Identité de Brahmagupta-Diophante

Groupe d'histoire de Mathématiques

2 septembre 2025

Table des matières

1 Quel type d'élèves peut tirer profit de cette identité ?

L'identité de Brahmagupta-Diophante [1] (que nous noterons BD dans la suite) peut être proposée à des élèves de Terminale experte dans le cadre de l'étude de l'arithmétique. Comme nous le verrons plus en détail dans un paragraphe suivant consacré à son origine historique, cette identité s'inscrit dans ce que l'on appelle aujourd'hui la théorie moderne des nombres. Cette perspective historique constitue à elle seule une justification pertinente pour l'introduire en classe. La démonstration visuelle que nous proposons permet de mieux capter l'intérêt des élèves moins à l'aise avec l'abstraction, en rendant ces notions théoriques plus accessibles. Sur le plan algébrique, la démonstration de cette identité ne mobilise pas d'idées particulièrement difficiles, et elle peut être revisitée à l'aide des nombres complexes. De même elle a une interprétation géométrique, avec une preuve visuelle par des aires qui n'utilise que des notions de niveau lycée. Si le temps et l'intérêt du professeur le permettent, c'est également une belle occasion d'évoquer les entiers de Gauss.

1. **Diophante d'Alexandrie (III^{e} siècle apr. J.-C.).** Mathématicien grec, auteur des *Arithmétiques*, recueil d'ouvrages où il s'intéresse aux équations polynomiales et à leurs solutions entières ou rationnelles. Son nom reste attaché aux *équations diophantiennes*, encore aujourd'hui un domaine central et actif de la théorie des nombres (par exemple, le grand théorème de Fermat appartient à ce champ). En 2013, Rashed et Houzel ont publié l'ouvrage *Les Arithmétiques de Diophante, lecture historique et mathématique*, sans doute l'étude la plus complète dans ce domaine.

Brahmagupta (598 – v. 668). Mathématicien et astronome indien, auteur du *Brāhmasphuṭasiddhānta*. Il a introduit de façon systématique le *zéro comme nombre* et a posé des règles opératoires générales pour les entiers, positifs et négatifs. Il est aussi connu pour l'*identité de Brahmagupta* (généralisation de l'identité de Diophante), qui joue un rôle important dans l'étude des formes quadratiques et de la représentation des entiers.

2 Un exemple pour les élèves de terminale

La décomposition des nombres : une pratique ancestrale

Depuis des temps immémoriaux, les mathématiciens et les savants ont manifesté un vif intérêt pour la représentation des nombres entiers sous forme de combinaisons plus simples. Cette fascination s'exprime notamment à travers deux approches principales :

— **La somme de nombres plus petits**
La décomposition d'un nombre en une addition avec des valeurs plus petites permet de le rendre plus accessible et compréhensible.
— **Le produit de facteurs**

La tendance à décomposer les grands nombres en éléments plus simples n'a rien de surprenant. Il est en effet plus intuitif et plus aisé de manipuler des quantités modestes, tant pour effectuer des calculs que pour appréhender les propriétés fondamentales des nombres. Cette approche, qui privilégie la simplicité, se révèle donc à la fois pratique et enrichissante.
L'histoire des mathématiques témoigne d'une évolution progressive des centres d'intérêt des savants. Après avoir étudié en profondeur les relations entre les longueurs dans les triangles rectangles (voir le paragraphe suivant), les mathématiciens se sont tout naturellement intéressés à un domaine voisin : la somme de deux carrés.
L'exploration de cette notion a conduit à des applications variées en géométrie, en théorie des nombres, et dans d'autres branches des mathématiques, illustrant la richesse et la fécondité de cette approche.
Pour introduire concrètement cette idée, considérons un exemple numérique.

