SPÉCIALE MP* : CORRIGÉ DU DEVOIR SUR LE THÉORÈME DE FERMAT

Partie I : généralités, étude du cas $n = 2$ — 23

I.1. Si $c = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ alors $p_1^{m\alpha_1} \dots p_k^{m\alpha_k} = ab$.
Si $p_1 | a$ alors, comme $a \wedge b = 1$ alors $p_1 \wedge b = 1$ donc $p_1^{m\alpha_1} \wedge b = 1$. Or $p_1^{m\alpha_1} | ab$ donc, grâce au théorème de Gauss, $p_1^{m\alpha_1} | a$ et c'est la plus grande puissance de p_1 qui divise a.
On va trouver (I, J) un partage de $[1, k]$ tel que $i \in I \Leftrightarrow p_i | a$ et $j \in J \Leftrightarrow p_j | b$, le raisonnement précédent s'appliquant pour chaque nombre premier p_k on obtient ainsi

$$a = \prod_{i \in I} p_i^{m\alpha_i} = \left(\prod_{i \in I} p_i^{\alpha_i} \right)^m \text{ et } b = \prod_{i \in J} p_i^{m\alpha_i} \left(\prod_{i \in J} p_i^{\alpha_i} \right)^m . \quad \boxed{4}$$

Le reste de la démonstration se fait alors par une récurrence immédiate sur n. 1

I.2. **a.** Soit d le P.G.C.D. de x, y, z alors $(x', y', z') = \dfrac{1}{d}(x, y, z)$ est aussi une solution non triviale et primitive. 1

b. Soit (x, y, z) une solution primitive, si p est un nombre premier qui divise x et y alors p^n divise z^n donc p divise z. On a donc $p = 1$ i.e. $x \wedge y = 1$. Les deux autres cas sont semblables. 2
On ne peut avoir deux pairs sur trois (sinon ils ne seraient pas premiers entre eux). Ils ne peuvent être tous impairs (dans $\mathbb{Z}/2\mathbb{Z}$, on a $\dots x^n = 1$, $\dot{y}^n = 1$ et $\dot{z}^n = 1$ et donc $\dot{x}^n + \dot{y}^n \neq \dot{z}^n$). Il ne reste donc qu'une seule éventualité pour une solution primitive, deux sont pairs, le troisième impair. 3

I.3. On raisonne dans $\mathbb{Z}/4\mathbb{Z}$.
Si x et y sont impairs alors $\dot{x}^2 = 1$ et $\dot{y}^2 = 1$ donc $\dot{z}^2 = 2$ ce qui est impossible (2 n'est pas un carré dans $\mathbb{Z}/4\mathbb{Z}$). x et y sont donc de parité différente. 2

Posons $u = \dfrac{y+z}{2}$, $v = \dfrac{z-y}{2}$ ($v > 0$ car $z > y$) alors u et v sont des entiers qui vérifient $y = u - v$, $z = u + v$. Soit $d = u \wedge v$ alors $d | u + v = z$ et $d | u - v = y$, comme (x, y, z) sont premiers deux à deux entre eux alors $d = 1$ i.e. $u \wedge v = 1$. 2

Si $x = 2x'$ alors $x'^2 = uv$ et donc u et v sont les carrés d'entiers premiers entre eux. . . 2

Toutes les solutions recherchées s'écriront donc sous la forme

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

La réciproque est évidente. 2

I.4. Par l'absurde, si l'équation (F_n) admettait une solution non triviale (x, y, z) alors, en prenant $n = dp$, (x^p, y^p, z^p) serait une solution non triviale de (F_d) ce qui est contraire à l'hypothèse. 2

Il suffit donc de prouver la conjecture de Fermat pour tous les nombres premiers supérieurs ou égaux à 3, ainsi que pour l'entier 4 (car cette conjecture est fausse pour $n = 2$). . . 2

Partie II : étude du cas $n = 4$ — 17

II.1. On a $m^2 + y^2 = n^2$, (m, y, n) est un triplet pythagoricien et il est primitif : $m \wedge n = 1$ donc $m \wedge n \wedge y = 1$. 3

On sait, vu le I.4, que y est impair et, toujours avec cette même question, que m est pair donc on a l'existence de p et q tels que

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

II.2. **a.** n, p et q sont premiers deux à deux et comme $\dfrac{x^2}{4} = \dfrac{nm}{2} = npq$, n, p et q sont donc des carrés (toujours grâce au I.1.), on va alors poser $n = z_1^2$, $p = x_1^2$ et $q = y_1^2$ et on aura $z_1^2 = x_1^4 + y_1^4$.

Enfin on a $0 < z_1 = \sqrt{n} \leqslant n^2 = z - m^2 < z$. 4

b. On va donc construire une suite d'entiers strictement positifs (z_n) et strictement décroissante ce qui est impossible. 2

Conclusion : E_4 n'a pas de solution non triviale, il en est de même de F_4 (en posant $z' = z^2$ on se ramène à E_4.) 2

II.3. Par l'absurde, s'il existe un rectangle qui répond à la question, soient a, b les côtés de ce rectangle.

