Quelques propriétés des carrés parfaits

François Brunault

▶ **To cite this version:**

François Brunault. Quelques propriétés des carrés parfaits. Images des Mathématiques, 2011, http://images.math.cnrs.fr/Quelques-proprietes-des-carres.html. hal-00599432

HAL Id: hal-00599432
https://hal.science/hal-00599432

Submitted on 9 Jun 2011

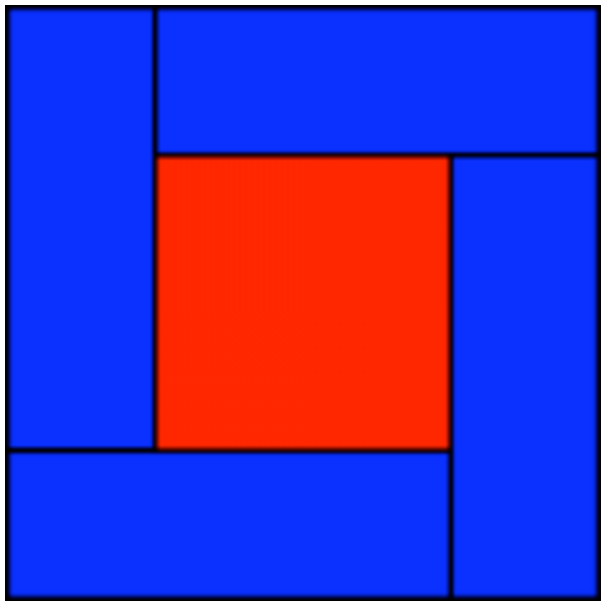
HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Quelques propriétés des carrés parfaits

Le 12 avril 2011, par **François Brunault**

Maître de conférences à l'École normale supérieure de Lyon (**page web**)



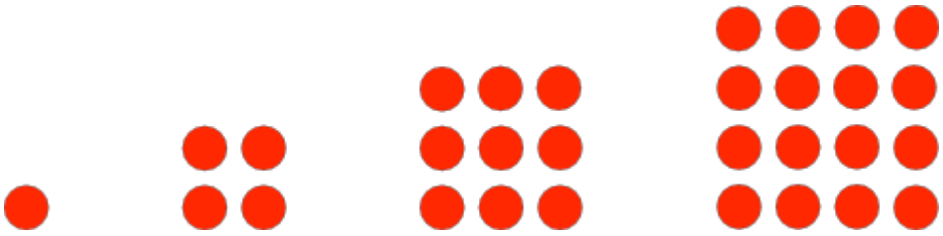
Où il est montré sur des exemples que la géométrie peut se mêler d'arithmétique, et réciproquement...

> ARITHMÉTIQUE ! algèbre ! géométrie ! trinité grandiose ! triangle lumineux ! Celui qui ne vous a pas connues est un insensé !
>
> Lautréamont, *Les Chants de Maldoror*, Chant deuxième.

Nous allons faire connaissance dans cet article avec une catégorie particulière de nombres entiers : les carrés parfaits. Ces nombres possèdent des propriétés très riches, parfois simples, parfois cachées, mais toujours savoureuses. Nous expliquerons comment la géométrie permet d'éclairer des propriétés de nature arithmétique, et réciproquement. Nous verrons également comment de simples observations numériques sur les sommes de carrés peuvent conduire naturellement à des questions intéressantes sur les nombres premiers...

Carrés parfaits

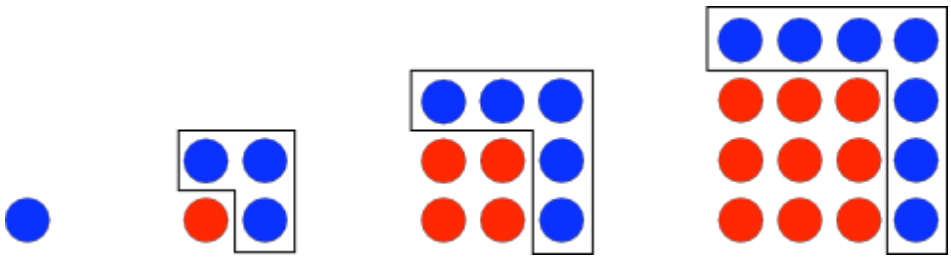
Un nombre entier N est dit *carré* s'il est possible de disposer N objets de manière à former exactement un carré, comme dans la figure suivante :



Les premiers entiers carrés sont donc 1, 4, 9, 16... On utilise parfois aussi la terminologie de *carré parfait*, qui s'explique en disant qu'il n'y a pas d'objet « manquant » ou « en trop » dans la figure carrée ainsi réalisée [1]. Algébriquement, les entiers carrés s'obtiennent en multipliant un entier

quelconque par lui-même : ainsi $1 = 1 \times 1$; $4 = 2 \times 2$; $9 = 3 \times 3$; etc.

Voici une première propriété des carrés parfaits, a priori surprenante : il est possible de calculer la suite de ces nombres en ne faisant que des additions. Pour voir cela, utilisons la définition géométrique des entiers carrés et observons comment passer d'un nombre au suivant :



Pour passer du premier carré au deuxième, on rajoute 3 objets. Pour passer du deuxième au troisième, on en rajoute 5. Du troisième au quatrième, on en rajoute 7, et ainsi de suite... On remarque que la suite des nombres à rajouter n'est autre que la suite des nombres impairs ! La table ci-dessous, appelée *table de différences*, résume la situation :

Carrés	1	4	9	16	25	36	49	64	…
Différences		3	5	7	9	11	13	15	…

Les nombres du bas s'obtiennent en calculant les différences successives des nombres du haut. Réciproquement, tout nombre dans la première ligne s'obtient en additionnant le nombre situé à sa gauche et le nombre en dessous de lui. La ligne du bas étant connue, on voit alors comment calculer, de proche en proche, la suite des carrés, en faisant uniquement des additions. Une démonstration algébrique de cette propriété est donnée ci-dessous.