Exemple. Outre sa factorisation classique $85 = 5 \times 17$, intéressons-nous à la possibilité d'écrire 85 comme somme de deux carrés parfaits. Quelques essais rapides permettent d'obtenir :

$$85 = 6^2 + 7^2 = 2^2 + 9^2$$

Considérons maintenant le produit $85 \times 17 = 1445$. Peut-on également exprimer 1445 comme somme de deux carrés ?
La réponse est affirmative, grâce à BD. Voici comment procéder :

1. On part du produit :
$$1445 = 17 \times 85$$
2. On utilise les décompositions suivantes :
$$17 = 1^2 + 4^2 \quad \text{et} \quad 85 = 2^2 + 9^2$$
3. On applique l'identité BD avec $a = 1, b = 4, c = 2, d = 9$:
$$(1^2 + 4^2) \times (2^2 + 9^2) = (1 \cdot 2 + 4 \cdot 9)^2 + (1 \cdot 9 - 4 \cdot 2)^2$$
4. Ce qui donne :
$$1445 = 38^2 + 1^2$$

Il est important de noter que la décomposition d'un nombre en somme de deux carrés n'est pas toujours unique. Par exemple, pour 1445, on trouve aussi $1445 = 34^2 + 17^2$.
La question de l'unicité a été étudiée en profondeur par Fermat[2], qui a apporté des éclaircissements fondamentaux. Il a notamment établi le théorème suivant :

2. **Pierre de Fermat (1607 – 1665).** Magistrat et mathématicien né à Toulouse. Il est un des fondateurs de la *théorie moderne des nombres*. On lui doit des résultats sur les nombres premiers, le petit théorème de Fermat, les nombres polygonaux, et ses fameuses conjectures, dont le *grand théorème de Fermat*, démontré seulement en 1994 par Andrew Wiles. Son intuition visionnaire a inspiré la plupart de la théorie des nombres ultérieure.

Un entier peut s'écrire de manière unique comme somme de deux carrés premiers entre eux (à l'ordre près) si et seulement si cet entier est un nombre premier congru à 1 modulo 4.

3 Éléments d'histoire

André Weil, comme l'explique dans *Number Theory, An Approach through History from Hammurapi to Legendre,* donne deux dates assez précises pour le commencement de l'histoire de la théorie moderne des nombres : la première entre 1621 et 1636 et l'autre en 1729. L'année 1621 correspond à la publication de l'*Arithmétique* en grec de Diophante par Bachet, accompagné d'une traduction latine et d'un commentaire très complet. En 1636, comme on peut le déduire de sa correspondance, Fermat avait déjà étudié cette version publiée par Bachet et avait commencé à développer plusieurs idées inspirées de l'Arithmétique de Diophante. Cependant, Weil souligne également que la théorie des nombres connaît une nouvelle renaissance (à l'image du dieu Bacchus) en 1729. En effet, dans une lettre datée du 1er décembre 1729, Goldbach interroge Euler sur l'affirmation de Fermat selon laquelle tous les nombres de la forme $2^{2^n}+1$ sont premiers. Euler exprime alors des doutes, mais c'est seulement dans une lettre du 4 juin 1730 qu'il révèle avoir entrepris la lecture des travaux de Fermat, dont il ressort profondément impressionné par certaines affirmations (comme le fait que tout entier peut être exprimé comme une somme de quatre carrés, ou de trois nombres triangulaires, etc.). Dès lors, Euler ne cessera d'explorer la théorie des nombres.
D'après Weil, tout ce qui relève de l'Antiquité (c'est-à-dire avant Fermat) se limite à « *quelques petites îles émergeant d'un vaste océan d'ignorance* », une période qu'il qualifie de protohistoire.
Les propriétés multiplicatives des entiers sont abordées dans les Éléments d'Euclide (livres VII, VIII et IX), bien que les historiens s'accordent sur l'origine plus ancienne du contenu de ces livres.
Quant à Aristote, il évoque dans les Premiers Analytiques une démonstration de l'irrationalité de racine de 2. Cependant, Weil souligne que cela ne suffit en aucun cas à attribuer cette découverte à une hypothétique école pythagoricienne. On peut aisément imaginer ce qu'il pensait de la légende selon laquelle un disciple aurait été assassiné pour avoir découvert l'irrationalité de racine de 2 ...

