JOURNAL DE MATHÉMATIQUES PURES ET APPLIQUÉES

LAMÉ

Mémoire d'analyse indéterminée, démontrant que l'équation $x^7 + y^7 = z^7$ est impossible en nombres entiers.

Journal de mathématiques pures et appliquées 1re série, tome 5 (1840), p. 195-210.

<http://portail.mathdoc.fr/JMPA/afficher_notice.php?id=JMPA_1840_1_5_A21_0>

MÉMOIRE D'ANALYSE INDÉTERMINÉE,

Démontrant que l'équation $x^7 + y^7 = z^7$ est impossible en nombres entiers;

PAR G. LAMÉ.

De tous les théorèmes sur les nombres, énoncés par Fermat, un seul reste incomplétement démontré. Ce théorème dit que l'équation $x^n + y^n = z^n$ est impossible en nombres entiers, lorsque l'exposant n est plus grand que 2. Euler a démontré cette impossibilité pour $n = 3$, et par suite pour tout multiple de 3, $(n = 3i)$; Fermat lui-même pour $n = 4$, $(n = 4i)$; M. Dirichlet pour $n = 14$, $(n = 14i)$; enfin Legendre, en complétant un travail de M. Dirichlet, pour $n = 5$, $(n = 5i)$.

Je me propose dans ce Mémoire d'établir la même impossibilité pour $n = 7$, et conséquemment aussi pour tous les multiples de 7, impairs et non divisibles par 3 ou 5, les seuls qui ne rentrent pas dans les cas précédemment traités. Je présente ici cette démonstration sans recourir à aucune théorie étrangère, et sans m'appuyer sur les propriétés secondaires que Legendre a réunies dans le second supplément à la première édition de sa *Théorie des Nombres*. Tous les lemmes nécessaires à cette démonstration particulière sont démontrés directement, et uniquement en vue du nombre 7.

§ I.

Si l'équation $x^7 + y^7 = z^7$ est possible en nombres entiers, on peut supposer l'existence d'une solution pour laquelle x, y, z n'auraient aucun facteur commun; car, si Δ représente le plus grand commun diviseur entre trois nombres Δx, Δy, Δz, qui vérifient l'équation proposée, on pourra diviser l'identité $(\Delta x)^7 + (\Delta y)^7 = (\Delta z)^7$ par Δ^7, et l'on aura l'équation

$$(1) \qquad x^7 + y^7 = z^7,$$

dans laquelle x, y, z, ne peuvent plus être divisibles tous les trois par un même nombre. Alors x, y, z, sont nécessairement premiers deux à deux, car un facteur premier δ ne pourrait diviser deux de ces nombres sans diviser le troisième.

Des trois nombres x, y, z, un est nécessairement pair, et les deux autres impairs. Il serait possible qu'aucun d'eux ne fût divisible par 7 : car les nombres premiers avec 7 étant compris dans les six formes $7i \pm 1, \pm 2, \pm 3$, leurs septièmes puissances le sont dans celles-ci : $49i \pm 1, \pm 19, \pm 18$, et la somme de trois des six restes $\pm 1, \pm 19, \pm 18$, peut être nulle. Ainsi, il y a lieu de considérer deux cas différents : 1° celui où 7 ne divise ni x, ni y, ni z; 2° celui où 7 divise un de ces nombres.

Premier cas.

§ II.

L'équation proposée (1) étant mise successivement sous les trois formes

$$\begin{cases} x^7 = (z-y)[(z-y)^6 + 7y(z-y)^5 + 3.7y^2(z-y)^4 + 5.7y^3(z-y)^3 + 5.7y^4(z-y)^2 + 3.7y^5(z-y) + 7y^6] = (z-y)X \\ y^7 = (z-x)[(z-x)^6 + 7x(z-x)^5 + 3.7x^2(z-x)^4 + 5.7x^3(z-x)^3 + 5.7x^4(z-x)^2 + 3.7x^5(z-x) + 7x^6] = (z-x)Y \\ z^7 = (x+y)[(x+y)^6 - 7y(x+y)^5 + 3.7y^2(x+y)^4 - 5.7y^3(x+y)^3 + 5.7y^4(x+y)^2 - 3.7y^5(x+y) + 7y^6] = (x+y)Z \end{cases}$$

X et $(z-y)$, ou Y et $(z-x)$, ou Z et $(x+y)$ ne pourraient avoir d'autre facteur premier commun que 7; car δ, nombre premier, divisant X et $(z-y)$, ou Y et $(z-x)$, ou Z et $(x+y)$, diviserait $7y^6$ et $(z-y)$, ou $7x^6$ et $(z-x)$, ou $7y^6$ et $(x+y)$; et si δ était autre que 7, il diviserait y et $(z-y)$, d'où y et z, ou x et $(z-x)$, d'où x et z, ou y et $(x+y)$, d'où y et x. Mais dans le cas actuel, x, y, z sont tous les trois premiers avec 7; donc les six nombres X, $(z-y)$, Y, $(z-x)$, Z, $(x+y)$, sont tous premiers entre eux. Ce qui conduit aux trois décompositions suivantes :

$$(3) \quad \begin{cases} x = m\mu, & X = m^7, & z - y = \mu^7; \\ y = n\nu, & Y = n^7, & z - x = \nu^7; \\ z = p\rho, & Z = p^7, & x + y = \rho^7; \end{cases}$$

les six nombres m, μ, n, ν, p, ρ, étant premiers entre eux.

