

JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

CASIMIR RICHAUD

**Démonstrations de quelques théorèmes concernant la résolution
en nombres entiers de l'équation $x^2 - Ny^2 = -1$**

Journal de mathématiques pures et appliquées 2^e série, tome 10 (1865), p. 235-280.

http://www.numdam.org/item?id=JMPA_1865_2_10__235_0



NUMDAM

Article numérisé dans le cadre du programme
Gallica de la Bibliothèque nationale de France
<http://gallica.bnf.fr/>

et catalogué par Mathdoc
dans le cadre du pôle associé BnF/Mathdoc
<http://www.numdam.org/journals/JMPA>

DÉMONSTRATIONS DE QUELQUES THÉORÈMES

CONCERNANT

LA RÉOLUTION EN NOMBRES ENTIERS DE L'ÉQUATION $x^2 - Ny^2 = -1$;

PAR M. CASIMIR RICHAUD.

1. Nous allons, en premier lieu, résumer succinctement le procédé de Lagrange pour la résolution en nombres entiers des équations $x^2 - Ny^2 = \pm 1$, dans lesquelles le déterminant N est un nombre entier positif non carré.

2. *Réduction de $\sqrt{N}$ en fraction continue.* — Lorsqu'on réduit $\sqrt{N}$ en fraction continue, les quotients incomplets forment une suite périodique; le premier de ces quotients, égal à la racine carrée a du plus grand carré a^2 contenu dans N , ne se reproduit pas; la période commence au second terme, et son dernier terme est double de l'initial a , qui n'en fait pas partie. De plus, au dernier terme près $2a$, la période est symétrique, c'est-à-dire qu'elle est la même quand on la lit en ordre rétrograde.

Les dénominateurs des quotients complets provenant du même développement de $\sqrt{N}$ forment aussi une période symétrique analogue à la période des quotients incomplets, et les seuls dénominateurs, qui puissent être égaux à l'unité, sont le premier $\frac{\sqrt{N} + 0}{1} = a + \frac{1}{j}$, et ceux qui produisent le dernier terme de la période à chacun de ses retours $\frac{\sqrt{N} + a}{1} = 2a + \frac{1}{j}$. Tous les termes de la période des dénominateurs sont d'ailleurs inférieurs à $2\sqrt{N}$.

3. *Résolution en nombres entiers des équations $x^2 - Ny^2 = \pm P$* ($P < \sqrt{N}$). — Pour que l'une de ces deux équations soit soluble en nombres entiers, il faut et il suffit que l'un des termes de la période

des dénominateurs provenant du développement de $\sqrt{N}$ en fraction continue soit égal à P .

Lorsque cette condition est remplie, les valeurs entières de x et de y sont égales respectivement au numérateur et au dénominateur des réduites qui précèdent le quotient complet dont le dénominateur est P à chacun de ses retours. En d'autres termes, si $\frac{H}{H'}$ représente l'une de ces réduites, on a toujours

$$(1) \quad H^2 - NH'^2 = \pm P.$$

Le deuxième membre de cette égalité doit être pris avec le signe $+$ si la réduite $\frac{H}{H'}$ est de rang impair, et avec le signe $-$ dans le cas contraire. (Dans cette évaluation des rangs, la première réduite est supposée égale à $\frac{1}{0}$.)

Le théorème compris dans l'égalité (1) peut s'énoncer de la manière suivante : *Le résultat de la substitution des deux termes d'une réduite quelconque $\frac{H}{H'}$ déduite du développement de $\sqrt{N}$, à la place de x et de y dans l'expression $x^2 - Ny^2$, est égal au dénominateur de la complète suivante pris avec son signe si $\frac{H}{H'}$ est de rang impair, et en signe contraire si $\frac{H}{H'}$ est de rang pair.*

4. *Résolution en nombres entiers des équations $x^2 - Ny^2 = \pm 1$.* — Résumons, toujours d'après Lagrange, les conditions qui doivent être remplies pour que ces équations soient possibles en nombres entiers.

Si les deux périodes signalées ci-dessus (n° 2) présentent un nombre pair de termes, auquel cas il y a dans chacune d'elles un terme du milieu de la symétrie qui ne se reproduit pas, les réduites qui précéderont le quotient complet $\frac{\sqrt{N} + a}{1}$, à chacun de ses retours, seront toujours de rang impair. Donc, dans ce cas, l'équation $x^2 - Ny^2 = 1$ aura une infinité de solutions entières, et l'équation $x^2 - Ny^2 = -1$ n'en admettra aucune de cette nature (n° 3).

