

DESBOVES

**Mémoire sur la résolution en nombres entiers
de l'équation $aX^m + bY^m = cZ^n$**

Nouvelles annales de mathématiques 2^e série, tome 18
(1879), p. 265-279

http://www.numdam.org/item?id=NAM_1879_2_18__265_1

© Nouvelles annales de mathématiques, 1879, tous droits réservés.

L'accès aux archives de la revue « Nouvelles annales de mathématiques » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

MÉMOIRE SUR LA RÉSOLUTION EN NOMBRES ENTIERS
DE L'ÉQUATION

$$aX^m + bY^m = cZ^n (*);$$

PAR M. DESBOVES.

I. — *Objet du Mémoire.*

1. Les géomètres, qui jusqu'ici se sont occupés de la résolution en nombres entiers des équations à plusieurs

(*) m, n, a, b, c sont des nombres entiers donnés dont les deux premiers ont toujours des valeurs positives, X, Y, Z désignent les trois inconnues, et (x, y, z) représentera toujours, dans la suite, la solution de l'équation

$$X = x, \quad Y = y, \quad Z = z.$$

inconnues, ont surtout cherché les cas où les équations étaient impossibles; ce sont, au contraire, les cas de possibilité qui doivent être traités ici. Laissant de côté le cas où m est égal à 2, quel que soit n , je me propose de trouver des formes générales de a , b , c telles, que l'équation (1) puisse être résolue en nombres entiers. Je ferai voir, en particulier, que, a et b ayant des valeurs arbitraires, on pourra toujours déterminer c d'une infinité de manières, de telle sorte que cette résolution soit possible. Il est clair que, si l'on admettait pour Z la valeur 1, la dernière question serait immédiatement résolue, puisque, si c est de la forme $ax^m + by^m$, on a immédiatement la solution $(x, y, 1)$; mais ce n'est point d'une pareille solution qu'il s'agira par la suite. De plus, lorsque l'équation à résoudre aura une infinité de solutions, je donnerai des formules qui permettront de déduire d'une première solution une deuxième, de celle-ci une troisième, et ainsi de suite indéfiniment.

Avant que le cas général soit abordé, les cas particuliers où, m étant égal à 3 ou 4, n est égal à 2, 3, 4, ..., seront successivement traités.

2. La seule méthode suivie dans tout le cours du Mémoire est fondée sur l'emploi de certaines identités, dont quelques-unes sont intuitives, mais qui, pour la plupart, seront démontrées d'après les principes exposés par Lagrange dans le Chapitre IX des Additions à l'*Algèbre* d'Euler. Le grand géomètre termine ainsi ce Chapitre : « Mais en voilà assez sur ce sujet, que nous pourrons peut-être reprendre dans une autre occasion ». Dans un Mémoire qui a pour titre : *De quelques problèmes de l'Analyse de Diophante*, il ajoute encore ces mots : « Au reste, la méthode la plus simple et la plus générale pour résoudre ces sortes d'égalités (il s'agit de

la résolution en nombres entiers des équations à trois inconnues) est peut-être celle des facteurs, que j'ai exposée dans le dernier Chapitre des Additions à l'*Algèbre* d'Euler ». Lagrange n'ayant pas tenu la promesse qu'il avait faite, j'ai essayé de deviner quelques-uns des développements qu'il aurait pu ajouter à son Chapitre IX. J'espère qu'on voudra bien me pardonner la témérité de ma tentative en faveur de quelques résultats nouveaux auxquels je suis parvenu.

II. — *Démonstration de quelques identités fondamentales.*

3. Les identités dont il s'agit seront obtenues en cherchant des fonctions du second, du troisième ou du quatrième degré, dans lesquelles le nombre des variables soit toujours égal au degré, et telles que, en multipliant deux fonctions de même espèce, on trouve un produit de même espèce que ses deux facteurs. On indiquera ensuite le moyen général d'obtenir des identités correspondant à des fonctions d'un degré quelconque.

Bien que la résolution des équations dans lesquelles m est égal à 2 soit exclue de ce travail, je donne les identités qui se rapportent aux fonctions du second degré, parce qu'elles serviront à trouver des identités d'un degré supérieur.