Calcul algébrique des différences

Il s'agit de calculer la différence entre deux nombres carrés consécutifs. Pour tout entier n, le n-ième nombre carré vaut $n^2 = n \times n$. Par conséquent, le $(n+1)$-ième nombre carré est égal à $(n+1)^2 = n^2 + 2n + 1$. Il suit que la différence entre le n-ième carré et le $(n+1)$-ième carré est donnée par $(n^2 + 2n + 1) - n^2 = 2n + 1$. Cette différence est bien un nombre impair, et lorsque n parcourt les entiers, le nombre $2n + 1$ parcourt bien tous les nombres impairs.

Le n-ième nombre carré est donc la somme des n premiers nombres impairs. De plus, le k-ième nombre impair est égal à $2k - 1$ (on vérifie en effet que $1 = 2 \times 1 - 1$; $3 = 2 \times 2 - 1$; $5 = 2 \times 3 - 1$; etc.). On en déduit finalement la formule algébrique suivante :

$$n^2 = 1 + 3 + 5 + \cdots + (2n - 1).$$

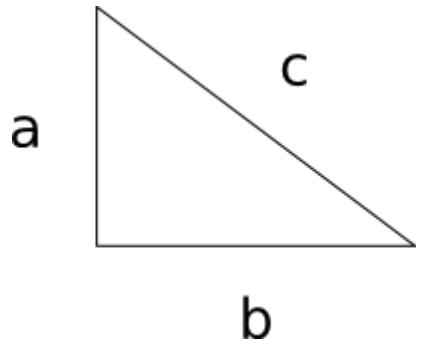
Cette méthode présente a priori un inconvénient : pour calculer *un* terme précis de la suite, il semble nécessaire de calculer *tous* les termes précédents... En réalité, on peut faire un peu mieux. Supposons par exemple que l'on sache que $11 \times 11 = 121$ et $12 \times 12 = 144$. La différence entre ces carrés vaut $144 - 121 = 23$. On en déduit alors $13 \times 13 = 144 + 25 = 169$, puis $14 \times 14 = 169 + 27 = 196$, etc. Un autre avantage de la méthode des différences est qu'elle se généralise. On peut par exemple calculer la suite des cubes par un procédé analogue [2].

De manière surprenante, le calcul de tables de différences apparaît (sous une forme beaucoup plus élaborée) dans d'autres domaines des mathématiques. Par exemple, la méthode des différences finies est un outil fondamental en analyse numérique, qui possède de nombreuses applications concrètes

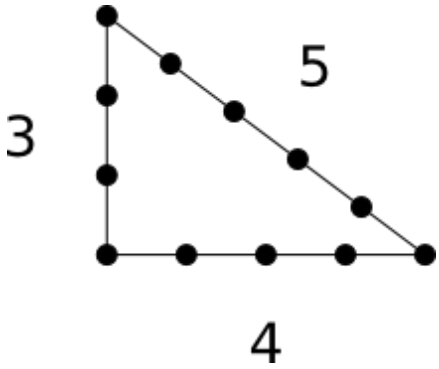
telles que la simulation d'équations issues de la physique ou de la biologie... Nous renvoyons le lecteur intéressé au cours de physique de Richard Feynman [**Fey**] pour un exemple de résolution numérique d'équations de la physique à l'aide de tables de différences. Pour un traitement mathématique des différences finies, on pourra se référer à l'ouvrage [**Cia**].

Triplets pythagoriciens

Nous allons maintenant considérer un problème de géométrie classique : est-il possible de trouver un triangle rectangle tel que toutes les longueurs de ses côtés soient des nombres entiers ? Notons a, b et c les longueurs des côtés du triangle, comme dans la figure ci-dessous :

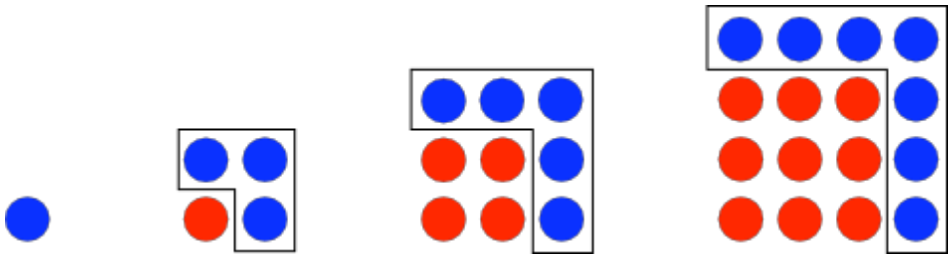


Le théorème de Pythagore nous dit que ce triangle est rectangle si et seulement si l'identité $a^2 + b^2 = c^2$ est vérifiée. Nous sommes donc ramenés à un problème purement arithmétique : trouver des entiers a, b et c tels que $a^2 + b^2 = c^2$. Un tel triplet (a,b,c) est appelé *triplet pythagoricien*. Le plus petit triplet pythagoricien est (3,4,5) : on vérifie en effet que 9 + 16 = 25. Un autre triplet pythagoricien est (5,12,13) : on a déjà vu plus haut que 25 + 144 = 169. Une application amusante des triplets pythagoriciens est que l'on peut mesurer des angles droits à l'aide d'une corde munie de nœuds espacés régulièrement, comme le montre la figure ci-dessous :



