JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

S. J. PÉPIN

Sur la décomposition d'un nombre entier en une somme de deux cubes rationnels

Journal de mathématiques pures et appliquées 2^e série, tome 15 (1870), p. 217-236.
<http://www.numdam.org/item?id=JMPA_1870_2_15__217_0>

Sur la décomposition d'un nombre entier en une somme de deux cubes rationnels;

PAR LE P. PEPIN, S. J.

Le problème de la décomposition d'un entier A en une somme de deux cubes rationnels se ramène évidemment à celui de résoudre en nombres entiers et différents de zéro l'équation indéterminée

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

On peut aussi le regarder comme un point particulier de la théorie des formes cubiques à trois indéterminées, celui où l'on chercherait les représentations de zéro par la forme cubique donnée

$$x^3 + y^3 - Az^3.$$

L'impossibilité de l'équation (1), quand A = 1, est un théorème de Fermat démontré depuis longtemps par Euler (*Algèbre*, 2e Partie, Ch. XV).

Le second supplément à la *Théorie des nombres*, p. 29 [*], nous apprend que l'équation (1) est encore impossible quand on prend pour A l'un des nombres 2^m, 3 ou 5. Legendre ajoute qu'en appliquant la même méthode au nombre 6, on démontrerait que ce nombre est indécomposable en deux cubes rationnels; mais en cherchant à faire cette démonstration j'ai trouvé qu'on vérifie l'équation (1)

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

en faisant $x = 17$, $y = 37$, $z = 21$. Du reste, cette solution se trouve

[*] *Voyez* aussi la 3e édition de Legendre, 4e Partie, nos 330 à 334.

dans l'étude intéressante de Lamé sur les propriétés du binôme cubique (*Comptes rendus des séances de l'Académie des Sciences*, t. LXI).

Une question des *Nouvelles Annales* proposée, je crois, par M. Sylvester, énonce quelques-uns des cas d'impossibilité auxquels je suis parvenu dans ce Mémoire : je regrette de ne pas pouvoir la citer textuellement.

Legendre fait aussi remarquer qu'une solution de l'équation (1) permet d'en obtenir une infinité d'autres; car si cette équation est vérifiée par des valeurs entières $x = a$, $y = b$, $z = c$, elle le sera encore par les valeurs

$$x = a(2b^3 + a^3), \quad y = -b(2a^3 + b^3), \quad z = c(a^3 - b^3).$$

Enfin, pour donner aux théorèmes qui vont nous occuper toute la généralité qu'ils comportent, il faut se rappeler que, si le nombre A est indécomposable en deux cubes rationnels, il en sera de même pour le produit Am^3, m désignant un nombre rationnel quelconque. Par conséquent si l'impossibilité de l'équation (1) est démontrée pour une valeur particulière $A = p^\alpha$, elle se trouve démontrée pour toutes les valeurs de A comprises dans la formule

$$A = p^{3m+\alpha},$$

m étant entier et positif.

Si l'on ajoute aux théorèmes qui précèdent les propriétés du binôme cubique, trouvées par Lamé, et particulièrement les identités remarquables qui terminent la première partie de son Mémoire (*Comptes rendus des séances de l'Académie des Sciences*, t. LXI, p. 924), on aura, à très-peu près, tout ce qu'on connaît aujourd'hui sur la solution, en nombres entiers, de l'équation cubique

$$x^3 + y^3 = Az^3.$$

On pourrait aussi rapprocher de cette question quelques problèmes analogues résolus soit par Euler, soit par Libri, soit par M. Le Besgue. Euler, à l'endroit cité de son *Algèbre*, donne une méthode pour obtenir une infinité de cubes entiers partagés chacun en trois cubes entiers. Libri a démontré (*Savants étrangers*, t. V, p. 71) que « tout

nombre positif est la somme de quatre cubes rationnels et positifs. » Enfin, M. Le Besgue, complétant un travail de Dirichlet, a démontré dans ce Journal (1843, t. VIII, p. 49) pour l'équation du cinquième degré plusieurs théorèmes généraux analogues à ceux qui font le sujet de ce Mémoire.

Après avoir indiqué les travaux faits jusqu'à ce jour sur la question qui m'occupe, j'ajouterai un mot sur la méthode que j'ai suivie et sur les résultats auxquels je suis parvenu. Ma méthode consiste à joindre quelques considérations sur les résidus cubiques à la décomposition employée par Euler et par Legendre dans les cas particuliers qu'ils ont résolus. J'ai pu démontrer ainsi les théorèmes renfermés dans cet énoncé général :

« Désignons par p et q deux nombres premiers dont les formes linéaires respectives sont $18m + 5$, $18m + 11$; il est impossible de décomposer en deux cubes rationnels aucun des nombres compris dans les formules suivantes :

$$p^m,\ q^m,\ 2p^{3m+1},\ 2q^{3m+2},\ 4p^{3m+2},\ 4q^{3m+1},$$
$$9p^{3m+1},\ 9q^{3m+1},\ 9p^{3m+2},\ 9q^{3m+2},\ 5p^{3m+2},\ 5q^{3m+1},\ 25p^{3m+1},\ 25q^{3m+2},$$

dans lesquelles m désigne un nombre entier quelconque positif ou nul.

