Devoir Maison n° 8: corrigé

MPSI Lycée Camille Jullian

24 février 2026

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

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

1. (a) Le triplet le plus « petit » et donc le plus simple est $(3, 4, 5)$: $3^2 + 4^2 = 9 + 16 = 25 = 5^2$. Bien sûr, une fois qu'on en tient un, il suffit de multiplier chacun des entiers le constituant par un même entier non nul k pour en obtenir plein d'autres. Ainsi, tous les triplets de la forme $(3k, 4k, 5k)$ sont des triplets pythagoriciens. Ce sont par ailleurs très loin d'être les seuls, comme on va le démontrer.

   (b) Si $x \wedge y = 1$, alors clairement x, y et z sont premiers entre eux dans leur ensemble (les seuls diviseurs communs aux trois entiers x, y et z étant a fortiori des diviseurs communs de x et de y). De plus, si on note p un diviseur commun **premier** de y et z, alors p divise $z^2 - y^2 = x^2$, donc p divise x en appliquant par exemple le théorème de Gauss (p divise $x \times x$, et ne peut pas être premier avec x puisque ça implique d'après Gauss qu'il divise « l'autre x »). L'entier p est donc un diviseur premier commun à y et x, ce qui contredit le fait que $x \wedge y = 1$. De même on montre facilement sous l'hypothèse $x \wedge y = 1$ qu'il n'y a pas de diviseur premier commun à x et z. On a donc prouvé que x et y premiers entre eux impliquait que les trois entiers sont premiers entre eux deux à deux.

   Pour la réciproque, il suffit de prouver que si les trois entiers sont premiers entre eux dans leur ensemble, alors $x \wedge y = 1$ (puisque la propriété « premiers entre eux deux à deux » implique elle-même le caractère « premiers entre eux dans leur ensemble »). On le fait par l'absurde : s'il existe un entier premier p diviseur commun de x et y, alors il est diviseur de z^2 donc de z (même raisonnement que ci-dessus), ce qui contredit notre hypothèse.

   (c) Si on suppose x et y pairs tous les deux, alors on ne peut pas avoir $x \wedge y = 1$, donc le triplet n'est pas primitif. Si on suppose au contraire x et y impairs, alors z^2 est pair comme somme de deux entiers impairs, donc z lui-même est pair. Dans ce cas, z^2 est en fait multiple de 4. Or, le carré d'un entier impair est toujours congru à 1 modulo 4 (en effet, $(2k + 1)^2 = 4k^2 + 4k + 1 \equiv 1[4]$), donc on devrait avoir $x^2 + y^2 \equiv 1 + 1[4] \equiv 2[4]$, ce qui contredit le fait que z^2 est multiple de 4. Il ne reste donc que la possibilité de la parité opposée pour x et y, et comme x^2 et y^2 sont de même parité que x et y, on en déduit que z est nécessairement un entier impair.

   (d) Commençons par vérifier que c'est un triplet pythagoricien : $(2pq)^2 + (p^2 - q^2)^2 = 4p^2q^2 + p^4 - 2p^2q^2 + q^4 = p^4 + 2p^2q^2 + q^4 = (p^2 + q^2)^2$, ça marche. Reste à prouver que le triplet est primitif. On peut par exemple le faire, en utilisant la question b, que deux de ses éléments sont premiers entre eux (les trois éléments étant alors nécessairement premiers entre eux dans leur ensemble). Or, si d est un diviseur commun de $p^2 - q^2$ et de $p^2 + q^2$, alors il divise leur somme et leur différence, donc $2p^2$ et $2q^2$. Comme p et q sont supposés de partié opposée, d ne peut pas être égal à 2 (ni même pair) puisque $p^2 + q^2$ est nécessairement impair. On en déduit (via le théorème de Gauss) que d divise q^2, donc q, et divise aussi

p^2, donc p. C'est absurde puisqu'on a supposé p et q premiers entre eux, donc p^2-q^2 et p^2+q^2 sont eux-mêmes premiers entre eux, et le triplet est bien primitif.

