NOUVELLES ANNALES DE MATHÉMATIQUES

ÉDOUARD LUCAS

Sur le système des équations indéterminées $x^2 - Ay^2 = u^2$, $x^2 + Ay^2 = v^2$

Nouvelles annales de mathématiques 2e série, tome 17 (1878), p. 446-453

<http://www.numdam.org/item?id=NAM_1878_2_17__446_1>

SUR LE SYSTÈME DES ÉQUATIONS INDÉTERMINÉES
$x^2 - Ay^2 = u^2,\ x^2 + Ay^2 = v^2$;

PAR M. ÉDOUARD LUCAS.

On a tout d'abord le théorème suivant :

Pour que le système indéterminé

$$x^2 - Ay^2 = u^2, \quad x^2 + Ay^2 = v^2 \tag{1}$$

soit vérifié par une série indéfinie de valeurs entières des inconnues x, y, u, v, il faut et il suffit que A *appartienne à la forme*

$$(2)\qquad A = \lambda_0\mu_0(\lambda_0 + \mu_0)(\lambda_0 - \mu_0),$$

que l'on peut supposer débarrassée de ses facteurs quadratiques.

En effet, en ajoutant membre à membre les deux équations du système (1), on a

$$\left(\frac{u+v}{2}\right)^2 + \left(\frac{u-v}{2}\right)^2 = x^2,$$

et l'on doit poser

$$\frac{u+v}{2} = \lambda_0^2 - \mu_0^2, \quad \frac{u-v}{2} = 2\lambda_0\mu_0, \quad x = \lambda_0^2 + \mu_0^2,$$

λ_0 et μ_0 désignant deux nombres quelconques, premiers entre eux, l'un pair et l'autre impair ; on en déduit la solution initiale

$$(3)\qquad \left\{\begin{aligned} x_0 &= \lambda_0^2 + \mu_0^2, \\ u_0 &= \lambda_0^2 - \mu_0^2 + 2\lambda_0\mu_0, \\ v_0 &= \lambda_0^2 - \mu_0^2 - 2\lambda_0\mu_0, \end{aligned}\right.$$

et, par suite,

$$A = \lambda_0\mu_0(\lambda_0 + \mu_0)(\lambda_0 - \mu_0), \quad y_0 = 2.$$

Ainsi le théorème est démontré ; on sait d'ailleurs que le nombre A est dit *congruent*, et représente l'aire d'un triangle rectangle, dont les côtés entiers ont pour longueurs

$$\lambda_0^2 - \mu_0^2, \quad 2\lambda_0\mu_0, \quad \lambda_0^2 + \mu_0^2\ (*).$$

Notre but est d'indiquer comment on peut parvenir à résoudre complétement le système proposé, pour les va-

(*) *Recherches sur les ouvrages de Léonard de Pise*, Ch. II.

leurs de A données par la formule (2). Nous observerons, à ce sujet, qu'il est nécessaire, pour traiter généralement la question, de connaître la décomposition de A en ses facteurs premiers. On sait, en effet, que Lagrange a ramené la résolution des équations quadratiques indéterminées à des équations de la forme

$$x^2 - y^2 = Az^2,$$

et que cette résolution est liée à la connaissance des facteurs premiers de A. Inversement, nous montrerons ultérieurement que la décomposition d'un nombre donné A, en ses facteurs premiers, se trouve notablement simplifiée par l'essai direct de la résolution de l'équation

$$x^2 - y^2 = A,$$

au moyen de la considération des résidus quadratiques. Nous ferons voir que, par cette méthode, imaginée par Aurifeuille, et que nous avons perfectionnée, il est possible d'arriver plus rapidement à la décomposition de nombres de seize et de dix-huit chiffres qu'à celle des nombres de huit et de dix chiffres, par l'application des anciennes méthodes.

