Une somme circulaire

Daniel PERRIN

1 La question

Si x, y et z sont trois entiers naturels non nuls tels que $\frac{x}{y}+\frac{y}{z}+\frac{z}{x}$ est un entier, montrer que le produit xyz est un cube.

2 Solution

2.1 Avertissement

Ce problème, et notamment la question subsidiaire de caractériser les entiers $s(x,y,z)$ obtenus, est magnifique, mais non trivial. Dans ce qui suit, ma contribution personnelle ne concerne que les paragraphes 2 et 3. Le problème est ramené à l'équation diophantienne $p^3+q^3+r^3-spqr=0$ qui correspond à une courbe elliptique. À partir de là, j'étais convaincu de deux choses : d'abord que le problème n'était pas évident et ensuite, qu'une équation aussi simple ne pouvait pas avoir échappé aux mathématiciens. De fait, elle a été étudiée par de nombreux arithméticiens et je donne un (petit) aperçu de leurs résultats dans le paragraphe 4. On y verra à la fois des résultats positifs (infinité de solutions) ou négatifs (une infinité de s non atteints), mais on verra aussi que le problème est loin d'être entièrement résolu.

2.2 Généralités

On appellera **convenables** les triplets x,y,z vérifiant la propriété et l'ensemble des entiers qui s'écrivent sous la forme $s(x,y,z):=\frac{x}{y}+\frac{y}{z}+\frac{z}{x}$ avec $x,y,z\in\mathbf{N}^*$ sera noté S. La condition que $s(x,y,z)$ est un entier signifie que xyz divise $x^2z+y^2x+z^2y$.

Notons qu'on peut supposer que x,y,z sont premiers entre eux dans leur ensemble (sinon, on se ramène à ce cas en les divisant par leur *pgcd*). Si (x,y,z) est une solution il en est de même des permutations circulaires (y,z,x) et (z,x,y). Si besoin est, cela permet de supposer, par exemple, que x est le plus petit des trois. Attention, la propriété ne subsiste pas pour les permutations non circulaires :

2.1 Proposition. *Si (x,y,z) sont convenables et non tous égaux, (y,x,z) ne le sont pas.*

Démonstration. On peut supposer x, y, z premiers entre eux. Dire que (x, y, z) est convenable signifie que xyz divise $A := x^2z + y^2x + z^2y$. Dire que (y, x, z) l'est signifie que xyz divise $B := y^2z + x^2y + z^2x$. Si les deux triplets sont convenables, xyz divise $yA - zB = x(y^3 - z^3)$, donc yz divise $y^3 - z^3$ et de même par permutation circulaire. Mais alors, si p est un facteur premier, disons [1] de y, il divise z, mais aussi x car xy divise $x^3 - y^3$. C'est une contradiction avec le fait que x, y, z sont premiers entre eux.

2.3 Le théorème principal

Le théorème suivant donne la forme des solutions :

2.2 Théorème. *1) Soient x, y, z des entiers positifs, premiers entre eux dans leur ensemble, tels que $s(x, y, z) = \dfrac{x}{y} + \dfrac{y}{z} + \dfrac{z}{x}$ soit un entier. Alors, il existe des entiers p, q, r premiers entre eux deux à deux tels que l'on ait $x = q^2p$, $y = p^2r$ et $z = r^2q$. L'entier pqr divise $p^3 + q^3 + r^3$, p divise $q^3 + r^3$, q divise $r^3 + p^3$ et r divise $p^3 + q^3$ et on a $s(x, y, z) = \dfrac{p^3 + q^3 + r^3}{pqr}$.*

2) Inversement, si p, q, r sont trois entiers premiers entre eux dans leur ensemble, si p divise q^3+r^3, si q divise r^3+p^3 et si r divise p^3+q^3, p, q, r sont deux à deux premiers entre eux, pqr divise $p^3 + q^3 + r^3$ et $x = pq^2$, $y = p^2r$ et $z = r^2q$ sont convenables.

La réponse à la question posée résulte aussitôt de ce théorème :

2.3 Corollaire. *Si x, y, z sont convenables, xyz est un cube.*

Démonstration. (du corollaire) Si d est le *pgcd* de x, y, z, $x/d, y/d$ et z/d vérifient encore la condition et, en vertu de 2.2, on a $x = dq^2p$, $y = dp^2r$ et $z = dr^2q$, donc $xyz = d^3p^3q^3r^3$ est un cube.

