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

PEPIN

Sur certains nombres complexes compris dans la formule $a+b\sqrt{-c}$

Journal de mathématiques pures et appliquées 3^e série, tome 1 (1875), p. 317-372.
<http://www.numdam.org/item?id=JMPA_1875_3_1__317_0>

Sur certains nombres complexes compris dans la formule $a+b\sqrt{-c}$;

PAR LE P. PEPIN, S. J.

1. Euler, dans la seconde Partie de son Algèbre (Chap. XII, XIII et XV), résout plusieurs questions d'Analyse indéterminée à l'aide des nombres complexes compris dans la formule générale $p+q\sqrt{c}$, dans laquelle p et q désignent deux nombres entiers quelconques, et c un nombre entier négatif, ou un nombre entier positif non carré. Ayant reconnu que le produit de deux fonctions semblables

$$p+cq^2, \quad r^2+cs^2$$

est une fonction semblable

$$(pr \pm cqs)^2 + c(ps \mp qr)^2,$$

il conclut que, pour transformer en carré la forme x^2+cy^2, dans le cas où c est premier, il faut poser

$$x+y\sqrt{-c} = m(p+q\sqrt{-c})^2,$$

ce qui donne

$$x = m(p^2-cq^2), \quad y = 2mpq,$$

m désignant le plus grand commun diviseur des deux nombres x et y. Dans le cas où c peut se décomposer en deux facteurs a et b, Euler pose

$$x+y\sqrt{-a.b} = (\sqrt{a}.p+\sqrt{-b}.q)^2,$$

d'où

$$x = ap^2-bq^2, \quad y = 2pq, \quad x^2+cy^2 = (ap^2+bq^2)^2.$$

2. Il est évident que les valeurs de x et de y, obtenues par cette

méthode, rendent la formule $x^2 + cy^2$ égale à un carré; mais il faudrait bien se garder d'affirmer qu'un problème est impossible lorsque cette méthode ne donne aucune solution. Il est des cas, il est vrai, où ce moyen donne toutes les solutions possibles du problème; mais plus souvent encore il est insuffisant. Il est donc nécessaire de n'introduire ces nombres complexes dans l'Analyse qu'en déterminant les conditions nécessaires pour rendre leur emploi légitime. C'est ce qu'Euler n'a pas fait; par exemple, il se propose cette question : « Trouver les carrés qui, multipliés par 5 et ajoutés à 7, produisent des cubes. » Cette question revient évidemment à trouver, parmi les solutions entières de l'équation $5x^2 + 7y^2 = z^3$, celles dans lesquelles $y = \pm 1$. Or, en appliquant sa méthode, Euler obtient, pour exprimer les solutions de cette équation, les formules suivantes :

$$x = 5p^3 - 21pq^2, \quad y = q(15p^2 - 7q^2), \quad z = 5p^2 + 7q^2,$$

dans lesquelles on doit attribuer aux indéterminées p et q toutes les valeurs rationnelles d'où résultent des valeurs entières pour x, y et z; puis, ayant reconnu que la seule solution dans laquelle y soit égal à ± 1 correspond aux valeurs $p = q = \pm \frac{1}{2}$, qui donnent $x = \pm 2$, $y = \pm 1$, Euler conclut que 4 est le seul carré qui réponde à la question.

Cette conclusion n'est pas légitime, puisque les formules données par Euler ne sont pas les seules qui puissent transformer en un cube la forme $5x^2 + 7y^2$; on satisfait également à cette condition par les formules suivantes :

$$\begin{aligned} x &= 2p^3 + 9p^2q - 18pq^2 - 16q^3, \\ y &= p^3 - 9p^2q - 18pq^2 + 8q^3, \\ z &= 3p^2 + 2pq + 12q^2. \end{aligned}$$

On en déduit la solution d'Euler en posant

$$q = 0, \; p = 1, \quad \text{d'où} \quad y = 1, \; x = 2, \; z = 3.$$

Ces formules et celles d'Euler renferment bien toutes les solutions du problème : on les obtient même toutes en ne donnant que des valeurs

entières aux nombres p et q; mais, pour conclure que 4 est le seul carré qui, multiplié par 5 et ajouté à 7, produit un cube, il reste à démontrer que l'unique manière de vérifier en nombres entiers l'équation

$$p^3 - 9p^2q - 18pq^2 + 8q^3 = \pm 1$$

est de poser $q = 0$, $p = \pm 1$. C'est ce que nous allons faire, afin de compléter la démonstration d'Euler.

On a identiquement

$$(p + 2q)(p^2 - 11pq + 4q^2) = p^3 - 9p^2q - 18pq^2 + 8q^3;$$

cette formule ne peut donc se réduire à ± 1 que pour des valeurs de p et q propres à vérifier les deux équations

$$p + 2q = \pm 1, \quad p^2 - 11pq + 4q^2 = \pm 1.$$

Or le système de ces deux équations n'admet que les solutions rationnelles $q = 0, p = \pm 1$; $p = 0$, $q = \pm \frac{1}{2}$, et des solutions non rationnelles. Les deux solutions rationnelles donnent $x = \pm 2$, $y = \pm 1$, $z = 3$; ce qui vérifie l'assertion d'Euler.

3. On ne peut pas non plus considérer comme entièrement démontrés les deux théorèmes de Fermat, qui sont l'objet des deux premières questions du Chapitre XII, tant que l'on n'a pas justifié l'emploi de la méthode précédente pour les deux formes $x^2 + y^2$, $x^2 + 2y^2$. Or, c'est ce qui n'a été fait ni par Euler, ni par Legendre; celui-ci s'est contenté de reproduire sur ce point les démonstrations d'Euler. Gauss est le premier qui ait introduit les nombres complexes d'une manière complétement rigoureuse; mais il ne l'a fait que pour les nombres complexes $a + b\sqrt{-1}$, dont il a donné la théorie dans son second Mémoire *Sur les résidus biquadratiques*. On trouve aussi les éléments de cette théorie dans un Mémoire de Dirichlet *Sur les formes quadratiques à coefficients et à indéterminées complexes* (*Journal de Crelle*, t. XXIV). Le même savant a considéré les nombres complexes $a + b\sqrt{5}$, dans son Mémoire *Sur l'impossibilité de l'équation* $x^5 + y^5 + z^5 = 0$, et les nombres complexes de la forme $a + b\sqrt{-7}$ dans son Mémoire

Sur l'impossibilité de l'équation $x^{14}+y^{14}=z^{14}$. Dans le premier de ces Mémoires (*Journal de Crelle*, t. III, p. 354), Dirichlet démontre que l'unique manière de vérifier l'équation

$$P^2-5Q^2=z^5,$$

quand la seconde indéterminée Q doit être divisible par 5, est de poser

$$P+Q\sqrt{5}=(\varphi\pm\psi\sqrt{5})^5,\quad z=\varphi^2-5\psi^2;$$

et dans l'autre Mémoire (*Journal de Crelle*, t. IX, p. 391) il s'appuie sur ce théorème, que la manière la plus générale de rendre égale à une quatorzième puissance la formule $\varphi^6+7\psi^2$, où φ et ψ désignent deux nombres entiers et premiers entre eux, est de poser

$$\varphi^3+\psi\sqrt{-7}=(g+h\sqrt{-7})^{14},$$

et il indique pour ce théorème une démonstration semblable à celle qui concerne l'équation

$$P^2-5Q^2=z^5.$$

4. Les nombres complexes $a+b\sqrt{-1}$, $a+b\sqrt{5}$, $a+b\sqrt{-7}$ sont-ils les seuls auxquels on puisse appliquer la méthode d'Euler? Nous montrerons qu'il en est plusieurs autres. De plus, l'emploi des nombres complexes $a+b\sqrt{-7}$ n'est pas borné au cas particulier considéré par Dirichlet; il est aussi étendu, nous le verrons, que celui des nombres complexes $a+b\sqrt{-1}$, du moins tant qu'il s'agit d'égaler la formule x^2+7y^2 à une puissance d'un nombre impair. Quels sont donc les nombres complexes que l'on peut introduire dans l'analyse indéterminée des nombres entiers, et quelles sont les conditions nécessaires pour en légitimer l'usage? Telle est la question que je me propose de résoudre dans la première Partie de ce Mémoire; non pas, il est vrai, d'une manière complète, mais en me bornant aux nombres complexes compris dans la formule $a+b\sqrt{-c}$, où a et b désignent des nombres entiers quelconques, et c un nombre entier et positif. La seconde Partie du Mémoire est consacrée à montrer, par la solution d'un grand nombre de problèmes, les avantages de la théorie exposée dans la première Partie.

PREMIÈRE PARTIE.

I.

5. Nous rappellerons d'abord un théorème déjà démontré par Legendre.

THÉORÈME I. — *Si le nombre p^2+cq^2 est impair et premier à c, et que les deux nombres p et q soient premiers entre eux, les nombres entiers x et y déterminés par l'équation*

$$x+y\sqrt{-c}=(p+q\sqrt{-c})^m \tag{1}$$

sont premiers entre eux.

Démonstration. — Soit θ un nombre premier diviseur commun des deux nombres x et y; l'équation $x^2+cy^2=(p^2+cq^2)^m$ montre que θ doit être diviseur de p^2+cq^2; θ est donc impair et premier relativement à c. D'ailleurs la valeur de x déterminée par l'équation proposée est

$$x=p^m-\frac{m(m-1)}{1.2}cq^2\,p^{m-2}+\frac{m(m-1)(m-2)(m-3)}{1.2.3.4}c^2q^4p^{m-4}-\dots.$$

Si dans le second membre on remplace partout cq^2 par $-p^2$, on aura, à cause de la congruence $cq^2\equiv -p^2 \pmod{\theta}$,

$$\begin{aligned}x&\equiv p^m\left[1+\frac{m(m-1)}{1.2}+\frac{m(m-1)(m-2)(m-3)}{1.2.3.4}+\dots\right]\\&\equiv\tfrac{1}{2}p^m[(1+1)^m+(1-1)^m]\equiv 2^{m-1}p^m \pmod{\theta}.\end{aligned}$$

Or, θ étant diviseur impair de x, devrait diviser p; mais alors on conclurait de la congruence $cq^2\equiv -p^2 \pmod{\theta}$, que le produit cq^2 serait divisible par θ, ce qui est impossible, puisque c est premier relativement à θ, et q relativement à p, multiple de θ. Les deux nombres x et y n'ont donc pas de diviseur commun.

6. THÉORÈME II. — *Soient*

$$a^2 + ca_1^2 = \mathrm{A}, \quad b^2 + cb_1^2 = \mathrm{B};$$

si A *et* B *sont premiers entre eux et premiers relativement à c, si de plus les deux nombres a et a_1 sont premiers entre eux, ainsi que les deux nombres b et b_1, les nombres x, y déterminés par l'équation*

$$x + y\sqrt{-c} = (a + a_1\sqrt{-c})(b + b_1\sqrt{-c}) \tag{2}$$

sont aussi premiers entre eux.

On déduit, en effet, de cette équation

$$x^2 + cy^2 = (a^2 + ca_1^2)(b^2 + cb_1^2) = \mathrm{AB};$$

en sorte que, si un nombre premier θ divisait en même temps x et y, il diviserait l'un des deux nombres A ou B sans diviser l'autre. Supposons B divisible par θ et A premier relativement à θ, et multiplions les deux membres de l'équation (2) par l'expression $a - a_1\sqrt{-c}$; du résultat de cette multiplication,

$$(ax + a_1cy) + \sqrt{-c}(ay - a_1x) = \mathrm{A}b + \sqrt{-c}\,\mathrm{A}b_1,$$

on déduit

$$ax + a_1cy = \mathrm{A}b, \quad ay - a_1x = \mathrm{A}b_1.$$

Le nombre θ devrait donc diviser en même temps les deux produits $\mathrm{A}b$, $\mathrm{A}b_1$, et, comme il est premier avec A, il diviserait les deux nombres b et b_1, contrairement à l'hypothèse. Donc les deux nombres x et y sont premiers entre eux.

7. COROLLAIRE I. — *L'équation*

$$x + y\sqrt{-c} = (a + b\sqrt{-c})(p + q\sqrt{-c})^m$$

détermine pour x et y des valeurs entières et premières entre elles, toutes les fois que, les deux nombres $a^2 + cb^2$, $p^2 + cq^2$ étant impairs

et premiers entre eux, comme avec le déterminant $-c$, les deux nombres a et b sont premiers entre eux, ainsi que les nombres p et q.

En effet, si l'on pose $(p+q\sqrt{-c})^m = P+Q\sqrt{-c}$, les deux fonctions entières de p, q et c désignées par P et Q auront des valeurs entières et premières entre elles (théorème I), en sorte que l'équation

$$x+y\sqrt{-c} = (a+b\sqrt{-c})(P+Q\sqrt{-c})$$

remplira les conditions du théorème II; les nombres x et y seront donc premiers entre eux.

COROLLAIRE II. — *Si les nombres a^2+cb^2, $a_1^2+cb_1^2$, $a_2^2+cb_2^2$,... sont impairs, premiers entre eux deux à deux et premiers relativement à c, si en outre les deux nombres a et b sont premiers entre eux, ainsi que les deux nombres a_1 et b_1, a_2 et b_2,..., l'équation*

$$x+y\sqrt{-c} = (a+b\sqrt{-c})^m (a_1+b_1\sqrt{-c})^{m_1}(a_2+b_2\sqrt{-c})^{m_2}\dots,$$

ou m, m_1, m_2,... sont des exposants entiers et positifs, détermine, pour x et y, des valeurs entières et premières entre elles.

Posons pour les valeurs 0, 1, 2,... de i

$$(a_i+b_i\sqrt{-c})^{m_i} = A_i+B_i\sqrt{-c};$$

les nombres A_i et B_i sont entiers et premiers entre eux (théorème I). Il en est de même, en vertu du théorème II, pour les nombres x_1 et y_1, x_2 et y_2,..., déterminés par les équations successives

$$(A+B\sqrt{-c})(A_1+B_1\sqrt{-c}) = x_1+y_1\sqrt{-c},$$
$$(A_2+B_2\sqrt{-c})(x_1+y_1\sqrt{-c}) = x_2+y_2\sqrt{-c},\dots,$$

et, comme cette suite de nombres $x_1, y_1; x_2, y_2;\dots$ se termine aux nombres x et y, ceux-ci sont aussi premiers entre eux.

