Sur une équation célèbre

Pythagore, Fermat, Wiles *et al.*

De l'Antiquité à nos jours

Table des matières

1 Le cas $n = 2$ **3**
1.1 Les triplets pythagoriciens 3
1.2 La caractérisation des triplets pythagoriciens 4
1.3 Quelques exemples numériques 4

2 Le cas $n > 2$ **5**
2.1 Historique du dernier théorème de Fermat 5
2.2 Le théorème de Wiles 6

Introduction

Étant donné un entier $n \geq 2$, on s'intéresse dans ce mémoire [1] à l'équation

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

dont on cherche les solutions en nombres entiers x, y, z.

1. Ce texte a été rédigé en $\LaTeX$.

Chapitre 1

Le cas $n = 2$

Dans ce chapitre, on résout l'équation (1) dans le cas $n = 2$.

1.1 Les triplets pythagoriciens

Commençons par une définition.

Définition 1. Un *triplet pythagoricien* est un triplet d'entiers naturels (x, y, z) vérifiant $x^2 + y^2 = z^2$.

Les triplets pythagoriciens sont les longueurs des côtés d'un triangle rectangle, comme illustré sur la figure 1.1 ci-dessous.

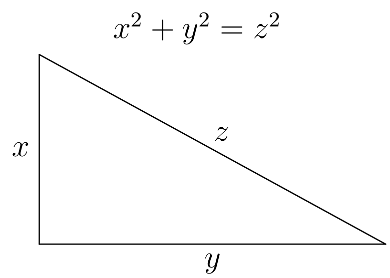

FIGURE 1.1 – Triplet pythagoricien

Remarque 1. Si d est un entier naturel et (x, y, z) un triplet pythagoricien, alors (dx, dy, dz) est encore un triplet pythagoricien.

Compte-tenu de la remarque précédente, on adopte la définition suivante.

Définition 2. Un triplet pythagoricien (x, y, z) est dit *primitif* si x, y, z sont premiers entre eux.

1.2 La caractérisation des triplets pythagoriciens

1.2.1 Un résultat préliminaire

Proposition 1. *Soit (x, y, z) un triplet pythagoricien primitif. Alors, x et y sont de parités différentes et z est impair.*

Démonstration. Laissée en exercice. □

1.2.2 La formule d'Euclide

On énonce désormais le résultat fondamental concernant l'équation (1) dans le cas $n = 2$.

Théorème 1 (Euclide)**.** *Soit (x, y, z) un triplet d'entiers naturels premiers entre eux avec x impair. Alors, (x, y, z) est un triplet pythagoricien primitif si et seulement si il existe $(p, q) \in \mathbf{N}^{*2}$ premiers entre eux et de parités différentes tels que $p > q$ et*

$$x = p^2 - q^2, \quad y = 2pq \quad \textit{et} \quad z = p^2 + q^2.$$

Démonstration. On montre seulement que la condition est suffisante. Supposons donc qu'il existe $(p, q) \in \mathbf{N}^{*2}$ premiers entre eux et de parités différentes tels que $p > q$, $x = p^2 - q^2$, $y = 2pq$ et $z = p^2 + q^2$. Alors, d'une part, x, y, z sont premiers entre eux et d'autre part, x et z sont impairs et y est pair. Enfin, on a

$$\begin{aligned}
x^2 + y^2 &= \left(p^2 - q^2\right)^2 + (2pq)^2 \\
&= p^4 - 2p^2q^2 + q^4 + 4p^2q^2 \quad \text{d'après une identité remarquable} \\
&= p^4 + 2p^2q^2 + q^4 \\
&= \left(p^2 + q^2\right)^2 \\
&= z^2.
\end{aligned}$$

D'où le résultat annoncé.