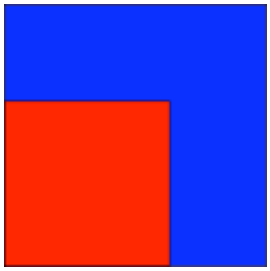
Une corde fermée à douze nœuds
permettant de mesurer un angle droit

Existe-t-il d'autres triplets pythagoriciens ? Voici une méthode, attribuée à Pythagore [**3**], pour en construire. Revenons à la définition géométrique des nombres carrés et observons de nouveau la figure utilisée précédemment :

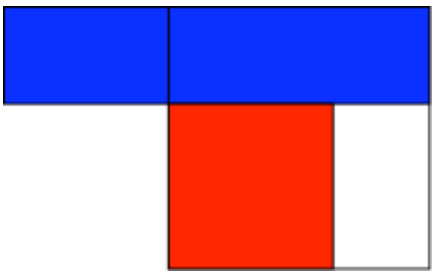


À chaque étape, le nombre de points bleus est visiblement égal à la différence entre deux carrés. D'autre part, nous avons déjà vu que le nombre de points bleus peut être rendu égal à un nombre impair arbitraire. Si l'on choisit pour ce nombre impair un carré (impair), alors on aura écrit un carré (le nombre de points bleus) comme différence de deux carrés, d'où un triplet pythagoricien ! Comme la suite des carrés impairs est infinie, ce procédé fournit en fait une infinité de triplets pythagoriciens. Les premiers triplets obtenus par cette méthode sont (3,4,5), (5,12,13), (7,24,25)...

Voici une autre construction de triplets pythagoriciens, que l'on trouve dans une œuvre monumentale, les *Éléments* d'Euclide [**4**]. Considérons deux carrés arbitraires et essayons de faire en sorte que leur différence soit un carré. Géométriquement, cela revient à considérer la figure suivante :



La région bleue est appelée *gnomon* par les Grecs. Son aire est la différence entre les aires des carrés extérieur et intérieur. Peut-on faire en sorte que l'aire du gnomon soit un carré ? Euclide montre que l'aire du gnomon est égale à l'aire d'un rectangle :

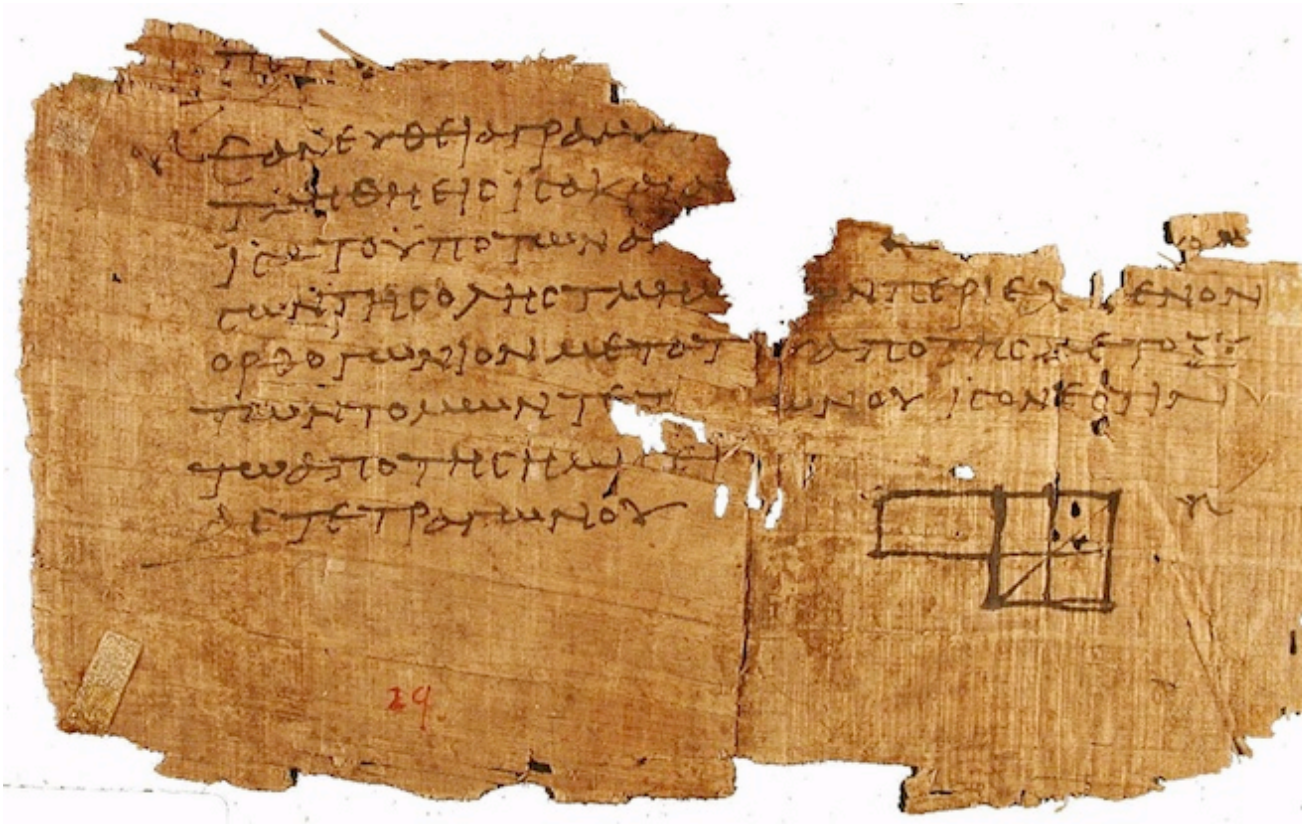


Si chacun des côtés du rectangle est un nombre carré, l'aire du rectangle sera également un carré, et on en déduira un triplet pythagoricien ! Lorsque le gnomon est de « largeur » égale à l'unité, on retrouve la construction de Pythagore. Mais la construction d'Euclide est plus générale. Par exemple, le triplet (8,15,17), découlant de la considération d'un carré de côté 8 dans un carré de côté 17, n'est pas obtenu par la méthode de Pythagore. Il se trouve en fait que presque [**5**] tous les triplets pythagoriciens peuvent être obtenus par la méthode d'Euclide [**6**].