Démonstration. (de 2.2) On note p le *pgcd* de x et y. On a donc $x = px'$, $y = py'$ avec x', y' premiers entre eux.

La condition signifie que xyz divise $x^2z+y^2x+z^2y$, donc que $p^2x'y'z$ divise $p^2x'^2z + p^3y'^2x' + pz^2y'$ ou encore que $px'y'z$ divise $px'^2z + p^2y'^2x' + z^2y'$. Il en résulte que p divise z^2y', mais, comme x, y, z sont premiers entre eux, p est premier avec z donc divise y'.

On pose $y' = pr$ et $p^2x'rz$ divise $px'^2z + p^4r^2x' + prz^2$ donc $px'rz$ divise $x'^2z + p^3r^2x' + rz^2$. On en déduit que r divise x'^2z, donc z puisque r et x' sont premiers entre eux (car x' et y' le sont).

1. Les trois entiers ne sont pas égaux à 1.

On pose $z = rz'$ et on voit que $pr^2x'z'$ divise $x'^2rz' + p^3r^2x' + r^3z'^2$, donc $prx'z'$ divise $x'^2z' + p^3rx' + r^2z'^2$. Il s'ensuit que r divise z' et on pose $z' = qr$, de sorte que $pr^2x'q$ divise $x'^2qr + p^3rx' + r^4q^2$ ou encore que $pqrx'$ divise $x'^2q + p^3x' + r^3q^2$. Mais q et p sont premiers entre eux, de sorte que q, qui divise p^3x', divise x', $x' = qx''$ et pq^2rx'' divise $x''^2q^3 + p^3qx'' + r^3q^2$ ou encore $pqrx''$ divise $x''^2q^2 + p^3x'' + r^3q$. On voit alors que q divise x'', mais aussi que x'' divise r^3q. Comme x'' est premier avec r c'est qu'il divise q et on a donc $x'' = q$.

On a $x' = q^2$, $y' = pr$ et $z' = qr$ (donc $x = pq^2$, $y = p^2r$ et $z = qr^2$ comme annoncé). Comme x' et y' sont premiers entre eux, q est premier avec p et r. De plus, p et r sont premiers entre eux, sinon un facteur commun diviserait à la fois x, y et z. Les conditions de divisibilité annoncées sont la traduction du fait que xyz divise $x^2z + y^2x + z^2y$.

Inversement, si l'on a les hypothèses de 2), supposons qu'un nombre premier l divise (par exemple) p et q. Il divise alors $q^3 + r^3$ donc r^3 donc r et c'est absurde. Comme p, q, r divisent $p^3 + q^3 + r^3$ et sont premiers entre eux deux à deux, le produit divise $p^3 + q^3 + r^3$ et les nombres x, y, z sont convenables.

2.4 *Remarque.* Un avantage de l'écriture de x, y, z en fonction de p, q, r c'est que les conditions sur p, q, r sont invariantes par **toutes** les permutations. Lorsqu'on a une solution p, q, r qui donne $x = pq^2$, $y = p^2r$ et $z = r^2q$ on a aussi la solution q, p, r qui donne $x = p^2q$, $y = q^2r$ et $z = r^2p$, différente de la précédente. Par exemple, avec $p = 1$, $q = 2$, $r = 3$ on a $x = 4$, $y = 3$, $z = 18$ tandis qu'avec q, p, r on a $x = 2$, $y = 12$ et $z = 9$.

3 Compléments

3.1 Une première liste de questions ouvertes

Le théorème 2.2, s'il donne la forme des solutions, laisse cependant beaucoup de questions ouvertes sur le thème : quelles sont les solutions possibles ? Ce thème se décline sur trois niveaux : quels nombres p, q, r possibles ? quels x, y, z ? quelles valeurs de la somme $s(x, y, z)$? Précisément :

1) Déterminer les entiers p, q, r vérifiant les conditions de 2.2. En existe-t-il une infinité ? Pour, disons, p fixé, existe-t-il une infinité de q, r vérifiant les conditions ?

