JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

PEPIN

Solution de l'équation $X^4 + 35Y^4 = Z^2$

Journal de mathématiques pures et appliquées 5e série, tome 1 (1895), p. 351-358.

<http://www.numdam.org/item?id=JMPA_1895_5_1__351_0>

Solution de l'équation $X^4 + 35Y^4 = Z^2$;

PAR LE P. PEPIN S. J.

1. Par une application convenable de la méthode de *descente* de Fermat on peut obtenir une solution complète d'un grand nombre d'équations indéterminées, renfermées dans la formule

$$ax^4 + by^4 = cz^2.$$

Comme cette équation admet un nombre indéfini de solutions toutes les fois qu'elle n'est pas impossible, on doit la considérer comme complètement résolue lorsqu'on a trouvé une méthode certaine pour obtenir toutes les solutions en nombres entiers et premiers entre eux, qui ne surpassent pas une limite assignée, et démontrer que l'on ne laisse échapper aucune solution plus simple que les solutions calculées. On y parvient le plus souvent en démontrant que toute solution de l'équation proposée, tant qu'elle est formée de nombres tous supérieurs à l'unité, peut se ramener à une solution de la même équation en nombres moindres, au moyen de laquelle on l'exprime par des formules dont le nombre varie suivant les cas. Le raisonnement destiné à démontrer que l'emploi méthodique des formules obtenues donne avec certitude toutes les solutions en nombres premiers entre eux, qui ne surpassent pas une limite assignée, ce raisonnement, dis-je, est au fond le même dans tous les cas; il a été complètement développé dans mon étude sur l'équation

$$7x^4 - 5y^4 = 2z^2,$$

publiée en 1879 dans le *Journal de Mathématiques*, 3ᵉ série, t. III, p. 105.

2. L'équation que je me propose de résoudre,

$$X^4 + 35Y^4 = Z^2, \tag{1}$$

présente une particularité remarquable. Elle est susceptible d'une solution complète, sans que les solutions formées de nombres supérieurs à l'unité soient toutes ramenées à d'autres solutions en nombres moindres, au moyen desquelles on puisse les exprimer. Cette réduction, facile tant que Y est un nombre pair, devient fort compliquée quand Y est impair. Mais, dans ce dernier cas, les solutions de l'équation (1) se ramènent à celles de l'équation citée plus haut, et elles jouent relativement aux autres solutions le rôle de solutions primitives.

Soit en effet $Y = ab$ un nombre impair. Comme nous supposons X, Y, Z premiers entre eux, la décomposition de l'équation (1) s'effectue au moyen des formules suivantes

$$\begin{aligned} Z \pm X^2 &= a^4,\ 7a^4, & Z \mp X^2 &= 35b^4,\ 5b^4, \\ 2Z &= a^4 + 35b^4, & \pm 2X^2 &= a^4 - 35b^4, \\ 2Z &= 7a^4 + 5b^4, & \pm 2X^2 &= 7a^4 - 5b^4. \end{aligned}$$

On doit rejeter la première décomposition, parce que $+2$ et -2 sont non-résidus quadratiques de 5. Dans la dernière formule, le signe inférieur est exclu par le module 7. Par conséquent les deux facteurs a, b de Y forment une solution de l'équation citée plus haut

$$7x^4 - 5y^4 = 2z^2. \tag{2}$$

Les solutions de l'équation proposée dans lesquelles Y est impair sont donc exprimées au moyen des solutions de l'équation (2) par les formules

$$\text{I.} \qquad Z = \frac{7x^4 + 5y^4}{2}, \qquad X = z, \qquad Y = xy.$$

Comme l'équation (2) a été complètement résolue dans le Mémoire cité, nous sommes assuré d'obtenir toutes les solutions de l'équation (1) dans lesquelles X et Y sont impairs et inférieurs à une limite assignée.

3. Quand Y est pair, la décomposition de l'équation proposée s'effectue par les formules suivantes

$$Y = 2ab, \qquad Z \pm X^2 = 2a^4,\ 10a^4,\ 14a^4,\ 70a^4,$$
$$Z \mp X^2 = 280b^4,\ 56b^4,\ 40b^4,\ 8b^4,$$

d'où l'on déduit respectivement

$$\pm X^2 = a^4 - 140b^4, \quad 5a^4 - 28b^4, \quad 7a^4 - 20b^4, \quad 35a^4 - 4b^4.$$

La première équation exige, suivant le module 8, que l'on prenne le signe supérieur et que b soit pair. La deuxième et la troisième sont impossibles, parce que $+7$ et -7 sont non-résidus quadratiques de 5. La quatrième n'est possible qu'avec le signe inférieur, et elle exige que b soit impair. On a par conséquent l'un des deux systèmes suivants

$$(3) \quad Y = 4ab, \qquad X^2 = a^4 - 16.140b^4, \qquad Z = a^4 + 16.140b^4,$$
$$(4) \quad Y = 2ab, \qquad -X^2 = 35a^4 - 4b^4, \qquad Z = 35a^4 + 4b^4.$$

La deuxième équation du premier système se décompose de la manière suivante

$$a^2 \pm X = 2m^4,\ 10m^4,\ 14m^4,\ 70m^4, \qquad b = mn,$$
$$a^2 \mp X = 32.35n^4,\ 32.7n^4,\ 32.5n^4,\ 32n^4,$$
$$a^2 = m^4 + 35(2n)^4,\ 5m^4 + 7(2n)^4,\ 7m^4 + 5(2n)^4,\ 35m^4 + (2n)^4.$$

La deuxième et la troisième équation sont impossibles parce que 7 est non-résidu quadratique de 5; la dernière est impossible suivant le module 4.