Par conséquent, on ne doit voir dans la présente Note que l'indication de la marche à suivre, pour résoudre complétement, pour toutes les valeurs numériques de A, décomposé en ses facteurs premiers, le système des équations proposées. On tire de la seconde des équations (1)

$$(v + x)(v - x) = Ay^2;$$

donc, en désignant par α et β deux nombres entiers dont le produit égale A, et par e et f deux indéterminées, on aura

$$v + x = 2\alpha e^2, \quad v - x = 2\beta f^2, \quad y = 2ef,$$

et, par suite,

$$x = \alpha e^2 - \beta f^2, \quad v = \alpha e^2 + \beta f^2, \quad y = 2ef.$$

En portant ces valeurs dans la première des équations proposées, on arrive à la condition

$$(\alpha e^2 - 3\beta f^2)^2 - u^2 = 8\beta^2 f^4.$$

Désignons par β_1 et β_2 deux nombres positifs ou négatifs, dont le produit est égal à β, par g et h deux nouvelles indéterminées, nous tirerons de la condition précédente

$$(4) \qquad \left\{ \begin{aligned} \alpha e^2 - 3\beta f^2 + u &= \pm 2\beta_1^2 g^4, \\ \alpha e^2 - 3\beta f^2 - u &= \pm 4\beta_2^2 h^4, \\ f &= gh. \end{aligned} \right.$$

Premier cas. — Si l'on prend, en même temps, les signes supérieurs dans les équations (4), on en déduit, par addition, après avoir remplacé f par gh et β par $\beta_1\beta_2$,

$$(\beta_1 g^2 + \beta_2 h^2)(\beta_1 g^2 + 2\beta_2 h^2) = \alpha e^2;$$

désignons par α_1 et α_2 deux nombres entiers dont le produit égale α, et par p et q deux nouvelles indéterminées; nous poserons

$$\begin{aligned} \beta_1 g^2 + \beta_2 h^2 &= \alpha_1 p^2, \\ \beta_1 g^2 + 2\beta_2 h^2 &= \alpha_2 q^2, \\ e &= pq; \end{aligned}$$

et, par suite,

$$(5) \qquad \alpha_1 p^2 - \beta_2 h^2 = \beta_1 g^2, \quad \alpha_1 p^2 + \beta_2 h^2 = \alpha_2 q^2.$$

Ce système est vérifié pour des valeurs égales des indéterminées g, h, p, q, lorsque l'on suppose

$$\alpha_1 = \lambda_0, \quad \beta_2 = \mu_0, \quad \beta_1 = \lambda_0 - \mu_0, \quad \alpha_2 = \lambda_0 + \mu_0;$$

il est facile de déduire de ces valeurs la solution initiale

(3). En général, une solution quelconque du système (5) donnera une solution du système proposé, et, par suite, une série indéfinie, comme nous allons le montrer.

Si l'on fait, dans le système (5),

$$\alpha_1 = \beta_1 = \alpha_2 = 1, \quad \beta_2 = \lambda_0\mu_0(\lambda_0^2 - \mu_0^2),$$

le système (5) coïncide avec le système proposé ; par conséquent, d'une première solution (x, y, u, v) du système (1), on déduit une série indéfinie de solutions nouvelles (X, Y, U, V) par les formules

$$(6)\quad \begin{cases} X = u^2x^2 - \lambda_0\mu_0(\lambda_0^2 - \mu_0^2)v^2y^2, & Y = 2xyuv, \\ V = u^2x^2 + \lambda_0\mu_0(\lambda_0^2 - \mu_0^2)v^2y^2, & U = u^4 - 2x^4. \end{cases}$$

En désignant par $x_0, x_1, x_2, \ldots, x_n$ les valeurs successives de x, on voit que ces valeurs sont des polynômes en λ de degré $2, 8, 32, \ldots, 2^{2n+1}$.

