BULLETIN DE LA S. M. F.

E. LUCAS

Théorèmes généraux sur l'impossibilité des équations cubiques indéterminées

Bulletin de la S. M. F., tome 8 (1880), p. 173-182

<http://www.numdam.org/item?id=BSMF_1880__8__173_0>

Théorèmes généraux sur l'impossibilité des équations cubiques indéterminées; par M. Édouard Lucas.

(Séance du 16 avril 1880.)

Les trois théorèmes suivants ont été énoncés par M. Sylvester. Nous en donnons des démonstrations élémentaires, et nous ajoutons quelques autres développements sur le même sujet.

Théorème I. — *Si p, p_1 désignent des nombres premiers de la forme $18n+5$, et q, q_1 des nombres premiers de la forme $18n+11$, il est impossible de décomposer en deux cubes entiers ou fractionnaires, positifs ou négatifs, aucun des nombres*

$$p,\ q,\ p^2,\ q^2,\ pq,\ p^2q^2,\ pp_1^2,\ qq_1^2.$$

Considérons l'équation

$$x^3+y^3=Az^3; \tag{1}$$

on peut supposer x, y, z premiers entre eux, deux à deux, le nombre A ne contenant aucun facteur cubique, et x, y, z différents de zéro. Si l'on pose

$$M=x+y,\quad N=x^2-xy+y^2,$$

le binôme x^3+y^3 égale le produit MN, dans lequel N est impair. De plus, il résulte de la formule

$$4N=(x+y)^2+3(x-y)^2$$

que le plus grand commun diviseur de M et de N est 3 ou 1, suivant que x^3+y^3 est ou n'est pas divisible par 3; de plus, N ne peut être divisible par une puissance de 3 autre que la première, puisque x et y seraient divisibles par 3. Ce théorème est un cas particulier d'un théorème plus général, démontré par Malebranche, sur les deux facteurs de x^p+y^p, ainsi que l'a fait remarquer récemment M. C. Henry (1).

---

(1) *Recherches sur les manuscrits de Pierre de Fermat, suivies de fragments inédits de Bachet et de Malebranche*, Rome, 1880, in-4°, p. 87-92. Le manuscrit dans lequel se

De plus, les diviseurs de N sont, en exceptant le nombre 3, de la forme quadratique $f^2 + 3g^2$ et de la forme linéaire correspondante $6h + 1$.

Enfin, on sait que le reste de la division d'un cube par le nombre 9 est toujours égal à 0 ou à ± 1.

Cela posé, nous considérerons quatre cas :

1° *Le nombre z est impair et divisible par* 3.

Si A prend l'une des valeurs indiquées dans l'énoncé, aucun des nombres p ou q ne divise N; on doit donc poser

$$x + y = 3^2 \mathrm{A} a^3, \quad \mathrm{N} = 3b^3, \quad z = 3ab,$$

et par suite

$$4b^3 = (x - y)^2 + 3\left(\frac{x+y}{3}\right)^2.$$

Mais, puisque b divise N, on a

$$b = f^2 + 3g^2, \quad b^3 = \mathrm{F}^2 + 3\mathrm{G}^2, \quad 4b^3 = (\mathrm{F} - 3\mathrm{G})^2 + 3(\mathrm{F} + \mathrm{G})^2,$$

et, en même temps

$$\mathrm{F} = f(f^2 - 9g^2), \quad \mathrm{G} = 3g(f^2 - g^2),$$

ainsi qu'on le voit, en faisant le cube de $f + g\sqrt{-3}$. En identifiant les deux valeurs de $4b^3$, on trouve

$$\mathrm{F} + \mathrm{G} = \frac{x+y}{3} = 3\mathrm{A}a^3,$$

ou bien

$$f(f^2 - 9g^2) \pm 3g(f^2 - g^2) = 3\mathrm{A}a^3.$$

Donc f serait divisible par 3, et par suite b, et aussi x et y, que nous avons supposés premiers entre eux. Donc z ne peut être impair et divisible par 3.

2° *Le nombre z est pair et divisible par* 3.

On doit poser

$$x + y = 3^2 . 2^3 \mathrm{A} a^3, \quad \mathrm{N} = 3b^3, \quad z = 6ab,$$

---

trouve copiée la démonstration en question est expressément attribué, par un Catalogue inédit des manuscrits de l'Oratoire, à Malebranche, qui d'ailleurs a laissé de nombreux autographes sur les Sections coniques, le Calcul différentiel et intégral, la Mécanique, l'Optique, etc.

