# Les triplets pythagoriciens

Victor ISSA

Janvier 2020

On dit qu'un triplet d'entiers naturels $(a, b, c)$ est un triplet pythagoricien lorsqu'il existe un triangle rectangle dans le plan euclidien dont la longueur de l'hypoténuse est $c$ et celles des ses deux autres côtés sont de longueur $a$ et $b$. Par le théorème de Pythagore les triplets pythagoricien sont exactement les triplets d'entiers positifs vérifiant :

$$a^2 + b^2 = c^2$$

Dans cet exposé on décrira l'ensemble $\mathcal{P}$ de ces triplets en l'identifiant à l'ensemble des points rationnels d'un arc du cercle unité (voir 1.0.3). On étudiera les propriétés géométriques de $\mathcal{P}$ via l'action de $GL_2(\mathbb{Z})$ sur celui-ci. Nous étudierons la distribution des triplets pythagoricien primtifs en donnant une formule asymptotique pour le nombre de triplet d'hypoténuse $\leq n$ ainsi que pour les triplets primitifs vérifiant $|a|, |b| \leq n$. Finalement nous placerons dans le cas plus général de l'équation $x^2 + y^2 = n$ et donnerons une condition nécessaire et suffisante sur $n$ pour que cette équation admette des solutions

## 1 Généralités sur les triplets

**Définition 1.0.1.** *On dit qu'un triplet pythagoricien d'entiers $(a, b, c)$ est primitf lorsque les entiers $a$, $b$ et $c$ sont premiers entre eux.*

**Définition 1.0.2.** *Soit $\mathcal{C}$ une courbe, on dit qu'une point $P$ de $\mathcal{C}$ est rationnel lorsque ses coordonnées sont rationelles.*

**Proposition 1.0.3.** *L'application $(a, b, c) \mapsto (\frac{a}{c}, \frac{b}{c})$ définie une bijection entre l'ensemble des triplets pythagoricien primitifs et l'ensemble des points rationnels à coordonnées positives du cercle.*

La proposition ci-dessus réduit donc le problème de la détermination de $\mathcal{P}$ à celle de l'étude des points rationnels du cercle. Pour étudier ces points on va se donner "une paramétrisation rationnelle" du cercle c'est à dire une fonction continue surjective $f : \mathbb{R} \to \mathbb{S}^1$ tel que $f(t)$ est un point rationnel si et seulement si $t \in \mathbb{Q}$.

**Proposition 1.0.4.** *L'application $f : t \mapsto (\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1})$ est une paramétrisation rationelle du cercle unité.*

*Preuve.* $f$ est continue et si $(x, y) \in \mathbb{S}^1$ alors il existe $\theta$ tel que $x = \cos\theta$ et $y = \sin\theta$ on pose alors $t = \tan\frac{\theta}{2}$ et on a $(x, y) = f(t)$ donc $f$ est surjective. Si $t \in \mathbb{Q}$ alors $f(t)$ est un point rationel et si $f(t) = (x, y)$ est rationel comme $t = \frac{x}{1-y}$ on en déduit que $t \in \mathbb{Q}$, d'où le résultat. □

On en déduit que les points rationnels du cercle sont les points de la forme $(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1})$ avec $t \in \mathbb{Q}$ en écrivant $t = \frac{p}{q}$ avec $p$ et $q$ premiers entre eux on en déduit que les points rationnels sont les points $(\frac{2pq}{p^2+q^2}, \frac{p^2-q^2}{p^2+q^2})$

**Théorème 1.0.5.** *Les triplets pythagoriciens primitifs sont les triplets $(2pq, p^2 - q^2, p^2 + q^2)$ avec $0 < q < p$ , $p \wedge q = 1$ et $p + q$ impair, à interversion de $2pq$ et $p^2 - q^2$ prêt.*

*Preuve.* Il s'agit de déterminer à quelles conditions le triplet pythagoricien $(a, b, c) = (2pq, p^2 - q^2, p^2 + q^2)$ est primitif lorsque $q < p$ sont premiers entre eux, puisque si ce n'est pas le cas le triplet n'est bien sûr pas primitif.

1er cas : $p + q$ impair

Montrons que dans ce cas le triplet est primitif, soit $d$ le pgcd de $(a,b,c)$ alors $d$ divise $p^2+q^2$ et $p^2-q^2$ qui sont des entiers impairs donc $d$ est impairs, de plus $d$ divise $(p^2+q^2)+(p^2-q^2)=2p^2$ donc $d$ divise $p^2$, de même $d$ divise $q^2$ et donc $d=1$ car $p^2$ et $q^2$ sont premiers entre eux.