Quoique mon but principal ait été de trouver les formes générales des valeurs de A qui rendent impossible l'équation (1), j'ai cru devoir terminer mon Mémoire en énonçant quelques théorèmes affirmatifs, et entre autres les deux suivants qui semblent nouveaux :

Le double d'un nombre triangulaire est toujours la somme de deux cubes rationnels;

Si la somme ou la différence de deux nombres est un cube, leur produit est la somme algébrique de deux cubes rationnels.

Puisse l'intérêt qui s'attache aux travaux dont Legendre a enrichi la science des nombres, mériter à ce Mémoire l'attention bienveillante des géomètres.

§ I.

1. Supposons d'abord que le nombre A n'ait aucun facteur premier $6m + 1$.

L'équation

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

se décompose de l'une des manières suivantes :

$$x + y = Au^3, \quad x^2 - xy + y^2 = v^3, \tag{2}$$

si Az est premier à 3;

$$x + y = \tfrac{1}{3}Au^3, \quad x^2 - xy + y^2 = 3v^3, \tag{3}$$

si Az est divisible par 3. La raison de cette décomposition est que le quotient

$$\frac{x^3 + y^3}{x + y}$$

n'admet que des facteurs premiers $6m + 1$, et en outre la première puissance de 3, lorsque la somme $x + y$ est divisible par 3.

2. Soit d'abord Az pair. Comme nous supposons x, y et z sans diviseur commun, x et y seront impairs, et la seconde équation (2) pourra s'écrire

$$\left(\frac{x+y}{2}\right)^2 + 3\left(\frac{x-y}{2}\right)^2 = v^3. \tag{2'}$$

Chacun des facteurs de v est lui-même de la forme $x^2 + 3y^2$, car cette forme est l'unique forme réduite proprement primitive pour le déterminant -3 : on sait aussi que le nombre des représentations propres de v^3 par cette forme est le même que celui des représentations de v, et que toutes ces représentations de v^3 peuvent se déduire de celles du nombre v, par l'équation

$$X + \sqrt{-3}\,Y = (f + \sqrt{-3}\,g)^3 = f(f^2 - 9g^2) + \sqrt{-3}.3g(f^2 - g^2),$$

dans laquelle on suppose $v = f^2 + 3g^2$. Comme les deux nombres $\frac{x+y}{2}$, $\frac{x-y}{2}$ sont entiers et premiers entre eux, la représentation (2′) de v^3 doit se déduire de la dernière équation en choisissant convenablement la représentation $f^2 + 3g^2$ de v, et l'on a

$$(4)\qquad \begin{cases} \frac{x+y}{2} = \frac{Au^3}{2} = f(f^2 - 9g^2), \\ \frac{x-y}{2} = 3g(f^2 - g^2), \quad f^2 + 3g^2 = v. \end{cases}$$

On verra de même que, si Az est divisible par 3, la deuxième équation (3) peut s'écrire

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

et qu'elle entraîne les équations suivantes :

$$(5)\qquad \begin{cases} \frac{x-y}{2} = f(f^2 - 9g^2), \\ \frac{x+y}{6} = \frac{Au^3}{18} = 3g(f^2 - g^2), \quad f^2 + 3g^2 = v. \end{cases}$$

3. Supposons que le produit Az soit impair. Les équations (2) et (3) peuvent s'écrire respectivement sous les deux formes

$$\left(\frac{2x-y}{2}\right)^2 + 3\left(\frac{y}{2}\right)^2 = v^3, \quad \left(\frac{y}{2}\right)^2 + 3\left(\frac{2x-y}{6}\right)^2 = v^3,$$

et elles entraînent respectivement les équations suivantes :

$$(6)\qquad \begin{cases} \frac{2x-y}{2} = f(f^2 - 9g^2), \quad \frac{y}{2} = 3g(f^2 - g^2), \\ x + y = F + 3G, \quad f^2 + 3g^2 = v; \end{cases}$$

$$(7)\qquad \begin{cases} \frac{y}{2} = f(f^2 - 9g^2), \quad \frac{2x-y}{6} = 3g(f^2 - g^2), \\ x + y = 3(F + G), \quad f^2 + 3g^2 = v, \end{cases}$$

dans lesquelles nous posons, pour abréger,

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

Puisque nous supposons x et y premiers entre eux, les deux nombres f et g n'ont aucun diviseur commun; de plus l'un d'eux est pair et l'autre impair, et g seul peut être divisible par 3. Les deux dernières propriétés résultent de l'équation

$$f^2 + 3g^2 = \nu,$$

où le nombre ν est de la forme $6m + 1$. Enfin G est toujours le multiple de g.