(e) i. On a $x=2pq$, donc $\dfrac{p}{q}=\dfrac{x}{2q^2}$. Or, comme on l'a vu à la question précédente, $2q^2=z-y$, donc $\dfrac{p}{q}=\dfrac{x}{z-y}$.

ii. Il suffit de calculer le quotient $\dfrac{p^2-q^2}{p^2+q^2}=\dfrac{(\frac{p}{q})^2-1}{(\frac{p}{q})^2+1}=\dfrac{(\frac{x}{z-y})^2-1}{(\frac{x}{z-y})^2+1}=\dfrac{x^2-(z-y)^2}{x^2+(z-y)^2}=\dfrac{x^2-y^2-z^2+2zy}{x^2+y^2+z^2-2yz}$. En exploitant l'hypothèse $x^2+y^2=z^2$, on peut simplifier $x^2+y^2+z^2$ en $2z^2$ et $x^2-y^2-z^2$ et $-2y^2$ pour obtenir le quotient $\dfrac{-2y^2+2yz}{2z^2-2yz}=\dfrac{y(z-y)}{z(z-y)}=\dfrac{y}{z}$. Comme par hypothèse la fraction $\dfrac{y}{z}$ est irréductible, on en déduit bien que p^2-q^2 et p^2+q^2 sont des multiples entiers identiques de y et z.

iii. En reprenant la démonstration de la question d, l'hypothèse p et q premiers entre eux de parité opposée implique que p^2+q^2 et p^2-q^2 sont premiers entre eux, et donc que $\alpha=1$. On a donc $p^2+q^2=z$ et $p^2-q^2=y$. On en déduit que $x^2=z^2-y^2=4p^2q^2$, donc $x=2pq$ (tout est positif), ce qui prouve la réciproque souhaitée.

2. (a) Supposons donc qu'un triplet pythagoricien non primitif a « une aire carrée », donc qu'on a un triplet (x,y,z) vérifiant $\dfrac{1}{2}xy=w^2$ (puisque l'aire du triangle correspond est la moitié du produit des deux côtés entourant l'angle droit), soit $xy=2w^2$. Si le triplet n'est pas primitif, cela signifie qu'il existe un diviseur d commun aux trois entiers x, y et z. Posons alors $x'=\dfrac{x}{d}$, $y'=\dfrac{y}{d}$ et $z'=\dfrac{z}{d}$. Le triplet (x',y',z') est pythagoricien primitif (quitte à prendre pour d le plus grand diviseur commun possible), et l'aire correspondante est $\dfrac{1}{2}x'y'=\dfrac{xy}{2d^2}=\left(\dfrac{w}{d}\right)^2$, donc l'aire reste un carré parfait (w étant lui-même divisible par d). Par contraposée, si aucun triplet primitif n'a une aire carrée, ce ne sera le cas d'aucun triplet pythagoricien.

(b) On l'a déjà dit : l'aire vaut $\dfrac{1}{2}xy$, donc, avec les notations de la question 1, elle est aussi égale à $pq(p^2-q^2)$.

(c) On commence par constater que les produits pq et $(p-q)(p+q)$ sont premiers entre eux. En effet, un diviseur **premier** non trivial du produit pq divise soit p soit q mais pas les deux (puisqu'ils sont supposés premiers entre eux), donc ne peut pas diviser $p+q$ ni $p-q$, et donc pas leur produit (puisqu'il est premier). Comme on peut nécessairement décomposer le produit $pq(p-q)(p+q)$, qui est un carré, comme produit de carrés $p_1^2\times\dots p_k^2$ avec les entiers p_i premiers (éventuellement répétés) chaque entier p_i divise soit pq, soit $(p+q)(p-q)$, donc son carré également. Autrement dit, les deux produits pq et $(p+q)(p-q)$ sont eux mêmes des produits de carrés d'entiers premiers, et donc des carrés parfaits. Il ne reste maintenant plus qu'à refaire exactement le même raisonnemment sur les deux facteurs p et q (qui sont premiers entre eux) d'un côté, et de l'autre sur les deux facteurs $p+q$ et $p-q$ (eux aussi premiers entre eux).

(d) Si e est un diviseur premier commun des deux entiers $c+d$ et $c-d$, alors e divise leur somme et leur différence, donc $2d$ et $2c$. Soit $e=2$, soit e divise à la fois d et c, donc à la fois leurs carrés $p+q$ et $p-q$, ce qui n'est pas possible. Reste à vérifier que 2 est bien diviseur commun de $c+d$ et de $c-d$. Or, p et q sont de parité opposée, donc $p+q$ et $p-q$ sont tous les deux impairs, ce qui implique que c et d dont également impairs, donc $c+d$ et $c-d$ pairs. Il ne faudrait par contre par que ces deux nombres soient divisibles par 4. Or, c étant impair, $2c$ n'est pas divisible par 4. Or, $2c=(c+d)+(c-d)$ serait divisible par 4 si 4 était diviseur commun de $c-d$ et $c+d$. Conclusion, on a bien $(c-d)\wedge(c+d)=2$.