et, par suite

$$\left(\frac{x-y}{2}\right)^2 + 3\left(\frac{x+y}{6}\right)^2 = b^3 = F^2 + 3G^2;$$

on en tire

$$G = \frac{x+y}{6} \quad \text{ou} \quad g(f^2 - g^2) = 4Aa^3.$$

D'ailleurs, $f^2 + 3g^2$ et $f^2 - g^2$ sont *impairs;* donc g est pair, et, en désignant par α, β, γ trois nombres premiers entre eux, on doit poser, avec $a = \alpha\beta\gamma$,

$$g = 4A\alpha^3, \quad f+g = \beta^3, \quad f-g = \gamma^3$$

ou

$$g = 4\alpha^3, \quad f+g = A\beta^3, \quad f-g = \gamma^3.$$

Il semble qu'il peut y avoir d'autre décomposition lorsque A contient plusieurs facteurs; mais il est facile de voir que ces décompositions conduiraient à la congruence impossible

$$\alpha^3 \pm 2\beta^3 \pm 4\gamma^3 \equiv 0 \pmod 9.$$

Quant aux deux décompositions précédentes, elles donnent

$$\beta^3 - \gamma^3 = A(2\alpha)^3, \quad \text{ou} \quad \gamma^3 + (2\alpha)^3 = A\beta^3.$$

On ramène donc l'équation proposée, dans laquelle l'inconnue z contient le facteur 3^λ, à une autre semblable dans laquelle l'inconnue z ne contient plus que le facteur $3^{\lambda-1}$, et ainsi de suite, de sorte que l'on peut supposer que z n'est pas divisible par 3.

3° *Le nombre z est impair et non divisible par* 3.

On doit poser

$$x+y = Aa^3, \quad (x+y)^2 + 3(x-y)^2 = 4b^3,$$

et par suite

$$F \pm 3G = Aa^3,$$

équation impossible suivant le module 9, puisque f n'est pas divisible par 3.

4° *Le nombre z est pair et non divisible par* 3.

On doit poser

$$x+y = 2^3 Aa^3, \quad \left(\frac{x+y}{2}\right)^2 + 3\left(\frac{x-y}{2}\right)^2 = b^3,$$

et, par l'identification,

$$f(f^2 - 9g^2) = 4\,\mathrm{A}a^3;$$

cette équation conduit aux décompositions suivantes, en laissant de côté celles qui donnent des congruences impossibles suivant le module 9 :

$$f = 4\alpha^3, \quad f + 3g = \mathrm{A}\beta^3, \quad f - 3g = \gamma^3$$

ou

$$f = 4\,\mathrm{A}\alpha^3, \quad f + 3g = \beta^3, \quad f - 3g = \gamma^3.$$

On en déduit l'équation

$$\mathrm{A}\beta^3 + \gamma^3 = (2\alpha)^3,$$

reconnue impossible, puisque z est impair et non divisible par 3, ou l'équation en moindres nombres

$$\beta^3 + \gamma^3 = \mathrm{A}(2\alpha)^3.$$

Donc l'équation proposée est impossible.

THÉORÈME II. — *Si p et q désignent des nombres premiers respectivement des formes $18n + 5$ et $18n + 11$, il est impossible de décomposer en deux cubes, soit entiers, soit fractionnaires, aucun des nombres suivants :*

$$2p, \quad 2q^2, \quad 4p^2, \quad 4q.$$

Considérons l'équation

$$x^3 + y^3 = 2^n \mathrm{A} z^3,$$

dans laquelle, A étant impair, le coefficient 2^nA représente l'un des quatre nombres $2p$, $2q^2$, $4p^2$, $4q$. On doit supposer x, y, z entiers et premiers entre eux, x et y étant impairs; il y a lieu d'étudier deux cas différents, suivant que z est ou n'est pas divisible par 3.

1° *Le nombre z n'est pas divisible par* 3.

On arrive, comme ci-dessus, à l'équation

$$f(f^2 - 9g^2) = 2^{n-1}\mathrm{A}a^3.$$

Mais $f^2 - 9g^2$ est impair avec b; on a donc

$$f = 2^{n-1}\mathrm{A}\alpha^3, \quad f + 3g = \beta^3, \quad f - 3g = \gamma^3$$

ou bien

$$f = 2^{n-1}\alpha^3, \quad f + 3g = A\beta^3, \quad f - 3g = \gamma^3.$$

Ces deux décompositions conduisent aux deux équations

$$\beta^3 + \gamma^3 = 2^n A\alpha^3 \quad \text{ou} \quad A\beta^3 + \gamma^3 = 2^n\alpha^3;$$

celles-ci sont impossibles suivant le module 9 ; pour la première, les indéterminées α, β, γ ne sont pas divisibles par 3.

2° *Le nombre z est divisible par* 3.