Ceux qui le souhaitent peuvent consulter les détails de la preuve d'Euclide sur ce **très beau site** (en anglais), qui contient l'intégralité des *Éléments*. La construction des triplets pythagoriciens se trouve **ici** et la transformation du gnomon en rectangle **ici**. La démonstration d'Euclide est en tout point remarquable : c'est l'un des premiers exemples d'utilisation de la géométrie dans un problème

purement arithmétique.

Signalons aussi qu'un des plus anciens fragments manuscrits connus des *Éléments* d'Euclide, un papyrus trouvé à la fin du 19ème siècle à Oxyrhynque près du Nil [7], comporte une figure illustrant l'équivalence entre le gnomon et un rectangle :

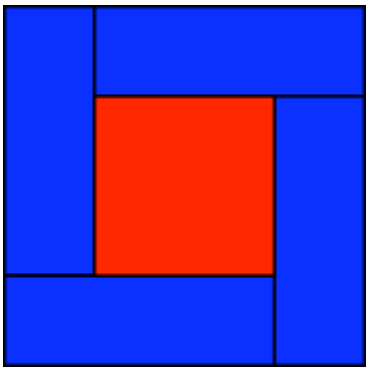


Pour terminer cette partie, je ne peux manquer de mentionner la célèbre tablette « Plimpton 322 », écrite en cunéiforme et datée environ de 1800 av. J.C. Découverte au début du 20ème siècle dans l'ancienne ville mésopotamienne de Larsa (au sud de l'Irak actuel), cette tablette présente une liste de nombres permettant de reconstituer 15 triplets pythagoriciens, le plus grand d'entre eux étant (12709,13500,18541) :

D'après les spécialistes [8], cette tablette ne constitue pas un calcul délibéré de triplets pythagoriciens, mais serait plutôt un document d'exercice à la résolution d'équations du second degré [9]. Quoi qu'il en soit (que l'auteur de « Plimpton 322 » ait eu conscience ou pas qu'il était en train de construire des triplets pythagoriciens), on ne peut qu'être ému devant ce document mathématique datant de plus de 3500 ans.

Nombres premiers et sommes de carrés

Considérons d'abord une variante de la construction d'Euclide :



Remarquons que dans cette figure, l'aire de la région bleue est encore la différence entre deux carrés. Notons L et ℓ la longueur et la largeur respectives d'un des rectangles bleus. Alors l'aire A de la

région bleue est égale à $A = 4L\ell$. Si L et ℓ sont des carrés parfaits, alors A le sera aussi. Dans ce cas, on aura construit un entier carré A qui est différence de deux carrés, d'où un triplet pythagoricien ! Encore une fois, cette construction fournit une infinité de triplets, puisqu'on peut choisir pour L et ℓ des carrés parfaits arbitraires. Une autre observation importante est que pour tout triplet pythagoricien (a,b,c) ainsi construit, l'entier c est *somme de deux carrés*. En effet c est le côté du grand carré de la figure, donc $c = L + \ell$, et par construction L et ℓ sont chacun des carrés.

Maintenant, faisons la liste de tous les triplets pythagoriciens (a,b,c) obtenus par cette méthode, avec $c \leq 100$. Classons-les par ordre croissant des valeurs de c. Pour simplifier, on ne garde que les triplets primitifs (voir la note [**5**]) et que les triplets vérifiant $a \leq b$ (on peut toujours échanger a et b pour que cette condition soit vérifiée). On obtient ainsi 16 triplets :

a	b	c
3	4	5
5	12	13
8	15	17
7	24	25
20	21	29
12	35	37
9	40	41
28	45	53
11	60	61
16	63	65
33	56	65
48	55	73
13	84	85
36	77	85
39	80	89
65	72	97

Ce tableau possède-t-il des propriétés intéressantes ? Regardons de plus près les valeurs de c. Avec un peu d'attention, on remarque que :

1. L'entier c est toujours impair. Plus précisément, son reste dans la division par 4 vaut toujours 1.
2. L'entier c est parfois premier (c'est-à-dire qu'il est divisible seulement par 1 et par lui-même).
3. Lorsque c n'est pas premier, ses diviseurs premiers ont aussi un reste de 1 dans la division par 4.
4. Certaines valeurs de c apparaissent plusieurs fois, telles $c = 65$ et $c = 85$.

Que se passe-t-il pour les triplets pythagoriciens plus grands ? Il se trouve que les propriétés 1 et 3 sont effectivement valables pour *tous* les triplets pythagoriciens primitifs. La démonstration de la propriété 1 est donnée ci-dessous. La propriété 3 est plus difficile d'accès, mais elle joue un rôle-clé dans cette histoire.