Tous ces théorèmes que nous venons d'établir supposent simplement que $-c$ ne soit pas un carré, en sorte que toute équation

$$A+B\sqrt{-c} = P+Q\sqrt{-c},$$

où A et B, P et Q désignent des nombres rationnels, soit équivalente aux deux équations

$$A = P, \quad B = Q.$$

Dans ce qui va suivre, nous supposerons que c désigne un nombre entier et positif, et nous considérerons d'abord le cas où toutes les formes quadratiques positives et impaires de déterminant $-c$ sont comprises dans une même classe. L'emploi du facteur complexe $p+q\sqrt{-c}$, conformément à la méthode d'Euler, est alors parfaitement légitime. C'est ce que nous verrons dans les théorèmes suivants; mais auparavant nous rappellerons certaines relations entre les représentations propres d'un nombre composé M par la formule x^2+cy^2, et les solutions de la congruence $x^2+c\equiv 0 \pmod{M}$.

8. Nous disons avec Gauss que deux nombres (x, y) forment une représentation propre d'un nombre impair M par la forme (a, b, c), lorsqu'ils sont premiers entre eux et qu'ils vérifient l'équation

$$ax^2+2bxy+cy^2=M.$$

Il est évident d'abord que toute représentation propre d'un nombre M par la forme x^2+cy^2 conduit à une solution de la congruence $x^2+c\equiv 0 \pmod{A}$; car, x et y étant premiers entre eux, on peut poser

$$x\equiv uy \pmod{M}, \quad y^2(u^2+c)\equiv 0 \pmod{M},$$

d'où

$$u^2+c\equiv 0 \pmod{M}.$$

De plus, comme, dans les cas dont nous nous occupons, c n'a pas de diviseur carré impair, le nombre M est nécessairement premier avec c, et, par conséquent, la valeur de u est différente de zéro.

Réciproquement, toute racine u de la congruence

$$x^2+c\equiv 0 \pmod{M}$$

conduit à deux représentations propres du nombre M par la forme x^2+cy^2, formées par les mêmes valeurs numériques p et q, ou $-p$

et $-q$ des indéterminées x et y, dont le rapport $\frac{p}{q}$ est congru à la racine u, suivant le module M. En effet, le quotient $\frac{u^2+c}{M}$ étant un nombre entier, la formule

$$Mx^2 - 2uxy + \frac{u^2+c}{M}y^2$$

sera une forme quadratique de déterminant $-c$, équivalente par conséquent à la forme x^2+cy^2, puisque nous supposons que toutes les formes quadratiques de déterminant $-c$ appartiennent à une même classe. Soit donc $x = px' + p_0y'$, $y = qx' + q_0y'$ la substitution propre à transformer $(1, 0, c)$ en la forme équivalente $\left(M, u, \frac{u^2+c}{M}\right)$. Comme la seconde forme devient égale à M pour les valeurs $x' = \pm 1$, $y' = 0$, la première x^2+cy^2 représentera aussi le nombre M pour les valeurs $x = p$, $y = q$, et pour les valeurs opposées $x = -p$, $y = -q$. Ce sont deux représentations propres, car les nombres p et q, devant satisfaire à la relation $pq_0 - qp_0 = 1$, sont nécessairement premiers entre eux. Enfin de l'équation

$$(px' + p_0y')^2 + c(qx' + q_0y')^2 = Mx'^2 + 2ux'y' + \frac{u^2+c}{M}y'^2$$

on déduit

$$p^2 + cq^2 = M, \quad pp_0 + cqq_0 = -u,$$

d'où

$$p(pq_0 - qp_0) = Mq_0 + qu, \quad p \equiv qu \,(\text{mod. M});$$

ainsi le rapport $\frac{p}{q}$ est équivalent suivant le module M à la racine u. Soit 2^λ le nombre des racines de la congruence $x^2 + c \equiv 0 \,(\text{mod. M})$. A chacune de ces racines correspondront deux représentations propres du nombre M par la forme x^2+cy^2, en sorte que le nombre de toutes ces représentations sera $2^{\lambda+1}$.

9. Théorème III. — *La manière la plus générale de résoudre l'équation*

$$x^2 + cy^2 = z^m, \tag{3}$$

quand les nombres x, y et z doivent être entiers et premiers entre eux, et qu'en outre z doit être impair, est de poser

$$(4) \qquad (p+q\sqrt{-c})^m = P+Q\sqrt{-c},$$

de prendre $x=\pm P$, $y=\pm Q$, $z=p^2+cq^2$, et d'attribuer aux lettres p et q toutes les valeurs entières et premières entre elles, qui déterminent pour z des valeurs impaires.

Démonstration. — Comme, par hypothèse, toutes les formes quadratiques positives et impaires de déterminant $-c$ sont équivalentes à la forme principale x^2+cy^2, toutes les valeurs impaires de z propres à vérifier l'équation (3) sont de la forme p^2+cq^2. Ainsi nos formules donnent pour z toutes les valeurs convenables; il reste à démontrer qu'elles font correspondre à chaque valeur de z toutes les valeurs compatibles de x et de y. D'abord les valeurs $x=\pm P$, $y=\pm Q$ sont bien premières entre elles (théorème I), et forment ainsi des représentations propres du nombre z^m par la forme x^2+cy^2. Nous aurons démontré que nos formules donnent toutes les représentations propres de z^m par la forme x^2+cy^2, et, par suite, qu'elles font correspondre à chaque valeur de z toutes les valeurs compatibles de x et de y, si nous faisons voir qu'en prenant successivement pour p et q toutes les représentations propres de z par la forme x^2+cy^2, les valeurs correspondantes de $\pm P$, $\pm Q$ formeront toutes les représentations propres de z^m par la même forme. Or, d'après ce que nous avons dit plus haut (8), ce dernier point est obtenu si nous montrons que les valeurs du rapport $\frac{P}{Q}$ sont congrues aux diverses racines de la congruence

$$x^2+c \equiv 0 \pmod{z^m}.$$

On sait d'ailleurs que les diverses racines de cette congruence correspondent une à une aux diverses racines de la congruence

$$x^2+c \equiv 0 \pmod{z}$$

et leur sont respectivement congrues suivant le module z. Il suffit donc de montrer que les diverses valeurs du rapport $\frac{P}{Q}$ déterminées par

nos formules sont congrues suivant le module z aux diverses racines de la congruence $x^2+c\equiv 0 \pmod{z}$, de telle sorte qu'à une racine α de cette congruence corresponde une valeur congrue, suivant le module z, du rapport $\frac{P}{Q}$. Et, en effet, les valeurs de P et Q qui satisfont à cette condition sont déterminées par celle des solutions de l'équation $p^2+q^2c=z$, dont les termes p et q sont liés entre eux par la relation $\frac{p}{q}\equiv\alpha \pmod{z}$. Pour le démontrer, il suffit de multiplier par $p-q\sqrt{-c}$ les deux membres de l'équation (4), ce qui donne

$$(p+q\sqrt{-c})^{m-1}(p^2+cq^2)=(Pp+cqQ)+\sqrt{-c}(Pq-Qp);$$

posant donc

$$(p+q\sqrt{-c})^{m-1}=H+K\sqrt{-c},$$

on aura

$$Pq-Qp=Kz,\quad \frac{P}{Q}\equiv\frac{p}{q}\equiv\alpha \pmod{z}.$$

Ainsi à toute racine α de la congruence $x^2+c\equiv 0 \pmod{z}$ nos formules font correspondre deux représentations propres P, Q; $-$P, $-$Q de z^m par la forme x^2+cy^2, telles que le rapport $\frac{P}{Q}$ soit congru à α suivant le module z. Nos formules donnent donc pour chaque valeur de z toutes les valeurs compatibles de x et de y; elles donnent, par conséquent, toutes les solutions de l'équation (3), qui satisfont aux conditions énoncées.

10. Théorème IV. — *Soient* A, B, C, ... *des diviseurs impairs de la formule* x^2+cy^2, *premiers entre eux deux à deux; pour obtenir toutes les solutions de l'équation*

$$x^2+cy^2=A^m B^{m_1} D^{m_2}\ldots \tag{5}$$

en nombres entiers et premiers entre eux, il suffit de poser

$$\pm x\pm y\sqrt{-c}=(a+a_1\sqrt{-c})^m(b+b_1\sqrt{-c})^{m_1}(d+d_1\sqrt{-c})^{m_2}\ldots \tag{6}$$

de ramener le second membre à la forme $P+Q\sqrt{-c}$ *en effectuant*

les calculs indiqués, puis de donner dans les deux polynômes P *et* Q *aux lettres* (a, a_1), (b, b_1), (d, d_1),... *toutes les valeurs entières qui forment respectivement des représentations propres des nombres* A, B, D *par la forme* x^2+cy^2.

Les valeurs de x et de y ainsi déterminées sont premières entre elles (7); elles vérifient l'équation (5), puisque celle-ci se déduit de l'équation (6) multipliée membre à membre par celle qu'on en déduit en changeant le signe de $\sqrt{-c}$. Elles forment donc des représentations propres du produit $A^m B^{m_1} D^{m_2}\ldots$; il s'agit de démontrer que toutes les représentations propres de ce produit sont données par la formule (6), ou bien, ce qui revient au même, d'après ce qui a été dit plus haut (8), que dans les diverses solutions déduites de la formule (6) les diverses valeurs du rapport $\frac{x}{y}$ sont respectivement congrues, suivant le module $A^m B^{m_1} D^{m_2}\ldots$ à toutes les racines de la congruence

$$u^2+c\equiv 0 \pmod{A^m B^{m_1} D^{m_2}\ldots}.$$

D'ailleurs les nombres A, B, D,... étant premiers entre eux deux à deux, on obtient toutes les racines de cette congruence en prenant, pour chacune des combinaisons α, β, δ,..., que l'on peut former avec les racines des congruences

$$(a)\quad \alpha^2+c\equiv 0 \pmod{A^m},\ \beta^2+c\equiv 0 \pmod{B^{m_1}},\ \delta^2+c\equiv 0 \pmod{D^{m_2}},\ldots,$$

la valeur de u, comprise entre $-\frac{1}{2}A^m B^{m_1} D^{m_2}\ldots$ et $+\frac{1}{2}A^m B^{m_1} D^{m_2},\ldots$, qui vérifie les congruences

$$(b)\quad u\equiv\alpha \pmod{A^m},\quad u\equiv\beta \pmod{B^{m_1}},\quad u\equiv\delta \pmod{D^{m_2}},\ldots.$$

Désignons par α', β', δ',... les résidus minimum de α, β, δ,..., suivant les modules respectifs A, B, D,.... La valeur de u déterminée par les congruences (b) vérifie évidemment les suivantes :

$$(c)\quad u\equiv\alpha' \pmod{A},\quad u\equiv\beta' \pmod{B},\quad u\equiv\delta' \pmod{D},\ldots,$$

et les nombres α', β', δ',... sont des racines des congruences respectives

$$(d)\quad \alpha'^2+c\equiv 0 \pmod{A},\ \beta'^2+c\equiv 0 \pmod{B},\ \delta'^2+c\equiv 0 \pmod{D},\ldots.$$

Or les racines des congruences (a) correspondent une à une aux racines des congruences (d) et leur sont congrues suivant les modules respectifs A, B, D,. .. Nous aurons donc démontré que la formule (6) donne toutes les solutions propres de l'équation (5), si nous montrons qu'elle détermine pour chaque système de solutions α', β', δ',... des congruences (d) des valeurs de x et de y, dont le rapport désigné par u vérifie les congruences (c). Effectivement, si l'on choisit parmi les diverses valeurs possibles de (a, a_1), (b, b_1), (d, d_1),... celles qui satisfont aux congruences

$$a \equiv \alpha' a_1 \,(\text{mod. A}), \quad b \equiv \beta' b_1 \,(\text{mod. B}), \quad d \equiv \delta' d_1 \,(\text{mod. D}),\ldots,$$

le rapport u des valeurs obtenues pour x et y vérifiera les congruences (c). Nous nous contenterons de le démontrer pour la première, la démonstration étant la même pour toutes.

Multiplions les deux membres de l'équation (6) par $a - a_1\sqrt{-c}$, et posons

$$(a + a_1\sqrt{-c})^{m-1}(b + b_1\sqrt{-c})^{m_1}(d + d_1\sqrt{-c})^{m_2}\ldots = \mathrm{F} + \mathrm{G}\sqrt{-c},$$

en désignant par F et par G la partie réelle et le coefficient de $\sqrt{-c}$ dans le développement de la fonction imaginaire renfermée dans le premier membre. Notre produit se mettra sous la forme

$$ax + a_1 cy + \sqrt{-c}(ay - a_1 x) = \mathrm{AF} + \mathrm{AG}\sqrt{-c},$$

et l'on en déduira

$$ay - a_1 x = \mathrm{AG}, \quad \frac{x}{y} \equiv \frac{a}{a_1} \equiv \alpha' \,(\text{mod. A}).$$

Ainsi la congruence $a \equiv \alpha' a_1 \,(\text{mod. A})$ entraîne comme conséquence nécessaire la congruence $\frac{x}{y} = u \equiv \alpha' \,(\text{mod. A})$. En remplaçant a, a_1, A, α', par b, b_1, B, β', ou par d, d_1, D, δ',..., nous démontrerions de même que les congruences $u \equiv \beta' \,(\text{mod. B})$, $u \equiv \delta' \,(\text{mod. D})$,... sont des conséquences des congruences $b \equiv \beta' b_1$, $d \equiv \delta' d_1$,.... Donc la méthode proposée dans notre théorème donne bien toutes les représentations propres du produit $\mathrm{A}^m \mathrm{B}^{m_1} \mathrm{D}^{m_2}\ldots$ par la forme $x^2 + cy^2$.

Ce théorème nous permet de donner à l'usage des facteurs complexes $p + q\sqrt{-c}$ une extension plus grande que celle qui résulte du théorème III.

11. THÉORÈME V. — *Si l'on désigne par* H *un diviseur impair de la formule* $x^2 + cy^2$, *et par* x, y, z *des nombres entiers et premiers entre eux deux à deux, dont le dernier* z *doit être impair, toutes les solutions de l'équation*

$$x^2 + cy^2 = \mathrm{H}z^m, \tag{7}$$

peuvent se déduire des formules

$$\pm x \pm y\sqrt{-c} = (a + b\sqrt{-c})(p + q\sqrt{-c})^m, \quad z = p^2 + cq^2, \tag{8}$$

en y combinant successivement chacune des représentations propres (a, b) *du nombre* H *par la forme* $x^2 + cy^2$, *avec toutes les valeurs entières et premières entre elles de* p *et* q *propres à donner des valeurs impaires à la formule* $p^2 + cq^2$.

