Le carré de tout nombre premier différent de 2 et de 5 est somme de 3 carrés non nuls[1]

J.P. Brevan
78150 Le Chesnay

Nota : Pour toute la suite, lorsqu'il est question de carrés, on autorise les carrés nuls, comme il est habituel en ce domaine, sauf précision contraire.

L'auteur du problème avait bien entendu une solution élémentaire, *sauf pour le cas délicat ou p est du type 8k + 5*, où il faisait appel à un théorème de JACOBI (1828) sur le nombre de représentations sous forme de quatre carrés, qui appartient plutôt à la théorie transcendante des nombres. C'est donc surtout pour ce cas que l'on cherchait des solutions élémentaires. F. BERTRAND de Toulouse en a effectivement trouvé une, mais elle est assez longue, comme on pouvait le craindre. E. DELPLANCHE de Créteil fournit une solution qui utilise de bout en bout la représentation par des *formes quadratiques particulières*, citées par LEGENDRE dans sa *Théorie des Nombres* (1798) ; cependant, la démonstration de ces formules fait appel à un difficile *Théorème de LEGENDRE* : "Tout entier non négatif qui n'est pas de la forme

[1] Réponse à l'avis de recherche n° 47 paru dans le *Bulletin* n° 403, page 203 et envoyé par par J.P. Brevan. Ce texte est la synthèse des solutions reçues et a été rédigé par J.P. BREVAN.

$4^a(8\ell + 7)$ est représentable en somme de trois carrés",et on vérifie avec frayeur que dans sa démonstration, LEGENDRE fait appel au *théorème de la progression arithmétique :* "Toute progression arithmétique $ak + b$, où a et b sont premiers entre eux, contient une infinité de nombres premiers", lequel théorème n'a été démontrté qu'en 1837 par LEJEUNE-DIRICHLET, et fait incontestablement partie de la théorie transcendante des nombres.

Si p n'est pas de la forme $8n + 5$, on peut proposer les démonstrations élémentaires suivantes :

1 - Cas où p est de la forme $4k + 3$

On va même prouver plus :

Si $t > 1$ est de la forme $4k + 3$ (t n'est pas nécessairement premier), t^2 est la somme de 3 carrés non nuls.

*Démonstration :*Par le théorème de LAGRANGE (1770), t est la somme de 4 carrés : $t = m^2 + n^2 + p^2 + q^2 \qquad m, n, p, q \geqslant 0.$

En raisonnant modulo 4, on voit que parmi les quatre nombres m, n, p, q, il y en a exactement 3 qui sont impairs. On suppose m, n, p impairs, donc non nuls et q pair. On vérifie l'identité suivante :

$$t^2 = x^2 + y^2 + z^2, \text{ avec :}$$
$$x = m^2 - n^2 - p^2 + q^2 ; y = 2(mn - pq) ; z = 2(mp + nq)$$

t étant impair, x est impair donc $\neq 0$, et z ne peut être nul. Supposons y nul, alors on a :

$$t = m^2 + n^2 + p^2 + q^2 = t + y$$
$$t = (m + n)^2 + (p - q)^2$$

mais ceci est impossible, puisque t est de la forme $4k + 3$, et ne peut être la somme de deux carrés. Donc y n'est pas nul.

On a bien : $t^2 = x^2 + y^2 + z^2$, avec : $xyz \neq 0$.■

2 - Cas où p est de la forme $8k + 1$

D'après FERMAT-EULER, tout nombre premier p de la forme $8k + 1$ est représentable souos la forme $p = x^2 + 2y^2$, et ici, $xy \neq 0$.

On en déduit les représentations :

$$p^2 = (x^2)^2 + (2y^2)^2 + (2xy)^2$$
$$= (x^2 - 2y^2) + (2xy)^2 + (2xy)^2 \quad \text{et } x^2 - 2y^2 \neq 0,$$

ce qui donne deux solutions (en général distinctes) de la proposition attribuée à FERMAT.

3 - Si p est de la forme $8k + 5$, donnons la démonstration élémentaire de F. BERTRAND. Il démontre le *théorème-clé* :

Si $2n$ est une somme de 3 ou 4 carrés non nuls, soit
$$2n = A^2 + B^2 + C^2 + D^2 \quad (A, B, C > 0, D \geqslant 0)$$
avec $AC \neq BD$ et $C^2 + D^2 \neq A^2 + B^2$, alors n^2 est la somme de 3 carrés non nuls.

Démonstration

On peut poser $2a = A^2 + B^2 - C^2 - D^2$, et $a \neq 0$. Alors :
$n^2 - a^2 = (A^2 + B^2)(C^2 + D^2) = (AD + BC)^2 + (AC - BD)^2$ (FIBONACCI).

Posons : $b = AD + BC > 0$ et $c = |AC - BD| > 0$.

On a bien : $n^2 = a^2 + b^2 + c^2 \quad a, b, c > 0$ ■

Corollaire : Tout entier n qui n'est pas somme de deux carrés est tel que n^2 est somme de 3 carrés non nuls.