4. Nous allons chercher les conséquences des formules précédentes pour le cas où le nombre A est premier avec 3. Si, dans ce cas, z est impair et multiple de 3, on a les équations (3) et (7) dans lesquelles u doit être divisible par 3. Posons $u = 3u_1$; l'équation

$$x + y = \mathrm{A} \cdot 27 \cdot u_1^3 = 3(\mathrm{F} + \mathrm{G})$$

donne

$$9\mathrm{A}u_1^3 = f(f^2 - 9g^2) + 3g(f^2 - g^2),$$

ce qui est impossible, f étant premier à 3. Donc :

THÉORÈME I. — *Si tous les diviseurs impairs du nombre* A *sont de la forme* $6m - 1$, *et qu'on puisse résoudre l'équation* (1) *en nombres entiers premiers entre eux, le nombre* z *ne peut être divisible par* 3 *sans être pair.*

Supposons donc z impair et premier à 3. Dans ce cas l'équation (1) donnera les équations (2) et (6), d'où l'on déduira

$$x + y = \mathrm{A}u^3 = \mathrm{F} + 3\mathrm{G}, \quad \text{et} \quad x - y = \mathrm{F} - \mathrm{G}.$$

Si dans la première nous supprimons les multiples de 9, en remarquant que le cube d'un nombre n premier à 3 est toujours un multiple de 9 plus ou moins 1, elle devient

$$\mathrm{A} \equiv \pm 1 \pmod 9.$$

On a aussi

$$2y = 4G = 12g(f^2 - g^2) \equiv 0 \pmod{36}.$$

De ces deux congruences, en ayant égard au premier théorème, on déduit :

THÉORÈME II. — 1° *Si le nombre* A *est de l'une des formes* $18m \pm 5$, $18m \pm 11$, *l'équation* (1) *ne peut être vérifiée en nombres entiers, sans que* z *soit un nombre pair.*

2° *Si le nombre* A *est de l'une des deux formes* $18m + 1$, $18m + 17$, *et que dans l'équation* (1) z *soit un nombre impair, l'un des deux autres nombres* x, y *est en même temps pair et divisible par* 9.

5. Si le produit Az est pair, l'équation (1) donnera les équations (2) et (4), ou les équations (3) et (5), suivant que z sera premier à 3 ou divisible par 3. Dans le premier cas, l'équation $\frac{x-y}{2} = 3g(f^2 - g^2)$ donne la congruence

$$x \equiv y \pmod{9}.$$

L'équation (1) donnera, par suite,

$$Az^3 \equiv 2x^3 \pmod{9}, \quad A \equiv \pm 2 \pmod{9}.$$

Dans le deuxième cas, l'équation

$$\frac{Au^3}{18} = 3g(f^2 - g^2)$$

ne peut subsister sans que le nombre u soit divisible par 9. Nous avons donc ce théorème :

THÉORÈME III. — *L'un des deux nombres* A *ou* z *étant pair, si* z *est divisible par* 3, *il est aussi divisible par* 9 ; *si au contraire* z *est premier à* 3, *le nombre* A *doit être de l'une des formes*

$$18m + (2, 7, 11, \text{ou } 16).$$

§ II.

6. Pour déduire quelques conséquences des résultats obtenus jusqu'ici, nous considérerons successivement le cas où le nombre A est une puissance d'un nombre premier $6m - 1$, et celui où il est le produit d'une semblable puissance multipliée par une puissance de 2. De plus nous considérerons immédiatement parmi les diverses solutions possibles, celle où la valeur numérique de z est la plus petite possible ; de telle sorte qu'une hypothèse sera toujours rejetée comme impossible, lorsqu'elle ramènera l'équation (1) résolue en nombres inférieurs à cette valeur *minima* de z.

Supposons d'abord que le nombre A soit égal à l'un des nombres p, q, p^2, q^2. Il sera de l'une des formes $18m + (5, 7, 11$ ou $13)$. Dans ce cas le deuxième théorème nous apprend que le nombre z doit être pair. Si de plus z est divisible par 3, l'équation (1) entraînera comme conséquence les équations (3) et (5), et l'on aura

$$u = 3u_1, \quad \mathrm{A}u_1^3 = 2g(f+g)(f-g).$$

Comme les trois facteurs $2g, f+g, f-g$ sont premiers entre eux, leur produit $\mathrm{A}u^3$ se décomposera de l'une des manières suivantes :

$$2g = \mathrm{A}\alpha^3, \quad f+g = \beta^3, \quad f-g = \gamma^3, \quad u_1 = \alpha\beta\gamma,$$
$$2g = \alpha^3, \quad f \pm g = \mathrm{A}\beta^3, \quad f \mp g = \gamma^3.$$

On en déduit respectivement les équations

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

qui ne sont autres que l'équation (1) résolue en attribuant aux indéterminées des valeurs α, β, γ toutes inférieures au *minimum* de $z = 3\alpha\beta\gamma . \rho$.

Il faut donc supposer z premier à 3 ; mais alors l'équation (1) entraîne comme conséquence les équations (2) et (4), et l'on a

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

Les trois facteurs $2f, f+3g, f-3g$ étant premiers entre eux, et le nombre A étant une puissance d'un nombre premier, on ne peut avoir que l'une des décompositions suivantes :

$$2f = A\alpha^3, \quad f+3g = \beta^3, \quad f-3g = \gamma^3, \quad u = \alpha\beta\gamma,$$
$$2f = \alpha^3, \quad f \pm 3g = A\beta^3, \quad f \mp 3g = \gamma^3,$$

qui donnent respectivement les deux équations

$$A\alpha^3 = \beta^3 + \gamma^3, \quad A\beta^3 = \alpha^3 + (-\gamma)^3.$$

On vérifierait donc l'équation (1) en attribuant aux indéterminées des valeurs α, β, γ toutes inférieures à la valeur *minima* de $z = \alpha\beta\gamma . \nu$. L'hypothèse est donc impossible.