Si les mêmes périodes contiennent un nombre impair de termes, c'est-à-dire si elles renferment au milieu de la partie symétrique deux termes consécutifs égaux entre eux, les réduites qui précèdent le quotient complet $\frac{\sqrt{N} + a}{1}$, aux périodes de rang impair, seront toujours de rang pair. Donc, dans ce cas, chacune de ces réduites fournira une solution entière de l'équation $x^2 - Ny^2 = -1$. De même, les réduites qui précèdent la fraction complète $\frac{\sqrt{N} + a}{1}$, aux périodes de rang pair, seront toujours de rang impair, et par suite chacune d'elles donnera une solution entière de l'équation $x^2 - Ny^2 = 1$.

Ainsi, en résumé, lorsque le déterminant N est un nombre positif non carré, l'équation $x^2 - Ny^2 = 1$ admet toujours des solutions entières, et, pour que l'équation $x^2 - Ny^2 = -1$ admette des solutions de la même nature, il faut et il suffit que les deux périodes provenant du développement de $\sqrt{N}$ en fraction continue contiennent un nombre impair de termes.

Pour simplifier le langage, nous formulerons cette dernière condition de la manière suivante : *L'équation $x^2 - Ny^2 = -1$ est toujours possible en nombres entiers, lorsque les périodes provenant du développement de $\sqrt{N}$ en fraction continue ne présentent pas de terme du milieu.*

5. La condition qu'on vient d'énoncer est peu utile dans la pratique, parce qu'elle ne dispense pas de trouver une première solution entière de l'équation $x^2 - Ny^2 = -1$, lorsqu'on veut reconnaître la possibilité des solutions de cette nature.

On peut cependant faire un pas de plus, et établir une condition nécessaire mais non suffisante, qui doit être remplie par le nombre N , pour que la même équation admette des solutions entières. Cette équation peut se mettre sous la forme

$$(1) \quad Ny^2 = x^2 + 1.$$

On reconnaît ainsi immédiatement que tous les facteurs premiers de N divisent une somme de deux carrés premiers entre eux ; par cela

même ces facteurs sont eux-mêmes égaux à la somme de deux carrés, ou, en d'autres termes, tous les facteurs premiers impairs de N sont de la forme $4n + 1$, lorsque l'équation (1) admet des solutions entières.

Dans cette dernière hypothèse, le facteur 2 ne peut d'ailleurs entrer qu'une fois dans N . Car si N est pair x , sera impair, et le second membre de l'équation (1) sera de la forme $8n + 2$. Ce deuxième membre ne pourra donc contenir qu'une fois le facteur 2, et par suite N sera dans le même cas.

Ainsi, pour que l'équation $x^2 - Ny^2 = -1$ admette des valeurs entières, il faut que tous les facteurs premiers de N ou de $\frac{N}{2}$ soient de la forme $4n + 1$.

Cette condition n'est pas suffisante; elle est remplie pour le nombre 178 par exemple, et cependant l'équation $x^2 - 178y^2 = -1$ n'admet pas de solutions entières. Nous verrons plus loin que cette équation ne peut pas être soluble en nombres entiers, parce que 178 étant de la forme $8n + 2$ ses deux carrés composants 13^2 et 3^2 ont des racines carrées des formes $8n + 3$, $8n + 5$ (nos 8 et 15).

6. Ces préliminaires posés, nous allons démontrer quelques théorèmes qui permettront de formuler, dans une série de cas, des conditions rigoureuses de possibilité en nombres entiers pour l'équation $x^2 - Ny^2 = -1$.

THÉORÈME. — Lorsque les parties symétriques des périodes provenant du développement de $\sqrt{N}$ en fraction continue ont un terme du milieu, le dénominateur du quotient complet, qui fournit ce terme du milieu, est un diviseur de $2N$ et aussi un diviseur du double du numérateur de la réduite précédente.