Dans le théorème III, les formules (3) et (4) sont équivalentes, sous les restrictions posées que z soit impair et que les nombres x et y soient premiers entre eux. Il n'en est pas de même des formules (7) et (8), car la dernière peut donner pour x et y des valeurs qui ne soient pas premières entre elles. Qu'on y fasse, en effet, $p = a$, $q = -b$; elle deviendra

$$\pm x \pm y\sqrt{-c} = (a^2 + cb^2)(a - b\sqrt{-c})^{m-1} = \mathrm{HA} + \mathrm{HB}\sqrt{-c},$$

les nombres rationnels et entiers A et B étant déterminés par l'équation

$$(a - b\sqrt{-c})^{m-1} = \mathrm{A} + \mathrm{B}\sqrt{-c}.$$

On aura donc $x = \pm \mathrm{HA}$, $y = \pm \mathrm{HB}$. Mais cela n'a pas d'inconvénient, pourvu que la formule (8) donne toutes les solutions de l'équation (7) qui satisfont aux conditions énoncées. C'est ce qui a lieu effectivement, ainsi que nous allons le démontrer.

D'abord la formule $z = p^2 + cq^2$ donne bien toutes les valeurs convenables de z, puisque, par hypothèse, le déterminant $-c$ est tel, que tout diviseur impair de la formule $x^2 + cy^2$ est lui-même représenté

par cette formule. De plus, à chaque valeur de z première avec H, la formule (8) fait correspondre toutes les valeurs entières et premières entre elles de x et de y, qui forment avec cette valeur de z des solutions de l'équation (7); on le déduit immédiatement du théorème IV, en réduisant à deux le nombre des facteurs dans le second membre de l'équation (5), et en remplaçant A^m, B^{m_1} par H et z^m. Il nous suffit donc de démontrer que, dans le cas où z reçoit une valeur divisible par quelque facteur premier de H, la formule (8) donne toutes les représentations propres du produit Hz^m par la forme x^2+cy^2.

Soient A_1, A_2,... les facteurs premiers communs de H et de z; posons

$$H = AA_1^{\alpha}A_2^{\beta},\ldots, \quad z = BA_1^{\alpha'}A_2^{\beta'}\ldots;$$

les nombres A, B, A_1, A_2,... seront tous premiers entre eux deux à deux. Il résulte du théorème IV que toutes les représentations propres du produit $Hz^m = AB^mA_1^{m\alpha'+\alpha}A_2^{m\beta'+\beta}\ldots$ par la forme x^2+cy^2 se déduisent de la formule

$$(9)\qquad \begin{cases} \pm x \pm y\sqrt{-c} = (f+g\sqrt{-c})(h+k\sqrt{-c})^m \\ \qquad \times (a_1+b_1\sqrt{-c})^{m\alpha'+\alpha}(a_2+b_2\sqrt{-c})^{m\beta'+\beta}\ldots \end{cases}$$

en prenant respectivement pour (f, g), (h, k), (a_1, b_1), (a_2, b_2),... toutes les représentations propres des nombres A, B, A_1, A_2,..., par la même forme x^2+cy^2.

Or l'un quelconque des couples de valeurs ainsi obtenues pour x et y peut aussi se déduire de la formule (8), en y donnant aux nombres a, b, p et q les valeurs déterminées par les deux équations suivantes :

$$a+b\sqrt{-c} = (f+g\sqrt{-c})(a_1+b_1\sqrt{-c})^{\alpha}(a_2+b_2\sqrt{-c})^{\beta}\ldots$$
$$p+q\sqrt{-c} = (h+k\sqrt{-c})(a_1+b_1\sqrt{-c})^{\alpha'}(a_2+b_2\sqrt{-c})^{\beta'}\ldots,$$

où les valeurs des nombres (f, g), (h, k),... sont supposées les mêmes que dans l'équation (9). D'un côté, ces valeurs sont admissibles dans la formule (8), puisque a et b sont premiers entre eux, ainsi que p et q (n° 7); de l'autre elles transforment la formule (8) en la

formule (9). Ainsi, pour chaque valeur de z, la formule (8) donne tous les couples de valeurs premières entre elles de x et de y, qui forment avec cette valeur de z des solutions de l'équation (7).

On obtient aussi des solutions étrangères; car, dans le cas auquel se rapporte la formule (9), si l'on associait entre elles dans l'équation (8) les valeurs de a, b, p et q, déterminées par les deux formules

$$a+b\sqrt{-c}=(f+g\sqrt{-c})(a_1+b_1\sqrt{-c})^{\alpha}(a_2+b_2\sqrt{-c})^{\beta}\ldots$$
$$p+q\sqrt{-c}=(h+k\sqrt{-c})(a_1-b_1\sqrt{-c})^{\alpha'}(a_2+b_2\sqrt{-c})^{\beta'}\ldots,$$

on en déduirait pour x et y des valeurs divisibles par $a_1^2+cb_1^2=A_1$.

12. Les déterminants négatifs qui jouissent de la propriété supposée dans les derniers théorèmes III, IV et V sont -1, -2, -3, -4, -7; les valeurs de c auxquelles s'applique la méthode définie dans ces théorèmes sont donc 1, 2, 3, 4 et 7 Nous avons appliqué le théorème III dans un Mémoire sur l'équation $x^3+y^3=Az^3$ (*Journal de Mathématiques pures et appliquées*, juillet 1870), et nous avons indiqué le principe sur lequel repose la démonstration précédente. Dans le cas particulier où $c=3$, les théorèmes précédents pourraient aussi se déduire de ce que tout nombre premier $6l+1$ est le produit de deux facteurs complexes irréductibles formés au moyen des racines cubiques imaginaires de l'unité, conformément à la belle théorie des facteurs complexes donnée par M. Kummer.

Les nombres complexes $a+b\sqrt{-1}$, $a+b\sqrt{-2}$, $a+b\sqrt{-3}$, $a+b\sqrt{-4}$, $a+b\sqrt{-7}$ ne sont pas les seuls dont l'analyse indéterminée puisse tirer de grands avantages; on peut en introduire d'autres beaucoup plus nombreux, mais en apportant quelques modifications aux théorèmes qui en définissent l'usage légitime.

II. — Extension de la méthode précédente.

13. Désignons par n un nombre entier et positif, tel que toutes les formes quadratiques de déterminant $-n$ soient distribuées en divers genres, dont chacun ne renferme qu'une seule classe. Ces déterminants

sont assez nombreux : par exemple, si le nombre n a l'une des valeurs

5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58,

toutes les formes quadratiques de déterminant $-n$ se distribuent en deux classes et en deux genres, en sorte que chaque genre est représenté par une seule classe. De même, si n est égal à l'un des nombres

21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78
85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253,

les formes quadratiques de déterminant $-n$ sont comprises dans quatre genres dont chacun ne renferme qu'une seule classe. Il y a encore d'autres déterminants négatifs, pour lesquels le nombre des classes est le même que celui des genres; ils appartiennent aux classifications VIII, 1 et XVI, 1 des Tables publiées dans le second volume des *OEuvres de Gauss*.

Tous ces déterminants jouissent de cette propriété, qu'un diviseur impair quelconque A de la formule x^2+ny^2 ne peut être représenté par une forme quadratique de déterminant $-n$ qu'autant que cette forme appartient à la classe unique du genre déterminé par le reste de la division du nombre A, par l'un des modules $4n$ ou $8n$. Si l'on ne prend qu'une forme quadratique par classe, on énonce cette propriété en disant que toutes les représentations du nombre A par les diverses formes quadratiques de déterminant $-n$ appartiennent à la même forme.

14. Proposons-nous d'abord de trouver toutes les solutions de l'équation

$$x^2+ny^2=z^{2m+1}, \tag{1}$$

en nombres entiers, premiers entre eux deux à deux, et dont l'un, z, doit être en outre impair. Le théorème III est ici applicable; car, z étant impair, les deux nombres z^{2m+1} et z appartiennent au même genre, savoir le genre principal, puisque z^{2m+1} est représenté par la

forme principale. Cette forme x^2+ny^2 donne donc toutes les représentations propres des deux nombres z^{2m+1} et z par le système des formes quadratiques choisies pour représenter les diverses classes de déterminant $-n$. Il est donc évident que, si l'on égale p et q de toutes les manières possibles à des nombres entiers et premiers entre eux, les formules

$$(2) \qquad \pm x \pm y\sqrt{-n} = (p+q\sqrt{-n})^{2m+1}, \quad p^2+nq^2 = z$$

donnent pour z toutes les valeurs propres à vérifier l'équation proposée (1). Or, pour chaque valeur de z, la première de ces deux formules détermine pour x et y toutes les représentations propres de z^{2m+1} par la forme x^2+ny^2. Pour le démontrer il nous suffit (9) de faire voir que, pour toute solution α de la congruence

$$\alpha^2+n \equiv 0 \pmod{z},$$

notre formule donne pour x et y des valeurs premières entre elles, dont le rapport, désigné par u, vérifie la congruence $u \equiv \alpha \pmod{z}$. C'est ce qu'on obtient en multipliant les deux membres par $p-q\sqrt{-n}$. Posons

$$(p+q\sqrt{-n})^{2m} = P+Q\sqrt{-n});$$

le produit sera

$$\pm(px+cqy) \pm \sqrt{-n}(py-qx) = Pz+Qz\sqrt{-n},$$

d'où

$$\frac{x}{y} \equiv \frac{p}{q} \pmod{z}.$$

Pour que la valeur u du rapport $\frac{x}{y}$ vérifie la condition $u \equiv \alpha \pmod{z}$, il suffit donc de prendre pour (p, q) l'une des deux représentations de z qui correspondent à la racine α et satisfont à la congruence

$$p \equiv \alpha q \pmod{z};$$

ce qui est toujours possible, puisque toutes les représentations de z pour le déterminant $-n$ sont de la forme p^2+nq^2. Donc :

THÉORÈME VI. — *Si pour le déterminant $-n$ le genre principal ne renferme qu'une seule classe de formes quadratiques, toutes les solutions en nombres entiers et premiers entre eux de l'équation*

$$x^2+ny^2=z^{2m+1}, \tag{1}$$

dans laquelle z a une valeur impaire, se déduisent des équations

$$\pm x\pm y\sqrt{-n}=(p+q\sqrt{-n})^{2m+1},\quad z=p^2+nq^2, \tag{2}$$

en donnant aux lettres p et q de toutes les manières possibles des valeurs entières et premières entre elles.

Nous devons remarquer que, si le nombre n n'est pas de la forme $8l+7$, et que l'exposant $2m+1$ soit >1, il est impossible de supposer x, y, z premiers entre eux, sans que u soit impair. Les équations (2) donnent alors toutes les solutions de l'équation (1) en nombres entiers et premiers entre eux; mais, si le nombre n est de la forme $8l+7$, l'équation (1) admet des solutions où le nombre z est pair, x et y étant impairs et premiers, soit entre eux, soit relativement à z. Ces solutions devront être étudiées séparément, dans chaque problème où l'on aura besoin de connaître toutes les solutions de l'équation (1) en nombres entiers et premiers entre eux deux à deux.

15. Proposons-nous de trouver toutes les solutions de l'équation

$$x^2+ny^2=z^{2m}=(z^2)^m \tag{3}$$

en nombres entiers et premiers entre eux deux à deux, dont le dernier, z, soit en outre impair. Quel que soit le genre auquel appartienne le nombre z, son carré z^2 sera du genre principal, et l'équation

$$p^2+ny^2=z^2 \tag{4}$$

aura autant de couples de solutions (p,q), $(-p,-q)$ qu'il y a de

racines de la congruence

$$\alpha^2 + n \equiv 0 \pmod{z^2}.$$

Or la formule

$$(5) \qquad \pm x \pm y\sqrt{-n} = (p + q\sqrt{-n})^m$$

détermine pour x et y des valeurs premières entre elles, dont le rapport est congru au rapport $p:q$ suivant le module $p^2 + nq^2$: on le démontre en multipliant les deux membres par le facteur $p - q\sqrt{-n}$, ce qui donne

$$\pm (px + nqy) \pm \sqrt{-n}\,(py - qx) = (p^2 + nq^2)\,(p + q\sqrt{-n})^{m-1},$$

d'où

$$py - qx = Q(p^2 + nq^2), \quad \frac{x}{y} \equiv \frac{p}{q} \pmod{p^2 + nq^2}.$$

Donc la formule (4) donne d'un côté toutes les valeurs de z^2 propres à vérifier l'équation (3) sous les conditions posées, et, pour chaque valeur de z^2, la formule (5) fait correspondre autant de couples de solutions $(x, y), (-x, -y)$ qu'il y a de racines de la congruence $\alpha^2 + n \equiv 0 \pmod{z^2}$, lorsqu'on égale successivement p et q aux diverses solutions propres de l'équation (4). La formule (5) donne ainsi toutes les représentations propres de $(z^2)^m$ par la forme $x^2 + ny^2$ (8), en sorte que toutes les solutions de l'équation (3) se déduisent de l'équation (5) en y donnant à p et à q, de toutes les manières possibles, des valeurs entières et premières entre elles, qui rendent la forme $p^2 + nq^2$ égale à des carrés impairs.

Or ces valeurs de p et de q peuvent s'exprimer d'une manière générale au moyen de deux nombres entiers indéterminés. Pour cela nous partagerons les solutions de l'équation (4) en deux groupes, dont le premier renfermera toutes les solutions où le nombre q est pair, et le second toutes celles où q est impair.

Si q est pair, nous posons $q = 2fg$, $n = ab$, et la décomposition de l'équation (4), mise sous la forme $(z + p)(z - p) = 4abf^2g^2$, donne

$$z + p = 2af^2, \quad z - p = 2bg^2.$$

d'où

$$(6)\qquad z=af^2+bg^2,\quad p=af^2-bg^2,\quad q=2fg,\quad ab=n.$$

Si q est impair, nous posons $q=fg$, et nous déduisons de l'équation (4)

$$z+p=af^2,\quad z-p=bg^2,$$

d'où

$$(7)\qquad z=\frac{af^2+bg^2}{2},\quad p=\frac{af^2-bg^2}{2},\quad q=fg,\quad ab=n.$$

Comme, dans la formule (3), z et x sont premiers entre eux, z doit être premier avec n, ce qui exige que les deux facteurs a, b soient premiers entre eux dans les formules (6), qu'ils le soient également dans les formules (7) si n est impair, mais qu'ils aient 2 pour plus grand diviseur commun si n est pair. Enfin, pour que z soit impair dans les formules (7), il faut, puisque f et g sont impairs, que le produit ab soit de l'une des deux formes $8l$ ou $4l+1$. Ainsi :

THÉORÈME VII. — *Pour trouver toutes les solutions entières et premières entre elles de l'équation*

$$(3)\qquad x^2+ny^2=z^{2m},$$

en supposant z impair, il faut d'abord chercher toutes les solutions de l'équation

$$(4)\qquad p^2+ny^2=z^2,$$

ou plutôt toutes les formules générales propres à les déterminer. Ces formules générales se déduisent des suivantes :

$$(6)\qquad z=af^2+bg^2,\quad p=af^2-bg^2,\quad q=2fg,\quad ab=n,$$

$$(7)\qquad z=\frac{af^2+bg^2}{2},\quad p=\frac{af^2-bg^2}{2},\quad q=fg,\quad ab=n,$$

en prenant pour a et b toutes les décompositions du nombre n en deux facteurs premiers entre eux pour les formules (6) *et, pour les for-*

mules (7), *en deux facteurs premiers entre eux, si n est de la forme* $4l+1$, *en deux facteurs dont le plus grand diviseur commun soit* 2, *si* $n = 8l$. *Puis on obtiendra les valeurs de* x *et de* y, *au moyen de l'équation*

$$(5) \qquad \pm x \pm y\sqrt{-n} = (p+q\sqrt{-n})^m = \mathrm{P} + \mathrm{Q}\sqrt{-n},$$

en remplaçant dans les fonctions entières P, Q *les indéterminées* p *et* q *par les fonctions quadratiques déduites des formules* (6) *et* (7).