4. *Identités résultant de la considération des fonctions du second degré à deux variables.* — Je vais d'abord démontrer le théorème suivant :

THÉORÈME I. — *Si l'on multiplie une fonction du second degré $x^2 + axy + by^2$ par une fonction de même espèce $x_1^2 + ax_1y_1 + by_1^2$, on obtient toujours une*

fonction $X^2 + aXY + bY^2$ de même espèce que les deux autres.

En effet, si l'on désigne par α, β les racines de l'équation du second degré

$$(1) \quad \frac{x^2}{y^2} + a \frac{x}{y} + b = 0,$$

dans laquelle $\frac{x}{y}$ est l'inconnue, on a

$$\begin{aligned} x^2 + axy + by^2 &= y^2 \left(\frac{x^2}{y^2} + a \frac{x}{y} + b \right) \\ &= y^2 \left(\frac{x}{y} - \alpha \right) \left(\frac{x}{y} - \beta \right) = (x - \alpha y)(x - \beta y), \end{aligned}$$

et de même

$$x_1^2 + ax_1y_1 + by_1^2 = (x_1 - \alpha y_1)(x_1 - \beta y_1).$$

On a ensuite

$$\begin{aligned} (x - \alpha y)(x_1 - \alpha y_1) &= xx_1 + \alpha^2 yy_1 - \alpha(xy_1 + yx_1) \\ &= xx_1 - byy_1 - \alpha(xy_1 + yx_1 + ayy_1), \end{aligned}$$

la dernière expression étant déduite de la précédente en remplaçant dans celle-ci α^2 par $-a\alpha - b$.

Si maintenant on pose

$$(2) \quad X = xx_1 - byy_1, \quad Y = xy_1 + yx_1 + ayy_1,$$

il vient

$$(x - \alpha y)(x_1 - \alpha y_1) = X - \alpha Y,$$

et l'on a de même

$$(x - \beta y)(x_1 - \beta y_1) = X - \beta Y.$$

Alors, si l'on multiplie, membre à membre, les deux dernières égalités, on obtient l'identité

$$(3) \quad X^2 + aXY + bY^2 = (x^2 + axy + by^2)(x_1^2 + ax_1y_1 + by_1^2),$$

qui démontre le théorème énoncé.

Ce théorème peut évidemment être étendu à un nombre quelconque de fonctions du second degré de même espèce. En effet, si l'on multiplie $X^2 + aXY + bY^2$, produit des deux premières fonctions par $x_2^2 + ax_2y_2 + by_2^2$, d'après le théorème démontré, le produit sera de la forme $X_1^2 + aX_1Y_1 + bY_1^2$, les fonctions X_1, Y_1 étant obtenues comme il suit. On remplace d'abord dans les formules (2) X, x, x_1, Y, y, y_1 respectivement par X_1, X, x_2, Y_1, Y, y_2 , et l'on a ainsi

$$(4) \quad X_1 = Xx_2 - bYy_2, \quad Y_1 = Xy_2 + Yx_2 + aYy_2;$$

il ne reste plus alors qu'à substituer, dans ces dernières formules, à X et Y les expressions que donnent les formules (2). On pourra de même passer du cas de trois facteurs à celui de quatre facteurs, et ainsi de suite; mais nous voulons seulement nous arrêter au cas des facteurs égaux.

Si l'on considère d'abord le cas de deux facteurs égaux, on fait, dans les équations (2) et (3), $x_1 = x$, et, en posant

$$(5) \quad Z = x^2 + axy + by^2,$$

on a l'identité

$$(6) \quad X^2 + aXY + bY^2 = Z^2,$$

X et Y étant données par les formules

$$(7) \quad X = x^2 - by^2, \quad Y = 2xy + ay^2.$$

Pour passer maintenant au cas de trois facteurs, il suffit de remplacer, dans les formules (4), x_2, y_2 par x, y et X, Y par les expressions que donnent les formules (7); on a ainsi

$$(8) \quad \begin{cases} X_1 = x^3 - 3bxy^2 - aby^3, \\ Y_1 = 3x^2y + 3axy^2 + (a^2 - b)y^3, \end{cases}$$

et l'identité

$$(9) \quad X_1^2 + aX_1Y_1 + bY_1^2 = Z^3$$

est satisfaite par les valeurs de X_1, Y_1, Z que donnent les formules (8) et (5).

