SPÉCIALE MP* : DEVOIR SUR LE THÉORÈME DE FERMAT

On va dans ce problème étudier les cas suivants de la célèbre équation

$$(\mathrm{F}_n) \qquad x^n + y^n = z^n.$$

pour $(x, y, z) \in \mathbb{Z}^3$.

On appelle *solutions triviales* de (F_n) les solutions (x, y, z) telles que $xyz = 0$.
On sait que cette équation admet des solutions non triviales dans le cas où $n = 2$.
Le but du jeu est de prouver que pour $n > 2$, l'équation (F_n) n'admet que les solutions triviales.
On se limitera aux cas $n = 3, 4$ et on pourra avantageusement se placer dans les anneaux $\mathbb{Z}/m\mathbb{Z}$.

Partie I : généralités, étude du cas $n = 2$

I.1. Montrer soigneusement que, si a, b, c et m sont des entiers strictement positifs tels que $a \wedge b = 1$ et $ab = c^m$ alors a et b sont les puissances $m^{\text{ièmes}}$ d'entiers (on utilisera la décomposition en produit de facteurs premiers).

Généraliser au cas où $\prod_{i=1}^{n} a_i = c^m$ et où les (a_i) sont premiers deux à deux.

I.2. **a.** Montrer que, si (x, y, z) n'est pas une solution triviale, on peut prendre x, y, z premiers entre eux dans leur ensemble, on dira alors qu'on a une solution primitive.

b. Montrer que si (x, y, z) est une solution primitive alors les nombres x, y, z sont premiers deux à deux. En déduire que deux des trois nombres d'une solution primitive sont impairs, le troisième pair.

I.3. On suppose que (x, y, z) est un triplet pythagoricien primitif (c'est-à-dire vérifiant $x^2 + y^2 = z^2$ avec (x, y, z) entiers naturels non nuls premiers entre eux).

Montrer alors qu'il existe deux entiers naturels premiers entre eux et de parités distinctes $n > m > 0$ tels que :

$$x = n^2 - m^2,\ y = 2mn, \text{ ou } x = 2mn,\ y = n^2 - m^2, \text{ et } z = n^2 + m^2.$$

I.4. Soit n un entier naturel supérieur ou égal à 6, montrer que si l'on a prouvé que l'équation (F_d) n'admet que les solutions triviales pour un diviseur d de n alors l'équation (F_n) n'admet que les solutions triviales.

En déduire la forme des entiers pour lesquels il suffit de prouver la conjecture de Fermat.

Partie II : étude du cas $n = 4$

On suppose ici que (x, y, z) est un triplet primitif vérifiant la relation

$$x^4 + y^4 = z^2. \tag{E_4}$$

À l'aide du résultat de la partie précédente, on sait qu'il existe deux entiers m et n premiers entre eux tels que

$$x^2 = 2mn,\ y^2 = n^2 - m^2,\ z = n^2 + m^2.$$

(on peut intervertir x et y si besoin est.)

II.1. Montrer que l'on peut trouver deux entiers p et q premiers entre eux tels que

$$m = 2pq,\ y = p^2 - q^2,\ n = p^2 + q^2$$

(résoudre $m^2 + y^2 = n^2$).

II.2. **a.** En déduire l'existence d'un autre triplet primitif (x_1, y_1, z_1) vérifiant (E_4) avec $0 < z_1 < z$.

b. Prouver alors par l'argument de "descente infinie" de Fermat (i.e. avec le a, on met en évidence une suite d'entiers (z_n) strictement décroissante, ce qui est absurde) que (E_4) n'a pas de solution non triviales. Prouver qu'il en est de même de (F_4).

II.3. Application géométrique :

Montrer qu'il n'existe pas de rectangle, dont les côtés et la diagonale sont des entiers, ayant même aire qu'un carré à côtés entiers.

Partie III : étude du cas $n = 3$

On suppose ici que (x, y, z) est un triplet primitif solution de (F_3).

III.1. On sait (petit théorème de Fermat) que, si p est un entier premier, alors $x^p \equiv x \mod p$. Montrer que $xy(x + y)$ est divisible par 3.

En déduire que l'un des entiers x, y, z est divisible par 3.