(e) Le produit $(d-c)(c+d)$ étant égal à d^2-c^2, donc à $(p+q)-(p-q)=2q$, on peut

l'écrire sous la forme $2b^2$. Mais on vient de prouver que $d-c$ et $d+c$ étaient tous les deux pairs, ce qui prouve que leur produit est divisible par 4 et donc que b^2 est lui-même pair, ce qui prouve que b est pair, et donc que notre produit est en fait divisible par 8. L'un des deux facteurs $d-c$ ou $d+c$ est donc divisible par 4. Supposons par exemple que ce soit $d-c$ (l'autre cas est complètement similaire), alors $\frac{d-c}{4} \times \frac{d+c}{2} = \left(\frac{b}{2}\right)^2$, avec les deux facteurs de gauche qui sont premiers entre eux d'après la question précédente. Par le raisonnement déjà fait plusieurs fois dans les questions précédentes, chaque facteur est donc un carré parfait, ce qui est exactement ce qu'on voulait prouver.

(f) Vérifions : $r^4 + 4s^4 = \frac{(c+d)^2}{4} + \frac{(d-c)^2}{4} = \frac{c^2+d^2}{2} = \frac{p-q+p+q}{2} = p = a^2$, donc le triplet est bien un triplet pythagoricien. De plus, $a \leqslant a^2 = p < p^2 + q^2$.

(g) Non seulement le triplet précédent est pythagoricien, mais il a une aire qui est un carré (elle vaut r^2s^2) et il est primitif (r et s sont premiers entre eux et r est impair, donc r^2 et $2s^2$ sont premiers entre eux). À partir d'un triplet primitif d'aire carrée, on peut donc construire un nouveau triplet primitif d'aire carrée dont la troisième composante est strictement inférieure à celle du premier triplet. C'est absurde : s'il existe des triplets primitifs d'aire carrée, alors l'ensemble des valeurs prises par leur troisième paramètre est un sous-ensemble non-vide de $\mathbb{N}^*$, qui admet donc un minimum. Ça ne peut pas être le cas ici, ce qui prouve qu'aucun triplet ptimitif, et donc aucun triplet pythagoricien tout court, ne peut avoir une aire qui est un carré parfait.

3. (a) S'il existe une solution de l'équation pour laquelle x, y et z admettent un diviseur commun, on peut les diviser tous les trois par ce diviseur pour obtenir une solution « primitive » au même sens que celui utilisé pour décrire les triplets pythagoriciens. Une telle solution primitive est forcément constituée de trois entiers x, y et z premiers entre eux deux à deux, par la même démonstration que celle effectuée en tout début de problème.

Puisque x et y sont désormais premiers entre eux, au moins l'un des deux est impair. S'ils le sont tous les deux, alors x^2 et y^2 sont aussi impairs, dont on déduit que $x^4 \equiv 1[4]$ et $y^4 \equiv 1[4]$, donc $z^4 \equiv 2[4]$. Or, z est nécessairement pair dans ce cas, donc z^4 est divisible par 4, ce qui produit une contradiction. Quitte à échanger le rôle de x et y, on peut donc supposer x pair (et donc y impair).

(b) Commençons déjà par constater que $(z^2+y^2)(z^2-y^2) = z^4 - y^4 = x^4$ si (x, y, z) est solution de l'équation de Fermat. Or, avec z et y impairs (cf question précédente), y^2 et z^2 sont tous deux congrus à 1 modulo 4. On en déduit directement que $z^2 - y^2$ est divisible (au moins) par 4, et $z^2 + y^2$ par 2 mais pas par 4. Or, x^4, en tant que puissance quatrième d'un nombre supposé pair, est divisible par $2^4 = 16$, donc $z^2 - y^2$ est en fait (au moins) divisible par 8. On a alors bien sûr $\frac{z^2-y^2}{8} \times \frac{z^2+y^2}{2} = \left(\frac{x}{2}\right)^4$. Or, les deux facteurs du produit de gauche sont premiers entre (même raisonnement que ci-dessus à la question 3.*d*, le seul diviseur premier commun de $z^2 - y^2$ et de $z^2 + y^2$ est 2). En effectuant à nouveau un raisonnement récurrent dans ce problème, on en déduit que chaque facteur est puissance quatrième d'un entier (le membre de droite de l'égalité est produit de puissances quatrièmes de nombres premiers, qui ne peuvent pas diviser à la fois le premier facteur de gauche et le deuxième, ce qui prouve que chacun de ces deux facteurs a lui-même des valuations p-adiques qui sont toutes multiples de 4), donc on peut bien écrire $z^2 - y^2 = 8a^4$ et $z^2 + y^2 = 2b^4$.