4 L'identité de Brahmagupta-Diophante

Ce que nous appelons maintenant *triplets pythagoriciens* étaient déjà étudiés par les Babyloniens entre 1900 et 1600 avant notre ère. Il s'agit des triplets d'entiers (a,b,c) qui représentent les côtés des triangles rectangles vérifiant $a^2+b^2=c^2$. Si on s'interesse à l'étude de triplets pythagoriciens on est conduit inévitablement à cette égalité :

$$(a^2+b^2)(c^2+d^2)=(ac\pm bd)^2+(ad\mp bc)^2 \qquad (BD)$$

désormais appelée **identité de Brahmagupta-Diophante (BD).** (Brahmagupta VII siècle).
Si nous posons $c=d=1$ dans BD on trouve $2(a^2+b^2)=(a+b)^2+(a-b)^2$, égalité déjà exposée par Euclide (Éléments, livre II 9-10).
Cette égalité est communément attribuée à Diophante, en effet Weil nous dit que cette égalité devait être familière à Diophante puisqu'on lit (Dioph. III 19) :

C'est dans la nature de 65 *qui puisse être écrit en deux façons différentes, comme somme de deux carrés, c'est-à-dire comme* $16+49$ *et* $64+1$ *; cela arrive car il est le produit de* 13 *et* 5*, chacun d'eux étant somme de deux carrés.*

Même si Diophante ne l'a pas écrite explicitement, il faisait explicitement référence à un

livre (perdu) de porismes (*théorème auxiliaires*) [3] et l'un des ce porisme devait être justement cette identité. En tout cas, Bachet, dans sa traduction latine de Diophante, l'a insérée comme l'un des ses porisme. Il semble que la première énonciation explicite de BD se trouve dans le *Liber quadratorum* (1225) di Fibonacci [4] qui ne revendique pas la découverte du résultat, mais le considérait bien connu parmi les spécialistes de l'époque. Il convient toutefois de préciser que le *Liber quadratorum* est longtemps resté ignoré, contrairement au *Liber abaci* son ouvrage plus célèbre, notamment parce qu'on y trouve la fameuse suite de Fibonacci.
L'identité BD établit que si un entier est le produit de deux nombres pouvant s'écrire comme somme de deux carrés, alors lui-même peut aussi s'exprimer sous cette forme. Par conséquent, pour déterminer quels entiers peuvent être écrits comme somme de deux carrés, il suffit d'identifier d'abord les nombres premiers vérifiant cette propriété.
Dans l'oeuvre de Brahmagupta (mathématicien et astronome indien, 598-670), on trouve une explicite mention à l'identité

$$(a^2 - Nb^2)(c^2 - Nd^2) = (ac \pm Nbd)^2 - N(ad \pm Nbc)^2 \tag{2}$$

avec N entier positif. Pour nous c'est clair que la (2) est une généralisation de BD en posant $N = -1$. Cette égalité a un rôle central dans la résolution de l'équation $x^2 - Ny^2 = \pm 1$ (ou plus en général l'équation $x^2 - Ny^2 = m$, m entier) appelée équation de Pell-Fermat. Les cas $N = 61, 67, m = \pm 1$ ont été résolus avec succès par les mathématiciens indiens. Pour illustrer la complexité du problème, voici les solutions minimales de deux équations de Pell-Fermat ($N = 61$) :

$$29718^2 - 61 \cdot 3805^2 = -1 \quad \text{et} \quad 1766319049^2 - 61 \cdot 226153980^2 = 1$$

5 Démonstrations de l'identité de Brahmagupta-Diophante

5.1 5.1 Démonstration algébrique (François Viète)

En explorant le Liber Quadratorum, on n'a pas pu établir avec certitude si Fibonacci avait donné une démonstration de l'égalité BD. Ce n'était pas tant la difficulté du latin qui pose problème, mais plutôt l'absence de références explicites et de titres, rendant la lecture particulièrement laborieuse et chronophage. Toutefois, Viète [5] a proposé une démonstration algébrique dans les *Notes Priores,* en s'appuyant sur un schéma géométrique illustrant deux triangles rectangles.
Toutefois, la démonstration reste purement algébrique, comme en témoigne l'extrait suivant :

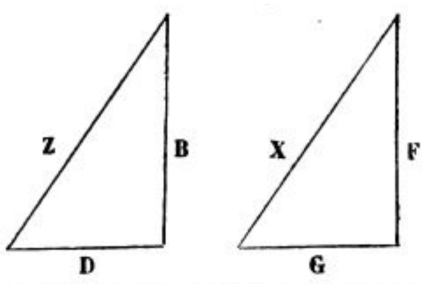
3. On trouve le terme *porisme* dans le Littré : Terme par lequel les mathématiciens des temps modernes désignent certaines propositions qui étaient en usage dans la géométrie des Grecs. Un porisme est une question dont la solution consiste à tirer une vérité géométrique de conditions assignées par l'énoncé.