Démonstration de la première propriété

Notons $L = m^2$ et $\ell = n^2$ les longueur et largeur du rectangle bleu utilisé pour obtenir le triplet pythagoricien primitif (a,b,c). Par construction, on a $c = L + \ell = m^2 + n^2$. On a aussi $a = L - \ell = m^2 - n^2$. De plus $A = 4L\ell = 4m^2n^2 = (2mn)^2$ et donc $b = 2mn$. Si m et n sont pairs, alors a, b et c le sont aussi, c'est impossible car le triplet est supposé primitif. On vérifie de même que si m et n sont impairs alors a, b et c sont pairs, d'où encore une impossibilité. Les entiers m et n sont donc de parité différente. Supposons par exemple que m est pair et n impair. On peut écrire $m = 2u$ et $n = 2v + 1$ avec u et v entiers. On en déduit $c = m^2 + n^2 = (2u)^2 + (2v+1)^2 = 4u^2 + 4v^2 + 4v + 1 = 4(u^2 + v^2 + v) + 1$. Le reste de c dans la division par 4 est donc bien égal à 1. Le raisonnement est le même lorsque m est impair et n est pair.

Parmi les valeurs de c dans le tableau ci-dessus, on trouve en fait *tous* les nombres premiers inférieurs à 100 et ayant pour reste 1 dans la division par 4. Par ailleurs, comme nous l'avons expliqué précédemment, tous les entiers c obtenus sont sommes de deux carrés (les incrédules peuvent le vérifier à la main pour les valeurs du tableau !). Une question très naturelle surgit alors :

Tout nombre premier ayant pour reste 1 dans la division par 4 est-il somme de deux carrés parfaits ?

Cette question a joué un grand rôle dans le développement de la théorie des nombres. **Albert Girard** (1595-1632) semble être le premier mathématicien à énoncer que tout nombre premier de la forme $4k + 1$ est somme de deux carrés. Il ne donne cependant pas de preuve. Dans une lettre à **Marin Mersenne** datée du 25 décembre 1640, **Pierre de Fermat** annonce avoir démontré le résultat. Nous n'avons malheureusement pas les détails de sa preuve, ni la certitude que celle-ci était complète. Pour résoudre cette question, Fermat a inventé une nouvelle méthode. Il s'en explique dans une lettre à **Pierre de Carcavi** en août 1659 :

> Et pour ce que les méthodes ordinaires, qui sont dans les Livres, étoient insuffisantes à démontrer des propositions si difficiles, je trouvai enfin une route tout à fait singulière pour y parvenir.
>
> J'appelai cette manière de démontrer la *descente infinie* ou *indéfinie* (...).
>
> Je fus longtemps sans pouvoir appliquer ma méthode aux questions affirmatives, parce que le tour et le biais pour y venir est beaucoup plus malaisé que celui dont je me sers aux négatives. De sorte que, lorsqu'il me fallut démontrer que *tout nombre premier, qui surpasse de l'unité un multiple de 4, est composé de deux quarrés*, je me trouvai en belle peine. Mais enfin une méditation diverses fois réitérée me donna les lumières qui me manquoient, et les questions affirmatives passèrent par ma méthode, à l'aide de quelques nouveaux principes qu'il y fallut joindre par nécessité. Ce progrès de mon raisonnement en ces questions affirmatives est tel : si un nombre premier pris à discrétion, qui surpasse de l'unité un multiple de 4, n'est point composé de deux quarrés, il y aura un nombre premier de même nature, moindre que le donné, et ensuite un troisième encore moindre, etc. en descendant à l'infini jusques à ce que vous arriviez au nombre 5, qui est le moindre de tous ceux de cette nature, lequel il s'ensuivroit n'être pas composé de deux quarrés, ce qu'il est pourtant. D'où on doit inférer, par la déduction à l'impossible, que tous ceux de cette nature sont par conséquent composés de deux quarrés.

Comme on le voit, Fermat donne peu de détails... C'est le mathématicien suisse **Leonhard Euler** qui donna le premier une démonstration complète du théorème, en 1749. Sa démonstration repose effectivement sur un argument de descente. Dans le langage des triplets pythagoriciens, la preuve se

présente ainsi. Soit p un nombre premier de la forme $4k+1$.

- On commence par montrer qu'il existe un triplet pythagoricien primitif (a,b,c) tel que c est *divisible* par p.
- On montre que si (a,b,c) est un triplet pythagoricien primitif, alors non seulement c est somme de deux carrés, mais encore *tout diviseur de* c est somme de deux carrés.

Ces deux points mis ensemble entraînent que p est somme de deux carrés. C'est dans la deuxième étape qu'intervient l'argument de descente. On raisonne par l'absurde et on suppose qu'il existe un triplet pythagoricien primitif (a,b,c) tel que c possède un diviseur d qui n'est pas somme de deux carrés. On construit alors un triplet (a',b',c') avec la même propriété et qui est plus petit que le précédent, c'est-à-dire qui vérifie $c' < c$. Par le même procédé, on construit un triplet encore plus petit (a'',b'',c'') avec la même propriété. En continuant ainsi, on en déduit qu'il existe une suite infinie d'entiers naturels $c > c' > c'' > \dots$, ce qui est impossible !

Le théorème sur les sommes de deux carrés a donné lieu à de nombreuses généralisations intéressantes. **Joseph-Louis Lagrange** démontre en 1770 que tout entier est somme de quatre carrés. Fermat avait avancé que tout nombre entier est somme de trois **nombres triangulaires** [10]. Ce n'est qu'à la fin du 18ème siècle que l'assertion de Fermat sera démontrée, par **Carl Friedrich Gauss**. Le 10 juillet 1796, alors qu'il n'a pas encore vingt ans, Gauss écrit en effet avec enthousiasme dans son journal mathématique :

EURÊKA ! NUM = Δ + Δ + Δ

Il faut bien comprendre que ces résultats sont difficiles, en ce sens que la décomposition obtenue n'est pas « donnée par une formule ». Les résultats d'Euler, Lagrange et Gauss établissent l'existence d'une décomposition, mais ne disent pas comment la trouver...