Traisons enfin le cas de quatre facteurs égaux. A cet effet, on remplace d'abord, dans les formules (2), X, x, x_1, Y, y, y_1 respectivement par X_2, X_1, x, Y_2, Y_1, y , puis, dans les formules ainsi obtenues, X_1, Y_1 par les valeurs que donnent les formules (8); on a ainsi

$$(10) \quad \begin{cases} X_2 = x^4 - 4abxy^3 - 6bx^2y^2 - b(a^2 - b)y^4, \\ Y_2 = -4x^3y + 4(a^2 - b)xy^3 + 6ax^2y^2 + a(a^2 - 2b)y^4, \end{cases}$$

et l'on satisfait à l'identité

$$(11) \quad X_2^2 + aX_2Y_2 + bY_2^2 = Z^4$$

par les valeurs précédentes de X_2, Y_2 , et toujours par la valeur de Z que donne la formule (5).

5. *Identities résultant de la considération des fonctions du troisième degré à trois variables.* — En suivant une méthode toute semblable à la précédente, Lagrange démontre que, si l'on multiplie entre elles des fonctions du troisième degré à trois variables de la forme

$$x^3 + cy^3 + cz^3 + (ab - 3c)xyz + ax^2y + bxy^2 + acy^2z \\ + bcyz^2 + (a^2 - 2b)x^2z + (b^2 - 2ac)xz^2,$$

on obtient toujours une fonction de même forme. Mais, si l'on fait, dans cette expression, a et b nuls, elle se réduit à

$$x^3 + cy^3 + cz^3;$$

or, comme il n'est besoin ici que d'expressions de cette forme, pour simplifier les calculs, je modifierai la marche suivie par Lagrange.

λ et μ étant les racines cubiques imaginaires de l'unité, faisons le produit des trois facteurs $x + \lambda y + \lambda^2 z$, $x + \mu y + \mu^2 z$, $x + y + z$. Les deux premiers facteurs, après que l'on y a remplacé λ et μ par leurs valeurs, deviennent

$$\frac{1}{2} [2x - y - z + (\gamma - z) \sqrt{-3}],$$

$$\frac{1}{2} [2x - y - z - (\gamma - z) \sqrt{-3}],$$

et ont pour produit

$$x^2 + y^2 + z^2 - xy - xz - yz.$$

En multipliant ensuite ce dernier produit par

$$x + y + z,$$

on a, pour le produit des trois facteurs,

$$x^3 + y^3 + z^3 - 3xyz;$$

on obtient donc l'identité

$$\begin{aligned} (x + \lambda y + \lambda^2 z) (x + \mu y + \mu^2 z) (x + y + z) \\ = x^3 + y^3 + z^3 - 3xyz. \end{aligned}$$

Si maintenant on désigne par α , β , γ les trois racines cubiques d'un nombre quelconque r , on a

$$\alpha = \lambda \gamma, \quad \beta = \mu \gamma,$$

et alors, en changeant dans l'identité précédente y et z en γy et $\gamma^2 z$, on a la nouvelle identité

$$(12) \quad \left\{ \begin{aligned} (x + \alpha y + \alpha^2 z) (x + \beta y + \beta^2 z) (x + \gamma y + \gamma^2 z) \\ = x^3 + r y^3 + r^2 z^3 - 3 r x y z. \end{aligned} \right.$$

Cela posé, on peut démontrer le théorème suivant :

THÉORÈME II. — *Si l'on multiplie entre elles deux*

expressions de même forme que le second membre de l'identité (12), on obtient encore une expression de même forme.