Puisqu'il n'y a pas de milieu entre ces deux hypothèses, z multiple de 3, ou z premier à 3, nous avons ce théorème :

THÉORÈME IV. — *Si nous désignons par p un nombre premier $18m+5$, et par q un nombre premier $18m+11$, aucun des nombres p, p^2, q, q^2 n'est décomposable en une somme de deux cubes rationnels.*

7. Considérons l'équation de Fermat $x^3 + y^3 = z^3$.

Comme z désigne l'un quelconque des trois nombres, nous pouvons le supposer impair. Puis, remarquant que la valeur $A = 1$ satisfait aux conditions du premier paragraphe, nous concluons du premier théorème que z est premier à 3, et du second, que l'un des deux nombres x ou y est multiple de 18. Nous avons donc

$$z^3 - x^3 = 2^3 . 9^3 u^3 \nu^3,$$

d'où

$$z - x = 2^3 . 3^5 u^3, \quad \left(\frac{z+x}{2}\right)^2 + 3\left(\frac{z-x}{6}\right)^2 = \nu^3 = F^2 + 3G^2.$$

En répétant le raisonnement employé au n° **2**, nous concluons que

$$\frac{z+x}{2} = F, \quad \frac{z-x}{6} = G, \quad \text{ou} \quad 2^2 . 3^4 u^3 = 3g(f^2 - g^2).$$

Or, les trois facteurs $g, f+g, f-g$ étant premiers entre eux, la dernière équation ne peut se décomposer que de l'une des manières suivantes :

$$g = 2^2 . 3^3 \alpha^3, \quad f+g = \beta^3, \quad f-g = \gamma^3,$$
$$g = 2^2 \alpha^3, \quad f \pm g = 3^3 \beta^3, \quad f \mp g = \gamma^3;$$

on en déduit respectivement les deux équations

$$\beta^3 - \gamma^3 = 2g = (2 . 3\alpha)^3$$
$$(3\beta)^3 - \gamma^3 = \pm 2g = (\pm 2\alpha)^3.$$

Or nous pouvons supposer que, dans la solution considérée, z est le plus petit des deux nombres impairs et qu'il a la plus petite valeur possible. Puisque nous déduisons de cette solution *minima* une autre solution en nombres tous inférieurs à $z = 18\alpha\beta\gamma . \nu$, nous concluons que l'équation est impossible. Donc :

THÉORÈME V. — *Aucun cube n'est égal à la somme de deux cubes.*

8. Supposons $A = 2^\mu a$, en désignant par μ l'un des nombres 1 ou 2, et par a l'un des nombres premiers p, q, ou de leurs carrés p^2, q^2.

Si $\mu = 1$, les valeurs de A sont respectivement des quatre formes $18m + (10, 4, 14, 8)$; le nombre z doit donc être multiple de 3 et même de 9. (Théorème III.)

Soit $\mu = 2$. Les nombres $4p$, $4q$, $4p^2$, $4q^2$ sont respectivement des quatre formes $18m + (2, 8, 10, 16)$; nous concluons donc du troisième théorème que, si A est l'un des nombres $4q$, $4p^2$, z doit être multiple de 9. Donc :

« 1° Si A désigne l'un des nombres $2p$, $2q$, $2p^2$, $2q^2$, $4q$, $4p^2$, l'équation (1) ne peut être résolue en nombres entiers qu'en faisant z multiple de 3. »

La décomposition en facteurs de l'équation (1) donne alors les équations (3) et (5), dont la dernière

$$\frac{x+y}{6} = \frac{Au^3}{18} = 3g(f^2 - g^2$$

devient

$$2^{\mu-1} a u_1^3 = g(f^2 - g^2)$$

en posant

$$u = 3u_1.$$

Cette équation se décompose nécessairement de l'une des manières suivantes :

$$g = 2^{\mu-1} a\alpha^3, \quad f + g = \beta^3, \quad f - g = \gamma^3,$$
$$g = 2^{\mu-1} \alpha^3, \quad f \pm g = a\beta^3, \quad f \mp g = \gamma^3;$$

et l'on obtient respectivement les deux équations

$$\beta^3 + (-\gamma)^3 = A\alpha^3, \quad \gamma^3 \pm 2^\mu \alpha^3 = a\beta^3.$$

La première n'est autre que l'équation (1) vérifiée en égalant les indéterminées à des diviseurs α, β, γ de la plus petite valeur possible de z; on doit donc la rejeter. Quant à la seconde, comme l'un des nombres α, β, γ est multiple de 3, elle donne l'une des congruences

$$2^\mu \pm 1 \equiv 0, \quad a \equiv \pm 1, \quad a \equiv \pm 2^\mu \pmod 9.$$

La première est impossible; la seconde l'est également lorsqu'on désigne par a l'un des nombres p, q, p^2, q^2, ainsi que nous le faisons. Pour la troisième, il faut distinguer les deux valeurs de μ. Si $\mu = 1$, le nombre a doit être de l'une des deux formes $18m + 11$, $18m + 7$, ce qui exclut les deux valeurs p, q^2. Si $\mu = 2$, a doit être de l'une des deux formes $18m + 13$, $18m + 5$, ce qui exclut p^2 et q. Donc :

2° « Si A désigne l'un des nombres $2p$, $2q^2$, $4q$, $4p^2$, l'équation (1) ne peut être vérifiée en faisant z multiple de 3. »

Si nous réunissons les deux conclusions 1° et 2°, nous avons ce théorème :

THÉORÈME VI. — *Aucun des nombres $2p$, $2q^2$, $4p^2$, $4q$ ne peut se décomposer en une somme de deux cubes rationnels.*

§ III.