16. Afin d'éclaircir cette méthode par un exemple, proposons-nous de trouver toutes les solutions de l'équation

$$x^2 + 5y^2 = z^4,$$

en nombres entiers et premiers entre eux deux à deux. La valeur de z sera nécessairement impaire; car autrement x et y seraient tous deux impairs, et le premier membre de notre équation aurait la forme $8l+6$, ce qui est impossible pour un bicarré. Comme d'ailleurs 5 est l'une des valeurs de n auxquelles s'appliquent les derniers théorèmes, les valeurs premières entre elles de x, de y et de z seront déterminées par les deux équations

$$\pm x \pm y\sqrt{-5} = (p+q\sqrt{-5})^2, \quad p^2 + 5q^2 = z^2.$$

Toutes les solutions de la dernière équation sont exprimées en fonction de deux nouvelles indéterminées f, g, au moyen des formules

$$z = f^2 + 5g^2, \quad \pm p = f^2 - 5g^2, \quad q = 2fg,$$
$$z = \frac{f^2+5g^2}{2}, \quad \pm p = \frac{f^2-5g^2}{2}, \quad q = fg.$$

En substituant ces valeurs de p et de q dans les formules

$$x = p^2 - 5q^2, \quad y = 2pq,$$

on obtient, pour exprimer d'une manière générale toutes les solutions

cherchées, les deux systèmes de formules

$$x=f^4-30f^2g^2+25g^4,\quad y=4fg(f^2-5g^2),\quad z=f^2+5g^2,$$
$$x=\frac{f^4-30f^2g^2+25g^4}{4},\qquad y=fg(f^2-5g^2),\qquad z=\frac{f^2+5g^2}{2}.$$

Les nombres indéterminés f et g doivent être entiers et premiers entre eux; de plus, l'un d'eux doit être pair dans le premier groupe de formule, tandis qu'ils doivent être tous deux impairs dans le second.

Dans l'exemple que nous venons de choisir, la méthode de décomposition employée par Fermat et par Euler pouvait conduire au même résultat.

Mais nous donnerons dans la seconde Partie un grand nombre d'applications où la méthode de Fermat serait complétement impuissante.

17. On peut établir des théorèmes analogues aux précédents pour les nombres complexes $\sqrt{a}x+\sqrt{-c}y$, employés par Euler au Chapitre XII de la deuxième Partie de son Algèbre, pourvu que le nombre des classes de formes quadratiques de déterminant $-ac$ soit égal au nombre des genres, comme cela a lieu quand le produit ac est l'un des déterminants composés mentionnés précédemment (13). Supposant donc cette condition remplie, proposons-nous de trouver toutes les solutions propres de l'équation

$$(1)\qquad ax^2+cy^2=z^m,\quad a>1,\quad c>1.$$

THÉORÈME VIII. — *Si l'exposant m est pair, l'équation proposée n'admet aucune solution en nombres entiers et différents de zéro.*

Comme, par hypothèse, chaque genre de formes quadratiques de déterminant $-ac$ ne renferme qu'une seule classe, le genre principal sera représenté par la classe principale, et la classe représentée par la forme réduite $(a, 0, c)$ constituera un genre différent du genre principal. Il est donc impossible que cette forme ax^2+by^2 devienne égale à un carré, puisque tout carré appartient nécessairement au genre principal.

18. Si m est impair, les deux nombres z et z^m appartiennent au même genre relativement au déterminant $-ac$; le second étant, par hypothèse, représenté par la forme (a, o, c), il en est de même du premier z, en sorte que l'équation

$$ap^2 + cq^2 = z \tag{2}$$

donnera toutes les valeurs de z propres à vérifier l'équation (1), lorsqu'on égalera, de toutes les manières possibles, aux lettres p et q des valeurs entières et premières entre elles. Nous écarterons les solutions où z reçoit une valeur paire; dans le petit nombre de cas où ces solutions sont possibles, elles devront être étudiées séparément. Le nombre z étant impair, toutes les représentations propres de z^m par la forme (a, o, c) se déduisent de la formule

$$\pm\sqrt{a}x \pm \sqrt{-c}y = (\sqrt{a}p + \sqrt{-c}q)^m, \tag{3}$$

en y égalant les indéterminées p et q à toutes les représentations propres de z par la même forme (a, o, c). En effet, d'après les principes rappelés précédemment (8 et 9), les diverses représentations de z^m par les diverses classes de formes quadratiques de déterminant $-ac$ correspondent deux à deux aux diverses solutions de la congruence

$$\alpha^2 + ac \equiv o \pmod{z^m};$$

d'ailleurs, z étant impair, les racines de cette congruence correspondent une à une aux racines de la congruence

$$\beta^2 + ac \equiv o \pmod{z};$$

nous aurons donc démontré que la formule (3) détermine toutes les représentations propres de z^m, si nous faisons voir qu'elle donne, pour chacune des racines β, des valeurs de x et de y qui satisfont à la congruence $x \equiv \beta y \pmod{z}$.

Nous démontrerons, du reste, que ces valeurs sont premières entre elles, et qu'ainsi elles forment des représentations propres de z^m par (a, o, c). Multiplions à cet effet les deux membres de l'équation (3)

par $\sqrt{ap}-\sqrt{-cq}$, ce qui donnera pour produit

$$\pm(apx+cqy)\pm\sqrt{-ac}(py-qx)=\left[(ap^2-cq^2)+\sqrt{-ac}\,2pq\right]^{\frac{m-1}{2}}z.$$

Comme l'exposant $\frac{m-1}{2}$ est entier, nous pouvons poser

$$(a)\qquad \left[(ap^2-cq^2)+\sqrt{-ac}\,2pq\right]^{\frac{m-1}{2}}=\mathrm{P}+\sqrt{-ac}\,\mathrm{Q},$$

en désignant par P et par Q deux fonctions entières de p et de q; et nous aurons les deux équations

$$(b)\qquad apx+cqy=\pm\mathrm{P}z,\quad py-qx=\pm\mathrm{Q}z;$$

d'où, ayant égard à l'équation $ap^2+cq^2=z$, nous déduirons

$$(c)\qquad x=\mp(\mathrm{P}p\mp cq\mathrm{Q}),\quad y=\pm(q\mathrm{P}\pm ap\mathrm{Q}).$$

D'abord la seconde des équations (b) montre que les valeurs de x et de y vérifieront la congruence $x\equiv\beta y\pmod{z}$, si l'on choisit pour p et q celle des représentations de z qui correspond à la racine β de la congruence $\beta^2+ac\equiv 0\pmod{z}$, puisque alors on aura

$$p\equiv\beta q\pmod{z}.$$

De plus, ces valeurs de x et de y sont premières entre elles, pourvu que z soit premier avec le module $-ac$, ce qui a toujours lieu quand ac ne renferme pas de facteur carré impair. En effet on déduit de la formule (3)

$$\pm x=p\left[(ap^2)^{\frac{m-1}{2}}-\frac{m(m-1)}{1.2}(ap^2)^{\frac{m-3}{2}}(cq^2)+\frac{m(m-1)(m-2)(m-3)}{1.2.3.4}(ap^2)^{\frac{m-5}{2}}(cq^2)^2+\ldots\right].$$

Si x et y avaient un diviseur premier commun θ, on voit par l'équation (1) que ce diviseur serait un facteur de z; on aurait donc

$$cq^2\equiv -ap^2\pmod{\theta}.$$

La dernière équation se changerait donc en congruence suivant le

module θ par la substitution de cq^2 à $-ap^2$; donc

$$\pm x \equiv p(ap^2)^{\frac{m-1}{2}}\left[1+\frac{m(m-1)}{1.2}+\frac{m(m-1)(m-2)(m-3)}{1.2.3.4}+\ldots\right],$$

$$\pm x \equiv 2^{\frac{m-1}{2}}p(ap^2)^{\frac{m-1}{2}} \pmod{\theta};$$

θ serait donc diviseur commun de z et du produit ap. On déduirait de l'équation $ap^2+cq^2=z$, que θ diviserait aussi cq. D'ailleurs il ne divise ni a ni c, puisque l'on suppose z premier avec le produit ac; il devrait donc diviser en même temps p et q, contrairement à l'hypothèse.

Donc, pour toute valeur de z impaire et première avec le produit ac, l'équation (3) détermine pour x et y toutes les représentations propres de z^m par la forme ax^2+cy^2, pourvu qu'on prenne pour p et q toutes les solutions propres de l'équation $ap^2+cq^2=z$. D'ailleurs la formule $ap^2+cq^2=z$ donne toutes les valeurs de z compatibles avec l'équation proposée. Toutes les solutions de cette équation se déduisent donc de la formule (3) jointe à la formule (2), en donnant aux lettres p et q, de toutes les manières possibles, des valeurs entières et premières entre elles. Donc :

THÉORÈME IX. — *Si l'exposant m est un nombre entier impair, les solutions de l'équation*

$$ax^2+cy^2=z^m, \tag{1}$$

en nombres entiers et premiers entre eux, dont le dernier z doit être impair et premier avec le produit ac, sont exprimées d'une manière générale par les formules

$$\left\{\begin{aligned}
\pm x &= p\left[(ap^2)^{\frac{m-1}{2}}-\frac{m(m-1)}{1.2}(ap^2)^{\frac{m-3}{2}}(cq^2)\right.\\
&\qquad\left.+\frac{m(m-1)(m-2)(m-3)}{1.2.3.4}(ap^2)^{\frac{m-5}{2}}(cq^2)^2-\ldots\right],\\
\pm y &= q\left[m(ap^2)^{\frac{m-1}{2}}+\frac{m(m-1)(m-2)}{1.2.3}(ap^2)^{\frac{m-3}{2}}(cq^2)\right.\\
&\qquad\left.+\frac{m(m-1)\ldots(m-4)}{1.2\ldots5}(ap^2)^{\frac{m-5}{2}}(cq^2)^2-\ldots\right].
\end{aligned}\right. \tag{3}$$

$$z=ap^2+cq^2, \tag{2}$$

où l'on désigne par p et q deux nombres entiers et premiers entre eux.

19. Soit $m=3$. La formule $2x^2+3y^2$ ne peut devenir égale à un cube pair ou multiple de 3, tant que les valeurs de x et de y sont des nombres entiers et premiers entre eux. D'ailleurs 6 est l'un des déterminants qui remplissent les conditions supposées dans le théorème précédent. Les solutions, en nombres entiers et premiers entre eux, de l'équation

$$2x^2+3y^2=z^3$$

sont donc exprimées d'une manière générale par les formules

$$z=2p^2+3q^2, \quad \pm x=p(2p^2-9q^2), \quad \pm y=q(6p^2-3q^2).$$

Aucun des deux nombres x ou y déterminés par ces formules ne devient égal à l'unité pour des valeurs de p et de q entières et premières entre elles. On peut donc énoncer ces deux théorèmes :

Il est impossible d'obtenir un cube en ajoutant 3 *unités au double d'un carré entier.*

Si l'on triple les carrés 1, 4, 9, 16,... *et qu'on ajoute* 2 *à chacun des produits, aucune des sommes obtenues n'est égale à un cube.*

20. Les formes quadratiques dont le déterminant est positif donnent lieu à des théorèmes analogues aux précédents, avec cette différence que, dans le second membre des équations complexes, auxquelles on a recours pour déterminer les solutions des équations proposées, on doit introduire un facteur complexe de l'unité déduit d'une solution de l'équation

$$t^2-nu^2=1.$$

La présence de ce facteur rend plus difficile l'emploi des nombres complexes compris dans la formule $a+b\sqrt{n}$, où n désigne un nombre positif non carré, excepté les cas particuliers où l'on peut démontrer que le facteur complexe de l'unité doit se réduire à ± 1. C'est ce qui a lieu, par exemple, dans l'application que Dirichlet a faite des nom-

bres $f+g\sqrt{5}$, pour démontrer l'impossibilité de l'équation de Fermat

$$x^5+y^5+z^5=0.$$

21. Je terminerai cette partie théorique de mon travail en rappelant quelques résultats analogues obtenus par Euler et par Legendre. Le premier reconnaît, dans la seconde Partie de son *Algèbre* (nos **186, 187, 188**), que la formule ax^2+cy^2 ne peut pas toujours se transformer en un carré, tandis qu'elle peut toujours se transformer en une puissance de degré impair quelconque; mais il ne dit rien qui puisse faire distinguer le cas où sa méthode peut faire connaître toutes les solutions du problème de ceux où elle n'en donne qu'une partie. De plus, la formule ax^2+cy^2 peut aussi se transformer en des puissances de degré pair; il suffit, pour cela, qu'elle soit comprise dans le genre principal pour le déterminant $-ac$. Cela a lieu, évidemment, pour la formule $5x^2+11y^2$, qui devient égale à 16 quand on y fait $x=y=1$, et à 49 quand on pose $x=1$, $y=2$.

Legendre, dans sa théorie de la multiplication des formes quadratiques (*Théorie des nombres*, IV, § 4 et 5), donne la solution d'un problème qui offre beaucoup d'analogie avec ceux dont nous nous sommes occupés. Il apprend à déterminer, quand cela est possible, une fonction x, homogène et du second degré, de deux variables arbitraires y et z, et deux autres fonctions homogènes des mêmes variables, Y, Z, du degré m, et propres à rendre l'équation

$$\text{(A)} \qquad LY^2+MYZ+NZ^2=bx^m,$$

identique par rapport aux variables arbitraires y et z. Il est évident que cette solution analytique de l'équation (A) donnera une infinité de solutions numériques, lorsqu'on attribuera des valeurs entières aux variables y et z. Mais il n'est pas évident qu'on obtienne, par ce moyen, tous les systèmes de nombres entiers et premiers entre eux Y, Z, x, propres à vérifier cette équation. C'est là une question importante dont Legendre ne s'est pas occupé. Nous sommes loin de l'avoir envisagée dans toute son étendue. Toutefois les théorèmes que nous venons d'établir apportent à l'Analyse indéterminée des ressources nouvelles, dont j'essayerai de faire connaître les avantages dans les applications qui formeront la deuxième Partie de ce Mémoire.