□

1.3 Quelques exemples numériques

D'après le théorème 1, il existe une infinité de triplets pythagoriciens primitifs $(x, y, z) \in \mathbf{N}^3$. On en a indiqué quelques uns dans le tableau 1.1.

x	3	5	8	7	20	12
y	4	12	15	24	21	35
z	5	13	17	25	29	37

TABLE 1.1 – Quelques triplets pythagoriciens

Chapitre 2

Le cas $n > 2$

Ce cas est **beaucoup** plus difficile ! Quelle que soit la valeur de l'entier n on a toujours des solutions pour lesquelles le produit xyz est nul [1]. Donnons-leur un nom :

Définition 3. Une solution $(x, y, z) \in \mathbf{Z}^3$ à l'équation (1) est dite *triviale* si on a $xyz = 0$.

Y a-t-il d'autres solutions que celles-ci pour $n > 2$? Fermat [2] pensait savoir montrer que non :

> Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere : cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Ainsi, le « dernier théorème de Fermat » qui affirme que les seules solutions de l'équation (1) pour $n > 2$ sont les solutions triviales est resté un problème ouvert pendant plus de 350 ans avant qu'Andrew Wiles ne le démontre au début des années 1990 (voir [3]).

2.1 Un bref aperçu historique du dernier théorème de Fermat

Voici un aperçu (fort incomplet !) de quelques approches du théorème de Fermat.

— Antiquité : résolution du cas $n = 2$ (voir le chapitre 1) ;

— $17^{\text{ième}}$ siècle : Fermat énonce son « théorème » et introduit la *méthode de descente infinie* pour résoudre le cas $n = 4$;

1. Par exemple, $(1, 0, 1)$ est solution quel que soit n.
2. Fermat : magistrat et mathématicien français du $17^{\text{ième}}$ siècle.

— Début du $19^{\text{ième}}$ siècle : Sophie Germain développe une stratégie d'attaque du théorème de Fermat et obtient plusieurs résultats importants sur « le premier cas » notamment ;
— Milieu du $19^{\text{ième}}$ siècle : Ernst Kummer développe sa théorie des « nombres idéaux » (qui mènera plus tard à la notion d'idéal d'un anneau) et démontre le théorème de Fermat pour tous les exposants premiers *réguliers* ;
— 1985 : É. Fouvry d'une part et L. M. Adleman et D. R. Heath-Brown d'autre part démontrent que le premier cas du théorème de Fermat est vrai pour une infinité d'exposants premiers ;
— Années 1980 : guidé par les travaux de Jean-Pierre Serre sur les représentations galoisiennes, Gerhard Frey « réduit » la preuve du théorème de Fermat à celles d'une conjecture de Shimura-Taniyama-Weil sur les courbes elliptiques et d'une autre appelée « conjecture ϵ », ce que Serre résume ainsi :

$$\text{Weil} + \text{epsilon} \Rightarrow \text{Fermat}.$$

— 1987 : Kenneth A. Ribet démontre la conjecture ϵ de Serre. Dans le secret, Wiles commence à travailler sur le dernier chaînon manquant, à savoir la conjecture de modularité de Shimura-Taniyama-Weil ;
— 1994 : après une première annonce prématurée en 1993, Andrew J. Wiles rend publique sa démonstration d'un cas particulier (mais très important) de la conjecture de Shimura-Taniyama-Weil. Le dernier théorème de Fermat est enfin démontré !

2.2 Le théorème de Wiles

Comme corollaire de ses travaux ([3]) sur la conjecture Shimura-Taniyama-Weil mentionnée au § précédent, Wiles obtient le fameux résultat suivant :

Théorème 2 (Wiles)**.** *Lorsque $n > 2$, l'équation $x^n + y^n = z^n$ n'admet d'autres solutions en nombres entiers x, y, z que celles dites triviales.*

Le lecteur intéressé pourra consulter les ouvrages cités en bibliographie pour plus de renseignements.

Bibliographie

[1] Paulo Ribenboim. *Fermat's last theorem for amateurs.* Springer-Verlag, New York, 1999.

[2] Simon Singh. *Fermat's enigma.* Walker and Company, New York, 1997. The epic quest to solve the world's greatest mathematical problem.

[3] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3) :443–551, 1995.