Considérons les deux périodes provenant du développement de $\sqrt{N}$ en fraction continue, savoir :

Quotients incomplets. $a, (b, c, \dots, g, h, m, h, g, \dots, c, b, 2a),$
 Dénominateurs. $(1, \epsilon, \gamma, \dots, \epsilon, \rho, \mu, \rho, \epsilon, \dots, \gamma, \epsilon) 1, \dots$

Nous représentons ici par m et μ les termes du milieu des deux

périodes, et nous avons à démontrer que μ est un diviseur des nombres $2N$ et $2H$ (H étant le numérateur de la réduite $\frac{H}{H'}$ correspondante au quotient incomplet h qui précède immédiatement m).

Les trois réduites consécutives $\frac{G}{G'}$, $\frac{H}{H'}$, $\frac{M}{M'}$ placées par ordre de grandeur, et correspondantes aux quotients incomplets g , h , m , nous donneront (n° 3) les relations suivantes :

$$\begin{aligned} (1) \quad & NH'^2 = H^2 \pm \mu, \\ (2) \quad & NG'^2 = G^2 \mp \rho, \\ (3) \quad & NM'^2 = M^2 \mp \rho. \end{aligned}$$

D'après la loi de formation des réduites, nous avons $M = Hm + G$, $M' = H'm + G'$, ce qui donne la nouvelle relation

$$(4) \quad \frac{M - G}{M' - G'} = \frac{H}{H'}.$$

L'élimination de ρ entre (2) et (3) donne $N(M'^2 - G'^2) = M^2 - G^2$, ou, en ayant égard à la relation (4),

$$(5) \quad N(M' + G')H' = (M + G)H.$$

En combinant cette dernière relation avec l'égalité (1), il viendra

$$NH'[(HG' - GH') - (MH' - M'H)] = \mp \mu(M + G).$$

Or, d'après les propriétés des réduites, la valeur absolue des différences $HG' - GH'$, $MH' - M'H$ est égale à l'unité, de telle sorte qu'en ayant égard à la corrélation des signes, nous aurons finalement

$$(6) \quad 2NH' = \mu(M + G).$$

Cette dernière relation prouve que $2NH'$ est divisible par μ . Mais le nombre H' est premier avec μ , en vertu de la relation (1), parce que, dans le cas contraire, H et H' auraient un facteur commun, ce qui est

impossible puisque $\frac{H}{H'}$ est une réduite. Le nombre $2N$ est donc divisible par μ .

Pour démontrer la deuxième partie du théorème, remplaçons dans (5) N par sa valeur déduite de (1), nous aurons

$$(H^2 \pm \mu)(M' + G') = (M + G)HH'$$

ou

$$\pm \mu(M' + G') = H[(MH' - M'H) + (GH' - HG')],$$

ou, en ayant égard à la corrélation des signes,

$$(7) \quad 2H = \mu(M' + G').$$

Ainsi, $2H$ est divisible par μ .

7. Remarque. — Lorsque, dans le développement de $\sqrt{N}$ en fraction continue, aucun dénominateur des quotients complets ne pourra être égal à un diviseur de $2N$, l'équation $x^2 - Ny^2 = -1$ sera toujours possible en nombres entiers (n° 4).

La réciproque n'est pas exacte, ou, en d'autres termes, la même équation pourra admettre des solutions entières, même dans le cas où certains dénominateurs des quotients complets seraient des diviseurs de $2N$. C'est ce qui arrive en particulier pour l'équation $x^2 - 925y^2 = -1$ qui admet des solutions entières, malgré que le nombre 25, diviseur du déterminant, se trouve dans la période des dénominateurs des quotients complets. Mais la réciproque sera évidemment vraie, si aucun dénominateur ne peut être simultanément un diviseur des deux nombres $2N$ et $2H$. Il était donc indispensable d'établir la deuxième partie du théorème précédent, au point de vue de la recherche des conditions de possibilité de l'équation $x^2 - Ny^2 = -1$.

8. THÉORÈME. — Lorsque le développement de $\sqrt{N}$ en fraction continue ne présente pas de terme du milieu, auquel cas l'équation $x^2 - Ny^2 = -1$ est soluble en entiers, le terme qui se répète, au milieu de la période des dénominateurs, est égal à la racine carrée de l'un des carrés composants du nombre N .