Les équations (3) donnent aisément

$$x+y-z=\mu(m-\mu^6)=\nu(n-\nu^6)=\rho(\rho^6-p).$$

La valeur commune des trois derniers produits étant divisible séparément par μ, par ν, par ρ, facteurs premiers entre eux, le sera nécessairement par le produit de ces facteurs, et l'on pourra poser

$$(4)\qquad \mu(m-\mu^6)=\nu(n-\nu^6)=\rho(\rho^6-p)=\mathrm{A}\mu\nu\rho=x+y-z;$$

A étant un nombre entier. On déduit de là

$$(5)\qquad m=\mu^6+\mathrm{A}\nu\rho,\quad n=\nu^6+\mathrm{A}\rho\mu,\quad p=\rho^6-\mathrm{A}\mu\nu.$$

D'où il suit que le nombre A est premier avec μ, ν, ρ; car si A et μ, par exemple, avaient un facteur premier commun δ, m serait divisible par δ, d'après la première (5); m et μ ne seraient donc pas premiers entre eux. Par la même raison, A est premier avec m, n, p; ainsi A est premier avec x, y, z. Les groupes (4) et (5) donnent successivement

$$\mathrm{A}\mu\nu\rho=x+y-z=m\mu+n\nu-p\rho=\mu^7+\nu^7-\rho^7+3\mathrm{A}\mu\nu\rho:$$

ce qui donne la relation

$$(6)\qquad \rho^7-\nu^7-\mu^7=2\mathrm{A}\mu\nu\rho.$$

§ III.

La troisième colonne du groupe (3) conduit aux valeurs suivantes

$$2x=\mu^7-\nu^7+\rho^7,\quad 2y=-\mu^7+\nu^7+\rho^7,\quad 2z=\mu^7+\nu^7+\rho^7,$$

qui transforment ainsi l'équation (1)

$$(7)\qquad (\mu^7-\nu^7+\rho^7)^7+(-\mu^7+\nu^7+\rho^7)^7=(\mu^7+\nu^7+\rho^7)^7.$$

Mais on a généralement, comme il est facile de le vérifier par le développement des puissances indiquées,

$$(8)\qquad \begin{cases}(c+b+a)^7-(c-b+a)^7-(c+b-a)^7+(c-b-a)^7=\\ =7.8abc\,[3(a^4+b^4+c^4)+10(a^2b^2+c^2a^2+b^2c^2)];\end{cases}$$

si donc on pose, pour simplifier,

$$(9)\qquad \mu^7 = a, \quad \nu^7 = b, \quad \rho^7 = c,$$

l'équation (8) est réduite par celle (7) à

$$(10)\quad (c-b-a)^7 = 7.8abc\,[3(a^4+b^4+c^4)+10(a^2b^2+c^2a^2+b^2c^2)];$$

et l'équation (6) donnant

$$c-b-a = 2A\mu\nu\rho, \text{ et } (c-b-a)^7 = 2^7A^7abc,$$

cette valeur substituée, l'équation (10) devient

$$(11)\quad 2^4A^7 = 7[3(a^4+b^4+c^4)+10(a^2b^2+c^2a^2+b^2c^2)];$$

d'où l'on voit que A est nécessairement divisible par 7.

L'équation (11), combinée avec celle (6), démontre que A est essentiellement un carré. Voici comment s'établit cette propriété, importante pour la question actuelle.

Si l'on résout l'équation (11) par rapport à a^2, il vient

$$3a^2 = -5(b^2+c^2) + 2\sqrt{4b^4+5b^2c^2+4c^4+\tfrac{3}{7}2^2A^7};$$

la quantité soumise au radical devant être un carré φ^2, si l'on pose, pour simplifier, $b^2+c^2 = \psi$, on aura

$$(12)\qquad 3a^2 = 2\varphi - 5\psi, \quad \tfrac{12}{7}A^7 = \varphi^2 + 3b^2c^2 - 4\psi^2;$$

mais l'équation (6) donne, en désignant par P le produit $\mu\nu\rho$,

$$a = c-b-2AP, \quad a^2 = \psi - 2cb - 4AP(c-b-AP),$$

ou simplement, en remarquant que $c-b-AP = a+AP = x$,

$$a^2 = \psi - 2cb - 4APx;$$

cette valeur de a^2 substituée dans la première des équations (12) donne $\varphi = 4\psi - 3cb - 6APx$. Enfin cette valeur de φ transforme facilement la seconde équation (12) dans la suivante :

$$(13)\quad A[\tfrac{1}{7}A^6 + Px(4\psi - 3cb - 3APx)] = (\psi - cb)^2 = (b^2-cb+c^2)^2.$$