DEUXIÈME PARTIE.

I. — Sur l'équation $x^2+cy^2=z^3$.

22. Fermat rappelle, dans une Lettre au chevalier Digby, deux théorèmes qu'il avait communiqués à Frénicle : « Je lui avais écrit, dit-il, qu'il n'y a qu'un nombre carré entier qui, joint au binaire, fasse un cube, et que ledit carré est 25, auquel, si vous ajoutez 2, il se fait 27, qui est un cube. Il a peine à croire cette proposition négative, et la trouve trop hardie et trop générale. Mais, pour augmenter son étonnement, je dis que, si l'on cherche un carré qui, ajouté à 4, fasse un cube, il ne s'en trouvera jamais que deux en nombres entiers, savoir 4 et 121; car 4 ajouté à 4 fait 8, qui est un cube; et 121 ajouté à 4 fait 125, qui est aussi un cube; mais, après cela, toute l'infinité des nombres n'en saurait fournir un troisième qui ait la même propriété. »

Euler et Legendre ont démontré ces théorèmes à l'aide des nombres complexes $a+b\sqrt{-1}$, $a+b\sqrt{-2}$, sans se mettre en peine de justifier cet emploi. Leur démonstration est complétée par notre théorème III (9), où l'usage qu'ils ont fait de ces nombres complexes est démontré légitime. Nous retrouverons ces théorèmes de Fermat comme cas particuliers dans la solution d'une question plus générale dont nous allons nous occuper.

23. Désignons par n un nombre premier impair, et par c l'un des nombres 1, 2, 3, 4 ou 7, et proposons-nous de trouver toutes les solutions entières de l'équation

$$x^2+cn^{2\alpha}=z^3, \tag{1}$$

en nous bornant toutefois à celles où la valeur de z est impaire, quand $c=7$. Nous partagerons ces solutions en deux groupes, dont l'un renfermera celles où les deux nombres x et n sont premiers entre eux, et l'autre celles où x est multiple de n. Quand $c=1$, 2 ou 3, z est néces-

sairement impair, premier avec c, avec n et avec x, tant que les deux nombres x et n sont premiers entre eux; comme d'ailleurs le théorème III est applicable à ces valeurs de c, toutes les solutions du premier groupe sont données par les formules du n° 9, d'où l'on déduit

$$(2) \quad \pm x = p(p^2 - 3cq^2), \quad \pm n^\alpha = q(3p^2 - cq^2), \quad z = p^2 + cq^2.$$

Si $c = 4$, outre les solutions en nombres impairs déterminées par les formules (2), le premier groupe renferme aussi des solutions en nombres pairs non divisibles par n. Pour les trouver, posons $x = 2x_1$, $z = 2z_1$; l'équation (1) divisée par (4) devient

$$x_1^2 + n^{2\alpha} = 2z_1^3.$$

Or cette équation est résolue d'une manière générale par les formules

$$z_1 = f^2 + g^2, \quad \pm x_1 \pm n^\alpha \sqrt{-1} = (1 + \sqrt{-1})(f + g\sqrt{-1})^3,$$

dans lesquelles f et g sont des nombres premiers entre eux, l'un pair et l'autre impair. D'abord la formule $z_1 = f^2 + g^2$ donne toutes les valeurs convenables de z_1; ensuite pour chaque valeur particulière de z, on obtient toutes les représentations propres du produit $2z^3$ par la forme $x^2 + y^2$, au moyen de la formule

$$\pm x_1 \pm y\sqrt{-1} = (1 + \sqrt{-1})(f + g\sqrt{-1})^3,$$

en prenant pour f et g toutes les solutions propres de la formule $z_1 = f^2 + g^2$; car les valeurs de x_1 et de y sont impaires, et par conséquent leur rapport vérifie la congruence $u^2 + 1 \equiv 0 \pmod 2$; de plus, comme f et g reçoivent des valeurs liées avec toutes les racines de la congruence $\beta^2 + 1 \equiv 0 \pmod{z_1}$ par la relation $f - g\beta \equiv 0 \pmod{z_1}$, les divers systèmes de valeurs de x_1 et de y seront aussi liés respectivement par la relation semblable $x_1 \equiv \beta y \pmod{z_1}$ avec toutes les diverses racines de la congruence $\beta^2 + 1 \equiv 0 \pmod{z_1}$; on le démontre comme au n° 9, en multipliant les deux membres de la formule par $f - g\sqrt{-1}$. Si l'on tient compte du double signe $\pm$ qu'on peut donner aux indéterminées, on a deux fois autant de représentations propres et diffé-

rentes entre elles du produit $2z^3$ qu'il y a de solutions de la congruence $\beta^2+1\equiv 0 \pmod{z_1}$; d'ailleurs le nombre des solutions de cette congruence est le même que celui des solutions de la congruence $u^2+1\equiv 0 \pmod{2z_1^3}$. Donc, à cause des principes rappelés au n° 8, notre formule donne toutes les représentations propres du produit $2z_1^3$, lorsqu'on y substitue successivement toutes les solutions propres de l'équation $z_1=f^2+g^2$. On en déduit les formules

$$\pm x_1=(f+g)(f^2-4fg+g^2),$$
$$\pm n^\alpha=(f-g)(f^2+4fg+g^2), \quad z_1=f^2+g^2,$$

dont la seconde permettra de déterminer les valeurs des deux nombres f et g, et par suite celles de x_1 et de z_1.

Comme f et g sont de parités différentes, si l'on pose $f+g=p$, $-g=q$, les deux nombres p et q seront impairs, et les formules précédentes deviendront

$$(3)\quad \pm 2x_1=\pm x=p(p^2-3q^2), \quad \pm 2n^\alpha=q(3p^2-q^2), \quad 2z_1=z=p^2+q^2.$$

Quand $c=7$, les solutions du premier groupe sont données par les formules (2) si le carré x^2 est pair, et par d'autres formules que nous omettrons si, le carré x^2 étant impair, le nombre z est pair.

Ainsi celles des solutions de l'équation (1), où les deux nombres x et n sont premiers entre eux, seront complétement déterminées par les formules (2), si c désigne l'un des trois nombres 1, 2 ou 3; elles seront déterminées par les formules (2) et (3) si c égale 4; enfin, si c égale 7, nous nous bornerons à chercher les solutions où le carré x^2 est pair; celles de ces solutions où x n'est pas multiple de n sont complétement déterminées par les formules (2).

24. Pour obtenir les solutions du second groupe, celles où x est multiple de n, posons $x=n^\beta\xi$, $z=n^\gamma\zeta$, en désignant par ξ et ζ deux nombres entiers divisibles par n. De plus, pour ne pas trop allonger la discussion, supposons n et c premiers entre eux. L'équation proposée (1) prend la forme

$$n^{2\beta}\xi^2+cn^{2\alpha}=n^{3\gamma}\zeta^3,$$

et elle n'est possible qu'autant que les deux plus petits des exposants 2α, 2β, 2γ sont égaux. Le cas où les trois exposants sont égaux se ramène à celui où $n=1$; car alors l'équation devient $\xi^2+c=\zeta^3$. Mais cela n'a lieu que si $\alpha=3\lambda$. Les solutions de cette forme se déduiront de celles de l'équation $\xi^2+c=\zeta^3$, qui sera résolue plus bas, en multipliant ξ par $n^{3\lambda}$, et ζ par $n^{2\lambda}$. Nous pouvons donc supposer que l'un des trois exposants 2α, 2β, 3γ est plus grand que les deux autres. Les solutions cherchées seront comprises dans les trois équations

$$(4)\qquad n^{2(\beta-\alpha)}\xi^2+c=\zeta^3,\quad \xi^2+cn^{2(\alpha-\beta)}=\zeta^3,\quad \xi^2+c=n^{3\gamma-2\alpha}\zeta^3.$$

La première suppose $\alpha=3\lambda$, puisque l'on a $2\alpha=3\gamma$. De plus elle rentre comme cas particulier dans l'équation $x^2+c=\zeta^3$, dont nous allons immédiatement nous occuper.

25. Si l'on suppose $n=1$, les deux nombres x et n seront nécessairement premiers entre eux, en sorte que toutes les solutions de l'équation (1) seront comprises dans le premier groupe, et se déduisent des formules (2) et (3), avec la restriction posée pour le cas où $c=7$. Quand $c=1$, 2 ou 3, toutes ces solutions sont données par les formules (2), dont la seconde exige qu'on fasse

$$q=\pm 1,\quad 3p^2=c\pm 1,\quad \pm x=p(p^2-3cq^2),$$

ce qui est impossible si $c=3$. Dans le cas où $c=1$, on doit faire $p=0$, $x=0$; et si $c=2$, on doit faire $q=\pm 1$, $p=\pm 1$, ce qui donne $\pm x=5$, $z=3$. Donc :

THÉORÈME I. — *Dans toute la série des carrés* 1, 4, 9, 16, 25,..., *il n'en existe aucun qui devienne égal à un cube quand on l'augmente d'une unité.*

THÉORÈME II. — *Le seul cube qu'on puisse obtenir en ajoutant* 2 *à un carré entier est* 27, *qu'on obtient en ajoutant* 2 *à* 25. (FERMAT.)

THÉORÈME III. — *Aucun cube n'est égal à un carré entier augmenté de trois unités.*

Soit $c=4$. Les solutions en nombres impairs sont déterminées par les formules (2), dont la seconde $q(3p^2-4q^2)=\pm 1$ n'admet que les solutions $p=\pm 1$, $q=\pm 1$, d'où l'on déduit $x=\pm 11$, $y=5$. Les

solutions en nombres pairs se déduisent des formules (3), dont la seconde $q(3p^2-q^2)=\pm 2$ n'admet, en nombres impairs, que les solutions $p=\pm 1$, $q=\pm 1$, auxquelles correspondent $x=\pm 2$, $z=2$. Donc :

THÉORÈME IV. — *Dans la suite indéfinie des carrés* 1, 4, 9, 16, 25,..., *il n'y en a que deux qui, ajoutés à* 4, *fassent des cubes; ces deux carrés sont* 4 *et* 121, *qui, ajoutés à* 4, *font respectivement les deux cubes* 8 *et* 125. (FERMAT.)

Soit $c=7$, et supposons x pair. Toutes les conditions du théorème III (**9**) se trouvant remplies, les solutions cherchées sont déterminées par les formules (2). La seconde $q(3p^2-7q^2)=\pm 1$ étant impossible, nous concluons :

THÉORÈME V. — *Dans la suite indéfinie des carrés pairs, il n'en est aucun qui, étant ajouté à* 7, *fasse un cube.*

26. Supposons $n>1$ et non diviseur de c. Si α est multiple de 3, outre les solutions où le nombre x est premier avec n, et qui seront déterminées par les formules (2) et (3), conformément à ce que nous avons vu au n° **23**, il y aura des solutions déduites de celles de l'équation $\xi^2+c=\zeta^3$, en posant $x=n^\alpha\xi$ et $z=n^{\frac{2\alpha}{3}}\zeta$. Il pourra de plus y avoir des solutions déterminées par la première des équations (4). Elle ne diffère de l'équation que nous venons de résoudre (5) qu'en ce que l'on doit avoir $x=n^{\alpha-\beta}\zeta$. Comme n doit être impair, elle est impossible si $c=1$, 2 ou 3; elle n'est possible qu'en supposant $\alpha=\beta+1$, et $n=5$ ou 11, si $c=4$. Enfin, quand $c=7$ et qu'on exige que la valeur de x soit paire, il n'y a aucune solution de ce genre.

Dans la suite, nous supposerons que l'exposant α est de l'une des deux formes $3l+1$, $3l+2$, en sorte que toutes les solutions du second groupe se déduiront respectivement de celles des deux équations

$$\xi^2+cn^{2(\alpha-3\lambda)}=\zeta^3, \tag{5}$$

$$\xi^2+c=n^{3\gamma-2\alpha}\zeta^3, \tag{6}$$

en faisant $x=n^{3\lambda}\xi$, $z=n^{2\lambda}\zeta$ pour la première, et $x=n^\alpha\xi$, $z=n^\gamma\zeta$

pour la seconde. D'ailleurs la première suppose $\alpha > 3\lambda$; il n'y a donc pas lieu de la considérer si $\alpha = 1$ ou 2. La seconde suppose que le nombre premier n soit lui-même de la forme $x^2 + cy^2$.

Nous réduirons donc les solutions de l'équation (1) aux seules solutions du premier groupe, si, supposant $\alpha = 1$ ou 2, nous désignons par n un nombre premier impair non diviseur de la formule $x^2 + c$, et premier avec c. C'est ce que nous allons faire successivement pour les diverses valeurs de c.

27. Supposons que dans l'équation (1) on ait $c = 1$, $\alpha = 1$ ou 2, et que n soit un nombre premier $4l + 3$. Le nombre n sera non diviseur de la formule $x^2 + 1$, en sorte que (**26**) toutes les solutions cherchées devront se déduire des formules (2). La seconde de ces formules

$$\pm n^\alpha = q(3p^2 - q^2)$$

ne peut être vérifiée en nombres premiers entre eux qu'en posant

$$(a) \qquad q = \pm n^\alpha, \quad 3p^2 = n^{2\alpha} - 1,$$

ou

$$(b) \qquad q = \pm 1, \quad 3p^2 = 1 + n^\alpha.$$

Prenons d'abord $\alpha = 1$. Les équations (b) ne sont possibles qu'autant que le nombre n est de l'une des formes $9l + 2$ ou $27l - 1$. Il faut, en outre, que le quotient $\frac{n+1}{3}$ soit un carré p^2. Les valeurs de n qui vérifient la dernière condition se déduiront de la formule $n = 3p^2 - 1$, en donnant à p des valeurs paires 2, 4, 6,..., et en rejetant tous les résultats qui ne sont pas des nombres premiers. En faisant $p = 2, 4, 6, 8, 12, 14,...$, on trouve les nombres premiers 11, 47, 107, 191, 431, 487,....