Démonstration

Montrons que $2n$ n'est pas la somme de deux carrés. S'il l'était, on aurait $2n = a^2 + b^2$, où a et b sont de même parité. On a alors :
$$n = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2$$
où les nombres écrits sont entiers, ce qui est impossible car, par hypothèse, n n'est pas la somme de deux carrés. On écrit donc, par le théorème de LAGRANGE : $\quad 2n = X^2 + Y^2 + Z^2 + T^2 \quad X, Y, Z > 0, T \geqslant 0.$

Montrons que l'on peut se placer dans les conditions du théorème-clé :
si $XZ = YT$ et $XT = YZ$, on a $T = Z$ et $X = Y$,
de sorte que n serait somme de deux carrés, ce qui n'est pas. Si $XZ \neq YT$, onpose $A = X$, $B = Y$, $C = Z$, $D = T$ et si $XZ = YT$ donc $XT \neq YZ$, on pose $A = X$, $B = Y$, $C = T$, $D = Z$. Par ailleurs, on aura $C^2 + D^2 \neq A^2 + B^2$, car sinon, n serait encore somme de deux carrés, ce qui n'est pas.

Donc, par le théorème-clé, on a :
$$n^2 = a^2 + b^2 + c^2 \qquad a, b, c > 0$$ ■

Ce théorème englobe le **1** ci-dessus.

On peut alors démontrer la *proposition :*

Soit p premier de la forme $8k + 5$, et $p \neq 5$,
p^2 est la somme de 3 carrés non nuls.

Démonstration : p étant premier de la forme $4k + 1$, il est somme de deux carrés (Fermat) :
$$p = a^2 + b^2 \qquad \text{avec} \qquad a, b > 0$$
a impair, b pair, a et b premiers entre eux.

En raisonnat modulo 4 et 8, on voit que $b \equiv 2 \bmod 4$. On écrit :

$$2p = (a+b)^2 + (a-b)^2$$

soit, en posant $X = a+b$ et $Y = |a-b|$: $2p = X^2 + Y^2$ avec $X, Y > 0$
où X et Y sont impairs d'où $X^2 \equiv 1 \pmod 4$.

Supposons que X *ne soit pas somme de deux carrés.*

Par le corollaire ci-dessus, on peut écrire :

$$X^2 = \alpha^2 + \beta^2 + \gamma^2 \qquad \alpha, \beta, \gamma > 0$$

En raisonnant modulo 4, on voit que l'on peut prendre α et β pairs et γ impair, donc : $2p = \alpha^2 + \beta^2 + \gamma^2 + Y^2 \qquad \alpha, \beta, \gamma, Y > 0.$

On a $\alpha^2 + \beta^2 \equiv 0 \pmod 4$ et $\gamma^2 + Y^2 \equiv 2 \pmod 4$

de sorte que $\alpha^2 + \beta^2 \neq \gamma^2 + Y^2$.

Si $\alpha Y \neq \beta\gamma$, on a $\alpha\gamma \neq \beta Y$, on applique le théorème-clé et la proposition est démontrée.

Sinon, on a $\alpha = \beta$ et $\gamma = Y$, soit $X^2 = (a+b)^2 = 2\alpha^2 + Y^2$, soit $\alpha^2 = 2ab$, et comme a et b sont premiers entyre eux, il existe u et v positifs premiers entre eux, tels que $a = u^2$ et $b = 2v^2$, de sorte que l'on a : $p = u^4 + 4v^4$.

On redémontre au passage un résultat de Sophie GERMAIN, que le seul nombre premier de cette forme est $p = 5$. En effet,

$$p = u^4 + 4v^4 = (u^2 + 2uv + 2v^2)(u^2 - 2uv + 2v^2)$$

et comme p est premier, il faut que

$$u^2 - 2uv + 2v^2 = 1 \quad \text{d'où} \quad (u-v)^2 + v^2 = 1$$

ce qui entraîne : $u = v = 1$ d'où $p = 5$.

Mais par hypothèse, on a exclu $p = 5$, et notre conclusion est que la proposition est vraie si X n'est pas somme de deux carrés, et vu le rôle similaire joué par Y, *la proposition est vraie si* X *ou* Y *n'est pas somme de deux carrés.*

La proposition ne peut être *fausse que si Y et Y sont des sommes de deux carrés.*

Etudions ce cas. $X = a + b$ étant somme de deux carrés, comme $b \equiv 2 \pmod 4$ et $X \equiv 1 \pmod 4$, on a $a \equiv 3 \pmod 4$.

Si X ou Y est somme de deux carrés non nuls, par exemple $X = \alpha^2 + \beta^2$, on a : $X^2 = (\alpha^2 - \beta^2)^2 + (2\alpha\beta)^2$

d'où $2p = (\alpha^2 - \beta^2)^2 + (2\alpha\beta)^2 + Y^2 = A^2 + Y^2 + B^2$

avec $A = |\alpha^2 - \beta^2|$, $B = 2\alpha\beta$, $A, B, Y > 0$

donc $AB \neq 0$ et $A^2 + Y^2 \neq B^2$

car $A^2 + Y^2 \equiv 2 \pmod 4$ et $B^2 \equiv 0 \pmod 4$.

On est alors dans les coditions du théorème-clé et la proposition est démontrée.

Reste le cas où X et Y sont des carrés :

$X = u^2$ et $Y = v^2$. Il vient $2a = X \pm Y = u^2 \pm v^2$. Par raisonnement modulo 4, on voit que seul le signe + est possible : $2a = u^2 + v^2$, et par un raisonnement déjà effectué,

$$a = \left(\frac{u+v}{2}\right)^2 + \left(\frac{u-v}{2}\right)^2$$

où les nombres écrits sont entiers. a serait une somme de deux carrés, ce qui est impossible, car $a \equiv 3 \pmod 4$.

On en conclut que *X et Y ne peuvent être tous deux des sommes de deux carrés*, et la proposition est démontrée.