Considérons les deux périodes provenant du développement de $\sqrt{N}$:

Quotients incomplets . . . $a, [b, c, \dots, h, r, r, h, \dots, c, b, 2a],$

Dénominateurs $[1, \epsilon, \gamma, \dots, \epsilon, \rho, \rho, \epsilon, \dots, \gamma, \epsilon], 1 \dots$

et représentons par u le quotient complet

$$u = r + \frac{1}{r + \frac{1}{h + \dots}}$$

ce quotient sera de la forme

$$u = \frac{\sqrt{N} + p}{\rho} = r + \frac{1}{\nu},$$

d'où

$$\left(\frac{1}{\nu}\right) = \frac{\sqrt{N} - (\rho r - p)}{\rho}$$

et

$$\nu = \frac{\rho(\sqrt{N} + \rho r - p)}{N - (\rho r - p)^2},$$

par suite, comme par hypothèse le dénominateur de ν est égal à ρ , nous aurons

$$N = (\rho r - p)^2 + \rho^2.$$

Le carré du dénominateur ρ , qui se reproduit deux fois consécutives au milieu de la période, est donc l'un des carrés composants du nombre N .

9. Remarque. — Il est facile de voir que, dans la période des dénominateurs du développement de $\sqrt{N}$, deux termes consécutifs ne peuvent être simultanément pairs. Donc, dans le cas du théorème précédent, le carré composant de N , dont la racine se reproduit deux fois consécutives dans la période des dénominateurs, est toujours impair.

10. Dans le cas du même théorème, on démontrerait facilement qu'en représentant par $\frac{H}{H'}$ et $\frac{R}{R'}$ les réduites consécutives, qui correspondent aux quotients incomplets h, r de la première période, les nom-

bres $y = H'^2 + R'^2$, et $x = HH' + RR'$ constitueraient la plus petite solution entière de l'équation $x^2 - Ny^2 = -1$.

11. THÉORÈME. — *Si N est de la forme $8n + 1$, les dénominateurs pairs des quotients complets, qu'on obtient en réduisant $\sqrt{N}$ en fraction continue, sont forcément des multiples de 8.*

Soit $2p$ un dénominateur pair et $\frac{H}{H'}$ la réduite précédente, nous aurons (n° 5)

$$H^2 - NH'^2 = \pm 2p.$$

H et H' sont ici impairs; H^2 et H'^2 sont donc l'un et l'autre de la forme $8n + 1$, à laquelle le déterminant N se rattache d'après l'énoncé. Mais alors la différence $2p$ entre H^2 et NH'^2 est nécessairement un multiple de 8, ce qui démontre la proposition.

12. THÉORÈME. — *Si N est de la forme $8n + 5$, les dénominateurs pairs des quotients complets, provenant du développement de $\sqrt{N}$ en fraction continue, sont forcément des multiples de 4.*

En conservant les notations du théorème précédent, nous aurons

$$H^2 - NH'^2 = \pm 2p,$$

et comme H^2 et H'^2 sont nécessairement de la forme $8n + 1$, la différence $H^2 - (8n + 5)H'^2$ est toujours de la forme $8n + 4$, ce qui démontre le théorème.

13. Remarque. — Il résulte des deux théorèmes précédents que les deux équations

$$x^2 - Ny^2 = \pm 2, \quad x^2 - Ny^2 = \pm 2(2a + 1)$$

sont impossibles en valeurs entières de x et de y pour tout déterminant N de la forme $4n + 1$.

14. THÉORÈME. — *Si N est de la forme $8n + 2$, les dénominateurs pairs des quotients complets, qu'on obtient en réduisant $\sqrt{N}$ en fraction continue, ne peuvent contenir qu'une fois le facteur 2.*

En représentant par $2p$ un dénominateur pair, nous aurons

$$H^2 - NH'^2 = \pm 2p.$$

Dans cette relation H est pair et H' impair; par suite H^2 est de l'une des formes $8n$ ou $8n + 4$, tandis que NH'^2 est de la forme $8n + 2$. La différence $H^2 - NH'^2$ ne peut donc contenir qu'une fois le facteur 2, ce qui démontre le théorème.

On arriverait à la même conclusion dans le cas où N serait de la forme $8n + 6$.