(c) Puisque $z^2 - y^2 + z^2 + y^2 = 2z^2$, on a $4a^4 + b^4 = z^2$, donc $(2a^2)^2 + (b^2)^2 = z^2$, ce qui signifie que $(2a^2, b^2, z)$ est un triplet pythagoricien. Or, l'aire du triangle rectangle correspondant vaut a^2b^2, qui est évidemment un carré parfait. La question 3 a montré que cette situation n'est pas possible, ce qui prouve qu'il n'existe aucune solution à l'équation $x^4 + y^4 = z^4$ dans $\mathbb{N}^*$. Fermat aurait vraiment eu besoin de marges super grandes dans ses bouquins

pour arriver à faire tenir ne serait-ce que la démonstration de ce cas particulier de son théorème...

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

1. (a) Cette question est en fait complètement débile : si p et q sont premiers entre eux dans $\mathbb{Z}$, ils le sont nécessairement dans $\mathbb{Z}[j]$ qui inclut $\mathbb{Z}$ (la réciproque n'est par contre par nécessairement vraie). Il suffit pour le prouver très rapidement de recourir au théorème de Bézout : il existe deux entiers a et b tels que $ap + bq = 1$. Or, a et b sont aussi des éléments de $\mathbb{Z}[j]$, donc la relation précédente est également une relation de Bézout dans $\mathbb{Z}[j]$, ce qui prouve bien que p et q sont aussi premiers entre eux dans cet ensemble.

   (b) Commençons par prouver par l'absurde que 2 est un nombre premier dans $\mathbb{Z}[j]$: si on peut décomposer 2 sout la forme $2 = z_1 z_2$, avec $|2|^2 = 4 = |z_1|^2|z_2|^2$. Or, si $z = a + jb \in \mathbb{Z}[j]$, alors $|z|^2 = \left(a - \frac{b}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}b\right)^2 = a^2 - ab + b^2 \in \mathbb{N}$, donc les seules possibilités sont d'avoir $|z_1| = 1$ ou $|z_2| = 1$ (mais dans ce cas la décomposition n'empêche pas 2 d'être premier), ou $|z_1|^2 = |z_2|^2 = 2$. Or, l'équation $a^2 - ab + b^2 = 2$ n'a pas de solutions dans $\mathbb{Z}^2$ (en effet, $a^2 + b^2 - ab$ est impair sauf si a et b sont tous les deux pairs, mais si c'est le cas $a^2 + b^2 - ab$ est un multiple de 4 qui ne peut donc pas être égal à 2), ce qui prouve bien que la décomposition est impossible et donc que 2 est premier.

   Passons au cas de $i\sqrt{3}$. Constatons déjà que $i\sqrt{3} = 2j+1 \in \mathbb{Z}[j]$, et qu'il vérifie $|i\sqrt{3}|^2 = 3$. C'est encore plus rapide que tout à l'heure puisque 3 ne peut pas s'écrire comme produit de deux entiers positifs différents de 1, ce qui prouve immédiatement que $i\sqrt{3}$ est premier dans $\mathbb{Z}[j]$.

   Supposons désormais que les deux nombres $p + i\sqrt{3}q = p + (2j + 1)q$ et $p - i\sqrt{3}q = p - (2j + 1)q$ admettent comme diviseur commun $d \in \mathbb{Z}[j]$, alors d divise leur somme et leur différence, donc divise $2p$ et $(4j + 2)q = 2i\sqrt{3}q$. On peut supposer d premier, il divise alors 2 ou p (théorème de Gauss), et d divise 2 ou $i\sqrt{3}$ ou q. Comme p et q sont supposés premiers entre eux, il faut donc éliminer les cas $d = 2$ et $d = i\sqrt{3}$ (dont on vient de démontrer qu'il n'ont pas de diviseurs « plus petits ») pour aboutir à la contradition que d divise à la fois p et q et donc que d est une unité (ce qui prouvera que $p + i\sqrt{3}q$ et $p - i\sqrt{3}q$ n'ont pas de diviseur commun autre que les unités, et sont donc premiers entre eux).

