Les triplets pythagoriciens

Document établi à partir de https://www2.mat.ulaval.ca/fileadmin/Cours/MAT-3900/Tripletspythagoriciens.pdf

Étudier les solutions entières de l'équation diophantienne $x^2+y^2=z^2$ revient à chercher tous les triangles rectangles dont les longueurs des côtés sont des entiers, la variable z correspondant à l'hypoténuse. En l'honneur du mathématicien grec Pythagore (6ème siècle av. J.-C.),

Définition 1. *On appelle triplet pythagoricien un triplet d'entiers positifs* (u,v,w) *tels que* $x=u$, $y=v$ *et* $z=w$ *constituent une solution de cette équation.*

Le triplet pythagoricien le plus célèbre est sans doute $(3,4,5)$; le triplet $(5,12,13)$ est aussi bien connu. Il est clair qu'il existe une infinité de triplets pythagoriciens ; en effet, si (u,v,w) est une solution de l'equation $x^2+y^2=z^2$, alors il en est de même de $(k\times u, k\times v, k\times w)$ pour tout entier positif k, car $(k\times u)^2+(k\times v)^2=k^2\times u^2+k^2\times v^2=k^2\times(u^2+v^2)=k^2\times w^2=(k\times w)^2$.

Exemple 2. Partant de $(3,4,5)$, on trouve que $(9,12,15)$, $(12,16,20)$ et $(15,20,25)$ sont aussi des triplets pythagoriciens. (5,12,13) donne (10,24,26).

Il existe diverses méthodes permettant d'engendrer des triplets pythagoriciens ; la plus simple, connue de l'ecole pythagoricienne, est sans doute de considérer les triplets de la forme $u=m$,$v=\frac{m^2-1}{2}$, $w=\frac{m^2+1}{2}$, $(*)$ où m est un nombre impair. Elle peut être vue comme découlant de l'identité $n^2+(2n+1)=(n+1)^2$, dans laquelle on a posé $m^2=2n+1$ (donc avec m impair) — voir Buntet al., The Historical Roots of Elementary Mathematics, pp. 77–78. Posant $m=2\times k+1$ dans $(*)$, on obtient que pour tout entier positif k, le triplet $(2\times k+1, 2\times k^2+2\times k, 2\times k^2+2\times k+1)$, $(**)$ est solution de l'equation $x^2+y^2=z^2$.

Exemple 3. Pour $k=1,2,3,4$ et 5, cette dernière formule donne les triplets pythagoriciens $(3,4,5)$, $(5,12,13)$,$(7,24,25)$, $(9,40,41)$ et $(11,60,61)$.

De $(*)$, on tire aussi que $(2m, m^2-1, m^2+1)$, $(***)$ est un triplet de Pythagore, formule connue de Platon.

La question que nous voulons examiner s'il est possible de donner une règle permettant de trouver tous les triplets pythagoriciens. Remarquons que tout triplet pythagoricien ne relève pas forcément de l'une des techniques qui précèdent. Par exemple on a bien $20^2+21^2=29^2$; mais cette solution de l'équation de Pythagore n'est ni de la forme (ku,kv,kw), ni d'aucune des formes $(*)$, $(**)$ ou $(***)$.

Définition 4. *Un triplet pythagoricien* (u,v,w) *est dit primitif lorsque* $\text{pgcd}(u,v,w)=1$.

En d'autres termes, un tel triplet n'est pas un multiple d'un autre triplet pythagoricien.

Exemple 5. $(3,4,5)$, $(5,12,13)$, $(8,15,17)$, $(20,21,29)$ et $(15,112,113)$ sont des triplets pythagoriciens primitifs.

Remarque 6. Gardons en mémoire les remarques suivantes.

- Tout triplet pythagoricien primitif (u,v,w) engendre une infinité de triplets non primitifs (ku,kv,kw) où $k=2,3,\ldots$.

- Réciproquement, tout triplet pythagoricien correspond à un unique triplet primitif obtenu en divisant u, v et w par leur pgcd. Il suffit donc de concentrer notre étude sur les triplets pythagoriciens primitifs.

- Soit donc un triplet pythagoricien primitif (u, v, w).

  i. Il va de soi que u et v ne peuvent être tous deux pairs.

  ii. Mais ils ne peuvent non plus être tous deux impairs, car on aurait alors $u^2 \equiv v^2 \equiv 1 \pmod 4$, et donc $w^2 \equiv 1+1 \equiv 2 \pmod 4$, ce qui est impossible — en effet, le carré d'un entier a est forcément congru, modulo 4, soit à 0 soit à 1, selon que a est pair ou impair. Il faut donc que l'un de ces deux paramètres, disons v, soit pair et l'autre, u, impair.

  iii. Il s'ensuit que w^2 est impair (car il est la somme de deux carrés dont l'un est pair et l'autre impair), et donc w aussi.

  iv. Le fait que $\text{pgcd}(u, u, v) = 1$ entraîne que u, v et w sont deux à deux premiers entre eux. Sinon, l'égalité $w^2 = u^2 + v^2$ et l'existence d'un diviseur commun différent de 1 à deux des nombres entrainerait la divibilité du troisième.