On a donc $ab = c^2$ (où c est le coté du carré) et $d^2 = a^2 + b^2$ d'où $(bd)^2 = c^4 + b^4$ ce qui est impossible avec des nombres strictement positifs. 4

Partie III : étude du cas $n = 3$ — 37

III.1. On a $z \equiv z^3 \mod 3 \equiv x^3 + y^3 \mod 3 \equiv x + y \mod 3$ d'où en travaillant dans $\mathbb{Z}/9\mathbb{Z}$, on peut écrire

$$\begin{aligned} \dot{x}^3 + \dot{y}^3 = \dot{z}^3 &= (\dot{x} + \dot{y} + 3\dot{k})^3 \\ &= (\dot{x} + \dot{y})^3 \qquad \text{car } (\dot{a} + 3\dot{k})^3 = \dot{a}^3 \text{ dans } \mathbb{Z}/9\mathbb{Z} \\ &= \dot{x}^3 + \dot{y}^3 + 3\dot{x}\dot{y}(\dot{x} + \dot{y}) \end{aligned}$$

i.e. $3\dot{x}\dot{y}(\dot{x} + \dot{y}) = 0$ et donc $xy(x + y)$ est divisible par 3. 5

L'un des entiers x, y, $x + y \equiv z \mod 3$ est par conséquent divisible par 3 c.q.f.d. 1

Remarque : on pouvait aussi raisonner de la sorte :

Dans $\mathbb{Z}/9\mathbb{Z}$ on a $(3n + \varepsilon)^3 = \varepsilon$ pour $\varepsilon \in \{0, 1, -1\}$ donc les seuls cubes dans $\mathbb{Z}/9\mathbb{Z}$ sont 0, 1, -1 (en effet, tout élément de $\mathbb{Z}/9\mathbb{Z}$ peut s'écrire $3n + \varepsilon$). Or $x^3 + y^3 + (-z)^3 = 0$ qui est somme des éléments de l'ensemble $\{0, 1, -1\}$ donc l'un au moins de ces éléments est nul i.e. x^3 ou y^3 ou z^3 est divisible par 3 ce qui donne le résultat.

III.2. **a.** On remarque que A est l'ensemble des modules des éléments de $\mathbb{Z}[i\sqrt{3}]$ et comme ce dernier ensemble est stable pour la multiplication (c'est un anneau), il en est de même pour A. 3

b. On a

$$(a + ib\sqrt{3})^3 = a^3 - 9ab^2 + i(3a^2b - 3b^3)\sqrt{3}$$

et, en prenant les modules, on obtient

$$(a^2 + 3b^2)^3 = (a^3 - 9ab^2)^2 + 3(3a^2b - 3b^3)^2.$$

ce qui donne

$$a' = a^3 - 9ab^2,\ b' = 3a^2b - 3b^3.$$ 2

c. La réponse est alors immédiate ! Il suffit de remplacer a par n et b par m. 1
On pourra consulter ici le livre de Hardy & Wright, *An introduction to the theory of numbers*

III.3. On peut réécrire l'équation (F_3) sous la forme $x^3 + y^3 + (-z)^3 = 0$ ce qui est symétrique en x, y, z et ainsi supposer que z est l'entier pair (les deux autres étant nécessairement impairs). 2

$u = \dfrac{x+y}{2}$ et $v = \dfrac{x-y}{2}$ sont des entiers premiers entre eux, en effet, si $d|u$ et $d|v$ alors $d|x$ et $d|y$ i.e. $d = 1$. 1

III.4. **a.** On remarque tout d'abord que u et v sont de parité contraire (en effet $u - v$ est impair). Si d est un nombre premier tel que $d|2u$ et $d|u^2 + 3v^2$ alors d ne peut être égal à 2 ($u^2 + 3v^2$ est forcément impair). $d \neq 3$ car u n'est pas divisible par 3, et donc $d|u$, $d|3v^2$ i.e. $d|v$, $d = 1$ c.q.f.d. 3
On peut alors dire que $2u$ et $u^2 + 3v^2$ sont les cubes de deux entiers t et w premiers entre eux (quitte à multiplier par $-1 = (-1)^3$ si $u < 0$) avec t pair et w impair car 2 divise t. u est alors pair car $t = 2t'$ entraîne $u = 4t'^3$. 2

b.
- On écrit $2u = (n-3m)2n(n+3m)$ et $v = (3n-3m)m(n+m)$. Si $d = 2n \wedge (n-3m)$ alors $d|u$ et $d|(3n - 3m) = 2n + (n - 3m)$ donc $d|v$ soit $d = 1$. On en déduit que : $2n \wedge (n - 3m) = 1$. 3
- On procède de même pour prouver que $2n \wedge (n + 3m) = 1$. 1
- Enfin, en utilisant la propriété $(a + b) \wedge (a - b) = a \wedge b$ (pour a et b de parité différente) on a