Or, dans le premier membre, A est premier avec la parenthèse; car un facteur premier δ, qui diviserait A et cette parenthèse, diviserait le produit $Px(4\psi - 3cb)$. Mais A est premier avec P et avec x; δ diviserait donc $(4\psi - 3cb)$; divisant le second membre de l'équation (13), ou $(\psi - cb)$, δ diviserait $(4\psi - 3cb) - 4(\psi - cb) = cb = \rho^7\nu^7$, c'est-à-dire ρ ou ν, qui ne doivent avoir aucun facteur commun avec A. D'après cela, l'équation (13) ne pourra se décomposer que de la manière suivante :

$$(14)\quad b^2 - cb + c^2 = BG,\quad A = B^2,\quad \tfrac{1}{7}A^6 + Px(4\psi - 3cb - 3APx) = G^2,$$

B et G étant des nombres premiers entre eux. *Ainsi* A *est un carré.* Soit pris $D = G - 2BPa$; la première des équations (14), combinée avec la relation (6), devient alors

$$(15)\qquad a^2 + b^2 + c^2 - bc - ca + ab = BD.$$

§ IV.

Si l'on réunit les équations (6), (15) et (11), on formera le groupe suivant :

$$(16)\quad \begin{cases} abc = P^7; \\ c - a - b = 2B^2P; \\ a^2 + b^2 + c^2 - bc - ca + ab = BD; \\ 3(a^4 + b^4 + c^4) + 10(a^2b^2 + c^2a^2 + b^2c^2) = \tfrac{16}{7}B^{14}. \end{cases}$$

Il s'agit d'éliminer a, b, c, entre ces quatre équations, afin d'obtenir une équation finale entre les trois nombres B, D, P. La seconde (16), élevée au carré et combinée avec la troisième, donne

$$a^2 + b^2 + c^2 = 2BD - 4B^4P^2,\qquad -bc - ca + ab = 4B^4P^2 - BD;$$

d'où il est facile de conclure successivement, par l'élévation au carré, et en ayant égard aux deux premières (16),

$$a^4 + b^4 + c^4 + 2(b^2c^2 + c^2a^2 + a^2b^2) = (2BD - 4B^4P^2)^2,$$
$$b^2c^2 + c^2a^2 + a^2b^2 = (4B^4P^2 - BD)^2 - 4B^2P^8.$$

Enfin ces valeurs substituées dans la quatrième (16), donnent pour l'équation finale cherchée,

$$\tfrac{16}{7}B^{14} = 3(2BD - 4B^4P^2)^2 + 4(4B^4P^2 - BD)^2 - 16B^2P^8.$$

Si l'on développe les carrés indiqués dans le second membre, cette dernière équation devient divisible par $16B^2$, et peut s'écrire ainsi

$$(17)\qquad 7\left(\frac{B^6}{7}\right)^2 + P^8 = D^2 - 5B^3P^2D + 7B^6P^4;$$

B est divisible par 7, comme on l'a vu (§ III); ainsi $\frac{B^6}{7}$ est un nombre entier.

§ V.

On établit facilement que $P = \mu\nu\rho$ est un nombre pair; en effet, l'équation $x + y - z = AP$ exige que AP soit divisible par 2, puisque des trois nombres x, y, z, un seul est pair et les deux autres sont impairs; or A ne saurait être divisible par 2, qui divise ou x, ou y, ou z, avec lesquels A doit être premier; donc 2 divisera P, c'est-à-dire l'un des trois nombres μ, ν, ρ; et A ou B^2, et par suite B sera un nombre impair. D'ailleurs un des trois nombres μ, ν, ρ, ou des trois autres $a = \mu^7$, $b = \nu^7$, $c = \rho^7$, étant pair, le premier membre de la troisième équation (16) est essentiellement impair, d'où il suit que non-seulement B, mais aussi D est impair.

Il résulte de là que l'équation (17) est impossible en nombres entiers, avec ces conditions; car elle peut se mettre sous la forme

$$P^2(7B^6P^2 - 5B^3D - P^6) = 7\left(\frac{B^6}{7}\right)^2 - D^2,$$

et le premier membre, étant divisible par P^2, est de la forme $4i$, puisque P est pair; tandis que les carrés de nombres impairs $\left(\frac{B^6}{7}\right)^2$ et D^2 étant de la forme $(8n+1)$, le second membre sera de la forme $(8n+6)$ ou $(4i+2)$. Il résulte de l'incompatibilité de ces deux formes, que l'équation (17) est impossible avec les conditions imposées aux nombres B, D, P; et par conséquent que l'équation (1) ne saurait être satisfaite par des nombres entiers x, y, z, sans que 7 soit facteur de l'un de ces nombres.

Deuxième cas.

§ VI.

