Revue **Quadrature**, n°142 (octobre-novembre-décembre 2026)

$(2027, 2029)$ et $(2087, 2089)$: deux couples d'entiers pépites du XXI^e siècle

Jean-Baptiste Hiriart-Urruty [1]

Chaque entier d'année a ses propres propriétés, qu'on énonce à l'envi en début d'année, même si certains de ces entiers sont plus riches en propriétés intéressantes que d'autres. L'année 2026 que nous laisserons derrière nous bientôt et l'année 2027 qui se profile à l'horizon n'échappent pas à la règle.

Avant de quitter 2026

2026 n'est évidemment pas un nombre premier mais il n'en est pas loin : il n'a que deux facteurs premiers, 2 et 1013 (car $2026 = 2 \times 1013$), on dit dans ce cas que le nombre est *semi-premier.* Une propriété des facteurs 2 et 1013 est qu'ils sont tous les deux des nombres premiers de Sophie Germain. En effet, un nombre premier p est appelé *nombre premier de S.Germain* si $2p + 1$ est aussi premier ; c'est le cas ici car $2 \times 2 + 1 = 5$ est premier et $2 \times 1013 + 1 = 2027$ est également premier. Voilà la transition toute faite vers 2027...

Avant d'aborder 2027

Nous commençons par le fait bien particulier, déjà noté au-dessus, que 2027 est *nombre premier.* Ce n'est pas tout, le nombre impair suivant, 2029, est aussi un nombre premier. Nous avons donc une première propriété saillante du couple $(2027, 2029)$, celui d'être constitué de *nombres premiers jumeaux.* Ajoutons à cela que le second nombre premier, à savoir 2029, est *la somme de deux carrés d'entiers*, propriété qui se vérifie facilement grace à un beau thèorème de Fermat.

La conjonction des deux propriétés énoncées au-dessus arrive-t-elle souvent ? Pas vraiment, par exemple $(2027, 2029)$ est *le seul cas entre* 2000 *et* 2050. Et après ? Les jeunes lecteurs de Quadrature auront peut-être l'occasion de vivre un autre exemple, c'est $(2087, 2089)$**,** *le seul cas entre* 2050 *et* 2100 (en effet, les nombres 2087 et 2089 sont *premiers jumeaux* et le deuxième, 2089, est *la somme de deux carrés d'entiers*) [2]

C'est l'occasion ici de reparler de ce "théorème des deux carrés" de Fermat et d'en proposer une démonstration détaillée.

Le thèorème des deux carrés ou le cadeau de Noël de Fermat

Théorème. *Un nombre premier p (plus grand que 3) est la somme de deux carrés d'entiers si, et seulement si, il est de la forme $4k+1$, avec k entier positif (en termes plus savants, on dit que p est congru à 1 modulo 4).*

1. Université de Toulouse (ex-Université Paul Sabatier), 118 Route de Narbonne
31062 Toulouse Cedex 09
Mél. : jbhu@math.univ-toulouse.fr. Site web professionel : www.math.univ-toulouse.fr/˜jbhu/

2. Pour être tout à fait complet, il y aussi les nombres premiers jumeaux $(2081, 2083)$ où, cette fois-ci c'est le premier des deux, 2081, qui est la somme de deux carrés.

Les deux entiers de la décomposition de p sont alors uniques, l'un est pair et l'autre impair. Le théorème s'applique ainsi à 5, 13, 17,... , 2017, 2029, etc. Ce qui est assez extraordinaire avec ce théorème est qu'il fournit une *caractérisation* des nombres premiers sommes de deux carrés d'entiers, caractérisation de surcroît facile à vérifier.

Le théorème au-dessus fut énoncé par FERMAT dans une lettre qu'il écrivit le soir de Noël 1640, c'est pourquoi il est parfois référencé comme "le cadeau de Noël de FERMAT". FERMAT écrivait beaucoup de lettres, y énonçait des conjectures (dont certaines sont restées célèbres) et lançait à ses correspondants des défis de démonstration. On retrouvera cette frénésie épistolaire bien plus tard avec TH. J. STIELTJÈS et ses échanges avec CH. HERMITE. Qu'auraient-ils fait s'ils avaient disposé du courrier électronique ? [3]

La première vraie démonstration du théorème vint plus tard, avec EULER comme souvent ; nous pouvons ainsi désigner ce théorème comme celui de FERMAT & EULER.