15. THÉORÈME. — *Si N est de la forme $8n + 2$, les dénominateurs impairs des quotients complets, qu'on obtient en réduisant $\sqrt{N}$ en fraction continue, ne sont jamais de l'une des deux formes $8n + 3$, $8n + 5$.*

$2p + 1$ désignant un dénominateur impair, nous aurons

$$H^2 - NH'^2 = \pm (2p + 1).$$

Ici H est impair, tandis que H' peut être pair ou impair; par suite,

$$H^2 = 8n + 1 \quad \text{et} \quad NH'^2 = \begin{cases} 8n, \\ 8n + 2. \end{cases}$$

La différence $H^2 - NH'^2$ sera toujours de l'une des deux formes $8n + 1$, ou $8n + 7$, ce qui démontre la proposition.

16. THÉORÈME. — *Si N est de la forme $5n$, les dénominateurs des quotients complets, provenant de la réduction de $\sqrt{N}$ en fraction continue, ne sont jamais de l'une des deux formes $5n + 2$, $5n + 3$.*

En désignant par d l'un de ces dénominateurs, nous aurons

$$H^2 - NH'^2 = \pm d.$$

Il est facile de voir que, par rapport au module 5, H^2 ne pourra être que de l'une des trois formes suivantes :

$$5n, \quad 5n + 1, \quad 5n + 4,$$

31..

et comme, par hypothèse, NH'^2 est de la forme $5n$, la différence $H^2 - NH'^2$ ne sera jamais de l'une des formes $5n + 2$, $5n + 3$, indiquées ci-dessus.

17. Remarque. — Sans multiplier davantage ces théorèmes, qui se rattachent à la théorie des résidus quadratiques, nous nous bornons à énoncer le suivant :

Si N est de la forme $3n + 2$, aucun dénominateur des quotients complets, provenant de la réduction de $\sqrt{N}$ en fraction continue, ne sera divisible par 3.

18. THÉORÈME. — *Lorsque $N = a^\alpha b^\beta c^\gamma \dots$ contient des facteurs premiers a, b, c , élevés à des puissances supérieures à la première, le terme du milieu, dans la période des dénominateurs provenant de la réduction de $\sqrt{N}$ en fraction continue, ne peut pas contenir un facteur premier a , affecté d'une puissance inférieure à l'indice de ce même facteur dans N .*

Admettons, conformément à l'hypothèse de l'énoncé, qu'il existe un terme du milieu dans la période des dénominateurs, et représentons par $\mu = a^{\alpha-n} p$ ce terme, que nous supposerons d'abord impair, nous aurons (n° 5)

$$(1) \quad H^2 - a^\alpha b^\beta c^\gamma \dots H'^2 = \pm a^{\alpha-n} p.$$

On sait (n° 6) que le terme du milieu μ est un diviseur des nombres $2N$ et $2H$, nous aurons donc la relation $H = a^{\alpha-n} p \times h$. Substituons cette valeur dans (1), il viendra

$$a^{2\alpha-2n} p^2 h^2 - a^\alpha b^\beta c^\gamma \dots H'^2 = \pm a^{\alpha-n} p,$$

ou

$$a^{\alpha-n} p h^2 - a^n K H'^2 = \pm 1,$$

relation impossible, si n n'est pas nul, puisque le deuxième membre est égal à l'unité, tandis que, d'après les conditions de l'énoncé, les termes du premier membre contiendraient tous les deux le facteur a .

On verrait d'une manière analogue que l'égalité (1) est impossible en

valeurs entières, lorsque $a^{\alpha-n}p$ est pair. Le théorème est donc démontré.

19. THÉORÈME. — *Si l'équation $x^2 - a^\alpha b^\beta c^\gamma \dots y^2 = -1$, dans laquelle $a, b, c, \dots$, désignent des facteurs premiers $4n+1$, admet des solutions entières, il en sera de même de l'équation*

$$x^2 - a^{\alpha+2} b^\beta c^\gamma \dots y^2 = -1,$$

qui se déduit de la première par l'addition de deux unités à l'exposant de l'un des facteurs premiers du déterminant.