L'un des nombres x, y, z, est divisible par 7. L'équation (1) peut toujours être mise sous les trois formes (2). Si 7 divise x, il divisera sept fois x^7, ne pourra diviser X qu'une seule fois, puisqu'il ne divise pas y, et divisera six fois $(z-y)$; les nombres $(z-x)$, Y, $(x+y)$, Z, seront premiers entre eux; on aura ainsi les trois décompositions

$$(18)\qquad \left\{\begin{array}{lll} x = 7m\mu, & X = 7m^7, & z-y = 7^6\mu^7 = a; \\ y = n\nu, & Y = n^7, & z-x = \nu^7 = b; \\ z = p\rho, & Z = p^7, & x+y = \rho^7 = c; \end{array}\right.$$

et l'on déduira de ce groupe, comme de celui (3), les conséquences suivantes :

$$(19)\qquad \left\{\begin{array}{c} x+y-z = 7\mu(m-7^5\mu^6) = \nu(n-\nu^6) = \rho(\rho^6-p) = 7\mathrm{A}\mu\nu\rho = 7\mathrm{AP}; \\ m = 7^5\mu^6 + \mathrm{A}\nu\rho, \qquad n = \nu^6 + 7\mathrm{A}\rho\mu, \quad p = \rho^6 - 7\mathrm{A}\mu\nu; \\ 7\mathrm{AP} = x+y-z = 7m\mu + n\nu - p\rho = 7^6\mu^7 + \nu^7 - \rho^7 + 3.7\mathrm{AP}; \\ c-a-b = 2.7\mathrm{AP}. \end{array}\right.$$

A est un nombre entier, nécessairement premier avec 7P; car 7 ne pourrait diviser A sans diviser m, d'où il suivrait que $\mathrm{X} = 7m^7$ contiendrait plus d'une fois le facteur 7; et un facteur premier δ ne pourrait diviser à la fois A et μ, ou ν, ou ρ, sans diviser aussi m, ou n, ou p, d'où il suivrait que les nombres m, μ, n, ν, p, ρ, ne seraient pas premiers entre eux. Par la même raison, A est premier avec m, n, p, et par suite avec x, y, z; d'où il suit que A est impair, car 2 divise l'un des nombres x, y, z; or 7AP est pair comme $x+y-z$, donc $\mathrm{P} = \mu\nu\rho$ est pair, c'est-à-dire que l'un des trois nombres μ, ν, ρ, est divisible par 2, tandis que m, n, p, restent tous les trois impairs.

On déduit encore du groupe (18), troisième colonne,

$$2x = c-b+a, \quad 2y = c+b-a, \quad 2z = c+b+a,$$

ce qui transforme l'équation (1) en celle-ci,

$$(c+b+a)^7 - (c-b+a)^7 - (c+b-a)^7 = 0,$$

et la formule générale (8) se réduit encore à celle (10). Or on a actuellement $7abc = (7\mu\nu\rho)^7$, et $c - b - a = 2.7\mathrm{A}\mu\nu\rho$; la substitution de ces valeurs dans la formule (10) donne, en supprimant le facteur commun $(7\mu\nu\rho)^7$,

$$2^4\mathrm{A}^7 = 3(a^4 + b^4 + c^4) + 10(b^2c^2 + c^2a^2 + a^2b^2). \tag{20}$$

Si 7 divisait z, et non x, le groupe (18) serait remplacé par celui-ci

$$\left\{\begin{array}{lll} x = m\mu, & \mathrm{X} = m^7, & z - y = \mu^7 = a; \\ y = n\nu, & \mathrm{Y} = n^7, & z - x = \nu^7 = b; \\ z = 7p\rho, & \mathrm{Z} = 7p^7, & x + y = 7^6\rho^7 = c; \end{array}\right. \tag{18 bis}$$

et les formules (19) deviendraient

$$\left\{\begin{array}{l} x + y - z = \mu(m - \mu^6) = \nu(n - \nu^6) = 7\rho(7^5\rho^6 - p) = 7\mathrm{A}\mu\nu\rho = 7\mathrm{AP}; \\ \qquad m = \mu^6 + 7\mathrm{A}\nu\rho, \quad n = \nu^6 + 7\mathrm{A}\rho\mu, \quad p = 7^5\rho^6 - \mathrm{A}\mu\nu; \\ 7\mathrm{AP} = x + y - z = m\mu + n\nu - 7p\rho = \mu^7 + \nu^7 - 7^6\rho^7 + 3.7\mathrm{AP}; \end{array}\right. \tag{19 bis}$$

on démontrerait de la même manière que le nombre entier A est premier avec μ, ν, 7ρ, m, n, p, x, y, z, et conséquemment impair, tandis que P est pair. Enfin la relation de même forme $c - a - b = 2.7\mathrm{AP}$, et les valeurs de $2x$, $2y$, $2z$, déduites de la troisième colonne (18 *bis*), conduiraient de la même manière à l'équation (20).

Ainsi, quel que soit celui des trois nombres x, y, z, que 7 divise, l'équation (20) subsiste; A étant toujours le nombre qui vérifie l'équation

$$c - b - a = 2.7\mathrm{AP} = 2.7\mathrm{A}\mu\nu\rho; \tag{21}$$

les valeurs de c, b, a, étant

$$\left\{\begin{array}{llll} a = 7^6\mu^7, & b = \nu^7, & c = \rho^7, & \text{si 7 divise } x; \\ a = \mu^7, & b = 7^6\nu^7, & c = \rho^7, & \text{si 7 divise } y; \\ a = \mu^7, & b = \nu^7, & c = 7^6\rho^7, & \text{si 7 divise } z; \end{array}\right. \tag{22}$$

et l'on a, dans tous les cas,

$$\left\{\begin{array}{l} 7abc = (7\mu\nu\rho)^7 = 7^7\,\mathrm{P}^7; \\ x = a + 7\mathrm{AP}, \quad y = b + 7\mathrm{AP}, \quad z = c - 7\mathrm{AP}. \end{array}\right. \tag{23}$$

§ VII.