La première décomposition est seule admissible; on a

$$\text{II.} \qquad a^2 = m^4 + 35(2n)^4, \qquad Y = 4amn,$$
$$\pm X = m^4 - 35(2n)^4, \qquad Z = a^4 + 140(2mn)^4.$$

Ainsi toute solution de l'équation (1) dans laquelle Y est un multiple de 4 se ramène à une autre solution de la même équation en nombres moindres (m, $2n$, a) au moyen de laquelle on l'exprime par les formules II. Quant aux solutions dans lesquelles Y est de la forme $4l + 2$, elles sont exprimées par les formules (4) dont la deuxième se décompose de la manière suivante

$$a = mn, \qquad 2b^2 \pm X = m^4,\ 7m^4, \qquad 2b^2 \mp X = 35n^4,\ 5n^4,$$
$$4b^2 = m^4 + 35n^4, \qquad 4b^2 = 7m^4 + 5n^4.$$

La dernière équation étant impossible, parce que 7 est non-résidu quadratique de 5, la première décomposition est seule admissible; la solution considérée se ramène à une solution plus simple (m, n, $2b$) de la même équation, au moyen de laquelle on l'exprime par les formules suivantes

$$\text{III.} \qquad m^4 + 35n^4 = (2b)^2, \qquad Y = 2bmn,$$
$$\pm X = \frac{m^4 - 35n^4}{2}, \qquad Z = 4b^4 + 35m^4n^4.$$

4. Les formules II et III peuvent être remplacées par un système unique

$$\text{IV.} \qquad x^4 + 35y^4 = z^2, \qquad \theta Y = 2xyz,$$
$$\theta X = x^4 - 35y^4, \qquad \theta^2 Z = z^4 + 4.35(xy)^4,$$

où θ est égal à 1 ou 2, suivant que y est pair ou impair.

Toute solution de l'équation proposée, lorsque la seconde indéterminée est un nombre impair, sert de base à une suite indéfinie de solutions dans lesquelles la valeur de Y est divisible par les puissances successives de 2. On les obtient par l'emploi répété des formules IV.

D'ailleurs les solutions dans lesquelles X et Y sont impairs sont exprimées par les formules I au moyen des solutions de l'équation (2) dont nous avons donné une solution complète dans le Mémoire cité de 1879. Nous pouvons donc obtenir toutes celles de ces solutions qui sont formées de nombres inférieurs à une limite donnée. Comme nous savons que le nombre des solutions de l'équation proposée est infini, nous pouvons la considérer comme complètement résolue.

Proposons-nous, par exemple, de déterminer toutes celles des solutions de l'équation (1) dans lesquelles Y ne surpasse pas 15 millions. Nous déterminerons d'abord celles de ces solutions où la valeur de Y est impaire. Elles sont exprimées par les formules I au moyen des solutions de l'équation (2). Il suffit de déterminer celles des solutions de cette dernière équation dans lesquelles le produit xy des deux premières indéterminées ne surpasse pas la limite assignée. Or nous avons trouvé dans le Mémoire cité que les solutions les plus simples de l'équation (2) sont

$$(1, 1, 2), \quad (23, 11, 971), \quad (10127, 1525, z).$$

Comme le produit

$$10127 . 1525 = 15443675$$

surpasse la limite assignée, il suffit d'employer les deux premières solutions.

On en déduit par les formules I les deux solutions

$$X = 1, \qquad Y = 1, \qquad Z = 6;$$
$$X = 971, \qquad Y = 253, \qquad Z = 1016046.$$

Ces deux solutions sont, dans les limites assignées, les seules dans lesquelles la deuxième indéterminée soit un nombre impair. On déduit de chacune d'elles une solution par les formules III, puis une suite indéfinie d'autres solutions en nombres croissants, par l'emploi répété des formules II.

En faisant $m = n = 1$, $2b = 6$ dans les formules III, on en déduit

$$X = 17, \qquad Y = 6, \qquad Z = 359.$$

Cette solution donne par les formules II, en y faisant $m = 17$, $2n = 6$, $a = 359$,

$$X = 38161, \qquad Y = 73236, \qquad Z = 3176436 2401.$$

La solution suivante dépasserait de beaucoup la limite assignée. Il en est de même de celle qu'on déduirait de la solution (971, 233, 1016046) au moyen des formules III. Par conséquent l'équation proposée n'admet que quatre solutions en nombres entiers et premiers entre eux, dans lesquelles la valeur de Y ne surpasse pas 15 millions, savoir

$$(1, 1, 6), \quad (17, 6, 359), \quad (971, 253, 1016046),$$
$$(38161, 73236, 31764362401).$$