   Commençons par exclure le cas $d = 2$: si 2 divise $p + i\sqrt{3}q = p + q + 2jq$, alors il existe deux entiers a et b tels que $p + q + 2jq = 2a + 2bj$. Par identification, $2a = p + q$ et $b = q$. Les entiers p et q sont donc de même parité (leur somme est paire), donc impairs tous les deux (sinon ils ne seraient pas premiers entre eux !). Or, si p est impair, $p^2 \equiv 1[8]$ (calcul facile laissé en petit exercice au lecteur). De même, $3q^2 \equiv 3[8]$, donc $p^2 + 3q^2 \equiv 4[8]$. Or, on a supposé il y a quelques heures de cela que le nombre $p^2 + 3q^2$ était le cube d'un entier, et aucun cube n'est congru à 4 modulo 8 (il faudrait que l'entier soit pair pour que ça puisse être le cas, et dans ce cas son cube est divisible par 8), ce qui apporte la contradiction souhaitée : on ne peut pas avoir $d = 2$.

   Essayons maintenant d'exclure le cas $d = i\sqrt{3} = 2j + 1$ (à un facteur inversible près). Puisque d est supposé diviser p, il divise $p \pm i\sqrt{3}$, donc son carré -3 (et son opposé 3) divise le produit $(p + i\sqrt{3})(p - i\sqrt{3}) = p^2 + 3q^2$, donc il divise un cube d'entier. Ce n'est possible que si l'entier correspondant est un multiple de 3 et donc son cube un multiple de 27, et a fortiori un multiple de 9. Bref, on devrait avoir $p^2 + 3q^2$ mutliple de 9. Or, $p^2 + 3q^2$ est un multiple de 3 donc p^2 aussi, donc p aussi, ce qui implique à son tour quep^2 est en fait un multiple de 9. Il faudrait donc que $3q^2$ soit lui aussi multiple de 9, donc que

q^2 et donc q soient divisibles par 3. Mais alors p et q ne peuvent pas être premiers entre eux, ce qui nous donne à nouveau une contradition. Ouf...

(c) De loin, ça a l'air facile : il suffit de constater que $(p + i\sqrt{3})(p - i\sqrt{3})$ est un cube, donc le produit de cubes de nombres premiers (ici premiers dans $\mathbb{Z}[j]$), donc chacun de ses facteurs est lui-même produit de cubes (toujours dans $\mathbb{Z}[j]$). Sauf qu'on ne demande pas d'écrire $p + i\sqrt{3}$ comme cube d'un élément de $\mathbb{Z}[j]$, mais d'un élément de $\mathbb{Z}[i\sqrt{3}]$ (donc de la forme $a + bi\sqrt{3}$). Il y a par ailleurs un autre problème, c'est que dans $\mathbb{Z}[j]$ la décomposition en facteurs premiers est unique **à multiplication par un inversible près**. Pour l'instant, tout ce qu'on peut affirmer, c'est donc que $p + i\sqrt{3}q = u(\alpha + \beta j)^3$. Dans la mesure où $j^3 = 1$, on peut aussi écrire $p+i\sqrt{3}q = u(\alpha j+\beta j^2)^3 = u(-\beta+(\alpha_\beta)j)^3$. De même, en multipliant par j^2 avant d'élever au cube, on aura une troisième expréssion : $p+i\sqrt{3}q = u(\alpha j^2+\beta)^3 = u(\beta-\alpha-\alpha j)^3$ (on rappelle à ceux qui ont trop dormi en cours lors du chapitre sur les complexes que $1 + j + j^2 = 0$). Parmi ces trois écritures, une au moins des trois fait intervenir un coefficient pair devant j (on ne peut pas avoir β, $\alpha - \beta$ et α tous les trois impairs). Quitte à le diviser par 2, on a alors $p+i\sqrt{3}q = u(\gamma+i\sqrt{3}\delta)^3$, avec γ et δ tous les deux entiers.