Si l'on résout l'équation (20) par rapport à a^2, il vient

$$3a^2 = -5(b^2+c^2) + 2\sqrt{4b^4+5c^2b^2+4c^4+12A^7},$$

et le radical devant être un nombre entier φ, on aura, en posant $b^2+c^2=\psi$,

$$(24)\qquad 3a^2 = 2\varphi - 5\psi,\quad 12A^7 = \varphi^2 + 3b^2c^2 - 4\psi^2.$$

Mais l'équation (21) donne

$$a = c - b - 2.7AP,\quad a^2 = \psi - 2bc - 4.7AP(c-b-7AP),$$

ou, comme $\qquad c - b - 7AP = a + 7AP = x,$

plus simplement $\qquad a^2 = \psi - 2bc - 4.7APx;$

cette valeur de a^2, substituée dans la première (24), donne

$$\varphi = 4\psi - 3bc - 6.7APx;$$

enfin cette valeur de φ, substituée dans la dernière (24), la rend divisible par 12; et le résultat, mettant A comme facteur, est

$$(25)\quad A[A^6 + 7Px(4\psi - 3bc - 3.7APx)] = (\psi - bc)^2 = (b^2 - bc + c^2)^2.$$

Si A, premier avec 7P et avec x, et divisant $(\psi - bc)^2$, avait un facteur premier δ commun avec la parenthèse, qu'il multiplie dans le premier membre de l'équation (25), δ diviserait $(4\psi - 3bc)$ et $(\psi - bc)$, par suite bc, conséquemment b ou c, ν ou ρ; A ne serait donc pas premier avec 7P. Donc le seul moyen de décomposer l'équation (25) est celui-ci :

$$(26)\quad b^2 - bc + c^2 = BG,\quad A = B^2,\quad A^6 + 7Px(4\psi - 3bc - 3.7APx) = G^2:$$

B et G étant deux nombres premiers entre eux, et tous les deux impairs, car $(b^2 - bc + c^2)$ est toujours impair, que l'un des deux nombres b et c soit pair, ou qu'ils soient tous les deux impairs, seuls cas possibles. Il est donc démontré que A *est un carré*. Soit pris $D = G - 2.7BPa$, d'où $G = D + 2.7BPa$, la première (26) devient

$$b^2 - bc + c^2 = BD + 2.7B^2Pa = BD + a(c - b - a),$$

ou bien

$$a^2 + b^2 + c^2 - bc - ca + ab = BD; \tag{27}$$

D est impair, comme G et B.

§ VIII.

Les équations (20), (21), (23) et (27) fournissent le groupe suivant :

$$\left\{\begin{aligned} c - b - a &= 2.7B^2P; \\ a^2 + b^2 + c^2 - bc - ca + ab &= BD; \\ abc &= 7^6P^7; \\ 3(a^4 + b^4 + c^4) + 10(b^2c^2 + c^2a^2 + a^2b^2) &= 16B^{14}. \end{aligned}\right. \tag{28}$$

Il s'agit d'éliminer a, b, c, entre ces quatre équations. Le carré de la première combiné avec la seconde, donne

$$a^2 + b^2 + c^2 = 2BD - 4.7^2B^4P^2, \quad -bc - ca + ab = 4.7^2B^4P^2 - BD;$$

et de ces deux nouvelles équations, élevées au carré, on déduit

$$\begin{gathered} a^4 + b^4 + c^4 + 2(b^2c^2 + c^2a^2 + a^2b^2) = (2BD - 4.7^2B^4P^2)^2, \\ b^2c^2 + c^2a^2 + a^2b^2 = (4.7^2B^4P^2 - BD)^2 - 4.7^7B^2P^8; \end{gathered}$$

ces valeurs, substituées dans la quatrième (28), donnent une équation finale où $16B^2$ peut être supprimé comme facteur commun, et qui donne définitivement

$$B^{12} + 7(7^3P^4)^2 = (D - \tfrac{5}{2}7^2P^2B^3)^3 + 3(\tfrac{1}{2}7^2P^2B^3)^2.$$

En posant

$$D = D_1 + \tfrac{5}{2}7^2P^2B^3, \tag{29}$$

on a plus simplement

$$B^{12} + 7(7^2P^4)^2 = D_1^2 + 3(\tfrac{1}{2}7^2P^2B^3)^2. \tag{30}$$

Le nombre P étant divisible par 2, et P^2 par 4, $\frac{1}{2}P^2$ sera entier et pair, D_1 impair comme D et B. La différence des deux carrés de nombres impairs $(B^6)^2$ et D_1^2 étant divisible par 8, ainsi que le terme $7(7^3P^4)^2$, il faut que 8 divise le terme $3(\frac{1}{2}7^2P^2B^2)^2$, ce qui exige que P soit au moins divisible par 4. B et 7P devant être premiers entre eux, l'équation (30) démontre que D_1 est premier avec B et avec 7P. L'équation (30) ne présente plus la même circonstance d'incompatibilité de formes que celle (17); aussi la démonstration de son impossibilité exige une recherche plus laborieuse.