9. Supposons $A = 3^{\lambda} 2^{\mu} a$, a désignant encore une puissance d'un nombre premier $6m - 1$, μ l'un des nombres 0, 1, 2, et λ l'un des nombres 1 ou 2.

1° Soit $\lambda = 1$. Comme la somme $x^3 + y^3$ ne peut être divisible par 3 sans l'être par 9, il faut que z soit multiple de 3, de telle sorte que l'équation (1) se décomposera de la manière suivante :

$$x + y = 27 \cdot 2^{\mu} a u^3, \quad x^2 - xy + y^2 = 3v^3, \quad z = 3uv.$$

On peut obtenir, dans ce cas, certaines conditions que les indéterminées doivent remplir, mais aucun caractère général d'impossibilité.

2° Soit $\lambda = 2$. L'équation (1) se décomposera de la manière suivante :

$$x + y = 3 \cdot 2^{\mu} a \cdot u^3, \quad x^2 - xy + y^2 = 3v^3, \quad z = uv, \quad f^2 + 3g^2 = v.$$

Supposons d'abord $\mu = 0$, et z impair. L'un des deux nombres x ou y devant être pair, nous ferons $y = 2t$. La seconde équation pourra s'écrire

$$\left(\frac{2x - y}{2}\right)^2 + 3\left(\frac{y}{2}\right)^2 = 3v^3, \quad \text{ou} \quad t^2 + 3\left(\frac{x - t}{3}\right)^2 = v^3 = F^2 + 3G^2;$$

et, en répétant le raisonnement que nous avons fait (n° **2**), nous concluons

$$t = F, \quad \frac{x - t}{3} = G = 3g(f^2 - g^2);$$

d'où

$$G + F = \frac{x + 2t}{3} = au^3.$$

Mais G est divisible par 9, tandis que $F \equiv f^3 \equiv \pm 1 \pmod 9$; donc l'équation précédente, réduite à une congruence suivant le module 9, devient

$$a \equiv \pm 1 \pmod 9.$$

Donc, « si le nombre a est de l'une des quatre formes p, q, p^2, q^2, l'équation

$$x^3 + y^3 = 9az^3$$

ne peut être vérifiée par aucune valeur impaire de z. »

10. Il résulte de là que, quel que soit μ, les deux nombres x et y sont nécessairement impairs, et que l'équation

$$x^2 - xy + y^2 = 3v^3$$

s'écrit de la manière suivante :

$$\left(\frac{x+y}{2}\right)^2 + 3\left(\frac{x-y}{2}\right)^2 = 3v^3, \quad \text{ou} \quad \left(\frac{x-y}{2}\right)^2 + 3\left(\frac{x+y}{6}\right)^2 = v^3 = F^2 + 3G^2.$$

Le raisonnement précédemment indiqué nous donnera

$$\frac{x-y}{2} = F, \quad \frac{x+y}{6} = \frac{2^\mu . a u^3}{2} = G = 3g(f^2 - g^2).$$

Décomposons de toutes les manières possibles la dernière équation, en remarquant que les trois facteurs $2g$, $f+g$, $f-g$ sont premiers entre eux; nous obtenons l'un des systèmes suivants :

$$\begin{aligned}
&2^\mu a\alpha^3 = 6g, \quad \beta^3 = f+g, \quad \gamma^3 = f-g,\\
&2^\mu \alpha^3 = 6g, \quad a\beta^3 = f \pm g, \quad \gamma^3 = f \mp g,\\
&2^\mu \alpha^3 = 2g, \quad \frac{a\beta^3}{3} = f \pm g, \quad \gamma^3 = f \mp g,\\
&2^\mu \alpha^3 = 2g, \quad a\beta^3 = f \pm g, \quad \frac{\gamma^3}{3} = f \mp g,\\
&2^\mu a\alpha^3 = 2g, \quad \frac{\beta^3}{3} = f \pm g, \quad \gamma^3 = f \mp g;
\end{aligned}$$

d'où l'on déduit respectivement ces cinq équations :

$$\begin{aligned}
9\cdot 2^\mu a\alpha_1^3 = \beta^3 + (-\gamma)^3, \quad \pm 9\cdot 2^\mu \alpha_1^3 = a\beta^3 - \gamma^3, \quad \pm 2^\mu \alpha^3 = 9a\beta_1^3 - \gamma^3,\\
\pm 2^\mu \alpha^3 = a\beta^3 - 9\cdot\gamma_1^3, \quad \pm 2^\mu a\alpha^3 = 9\beta_1^3 - \gamma^3,
\end{aligned}$$

dans lesquelles nous posons $3\alpha_1 = \alpha$, $3\beta_1 = \beta$, $3\gamma_1 = \gamma$.