2nd cas : $p+q$ pair

Dans ce cas $p^2+q^2$ et $p^2-q^2$ sont pairs et donc 2 est un facteur commun aux trois composantes du triplet, qui n'est alors pas primitif. □

De la même façon on peut s'intéresser à l'équation $x_1^2+....+x_n^2=y^2$ dont la résolution se ramène comme précédemment à la recherche des points rationnels sur $\mathbb{S}^{n-1}$. Une paramétrisation rationelle de $\mathbb{S}^{n-1}$ est donnée par :

$$f(a_1,...,a_{n-1})=\left(\frac{2a_1}{N(a)^2+1},...,\frac{2a_{n-1}}{N(a)^2+1},\frac{N(a)^2-1}{N(a)^2+1}\right)$$

où $N$ est la norme euclidienne, chaque point de $\mathbb{Q}^{n-1}$ est envoyé sur un point rationnel et si $f(a)=(y_1,....,y_n)$ est rationnel alors $a_i=\frac{y_i}{1-y_n}$, notons que $f$ n'atteint pas le pôle nord $(0,...,0,1)$.

# 2 Point de vue algébrique

## 2.1 Un peu de théorie algébrique des nombres

Rappelons que l'anneau des entiers de Gauss $R=\mathbb{Z}[i]$ est factoriel, dans $R$ l'équation de pythagore s'écrit $(a+bi)(a-bi)=c^2$ ce qui implique que $a+bi$ est un carré dans $R$ en particulier il existe des entiers $p,q$ tel que $a+ib=(p+iq)^2$ on a alors $a=p^2-q^2$ et $b=2pq$ et l'équation $((p+iq)(p-iq))^2=c^2$ impose $|c|=(p+iq)(p-iq)$ et donc $|c|=p^2+q^2$ comme $c$ est positif on en déduit $c=p^2+q^2$. On retrouve ainsi la description des triplets de la section 1
De même des expressions de la forme $x^p+y^p=z^p$ avec $p$ premier peuvent se factoriser dans $R_p=\mathbb{Z}[\zeta_p]$ où $\zeta_p$ est une racine $p$-ième de l'unité et s'écrivent alors :

$$\prod(x+\zeta_p^k y)=z^p$$

En revanche comme $R_p$ n'est pas factoriel pour $p>19$, la méthode précédente ne s'applique plus en générale. Toutefois Kummer a trouvé un moyen de faire fonctionner l'argument ci-dessus, à condition que $p$ ne divise pas le nombre de classe d'idéaux de $R_p$, et ainsi prouve le théorème de Fermat pour ces nombres premiers. A la fin des années 90 Andrew Wiles, par des méthode complètement différentes, donne une preuve ud théorème suivant, aujourd'hui connu sous le nom de théorème de Fermat-Wiles :

**Théorème 2.1.1** (Fermat-Wiles)**.** *Soit $n\geq 3$ $x,y,z\in\mathbb{Z}^3$, si $x^n+y^n=z^n$ alors $xyz=0$.*

Notons que pour prouver le théorème de Fermat, il suffit de le prouver pour $n=4$ et $n$ premier impair car si un des diviseurs de $n$ vérifie les théorème, $n$ vérifie le théorème et tout nombre $\geq 3$ est divisible par 4 ou un nombre premier impair.

## 2.2 Une heuristique pour les solutions entières d'équations polynomiale à coefficients entiers

Soit $P$ un polynôme homogène de degrés $n$ en $d$ variable à coefficients entiers on s'intéresse aux solutions entières de l'équation :

$$P(x_1,...,x_d)=0$$

Comme $P$ est homogène on peut écrire, $P(X_1,...,X_d)=\sum_{k_1+...+k_d=n}a_{k_1,...,k_d}X_1^{k_1}...X_d^{k_d}$ en particulier si $|x_i|\leq N$, alors $|P(x_1,...,x_n)|\leq cN^n$ ainsi $P$ induit une application :

$$P:[-N,N]^d\to[-cN^n,cN^n]$$

donc sous réserve que les valeurs de $P$ soient "uniformément distribuées" $\#P^{-1}(0)\simeq 2^{d-1}cN^{d-n}$ ainsi si $d>n$ l'équation admet beaucoup de solutions entières et si $d\leq n$ l'équation admet peu de solutions entières, dans le cas

de l'équation de pythagore on a $P = X^2 + Y^2 - Z^2$ donc $n = 2$ et $d = 3$ dans le cas de l'équation de Fermat on a $n \geq 3$.
En pratique, les valeurs de $P$ ne sont pas vraiment "uniformément distribuées", par exemple si :

$$P = X_1^2 + .... + X_d^2$$

avec $d \geq 3$ l'heuristique prédit une infinité de solutions alors que l'équation n'admet qu'une solution, c'est parce que ici $P$ est à valeurs positives donc ses valeurs ne se distribuent pas uniformément dans $[-cN^n, cN^n]$