2) Quels sont tous les x, y, z convenables ? Si l'on suppose que x est le plus petit, quels sont les x possibles ? Les nombres x, y, z peuvent-ils être égaux ? Y a-t-il une infinité de solutions ?

En fait, grâce à 2.2, si l'on a la réponse à la question 1), cette deuxième question sera résolue aussi.

3) Quels sont les entiers naturels qui s'écrivent sous la forme $s(x,y,z) := \dfrac{x}{y}+\dfrac{y}{z}+\dfrac{z}{x}$ *avec* x,y,z *entiers ? Leur ensemble* S *est-il infini ?*

On a vu que ce sont aussi les entiers qui s'écrivent $s = \dfrac{p^3+q^3+r^3}{pqr}$ avec p,q,r entiers.

Une recherche avec le logiciel SAGE des entiers p,q,r convenables plus petits que 1000 donne de nombreuses solutions et fournit les valeurs suivantes de s plus petites que 100 (mais on n'en garantit pas l'exhaustivité [2]) : 3, 5, 6, 9, 10, 13, 14, 17, 18, 19, 21, 26, 29, 30, 38, 41, 51, 53, 54, 57, 66, 69, 83, 86, 94.

Cette liste mène à une autre question :

4) Montrer que les valeurs absentes de la liste ci-dessus (au moins pour les plus petites d'entre elles comme 4, 7, 8, 11*) ne sont pas dans* S*. Le complémentaire de* S *est-il infini ?*

Sur ce point, l'examen des résultats produits par l'ordinateur conduit à proposer :

3.1 Conjecture. *Les entiers* $\equiv 0 \pmod 4$ *ou* $\equiv -1 \pmod 8$ *ne sont pas dans* S*.*

On verra que cette conjecture est maintenant prouvée, voir 4.6.

3.2 Quelques résultats sur les (x,y,z) convenables

La proposition suivante résume les premiers résultats sur les triplets convenables, obtenus souvent grâce au théorème 2.2 :

3.2 Proposition. *1) Pour tous réels* x,y,z *positifs, on a* $s(x,y,z) \geq 3$*, l'égalité ayant lieu si et seulement si* $x=y=z$*.*

2) Si (x,y,z) *est convenable avec deux termes égaux on a* $x=y=z$*.*

3) On suppose (par exemple) x *fixé. Il existe au plus un nombre fini de couples* (y,z) *tels que* (x,y,z) *soit convenable et que* x,y,z *soient premiers entre eux et on a un algorithme pour les déterminer.*

Démonstration. 1) Le minimum de la fonction $s(x,y,z)$ sur $(\mathbf{R}^{+*})^3$ est atteint pour $x=y=z$ et vaut 3 car le gradient de la fonction ne s'annule que sur la demi-droite $x=y=z$ (comme on le voit en annulant $\dfrac{\partial s}{\partial x} = \dfrac{1}{y} - \dfrac{z}{x^2}$ et les autres). Il en résulte que S ne contient pas d'entier < 3.

2. En comparant avec la table donnée dans [2] j'ai vu qu'il manque dans cette liste les nombres 67, 73 et 74 pour lesquels les solutions sont plus grandes que 1000. Par exemple pour 73 les solutions sont toutes $> 10^{13}$.

2) On peut supposer x, y, z premiers entre eux. Alors, $x = y$ (par exemple) implique $q^2 = pr$ et comme q est premier avec p et r c'est qu'il est égal à 1, ainsi que p et r.

3) On écrit $x = pq^2$ avec p, q premiers entre eux, ce qui n'est possible que d'un nombre fini de façons. Ensuite, on cherche r qui divise $p^3 + q^3$. Là encore, il n'y a qu'un nombre fini de solutions.

3.3 *Remarques.* 1) Pour $x = 1$ on a $p = q = 1$ et r divise $p^3 + q^3 = 2$, donc $r = 1$ (qui donne la solution triviale $(1, 1, 1)$) ou $r = 2$ qui donne $(x, y, z) = (1, 2, 4)$. Pour $x = 2$ on a $p = 2$ et $q = 1$ et r divise 9 donc $r = 1, 3, 9$. On obtient les solutions $(2, 12, 9)$ et $(2, 36, 81)$. Pour $x = 3$ on a $p = 3$, $q = 1$, $r = 2$ ou $r = 14$ et les deux solutions $(3, 18, 4)$ et $(3, 126, 196)$.