La première équation doit être rejetée, parce qu'elle est de même

forme que l'équation proposée, et que les valeurs α_1, β, $-\gamma$ des indéterminées sont des diviseurs de la valeur minima de z. La seconde doit être aussi rejetée si a désigne l'un des nombres p, q, p^2, q^2, parce qu'elle se réduit à la congruence

$$a \mp 1 \equiv 0 \pmod 9,$$

qui est impossible dans cette hypothèse. La troisième doit être rejetée pour la même raison que la première si $\mu = 0$, et, dans le cas contraire, parce qu'elle donne la congruence impossible

$$2^\mu \equiv \pm 1 \pmod 9, \quad (\mu = 1 \text{ ou } 2).$$

Restent donc les deux dernières, qui se réduisent aux deux congruences

$$(B) \qquad 2^\mu \equiv \pm a \pmod 9, \quad 2^\mu a \equiv \pm 1 \pmod 9,$$

pour lesquelles il faut distinguer la valeur de μ. Quand $\mu = 0$, elles sont l'une et l'autre impossibles, si a est de l'une des quatre formes supposées p, q, p^2, q^2. Donc :

THÉORÈME VII. — *Aucun des nombres* $9p$, $9q$, $9p^2$, $9q^2$ *ne peut se décomposer en une somme de deux cubes rationnels.*

Dans le cas où μ est égal à l'un des nombres 1 ou 2, les congruences (B) n'excluent que les deux formes $18m + (1, 17)$. Mais il faut nous rappeler que, si le nombre a est de l'une de ces deux formes, la seconde décomposition cesse d'être impossible. Ainsi la considération du facteur 2 ne fournit aucun caractère d'impossibilité.

§ IV.

11. On reconnaît aisément, au moyen du théorème de Fermat $a^5 - a \equiv 0 \pmod 5$, que le produit

$$fg(f^2 + g^2)(f^2 - g^2)$$

est toujours multiple de 5; d'où nous pouvons conclure que l'un des

deux nombres

$$f(f^2 - 9g^2), \quad 3g(f^2 - g^2)$$

est nécessairement divisible par 5. Dès lors nous pouvons espérer que la considération de ce diviseur fournira quelques caractères d'impossibilité pour l'équation (1), dans le cas où A sera multiple de 5. Soit donc $A = 5^\mu a$, a désignant une puissance d'un nombre premier $6m - 1$. Le premier théorème (§ I) nous apprend que, si l'équation

$$x^3 + y^3 = 5^\mu a z^3 \tag{1}$$

est possible en nombres entiers, le nombre z ne peut être impair sans être premier à 3; d'où l'on déduit aisément que z doit être pair.

En effet, si l'on suppose que z est impair et premier à 3, l'équation (1) conduit aux équations (2) et (6). Or l'équation

$$x + y = f(f^2 - 9g^2) + 9g(f^2 - g^2) = 5^\mu a u^3 = F + 3G$$

est évidemment impossible, puisque des deux nombres premiers entre eux, F, G, l'un est multiple de 5.

Soit donc z pair. Et d'abord supposons z premier à 3. La décomposition de l'équation (1) donnera les équations (2) et (4). Or l'équation

$$5^\mu a u^3 = 2f(f^2 - 9g^2),$$

dans laquelle $2f$, $f + 3g$, $f - 3g$ sont des nombres premiers entre eux, se décompose nécessairement de l'une des manières suivantes :

$$\begin{aligned}
5^\mu a\alpha^3 &= 2f, \quad f + 3g = \beta^3, \quad f - 3g = \gamma^3,\\
5^\mu \alpha^3 &= 2f, \quad f \pm 3g = a\beta^3, \quad f \mp 3g = \gamma^3,\\
a\alpha^3 &= 2f, \quad f \pm 3g = 5^\mu \beta^3, \quad f \mp 3g = \gamma^3,\\
\alpha^3 &= 2f, \quad f \pm 3g = 5^\mu a\beta^3, \quad f \mp 3g = \gamma^3,\\
\alpha^3 &= 2f, \quad f \pm 3g = a\beta^3, \quad f \mp 3g = 5^\mu \gamma^3.
\end{aligned}$$

On en déduit respectivement les cinq équations :

$$\begin{aligned}
&\beta^3 + \gamma^3 = 5^\mu a\alpha^3, \quad 5^\mu \alpha^3 = a\beta^3 + \gamma^3, \quad a\alpha^3 = 5^\mu \beta^3 + \gamma^3,\\
&\alpha^3 - \gamma^3 = 5^\mu a\beta^3, \quad \alpha^3 = a\beta^3 + 5^\mu \gamma^3.
\end{aligned}$$

La première et la quatrième doivent être rejetées, parce qu'elles donnent une solution de l'équation (1), dans laquelle les indéterminées sont égalées à trois diviseurs de la valeur *minima* de z, ce qui est absurde. Quant aux trois autres, elles se ramènent à l'équation unique

$$(C) \qquad a\alpha^3 + 5^\mu\beta^3 + \gamma^3 = 0,$$

dans laquelle on doit supposer $\alpha\beta\gamma$ premier à 3.