Il reste à prouver que le facteur inversible u est égal à 1, ou éventuellement à -1 (on change alors les signes de γ et δ et ça marche). Les seules autres valeurs possibles pour u sont les autres éléments de $\mathbb{Z}[j]$ de module 1, c'est-à-dire j, j^2, $-j$ et $-j^2$ (démonstration de ce fait effectuée dans le DM5 sur les ensembles réticulés). Supposons par exemple $u = j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ et essayons d'aboutir à une contradiction. On aurait donc $p + i\sqrt{3} = j(\gamma+i\sqrt{3}\delta)^3 = \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)(\gamma^3+3i\sqrt{3}\gamma^2\delta-9\gamma\delta^2-3i\sqrt{3}\delta^3) = \frac{1}{2}(\gamma^3-9\gamma\delta^2-9\gamma^2\delta+9\delta^3+ i\sqrt{3}(\gamma^3-9\gamma\delta^2-3\gamma^2\delta+3\delta^3))$. Histoire de compléter un peu notre bestiaire issu de l'alphaber grec, posons donc $\xi = \gamma^3 - 9\gamma\delta^2 = \gamma(\gamma - 3\delta)\gamma + 3\delta)$ et $\theta = 3\delta^3 - 3\gamma^2\delta = 3\delta(\delta - \gamma)(\delta + \gamma)$. Si ξ est impair, alors chacun des facteurs γ, $\gamma - 3\delta$ et $\gamma + 3\delta$ est impair, donc δ est pair (et γ impair), donc θ est pair. Dans ce cas, les parties réelle et imaginaire de $2u(\alpha + i\beta)^3$ (calculées plus haut, elles sont égales respectivement à $-\xi+3\theta$ et $\xi+\theta$) sont impaire, ce qui veut dire que $u(\alpha + i\beta)^3$ ne'st pas un élément de $\mathbb{Z}[i\sqrt{3}]$, ce qui est une contradiction. On exclut de même le cas où θ est impair (dans ce cas, ξ est pair et on a le même problème). On peut donc affirmer que ξ et θ sont tous les deux pairs, ce qui implique que γ et δ sont de même parité (je vous laisse vérifier, c'est toujours le même type de raisonnement). Tous les facteurs $\gamma + \delta$, $\delta - \gamma$, $\gamma + 3\delta$ et $\gamma - 3\delta$ sont donc pairs, ce qui prouve que ξ et θ sont en fait divisibles par 4. Du coup, $p + i\sqrt{3}q$ est divisible par 4 dans $\mathbb{Z}[j]$, et peut donc s'écrire sous la forme $p+i\sqrt{3}q = 4(k+lj) = 4k-2l+2i\sqrt{3}l$ (avec k et l entiers), ce qui prouve par une simple identification que p et q sont tous les deux pairs. C'est évidemment absurde puisqu'on les a supposé premiers entre eux il y a quelques siècles de cela. On en déduit (enfin) que l'hypothèse $u = j$ est aberrante. Je vous épargne le raisonnements pour exclure les cas $u = -j$, $u = j^2$ et $u = -j^2$ qui sont très similaires (quelques signes à changer).

On a donc à peu près prouvé que $p + i\sqrt{3}q = (a + i\sqrt{3}b)^3$, et en développant bêtement le cube (ce qu'on a déjà fait en cours de calcul plus haut) puis en identifiant les parties réelle et imaginaire, on trouve $p = a^3 - 9ab^2$ et $q = 3a^2b - 3b^3$.

(d) Par hypothèse, p et q sont premiers entre eux, donc il existe une combinaison linéaire à coefficients entiers de p et de q qui est égale à 1 (théorème de Bézout). Comme p et q eux-même sont combinaisons linéaires à coefficients entiers de a et b (cf formules de la question précédente), il existe donc une combinaison de a et de b qui est égale à 1, ce qui prouve que $a \wedge b = 1$ (réciproque du théorème de Bézout).

2. (a) C'est le même principe qu'on a déjà appliqué quelques fois dans la première partie : si x, y et z ont un diviseur commun, on peut tout diviser par ce diviseur pour obtenir un triplet

solution constitué de nombres premiers entre eux dans leur ensemble. Et cette dernière propriété est facilement équivalente au caractère premiers entre eux deux à deux des trois variables. Puisque x, y et z sont désormais premiers entre eux, ils ne peuvent évidemment pas être tous les trois pairs. Il ne peut pas non plus y en avoir deux sur les trois qui sont pairs (sinon le troisième le serait aussi !). On a donc au moins deux variables sur les trois qui sont impaires. S'il s'agit de x (ou y, le cas est traité de façon similaire) et z, on écrit que $x^3 + (-z)^3 = (-y)^3$ pour obtenir une solution avec les deux variables du membre de gauche impaires. Ah, l'énoncé n'avait pas précisé que, dans cette partie, les x, y et z avaient le droit d'être des entiers **relatifs**. Il aurait dû le faire.