Puisque P est pair, et même de la forme $4i$, soit posé $P = 2P_0$; P_0 sera pair, et l'équation (30) devient

$$D_1^2 = B^{12} - 12.7^4P_0^4B^6 + 2^8.7^7P_0^8 = (B^6 - 6.7^4P_0^4)^2 + (2^8.7^7 - 2^2.3^2.7^8)P_0^8;$$

mais on a $\quad (2^8.7^7 - 2^2.3^2.7^8) = 2^2.7^7.(2^6 - 3^2.7) = 2^2.7^7;$

on a donc simplement

$$(31) \qquad D_1^2 = (B^6 - 6.7^4P_0^4)^2 + 7(2.7^3P_0^4)^2.$$

§ IX.

Pour satisfaire à cette équation on pourrait s'appuyer sur des théorèmes concernant les formes quadratiques et leurs diviseurs; mais, sans rien emprunter à des théories étrangères, il suffit ici de résoudre directement l'équation indéterminée $t^2 = u^2 + 7v^2$, dans laquelle les nombres t, u, impairs, et v pair, doivent être premiers entre eux. Cette équation peut se mettre sous la forme $(t-u)(t+u) = 7v^2$; les facteurs $(t-u)$ et $(t+u)$ étant pairs, ne pourront avoir un facteur premier commun δ autre que 2, car alors δ divisant leur somme $2t$ et leur différence $2u$, diviserait t et u, qui doivent rester premiers entre eux.

Si donc on pose $V = 2^iMN$, M et N étant deux nombres impairs, premiers entre eux, la seule manière de décomposer l'équation $(t-u)(t+u) = 7v^2$, compatible avec les conditions imposées aux nombres t, u, v, sera donnée par le groupe suivant :

$$v = 2^iMN, \quad t \mp u = 7.2^mM^2, \quad t \pm u = 2^nN^2, \quad m + n = 2i;$$

d'où l'on déduit

$$t = 7.2^{m-1}M^2 + 2^{n-1}N^2, \quad \mp u = 7.2^{m-1}M^2 - 2^{n-1}.N^2;$$

t et u devant être impairs, il faut nécessairement que l'un des exposants $(m-1)$ ou $(n-1)$ soit zéro, et leur somme $(m+n-2)$ étant $2(i-1)$, celui qui restera sera nécessairement pair.

Il suit de là qu'en posant $2^{i-1}M = g$, $N = f$, ou $M = g$, $2^{i-1}N = f$; ce qui donne dans les deux cas $2^{i-1}MN = fg$, et $v = 2^i MN = 2fg$, on aura définitivement

$$v = 2fg, \quad t = f^2 + 7g^2, \quad \pm u = f^2 - 7g^2,$$

pour satisfaire généralement à l'équation indéterminée $t^2 = u^2 + 7v^2$.

§ X.

D'après cette solution, l'équation (31) conduit au groupe suivant :

$$(32) \quad D_1 = f^2 + 7g^2, \quad \pm B^6 \mp 6.7^4 P_0^4 = f^2 - 7g^2, \quad fg = 7^3 P_0^4;$$

f ne peut être divisible par 7, sans quoi 7 diviserait D_1 et B, ce qui ne peut avoir lieu; f et g sont nécessairement premiers entre eux; car un facteur premier δ qui les diviserait tous deux, ainsi que leur produit $7^3 P_0^4$, diviserait aussi P_0, et par suite B^6 et B; B et P_0 ne seraient donc pas premiers entre eux. Ainsi la troisième équation (32) ne peut être décomposée que de cette manière,

$$(33) \quad P_0 = Q_1 P_1, \quad f = Q_1^4, \quad g = 7^3.P_1^4;$$

Q_1 est premier avec $7P_1$; comme P_0 est divisible par 2, Q_1 ou P_1 est pair.

La seconde (32) devient

$$\pm B^6 = (Q_1^4 \pm 3.7^4.P_1^4)^2 - 7(2^3.7^3 P_1^4)^2;$$

le signe inférieur est inadmissible, car il en résulterait

$$7(2^3.7^3.P_1^4)^2 = (Q_1^4 - 3.7^4 P_1^4)^2 + B^6,$$

et le second membre, somme de deux carrés impairs, serait de la forme

$8n + 2$, tandis que le premier est divisible par 8. On a donc nécessairement

$$(34)\qquad (Q_1^4 + 3.7^4 P_1^4)^2 = (B^3)^2 + 7(2^3.7^3 P_1^4)^2.$$

Ici, comme pour l'équation (31), on devra poser

$$(35)\qquad Q_1^4 + 3(7^2 P_1^2)^2 = f_1^2 + 7g_1^2,\quad \pm B^3 = f_1^2 - 7g_1^2,\quad f_1 g_1 = 2^2.7^3 P_1^4;$$

f_1 et g_1 sont nécessairement l'un pair et l'autre impair, comme Q_1 et P_1, et pour que B reste impair; ainsi f_1 et g_1 n'ont pas le facteur commun 2; ils ne sauraient non plus avoir de commun un autre facteur premier δ, qui les divisant tous deux, ainsi que leur produit $2^2.7^3.P_1^2$, diviserai $7P_1$, par suite B et Q_1, en sorte que B et $7P = 2.7P_1Q_1$ ne seraient pas premiers entre eux; f_1 n'est donc pas divisible par 7.