La solution (a) dépend de l'équation $3p^2 = n^2 - 1$. Posons $p = 2fg$; nous obtiendrons par décomposition

$$n \pm 1 = 2f^2, \qquad n \mp 1 = 6g^2,$$
$$n = f^2 + 3g^2, \quad f^2 - 3g^2 = 1.$$

Le signe choisi dans la dernière équation est commandé par ce fait, que -1 n'est pas résidu quadratique de 3. La première conséquence de ces formules est que le nombre n doit être de la forme $6l+1$ pour que la solution (a) puisse exister. Mais cette condition n'est pas suffisante; car toutes les valeurs positives de f et de g propres à vérifier l'équation $f^2-3g^2=1$ se déduisent de la formule

$$f+g\sqrt{3}=(2+\sqrt{3})^m,$$

en donnant à l'exposant m des valeurs entières et positives. En élevant au carré les deux nombres de cette équation, on trouve

$$f^2+3g^2+2fg\sqrt{3}=n+p\sqrt{3}=(2+\sqrt{3})^{2m},$$

et l'on en déduit

$$(8)\quad\begin{cases} n=7^m+\dfrac{m(m-1)}{1.2}7^{m-2}4^2 3+\dfrac{m(m-1)(m-2)(m-3)}{1.2.3.4}7^{m-4}4^4 3^2+\ldots, \\ p=m7^{m-1}4+\dfrac{m(m+1)(m-2)}{1\ 2.3}7^{m-3}4^3 3 \\ \qquad +\dfrac{m(m-1)\ldots(m-4)}{1.2\ldots5}7^{m-5}4^5 3^2+\ldots. \end{cases}$$

Ainsi, dans le cas où $\alpha=1$, aucune des solutions (a) ou (b) n'est possible si le nombre n n'est pas de l'une des trois formes $6l+1$, $9l+2$, $17l-1$. La solution (b) est seule possible si le nombre n est de l'une des formes $9l+2$, $27l-1$. Au contraire la solution (a) est seule possible si n est de la forme $6l+1$.

28. Or les nombres premiers $4l+3$, qui ne sont d'aucune des formes $6l+1$, $9l+2$, $27l-1$, sont le nombre 3 et les nombres premiers renfermés dans les cinq formules $108l+(23, 35, 59, 71, 95)$. Nous avons ainsi deux théorèmes analogues à ceux de Fermat.

THÉORÈME VI. — *Aucun carré entier, ajouté à* 9, *ne fait un cube.*

THÉORÈME VII. — *Si l'on désigne par n l'un des nombres premiers compris dans les formules* $108l+(23, 35, 59, 71, 95)$, *tels que* 23,

59, 71, 131, 167,..., *il est impossible d'obtenir un cube en ajoutant un carré entier au carré du nombre n.*

Si le nombre n est de la forme $36l+11$, la solution (b) est la seule possible, et elle exige que n soit de la forme $12k^2-1$. Or, au-dessous de 1000, les seuls nombres premiers compris en même temps dans les deux formules $36l+11$, $12k^2-1$ sont 11, 47, 191, 587, qui correspondent aux valeurs 1, 2, 4 et 7 de k. Pour tous les autres nombres premiers $36l+11$, inférieurs à 1000, l'équation $x^2+n^2=z^3$ est impossible en nombres entiers. Ces nombres premiers sont 83, 263, 407, 443, 479, 659, 839, 911, 947, au sujet desquels nous pouvons énoncer le théorème suivant :

THÉORÈME VIII. — *Si l'on désigne par n l'un des nombres premiers* 83, 263, 407, 443, 479, 659, 839, 911, 947, *il est impossible de trouver un carré entier qui fasse un cube, lorsqu'on l'ajoute au carré* n^2.

Si n est l'un des nombres 11, 47, 191, 587, l'équation $x^2+n^2=z^3$ n'admet, en nombres entiers et positifs, qu'une seule solution déterminée par les formules (2) et (b) : $x=2k(4k^2-3)$, $z=1+4k^2$, $n=12k^2-1$. Les solutions correspondantes sont : $x=2$, $z=5$, $n=11$; $x=52$, $z=17$, $n=47$; $x=488$, $z=65$, $n=191$; $x=2702$, $z=197$, $n=587$. Nous pouvons donc énoncer les théorèmes suivants :

THÉORÈME IX. — *Dans toute la série des carrés entiers* 1, 4, 9, 16,..., *il n'y en a qu'un seul qui, ajouté à* 121, *forme un cube : ce carré est* 4, *qui fait le cube* 125, *quand on l'ajoute à* 121.

THÉORÈME X. — *Si l'on cherche à former un cube en ajoutant un carré entier au carré* 2209, *on n'y parviendra que d'une seule manière, savoir en ajoutant le carré* 2704, *ce qui fait* 4913, *cube de* 17.

THÉORÈME XI. — *La seule manière d'obtenir un cube en ajoutant un carré entier au nombre* 36481 *est d'ajouter le carré* 238144, *ce qui fait* 274625, *cube de* 65.

THÉORÈME XII. — *Le seul cube que l'on obtienne en ajoutant un carré entier au carré de* 587 *est le cube de* 197.

Les nombres renfermés dans la formule $27l-1$ donneraient des théorèmes analogues, car les seuls de ces nombres qui soient en même

temps de la forme $12k^2-1$ sont, au-dessous de 1000, 107, 431, 971. Le carré de chacun de ces trois nombres ne fait qu'un seul cube quand on lui ajoute successivement tous les carrés entiers. Les racines de ce carré et de ce cube se déduisent des formules (2) et (6), comme nous l'avons fait dans le cas précédent. Les autres nombres premiers compris dans la formule $27l-1$ et inférieurs à 1000, savoir 53, 269, 539, 593, 647, 701, 809, 863, donnent lieu à un théorème semblable au théorème VIII.

29. Si le nombre premier n est de la forme $12l+7$, l'équation $x^2+n^2=z^3$ n'admet pas de solution en nombres entiers, à moins que le nombre n ne vérifie la première des formules (8), pour une valeur convenablement choisie de l'exposant m. Dans ce cas les solutions sont données par les formules

$$\pm x = p(p^2-3n^2),\quad z=p^2+n^2,$$

où les valeurs de p et de n doivent vérifier les formules (8) pour une même valeur de l'exposant m. En faisant $m=1, 2, 3$, on trouve

$$n = 7,\ 97,\ 1351.$$

Laissant de côté 97, qui est de la forme $12l+1$, nous concluons de ce résultat que, pour tout nombre premier $12l+7$, inférieur à 1350 et différent de 7, l'équation $x^2+n^2=z^3$ est impossible. A la valeur $n=7$ correspond la solution $x=524$, $z=65$. Donc :

THÉORÈME XIII. — *Si l'on désigne par n l'un des nombres premiers* $12l+7$, *inférieur à* 1350 *et différent de* 7, *tels que* 19, 31, 43, 67, 79, 103, 127,..., *il est impossible de faire un cube en ajoutant un carré entier au carré* n^2.

THÉORÈME XIV. — *Dans toute la série des carrés entiers, le carré* 274 579 *est le seul qui, ajouté à* 49, *fasse un cube.*

30. Soit $a=2$. L'équation $3p^2=1+n^2$ (27) est impossible, en sorte que l'équation (1) n'admet pas d'autre solution entière que celle qui est déterminée par les équations (*a*) $q=\pm n^2$, $3p^2=n^4-1$. En posant comme précédemment $p=2fg$, on trouve par décomposition

$$n^2+1=2f^2,\quad n^2-1=6g^2,\quad n^2=f^2+3g^2,\quad f^2-3g^2=1.$$

Le nombre n doit donc être de la forme $6l+1$; il sera donc de la forme $12l+7$, puisqu'il doit être en même temps de la forme $4x+3$. De plus son carré doit vérifier l'équation

$$n^2 = 7^m + \frac{m(m-1)}{1.2} 7^{m-2} 4^2 3 + \frac{m(m-1)(m-2)(m-3)}{1.2.3.4} 7^{m-4} 4^4 3^2 + \dots$$

Comme les carrés ne peuvent correspondre qu'aux valeurs paires de m, on peut employer la formule suivante, où p désigne un nombre entier quelconque :

$$(9) \quad \begin{cases} n^2 = (97)^p + \frac{p(p-1)}{1.2} (97)^{p-2} (56)^2 3 \\ \qquad + \frac{p(p-1)(p-2)(p-3)}{1.2.3.4} (97)^{p-4} (56)^4 3^2 + \dots \end{cases}$$

On reconnaît aisément que les trois premières valeurs de cette formule ne sont pas des carrés; qu'à partir de la quatrième la valeur de n serait supérieure à 20 000. L'équation $x^2 + n^4 = z^3$ n'admet donc pas de solution entière quand n désigne un nombre premier compris dans la formule $12l+7$ et inférieur à 20 000.

THÉORÈME XV. — *Si l'on désigne par n un nombre premier* $12l+7$, *inférieur à* 20 000, *tel que* 19, 31, 43, 67, 79, 103,..., *on ne trouvera aucun carré entier qui, ajouté au bicarré* n^4, *fasse un cube.*

31. Quand $n=3$, les équations (a) et (b) sont évidemment impossibles; mais si l'on suppose en même temps $\alpha = 2$, l'équation

$$\pm 3^2 = q(3p^2 - q^2)$$

peut se décomposer d'une troisième manière, sans qu'il soit nécessaire que p et q aient un facteur commun; on peut poser

$$q = \pm 3, \quad 3p^2 - 9 = 3, \quad p = \pm 2, \quad x = 46, \quad z = 13.$$

THÉORÈME XVI. — *Dans toute la série des carrés entiers,* 2116 *est le seul qui fasse un cube, lorsqu'on l'ajoute au carré* 81.

32. Soit $c=2$; les non-diviseurs de la formule $x^2 + 2y^2$ son'

$8l+5$ et $8l+7$. Nous supposerons que n est un nombre premier de l'une de ces deux formes, et que $\alpha = 1$ ou 2, en sorte que toutes les solutions entières de l'équation $x^2+n^{2\alpha}=z^3$ se déduiront (26) des seules formules (2), qui deviennent, dans notre cas,

$$(2)\quad \pm x = p(p^2-6q^2), \quad \pm n^\alpha = q(3p^2-2q^2), \quad z = p^2+2q^2.$$

La seconde se décompose de l'une des deux manières suivantes :

$$(a)\qquad q = \pm n^\alpha, \quad 3p^2 = 2n^{2\alpha}+1,$$

$$(b)\qquad q = \pm 1, \quad 3p^2 = 2+n^\alpha.$$

Toutes les valeurs de p et de n propres à vérifier les équations (a) sont données par les formules (**11**)

$$p = f^2+2g^2, \quad \pm 1 \pm n^\alpha\sqrt{-2} = (1+\sqrt{-2})(f+g\sqrt{-2})^2.$$

Les nombres f et g devront vérifier la condition $f^2-2g^2-4fg=1$; on aura ensuite $\pm n^\alpha = f^2-2g^2+2fg = (f+g)^2-3g^2$. On conclut de cette formule que le nombre n doit être résidu ou non-résidu quadratique de 3, suivant qu'il est de la forme $8l+5$ ou de la forme $8l+7$. Le nombre n doit donc être de l'une des deux formes $24l+13$ ou $24l+23$. Si donc le nombre n est de l'une des deux formes $24l+5$ ou $24l+7$, l'équation $3p^2 = 2n^{2\alpha}+1$ est impossible, et l'équation proposée n'admet pas d'autre solution entière que celle qui est déterminée par les équations (b).

Si l'on suppose de plus $\alpha = 1$, le nombre n devra vérifier l'équation $n = 3p^2-2$ pour une valeur entière de p; en sorte que l'on aura

$$p = 2\lambda+1, \quad n = 12\lambda(\lambda+1)+1.$$

Le nombre n sera donc nécessairement de la forme $24l+1$. Donc :

THÉORÈME XVII. — *Il est impossible de former un cube en ajoutant un carré entier au double du carré d'un nombre premier $24l+5$ ou $24l+7$.*

33. Soit $\alpha = 2$, et continuons à supposer que le nombre premier

n est de l'une des deux formes $24l + (5, 7)$. L'équation $x^2 + 2n^4 = z^3$, quand elle n'est pas impossible en nombres entiers, n'admet qu'une seule solution, déterminée par les équations (b), dont la seconde $3p^2 = n^2 + 2$ est résolue d'une manière générale (**11**) par les formules

$$p = f^2 + 2g^2, \quad \pm n \pm \sqrt{-2} = (1 + \sqrt{-2})(f + g\sqrt{-2})^2,$$
$$\pm n = 6fg - 1, \quad (f + g)^3 - 3g^2 = 1.$$

Les solutions de la dernière équation, en se bornant à celles où f est positif, sont données par la formule

$$f + g \pm g\sqrt{3} = (2 + \sqrt{3})^m.$$

Pour chaque valeur entière de l'exposant m, on obtient deux valeurs de n, en prenant alternativement la valeur positive et la valeur négative de g. Les plus petites valeurs de n sont 5, 19, 71, 265, 987, 2291, 3691, dont trois, 265, 987, 2291, sont des nombres composés, et trois autres, 19, 71, 3691, ne sont compris dans aucune des deux formes $24l + (5, 7)$. Donc :

THÉORÈME XVIII. — *Si l'on désigne par n un nombre premier inférieur à* 3690, *compris dans l'une des deux formules* $24l + 5$, $24l + 7$, *sans être égal à* 5, *tel que* 7, 29, 53, 101, 103, 127, 149,..., *on ne pourra former aucun cube en ajoutant un carré entier au double du bicarré* n^4.

Quand $n = 5$, l'équation proposée n'admet que la solution $x = 9$, $z = 11$. On a donc ce théorème :

THÉORÈME XIX. — *En ajoutant* 1250 *au carré* 81 *on obtient un cube,* 1331; *mais il n'existe aucun carré entier, autre que* 81, *qui fasse un cube lorsqu'on lui ajoute* 1250.

54. Soit $c = 3$. Nous désignerons par n un nombre premier $6l + 5$, en sorte que, n étant non-diviseur de la formule $x^2 + 3y^2$, toutes les solutions entières de l'équation $x^2 + 3n^{2\alpha} = z^3$ seront exprimées par les formules (2), pourvu que l'exposant α ne surpasse pas 2. Or la

seconde de ces formules

$$\pm n^{\alpha} = q\,(3p^2 - 3q^2)$$

est évidemment impossible si n est différent de 3. Donc :

THÉORÈME XX. — *Si aux carrés entiers* 1, 4, 9, 16,... *on ajoute trois fois le carré ou le bicarré d'un nombre premier* $6l+5$, *aucune des sommes n'est égale à un cube.*

35. La formule $x^2+cy^2=z^3$ donne, pour les valeurs de c auxquelles s'appliquent les théorèmes VI et VII de la première Partie, des théorèmes semblables à ceux que nous venons de démontrer. Nous nous bornerons à un petit nombre d'exemples.