2) Si x est un nombre premier, on a $x = p$, $q = 1$ et r est un diviseur de $p^3 + 1$ qui doit être tel que p divise $r^3 + 1$. Cette dernière condition signifie qu'on a $r \equiv -1 \pmod{p}$, sauf si p est congru à 1 modulo 3 auquel cas il y a trois racines de -1 dans $\mathbf{Z}/p\mathbf{Z}$ et r peut être congru à l'une quelconque d'entre elles. C'est le cas des exemples suivants : $p = 61$, $r = 14$ ou encore $p = 619$, $r = 2110$ (congru à 253 modulo 619 qui est une racine de -1).

3.3 Des questions sur l'équation en p, q, r

La question principale est de savoir s'il existe une infinité de solutions de l'équation $p^3 + q^3 + r^3 = spqr$. Cette question a deux sens possibles : y a-t-il une infinité de solutions pour s fixé ? Là, la réponse est non, voir 3.5 ci-dessous. Ou bien : y a-t-il une infinité de s tels que l'équation admette une solution ?

Cette question là est plus raisonnable et on peut même se demander si, pour certains p fixés, il n'y a pas une infinité de solutions. Le cas le plus simple est $p = 1$ et la conjecture est alors la suivante :

3.4 Conjecture. *Il existe une infinité de couples q, r tels que q divise $r^3 + 1$ et r divise $q^3 + 1$.*

Cette conjecture a été prouvée en 1977 par Mohanty, voir 4.1.

3.4 Détermination de S : apparition d'une courbe elliptique

Vu le théorème 2.2, dire qu'un entier s est dans S (donc de la forme $\frac{x}{y} + \frac{y}{z} + \frac{z}{x}$ avec x, y, z entiers) signifie encore qu'il est de la forme $s =$

$\dfrac{p^3+q^3+r^3}{pqr}$ avec p,q,r entiers. La question revient donc à la recherche des solutions non nulles [3] de l'équation diophantienne $p^3+q^3+r^3-spqr=0$.

Cette équation est celle d'une courbe Γ_s du plan projectif, avec les coordonnées homogènes p,q,r, de degré 3. On vérifie qu'elle est lisse et c'est donc une courbe elliptique. On entre ici dans l'un des paradis des mathématiciens, pour lequel on renvoie, par exemple, au livre de Silverman [8].

La théorie permet en particulier de prouver le résultat suivant :

3.5 Théorème. *Soit s un entier positif. Il existe un nombre fini (peut-être nul) de triplets p,q,r d'entiers positifs premiers entre eux vérifiant $p^3+q^3+r^3-spqr=0$, donc aussi d'entiers x,y,z premiers entre eux dans leur ensemble et vérifiant $s=\dfrac{x}{y}+\dfrac{y}{z}+\dfrac{z}{x}$.*

Démonstration. Un théorème non trivial de Siegel assure que le nombre de points entiers d'une courbe elliptique est fini, voir [8] p. 276.

On sait qu'une courbe elliptique est munie d'une structure de groupe abélien de type fini, avec une partie libre $\mathbf{Z}^r$ (r est le rang de la courbe) et un sous-groupe de torsion, fini et relativement facile à calculer. Comme on l'a vu, la courbe a toujours trois points entiers : $(1,-1,0)$, $(-1,0,1)$ et $(0,1,-1)$ qui forment un sous-groupe $\mathbf{Z}/3\mathbf{Z}$ de son sous-groupe de torsion. Le problème essentiel est de déterminer si cette courbe admet des points entiers autres que ceux là. Pour réaliser cela, il faut mettre son équation sous forme canonique. On effectue d'abord le changement de variables $x=p+q$, $y=p-q$, $z=r$, puis on pose $t=3x+sz$, puis $T=\dfrac{s^3t}{108-4s^3}$ et on obtient l'équation canonique de la courbe :

$$y^2T=x^3+\frac{s^3-108}{s^3}x^2T-\frac{144(s^3-27)}{s^6}xT^2-\frac{64(s^3-27)^2}{s^9}T^3,$$

par exemple, pour $s=4$:

$$y^2T=x^3-\frac{11}{16}x^2T-\frac{333}{256}xT^2-\frac{1369}{4096}T^3$$

avec sa variante affine obtenue en faisant $T=1$:

$$y^2=x^3-\frac{11}{16}x^2-\frac{333}{256}x-\frac{1369}{4096}.$$

Avec cette écriture on peut confier la courbe à un logiciel spécialisé (par exemple *Pari*) qui en calcule le groupe de torsion et le rang analytique [4]. On