§ XI.

Avant d'aller plus loin, il importe de remarquer que l'équation $t^2 + 3u^2 = v^2 + 7w^2$, dans laquelle t et u sont premiers entre eux ainsi que v et w, et les deux membres des nombres impairs, exige que t et v soient pairs ensemble, ou impairs ensemble.

En effet, de t et u l'un doit être pair et l'autre impair; il en est de même de v et w. Or si t et w étaient pairs, u et v seraient impairs, le premier membre serait de la forme $(4n + 3)$, et le second de celle $(4n + 1)$ qui est incompatible avec la première; si u et v étaient pairs, t et w impairs, le premier membre aurait au contraire la forme $4n + 1$, et le second celle $4n + 3$, d'où résulterait la même impossibilité. Donc t et v sont pairs ou impairs ensemble, u et w impairs ou pairs tous les deux.

§ XII.

Il résulte de ce lemme, de ce que f_1 et g_1 sont premiers entre eux, et de la première équation du groupe (35), que la troisième équation du même groupe pourra se décomposer de l'une ou de l'autre des deux manières suivantes :

$$P_1 = P_2 Q_2 \begin{cases} f_1 = 2^2 Q_2^4, & g_1 = 7^3 P_2^4, \quad \text{si } Q_1 \text{ pair,} \quad P_1,\ P_2,\ Q_2,\ \text{impairs};\\ f_1 = Q_2^4, & g_1 = 2^2\ 7^3.P_2^4, \quad \text{si } P_1 \text{ pair,} \quad Q_1,\ Q_2,\ \text{impairs.}\end{cases}$$

La première équation (35) devient ainsi

$$Q_1^4 = 2^4 Q_2^8 - 3.7^4 Q_2^4 P_2^4 + 7^7 P_2^8, \text{ si } Q_1 \text{ pair, } P_2 \text{ et } Q_2 \text{ impairs;}$$
$$Q_1^4 = Q_2^8 - 3.7^4 P_2^4 Q_2^4 + 2^4.7^7 P_2^8, \text{ si } Q_1, Q_2 \text{ impairs.}$$

Ce sont maintenant ces deux équations qu'il s'agit de résoudre en nombres entiers. Or la première est impossible avec les conditions que Q_1 soit pair, que P_2, Q_2, facteurs de P_1, soient impairs; en effet, cette équation peut se mettre sous la forme

$$16\left[\left(\frac{Q_1}{2}\right)^4 - Q_2^8\right] = 7(7^3 P_2^4)^2 - 3(7^2 Q_2^2 P_2^2)^2,$$

et les deux membres sont incompatibles, l'un étant de la forme $4.4n$, tandis que l'autre est de la forme $4.(2n+1)$.

La même impossibilité n'existe plus pour la seconde équation

$$(36) \qquad Q_1^4 = Q_2^8 - 3.7^4 P_2^4 Q_2^4 + 2^4.7^7 P_2^8.$$

Comme elle peut se mettre sous la forme

$$(Q_1^2)^2 + 3(7^2 P_2^2 Q_2^2)^2 = (Q_2^4)^2 + 7(2^2.7^3.P_2^4)^2,$$

que Q_1 et Q_2 sont impairs, le lemme précédent (§ XI) exige que P_2 soit divisible par 2. On peut donc poser $P_2 = 2\Pi_2$; l'équation dont il s'agit devient

$$Q_1^4 = Q_2^8 - 3.2^4.7^4 \Pi_2^4 Q_2^4 + 2^{12}.7^7 \Pi_2^8 = (Q_2^4 - 3.2^3.7^4 \Pi_2^4)^2 + 2^6.7^7(2^6 - 7.3^2)\Pi_2^8,$$

et comme $2^6 - 7.3^2 = 64 - 63 = 1$, plus simplement

$$(37) \qquad Q_1^4 = (Q_2^4 - 3.2^3.7^4 \Pi_2^4)^2 + 7(2^3.7^3 \Pi_2^4)^2.$$

§ XIII.

Pour résoudre l'équation (37), on peut poser

$$(38) \quad Q_1^2 = f_2^2 + 7g_2^2, \quad \pm Q_2^4 \mp 3.2^3 7^4 \Pi_2^4 = f_2^2 - 7g_2^2, \quad f_2 g_2 = 2^2 7^3 \Pi_2^4;$$

f_2 ne peut être divisible par 7, puisque Q_1 ne peut l'être; f_2 et g_2 sont premiers entre eux, sans quoi un facteur premier δ qui les diviserait tous deux, ainsi que leur produit, diviserait Q_1 et Q_2 qui doivent être premiers entre eux. Puisque Q_1 est impair, il faut que l'un des deux nombres f_2 et g_2 soit pair et l'autre impair; or ce ne peut être f_2 qui soit pair, car g_2 étant alors impair, le second membre de l'équation $Q_1^2 = f_2^2 + 7g_2^2$ serait de la forme $4n+3$, ou de l'une des deux formes $8n+3$, $8n+7$, tandis que le premier membre ne peut être que de la forme $8n+1$; donc g_2 est pair et f_2 impair.