1° Soit $c=5$. Désignons par n un nombre premier de l'une des formes $20l+(11, 13, 17, 19)$ et cherchons toutes les solutions entières de l'équation

$$x^2 + 5.n^{2\alpha} = z^3, \tag{1}$$

en y supposant $\alpha = 1$ ou 2. Le nombre z sera nécessairement impair, puisque son cube doit être de l'une des trois formes $8l+(1, 5, 6)$, dont la dernière, la seule qui soit paire, ne peut aucunement convenir à un cube. De plus, x et z sont premiers entre eux; car, s'ils avaient un diviseur commun, ce serait une puissance de n. Posons $x=n^{\beta}\xi$, $z=n^{\gamma}\zeta$; comme α est <3, l'équation (1) se ramène à la suivante :

$$\xi^2 + 5 = n^{3\gamma-2\alpha}\zeta^3,$$

dans laquelle la différence 3γ et 2α ne peut pas se réduire à zéro. Cette équation est évidemment impossible, puisque n est non-diviseur de la formule x^2+5. Donc, dans toutes les solutions entières de l'équation proposée, z est impair et premier avec chacun des deux nombres x et n. Ces solutions (**14**) seront donc déterminées par les formules

$$\text{(2)}\qquad \begin{cases} \pm x \pm n^{\alpha}\sqrt{-5} = (p+q\sqrt{-5})^3, \quad z = p^2+5q^2, \\ \pm x = p\,(p^2-15q^2), \quad \pm n^{\alpha} = q\,(3p^2-5q^2). \end{cases}$$

Or la dernière se décompose de l'une des deux manières suivantes :

$$(a) \qquad q = \pm n^{\alpha}, \quad 3p^2 = 5q^2 \pm 1,$$

$$(b) \qquad q = \pm 1, \quad 3p^2 = 5q^2 \pm n^{\alpha}.$$

La première (a) est toujours impossible, parce qu'on en déduirait que 3 est résidu quadratique de 5. La seconde est impossible pour la même raison, si α est pair, ou si n est de l'une des formes $20l + 11$, $20l + 19$. Donc :

THÉORÈME XXI. — *Il est impossible de faire un cube en ajoutant à un carré entier* 5 *fois le bicarré d'un nombre premier* $20l + (11, 13, 17, 19)$ *ou* 5 *fois le carré d'un nombre premier* $20l + (11, 19)$.

Si $\alpha = 1$, et que le nombre premier n soit compris dans l'une des deux formules $20l + (13, 17)$, il y a lieu d'examiner si l'équation

$$3p^2 = 5 \pm n$$

est possible. Comme le nombre n est > 5, il faut prendre le signe supérieur. Posant donc $p = 2\lambda$, on aura $n = 12\lambda^2 - 5$. Cette valeur de n est nécessairement de la forme $4x + 3$, ce qui ne peut s'accorder avec aucune des deux formes supposées $20l + (13, 17)$. Donc :

THÉORÈME XXII. — *Qu'on ajoute les carrés entiers* 1, 4, 9, 16,..., *successivement à* 5 *fois le carré d'un nombre premier* $20l + 13$, *ou* $20l + 17$, *aucune des sommes ne sera un cube.*

Si l'on suppose $n = 1$, les trois nombres x, n, z seront nécessairement premiers entre eux deux à deux ; de plus z ne peut être qu'un nombre impair. Les solutions de l'équation (1) seront donc encore exprimées par les formules (2), dont la seconde conduit à l'équation $3p^2 = 5 \pm 1$, qui est évidemment impossible. Donc :

THÉORÈME XXIII. — *Il est impossible de faire un cube en ajoutant* 5 *unités à un carré entier.*

36. On peut aussi remplacer le nombre premier n par un nombre composé, pourvu que ce nombre ne soit divisible par aucun cube ou par aucun nombre premier diviseur de la formule $x^2 + cy^2$; alors, en effet, les nombres x, n, z seront nécessairement premiers entre eux

deux à deux dans la formule $x^2+cn^2=z^3$. Si, de plus, on ne considère que des valeurs de c qui ne soient pas de l'une des formes $4l$ ou $8l+7$, la valeur de z sera nécessairement impaire, en sorte que toutes les solutions cherchées seront exprimées par les formules (2) du n° **23**. La seconde,

$$\pm n = q(3p^2 - cq^2),$$

n'admettra qu'un nombre limité de solutions, et donnera lieu à des théorèmes analogues aux précédents. Si le nombre n est multiple de 3 sans l'être de 9, si, de plus, il est premier avec c, il n'est pas nécessaire d'exiger qu'il ne soit divisible par aucun cube. L'équation proposée n'admet alors aucune solution. D'abord elle ne peut pas en admettre en nombres premiers entre eux, puisque ces solutions sont données par les formules (2), dont la seconde $\pm n = q(3p^2 - cq^2)$ est évidemment impossible quand n est divisible par 3 sans l'être par 9. Les solutions où les deux nombres n et x ne sont pas premiers entre eux doivent se déduire de solutions en nombres premiers entre eux d'équations toutes semblables. En effet, soit θ le plus grand diviseur commun des deux nombres n et x; posons $x=\theta u$, $n=\theta m$; l'équation proposée se ramène à la suivante $u^2+cm^2=\frac{z^3}{\theta^2}$, où les deux nombres u et m sont premiers entre eux. D'ailleurs, comme θ ne renferme aucun diviseur de la formule x^2+cy^2, le quotient $\frac{z^3}{\theta^2}$ doit être premier avec θ, ce qui exige que θ soit un cube. Le nombre θ ne sera donc pas divisible par 3. Les solutions de l'équation proposée, dans lesquelles x et n ont un diviseur commun, se ramènent donc aux solutions en nombres premiers entre eux d'équations semblables $u^2+cm^2=v^3$, où m remplit les mêmes conditions que n. Ces solutions n'existent donc pas. Pour chacune des valeurs convenables de c, on pourra énoncer un théorème analogue aux deux suivants :

THÉORÈME XXIV. — *Si le nombre n est multiple de* 3, *sans être divisible ni par* 9, *ni par aucun facteur premier* $4l+1$, *on ne peut former aucun cube en ajoutant un carré entier au carré* n^2.

THÉORÈME XXV. — *Si le nombre n est multiple de* 3, *sans être divisible ni par* 9, *ni par* 5, *ni par un nombre premier de l'une des*

formes $20l + (1, 3, 7, 9)$, *aucune des sommes obtenues en ajoutant un carré entier au carré* n^2, *multiplié par* 5, *n'est égale à un cube.*

37. Avant de passer à d'autres applications, nous devons faire connaître pour quelle raison nous avons dû écarter le cas où le nombre n aurait comme facteur quelque diviseur de la formule $x^2 + cy^2$. Soit n un diviseur premier de cette formule. L'équation $x^2 + cn^{2\alpha} = z^3$ peut admettre des solutions de la forme $x = n^\beta u$, $z = n^\gamma v$, qui se déduiront des solutions en nombres entiers et premiers entre eux de l'équation

$$u^2 + c = n^\lambda . v^3. \tag{5}$$

Celles-ci se déduiront des formules

$$v = p^2 + cq^2, \quad \pm u \pm \sqrt{-c} = (a + b\sqrt{-c})(p + q\sqrt{-c})^3,$$

où

$$a^2 + b^2 c = n^\lambda.$$

Il y aura autant de solutions que de manières différentes de vérifier en nombres entiers p et q l'équation

$$bp(p^2 - 3cq^2) + aq(3p^2 - cq^2) = \pm 1.$$

Or, si le premier membre de cette équation est un polynôme irréductible, il n'existe aucune méthode pour décider si elle est possible oui ou non. On peut trouver toutes les solutions où les nombres p et q ne surpassent pas une limite donnée; mais on ne peut pas affirmer qu'il n'y aura pas d'autres solutions au delà de cette limite.

II. — Impossibilité de quelques équations de la forme $x^3 + y^3 = az^3$.

38. Dans notre Mémoire sur la décomposition d'un nombre entier A en une somme de deux cubes rationnels, nous avons considéré le cas où le nombre A ne contient aucun facteur de la forme $6l + 1$.

La méthode que nous avons employée n'est qu'une application de

notre théorème III; nous nous sommes contenté alors d'indiquer la démonstration que nous avons développée dans le présent Mémoire. Le théorème V (11) nous permet d'étendre ces recherches aux cas où le nombre donné renferme quelque facteur premier de la forme $6l+1$. Un petit nombre d'exemples suffiront pour faire connaître la méthode à suivre dans ces cas. Comme, dans ces exemples, le nombre donné a n'est divisible par aucun cube, nous pourrons admettre que les trois indéterminées x, y, z sont premières entre elles deux à deux; de plus nous supposerons que, dans la solution considérée, la valeur de z est la plus petite possible, de telle sorte que nous devons rejeter comme impossible toute hypothèse dans laquelle l'équation proposée serait vérifiée, en égalant les indéterminées à des diviseurs de z.

Exemple I.

(1) $$x^3+y^3=14.z^3.$$

D'abord le nombre z doit être multiple de 3; car autrement l'équation proposée donnerait, suivant le module 9, l'une des deux congruences également impossibles

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

On aura donc l'une des deux décompositions suivantes :

$$(a) \qquad x+y=14.9u^3, \quad \left(\frac{x-y}{2}\right)^2+3\left(\frac{x+y}{6}\right)^2=v^3,$$

$$(b) \qquad x+y=2.9u^3, \quad \left(\frac{x-y}{2}\right)^2+3\left(\frac{x+y}{6}\right)^2=7v^3.$$

Dans le premier cas, on conclut du théorème III que l'on a

$$\frac{x-y}{2}+\sqrt{-3}\,\frac{x+y}{6}=(f+\sqrt{-3}\cdot g)^3$$
$$=f(f^2-9g^2)+\sqrt{-3}.3g(f^2-g^2);$$

d'où

$$\frac{x+y}{6}=7.3u^3=3g(f^2-g^2), \quad 7u^3=g(f^2-g^2).$$

Les trois facteurs $g, f+g, f-g$ étant premiers entre eux, la dernière équation se décomposera de l'une des manières suivantes :

$$7\alpha^3 = g, \quad f+g=\beta^3, \quad f-g=\gamma^3,$$
$$\alpha^3 = g, \quad f\pm g = 7\beta^3, \quad f\mp g = \gamma^3;$$

La première décomposition doit être rejetée, parce qu'on en déduit l'équation

$$\beta^3 + (-\gamma)^3 = 14\alpha^3,$$

qui n'est autre que l'équation (1), vérifiée en égalant les indéterminées à des diviseurs de z. La seconde donne l'équation

$$7\beta^3 - \gamma^3 = \pm 2\alpha^3,$$

d'où l'on conclurait que 2 est résidu cubique de 7, ce qui est faux.

Le système des équations (a) est donc inadmissible.

Le théorème V nous apprend que la seconde des équations (b) est résolue de la manière la plus complète au moyen de la formule

$$\frac{x-y}{2} + \sqrt{-3}\,\frac{x+y}{6} = (2 \pm \sqrt{-3})(f+g\sqrt{-3})^3,$$

pourvu qu'on attribue aux nombres f et g toutes les valeurs entières et premières entre elles, l'une paire et l'autre impaire; en outre la formule

$$v = f^2 + 3g^2$$

exige que le nombre f soit premier relativement à 3.

Dans cet exemple et dans les suivants, nous poserons pour abréger

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

et nous remarquerons, une fois pour toutes, que l'on a

$$\mathrm{F} \equiv \pm 1 \pmod 9, \quad \mathrm{G} \equiv 0 \pmod 9.$$

La formule précédente deviendra donc

$$\frac{x-y}{2} + \sqrt{-3}\,\frac{x+y}{6} = (2\mathrm{F} \mp 3\mathrm{G}) + \sqrt{-3}(2\mathrm{G} \pm \mathrm{F}),$$

et l'on en déduira

$$\frac{x+y}{6} = 3u^3 = 2G \pm F,$$

ce qui est impossible, puisque G est multiple de 3, tandis que le nombre F ne l'est pas; donc les équations (b) sont impossibles. Donc :

THÉORÈME XXVI. — *Le nombre 14 n'est pas décomposable en une somme de deux cubes rationnels.*

Exemple II.

$$x^3 + y^3 = 21.z^3. \tag{2}$$

39. La somme de deux cubes ne pouvant être divisible par 3 sans l'être par 9, il faut que le nombre z soit multiple de 3.

La décomposition de l'équation (2) donnera donc l'un des systèmes suivants :

$$(a) \qquad x+y = 7.27u^3, \quad x^2 - xy + y^2 = 3v^3,$$
$$(b) \qquad x+y = 27u^3, \quad x^2 - xy + y^2 = 21.v^3.$$

Suivant que le nombre u sera pair ou impair, la seconde équation (a) se mettra sous l'une des formes

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

de la première on déduit

$$\frac{x+y}{6} = \frac{9.7u^3}{2} = G = 3g(f^2 - g^2),$$
$$3.7u^3 = 2g(f^2 - g^2).$$

Le second membre étant composé de trois facteurs premiers entre eux, $2g, f+g, f-g$, le produit $3.7u^3$ doit aussi se décomposer en

facteurs premiers entre eux. Or on ne peut faire que deux hypothèses : ou bien l'un de ces facteurs est multiple de 3.7, ou bien l'un est multiple de 3 et un autre est multiple de 7. Dans le premier cas, on trouve l'équation (2) vérifiée en attribuant aux indéterminées des valeurs égales à des diviseurs de z, ce qui est impossible. Dans le second, on est ramené à la solution d'une équation de la forme

$$\alpha^3 + 3\beta^3 + 7\gamma^3 = 0,$$

dans laquelle α et β sont premiers à 7. On en conclurait que 3 est résidu cubique de 7, ce qui est faux.

Donc, si le système (a) est possible, il faut que la somme $x + y$ soit impaire. Dans ce cas, on a les deux équations

$$\frac{y}{2} = \mathrm{F}, \quad \frac{2x - y}{6} = \mathrm{G}, \quad \text{d'où} \quad \frac{2(x+y)}{6} = 7.9u^3 = \mathrm{F} + \mathrm{G},$$

ce qui est impossible, F étant premier à 3, tandis que G est multiple de 9. Le système (a) est donc impossible.

Il en est de même du système (b), dont la deuxième équation s'écrit sous l'une des deux formes

$$\left(\frac{x-y}{2}\right)^2 + 3\left(\frac{x+y}{6}\right)^2 = 7v^3, \quad \left(\frac{y}{2}\right)^2 + 3\left(\frac{2x-y}{6}\right)^2 = 7v^3,$$

suivant que la somme $x + y$ est paire ou impaire. En vertu du théorème IV, elles entraînent respectivement les deux équations

$$\frac{x-y}{2} + \sqrt{-3}\,\frac{x+y}{6} = (2 \pm \sqrt{-3})(\mathrm{F} + \sqrt{-3}.\mathrm{G}),$$

$$\frac{y}{2} + \sqrt{-3}\,\frac{2x-y}{6} = (2 \pm \sqrt{-3})(\mathrm{F} + \sqrt{-3}.\mathrm{G}),$$

La première donne

$$\frac{x+y}{6} = \frac{9.u^3}{2} = 2\mathrm{G} \pm \mathrm{F},$$

ce qui est impossible.