Il y a plusieurs démonstrations du théorème de FERMAT & EULER ; comme souvent en mathématiques, cela dépend des prérequis... La démonstration que nous présentons ci-dessous est celle que nous préférons, elle a indéniablement une saveur "combinatoire" ; l'idée en revient à D. ZAGIER ([5]), mais on doit reconnaitre que sa présentation est très condensée et qu'on n'y voit pas pourquoi une involution "diabolique" f y est introduite ainsi que la nécessité d'avoir un point fixe $(1, k, 1)$ pour elle. Nous "mâchons" donc le tout en détail ici.

Démonstration du Théorème (que nous reprenons de ([2, Tapa 218])

A. *La partie facile, ou "la condition énoncée est nécessaire"*

Vérifions qu'un nombre premier qui est la somme de deux carrés d'entiers est nécessairement de la forme $4k + 1$.

Le carré de tout entier pair $2n$ est $4n^2$, tandis que le carré de tout entier impair $2m + 1$ est $4m^2 + 4m + 1$. Par conséquent, la somme des carrés de deux entiers est de la forme $4k, 4k + 1$ ou $4k + 2$. Ainsi, si, de plus, cette somme est supposée être un nombre premier (plus grand que 3), il est nécessairement de la forme $4k + 1$.

B. *La réciproque, ou "la condition énoncée est suffisante"*

1°) Préliminaire. Soit S un ensemble fini et $f : S \to S$. Nous disons que :

- Si f est une involution [4] qui n'a qu'un seul point fixe, alors le nombre d'éléments de S est impair.

- Si le nombre d'élements de S est impair, alors toute involution f sur S possède au moins un point fixe.

Voyons pourquoi cela. Quand $f : S \to S$ est une involution, nous avons : pour tout $s \in S$,

$$f(s) = s' \ (\in S) \text{ et } f(s') = s. \tag{1}$$

3. De nos jours, avec cet outil de communication, il nous arrive d'écrire du courrier n'importe quel jour,... y compris à Noël.

4. Une application $f : S \to S$ est une *involution* sur S lorsqu'elle est bijective et que $f = f^{-1}$; c'est ce qui est exprimé dans (1) plus bas. Autre manière de dire les choses : $(f \circ f)(s) = s$ pour tout $s \in S$ (en appliquant f deux fois de suite, on retombe sur nos pieds). Un exemple typique pour $S = \{1, 2, ..., n\}$ est la permutation f dans S qui est juste la *transposition* de deux éléments différents i et j : $f(i) = j, f(j) = i$, et $f(s) = s$ pour tout s différent de i et j.

Ainsi, il n'y a que deux possibilités : des points fixes s (*i.e.,* $f(s) = s$) ou bien des échanges de deux éléments $s \neq s'$ (*i.e.,* $f(s) = s'$ et $f(s') = s$).

- D'une part. Si nous supposons que l'involution f a un seul point fixe, l'action de f sur les autres éléments de S consiste à échanger deux éléments différents ; ces derniers vont donc deux par deux. En conséquence, le nombre d'éléments de S est impair.

- D'autre part. Si le nombre d'éléments de S est impair, le nombre de points fixes pour f est $1, 3, 5, ...$ (un nombre impair) ; ainsi, f possède au moins 1 point fixe.

2°) La preuve elle-même.

Soit p un nombre premier de la forme $4k + 1$, avec k entier positif. Définissons

$$\mathcal{E}(p) = \left\{(a, b, c) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N} : 4ab + c^2 = p \ (= 4k + 1)\right\}. \tag{2}$$

(i) Etape 1. $\mathcal{E}(p)$ est un ensemble fini non vide de triplets d'entiers positifs.