En posant $z = 3ab$, on arrive, comme ci-dessus, à l'équation

$$g(f^2 - g^2) = 2^{n-1} A a^3,$$

et, puisque $f^2 - g^2$ est impair, à l'une des décompositions

$$g = 2^{n-1} A\alpha^3, \quad f + g = \beta^3, \quad f - g = \gamma^3,$$

ou bien

$$g = 2^{n-1}\alpha^3, \quad f + g = A\beta^3, \quad f - g = \gamma^3.$$

La seconde décomposition conduit à une équation déjà reconnue impossible; la première conduit à l'équation

$$\beta^3 - \gamma^3 = 2^n A\alpha^3,$$

de même forme que la proposée, mais contenant un facteur 3 en moins. On conclura, comme précédemment, que l'équation proposée est impossible à résoudre en nombres entiers.

Théorème III. — *Si p et q désignent des nombres premiers des formes* $18n + 5$ *et* $18n + 11$, *il est impossible de décomposer en deux cubes soit entiers, soit fractionnaires, l'un des nombres suivants :*

$$9p, \ 9q, \ 9p^2, \ 9q^2.$$

Nous considérerons deux cas suivant que z est impair ou pair dans l'équation (1).

1° *Le nombre z est impair.*

On a, dans ce cas,

$$x + y = 3A a^3, \quad (x + y)^2 + 3(x - y)^2 = 12 b^3,$$

et par suite

$$(x-y)^2+3\left(\frac{x+y}{3}\right)^2=4b^3=(\mathrm{F}-3\mathrm{G})^2+3(\mathrm{F}+\mathrm{G})^2;$$

il résulte de l'identification

$$\mathrm{F}+\mathrm{G}=\mathrm{A}a^3,$$

ou bien

$$f(f^2-9g^2)+3g(f^2-g^2)=\mathrm{A}a^3.$$

Cette équation est impossible suivant le module q, puisque le produit $g(f^2-g^2)$ est toujours divisible par 3.

2° *Le nombre z est pair.*

On doit poser

$$x+y=3.2^3\mathrm{A}a^3,\quad \left(\frac{x-y}{2}\right)^2+3\left(\frac{x+y}{6}\right)^2=b^3,\quad z=6ab,$$

par suite

$$\mathrm{G}=\frac{x+y}{6},\quad \text{ou}\quad 4\mathrm{A}a^3=3g(f^2-g^2).$$

On en déduit, en laissant de côté les congruences impossibles suivant le module 9, les décompositions

$$g=4.9\mathrm{A}\alpha^3,\quad f+g=\beta^3,\quad f-g=\gamma^3,$$

et

$$g=4\mathrm{A}\alpha^3,\quad f+g=9\beta^3,\quad f-g=\gamma^3.$$

La première décomposition conduit à la même équation en moindres nombres; la seconde donne

$$9\beta^3-\gamma^3=\mathrm{A}(2\alpha)^3,$$

impossible suivant le module 9. C. Q. F. D.

M. Sylvester a indiqué de plus quatre autres formes (*Comptes rendus des séances de l'Académie des Sciences*, 16 février 1880),

$$9pq,\ 9p^2q^2,\ 9pp_1^2,\ 9qq_1^2,$$

pour lesquelles l'équation (1) serait impossible. Cet énoncé est trop général. Ainsi, en particulier, pour $p=5$, $q=11$, on a

$$9.5.11=\left(\frac{342361}{10803}\right)^3-\left(\frac{57241}{10803}\right)^3.$$

Cependant on peut modifier l'énoncé précédent, en tenant compte de la théorie des résidus cubiques; mais il semble que l'on ne peut obtenir d'énoncé général que lorsque l'on donne à l'un des nombres p ou q une valeur particulière. On peut alors déterminer, par les lois de réciprocité étendues aux résidus cubiques, des valeurs de q en nombre indéfini, en supposant donnée la valeur de p, ou inversement.

Nous ajouterons les deux théorèmes suivants :

THÉORÈME IV. — *Pour que l'équation*

$$X^3 + Y^3 = AZ^3$$

soit vérifiée par des valeurs entières de X, Y, Z, A, *il faut et il suffit que* A *appartienne à la forme*

$$xy(x+y),$$

préalablement débarrassée des facteurs cubiques qu'elle peut contenir.

En effet, on a l'identité

$$(x^3 - y^3 + 6x^2y + 3xy^2)^3 + (y^3 - x^3 + 6y^2x + 3yx^2)^3 = xy(x+y)3^3(x^2+xy+y^2)^3,$$

et l'on résout l'équation proposée par les valeurs

$$\begin{aligned} X &= x^3 - y^3 + 6x^2y + 3xy^2, \\ Y &= y^3 - x^3 + 6y^2x + 3yx^2, \\ Z &= 3(x^2+xy+y^2), \\ A &= xy(x+y). \end{aligned}$$

Réciproquement, si l'équation est vérifiée pour les valeurs x_0, y_0, z_0 des variables, et si l'on pose $x = x_0^3$, $y = y_0^3$, on a

$$xy(x+y) = A(x_0y_0z_0)^3.$$

C'est ce qu'il fallait démontrer. Il résulte encore de l'identité précédente que toute solution de l'équation proposée conduit à une série indéfinie d'autres solutions, en supposant A constant; il faut excepter le cas de $x = \pm y$.