On s'interesse dans la question suivante à une équation auxiliaire

$$u^2 + 3v^2 = w^3. \tag{E_3}$$

III.2. **a.** Soit $A = \{a^2 + 3b^2,\ (a, b) \in \mathbb{Z}^2\}$. Montrer que l'ensemble A est stable par multiplication (on pourra utiliser les nombres complexes de la forme $a + ib\sqrt{3}$).

b. Donner l'expression de $(a + ib\sqrt{3})^3$, en déduire la décomposition de $(a^2 + 3b^2)^3$ sous la forme $a'^2 + 3b'^2$, on donnera explicitement les expressions de a' et b' en fonction de a et b.

c. En déduire qu'une famille de solutions de l'équation (E_3) est donnée par $u = n^3 - 9nm^2$, $v = 3n^2m - 3m^3$, $w = n^2 + 3m^2$.

On admettra par la suite que l'on trouve par le procédé décrit ci-dessus toutes les solutions de l'équation (E_3) (on utilise un argument de divisibilité dans $\mathbb{Z}(j)$).

III.3. On revient à l'équation (F_3).

On suppose ici que x, y, z ne sont pas forcément positifs, montrer que l'on peut supposer (sans restreindre la généralité du problème) z pair, les deux autres impairs.

Montrer que $u = \dfrac{x+y}{2}$ et $v = \dfrac{x-y}{2}$ sont des entiers premiers entre eux, on vérifie alors sans problème que

$$z^3 = 2u(u^2 + 3v^2).$$

III.4. **a.** On suppose ici que u n'est pas multiple de 3. Montrer alors que $2u$ et $u^2 + 3v^2$ sont les cubes de deux entiers t et w. On sait alors qu'il existe des entiers m et n tels que $u = n^3 - 9nm^2$, $v = 3n^2m - 3m^3$, $w = n^2 + 3m^2$.

b. Montrer que les entiers $2n$, $n - 3m$ et $n + 3m$ sont premiers entre eux deux à deux, que ce sont des cubes d'entiers relatifs z_1, x_1, y_1 et que $|x_1y_1z_1| < |xyz|$.

III.5. On suppose maintenant que u est multiple de 3 que l'on écrit $3u'$. Montrer alors que $18u'$ et $v^2 + 3u'^2$ sont des cubes. Justifier alors rapidement l'existence d'un triplet (x_1, y_1, z_1) tel que $|x_1y_1z_1| < |xyz|$.

III.6. Conclure alors par un argument de descente infinie.

Partie IV : Le théorème de Sophie Germain

On suppose dans cette partie que p est premier tel que $q = 2p + 1$ est aussi premier. On veut prouver alors qu'à cette condition, si (x, y, z) est une solution primitive de

(F'_p) $$x^p + y^p + z^p = 0$$

alors p divise xyz .

On remarque que (F'_p) est équivalente à (F_p).

On aura alors traité le premier cas de Fermat i.e. si (x, y, z) est une solution, alors l'un des entiers est divisible par p.

IV.1. **a.** Montrer que, si a est un entier, alors $(a^p)^2$ est congru à 0 où à 1 modulo q puis que a^p est congru à 0, 1 ou -1 modulo q.

b. En déduire que si $a^p + b^p + c^p \equiv 0 \mod q$ alors q divise abc.

On va raisonner maintenant par l'absurde en supposant que p ne divise pas xyz (et donc qu'il ne divise aucun d'eux).

IV.2. **a.** On a $(-x)^p = (y+z)(y^{p-1} - y^{p-2}z + \cdots + z^{p-1}) = (y+z)X$ (car p est impair). Montrer que $(y+z)$ et X sont premiers entre eux et en déduire qu'il existe a et α deux entiers tels que

$$y + z = a^p, \qquad x = -a\alpha, \qquad y^{p-1} - y^{p-2}z + \cdots + z^{p-1} = \alpha^p$$

On a donc par symétrie l'existence de b, β, c et γ tels que

$$z + x = b^p, \qquad y = -b\beta, \qquad z^{p-1} - z^{p-2}x + \cdots + x^{p-1} = \beta^p$$
$$x + y = c^p, \qquad z = -c\gamma, \qquad x^{p-1} - x^{p-2}y + \cdots + y^{p-1} = \gamma^p$$

b. On suppose que $x \equiv 0 \mod q$. Montrer que $b^p + c^p + (-a)^p \equiv 0 \mod q$. En déduire que q divise abc.
Montrer alors que $a \equiv 0 \mod q$. En déduire que $p\gamma^p \equiv \alpha^p \mod q$ puis l'existence d'un entier a' tel que $a'^p \equiv p \mod q$.

c. Conclure.