Beaucoup de problèmes sur les nombres entiers restent non résolus à ce jour (les mathématiciens ne sont jamais à court de questions !). Par exemple, existe-t-il une infinité de nombres premiers de la forme n^2+1 ? Cette question fait partie des quatre **problèmes de Landau**. On pense que la réponse est oui, mais personne ne connaît de démonstration rigoureuse ! Il est cependant possible de démontrer le résultat plus faible suivant.

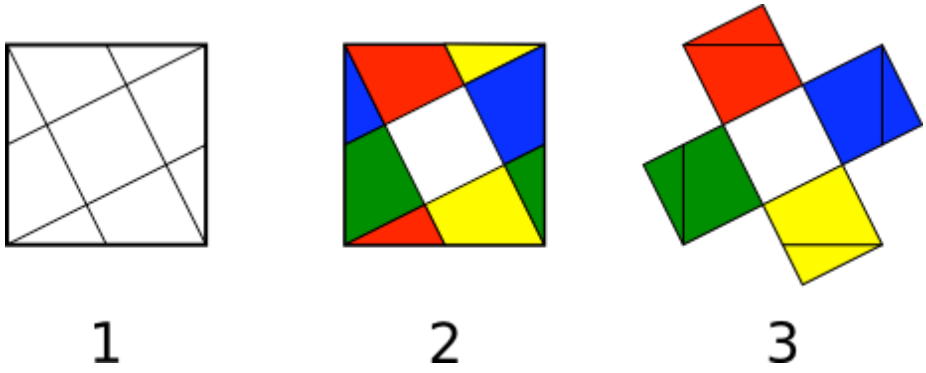
Théorème. *Pour tout nombre réel A arbitrairement grand, il existe une infinité de nombres premiers p de la forme m^2+n^2 , où les entiers m et n vérifient $\frac{m}{n} \geq A$.*

Ce résultat est un cas particulier d'un théorème démontré en 1920 par le mathématicien **Erich Hecke** en utilisant la théorie sophistiquée des fonctions L...

Un jeu géométrique

Je vous propose maintenant un petit puzzle géométrique, tiré du livre *Les jeux mathématiques* de Michel Criton [11]. Prenez une feuille de papier et tracez un carré. Pouvez-vous découper ce carré en morceaux et assembler les morceaux de manière à obtenir 5 carrés identiques, sans laisser des morceaux de côté ? Vous trouverez la solution en dépliant le bloc ci-dessous (attention, je vous conseille de bien chercher avant !).

Solution du découpage du carré en 5 carrés égaux

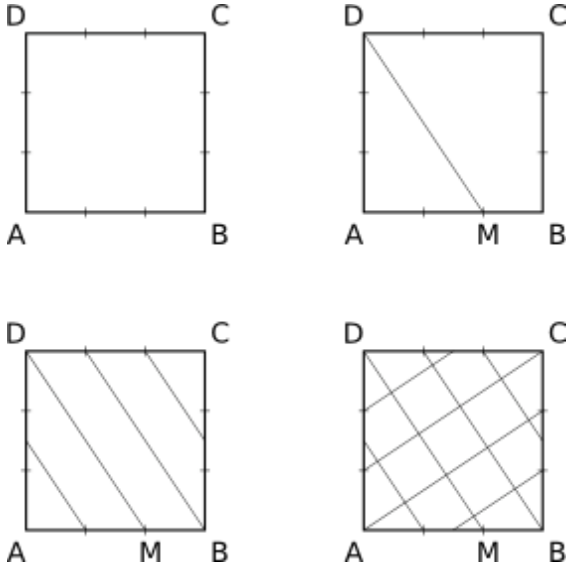


Cette solution fut trouvée par le mathématicien persan **Abul Wafa al-Buzjani** (940-998), dans son *Livre sur les constructions géométriques nécessaires à l'artisan*. Remplaçons maintenant, dans le problème précédent, le nombre 5 par un autre entier. Étant donné un entier N, est-il encore possible de découper un carré en N carrés égaux ?

Un des points-clé de la solution précédente est que le nombre 5 est *somme de deux carrés* : on a $5 = 2^2 + 1^2$. Montrons que si N est somme de deux carrés, la construction précédente se généralise. Posons $N = a^2 + b^2$, avec $a \geq b$. Partageons chaque côté du carré $ABCD$ initial en a segments égaux (pour visualiser la construction, déplier le bloc ci-dessous). Imaginons que chaque petit segment est de longueur 1. Le carré $ABCD$ est donc de côté a. On commence par marquer le point M sur le segment $[AB]$ tel que $AM = b$ et $MB = a - b$. On relie ensuite ce point M au point D. On trace alors toutes les parallèles à la droite (MD) passant par un des points de division des côtés $[AB]$ et $[CD]$. Enfin, on trace toutes les perpendiculaires à la droite (MD) passant par un des points de division des côtés $[BC]$ et $[AD]$. Il ne reste qu'à prendre ses ciseaux et assembler les morceaux comme dans le cas $N = 5$. Voilà, notre découpage est réalisé !

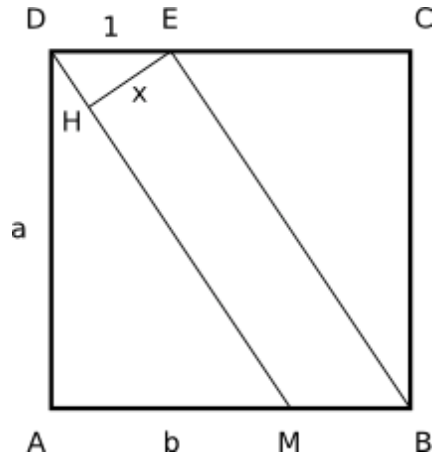
Explication en images

Dans la figure ci-dessous, on prend $N = 13$. *On a* $N = 3^2 + 2^2$ *et donc* $a = 3$ *et* $b = 2$.



