Triplets Pythagoriciens

Leçons 126,142

Théorème (Triplets Pythagoriciens)

Les triplets d'entiers $(x, y, z) \in \mathbb{Z}^3$ qui vérifient l'équation:

$$x^2 + y^2 = z^2 \tag{1}$$

sont exactement ceux de la forme:

$$(x, y, z) = \big(a(q^2 - p^2), 2apq, a(p^2 + q^2)\big) \tag{2}$$

avec $a \in \mathbb{Z}$ et $p, q \in \mathbb{Z}$ des entiers premiers entre eux.

Voici le plan de la démonstration:

1. En supposant $z \neq 0$ et $pgcd(x, y, z) = 1$, montrer que $x \wedge y = y \wedge z = z \wedge x = 1$
2. Montrer que x ou y est impair (le ou est exclusif)
3. En réécrivant $\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$, utiliser la paramétrisation rationnelle de $\$^1$, le lemme de Gauss et les résultats obtenus afin de dire que $(q^2 - p^2, 2pq, p^2 + q^2) = k(x, y, z)$ avec $k \in \mathbb{Z}$, $p \wedge q = 1$, $q \neq 0$
4. En utilisant le fait que y est impair et que $pq \wedge p^2 + q^2 = 1$, montrer que $k = \pm 1$ et obtenir le résultat

Démonstration. *1. Si $z = 0$, on a $x^2 + y^2 = 0$, soit $x = y = 0$, donc on peut supposer que $z \neq 0$.*

Soient alors $d = pgcd(x, y, z)$ et $(X, Y, Z) = \left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$. On a donc $X^2 + Y^2 = Z^2$ et $pgcd(X, Y, Z) = 1$. Donc on peut supposer que $pgcd(x, y, z) = 1$. Montrons que x, y et z sont premiers entre eux deux à deux.

- *Si $d = x \wedge y$, alors $d^2 | x^2 + y^2 = z^2$ donc $d | z$ soit $d = 1$ car $pgcd(x, y, z) = 1$*
- *Si $d = y \wedge z$, alors $d^2 | z^2 - y^2 = x^2$ donc $d | x$ soit $d = 1$ car $pgcd(x, y, z) = 1$.*
- *De même, $x \wedge z = 1$*

Donc x, y et z sont premiers entre eux deux à deux.

2. Montrons que soit x est pair, soit y est pair. x et y ne peuvent pas être pairs tous les deux car étant premiers entre eux. Si x et y sont tous les deux impairs, alors on a $x \equiv 1, 3[4]$ et $y \equiv 1, 3[4]$.

On a ainsi $x^2, y^2 \equiv 1[4]$, soit $z^2 = x^2 + y^2 \equiv 1[2]$. Mais on ne peut seulement avoir que $z^2 \equiv 0, 1[4]$, ce qui est absurde.

Donc soit x est pair, soit y est impair. Par symétrie des rôles joués par x et y, on peut supposer que y est pair.

3. *On a donc, puisque $x^2 + y^2 = z^2$, $\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$, i.e. $\left(\frac{x}{z}, \frac{y}{z}\right) \in \$ \cap \mathbb{Q}^2$. Or, la paramétrisation du cercle unité par des coordonnée rationnelles assure qu'il existe $t \in \mathbb{Q}$ tel que $\frac{x}{z} = \frac{1-t^2}{1+t^2}$ et $\frac{y}{z} = \frac{2t}{1+t^2}$.*

Si $t = \frac{p}{q}$ avec $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$ et $p \wedge q = 1$, alors on a:

$$\frac{x}{z} = \frac{1-t^2}{1+t^2} \text{ et } \frac{y}{z} = \frac{2t}{1+t^2} \quad \Leftrightarrow \quad \begin{cases} x(p^2+q^2) &= z(q^2-p^2)) \\ y(p^2+q^2) &= 2pqz \end{cases}$$

$$\text{On a ainsi: } \begin{cases} z \mid x(p^2+q^2) \\ x \mid z(q^2-p^2) \\ y \mid 2pqz \end{cases} \text{. Donc, comme } x \wedge y = y \wedge z = z \wedge x = 1,$$

$$\text{Le lemme de Gauss donne: } \begin{cases} z \mid p^2+q^2 \\ x \mid q^2-p^2 \\ y \mid 2pq \end{cases}$$

$$\text{Donc il existe } (k_1, k_2, k_3) \in \mathbb{Z}^3 \text{ tel que } \begin{cases} k_1 z &= p^2+q^2 \\ k_2 x &= q^2-p^2 \\ k_3 y &= 2pq \end{cases}$$

$$\text{Donc on a: } \begin{cases} \frac{x}{z} = \frac{q^2-p^2}{p^2+q^2} = \frac{k_2}{k_1}\frac{x}{z} \\ \frac{y}{z} = \frac{2pq}{p^2+q^2} = \frac{k_3}{k_1}\frac{x}{z} \end{cases}$$