Ainsi, pour $x = 1, y = 2$, on a la solution

$$17^3 + 37^3 = 6.21^3,$$

qui donne ensuite une série indéfinie d'autres solutions de l'équation

$$x^3 + y^3 = 6z^3,$$

bien que Legendre ait affirmé son irrésolubilité. De même, pour $x = 9, y = 55$, on retrouve l'exemple donné plus haut.

THÉORÈME V. — *Si x, y, z vérifient l'équation*

$$x^3 - 3xy^2 + y^3 = 3Az^3,$$

on peut décomposer le nombre A *en deux cubes, ou résoudre l'équation*

$$X^3 + Y^3 = AZ^3$$

par les formules

$$X = 2x^3 - 3x^2y - 3xy^2 + 2y^3,$$
$$Y = x^3 + 3x^2y - 6xy^2 + y^3,$$
$$Z = 3z(x^2 - xy + y^2).$$

Il suffit de vérifier l'identité correspondante; les valeurs de A sont telles, que les diviseurs sont de la forme $18n \pm 1$, ainsi que cela résulte de la théorie des fonctions cyclotomiques. M. Sylvester arrive au même résultat par des formules du neuvième degré, tandis que les nôtres ne sont que du troisième.

THÉORÈME VI. — *Un nombre positif quelconque entier ou fractionnaire est, d'une infinité de manières, le produit ou le quotient de deux nombres formés de la somme de deux cubes positifs.*

Euler a démontré qu'un nombre positif quelconque, entier ou fractionnaire, est égal à la somme de quatre cubes positifs, entiers ou fractionnaires. On trouve la formule correspondante dans une Note qui termine les *Exercices d'Analyse numérique* de Lebesgue. Nous ferons d'abord observer que Lebesgue ne paraît pas avoir deviné la méthode qui a dû servir à Euler pour obtenir cette formule. En effet, il nous paraît évident que celle-ci provient des recherches entreprises par Euler pour obtenir la décomposition

d'un nombre A en deux cubes. L'identité d'Euler est la suivante,

$$n=\left(\frac{n}{6m^2}\right)^3[(2-a)^3+a^3(b-1)^3+b^3(c-1)^3+c^3],$$

dans laquelle on suppose m tel que l'on ait

$$\frac{n}{12}<m^3<\frac{n}{6},$$

et, de plus,

$$a=1+\frac{6m^3}{n},\quad b=\frac{2a^3-1}{a^3+1},\quad c=\frac{2b^3-1}{b^3+1}.$$

Il est fort probable que cette identité provient de l'Arithmétique, et non de l'Algèbre, contrairement à la supposition de Lebesgue.

Le théorème proposé revient à dire que l'on peut résoudre en nombres rationnels et *positifs,* et d'une infinité de manières, les équations

$$\text{(1)}\qquad N=\frac{x^3+y^3}{z^3+u^3},$$

et

$$\text{(2)}\qquad N=(x^3+y^3)(z^3+u^3).$$

Pour l'équation (1), on pose $N=2^\lambda 3^\mu\frac{A}{B}$; on choisit $\frac{a}{b}$ par les conditions d'inégalité

$$\frac{B}{2^\lambda 3^{\mu-2}A}>\frac{a^3}{b^3}>\frac{B}{2^\lambda 3^{\mu-1}A},$$

et l'on a

$$x=\frac{Bb^3}{a},\qquad y=\frac{2^\lambda 3^{\mu-1}Aa^3-Bb^3}{a},$$

$$u=\frac{2^\lambda 3^{\mu-2}Aa^3}{b},\quad z=\frac{Bb^3-2^\lambda 3^{\mu-2}Aa^3}{b}.$$

Pour l'équation (2), nous observerons que l'on a les deux identités

$$(6LM+L^2-3M^2)^3+(6LM-L^2+3M^2)^3=2^2\,3^2\,LM(L^2+3M^2)^2,$$

$$(L+M)^3+(L-M)^3=2L(L^2+3M^2).$$

Donc, en multipliant membre à membre, et divisant les deux membres de l'égalité obtenue par $(L^2+3M^2)^3$, on aura décom-

posé $2^3 3^2 L^2 M$ en un produit de deux facteurs égaux à une somme de deux cubes; en supposant, de plus,

$$L = B b^3, \quad M = 2^{\lambda-3} 3^{\mu-2} A a^3,$$

on décomposera ainsi en ce produit le nombre

$$N = 2^{\lambda} 3^{\mu} A B^2;$$

on détermine d'ailleurs $\frac{a^3}{b^3}$ de telle sorte que les cubes x, y, z, u soient tous positifs.