# 3 Transformation de l'ensemble des triplets

Si $(a, b, c)$ est un triplet pythagoricien on peut lui associer une matrice $X = \begin{pmatrix} -b & c-a \\ c+a & -b \end{pmatrix}$ symétrique à coeffcients entiers de déterminant nul, de plus on vérfie qu'une telle matrice vérifie $X^2 = 0$. On s'intéresse donc à la strucutre de l'ensemble des matrices nilpotentes de $M_2(\mathbb{Z})$ :

**Proposition 3.0.1.** *Toute matrice nilpotente $2 \times 2$ à coefficients entiers est semblable, via une matrice de $GL_2(\mathbb{Z})$, à une matrice de la forme $\lambda E$ avec $\lambda \in \mathbb{N}$ et où :*

$$E = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}$$

*Preuve.* Soit $X$ une telle matrice comme le déterminant de $X$ est nul et que $X^2 = 0$ par le théorème de Caley-Hamilton $X$ est de trace nulle, ainsi $X$ est de la forme :

$$X = \begin{pmatrix} x & y \\ z & -x \end{pmatrix}$$

avec $x^2 + yz = 0$. Si l'un des coefficients de $X$ est nul alors c'est la matrice nulle, ou un multiple de $E$ ou $E^T$ comme $E$, $E^T$, $-E$ sont toute semblalbes il s'ensuit que $X$ est bien semblable à un $\lambda E$ avec $\lambda \geq 0$.

Dans le cas contraire, les lignes de $X$ sont liées sur $\mathbb{Q}$ il existe donc des entiers premiers entre eux $m$ et $n$ tel que $mx = nz$ et $my = -nx$ on va montrer que $x = mn$, $y = -n^2$ et $z = m^2$. Comme $m$ et $n$ sont premiers entre eux on a $n$ divise $x$, $m$ divise $z$, $m$ divise $x$ et $n$ divise $y$. On peut donc écrire $x = mnx_1$, $y = ny_1$ et $z = mz_1$, avec $mx_1 = z_1$ et $-nx_1 = y_1$ ainsi $m$ divise $z_1$ et $n$ divise $y_1$. finalement $x = mn\lambda$, $y = -n^2\lambda$, $z = m^2$ ainsi on a :

$$X = \lambda \begin{pmatrix} mn & -n^2 \\ m^2 & -mn \end{pmatrix} = \lambda \begin{pmatrix} n \\ m \end{pmatrix} \begin{pmatrix} m & -n \end{pmatrix}$$

Enfin il existe $u, v$ telle que $un + vm = 1$ on pose alors :

$$T \begin{pmatrix} u & -v \\ -m & n \end{pmatrix}$$

et on a $T \begin{pmatrix} n \\ m \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ainsi que $\begin{pmatrix} m & -n \end{pmatrix} = \begin{pmatrix} 0 & -1 \end{pmatrix} T$ ce qui assure que $TXT^{-1} = \lambda E$

□

De la preuve de la propposition précédente il résulte que toute matrice semblable à $E$ est de la forme :

$$\begin{pmatrix} mn & -n^2 \\ m^2 & -mn \end{pmatrix}$$

et qu'on peut lui associer un triplet pythagoricien $(2mn, m^2 - n^2, m^2 + n^2)$ et réciproquement. On a donc un moyen d'engendrer tous les triplets pythagoricien et on connait un moyen de transformer les solutions de l'équation de pythagore : Si $X$ est la matrice d'une solution de l'équation alors pour toute matrice $T$ de $GL_2(\mathbb{Z})$, $TXT^{-1}$ est encore solution de plus l'action de $GL_2(\mathbb{Z})$ est transitive.