Donc $\frac{k_3}{k_1} = \frac{k_2}{k_1} = 1$, i.e. $k_1 = k_2 = k_3 =: k \in \mathbb{Z}$

4. *Par ailleurs, vu que y est pair, on a $y = 2y'$ où $y' \in \mathbb{Z}$. Donc on a $2ky' = 2pq$ soit $ky' = pq$ d'où:*

$$y' \mid pq \tag{3}$$

De plus, on a $y'(p^2+q^2) = pqz$, donc $pq | y'(p^2+q^2)$. Soit d un diviseur premier commun à p et q. Si d divise p alors d ne divise pas q car $p \wedge q = 1$, donc d ne divise pas p^2+q^2. D'où $pgcd(pq, p^2+q^2) = 1$, donc, par le lemme de Gauss, on a:

$$pq \mid y' \tag{4}$$

Par (3) *et* (4), *on a* $pq = \pm y'$, *i.e.* $k = \pm 1$. *Ainsi, on a:*

$$\begin{cases} x &= q^2 - p^2 \\ y &= 2pq \\ z &= p^2 + q^2 \end{cases}$$

Le facteur a donné dans le théorème vient de la multiplication par $pgcd(x, y, z)$.

Réciproquement, on vérifie que les triplets de la forme (2) *vérifient l'équation* (1).

■

Remarques. *1. On obtient une paramétrisation du cercle unité* $\$^1$ *de cette manière:*

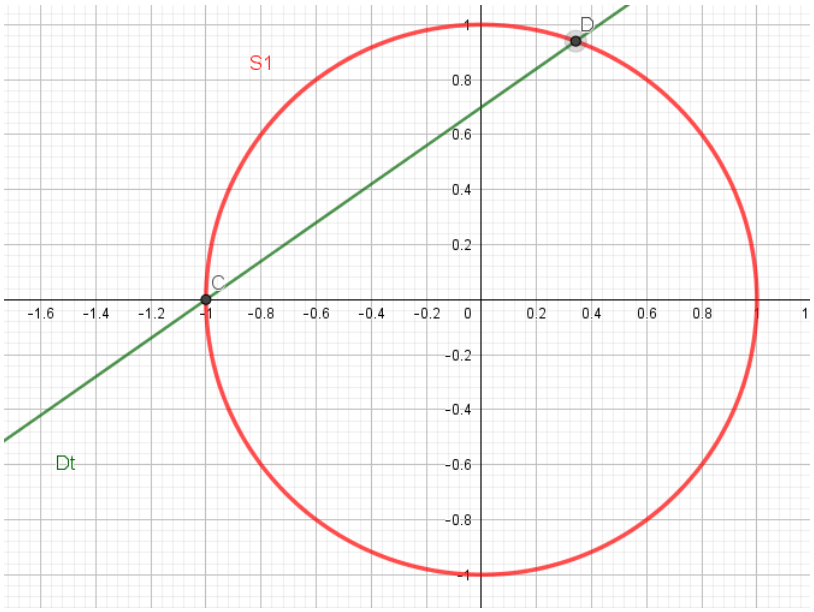

Figure 1: Illustration de la paramétrisation du cercle unité $\$^1$ (en rouge). La droite D_t (en vert) a pour coefficient directeur t.

On considère le cercle unité $\$^1$ *d'équation* $x^2 + y^2 = 1$, *et, pour* $t \in \mathbb{R}$, *la droite* D_t *d'équation* $y = t(x + 1)$, *reliant les points* $C = (-1, 0)$ *et* D. *On note* (u, v) *les coordonnées du point* D, *point d'intersection entre* $\$^1$ *et* D_t.

D'une part, on a $u^2 + v^2 = 1$, *et d'autre part, on a* $v = t(u + 1)$, *ce qui donne* $u^2 + t^2(u + 1)^2 = 1$ *après substitution. En développant, on obtient cette équation du second degré en* u: $(1 + t^2)u^2 + 2t^2u - (1 - t^2) = 0$. *L'unique solution supérieure à* -1 *pour* u *est* $u = \frac{1-t^2}{1+t^2}$. *Comme* $v = t(u + 1)$, *on obtient ainsi* $v = \frac{2t}{1+t^2}$. *Donc une paramétrisation de* $\$^1 \setminus \{C\}$ *est donnée par* $\left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right), t \in \mathbb{R} \right\}$

2. Pour $n \geqslant 3$, *l'équation* $x^n + y^n = z^n$ *n'a pas de solution, il s'agit du théorème de Fermat-Wiles. Seul les cas* $n \in \{1, 2\}$ *ont des solutions.*