En effet, si l'on change x, y, z en x_1, y_1, z_1 dans l'identité (12) et que l'on multiplie, membre à membre, cette identité et celle qu'on en a déduit, on aura, dans le second membre de la nouvelle équation, l'indication du produit de deux fonctions de la forme considérée. Pour obtenir ensuite le développement de ce produit, on remarque que l'on a

$$\begin{aligned} (x + \alpha y + \alpha^2 z)(x_1 + \alpha y_1 + \alpha^2 z_1) \\ = xx_1 + r(yz_1 + zy_1) + (xy_1 + yx_1 + rzz_1)\alpha \\ + (xz_1 + zx_1 + yy_1)z^2; \end{aligned}$$

et, si l'on pose

$$(13) \quad \begin{cases} X = xx_1 + r(yz_1 + zy_1), & Y = xy_1 + yx_1 + rzz_1, \\ & U = xz_1 + zx_1 + yy_1, \end{cases}$$

il vient

$$X + \alpha Y + \alpha^2 U = (r + \alpha y + \alpha^2 z)(x_1 + \alpha y_1 + \alpha^2 z_1).$$

On a de même

$$X + \beta Y + \beta^2 U = (x + \beta y + \beta^2 z)(x_1 + \beta y_1 + \beta^2 z_1),$$

$$X + \gamma Y + \gamma^2 Z = (x + \gamma y + \gamma^2 z)(x_1 + \gamma y_1 + \gamma^2 z_1);$$

alors, en multipliant, membre à membre, les trois dernières équations, on a l'identité

$$(14) \quad \begin{cases} X^3 + rY^3 + r^2U^3 - 3rXYU \\ = (x^3 + r y^3 + r^2 z^3 - 3rxyz) \\ \times (x_1^3 + r y_1^3 + r^2 z_1^3 - 3r x_1 y_1 z_1) \end{cases}$$

qui démontre le théorème énoncé.

Si dans l'identité précédente on fait x_1, y_1, z_1 respec-

tivement égaux à x, y, z et que l'on pose

$$(15) \quad Z = x^3 + ry^3 + r^2z^3 - 3rxyz,$$

on voit que l'on satisfera à l'équation

$$(16) \quad X^3 + rY^3 + r^2U^3 - 3XYU = Z^3,$$

en déterminant Z par la formule (15) et X, Y, U par les formules

$$(17) \quad X = x^2 + 2ryz, \quad Y = 2xy + rz^2, \quad U = 2xz + y^2,$$

que l'on déduit des formules (13) en y faisant x_1, y_1, z_1 respectivement égaux à x, y, z .

Maintenant, si l'on veut satisfaire à l'équation

$$(18) \quad X_1^3 + rY_1^3 + r^2U_1^3 - 3rX_1Y_1U_1 = Z^3,$$

Z étant toujours donnée par la formule (15), on prendra les expressions de X_1, Y_1, U_1 déterminées par les formules suivantes :

$$(19) \quad \begin{cases} X_1 = x^3 + ry^3 + r^2z^3 + 6rxyz, \\ Y_1 = 3(x^2y + rxz^2 + ry^2z), \\ U_1 = 3(r^2z + xy^2 + ryz^2), \end{cases}$$

que l'on déduit des formules (13) en y remplaçant d'abord $X, x, x_1, \dots$ par $X_1, X, x, \dots$, puis X, Y, U par les expressions (17).

Enfin on satisfera à l'équation

$$(20) \quad X_2^3 + rY_2^3 + r^2U_2^3 - 3rX_2Y_2U_2 = Z^4,$$

Z étant encore déterminée par la formule (15), en prenant

$$(21) \quad \begin{cases} X_2 = x^4 + 4rxy^3 + 4r^2xz^3 + 12rx^2yz + 6r^2y^2z^2, \\ Y_2 = ry^4 + 4x^3y + 4r^2yz^3 + 12ry^2xz + 6rx^2z^2, \\ U_2 = r^2z^4 + 4r^3z + 4r^2yz^3 + 12z^2xy + 6r^2y^2z. \end{cases}$$

Ces dernières formules s'obtiennent de la même manière que les précédentes, c'est-à-dire en remplaçant dans les formules (13) $X, x, x_1, \dots$ par $X_2, X_1, x, \dots$, puis X_1, Y_1, U_1 par les expressions (19).