5. Si l'on ne se bornait pas aux solutions en nombres premiers entre eux, le nombre des solutions comprises dans les limites assignées surpasserait 17 millions. Le nombre de celles de ces solutions dans lesquelles X, Y sont inégaux et où le plus grand commun diviseur des trois nombres ne renferme aucun des facteurs 2, 3, 5, 11 trop faciles à reconnaître, ce nombre, dis-je, est égal à 620482. On pourra citer, par exemple, les solutions suivantes

$$(119, 42, 2515), \quad (221, 78, 1077), \quad (323, 114, 129599)$$

et un grand nombre d'autres. Mais qu'on débarrasse ces solutions de tout facteur commun, on verra qu'elles se ramènent à celles que nous venons d'indiquer.

6. On voit assez bien par l'analyse précédente qu'on est assuré d'obtenir par la méthode indiquée toutes les solutions de l'équation proposée en nombres premiers entre eux, dont le second Y ne surpasse pas une limite assignée L. Néanmoins, il n'est pas inutile d'en développer la démonstration. Pour cela nous distinguerons deux cas suivant que la seconde indéterminée Y reçoit une valeur impaire ou une valeur paire.

1° $Y \equiv 1 \pmod{2}$. — La solution T est exprimée par les formules I au moyen d'une solution de l'équation (2); et l'on a $xy = Y$. Comme l'équation (2) est complètement résolue, nous pouvons déterminer avec certitude toutes celles des solutions de cette équation dans lesquelles le produit xy des deux premières indéterminées ne dépasse pas la limite L, et déduire de chacune d'elles la solution (X, Y, Z) de l'équation (1), qui en dépend par les formules I. Nous sommes donc assuré d'obtenir toutes celles des solutions (X, Y, Z) de l'équation (1) qui satisfont à la double condition $Y \equiv 1 \pmod{2}$, $Y \leqq L$.

2° $Y = 2^\alpha Y_1$, $Y_1 \equiv 1 \pmod{2}$. — Si l'exposant α est > 1, la solution T se ramène à une solution $(m, 2n, a)$, au moyen de laquelle elle s'exprime par les formules II. On déduit de la formule

$$Y = 4amn = 2^\alpha Y_1$$

que la plus haute puissance de 2 qui divise la valeur $2n$ de la seconde indéterminée est $2^{\alpha-1}$. Soit $T_{\alpha-1}$ cette nouvelle solution. Si l'exposant $\alpha - 1$ surpasse encore l'unité, cette solution s'exprime par les mêmes formules, au moyen d'une solution $T_{\alpha-2}$ dans laquelle l'exposant de 2 est diminué d'une unité. Et ainsi de suite jusqu'à ce qu'on arrive à une solution T_1, dans laquelle Y est de la forme $4l + 2$.

Cette solution T_1 se ramène à une solution $T_0 = (m, n, 2b)$ dans laquelle les deux premiers nombres m, n sont impairs, et au moyen de laquelle on l'exprime par les formules III.

Ainsi, à partir d'une solution quelconque T, on peut former une suite de solutions en nombres décroissants, se terminant à une solution T_0.

Soit (S) cette suite écrite dans l'ordre inverse

$$(S) \qquad T_0,\ T_1,\ T_2,\ \ldots,\ T_{\alpha-2},\ T_{\alpha-1},\ T.$$

Je dis qu'en employant la méthode indiquée on obtient tous les termes de cette suite, et par conséquent la solution considérée T.

D'abord nous avons démontré (1°) que le premier terme s'obtenait avec certitude. Nous ne le connaissons pas, il est vrai; mais, en prenant toutes les solutions comprises dans les limites déterminées par les deux conditions $Y \equiv 1 \pmod{2}$, $Y \leqq L$, et en déduisant de chacune d'elles la solution qui en dépend par les formules III, nous sommes assuré d'employer la solution T_0 et d'en déduire la solution T_1. Si nous employons toutes les solutions obtenues pour en déduire par les formules II les solutions qui en dépendent, nous sommes certain d'employer la solution T_1 et d'en déduire la solution T_2. En employant dans les formules II toutes les solutions ainsi obtenues, nous sommes assuré d'employer la solution T_2 et d'en déduire la solution T_3 qui est le quatrième terme de la suite (S), et ainsi de suite. Nous sommes donc certain d'obtenir par l'emploi répété des formules II, à partir des solutions où la deuxième indéterminée est divisible par 4, tous les termes de la suite (S), et par conséquent la solution T, qui en est le dernier terme.

La formule $Y = 4amn$ montre que chacune des solutions obtenues est du quatrième ordre, puisque a est du second ordre par rapport aux deux nombres m, n. C'est pourquoi le nombre des solutions est très petit par rapport à la limite assignée. Mais il ne faut pas oublier qu'il s'agit de solutions formées de nombres premiers entre eux; car autrement une seule solution

$$X = a, \qquad Y = b, \qquad Z = c$$

en détermine par les formules

$$X = am, \qquad Y = bm, \qquad Z = cm^2$$

un nombre égal à la partie entière du quotient $L : b$.