(b) Si x et y sont tous les deux impairs, $p = \dfrac{x+y}{2}$ et $q = \dfrac{x-y}{2}$ sont effectivement entiers. Avec les notations de l'énoncé, $z^3 = x^3+y^3 = (p+q)^3+(p-q)^3 = 2p^3+6pq^2 = 2p(p^2+3q^2)$ (les autres termes se simplifient), donc $\left(\dfrac{z}{2}\right)^3 = \dfrac{p}{4}(p^2+3q^2)$.

(c) On a supposé x et y tous les deux impairs, donc p et q sont de parité opposée. C'est donc aussi le cas de p^2 (qui a la même parité que p) et $3q^2$ (qui a la même parité que q), donc p^2+3q^2 est effectivement impair. Or, z étant pair, $\left(\dfrac{z}{2}\right)^3$ est entier, donc 4 divise le produit $p(p^2+3q^2)$, et donc divise p puisque le deuxième facteur est impair. On en déduit que p est pair, et q est donc impair.

3. (a) On va utiliser des arguments déjà exploités quelques fois dans ce corrigé, mais on a pour cela besoin que $\dfrac{p}{4}$ et p^2+3q^2 soient premiers entre eux. Constatons déjà que p et q sont premiers entre eux : ils ne peuvent pas avoir un diviseur commun non trivial, sinon il diviserait aussi $p+q$ et $p-q$, donc x et y, qui sont supposés premiers entre eux. Supposons désormais que d soit un diviseur premier commun de $\dfrac{p}{4}$ et de p^2+3q^2, alors d divise p donc p^2, donc divise aussi $3q^2$. Ce diviseur d ne peut pas diviser q^2, sinon il diviserait q alors que p et q sont premiers entre eux. Il est donc égal à 3. Or, cela imposerait que 3 divise $\left(\dfrac{z}{2}\right)^3$, donc divise z, alors même qu'on a supposé dans cette question que z n'était pas multiple de 3. On a donc bien $\dfrac{p}{4}$ et p^2+3q^2 premiers entre eux. Comme leur produit est un cube (donc un produit de cubes de facteurs premiers), ils sont eux-mêmes des cubes par un raisonnement désormais classique.

(b) C'est une conséquence immédiate des questions 1c et 1d (il faut que ça serve à quelque chose, tout de même !).

(c) On sait que q est impair et divisible par b, donc b est aussi impair. De plus, b^2-a^2 doit également être impair, donc a ne peut pas être impair. Il est donc pair.

(d) Les facteurs $a-3b$ et $a+3b$ de la décomposition de p sont tous les deux impairs d'après la question précédente. Comme p est divisible par 4, c'est donc nécessairement le dernier facteur a qui est divisible par 4. Le produit $\dfrac{a}{4}(a+4b)(a-3b)$ est un cube (question a), et les trois facteurs sont premiers entre eux deux à deux (même démonstration qu'en question a, en exploitant le fait que z n'est pas divisible par 3), donc chaque facteur est lui-même un cube : $\dfrac{a}{4} = \alpha^3$, $a+3b = \beta^3$ et $a-3b = \gamma^3$. Or, $\beta^3+\gamma^3 = 2a = 8\times\dfrac{a}{4} = (2\alpha)^3$, donc $(\beta, \gamma, 2\alpha)$ est une nouvelle solution de l'équation de Fermat.

(e) Le produit en question (en valeur absolue puisqu'on peut en fait avoir des entiers négatifs) vérifie $|2\alpha\beta\gamma|^3 = 2|a(a+3b)(a-3b)| = 2|p| < 2(p^2+3q^2) \leqslant z^3 \leqslant |xyz|^3$, donc on a bien $|2\alpha\beta\gamma| < |xyz|$ (et même très largement a priori). On ne peut pour l'instant rien en déduire du tout, car on ne sait pas si le dernier entier 2α est divisible par 3 dans cette nouvelle solution. On ne pourra donc conclure à l'absurdité (comme à la fin de la première partie) que si on arrive à prouver qu'on peut obtenir une solution plus petite aussi dans le cas où z est divisible par 3.