$$(n + 3m) \wedge (n - 3m) = n \wedge (3m) = 1.$$ 1

Comme u est un cube alors il existe des entiers z_1, x_1, y_1 tels que $2n = z_1^3$, $n-3m = x_1^3$ et $n + 3m = y_1^3$ (cf. I.1). 1
On a enfin $|x_1y_1z_1|^3 = 2|u| = |x + y|$ qui divise strictement $|x^3 + y^3| = |z|^3$ car

$$z^3 = 2u(u^2 + 3v^2) = x_1y_1z_1(u^2 + 3v^2)$$

et comme $u \neq 0$, $v \neq 0$ ($x \neq \pm y$) alors $u^2 + 3v^2 > 1$ et par conséquent

$$|x_1y_1z_1| < |xyz|.$$ 3

III.5. Si $u = 3u'$ alors v n'est pas multiple de 3. Soit $d = (18u') \wedge (3u'^2 + v^2)$, 3 ne divise pas d car il ne divise pas $3u'^2 + v^2$ donc

$$d = (2u') \wedge (3u'^2 + v^2).$$

On sait aussi que u est pair, v impair donc $3u'^2 + v^2$ est impair, d est lui aussi impair donc

$$d = u' \wedge (3u'^2 + v^2) = u' \wedge v^2 = 1$$ 4

car $u \wedge v = 1$.
$18u'$ et $v^2 + 3u'^2$ sont donc premiers entre eux et ce sont donc des cubes d'entiers. On procède alors comme ci-dessus, on en déduit l'existence d'un triplet (x_1, y_1, z_1) tel que $|x_1y_1z_1| < |xyz|$. 2

III.6. On a vu que l'on pouvait construire une suite de triplets (x_n, y_n, z_n) de solutions primitives non nulles de (F_3) et que la suite $(|x_n y_n z_n|)$ est strictement décroissante, ce qui est impossible. 2

Conclusion : il n'existe pas de solution non triviale à l'équation (F_3).

Partie IV : Le théorème de Sophie Germain 19

IV.1. **a.** D'après le petit théorème de Fermat, on sait que $a^q \equiv a \mod q$ donc, en distinguant les deux cas (a multiple de q et a non multiple de q), $a^{q-1} = (a^p)^2$ est congru à 0 ou à 1 modulo q. 2

Comme l'équation $x^2 = 1$ n'a que deux solutions sur un corps (en l'occurrence sur $\mathbb{Z}/q\mathbb{Z}$) ($(x^2-1) = (x-1)(x+1) = 0 \Leftrightarrow x = \pm 1$), alors a^p est congru à 0, 1 ou -1 modulo q. 2

b. Vu la question précédente, si a, b et c ne sont pas divisibles par q, alors a^p, b^p, c^p sont congrus à ± 1 modulo q, ce qui est incompatible avec la condition $a^p + b^p + c^p = 0$ en effet, dans $\mathbb{Z}/q\mathbb{Z}$, on va trouver ± 1 ou ± 3 selon les cas, c'est le même genre d'argument que pour la question III.1. On a donc q qui divise abc. 3

IV.2. **a.** En effet, si r est un nombre premier qui divise $y+z$ et X alors on a (dans $\mathbb{Z}/r\mathbb{Z}$) $\dot{z} = -\dot{y}$ donc $p\dot{y}^{p-1} = 0$ et comme $p \wedge r = 1$ (on a supposé que p ne divisait pas $x = (y+z)X$) alors $\dot{y} = 0$ puis $\dot{z} = 0$ et finalement $\dot{x} = 0$. r divise x, y, z ce qui est impossible. 3

X et $y+z$ sont bien premiers entre eux.
On peut alors conclure que X et $y+z$ sont des puissances $p^{\text{ièmes}}$ et que l'on peut écrire :

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

b. On utilise la relation $2x = b^p + c^p + (-a)^p \equiv 0 \mod q$. Vu le 1.b., q divise abc... 1

Si q divise b alors $y = -b\beta$ est divisible par q ce qui est impossible car on a supposé x et y premiers entre eux. De même pour c donc il ne reste que a pour être divisible par q. 2

On a alors dans $\mathbb{Z}/q\mathbb{Z}$ $\dot{y} = -\dot{z}$ et donc $\dot{\alpha}^p = p\dot{y}^{p-1}$. 1

Comme $y^{p-1} = \gamma^p - x^{p-1} + x^{p-2}y + \cdots + xy^{p-2}$ et $\dot{x} = 0$ (car q divise x) alors $\dot{y}^{p-1} = \dot{\gamma}^p$. On a enfin $\dot{\alpha}^p = \dot{p}\dot{\gamma}^p$ dans $\mathbb{Z}/q\mathbb{Z}$ (avec $\dot{\gamma} \neq 0$ sinon $p|c$ ce qui a été écarté), ce qui donne $(\dot{\alpha}\dot{\gamma}^{-1})^p = \dot{p}$ dans $\mathbb{Z}/q\mathbb{Z}$ et on a vu au IV.1.a. que c'était impossible. 3

c. La conclusion est alors immédiate : comme on a raisonné par l'absurde, l'hypothèse p ne divise pas xyz est fausse et en conclusion l'un des termes x, y ou z est divisible par p. 1