6. *Identités résultant de la considération de certaines fonctions du quatrième degré à quatre variables.* — λ, μ, ν, ρ étant les quatre racines quatrièmes de l'unité, on multiplie les facteurs

$$\begin{aligned} x + \lambda y + \lambda^2 z + \lambda^3 u, & \quad x + \mu y + \mu^2 z + \mu^3 u, \\ x + \nu y + \nu^2 z + \nu^3 u, & \quad x + \rho y + \rho^2 z + \rho^3 u, \end{aligned}$$

ou

$$\begin{aligned} x - z + (y - u)\sqrt[4]{-1}, & \quad x - z - (y - u)\sqrt[4]{-1}, \\ x + z + y + u, & \quad x + z - y - u, \end{aligned}$$

et l'on obtient pour produit la fonction

$$\begin{aligned} x^4 - y^4 + z^4 - u^4 - 2x^2z^2 \\ + 2y^2u^2 - 4x^2yu - 4z^2yu + 4y^2xz + 4u^2xz. \end{aligned}$$

Employant ensuite le même procédé que celui qui a donné le second membre de l'identité (12), on déduit de la fonction précédente celle-ci, qui est plus générale :

$$(22) \quad \begin{cases} x^4 - r_1^4 + r^2z^4 - r^4u^4 - 2rx^2z^2 + 2r^2y^2u^2 \\ - 4rx^2yu - 4r^2z^2yu + 4r_1^2xz + 4r^2u^2xz, \end{cases}$$

et l'on démontre, de la même manière que le théorème II, le théorème suivant :

THÉORÈME III. — *Si l'on multiplie entre elles deux fonctions du quatrième degré de la forme (22), on obtient pour produit une fonction de la même forme.*

En d'autres termes, si l'on pose

$$(23) \quad \begin{cases} X = xx_1 + rz_1 + ryu_1 + rv_1, \\ Y = xy_1 + yx_1 + rzu_1 + ru_1z, \\ U = xz_1 + zx_1 + yv_1 + ruu_1, \\ V = xu_1 + ux_1 + yz_1 + zy_1, \end{cases}$$

on a l'identité

$$(24) \quad \begin{cases} X^4 - rY^4 + r^2U^4 - r^3V^4 - 2rX^2U^2 + 2r^2Y^2V^2 \\ - 4rX^2YV - 4r^2U^2YV + 4rY^2XU + 4r^2V^2XU \\ = (x^2 - ry^4 + \dots)(x_1^4 - ry_1^4 + \dots). \end{cases}$$

Supposons maintenant que, dans les formules (23) et dans l'identité (24), on fasse x_1, y_1, z_1, u_1 respectivement égaux à x, y, z, u et que l'on pose

$$(25) \quad \begin{cases} Z = x^4 - ry^4 + r^2z^4 - r^3u^4 - 2rx^2z^2 \\ + 2r^2y^2u^2 - 4rx^2yu - 4r^2z^2yu \\ + 4ry^2xz + 4r^2u^2xz, \end{cases}$$

on voit que l'on satisfait à l'identité

$$(26) \quad X^4 - rY^4 + r^2U^4 - r^3V^4 - 2rX^2U^2 + \dots = Z^2,$$

en prenant l'expression de Z (25) et en déterminant X, Y, U, V par les formules

$$(27) \quad \begin{cases} X = x^2 + rz^2 + 2ryu, \\ Y = 2(xy + rzu), \\ U = 2xz + y^2 + ru^2, \\ V = 2(xu + yz). \end{cases}$$

Si l'on veut maintenant satisfaire à l'équation

$$(28) \quad X_1^4 - rY_1^4 + r^2U_1^4 - r^3V_1^4 - 2rX_1^2U_1^2 + \dots = Z^2.$$

on prendra toujours l'expression de Z (25), et l'on aura

$$(29) \quad \begin{cases} X_1 = 3rxz + 3r^2z + 3r^2zu^2 + 6rxyu + x^3, \\ Y_1 = 3r^2y + 3r^2z^2 + 3r^2y^2u + 6rxzu + r^2u^3, \\ U_1 = 3x^2z + 3rxy^2 + 3rxu^2 + 6rjzu + rz^3, \\ V_1 = 3x^2u + 3rz^2u + 3rjy^2u^2 + 6xyz + r^3. \end{cases}$$

Ces dernières formules se déduisent facilement des formules (23) et (27).

Nous ne donnerons pas ici les expressions générales de X_2, Y_2, U_2, V_2 satisfaisant à l'équation

$$(30) \quad X_2^4 - rY_2^4 + \dots = Z^4,$$

parce que ces expressions sont compliquées et qu'elles ne seront pas employées dans ce travail, du moins dans leur généralité.