4. Le but est à nouveau de créer une nouvelle solution « plus petite » de l'équation de Fermat,

en exploitant des écritures comme produit de cubes qui supposent que les différents facteurs soient premiers entre eux. On repart de l'égalité $\left(\frac{z}{2}\right)^3 = \frac{p}{4}(p^2+3q^2)$ et on suppose cette fois-ci que z est un multiple de 3. On effectue alors les étapes de raisonnement suivantes :

- si on suppose que p n'est pas un multiple de 3, comme $\left(\frac{z}{2}\right)^3$ est quand à lui divisible par 3, on en déduit que p^2+3q^2 est divisible par 3, donc que 3 divise p^2, puis divise p, ce qui est légèrement absurde. L'entier p est donc divisible par 3, mais ça ne peut pas être le cas de q qui est premier avec p. Du coup, p^2+3q^2 est un multiple de 3 mais pas de 9 (p^2 est un multiple de 9 mais pas $3q^2$). Comme $\left(\frac{z}{2}\right)^3$ est de son côté divisible par $3^3 = 27$, cela impose que $\frac{p}{4}$ soit divisible par 9, ce qui prouve bien que p est divisible par 36.
- on peut donc écrire la nouvelle identité $\left(\frac{z}{6}\right)^3 = \frac{p}{36}\left(3\left(\frac{p}{3}\right)^2+q^2\right)$, tous les éléments intervenant dans cette égalité étant entiers. Supposons maintenant que $\frac{p}{36}$ et $3\left(\frac{p}{3}^2+q^2\right)$ aient un diviseur premier commun d. Si $d \neq 3$, il divise donc p et pas q (ils sont toujours premiers entre eux), donc divise $3\left(\frac{p}{3}\right)^2$ mais pas q^2, ce qui est absurde. Si $r = 3$, c'est en fait pareil puisque 3 divise $3\left(\frac{p}{3}\right)^2$, on aboutit à la même absurdité. Nos deux facteurs sont donc premiers entre eux, et sont donc tous les deux des cubes d'entiers.
- en reprenant les calculs effectués plus haut dans la question 1, il existe deux entiers a et b tels que $\frac{p}{3} = 3a^2b - 3b^3 = 3b(a^2-b^2)$ et $q = a^3 - 9ab^2$, avec de plus a et b premiers entre eux. En particulier, a et b sont de parité opposée, donc a^2-b^2 est impair. Comme $\frac{p}{3}$ est pair (on rappelle que p est divisible par 36), cela impose que b est impair, donc a pair. En fait, p est même divisible par 4, ce qui montre que b est lui aussi un multiple de 4. On peut donc écrire $\frac{p}{36} = \frac{b}{4}(a+b)(a-b)$ avec à droite trois facteurs entiers. Comme d'habitude, on a trois facteurs qui sont premiers entre eux et qui vont donc être eux-même des cubes : $\frac{b}{4} = \alpha^3$, $a+b = \beta^3$ et $a-b = \gamma^3$. On a comme dans la question précédente $\beta^3 + (-\gamma)^3 = 2b = (2\alpha)^3$, ce qui prouve que le triplet $(2\alpha, \gamma, \beta)$ est une nouvelle solution primitive de l'équation de Fermat. Or, $|2\alpha\beta\gamma| = \frac{1}{2}\left|\frac{p}{9}\right| < \left(\frac{z}{2}\right)^3 < |xyz|^3$. On a donc trouvé une solution plus petite que la solution initiale (encore une fois, en pratique, la solution serait même a priori énormément plus petite, la majoration qu'on vient de faire étant loin d'être subtile.

On peut enfin conclure : indépendamment de l'hypothèse de divisibilité par 3 effectuée sur z, on peut toujours trouver, à partir d'une solution donnée de l'équation de Fermat, une nouvelle solution dont le produit des valeurs absolues des entiers est strictement inférieur à celui de la solution initiale. S'il existait vraiment une solution, il y en aurait une pour laquelle ce produit serait minimal (sous-ensemble non-vide de $\mathbb{N}$), on a donc obtenu une absurdité qui prouve que l'équation ne peut pas avoir de solutions.