4. En Italie, Fibonacci est connu sous plusieurs noms : Leonardo Bonacci, dit Fibonacci (c'est-à-dire fils de Bonacci), Leonardo Pisano ou encore Leonardo Fibonacci. Non seulement son nom varie, mais sa date de naissance reste également incertaine. Il serait né vers 1170 et décédé aux alentours de 1242.

5. **François Viète (1540 – 1603).** Mathématicien français, considéré comme le père de l'algèbre symbolique. Il a introduit l'usage systématique des lettres pour représenter aussi bien les inconnues que les coefficients, ouvrant la voie à l'algèbre moderne. Ses travaux ont profondément influencé l'arithmétique et l'algèbre de la Renaissance.

Proposition XLVI

Avec deux triangles rectangles former un troisième triangle rectangle.
Soient les deux triangles rectangles ci-dessous :



On fera l'hypoténuse du troisième triangle semblable au produit de l'hypoténuse du premier par l'hypoténuse du second, c'est-à-dire de Z par X. Donc les plans semblables à la base et à la perpendiculaire, élevés au carré, formeront le produit de Z^2 par X^2, c'est-à-dire le produit de B carré, $+D$ carré par G carré, $+F$ carré *(N.D.L.R : i.e.* $(B^2 + D^2)(G^2 + F^2)$*)*. Ce produit se compose de quatre plano-plans, c'est-à-dire, B carré par G carré, $+D$ carré par F carré, et B carré par F carré, $+D$ carré par G carré *(N.D.L.R. : i.e.* $B^2G^2 + D^2F^2 + B^2F^2 + D^2G^2$*)*.
On ajoutera à la somme de deux premiers le double plano-plan formé continuellement par B, D, F, G, et on le retranchera de la somme de deux derniers, ou bien, au contraire on retranchera ce double plano-plan de la somme de deux premiers, et on l'ajoutera la somme de deux derniers.

La démonstration de Viète s'appuie sur des figures géométriques, mais repose en réalité sur des manipulations algébriques. De nos jours, elle se résume à la ligne suivante :

$$(B^2+D^2)(G^2+F^2) = B^2G^2+D^2F^2+B^2F^2+D^2G^2-2BDFG+2BDFG = (BF-DG)^2+(DF+BG)^2$$

5.2 Point de vue géométrique

Considérons un point U de coordonnées (a, b) et un point V de coordonnées (c, d), tous deux vus comme vecteurs depuis l'origine O : $\vec{OU} = (a, b)$ et $\vec{OV} = (c, d)$. Le terme $ac + bd$ est alors le produit scalaire de ces deux vecteurs :

$$\overrightarrow{OU} \cdot \overrightarrow{OV} = |OU||OV| \cos(\theta),$$

ou θ est l'angle orienté entre les vecteurs $\overrightarrow{OU}$ et $\overrightarrow{OV}$.
De même, le terme $ad - bc$ est le déterminant du plan formé par ces deux vecteurs, et sa valeur absolue donne l'aire du parallélogramme qu'ils engendrent :

$$|ad - bc| = |OU||OV| \sin(\theta).$$

Ainsi, l'identité de Diophante–Brahmagupta s'écrit :

$$(ac + bd)^2 + (ad - bc)^2 = (a^2 + b^2)(c^2 + d^2),$$

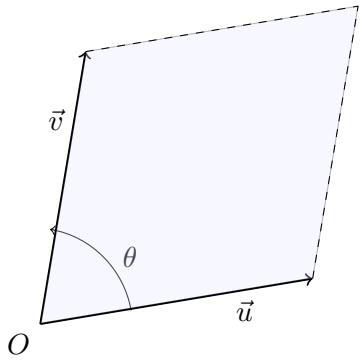
et se réinterprète géométriquement comme la somme des carrés des projections (selon $\cos$ et $\sin$) du produit $|OU||OV|$. En effet :

$$(ac + bd)^2 + (ad - bc)^2 = |OU|^2|OV|^2(\cos^2\theta + \sin^2\theta) = |OU|^2|OV|^2.$$

