NOUVELLES ANNALES DE MATHÉMATIQUES

ÉDOUARD LUCAS

Sur l'analyse indéterminée du troisième degré et sur la question 802 (Sylvester)

Nouvelles annales de mathématiques 2e série, tome 17 (1878), p. 507-514

<http://www.numdam.org/item?id=NAM_1878_2_17__507_1>

SUR L'ANALYSE INDÉTERMINÉE DU TROISIÈME DEGRÉ ET SUR LA QUESTION 802 (*) (SYLVESTER);

PAR M. ÉDOUARD LUCAS.

I. Considérons l'équation du troisième degré

$$f(x, y, z) = 0$$

d'une courbe en coordonnées rectilignes et homogènes; soit m_1 un point dont les coordonnées (x_1, y_1, z_1) sont rationnelles, et qu'il est facile de rendre entières; on a ainsi une première solution en nombres entiers de l'équation proposée. On peut obtenir de nouvelles solutions, en nombres entiers, de l'équation, par l'un des trois procédés suivants :

1° Si l'on mène la tangente à la courbe en m_1, cette droite rencontre la courbe en un autre point m dont les coordonnées sont encore rationnelles; par conséquent, d'une première solution de l'équation (1) on déduit, en général, une nouvelle solution (x, y, z) de cette équation, par les formules

$$f(x, y, z) = 0, \quad x\frac{df}{dx_1} + y\frac{df}{dy_1} + z\frac{df}{dz_1} = 0.$$

Cependant, lorsque la tangente est parallèle à l'une des asymptotes, ou lorsque la tangente est menée par un

(*) *Nouvelles Annales*, 2e série, t. VI, p. 96.

point d'inflexion, on n'obtient pas de solutions nouvelles.

2° Si m_1 et m_2 désignent deux points dont les coordonnées (x_1, y_1, z_1) et (x_2, y_2, z_2) sont rationnelles, et par conséquent entières, on obtient, en général, une nouvelle solution, en prenant l'intersection de la sécante $m_1 m_2$ avec la courbe, c'est-à-dire par les équations

$$f(x, y, z) = 0, \quad \begin{vmatrix} x & y & z \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix} = 0,$$

en tenant compte des relations

$$f(x_1, y_1, z_1) = 0, \quad f(x_2, y_2, z_2) = 0.$$

3° Si l'on connaît cinq solutions de l'équation proposée, on obtient, en général, une sixième solution, en prenant le point d'intersection avec la courbe, de la conique passant par les cinq points qui correspondent aux solutions données; on peut d'ailleurs supposer plusieurs de ces points réunis en un seul, et en particulier tous les cinq réunis en un seul.

La méthode donnée par Fermat pour l'équation

$$(1) \qquad x^3 + y^3 = Az^3,$$

et par Lagrange, pour l'équation générale, revient au premier procédé. La méthode donnée par Cauchy pour l'équation

$$Ax^3 + By^3 + Cz^3 = 3Dxyz$$

revient au second (*).

II. Nous considérerons plus particulièrement, dans ce qui suit, l'équation (1). On doit supposer différents cas;

(*) Voir *Recherches sur les ouvrages de Léonard de Pise*, p. 49.

en effet, pour certaines valeurs de A, l'équation (1) est impossible, et ainsi, par exemple, pour

$$A = 1, \; 2, \; 3, \; 4, \; 5,$$

ainsi que pour d'autres valeurs générales, indiquées, pour la première fois, par M. Sylvester, dans la question 802.

Quant aux équations possibles, elles sont dites *monobasiques, bibasiques*, etc., suivant que l'on peut résoudre complétement l'équation proposée, par les formules qui résultent du premier procédé, en partant d'une, de deux, etc., solutions fondamentales. Il existe d'ailleurs des équations *monobasiques* et *bibasiques*, ainsi que nous le montrerons plus tard; cependant nous ajouterons que cette idée de classification et de résolution est due, je pense, à M. Sylvester, qui possède, depuis longtemps, un Mémoire inédit sur ce sujet intéressant.

III. Voici maintenant l'énoncé de la question 802 :

p et q désignant 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 :

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

Soit d'abord à résoudre l'équation indéterminée

$$(1) \qquad x^3 + y^3 = pz^3,$$

dans laquelle p désigne un nombre premier de la forme $18n+5$, en nombres entiers et premiers entre eux. Le cube d'un nombre entier divisé par 9 donne pour reste $0, +1$ ou -1; donc, pour que l'équation (1) soit possible, il faut que z^3 soit divisible par 9, et, par suite, $z = 3z_1$. Cela posé, nous considérerons deux hypothèses, suivant que z est impair ou pair.

1° *z impair*. Alors $x - y$ et $x + y$ sont impairs; on a

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2) = (x + y)\mathrm{M}$$

et

$$4\mathrm{M} = 3(x - y)^2 + (x + y)^2;$$

par conséquent M est divisible par 3, et non par une puissance supérieure; de plus, les diviseurs premiers de M appartiennent à la forme $6h + 1$; on doit donc poser, avec $z_1 = ab$,

$$x + y = 3^2 pa^3, \quad \mathrm{M} = 3\, b^3$$

et, par suite,

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

d'ailleurs b doit être de la forme $f^2 + 3\, g^2$, f et g étant premiers entre eux; on a ainsi