Nous allons maintenant montrer que le groupe $GL_2(\mathbb{Z})$ peut-être remplacé par un groupe moins compliqué tout en engendrant toujours les triplets primitifs. Comme le déterminant d'une matrice n'affecte pas la conjugaisons

$((\lambda P)A(\lambda P)^{-1} = PAP^{-1})$ on peut restreindre l'action à $SL_2(\mathbb{Z})$, pour les mêmes raisons on peut identifier les matrices $A$ et $-A$ dans le groupe qui agit on est donc ramener à une action de $\Gamma = PSL_2(\mathbb{Z})$. Enfin nous allons montrer que l'on peut se restreindre à l'action du groupe unimodulaire $\Gamma(2)$ qui le noyau du morphisme naturel :

$$\Gamma \to PSL_2(\mathbb{Z}/2)$$

On considère le triplet primitf $(2mn, n^2 - m^2, m^2 + m^2)$, d'aprés le théorème de la section 1, il existe $u, v$ tel que $un + vm = 1$ $n$ est impair et $m$ est pair, si on considère $X$ la matrice associée à ce triplet, on a $X = TET^{-1}$ avec $T = \begin{pmatrix} u & v \\ -m & n \end{pmatrix}$ tel que si jamais $v$ est impair alors nécessairement $u$ est impair et on peut remplacer $T$ par $T' = TV = \begin{pmatrix} u & u+v \\ -m & n-m \end{pmatrix}$ où $V = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, qui est bien une matrice du groupe unimodulaire et comme $V$ stabilise $E$ on a $X = T'ET'^{-1}$.
L'avantage de s'être ramené au groupe $\Gamma(2)$ est double : l'action du groupe unimodulaire sur $\mathbb{Z}^2$ préseve les vecteurs dont les coordonnées n'ont pas de facteur commun et ne change pas la parité des coordonnées, ainsi l'action envoie un triplet primitif sur un autre triplet primitf, de plus $\Gamma(2)$ est le groupe libre sur 2 générateurs $U = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et sa transposée on peut donc voir l'ensemble des triplets primitifs comme un arbre enraciné

**Théorème 3.0.2.** $\Gamma(2)$ *est le groupe libre sur* 2 *éléments.*

*Preuve.* c.f. exposé de William □

# 4 Distribution des triplets

**Théorème 4.0.1.** *On note $P(n)$ le nombre de triplet pythagoricien primitif $(a, b, c) \in \mathbb{Z}^3$ tel que $|c| \leq n$ alors on a :*

$$P(n) = \frac{2\pi}{\zeta(2)} n + O(\sqrt{n})$$

*Esquisse de preuve.* En utilisant les théorèmes précédents on a :

$$P(n) = 4 \times \#\{(p, q) \in \mathbb{Z}^2, p \geq 0, p \wedge q = 1, p^2 + q^2 \leq n\}$$

De plus on a $\#\{(p, q) \in \mathbb{Z}^2, p \geq 0, p^2 + q^2 \leq n\} = \frac{\pi}{2}(\sqrt{n})^2 + O(\sqrt{n})$, en effet le cardinal à calculer n'est autre que le nombre de carré de côté 1 du réseau $\mathbb{Z}^2$ inclus dans le demi-disque de rayon $\sqrt{n}$ d'air $\frac{\pi}{2}(\sqrt{n})^2$, l'erreur commis est le nombre de carré de côté 1 qui intersectent le demi-cercle de rayon $\sqrt{n}$ qui a un périmètre proportionnel à $\sqrt{n}$.
De plus la "probabilité" que deux nombres tirés uniformément et indépendamment dans $\mathbb{Z}$ soient premiers entre eux est $\frac{1}{\zeta(2)}$, en effet la "probabilité" qu'un nombre premier divise deux nombres tirés uniformément est $\frac{1}{p^2}$, donc si on suppose ces évènements indépendant la probabilité à calculer est

$$\prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)}$$

On a donc

$$P(n) = 4\frac{\pi}{2}\frac{1}{\zeta(2)} n + O(\sqrt{n}) = \frac{2\pi}{\zeta(2)} n + O(\sqrt{n})$$

□

**Théorème 4.0.2.** *On note $P'(n)$ le nombre de triplet pythagoricien primitif $(a, b, c) \in \mathbb{Z}^3$ tel que $|a| \leq n$ et $|b| \leq n$ alors on a :*

$$P'(n) = \frac{16}{\pi^2} \log(1 + \sqrt{2}) n + O(\sqrt{n})$$

*Preuve.* Voir [3] □

# 5 L'équation $x^2 + y^2 = n$

Dans cette section on cherche une condition nécessaire et suffisante sur $n$ pour que l'équation $x^2+y^2 = n$ admette des solutions en nombre entiers, autrement dit on détermine l'ensemble des entiers représentés par la forme quadratique $q(x, y) = x^2 + y^2$. On a la relation suivante :

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

Donc l'ensemble des entiers somme de 2 carrés est stable par multiplication.