Cette interprétation géométrique permet de visualiser l'identité comme une décomposition du produit des longueurs au carré, analogue au théorème de Pythagore en dimension 2.
On peut également relier cette identité à la relation fondamentale en géométrie vectorielle moderne :

$$|\vec{u}|^2|\vec{v}|^2 = (\vec{u} \cdot \vec{v})^2 + (\vec{u} \wedge \vec{v})^2,$$

ou $\vec{u} \wedge \vec{v}$ désigne le produit vectoriel dans le plan (ou le déterminant de la matrice formée par $\vec{u}$ et $\vec{v}$), dont la norme correspond à l'aire du parallélogramme.



Cette figure montre les deux vecteurs $\vec{u}$ et $\vec{v}$ depuis l'origine O, ainsi que le parallélogramme dont l'aire vaut $|\vec{u} \wedge \vec{v}|$.

5.3 Interprétation via les nombres complexes

Une autre démonstration de BD repose sur les nombres complexes. En remarquant que $a^2 + b^2 = (a - ib)(a + ib)$, on fait de même pour $c^2 + d^2$ on fait le produit de ces deux égalités et on trouve en réarrangeant

$$(a^2 + b^2)(c^2 + d^2) = (a - ib)(c - id)(a + ib)(c + id) = [ac - bd - i(bc + ad)][ac - bd + i(bc + ad)]$$

ce qui donnée BD en développant le dernier produit.
Pour aller plus loin, on propose un exercice pour les élèves de math experte plus motivés.

6 Un théorème de Fermat

On s'intéresse à un problème résolu par Fermat :

Quels sont les nombres premiers ou les nombres entiers qui peuvent s'écrire comme la somme de deux carrées ?

Pour résoudre ce problème, nous suivons la démarche proposée par Gauss. Il faut faire un détour dans $\mathbb{C}$ et définir les *entiers de Gauss.* Dans la partie A nous étudions les propriétés arithmétiques de ces nombres particuliers et dans la partie B on démontre le théorème de Fermat pour les nombres premiers, en utilisant les propriétés des entiers de Gauss. Gauss a introduit ses entiers pour montrer la loi de réciprocité biquadratique.

On note $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$. Cet ensemble s'appelle l'*anneau des entiers de Gauss.* On peut donc écrire :

$$z \in \mathbb{Z}[i] \iff a, b \in \mathbb{Z} \text{ tels que } \; z = a + bi$$

PARTIE A. Définitions et premières propriétés

1. Montrer que si $z, z' \in \mathbb{Z}[i]$, alors $\overline{z}, z + z', zz' \in \mathbb{Z}[i]$.
2. On note $N : \mathbb{Z}[i] \to \mathbb{N}, z \mapsto z\overline{z}$. On appelle $N(z)$ la norme de z. Justifier que $N(\mathbb{Z}[i]) \subset \mathbb{N}$.
3. Montrer que $N(zz') = N(z)N(z')$. Cette égalité nous donne une formule fantastique !
4. On note $\mathbb{Z}[i]^*$ l'ensemble des éléments inversibles de $\mathbb{Z}[i]$ et dont l'inverse est dans $\mathbb{Z}[i]$ (attention : $\mathbb{Z}[i]^*$ n'est pas $\mathbb{Z}[i] \setminus \{0\}$). Autrement dit :

$$\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid \exists z' \in \mathbb{Z}[i], z \times z' = 1\}$$

   (a) Montrer que $\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid N(z) = 1\}$.

(b) En déduire les quatre éléments de $\mathbb{Z}[i]^*$.

5. Dans cette question nous allons montrer que dans $\mathbb{Z}[i]$ on peut définir une division euclidienne comme dans $\mathbb{Z}$ (on dit que $\mathbb{Z}[i]$ est un anneau euclidien).

   (a) Soit $s \in \mathbb{C}$ (pas nécessairement un entier de Gauss).

   Montrer qu'il existe $z \in \mathbb{Z}[i]$ tel que $|z - s| \leq \dfrac{\sqrt{2}}{2}$.