12. Soit z multiple de 3, et posons $z = 3uv$. L'équation (1) donnera les équations (2) et (5), dont l'une

$$\frac{x+y}{6} = \frac{5^\mu.3au^3}{2} = 3g(f^2 - g^2)$$

donne

$$5^\mu au^3 = 2g(f^2 - g^2).$$

En décomposant cette équation, comme nous avons fait pour l'équation analogue du numéro précédent, et en excluant les décompositions qui ramènent l'équation proposée vérifiée par des diviseurs de la valeur *minima* de z, on trouve que toutes les autres décompositions donnent une équation de la forme

$$(C) \qquad a\alpha^3 + 5^\mu\beta^3 + \gamma^3 = 0,$$

dans laquelle on peut supposer l'un des nombres α, β, γ divisible par 3. En rapprochant ce résultat du précédent, nous concluons que l'équation (1) est impossible pour la valeur $A = 5^\mu a$, si le nombre a désigne une puissance d'un nombre premier $6m - 1$, et qu'en même temps il rende impossible l'équation (C).

13. Soit $\mu = 1$, et réduisons l'équation (C) à une congruence suivant le module 9. En ayant toujours égard à la congruence $m^3 \equiv \pm 1 \pmod 9$, si m est premier à 3, nous obtenons, suivant les différentes hypothèses possibles, l'une des quatre congruences

$$a \pm 5 \pm 1 \equiv 0, \quad 5 \pm 1 \equiv 0, \quad a \equiv \pm 1, \quad a \equiv \pm 5 \pmod 9.$$

La seconde est impossible; les trois autres exigent que a soit de

l'une des formes

$$9m + (\pm 5, \pm 1, \pm 4, \pm 6).$$

Comme a est premier à 3, il faut exclure la dernière forme; la première et la troisième rentrent l'une dans l'autre, de telle sorte qu'il ne reste que les formes

$$9m + (1, 4, 5, 8),$$

ce qui exclut les deux formes $9m + (2, 7)$, et par suite les valeurs q et p^2 de a.

THÉORÈME VIII. — *Aucun des nombres représentés par les formules* $5q$, $5p^2$ *n'est décomposable en une somme de deux cubes rationnels.*

14. Soit $\mu = 2$, et supposons $a = 18m + 5$, c'est-à-dire $a = p$ ou $a = q^2$.

L'équation (C) devient

$$a\alpha^3 + 25\beta^3 + \gamma^3 = 0,$$

et se ramène, par rapport au module 9, à l'une des quatre congruences

$$5 \pm 2 \pm 1 \equiv 0, \quad \pm 2 \pm 1 \equiv 0, \quad \pm 2 \pm 5 \equiv 0, \quad \pm 5 \pm 1 \equiv 0 \pmod 9,$$

qui sont toutes impossibles. Donc :

THÉORÈME IX. — *Aucun des nombres compris dans les deux formules* $25p$, $25q^2$ *n'est décomposable en une somme de deux cubes rationnels.*

Si nous avons égard à l'observation, faite dès l'introduction de ce Mémoire, que l'impossibilité de décomposer en deux cubes rationnels un nombre p^α entraîne la même impossibilité pour le nombre $p^{3m+\alpha}$, quel que soit d'ailleurs le nombre entier et positif m, nous pouvons réunir les résultats obtenus jusqu'ici dans le théorème général :

THÉORÈME X. — *Si l'on désigne par* p *et* q *deux nombres premiers compris respectivement dans les formes linéaires* $18m + 5$, $18m + 11$,

et par m un nombre entier et positif quelconque, aucun des nombres compris dans les formules suivantes :

$$p^m,\quad q^m,\quad 2p^{3m+1},\quad 2q^{3m+2},\quad 4p^{3m+2},\quad 4q^{3m+1},$$
$$9p^{3m+1},\quad 9q^{3m+1},\quad 9p^{3m+2},\quad 9q^{3m+2},\quad 5p^{3m+2},\quad 5q^{3m+1},\quad 25p^{3m+1},\quad 25q^{3m+2},$$

n'est décomposable en une somme de deux cubes rationnels.

Pour épargner un travail inutile à ceux qui voudraient faire des recherches sur le même sujet, j'ajouterai quelques observations.

1° On chercherait vainement à prouver l'impossibilité de décomposer en deux cubes rationnels les nombres premiers $(18m+17)$, ou les produits de ces nombres multipliés par une puissance de 2 ou de 3; car on a

$$17 = \left(\frac{18}{7}\right)^3 - \left(\frac{1}{7}\right)^3,$$
$$2\times 17 = \left(\frac{631}{182}\right)^3 - \left(\frac{359}{182}\right)^3,$$
$$4\times 17 = \left(\frac{2538163}{620505}\right)^3 - \left(\frac{472663}{620505}\right)^3,$$
$$3\times 17 = \left(\frac{730511}{197028}\right)^3 + \left(\frac{62641}{197028}\right)^3,$$
$$9\times 17 = \left(\frac{70}{13}\right)^3 - \left(\frac{19}{13}\right)^3.$$

2° On ne trouvera pas non plus de théorème du même genre pour les nombres premiers $6m+1$: tous ces nombres sont compris dans la forme quadratique

$$A^2 + 3B^2,$$

et il résulte des formules données par Lamé, dans son étude *Sur les binômes cubiques* (*Comptes rendus des séances de l'Académie des Sciences*, t. LXI, p. 924), que le nombre A^2+3B^2 est la somme de deux cubes rationnels, toutes les fois que l'un des trois nombres $2A$, $3B\pm A$ est un cube, ou que l'un des trois nombres $2B$, $A\pm B$ est le triple d'un cube.