Second cas. — Le système (4) donne de même, avec les signes inférieurs,

$$\begin{aligned} \beta_1 g^2 - \beta_2 h^2 &= \alpha_1 p^2, \\ 2\beta_2 h^2 - \beta_1 g^2 &= \alpha_2 q^2, \\ c &= pq, \end{aligned}$$

et, par suite,

$$\beta_2 h^2 - \alpha_1 p^2 = \alpha_2 q^2, \quad \beta_2 h^2 + \alpha_1 p^2 = \beta_1 g^2.$$

On arrive ainsi à un système analogue au système (5). Par conséquent, on décomposera A en un produit de quatre facteurs, de toutes les manières possibles, et l'on aura un certain nombre d'équations de la forme (5) ; plusieurs d'entre elles seront reconnues impossibles, par non-congruence ; d'autres seront possibles. Soit

$$Mp^2 - Nh^2 = Pg^2, \quad Mp^2 + Nh^2 = Qq^2,$$

un tel système admettant la solution (g_0, h_0, p_0, q_0) ; on posera

$$Mp_0^2 = \lambda, \quad Nh_0^2 = \mu, \quad Pg_0^2 = \lambda - \mu, \quad Qq_0^2 = \lambda + \mu,$$

et l'on aura

$$\lambda\mu(\lambda + \mu)(\lambda - \mu) = Az^2.$$

Il nous reste donc à considérer le système général

$$(7) \qquad \begin{cases} \lambda p^2 - \mu h^2 = \rho g^2, \\ \lambda p^2 + \mu h^2 = \sigma q^2, \end{cases}$$

dans lequel nous désignons, pour abréger, $\lambda - \mu$ par ρ et $\lambda + \mu$ par σ. On résout la première équation du système (7), mise sous la forme

$$p^2 - \left(\frac{\rho g + \mu h}{\rho + \mu}\right)^2 = \rho\mu\left(\frac{h - g}{\rho + \mu}\right)^2,$$

par les formules

$$\begin{aligned} p &= \mu_1 r^2 + \rho_1 s^2, \\ h &= \mu_1 r^2 - \rho_1 s^2 + 2\rho rs, \\ g &= \mu_1 r^2 - \rho_1 s^2 - 2\mu rs, \end{aligned}$$

dans lesquelles $\rho_1\mu_1 = \rho\mu$. En portant ces valeurs dans la seconde des équations (7), on obtient la condition

$$\lambda(\mu_1 r^2 + \rho_1 s^2)^2 + \mu(\mu_1 r^2 - \rho_1 s^2 + 2\rho rs)^2 = \sigma q^2,$$

ou bien

$$\sigma(\mu_1 r^2 + \rho_1 s^2)^2 + 4\rho\mu rs(\mu_1 r^2 - \rho_1 s^2) + 4\rho\mu r^2 s^2(\rho - \mu) = \sigma q^2,$$

ou, en posant $s = \sigma s'$,

$$(\mu_1 r^2 + 2\rho\mu rs' - \rho_1\sigma^2 s'^2)^2 + 8\lambda^2\mu\rho r^2 s'^2 = q^2.$$

On déduit de l'équation précédente

$$\begin{aligned} q \pm (\mu_1 r^2 + 2\rho\mu rs' - \rho_1\sigma^2 s'^2) &= 2\rho_2 u^2, \\ q \mp (\mu_1 r^2 + 2\rho\mu rs' - \rho_1\sigma^2 s'^2) &= 4\mu_2\lambda^2 t^2, \\ rs' &= ut, \end{aligned}$$

en désignant par ρ_2 et μ_2 deux nombres tels que

$$\rho_2\mu_2 = \rho\mu,$$

et par w et t deux nouvelles indéterminées; on en tire

$$(8) \qquad \mu_1 r^2 + 2\rho\mu r s' - \rho_1\sigma^2 s'^2 = \pm(\rho_2 w^2 - 2\mu_2\lambda^2 t^2).$$