D'une manière claire, $(1, k, 1) \in \mathcal{E}(p)$. Ensuite, parce que p est un nombre premier, il ne peut être factorisé (comme $p = c^2$ ou comme $p = 4ab$ (un nombre pair)) ; donc : $a > 0$, $b > 0$ et $c > 0$ dès que $(a, b, c) \in \mathcal{E}(p)$.

Comme majorants (certes un peu grossiers) pour a, b, c (lorsque $(a, b, c) \in \mathcal{E}(p)$), on obtient :

$$a \leqslant \frac{p}{4},\ b \leqslant \frac{p}{4},\ c \leqslant \sqrt{p}.$$

Evidemment, une fois que a and b ont été choisis, il ne reste qu'une possibilité pour c.

(ii) Etape 2. Soit $f : \mathbb{R}^3 \to \mathbb{R}^3$ définie comme suit :

$$f(a, b, c) = \begin{cases} (b, a - c - b, c + 2b) \text{ si } c < a - b; \\ (a, c - a + b, 2a - c) \text{ si } a - b < c < 2a; \\ (c - a + b, a, c - 2a) \text{ si } c > 2a. \end{cases} \tag{3}$$

Clairement, f est une application continue linéaire par morceaux sur $\mathbb{R}^3$; mais seule l'action de f sur l'ensemble fini $\mathcal{E}(p)$ est considérée ici.

- L'application f définie en (3) est une involution sur $\mathcal{E}(p)$.

Tout d'abord, comme cela est facile à vérifier, $f(a, b, c) = (a', b', c') \in \mathcal{E}(p)$ dès que $(a, b, c) \in \mathcal{E}(p)$ (simplement parce que $4a'b' + (c')^2 = 4ab + c^2$).

f est en fait une involution sur $\mathcal{E}(p)$; il suffit de vérifier que

$$(f \circ f)(a, b, c) = f(a', b', c') = (a, b, c)$$

dans les trois cas possibles exhibés dans la définition (3) de f. Pour prendre juste un exemple, supposons que $c < a - b$ de sorte que $f(a, b, c) = (a', b', c') = (b, a - c - b, c + 2b)$. Alors, $c' > 2a'$ et

$$f(a', b', c') = (c' - a' + b', a', c' - 2a') = (a, b, c).$$

- Le triplet $(1, k, 1)$ est le seul point fixe pour f.

Parce que $1 - k < 1 < 2$, l'image de $(1, k, 1)$ par f est $(1, k, 1)$. Il reste à vérifier que c'est le seul point fixe de f dans $\mathcal{E}(p)$. En effet, avoir $f(a, b, c) = (a', b', c') = (a, b, c)$ implique

que nous sommes dans le second cas de la "définition par parties" de f (donnée dans (3)) ; donc $c = a$. Mais, cela induit $a(4b+1) = p$; comme $p = 4k+1$ est premier, il n'y a que la possibilité $a = 1$ et $4b+1 = 4k+1$, ce qui conduit à $b = k$.

(iii) Soit $g : \mathbb{R}^3 \to \mathbb{R}^3$ l'involution très simple sur $\mathbb{R}^3$, et aussi sur $S = \mathcal{E}(p)$, définie par $g(a, b, c) = (b, a, c)$.

A présent, puisque le nombre d'éléments de S est impair, ce que nous avons vu en préliminaire de cette démonstration (voir 1°)) nous indique que l'involution g possède au moins un point fixe dans S, nécessairement de la forme (a^*, a^*, c^*) vu la définition de g. En conséquence, cela prouve bien l'existence d'entiers positifs a^* and c^*vérifiant

$$4a^*a^* + (c^*)^2 = (2a^*)^2 + (c^*)^2 = p.$$

CQFD.

Exemple. Rien de tel qu'un exemple pour voir le processus de la démonstration en action, dans le 2°) au-dessus.

Considérons le nombre premier $p = 41 = 4 \times 10 + 1$.

