Devoir Maison n° 8

MPSI Lycée Camille Jullian

pour le 24 février 2026

Problème : démonstration (de cas particuliers) du grand théorème de Fermat.

Le but de ce problème est de démontrer le très célèbre théorème de Fermat, dont l'énoncé est rappelé ci-dessous, pour les plus petites valeurs de n (on se limitera à $n \leqslant 4$, ce qui est déjà bien). On rappelle en passant que ce théorème, énoncé par Pierre de Fermat dans une note écrite sur son exemplaire d'un classique d'arithmétique de Diophante au dix-septième siècle (la note en question n'a été publiée par le fils de Fermat que quelques années après sa mort en 1 665, on ne sait donc pas précisément à quelle date Fermat lui-même a énoncé cette conjecture), n'a été démontré complètement qu'en 1 994 par le mathématicien anglais Andrew Wiles, à l'aide de méthodes bien trop compliquées pour être évoquées dans un DM à votre niveau. Avant cela, les plus grands mathématiciens s'étaient penchés sur les cas de petites valeurs de n, puisque la démonstration présentée ici pour $n = 3$ est basée sur une première démonstration d'Euler, qui s'est avérée erronée (sacré Euler, comme d'hab, il a rien vérifié et raconté n'importe quoi), et corrigée ensuite par Gauss. Pour les plus curieux, un théorème beaucoup plus général qui permet de traiter les valeurs de n inférieures ou égales à 100, mais avec une restriction sur les inconnues x, y et z, a été démontré au début du dix-neuvième siècle par la grande mathématicienne française Sophie Germain.

Théorème 1. Théorème de Fermat-Wiles.

L'équation $x^n + y^n = z^n$ n'admet aucun triplet de solutions entières strictement positives lorsque n est un entier supérieur ou égal à 3.

Partie I : Démonstration du théorème dans le cas $n = 4$.

1. Commençons par nous intéresser au cas $n = 2$: un triplet d'entiers non nuls (x, y, z) vérifiant $x^2 + y^2 = z^2$ est appelé triplet pythagoricien, et correspond aux longueurs entières de trois côtés d'un triangle rectangle. On dit qu'un triplet pythagoricien est primitif si $x \wedge y = 1$.
   (a) Donner un exemple de triplet pythagoricien, et expliquer comment on peut facilement, à partir d'un triplet primitif, créer une infinité d'autres triplets pythagoriciens non primitifs.
   (b) Montrer que le triplet (x, y, z) est primitif si et seulement si x, y et z sont premiers entre eux deux à deux, mais aussi si et seulement si ils sont premiers entre eux dans leur ensemble.
   (c) Montrer que, si (x, y, z) est un triplet pythagoricien primitif, alors z est impair, et x et y de parité opposée (on supposera pour la suite que x est pair et y impair).

(d) Soient p et q deux entiers premiers entre eux, de parité opposée, tels que $p > q$. Montrer que $(2pq, p^2 - q^2, p^2 + q^2)$ est un triplet pythagoricien primitif.

(e) On veut montrer la réciproque du résultat précédent.

i. On suppose qu'un triplet pythagoricien primitif (x, y, z) (avec x pair et y impair) s'écrit sous la forme $(2pq, p^2 - q^2, p^2 + q^2)$, avec $p > q$ et p et q de parité opposée et premiers entre eux. Exprimer alors le quotient $\frac{p}{q}$ en fonction de x et de $z - y$.

ii. Si p et q sont définis comme numérateur et dénominateur de la fraction irréductible $\frac{x}{z-y}$, montrer qu'il existe un entier α tel que $p^2 + q^2 = \alpha z$ et $p^2 - q^2 = \alpha y$.

iii. Montrer que $\alpha = 1$, et conclure.

2. Un triangle pythagoricien est un triangle rectangle dont les côtés ont pour longueurs (x, y, z), ces trois entiers formant un triplet pythagoricien. On souhaite prouver dans cette question que l'aire d'un tel triangle n'est jamais un carré parfait. On suppose pour cela dans toute cette question que (x, y, z) est un triangle pythagoricien dont l'aire est un carré parfait.

(a) Montrer qu'on peut se restreindre à traiter le cas d'un triplet pythagoricien primitif, qu'on décrira sous la forme $(2pq, p^2 - q^2, p^2 + q^2)$ comme expliqué en question 1.

(b) Que vaut l'aire du triangle en question en fonction de x et y, puis de p et q ?

(c) Montrer alors que p, q, $p - q$ et $p + q$ sont tous des carrés parfaits, qu'on écrira donc a^2, b^2, c^2 et d^2.

(d) Montrer que $(d - c) \wedge (c + d) = 2$.

(e) En déduire, en étudiant le produit $(d - c)(c + d)$, que $\frac{c+d}{2}$ et $\frac{d-c}{4}$ sont deux carrés parfaits, **ou** $\frac{c+d}{4}$ et $\frac{d-c}{2}$ sont deux carrés parfaits.