Posons $w = mr$, $s' = mt$, il vient, en prenant le signe $+$,

$$m^2(\rho_2 r^2 + \rho_1\sigma^2 t^2) - 2\rho\mu rtm = \mu_1 r^2 + 2\mu_2\lambda^2 t^2;$$

pour que la valeur de m soit rationnelle, on doit faire

$$\rho_2\mu_1 r^4 + 3\lambda\mu\rho\sigma r^2 t^2 + 2\rho_1\mu_2\sigma^2\lambda^2 t^4 = \mathrm{H}^2,$$

et l'on a

$$m = \frac{\rho\mu rt \pm \mathrm{H}}{\rho_2 r^2 + \rho_1\sigma^2 t^2}.$$

On peut écrire l'équation de condition sous la forme

$$(\rho_2\mu_1 r^2 + \mathrm{A}t^2)(\rho_2\mu_1 r^2 + 2\mathrm{A}t^2) = \rho_2\mu_1\mathrm{H}^2,$$

et la séparer, de diverses manières, en deux autres formant un système analogue au système (5); on traitera ces différents systèmes de la même façon que précédemment. En faisant plus particulièrement $\rho_2 = \mu_1 = 1$, on a, en désignant par a et b deux nouvelles indéterminées,

$$r^2 + \mathrm{A}t^2 = a^2,$$
$$r^2 + 2\mathrm{A}t^2 = b^2,$$
$$ab = \mathrm{H}.$$

Par suite, on obtient

$$a^2 - \mathrm{A}t^2 = r^2, \quad a^2 + \mathrm{A}t^2 = b^2;$$

c'est un système identique au système proposé. Par conséquent, *d'une solution x, y, u, v du système*

$$x^2 - \mathrm{A}y^2 = u^2, \quad x^2 + \mathrm{A}y^2 = v^2,$$

on déduit deux nouvelles solutions X, Y, U, V, *par les formules*

$$
(9)\quad
\left\{
\begin{aligned}
&\left\{
\begin{aligned}
m &= \mu\rho u y \pm v x,\\
n &= u^2 + \mu\rho\sigma^2 y^2;
\end{aligned}
\right.\\
&\left\{
\begin{aligned}
p &= n^2 u^2 + \mu\rho\sigma^2 m^2 y^2,\\
q &= m^2 u^2 + 2\mu\rho\lambda^2 n^2 y^2,\\
g &= n^2 u^2 - \mu\rho\sigma^2 m^2 y^2 - 2\rho\sigma mn\, uy,\\
h &= n^2 u^2 - \mu\rho\sigma^2 m^2 y^2 + 2\rho\sigma mn\, uy;
\end{aligned}
\right.\\
&\left\{
\begin{aligned}
&X = \lambda\sigma p^2 q^2 - \mu\rho g^2 h^2, \quad Y = 2ghpq,\\
&V = \lambda\sigma p^2 q^2 + \mu\rho g^2 h^2, \quad U = \rho^2 g^4 - 2\mu^2 h^4.
\end{aligned}
\right.
\end{aligned}
\right.
$$

Ces formules donnent des solutions distinctes de celles qui sont fournies par les équations (6); d'ailleurs le second cas conduirait aux mêmes formules.

Pour certaines valeurs de A, les formules (6) et (9) résolvent complétement le système (1), et par exemple pour A = 6. On traite ainsi complétement ce problème de Fermat :

Trouver tous les triangles rectangles dont l'aire soit six fois celle d'un carré.

Ces formules résolvent aussi complétement le système (7), pour le problème de Beha-Eddin, que l'on ramène au système

$$8x^2 - y^2 = 7u^2, \quad 8x^2 + y^2 = 9v^2,$$

ainsi que nous l'avons montré précédemment (*).

Remarque. — En prenant le signe — dans la formule (8), on arrive à des systèmes analogues au système (5).

(*) *Voir* tome XV, page 359.