Ici, $\mathcal{E}(41)$ contient 11 éléments (a, b, c), que nous décrivons ci-dessous avec leurs images (a', b', c') par l'involution f definie en (3) :

$$\left\{ \begin{array}{llll} \left(\begin{array}{c} \mathbf{a}, \mathbf{b}, \mathbf{c} \\ \mathbf{a}', \mathbf{b}', \mathbf{c}' \end{array} \right) = & \left(\begin{array}{c} 2,5,1 \\ 2,4,3 \end{array} \right), & \left(\begin{array}{c} 5,2,1 \\ 2,2,5 \end{array} \right), & \left(\begin{array}{c} 1,8,3 \\ 10,1,1 \end{array} \right), \\ \left(\begin{array}{c} 8,1,3 \\ 1,4,5 \end{array} \right), & \left(\begin{array}{c} 2,4,3 \\ 2,5,1 \end{array} \right), & \left(\begin{array}{c} 10,1,1 \\ 1,8,3 \end{array} \right), & \left(\begin{array}{c} 1,10,1 \\ 1,10,1 \end{array} \right), \\ \left(\begin{array}{c} 4,2,3 \\ 4,1,5 \end{array} \right), & \left(\begin{array}{c} 1,4,5 \\ 8,1,3 \end{array} \right), & \left(\begin{array}{c} 4,1,5 \\ 4,2,3 \end{array} \right), & \left(\begin{array}{c} 2,2,5 \\ 5,2,1 \end{array} \right). \end{array} \right.$$

Le seul point fixe pour f dans $\mathcal{E}(41)$ est $(1, k, 1) = (1, 10, 1)$.

En ce qui concerne l'involution $g : (a, b, c) \mapsto (b, a, c)$, un point fixe pour elle dans $\mathcal{E}(41)$ est $(a^*, b^* = a^*, c^*) = (2, 2, 5)$; il conduit bien à la décomposition $41 = 4^2 + 5^2$.

Commentaires. - Comme nous l'avons déjà dit au début, dans la décomposition du nombre premier $p = 4k+1$ comme $m^2 + n^2$, nécessairement l'un des entiers, disons m, est pair, et l'autre, n, est impair. Cette paire (m, n) est unique. Pour les deux nombres premiers de ce type considérés dans notre note, $2029 = 2^2 + 45^2$et, soixante ans plus tard, $2089 = 8^2 + 45^2$.

- Le procédé suivi dans la démonstration (au-dessus) de l'existence d'une décomposition de p comme somme de deux carrés d'entiers n'est pas vraiment constructif, excepté pour des petits p. Il y a toutefois des algorithmes spécifiquement conçus pour trouver de telles décompositions, des logiciels dans PAR/GP par exemple.

- Ce théorème qui démontre qu'un nombre premier p de la forme $4k+1$ peut être exprimé de manière unique comme une somme de carrés d'entiers fut énoncé par FERMAT ; il a fallu attendre un siècle pour avoir une démonstration parfaite avec EULER. Il y a d'autres résultats de ce type dans la littérature de la Théorie des nombres, par exemple : les nombres

premiers de la forme $8k+3$ peuvent être décomposés en m^2+2n^2 ; un entier est la somme de 3 carrés si, et seulement si, il est de la forme $4^k(8l+7)$ avec des entiers k et l (un résultat dû à LEGENDRE) ; tout entier peut être décomposé comme une somme de 4 carrés d'entiers (un résultat dû à LAGRANGE). Que des grands noms !

Références

1. R.-L. CLERC, *Calculs mathématiques en ligne.* Site http : // sayrac.free.fr/ sur internet.

2. J.-B. HIRIART-URRUTY, *Mathematical Tapas. Vol. 2* (from Undergraduate to Graduate, L3-M1). Springer Undergraduate Mathematics Series (December 2017).

3. J.-B. HIRIART-URRUTY, *Ah ! les nombres premiers... 57 pintxos sur ces "incassables" de l'arithmétique.* Editions CEPADUES de Toulouse (novembre 2024).

4. J.-B. HIRIART-URRUTY, *Nombres premiers jumeaux, triplés, quadruplés : tout ce qu'on peut en dire.* Quadrature $136, 44-46$ (2025).

5. D. ZAGIER, *A one-sentence proof that every prime $p \equiv 1$ (mod 4) is a sum of two squares.* Amer. Math. Monthly $97, 144$ (1990).