   (b) En déduire, en choisissant bien s, :

$$\forall x, y \in \mathbb{Z}[i], \exists (q, r) \in \mathbb{Z}[i] \text{ tels que } \ x = qy + r \text{ avec } 0 \leq N(r) < N(y)$$

   Remarques. Le couple (q, r) n'est pas unique. Si on définit le PGCD comme étant le dernier reste non nul d'une suite de division, c'est possible qu'il ne soit définit uniquement. Mais on peut montrer qu'on obtient quatre PGCD différents, mais ils diffèrent seulement d'une unité près.

   (c) Faire la division euclidienne de $3 + 2i$ par $1 - i$.

6. On dit que $p \in \mathbb{Z}[i]$ est **premier** si p n'est pas inversible et si pour tout $a, b \in \mathbb{Z}[i]$ et $p = ab$, alors a est inversible ou b est inversible.

   Montrer que cette définition généralise celle des nombres premiers sur $\mathbb{N}$.

   Dorénavant on écrira premier pour **premier**, en cas d'ambiguïté on explicitera premier dans $\mathbb{Z}[i]$.

7. Soit $p \in \mathbb{Z}[i]$. Montrer que si $N(p)$ est premier, alors p est premier dans $\mathbb{Z}[i]$.

   Donner un nombre **premier** de $\mathbb{Z}[i]$.

8. En considérant $3 \in \mathbb{Z}[i]$, montrer que la réciproque de la proposition précédente est fausse.

9. Soit p un premier de $\mathbb{Z}[i]$. Montrer que pour tout $a, b \in \mathbb{Z}[i]$ et $p|ab$, alors $p|a$ ou $p|b$.

10. **Théorème fondamental de l'arithmétique dans $\mathbb{Z}[i]$.**

    Tout entier de Gauss non inversible s'écrit comme un produit unique de nombres premiers de $\mathbb{Z}[i]$.

PARTIE B. Un nombre premier comme somme de deux carrées

Dans cette partie on va montrer le théorème de Fermat :

$$p \in \mathbb{N} \text{ premier et } p \neq 2 \text{ s'écrit sous la forme } \ a^2 + b^2 \ \text{ ssi } p \equiv 1 \pmod 4$$

Dans les questions 1, 2 on montrera la condition nécessaire (si p est somme de deux carrée, alors il est congru à 1 mod 4).
Dans la question 3, on va montrer le théorème de Wilson qu'on va utiliser dans la question 4 pour montrer la condition suffisante (si $p \equiv 1 \pmod 4$ alors il existe $a, b \in \mathbb{N}$ tels que $p = a^2 + b^2$).

1. Montrer que si $p = 2$ il existe un seule couple $(a, b) \in \mathbb{N}^2$ tel que $p = a^2 + b^2$.
2. Soit $p > 2$ un premier. Montrer que s'il existe $a, b \in \mathbb{N}$ tels que $p = a^2 + b^2$, alors $p \equiv 1 \mod 4$.
3. Soit q un premier.

   (a) Rappeler le petit théorème de Fermat avec les hypothèses :

$$q \text{ premier et } \mathrm{PGCD}(q, n) = 1.$$

   (b) On considère le polynôme $P(X) = X^{q-1} - 1 - (X - 1)(X - 2) \cdots (X - (q - 1))$.

   Montrer que le degré de P est strictement inférieur à $q - 1$.

   (c) Montrer que pour tout entier k avec $1 \leq k \leq q - 1$, $P(k) \equiv 0 \pmod q$.

(d) En déduire le théorème de Wilson : q premier, alors $(q-1)! \equiv -1 \pmod{q}$.
On admettra le théorème de Lagrange : *Soit P un polynôme de degré $d \geq 1$ a coefficients entiers, alors la congruence $P(X) \equiv 0 \pmod{q}$ a au plus d racines.*

4. Condition suffisante du théorème de Fermat. Soit p un premier et $p \equiv 1 \pmod{4}$.
(a) En utilisant le théorème de Wilson, montrer que

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}$$

(b) En déduire qu'il existe $x \in \mathbb{N}$ tel que $p|(x+i)(x-i)$.
(c) Par l'absurde montrer que p ne peut pas être premier dans $\mathbb{Z}[i]$.
(d) Conclure.
(e) Application : trouver $a, b \in \mathbb{N}$ tels que $a^2 + b^2 = 257$.