3° On ne sera pas dans de meilleures conditions si l'on considère

le produit d'un nombre premier $6m+1$ par une puissance de 5; car si le nombre a est compris dans l'une des formules suivantes :

$$(4\times 5^{\mu}m^3)^2+3l^2,\quad l^2+3(12\times 5^{\mu}m^3)^2,$$
$$(5^{\mu}m^3\pm 3l)^2+3l^2,\quad (3\times 5^{\mu}m^3\pm l)^2+3l^2,$$

le produit $5^{\mu}a$ est décomposable en deux cubes rationnels.

4° Quant aux nombres composés, la probabilité de leur décomposition en deux cubes rationnels augmente avec le nombre des facteurs. Par une méthode différente de celle qui a été suivie dans ce Mémoire, on peut obtenir les deux théorèmes suivants :

THÉORÈME XI. — *Le double d'un nombre triangulaire quelconque est toujours décomposable en deux cubes rationnels.*

Ainsi les doubles des nombres triangulaires compris dans la première centaine sont

$$2,\quad 6,\quad 12,\quad 20,\quad 30,\quad 42,\quad 56,\quad 72,\quad 90;$$

or on a

$$2=1^3+1^3,\qquad 6=\left(\frac{17}{21}\right)^3+\left(\frac{37}{21}\right)^3,\qquad 12=\left(\frac{19}{39}\right)^3+\left(\frac{89}{39}\right)^3,$$
$$20=\left(\frac{19}{7}\right)^3+\left(\frac{1}{7}\right)^3,\qquad 30=\left(\frac{107}{57}\right)^3+\left(\frac{163}{57}\right)^3,\qquad 42=\left(\frac{449}{129}\right)^3-\left(\frac{71}{129}\right)^3,$$
$$56=\left(\frac{73}{19}\right)^3-\left(\frac{17}{19}\right)^3,\qquad 72=(4)^3+(2)^3,\qquad 90=\left(\frac{12241}{273}\right)^3-\left(\frac{431}{273}\right)^3.$$

Ce théorème est lui-même compris dans un théorème plus général :

THÉORÈME XII. — *Tout nombre composé de deux facteurs, dont la somme ou la différence est égale à un cube, est lui-même la somme de deux cubes rationnels.*

Par exemple, on a

$$8=1+7=2+6=3+5=4+4=10-2=11-3=12-4,\ldots$$

Or chacun des produits

$$1\times 7,\quad 2\times 6,\quad 3\times 5,\quad 16,\quad 20,\quad 33,\quad 48,\quad 65,\quad 84,\ldots$$
$$30..$$

est décomposable en deux cubes rationnels. En omettant les décompositions évidentes et celles qui ont été données plus haut, on a

$$15 = \left(\frac{683}{294}\right)^3 + \left(\frac{397}{294}\right)^3, \quad 33 = \left(\frac{1853}{582}\right)^3 + \left(\frac{523}{582}\right)^3,$$
$$48 = \left(\frac{74}{21}\right)^3 + \left(\frac{34}{21}\right)^3, \quad 84 = \left(\frac{433}{111}\right)^3 + \left(\frac{323}{111}\right)^3, \ldots.$$

De même on a

$$3^3 = 25 + 2 = 24 + 3 = 23 + 4 = \ldots = 29 - 2 = 30 - 3 \ldots;$$

chacun des produits

$$25 \times 2, \quad 24 \times 3, \quad 23 \times 4, \quad 22 \times 5, \quad 21 \times 6, \quad 20 \times 7,$$
$$19 \times 8, \quad 18 \times 9, \quad 17 \times 10, \ldots, \quad 29 \times 2, \quad 30 \times 3, \ldots$$

est décomposable en deux cubes rationnels. On a

$$50 = \left(\frac{23417}{6111}\right)^3 - \left(\frac{11267}{6111}\right)^3, \quad 23 \times 4 = \left(\frac{25903}{5733}\right)^3 - \left(\frac{3547}{5733}\right)^3,$$
$$22 \times 5 = \left(\frac{26693}{5571}\right)^3 + \left(\frac{37}{5571}\right)^3, \quad 21 \times 6 = \left(\frac{27189}{5427}\right)^3 + \left(\frac{3429}{5427}\right)^3,$$
$$20 \times 7 = \left(\frac{27397}{5301}\right)^3 + \left(\frac{6623}{5301}\right)^3, \quad 19 \times 8 = \left(\frac{16}{3}\right)^3 + \left(\frac{2}{3}\right)^3,$$
$$18 \times 9 = \left(\frac{17}{7}\right)^3 + \left(\frac{37}{7}\right)^3, \quad 17 \times 10 = \left(\frac{26353}{5031}\right)^3 + \left(\frac{14957}{5031}\right)^3,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots, \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$29 \times 2 = \left(\frac{28747}{9 \times 787}\right)^3 - \left(\frac{14653}{9 \times 787}\right)^3, \quad 30 \times 3 = \left(\frac{1241}{273}\right)^3 - \left(\frac{431}{273}\right)^3, \ldots.$$