nous suivons [Mon03] p.128 et [Duv98] p.73. Voir aussi théorème 369 de [HW60] p.302. Nous aurons besoin du lemme suivant.

3.2 Lemme. — *Soit p premier impair. Alors il existe $(x, y) \in \mathbb{Z}^2$ tel que $1 + x^2 + y^2 \equiv 0\,[p]$.*

Preuve. — 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 $f(0), f(1), \ldots f\left(\dfrac{p-1}{2}\right)$.
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 $(a, b) \in (\mathbb{Z}/p\mathbb{Z})^2$ tel que $a^2 = -b^2 - 1$. ∎

Passons à la démonstration du théorème.

Preuve. — Elle est basée sur l'identité

$$\begin{aligned}(x^2+y^2+z^2+t^2)(x'^2+y'^2+z'^2+t'^2) \\ &= (xx'+yy'+zz'+tt')^2 + (xy'-yx'+tz'-zt')^2 \\ &+ (xz'-zx'+yt'-ty')^2 + (xt'-tx'+zy'-yz')^2 \qquad (1)\end{aligned}$$

liée à la théorie des quaternions, mais qui peut se vérifier directement.
Comme tout entier naturel peut se décomposer en un produit de facteurs premiers, il suffit de montrer, d'après l'identité (1), 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 $1 + x^2 + y^2 \equiv 0\,[p]$ et on peut les choisir avec $|x| < \dfrac{p}{2}$ et $|y| < \dfrac{p}{2}$ car p est impair, ainsi $0 < 1 + x^2 + y^2 < p^2$, et il existe k tel que $1 + x^2 + y^2 = kp$, avec $0 < k < p$. 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 $m > 1$. Soit x, y, z, t les éléments congrus modulo m à a, b, c, d respectivement avec $|x| < \frac{m}{2}$, $|y| < \frac{m}{2}$, $|z| < \frac{m}{2}$ et $|t| < \frac{m}{2}$. Posons

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

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 $1 < m \leqslant p - 1$ (par hypothèse) et p premier.
Du choix de x, y, z et t, on déduit que $n < 4 \times \left(\frac{m}{2}\right)^2 = m$, donc $0 < n < m^2$. Ajouté au fait que $n \equiv 0\,[m]$, on en déduit que $n = um$, avec $0 < u < m$. Puisque

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

on a, en faisant le produit grâce à l'identité (1),

$$m^2 up = A^2 + B^2 + C^2 + D^2$$

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,

$$m^2 up = A^2 + B^2 + C^2 + D^2 = m^2\alpha^2 + m^2\beta^2 + m^2\gamma^2 + m^2\delta^2$$

ce qui donne, après simplification par m^2,

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

avec, rappelons-le, $0 < u < m$. Ceci contredit donc le caractère minimal de m et par conséquent $m = 1$. Le théorème 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.

[HW60] Hardy, G.H. et Wright E.M., *An introduction to the theory of numbers*. Oxford University Press, 1960.

[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.