**Lemme 5.0.1.** *Soit $S$ un ensemble fini et $\sigma$ une involution de $S$ admettant $n$ points fixes alors $n$ et $\#S$ ont même parité.*

*Preuve.* On considère la relation d'équivalence $x \sim y \iff x = y$ ou $x = \sigma(y)$ les classe d'équivalences de cette relation sont les $\{x, \sigma(x)\}$ en particulier il existe un entier $k$ tel que :

$$S = n + 2k$$

car si $x$ n'est pas point fixe de $\sigma$ sa classe d'équivalence est de cardinal 2, ce qui conclut

□

**Théorème 5.0.2** (Cas $n$ premier)**.** *Soit $p$ un nombre premier impair , $p$ est somme de deux carrés si et seulement si $p = 1mod4$*

*Preuve.* Si $p$ est somme de deux carrés on vérifie que $p = 1mod4$. Si $p = 1mod4$ on considère $S = \#\{(x, y, z) \in \mathbb{N}^3, p = x^2 + 4yz\}$ on veut montrer qu'il existe un triplet dans $S$ avec $y = z$ c'est à dire un point fixe de l'involution $f : (x, y, z) \mapsto (x, z, y)$. On considère alors l'application $\sigma : S \to S$ définie par :

$$\sigma(x, y, z) = \begin{cases} (x + 2z, z, y - x - z) \text{ si } x < y - z \\ (2y - x, y, x - y + z) \text{ si } y - z < x < 2y \\ (x - 2y, x - y + z, y) \text{ si } 2y < x \end{cases}$$

On vérife que $\sigma$ est une involtion de $S$ et que cette involution admet un unique point fixe $(1, 1, k)$ où $p = 4k + 1$ ainsi par le lemme $\#S$ est impair et $f$ admet un point fixe ce qui conclut.

□

**Théorème 5.0.3.** *Un entier est somme de deux carrés si et seulement si ses facteurs premiers congrus à 3 modulo 4 interviennent par une puissance paire dans la décomposition de $n$ en facteurs premiers.*

*Preuve.* Commme l'ensemble des entiers somme de deux carrés est stable par multiplication cette condtion est nécessaire, montrons qu'elle est suffisante.

**Lemme 5.0.4.** *Soit $p$ un nombre premier congrus à 3 modulo 4 alors si $p$ divise $x^2 + y^2$ alors $p$ divise $x$ ou $y$.*

*preuve du lemme.* Si $m$ est impair $a^m + b^m = a^m - (-b)^m = (a + b) \sum_{k=0}^{m-1} a^k(-b)^{m-1-k}$ donc $x + y$ divise $x^m + y^m$ par hypothèse $\frac{p-1}{2}$ est impair donc si $p$ divise $x^2 + y^2$ $p$ divise $x^{p-1} + y^{p-1}$ or si $p$ ne divisait ni $x$ ni $y$ par le théorème de Fermat on aurait $x^{p-1} + y^{p-1} = 2modp$ ce qui conclut. □

On suppose alors que $n = x^2 + y^2$ soit $p$ un diviseur premier de $n$ congrus à 3 mod 4, par le lemme $p$ divise $x$ ou $y$ par exemple $p$ divise $x$ alors $p$ divise $n - x^2 = y^2$ ainsi $p$ divise $x$ et $y$ et $p^2$ divise $x^2$ et $y^2$. Si $v_p(n) \geq 2$ est impair, alors on a $\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$, ainsi en itérant le procédé on obtient des entiers $m, x', y'$ tel que $m = x'^2 + y'^2$ et $v_p(m) = 1$ mais alors par ce qui précéde $p^2$ divise $x'^2$ et $y'^2$ donc $p^2$ divise $m$, c'est absurde. □

# Références


[1] R. C. Alperin. "The Modular Tree Of Pythagoras". In: (2005).

[2] Daniel Bahrdt and Martin P. Seybold. "Rational Points on the Unit Sphere: Approximation Complexity and Practical Constructions". In: (2017).

[3] Manuel Benito and Juan L.Varona. "Pythagorean triangles with legs less than n". In: (2001).

[4] A. Hatcher. "Topology of numbers". In: ().

[5] Don Zagier. "A One-Sentence Proof That Every Prime p=1(mod 4) Is a Sum of Two Squares". In: (1990).