7. Généralisation des résultats précédents.

La question générale que nous nous proposons de résoudre est celle-ci : $\alpha, \beta, \gamma, \dots$ étant les racines de l'équation

$$(31) \quad \xi^m - r = 0,$$

et $x_0, x_1, x_2, \dots, x_{m-1}, m$ quantités quelconques, trouver l'expression du produit des m fonctions

$$\begin{aligned} & x_0 + r_1\alpha + x_2\alpha^2 + \dots + r_{m-1}\alpha^{m-1}, \\ & r_0 + r_1\beta + x_2\beta^2 + \dots + r_{m-1}\beta^{m-1}, \\ & \dots \dots \dots \end{aligned}$$

Si l'on pose

$$x_0 + r_1\xi + r_2\xi^2 + \dots + r_{m-1}\xi^{m-1} = \pi,$$

et que l'on élimine ξ entre l'équation (31) et la précédente, on aura une équation du degré m en π , dans laquelle le terme indépendant de cette variable sera, à un

Nous allons maintenant démontrer le théorème général suivant, qui comprend, comme cas particuliers, les théorèmes II et III.

THÉORÈME IV. — *Si l'on multiplie entre elles une fonction du degré m représentée par le déterminant général et une fonction de même espèce, on obtient une autre fonction de même espèce que les deux autres.*

En se reportant aux démonstrations particulières données aux n^{os} 5 et 6, on voit que tout revient à démontrer qu'en multipliant l'un par l'autre les deux facteurs

$$x_0 + x_1 \alpha + \dots + x_{m-1} \alpha^{m-1}, \quad x'_0 + x'_1 \alpha + \dots + x'_{m-1} \alpha^{m-1},$$

on obtient un produit de même forme. Or, en effectuant la multiplication, on a

$$\begin{array}{l} x_0 x'_0 + x_1 x'_0 \\ + r x_{m-1} x'_1 + x_0 x'_1 \\ + r x_{m-2} x'_2 + r x_{m-1} x'_2 \\ + \dots + \dots \\ \dots \dots \dots \\ + r x_1 x'_{m-1} + r x_2 x'_{m-1} \end{array} \left| \begin{array}{l} \alpha + x_2 x'_0 \\ + x_1 x'_1 \\ + x_0 x'_2 \\ + r x_{m-1} x'_3 \\ + r x_3 x'_{m-1} \\ + \dots \end{array} \right| \left| \begin{array}{l} \alpha^2 + \dots + x_{m-1} x'_0 \\ + x_{m-2} x'_1 \\ + \dots \\ + x_0 x'_{m-1} \end{array} \right| \alpha^{m-1}$$

Si donc on pose

$$X_0 = x_0 x'_0 + r (x_{m-1} x'_1 + x_{m-2} x'_2 + \dots + x_1 x'_{m-1}),$$

$$X_1 = x_1 x'_0 + x_0 x'_1 + r (x_{m-1} x'_2 + \dots + x_2 x'_{m-1}),$$

$$\dots \dots \dots$$

$$X_{m-1} = x_{m-1} x'_0 + x_{m-2} x'_1 + \dots + x_0 x'_{m-1},$$

on obtient la fonction $X_0 + X_1 \alpha + X_2 \alpha^2 + \dots + X_{m-1} \alpha^{m-1}$, de même espèce que les deux premières.

On voit, d'ailleurs, immédiatement de quelle manière se forme la fonction X_0 , et comment les autres fonctions s'en déduisent par la permutation circulaire des indices 0, 1, 2... $m-1$ dans les premiers facteurs de chaque

terme. On remarque encore que r est multiplicateur de tous les termes, excepté un dans la première formule, excepté deux dans la seconde, et ainsi de suite, de telle sorte que, dans la dernière formule, r n'est multiplicateur d'aucun terme.

On pourra maintenant, si l'on veut, obtenir les valeurs de $X_0, X_1, X_2, \dots, X_{m-1}$ correspondant aux cas où l'on multiplie entre eux un nombre quelconque de facteurs égaux.

(*A suivre.*)