3. Il y a toujours les solutions banales : $(1,-1,0)$, $(-1,0,1)$ et $(0,1,-1)$.

4. Qui, sauf en rang 0 ou 1, n'est égal au rang que *via* la conjecture de Birch et Swinnerton-Dyer (l'un des problèmes du Millenium).

a ainsi confirmation que, pour $s = 4$, la courbe elliptique est de rang 0 donc n'a pas de points entiers non triviaux, de sorte que 4 n'est pas dans S. C'est aussi le cas pour $s = 7, 8, 11, 12$.

Le cas $s = 5$ est spécial car la courbe Γ_5 est de rang 0 bien que l'équation admette les solutions non triviales $(1, 1, 2)$ et ses permutés circulaires. Dans ce cas, les six points $(1, -1, 0)$, $(-1, 0, 1)$, $(0, 1, -1)$, $(1, 1, 2)$, $(1, 2, 1)$ et $(2, 1, 1)$ constituent le groupe de torsion de Γ_5, isomorphe à $\mathbf{Z}/6\mathbf{Z}$.

4 L'équation diophantienne $x^3 + y^3 + z^3 = sxyz$ dans la littérature

Après avoir réfléchi à la question posée et montré qu'elle se ramenait à la recherche des points entiers sur certaines courbes elliptiques simples, je n'ai pas douté que ces équations avaient déjà été étudiées par des mathématiciens. De fait, on trouve sur Internet de très nombreux travaux qui évoquent ces questions. Le plus ancien est sans doute celui de Sylvester (1856) qui montre que l'équation n'a pas de solution non triviale pour $s = -6$. Ensuite, Mordell traite les cas $s = -1$ et $s = 5$, voir [6]. On renvoie aux articles cités ci-dessous et à leurs références pour de plus amples précisions. Je donne juste deux exemples de résultats, en sens inverse l'un de l'autre.

Rappelons qu'on appelle S l'ensemble des entiers s qui s'écrivent $s = \dfrac{x^3 + y^3 + z^3}{xyz}$ avec x, y, z entiers > 0.

4.1 Infinitude des solutions : un résultat de Mohanty

Je m'inspire ici de l'article [4] qui date de 1977. La preuve du résultat ci-dessous est très simple et je la donne intégralement.

4.1 Théorème. *L'ensemble S est infini.*

Démonstration. En fait, Mohanty montre qu'il y a une infinité de s tels que l'équation $x^3 + y^3 + 1 = sxy$ admette une solution entière avec $x, y > 0$. Cela résulte du lemme suivant :

4.2 Lemme. *Soit $x \leq y$ des entiers positifs tels que x divise $y^3 + 1$ et y divise $x^3 + 1$ (propriété $(*)$). On pose $X = \dfrac{y^3 + 1}{x}$ et $Y = \dfrac{X^3 + 1}{y}$. Alors X, Y sont des entiers qui vérifient $(*)$ et $X \leq Y$, $x < X$, $y < X$.*

Il y a une infinité de couples (x, y) distincts qui vérifient $(*)$.

Démonstration. 0) On note que les conditions imposent que x et y sont premiers entre eux.

1) Il est clair que X est entier et que x, y sont plus petits que X. Montrons que Y est entier, c'est-à-dire que y divise X^3+1. On a $xX = y^3+1$, donc $x^3(X^3+1) = y^9+3y^6+3y^3+1+x^3$. On voit que y divise le second membre, donc X^3+1 puisqu'on a $x \wedge y = 1$.

2) Il est clair que Y divise X^3+1.

3) Montrons que X divise Y^3+1. On a $y^3(Y^3+1) = X^9+3X^6+3X^3+1+y^3$ et comme X divise $1+y^3$ (donc est premier avec y), on a le résultat.

4) Il reste à montrer $X \leq Y$, c'est-à-dire $yX \leq X^3+1$, mais comme on a $y < X$, c'est clair.