Nous montrons maintenant que les triplets pythagoriciens primitifs sont d'une forme bien particulière.

Proposition 7. *Tout triplet pythagoricien primitif* (u, v, w) *est de la forme* $\begin{cases} u = r^2 - s^2, \\ v = 2\,r\,s, \\ w = r^2 + s^2, \end{cases}$ *, où* r *et* s *sont des entiers arbitraires de parités opposées et tels que* $\text{pgcd}(r, s) = 1$ *(avec* $r > s > 0$*).*

Remarque 8. Il est facile de vérifier que tout triplet d'entiers (u, v, w) satisfaisant ces trois équations est bel et bien un triplet pythagoricien ; en effet $u^2 + v^2 = (r^2 - s^2)^2 + (2\,r\,s)^2 = r^4 - 2\,r^2s^2 + s^4 + 4\,r^2s^2 = r^4 + 2\,r^2s^2 + s^4 = (r^2 + s^2)^2 = w^2$. Ce résultat était d'ailleurs essentiellement connu d'Euclide qui, dans le Livre X de ses éléments, donne une méthode de ce type pour trouver deux carrés dont la somme est aussi un carré — voir le Lemme 1 de la Proposition X.29. Notons qu'Euclide ne s'intéressait cependant pas à la notion de triplet pythagoricien primitif.

Nous voulons maintenant démontrer :

a) que les conditions sur r et s assurent qu'un tel triplet est primitif ;

b) que les triplets pythagoriciens primitifs sont tous de cette forme.

Démonstration.

a) Pour établir que le triplet est primitif, considérons un premier p tel que $p|u$ et $p|v$. Comme u et v sont de parité différente, $p \neq 2$. De la relation $u^2 + v^2 = w^2$ découle que $p|w$, de sorte qu'on a à la fois $p|u$ et $p|w$, et donc $p|(u + w)$ et $p|(w - u)$. Mais comme $u + w = 2r^2$ et $w - u = 2s^2$, on a $p|2r^2$ et $p|2s^2$. Et puisque p est impair, il faut donc que $p|r^2$ et $p|s^2$, d'où il suit que $p|r$ et $p|s$. Or, par hypothèse, r et s sont relativement premiers, de sorte qu'un tel premier p ne peut exister.

b) Soit donc (u, v, w) un triplet pythagoricien primitif. Comme v est pair, on a $v = 2t$, de sorte que l'égalité $u^2 + v^2 = w^2$ peut se réécrire $4t^2 = w^2 - u^2 = (w + u)(w - u)$.

Mais u et w étant impairs, $w + u$ et $w - u$ sont tous les deux pairs.

On a donc $t^2 = \frac{w+u}{2} \times \frac{w-u}{2}$, (†) où les facteurs à la droite de (†) sont non seulement des entiers, mais sont de plus premiers entre eux.

En effet, tout facteur qui leur est commun doit aussi diviser leur somme, qui est w, ainsi que leur différence, qui est u;

Mais comme nous avons un triplet primitif, le pgcd de u et w est 1.

Soit maintenant p, un premier divisant le membre de gauche de (†), $p|t \times t \Rightarrow p|t$, donc $t = k \times p$ et $t^2 = k^2 \times p^2$, l'exposant dont il est affecté dans la factorisation première de t^2 étant pair, il doit en être de même du côté droit de (†). Mais aucun premier ne pouvant diviser simultanément les deux facteurs à la droite (puisque ces deux nombres u et w sont premiers), p doit donc se retrouver dans un seul de ces facteurs et y être affecté d'un exposant pair. Autrement dit, la décomposition de t en facteur premier se retrouve dans l'un des facteurs du membre de droite avec un exposant pair. Ainsi chacun des deux facteurs à la droite de (†) est un carré parfait, disons $\frac{w+u}{2} = r^2$ et $\frac{w-u}{2} = s^2$, (*) où on peut supposer que r et s sont positifs.

En additionnant ces deux équations, on trouve $w = r^2 + s^2$, et en soustrayant, $u = r^2 - s^2$.

Puisque $u > 0$, il s'ensuit que $r > s$.

Comme w est impair, r et s ne peuvent être de la même parité.

On a vu plus haut que r^2 et s^2 sont relativement premiers, ce qui entraîne qu'il en est de même pour r et s.

Notons enfin que d'après (†) et (*), $t^2 = r^2 s^2$, de sorte que puisque $v = 2\,t$, on a $v = 2\,r\,s$. □

Il est clair, d'après le résultat précédent, qu'il existe une infinité de triplets pythagoriciens primitifs : on n'a qu'à balayer les valeurs possibles de r et de s.