Démonstration du fait que l'on obtient bien N petits carrés.

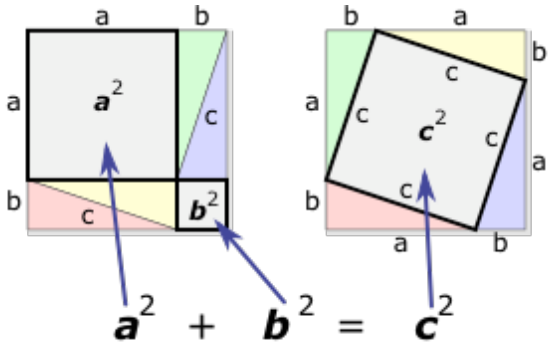
Reprenons la construction à l'étape où l'on construit les parallèles à la droite (MD) *:*



Notons x *le côté des petits carrés obtenus. C'est la largeur de la bande dans la figure ci-dessus. D'après le théorème de Pythagore dans le triangle rectangle* AMD *, on a* $MD^2 = AM^2 + AD^2 = b^2 + a^2 = N$ *. Notons* E *le point du segment* $[CD]$ *tel que* $DE = 1$ *, et* H *le point du segment* $[MD]$ *tel que le triangle* HDE *est rectangle en* H*. Les angles des triangles* AMD *et* HDE *étant égaux deux à deux, ces triangles sont semblables. On en déduit l'égalité des rapports* $\frac{AD}{MD} = \frac{HE}{DE}$ *, c'est-à-dire* $\frac{a}{MD} = \frac{x}{1}$ *ou encore* $a = MD \cdot x$ *. En élevant au carré, on obtient* $a^2 = MD^2 \cdot x^2 = N \cdot x^2$ *. Autrement dit, l'aire du grand carré est égale à* N *fois l'aire du petit carré. Il y a donc bien* N *petits carrés.*

Pour un entier N quelconque, on sait qu'un découpage du carré en N carrés égaux existe. C'est une conséquence du théorème de Bolyai-Gerwien-Wallace, qui affirme qu'étant donnés deux polygones de même aire, il est toujours possible de passer de l'un à l'autre par découpage et réassemblage [12]. Cependant, le découpage fourni par ce théorème est en général compliqué. Dans le cas $N = 3$ (pour lequel la méthode précédente ne s'applique pas puisque 3 n'est pas somme de deux carrés), Abul Wafa a également donné une solution [13]. Je ne connais pas de solution simple dans le cas $N = 7$. Quel est le nombre minimal de pièces nécessaires pour un tel découpage ?

On peut s'amuser à inventer et résoudre de nombreux autres problèmes de découpages géométriques. Certains théorèmes célèbres peuvent d'ailleurs se démontrer à l'aide de découpages astucieux. Par exemple, voici une preuve du théorème de Pythagore (source : **Wikimédia**) :



On pourra consulter avec profit l'article de Daniel Perrin mentionné en note [12] pour de nombreux autres exemples de découpages.

Sur quoi travaillent les théoriciens des nombres aujourd'hui ?

Notre compréhension des nombres entiers est encore bien modeste. Pour essayer de vous en convaincre, voici un exemple de question non encore résolue sur les nombres premiers. Nous avons vu plus haut quels nombres premiers sont sommes de deux carrés. Changeons maintenant légèrement la question : quels nombres premiers sont-ils sommes de deux cubes ? [14] On pourrait croire que ce problème ressemble au précédent, mais il est beaucoup plus compliqué ! Nous avions auparavant affaire à l'équation $x^2 + y^2 = p$, qui est l'équation d'un cercle et dont les solutions sont bien comprises. Maintenant, il s'agit de résoudre l'équation $x^3 + y^3 = p$, qui est l'équation d'une courbe elliptique.

Les **courbes elliptiques** sont des objets qui se situent au carrefour de la géométrie et de l'arithmétique, et dont la beauté fascine les mathématiciens. Déterminer si l'équation d'une courbe elliptique admet ou pas une infinité de solutions est l'objet d'une conjecture célèbre, formulée dans les années 1960 par les mathématiciens britanniques **Bryan Birch** et **Sir Peter Swinnerton-Dyer**. On dispose de résultats partiels sur cette conjecture, mais tous les spécialistes s'accordent à dire que des idées nouvelles sont nécessaires pour résoudre le cas général. En ce qui concerne l'équation $x^3 + y^3 = p$, on peut montrer que lorsque $p = 3$ ou lorsque p est impair et de la forme $9k + 2$ ou $9k + 5$, l'équation n'a pas de solutions, et donc p n'est pas somme de deux cubes. **Noam Elkies** a également montré que lorsque p est de la forme $9k + 4$ ou $9k + 7$, l'équation a une infinité de solutions, et donc p est somme de deux cubes d'une infinité de manières différentes. Les deux cas restants, à savoir $p = 9k + 1$ et $p = 9k + 8$, ne sont toujours pas complètement résolus [15].