D'après ces conditions, la troisième équation (38) ne peut se décomposer que de la manière suivante :

$$\Pi_2 = Q_3 P_3, \quad f_2 = Q_3^4, \quad g_2 = 2^2 \cdot 7^3 P_3^4 \quad (Q_3 \text{ premier avec } 2\ 7 \cdot Q_2).$$

La seconde des équations (38) devient ainsi

$$\pm Q_2^4 = Q_3^8 \pm 3.2^3.7^4 Q_3^4 P_3^4 - 7^7.2^4.P_3^8 = (Q_3^4 \pm 2^2.3.7^4 P_3^4)^2 - 2^4.7^7(3^2.7+1)P_3^8,$$

et comme $7.3^2 + 1 = 64 = 2^6$, plus simplement

$$\pm Q_2^4 = (Q_3^4 \pm 2^2.3.7^4 P_3^4)^2 - 7(2^5.7^3.P_3^4)^2.$$

On voit qu'on ne peut admettre le signe inférieur, car on en déduirait $7(2^5.7^3 P_3^4)^2 = Q_2^4 + (Q_3 - 3.2^2.7^4 P_3^4)^2$, et Q_2, Q_3, étant impairs, le second membre serait de la forme $8n+2$, et incompatible avec le premier, divisible par 2^{10}. On a donc nécessairement

$$(39) \qquad (Q_3^4 + 2^2.3.7^4 P_3^4)^2 = Q_2^4 + 7(2^5.7^3.P_3^4)^2.$$

§ XIV.

Pour résoudre l'équation (39), on posera

$$(40) \quad Q_3^4 + 2^2.3.7^4 P_3^4 = f_3^2 + 7g_3^2, \quad \pm Q_2^2 = f_3^2 - 7g_3^2, \quad f_3 g_3 = 2^4.7^3.P_3^4;$$

on verra, comme ci-dessus, que f_3 est premier avec 7 et avec g_3; et la première (40), d'après le lemme du § XI, exige que f_3 soit impair et g_3 pair. Il n'y a donc d'autre moyen que le suivant de décomposer la troisième (40),

$$P_3 = Q_4 P_4, \quad f_3 = Q_4^4, \quad g_3 = 2^4.7^3.P_4^4 \quad (Q_4 \text{ premier avec } 2.7.Q_3).$$

La première équation (40) devient

$$Q_3^4 = Q_4^8 - 2^2.3.7^4.P_4^4 Q_4^4 + 7^7.2^8.P_4^8 = (Q_4^4 - 2.3.7^4 P_4^4)^2 + 2^2.7^7(2^6 - 3^2.7)P_4^8,$$

et comme $(2^6 - 3^2.7) = 1$, plus simplement

$$(41) \qquad Q_3^4 = (Q_4^4 - 2.3.7^4.P_4^4)^2 + 7(2\;7^3.P_4^4)^2.$$

Pour résoudre cette équation (41), il faut encore poser

$$(42) \quad Q_3^2 = f_4^2 + 7g_4^2, \quad \pm Q_4^4 \mp 2.3.7^4.P_4^4 = f_4^2 - 7g^2, \quad fg = 7^3 P_4^4;$$

f_4 est encore nécessairement premier avec 7 et avec g_4; et, comme la première (38), la première (42) démontre que f_4 est impair et g_4 pair. On est ainsi conduit à la décomposition suivante de la dernière (42):

$$P_4 = Q_5 P_5, \quad f_4 = Q_5^4, \quad g_4 = 7^3 P_5^4 \quad (Q_5 \text{ premier avec } 2.7.Q_4;\ P_5 \text{ pair}).$$

La seconde (42) devient

$$\pm Q_4^4 = Q_5^8 \pm 2.3.7^4 P_5^4 Q_5^4 - 7^7 P_5^8 = (Q_5^4 \pm 3.7^4 P_5^4)^2 - 7^7(3^2.7 + 1)P_5^8,$$

ou, comme $3^2.7 + 1 = 2^6$, plus simplement

$$\pm Q_4^4 = (Q_5^4 \pm 3.7^4 P_5^4)^2 - 7(2^3.7^3 P_5^4)^2,$$

et l'on voit que P_5 étant pair, le signe inférieur ne peut être admis. On a donc nécessairement

$$(43) \qquad (Q_5^4 + 3.7^4 P_5^4)^2 = Q_4^4 + 7(2^3.7^3.P_5^4)^2.$$

Pour résoudre cette équation (43), il faut encore poser

$$(44) \quad Q_5^4 + 3.7^4 P_5^4 = f_5^2 + 7g_5^2, \quad \pm Q_4^2 = f_5^2 - 7g_5^2, \quad f_5 g_5 = 2^2.7^3 P_5^4;$$

P_5 étant pair, le lemme établi (§ XI) démontre que g_5 est pair; on voit encore que f_5 est premier avec $7.g_5$, ce qui conduit à la décomposition

$$P_5 = Q_6 P_6, \quad f_5 = Q_6^4, \quad g_5 = 2^2.7^3.P_6^4 \quad (Q_6 \text{ premier avec } 2.7.Q_5).$$