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

et, en identifiant d'après (2) et (3),

$$\mathrm{F} + \mathrm{G} = \frac{x + y}{3} = 3pa^3.$$

Mais le développement du cube de $f + g\sqrt{-3}$ donne

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

par suite,

$$f(f^2 - 9\, g^2) + 3\, g\, (f^2 - g^2) = 3\, pa^3:$$

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

2° En supposant *z pair*, on aurait

$$\mathrm{M} = \left(\frac{x + y}{2}\right)^2 + 3\left(\frac{x - y}{2}\right)^2,$$

et, puisque x et y sont impairs, il en est de même de M; on doit donc poser, avec $z = 6ab$,

$$x + y = 3^2.2^3.pa^3, \quad M = 3b^3,$$

et, par suite,

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

Soient encore

$$b = f^2 + 3g^2, \quad b^3 = F^2 + 3G^2,$$

on en déduira

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

d'ailleurs $f^2 + 3g^2$ et $f^2 + 3g^2 - 4g^2 = f^2 - g^2$ sont impairs : donc g est pair, et l'on doit poser, avec $a = \alpha\beta\gamma$,

$$\left\{\begin{aligned} g &= 4p\alpha^3, \\ f + g &= \beta^3, \\ f - g &= \gamma^3, \end{aligned}\right. \quad \text{ou} \quad \left\{\begin{aligned} g &= 4\alpha^3, \\ f + g &= p\beta^3, \\ f - g &= \gamma^3. \end{aligned}\right.$$

On déduit de ces deux décompositions

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

ces deux équations sont semblables à l'équation (1); on ramène donc l'équation proposée, dans laquelle l'une des inconnues contient le facteur 3^λ, à une autre semblable, dans laquelle l'une des inconnues ne contient plus que le facteur $3^{\lambda-1}$; en continuant de même, on ramènera l'équation proposée à une autre de même forme, dans laquelle aucune des inconnues ne sera divisible par 3. Donc l'équation proposée est impossible.

La démonstration précédente s'applique encore, en remplaçant le nombre premier $p = 18n + 5$ par le carré du nombre premier $q = 18n + 11$.

IV. Considérons maintenant l'équation

$$x^3 + y^3 = 2^n A z^3, \tag{4}$$

dans laquelle, A étant impair, le coefficient $2^n A$ représente l'un des quatre nombres $2p$, $2q^2$, $4p^2$, $4q$. Nous supposerons deux cas, suivant que z ne sera pas ou sera divisible par 3; d'ailleurs, x et y sont impairs.

1° Lorsque z n'est pas divisible par 3, on arrive facilement à l'équation

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

$f^2 - 9g^2$ est impair, en même temps que $b = f^2 + 3g^2$, et l'on a l'une ou l'autre des deux décompositions

$$\left\{\begin{aligned} f &= 2^{n-1} A \alpha^3, \\ f + 3g &= \beta^3, \\ f - 3g &= \gamma^3; \end{aligned}\right. \quad \text{ou} \quad \left\{\begin{aligned} f &= 2^{n-1} \alpha^3, \\ f + 3g &= A\beta^3, \\ f - 3g &= \gamma^3. \end{aligned}\right.$$

Ces deux décompositions conduisent aux deux équations

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

impossibles suivant le module 9, puisque, pour la première, les indéterminées α, β et γ ne sont pas divisibles par 3.

2° Lorsque z est divisible par 3, on arrive, en posant $z = 3ab$, 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

$$\left\{\begin{aligned} g &= 2^{n-1} A \alpha^3, \\ f + g &= \beta^3, \\ f - g &= \gamma^3, \end{aligned}\right. \quad \text{ou} \quad \left\{\begin{aligned} g &= 2^{n-1} \alpha^3, \\ f + g &= A\beta^3, \\ f - g &= \gamma^3; \end{aligned}\right.$$

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

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

Celle-ci est de même forme que l'équation (4) ; mais l'indéterminée du second membre contiendra un facteur 3 en moins. On conclura, comme pour l'équation (1), que l'équation (4) est impossible à résoudre en nombre entiers.

Remarque I. — En rapprochant les résultats de M. Sylvester avec ceux d'une Note précédente (*), on en déduit le théorème suivant :

L'équation

$$xy(x+y) = A z^3$$

est impossible, en nombres rationnels, en exceptant les valeurs égales ou nulles des indéterminées, dans les cas suivants :

$$A = 1,\ 2,\ 3,\ 4,\ 18,\ 36,\ p,\ 2p,\ 4p^2,\ q^2,\ 2q^2,\ 4q,$$

p désignant un nombre premier de la forme $18n+5$, *et q un nombre premier de la forme* $18n+11$.

En faisant $y=1$, on obtient plusieurs théorèmes concernant les nombres triangulaires, et le produit de deux nombres consécutifs ; en faisant $y = x+1$, on en déduira ceux qui concernent les nombres

$$x(x+1)(2x+1), \quad \text{et} \quad 2x(2x+1)(2x+2).$$

Remarque II. — De même, en rapprochant les résultats obtenus par Fermat et par M. Genocchi, sur les

(*) *Nouvelles Annales*, 2e série, t. XVII, p. 425.

nombres congruents (*), avec ceux d'une Note précédente (**), on en déduit le théorème suivant :

L'équation

$$xy(x+y)(x-y) = \mathrm{A}z^2$$

est impossible, en nombres rationnels, dans les cas suivants :

$$\mathrm{A} = 1, 2, \quad p, 2q,$$

p désignant un nombre premier de la forme $8n+3$, *et q un nombre premier de la forme* $8n+5$.

On observera que les résultats généraux, obtenus par MM. Genocchi et Sylvester, constituent des progrès importants, pour arriver à la solution de deux problèmes posés depuis près de *vingt siècles*.