Une avancée formidable dans la compréhension des courbes elliptiques a été réalisée dans les années 1990 par **Andrew Wiles**, qui a montré que *toute courbe elliptique est modulaire*. Essayons d'expliquer en quelques mots ce dont il s'agit. Pour chaque nombre premier ℓ, on peut considérer les solutions « modulo ℓ » de l'équation de la courbe elliptique [16]. On obtient un nombre fini de solutions, que l'on note $N(\ell)$. Lorsque ℓ varie, les nombres $N(\ell)$ n'ont a priori pas de lien entre eux. Le théorème étonnant démontré par Wiles est qu'il est possible d'encoder tous ces nombres $N(\ell)$ dans une fonction qui possède un nombre incroyable de symétries. La *modularité* de la courbe elliptique se réfère ici non pas à l'**arithmétique modulaire**, mais à ces symétries cachées, et la fonction encodant les nombres $N(\ell)$ est une *forme modulaire*. Un domaine de recherche très actif actuellement consiste à étendre le théorème de modularité de Wiles à des objets plus généraux que les courbes elliptiques.

Conclusion

Nous n'avons pu donner ici qu'un très bref aperçu de quelques propriétés des carrés parfaits ; d'ailleurs, la plupart des propriétés de ces nombres restent à découvrir ! Nous avons vu sur des exemples comment des considérations géométriques simples peuvent aider à résoudre certaines questions purement arithmétiques. Il y a là un phénomène général en mathématiques : il est souvent nécessaire d'aborder un problème en multipliant les approches et les points de vue. Beaucoup d'idées nouvelles et fécondes naissent au croisement de domaines différents des mathématiques. Les liens unissant l'arithmétique et la géométrie sont à cet égard particulièrement fructueux.

P.S. :

La rédaction d'Images des maths, ainsi que l'auteur, remercient pour leur relecture attentive, les relecteurs dont le pseudonyme est le suivant : Jacques Lafontaine, Sylvia, Laurent Bétermin et Sylvain Barré. L'auteur remercie également Étienne Ghys pour ses encouragements et ses conseils lors de la

rédaction de cet article.

Notes

[▲1] Il semble que la terminologie de carré parfait puisse également s'expliquer par l'étymologie. Au 18ème siècle, un rectangle était en effet aussi appelé « quarré long » (voir l'***Encyclopédie*** de Diderot et d'Alembert à l'article « rectangle »). Ainsi la **Maison Carrée** de Nîmes est de forme... rectangulaire. Voir également le dictionnaire de l'Académie française (4ème édition, 1764) à l'article **Carré**.

[▲2] Il est alors nécessaire d'introduire une ligne de plus dans le tableau, c'est-à-dire de calculer des différences de différences... Nous laissons au lecteur intéressé le soin de construire ce tableau.

[▲Fey] R. Feynman, *Cours de physique, Mécanique tome 1*, Dunod, 1999, chapitre 9, § 9.6 et 9.7.

[▲Cia] P. Ciarlet, *Introduction à l'analyse numérique matricielle et à l'optimisation*, Dunod, 1998, chapitre 3.

[▲3] D'après Proclus, dans ses *Commentaires sur le premier livre des Éléments d'Euclide*.

[▲4] Voir l'article sur **Euclide** écrit par **Fabio Acerbi**.

[▲5] De manière précise, on obtient au moins tous les triplets pythagoriciens (a,b,c) tels que a, b et c n'ont pas de diviseur commun autre que 1. De tels triplets sont dits *primitifs*. On montre que tout triplet pythagoricien s'écrit de manière unique sous la forme (ka,kb,kc) où (a,b,c) est un triplet pythagoricien primitif et k est un entier supérieur ou égal à 1.

[▲6] On ignore cependant si Euclide le savait.

[▲7] Datant de 75 à 125 après J.C., selon le papyrologue Eric Turner.

[▲8] Voir à ce sujet l'article d'Eleanor Robson, *Words and Pictures : New Light on Plimpton 322*, American Mathematical Monthly, vol. 109, no 2, 2002, p. 105–120.

[▲9] Plus précisément, il concernerait des équations du type $x - \frac{1}{x} = c$.

[▲10] Les amateurs de vieux films trouveront leur bonheur sur **cette page** de la revue *Mathématiques et sciences humaines*, déjà mentionnée dans **ce billet** d'**Étienne Ghys**. On y trouve en accès libre plusieurs films à destination du grand public, dont un expliquant les nombres carrés et un autre les nombres triangulaires.

[▲11] M. Criton, *Les jeux mathématiques*, Que sais-je ? n°3220, deuxième édition corrigée, 1998, p. 79.

[▲12] Voir **cet article** de **Michèle Audin** et **cet article** de **Daniel Perrin** sur le site.

[▲13] Voir l'article **Aires et volumes : découpage et recollement (I)**, figure 18a.

[▲14] Pour que la question soit intéressante, on s'intéresse ici aux cubes de nombres *rationnels*, et on autorise les nombres négatifs. Un nombre rationnel est un nombre (positif ou négatif) de la forme $\frac{a}{b}$ avec a,b entiers relatifs et $b \neq 0$.

[▲15] Plus précisément, en supposant vraie (une partie de) la conjecture de Birch et Swinnerton-Dyer, on sait montrer que tout nombre premier p de la forme $9k+8$ est somme de deux cubes. Dans le cas $p = 9k+1$, qui est le plus difficile, **Fernando Rodriguez-Villegas** et **Don Zagier** ont donné un critère (dépendant lui aussi de la conjecture de Birch et Swinnerton-Dyer) pour que p soit somme de deux cubes.

[▲16] On se place dans le système fini des nombres **« modulo ℓ »** (appelé aussi « arithmétique de l'horloge »), où deux nombres entiers sont identifiés lorsque leur différence est un multiple de ℓ. Les « solutions modulo ℓ » sont alors les nombres x et y appartenant à ce système fini et qui vérifient l'équation de la courbe elliptique.

Pour citer cet article : **François Brunault**, **« Quelques propriétés des carrés parfaits »** — *Images des Mathématiques*, CNRS, 2011. En ligne, URL : **http://images.math.cnrs.fr/Quelques-proprietes-des-carres.html**