La seconde entraîne comme conséquence les deux équations

$$\frac{y}{2} = 2F \mp 3G, \quad \frac{2x-y}{6} = 2G \pm F,$$

d'où

$$\frac{x+y}{3} = 9.u^3 = (2F \mp 3G) + (2G \pm F);$$

ce qui est impossible; car cette équation, réduite en congruence, suivant le module 9, donne le résultat absurde

$$2 \pm 1 \equiv 0 \pmod{9}.$$

L'équation proposée est donc impossible; en d'autres termes :

THÉORÈME XXVII. — *Le nombre* 21 *n'est pas décomposable en une somme de deux cubes rationnels.*

On démontrerait de la même manière l'impossibilité de résoudre en nombres entiers l'équation

$$x^3 + y^3 = 196.z^3.$$

Exemple III.

(3) $$x^3 + y^3 = 38.z^3.$$

40. 1° Si z n'est pas multiple de 3, cette équation se décomposera de l'une des manières suivantes :

(*a*) $x+y=38u^3$, $\left(\frac{x+y}{2}\right)^2+3\left(\frac{x-y}{2}\right)^2=v^3=F^2+3G^2$,

(*b*) $x+y=2u^3$, $\left(\frac{x+y}{2}\right)^2+3\left(\frac{x-y}{2}\right)^2=19v^3=(4^2+3)(F^2+3G^2)$.

Dans le premier cas on a

$$\frac{x+y}{2} = 19u^3 = F = f(f^2 - 9g^2).$$

Comme les trois facteurs f, $f+3g$, $f-3g$ sont premiers entre eux, la décomposition de cette équation n'aura lieu que de l'une des

manières suivantes :

$$19\alpha^3 = f,\ f+3g=\beta^3,\quad f-3g=\gamma^3,$$
$$\alpha^3 = f,\ f\pm 3g = 19\beta^3,\ f\mp 3g=\gamma^3;$$

d'où l'on déduit respectivement les deux équations

$$\beta^3+\gamma^3 = 38\alpha^3,\quad 19\beta^3+\gamma^3 = 2\alpha^3.$$

La première doit être rejetée, parce qu'elle ne diffère pas de l'équation (3) vérifiée par des diviseurs de z. La seconde est impossible, parce qu'on en déduit la conclusion fausse que 2 est résidu cubique de 19. Le système (a) est donc impossible.

En appliquant le théorème IV au système (b), on en déduit

$$\frac{x+y}{2}+\sqrt{-3}\,\frac{x-y}{2} = (4F\mp 3G)+\sqrt{-3}(4G\pm F),$$
$$\frac{x+y}{2} = 4F\mp 3G,\quad \frac{x-y}{2} = 4G\pm F,$$

d'où

$$\frac{x+y}{2}\mp\frac{x-y}{2} = x \quad \text{ou} \quad y = 3F-G(\pm 4\pm 3).$$

L'un des deux nombres x, y serait donc multiple de 3; mais alors l'équation proposée, réduite suivant le module 9, donne la congruence absurde

$$\pm 1 \equiv \pm 2 \pmod 9.$$

Le système (b) est donc aussi impossible.

2° Supposons que le nombre z est multiple de 3, la décomposition de l'équation proposée donne l'un des deux systèmes

$$(a')\quad x+y = 18.19u^3,\quad \frac{x-y}{2}+\sqrt{-3}\,\frac{x+y}{6} = F+\sqrt{-3}.G,$$

$$(b')\quad x+y = 18u^3,\quad \frac{x-y}{2}+\sqrt{-3}\,\frac{x+y}{6} = (4\pm\sqrt{-3})(F+\sqrt{-3}.G).$$

Dans le premier cas, on aurait l'équation

$$\frac{x+y}{18} = 19u^3 = \frac{1}{3}G = g(f^2-g^2),$$

dont la décomposition donne l'un des systèmes

$$19\alpha^3 = g, \quad f+g=\beta^3, \qquad f-g=\gamma^3,$$
$$\alpha^3 = g, \quad f\pm g = 19\beta^3, \quad f\mp g = \gamma^3;$$

d'où

$$\beta^3-\gamma^3 = 38\alpha^3, \quad 19\beta^3-\gamma^3 = \pm 2\alpha^3.$$

La première équation doit être rejetée, parce qu'elle ne diffère de l'équation proposée qu'en ce que les nouvelles valeurs des indéterminées β, $-\gamma$, α sont des diviseurs de z. La seconde est impossible, parce qu'elle conduit à cette fausse conclusion que 2 serait résidu cubique de 19. Donc le système (a') est impossible.

Le second système (b') conduit à l'équation impossible

$$\frac{x+y}{6} = 3u^3 = 4G \pm F = 12g(f^2-g^2) \pm f(f^2-3g^2);$$

il est donc aussi impossible.

En réunissant les résultats obtenus 1° et 2°, nous voyons que l'équation proposée ne peut être vérifiée ni en supposant z premier à 3, ni en supposant z divisible par 3; elle est donc impossible. Donc :

THÉORÈME XXVIII. — *Le nombre* 38 *n'est pas décomposable en une somme de deux cubes rationnels.*

Exemple IV.

$$x^3+y^3 = 76.z^3. \tag{4}$$

41. D'abord z doit être multiple de 3; car autrement cette équation donnerait, suivant le module 9, l'une des deux congruences impossibles

$$\pm 1 \pm 1 \equiv \pm 4, \quad \pm 1 \equiv \pm 4 \pmod 9.$$

Ainsi la décomposition de l'équation proposée donnera l'un des deux systèmes

$$(a) \quad x+y = 36.19u^3, \ \frac{x-y}{2}+\sqrt{+3}\,\frac{x+y}{6} = F+\sqrt{-3}.G,$$

$$(b) \quad x+y = 36.u^3, \ \frac{x-y}{2}+\sqrt{-3}\,\frac{x+y}{6} = (4\pm\sqrt{-3})(F+\sqrt{-3}.G).$$

Le second donne l'équation impossible

$$\frac{x+y}{6} = 6u^3 = 4G \pm F \equiv \pm 1 \pmod 9.$$

Le premier conduit à l'équation

$$\frac{x+y}{6} = 6.19u^3 = G, \quad 2.19u^3 = g(f^2 - g^2),$$

dont la décomposition donne l'un des systèmes suivants :

$$2.19\alpha^3 = g, \quad f+g = \beta^3, \quad f-g = \gamma^3,$$
$$2\alpha^3 = g, \quad f \pm g = 19\beta^3, \quad f \mp g = \gamma^3.$$

On en déduit respectivement les deux équations

$$76\alpha^3 = \beta^3 + (-\gamma)^3, \quad 19\beta^3 - \gamma^3 = \pm 4\alpha^3,$$

dont la seconde est impossible, parce qu'elle conduit à cette conclusion fausse, que 4 est résidu cubique de 19; et la première doit être rejetée, parce qu'elle ne diffère de l'équation proposée qu'en ce que les nouvelles valeurs des indéterminées sont des diviseurs de z.

L'équation proposée est donc impossible.

THÉORÈME XXIX. — *Il est impossible de décomposer le nombre* 76 *en une somme de deux cubes rationnels.*

Exemple V.

(5) $$x^3 + y^3 = 39.z^3.$$

42. D'abord, comme la somme de deux cubes ne peut être multiple de 3 sans l'être de 9, le nombre z doit être divisible par 3.

La résolution de l'équation proposée se trouve ainsi ramenée à celle de l'un des deux systèmes

(a) $$x + y = 27.13u^3, \quad x^2 - xy + y^2 = 3v^3,$$

(b) $$x + y = 27u^3, \quad x^2 - xy + y^2 = 39v^3.$$

Suivant que z est pair ou impair, la deuxième équation (a) se ramène à l'une des suivantes :

$$\frac{x-y}{2}+\sqrt{-3}\,\frac{x-y}{6}=\mathrm{F}+\sqrt{-3}.\mathrm{G},\quad \frac{y}{2}+\sqrt{-3}\,\frac{2x-y}{6}=\mathrm{F}+\sqrt{-3}.\mathrm{G}.$$

Dans le premier cas on doit résoudre l'équation

$$\frac{x+y}{6}=\frac{9\cdot 13u^3}{2}=3g(f^2-g^2),\quad 3.13u^3=2g(f^2-g^2).$$

Or, en excluant les décompositions qui donnent des équations de même forme que la proposée, on trouve que l'on doit résoudre une équation de la forme

$$3a^3+13b^3+c^3=0,$$

en attribuant aux indéterminées a, b, c des valeurs entières et premières entre elles deux à deux; ce qui est impossible, car 3 n'est pas résidu cubique de 13.

Dans le second on a les deux équations

$$\frac{y}{2}=\mathrm{F},\quad \frac{2x-y}{6}=\mathrm{G},\quad \text{d'où}\quad \frac{2(x+y)}{6}=\mathrm{F}+\mathrm{G}=9u^3,$$

ce qui est impossible. Le système (a) est donc impossible.

De même le système (b) se ramène à l'une des équations

$$\frac{x-y}{2}+\sqrt{-3}\,\frac{x+y}{6}=(1\pm 2\sqrt{-3})(\mathrm{F}+\sqrt{-3}.\mathrm{G}),$$

$$\frac{y}{2}+\sqrt{-3}\,\frac{2x-y}{6}=(1\pm 2\sqrt{-3})(\mathrm{F}+\sqrt{-3}.\mathrm{G}).$$

On déduit de la première

$$\frac{x+y}{6}=\frac{9u^3}{2}=\mathrm{G}\pm 2\mathrm{F},$$

ce qui est impossible, G étant multiple de 9 et F ne l'étant pas.

La seconde équation donne les suivantes :

$$\frac{y}{2} = F \mp 6G, \quad \frac{2x-y}{6} = G \pm 2F;$$

d'où

$$\frac{x+y}{3} = 9u^3 = (F \mp 6G) + (G \pm 2F),$$
$$\pm 1 \pm 2 \equiv 0 \pmod 9,$$

ce qui est absurde. Le système (b) est donc aussi impossible. Donc :

THÉORÈME XXX. — *Le nombre* 39 *n'est pas décomposable en une somme de deux cubes rationnels.*

Exemple VI.

$$x^3 + y^3 = 57.z^3. \tag{6}$$

43. De même que dans l'exemple précédent, et pour la même raison, le nombre z doit être multiple de 3; de telle sorte qu'on déduira de l'équation (b) l'un des deux systèmes

$$(a) \qquad x + y = 27.19u^3, \quad x^2 - xy + y^2 = 3v^3,$$

$$(b) \qquad x + y = 27.u^3, \quad x^2 - xy + y^2 = 3.19v^3.$$

Nous allons démontrer qu'ils sont l'un et l'autre impossibles.

D'abord la somme $x+y$ ne peut pas être impaire; car alors on déduirait du système (a)

$$\frac{y}{2} + \sqrt{-3}\,\frac{2x-y}{6} = F + \sqrt{-3}\,G;$$

d'où

$$\frac{y}{2} = F, \quad \frac{2x-y}{6} = G, \quad F + G = \frac{2(x+y)}{6} = 9.19u^3,$$

ce qui est impossible. Le système (b) donnerait l'équation

$$\frac{y}{2} + \sqrt{-3}\,\frac{2x-y}{6} = (4 \pm \sqrt{-3})(F + \sqrt{-3}\,G),$$

d'où

$$\frac{y}{2}=4F\mp 3G,\quad \frac{2x-y}{6}=4G\pm F;\quad \frac{2(x+y)}{6}=4G\pm F+4F\mp 3G;$$

$$9u^3=4G+4F\pm F\mp 3G\equiv\pm 4\pm 1\pmod 9,$$

ce qui est également impossible. La somme $x+y$ est donc paire, et par suite les deux systèmes (a) et (b) se ramènent respectivement aux deux équations

$$(a')\qquad \frac{x-y}{2}+\sqrt{-3}\,\frac{x+y}{6}=F+\sqrt{-3}\,G,$$

$$(b')\qquad \frac{x-y}{2}+\sqrt{-3}\,\frac{x+y}{6}=(4F\mp 3G)+\sqrt{-3}\,(4G\pm F).$$

La seconde donnerait l'équation impossible

$$\frac{x+y}{6}=\frac{9u^3}{2}=4G\pm F;$$

on doit donc la rejeter. Quant à la première, elle donne l'équation

$$3.19u^3=2g(f^2-g^2),$$

dont la décomposition ramène l'une des deux équations

$$3.19\alpha^3=\beta^3+\gamma^3,\quad 3\alpha^3+19\beta^3+\gamma^3=0,$$

dans lesquelles α, β, γ sont diviseurs de u et par conséquent de z; de plus ces trois nombres sont premiers entre eux-deux à deux. La première ne différant pas de l'équation proposée, on doit la rejeter. Quant à la seconde elle est impossible, parce qu'on en déduirait cette conclusion fausse que 3 serait résidu cubique de 19.

Ainsi les deux systèmes (a) et (b) sont impossibles, et par suite l'équation proposée n'est pas résoluble en nombres entiers. Donc :

THÉORÈME XXXI. — *Le nombre* 57 *n'est pas décomposable en une somme de deux cubes rationnels.*

44. Nous venons de rencontrer trois multiples de 19, qui ne peuvent pas se décomposer en deux cubes rationnels, 38, 76, 57. Quant au nombre 19 lui-même, on peut prévoir *a priori* qu'il est décomposable. Il suffit de se rappeler le théorème suivant, que nous avons donné à la fin du Mémoire cité :

Tout nombre $A^2 + 3B^2$ *est décomposable en une somme de deux cubes rationnels, lorsque 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.*

En effet, $19 = 4^2 + 3.1^2$; or le produit 2.4 est un cube.

D'ailleurs on vérifie sans peine que l'on a

$$19 = 3^3 - 2^3 = \left(\frac{8}{3}\right)^3 + \left(\frac{1}{3}\right)^3.$$

On démontrerait par la même méthode l'impossibilité de décomposer en deux cubes rationnels l'un des nombres 31, 93, 95, 190. Nous ne nous arrêterons pas sur ce sujet : les exemples qui précèdent suffiront pour montrer de quelle manière on doit appliquer les théorèmes III et V, en les combinant avec le principe de non-congruence suivant le module 9, ou suivant quelque module de la forme $6l + 1$.