L'existence d'une infinité de couples distincts vérifiant $(*)$ est alors claire par récurrence.

Revenons au théorème. Si l'on a (x, y) vérifiant $(*)$, comme ils sont premiers entre eux, on voit que xy divise x^3+y^3+1 et on a une solution de l'équation. Comme on a $s(x, y, 1) = \dfrac{x^3+y^3+1}{xy} > y$, on voit qu'il y a une infinité de s pour lesquels l'équation admet une solution.

4.3 *Exemple.* Partant de la solution $(1, 1, 1)$ de l'équation avec $s = 1$ on obtient successivement les solutions $(2, 9)$ ($s = 41$) puis $(365, 503014)$ ($s = 79979617217$), etc. On voit que la taille des solutions croît très vite !

4.2 Absence de solutions : les résultats de Dofs et Garaev

Le premier résultat obtenu du côté négatif est le suivant (voir [1] ou [2]) :

4.4 Théorème. *(Dofs, 1973) Soit s un entier. On suppose que s^2+3s+9 est premier, que $s-3$ n'a aucun facteur premier congru à 1 modulo 3 et que s est distinct de -1 et de 5. Alors s n'est pas dans S.*

4.5 *Exemple.* Le théorème de Dofs montre que l'équation n'a pas de solutions pour les valeurs suivantes de s (≤ 50) : 4, 7, 8, 11, 23, 25, 28, 32, 37, 43, 49. On conjecture, comme souvent dans ce genre de questions, qu'il y a une infinité de s vérifiant ces propriétés, mais on n'en a pas de démonstration.

Le résultat suivant, voir [3], montre que les conjectures 3.1 sont vraies (et il assure donc, sans discussion cette fois, qu'il y a une infinité d'entiers en dehors de S) :

4.6 Théorème. *(Garaev, 1997) Soit s un entier > 0. On suppose qu'on a $s \equiv 0 \pmod 4$ ou $s \equiv -1 \pmod 8$, ou $s = 2^{2m+1}(2k-1)+3$ avec $m, k > 0$. Alors s n'est pas dans S.*

4.7 *Exemple.* Voici des exemples du troisième type : 11, 27, 35, 43, etc.

La preuve de 4.4 est dans [1], mais elle est très complexe et je n'ai pas eu le courage de la lire. Quant à celle de 4.6, elle est dans l'article [3] que je n'ai pas réussi à me procurer.

4.3 Bilan

On voit que la question posée, pour anodine qu'elle puisse sembler, est loin d'être triviale, d'ailleurs, en 1970, Sierpinski ([7] p. 80) note qu'on ne sait pas si l'on peut écrire le nombre 4 sous la forme $\frac{x}{y}+\frac{y}{z}+\frac{z}{x}$ (on sait maintenant qu'on ne peut pas). En particulier, pour ce que je peux en dire après un examen superficiel de la littérature, on ne sait pas répondre complètement à la question subsidiaire : *quels sont les entiers $s(x,y,z)$ qui vérifient la condition*, on sait simplement qu'il y en a une infinité qui la vérifient et une infinité qui ne la vérifient pas, ce qui n'est déjà pas si mal !

Références

[1] E. Dofs, *On some classes of homogeneous ternary cubic Diophantine equations*, Ark. Mat. 13 (1975), pp. 29–72.

[2] E. Dofs, *Solutions of $x^3+y^3+z^3=nxyz$*, Acta arithmetica, LXXIII.3 (1995).

[3] M. Z. Garaev, *Third degree diophantine equations*, Proc. Steklov Inst. Math. 218 (1997), pp. 94–103.

[4] S. P. Mohanty, *A system of cubic diophantine equations*, J. Number Theory 9 (1977), 153–159.

[5] L.J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.

[6] L. J. Mordell, *The Diophantine Equation $x^3+y^3+z^3+kxyz=0$*, in : Colloque sur la théorie des nombres, Bruxelles, 1955, pp. 67–76.

[7] W. Sierpinski, *250 Problems in Elementary Number Theory*, American Elsevier Publ. Com, New York (1970).

[8] J.H. Silverman, *The Arithmetic of Elliptic Curves*, 2ème édition, Springer, 2009.