(f) En se plaçant dans le premier cas (le deuxième se traite de façon similaire) et en posant $\frac{c+d}{2} = r^2$ et $\frac{d-c}{4} = s^2$, montrer que $(r^2, 2s^2, a)$ est un triplet pythagoricien dont le troisième entier est inférieur à celui du triplet initial.

(g) Conclure rigoureusment que l'aire d'un triangle pythagoricien n'est jamais un carré parfait.

3. On démontre (enfin) le cas $n = 4$ du théorème de Fermat. Supposons donc que $x^4 + y^4 = z^4$, avec x, y et z entiers strictement positifs.

(a) Montrer qu'on peut supposer x et y premiers entre eux, et x pair (on suppose désomais que c'est le cas).

(b) Montrer qu'on peut trouver deux entiers a et b tels que $z^2 - y^2 = 8a^4$ et $z^2 + y^2 = 2b^4$.

(c) Montrer en exploitant la question 3 que la situation précédente est impossible, et conclure.

Partie II : Démonstration du théorème dans le cas $n = 3$.

Cette deuxième démonstration est déjà nettement plus technique que celle donnée pour $n = 4$. Autrement dit, si vous avez souffert sur la partie I, abordez prudemment cette partie II...

On note dans cette partie $\mathbb{Z}[j] = \{a + jb \mid (a, b) \in \mathbb{Z}^2\}$, où j désigne comme d'habitude le nombre complexe $e^{i\frac{2\pi}{3}}$. Cet ensemble est un sous-anneau de $\mathbb{C}$ dont les éléments inversibles sont les éléments de module 1 (propriétés admises). On admet également que $\mathbb{Z}[j]$ est un anneau **factoriel**, c'est-à-dire dans lequel tout élément peut se factoriser de façon unique (à l'ordre des facteurs près et à un produit par un inversible près) comme produit de nombres premiers. Ici, un nombre premier est un nombre de la forme $a + bj$ ne pouvant pas se factoriser comme produit de deux éléments de $\mathbb{Z}[j]$ de module strictement supérieur à 1. Par exemple, le nombre 3 n'est pas premier dans ce contexte, puisqu'il peut s'écrire sous la forme $(1 + 2j)(-1 - 2j)$, avec les deux facteurs qui ont pour module $\sqrt{3}$. Toutes les autres définitions et théorèmes (notamment Bézout et Gauss) vus dans $\mathbb{Z}$ s'adaptent sans problème dans $\mathbb{Z}[j]$.

1. On suppose que (p, q, s) sont trois entiers solutions de l'équation $p^2 + 3q^2 = s^3$, avec de plus $p \wedge q = 1$.
   (a) Montrer que p et q sont premiers entre eux **dans** $\mathbb{Z}[j]$.
   (b) Montrer que $p + i\sqrt{3}q$ et $p - i\sqrt{3}q$ sont des éléments de $\mathbb{Z}[j]$, et qu'ils sont premiers entre eux (question loin d'être facile, on pourra commencer par prouver que 2 et $i\sqrt{3}$ sont des nombres premiers dans $\mathbb{Z}[j]$).
   (c) En déduire qu'il existe deux entiers a et b tels que $p + i\sqrt{3}q = (a + i\sqrt{3}b)^3$. Exprimer p et q en fonction de a et b.
   (d) Montrer que a et b sont premiers entre eux.
2. On suppose désormais que (x, y, z) est une solution de l'équation de Fermat $x^3 + y^3 = z^3$.
   (a) Montrer qu'on peut supposer x, y et z premiers entre eux deux à deux, et x et y impairs. On supposera ces propriétés vérifiées par la suite.
   (b) En posant p et q tels que $x = p + q$ et $y = p - q$ (pourquoi sont-ils entiers ?), montrer que $\frac{p}{4}(p^2 + 3q^2) = \left(\frac{z}{2}\right)^3$.
   (c) Montrer que $p^2 + 3q^2$ est impair, puis déterminer la parité de p et q (on constatera en passant que $\frac{p}{4}$ est entier).
3. On suppose dans cette question que z n'est **pas** un multiple de 3.
   (a) Montrer qu'il existe deux entiers r et s tels que $\frac{p}{4} = r^3$ et $p^2 + 3q^2 = s^3$.
   (b) Montrer qu'il existe deux entiers a et b tels que $p = a(a + 3b)(a - 3b)$ et $q = 3b(a^2 - b^2)$. Vérifier que a et b sont premiers entre eux.
   (c) Déterminer la parité des entiers a et b.
   (d) Justifier que $\frac{a}{4}$, $a + 3b$ et $a - 3b$ sont des cubes, et en déduire une nouvelle solution de l'équation de Fermat pour $n = 3$.
   (e) Montrer que le produit des trois entiers constituant cette nouvelle solution est strictement inférieur à celui des trois entiers de la solution initiale. Que peut-on en conclure ?
4. Traiter de façon similaire à la question précédente le cas où z est un multiple de 3 (on pourra commencer par montrer, en conservant les notations des questions précédentes, que p est divisible par 36).