Posons $a^\alpha b^\beta c^\gamma \dots = N$, et considérons la plus petite solution entière $x=p, y=q$ de l'équation

$$(1) \quad x^2 - N y^2 = -1;$$

on sait que dans l'égalité

$$(p + q\sqrt{N})^{2k+1} = P_1 + Q_1\sqrt{N}$$

les nombres entiers $x = P_1, y = Q_1$ représentent toujours une solution de l'équation (1). Cela étant, considérons la solution de la même équation déduite de l'exposant impair et premier $4n+1 = a$. Dans la relation

$$(2) \quad (p + q\sqrt{N})^a = P + Q\sqrt{N},$$

nous aurons

$$Q = ap^{a-1}q + \frac{a(a-1)(a-2)}{1.2.3} p^{a-3}q^3N + \dots + q^a N^{\frac{a-1}{2}}.$$

Or, comme a est premier, tous les coefficients de cette expression de Q , à l'exception de celui du dernier terme, sont divisibles par a . Ainsi, puisque N contient a , la solution entière de l'équation (1), déduite de la relation (2), pourra se mettre sous la forme

$$x = P, \quad y = Q = aQ_2.$$

Substituant dans (1), nous aurons

$$P^2 - N(Q_2 a)^2 = -1,$$

égalité qui prouve que l'équation $x^2 - a^{\alpha+2} b^6 c^7 \dots y^2 = -1$ admet des solutions entières.

On comprend facilement que le raisonnement précédent est admissible dans le cas où le déterminant N est pair. Il suffira, pour que le théorème soit encore vrai dans ce cas, que le facteur premier de N , dont on augmente l'exposant de 2 unités, soit impair.

20. COROLLAIRE. — *Si l'équation $x^2 - pa^{\alpha} b^6 c^7 \dots y^2 = -1$ admet des solutions entières, il en sera de même de l'équation*

$$x^2 - pa^{\alpha+2\alpha'} b^{6+26'} c^{7+27'} \dots y^2 = -1,$$

qui dérive de la première par l'addition d'un nombre pair quelconque aux exposants des facteurs premiers impairs qui entrent dans le déterminant.

Ainsi, comme l'équation $x^2 - Ay^2 = -1$ admet toujours des solutions entières lorsque A désigne un nombre premier $4n+1$, il en sera de même de l'équation $x^2 - A^{2\alpha+1} y^2 = -1$.

21. Réciproquement, lorsqu'on aura à rechercher si une équation telle que

$$(1) \quad x^2 - a^{2\alpha+1} b^{26+1} \dots l^{2\lambda+1} A^{2a} B^{2b} \dots L^{2l} y^2 = -1$$

est soluble en entiers, il est évident, d'après le théorème qui précède, qu'en ramenant à la première puissance les exposants impairs des facteurs $a, b, \dots, l$, et à la deuxième puissance les exposants pairs des facteurs $A, B, \dots, L$, il faudra, et il suffira, pour que cette équation (1) soit soluble en entiers, qu'il en soit de même de l'équation

$$(2) \quad x^2 - ab \dots l A^2 B^2 \dots L^2 y^2 = -1.$$

De plus, on constate de suite que la possibilité de l'équation (2)

entraîne celle de l'équation suivante :

$$(3) \quad x^2 - ab \dots ly^2 = -1.$$

Mais la possibilité de cette dernière équation en valeurs entières de x et de y ne suffit pas pour qu'on puisse en conclure celle de l'équation (2). Ainsi, par exemple, l'équation $x^2 - 2.13y^2 = -1$ admet des valeurs entières de x et de y , tandis que l'équation $x^2 - 2.13.5^2y^2 = -1$ ne peut pas être satisfaite par des valeurs de même nature. Dans cette dernière équation, en effet, le déterminant $N = 2.13.5^2 = 650 = 25^2 + 25$, ou $N = a^2 + d$ (d étant un diviseur autre que l'unité du double $2a$ de la partie entière de la racine carrée de N). Or, dans ce cas, le développement du nombre littéral $\sqrt{a^2 + d}$ en fraction continue est toujours possible, et la période des dénominateurs a un terme du milieu égal à d , ce qui prouve (n° 4) que l'équation $x^2 - (a^2 + d)y^2 = -1$ est toujours impossible en valeurs entières de x et de y , dans le cas où d satisfait aux conditions précitées. Dans la même hypothèse, la plus petite solution en valeurs entières de l'équation $x^2 - (a^2 + d)y^2 = 1$ serait $x = \frac{2a^2}{d} + 1$, $y = \frac{2a}{d}$. Le signe de d pourrait même être changé, ou, en d'autres termes, si a surpasse d'une unité la racine carrée du plus grand carré contenu dans N , et si d est un diviseur de $2a$ autre que l'unité, la plus petite solution en valeurs entières de l'équation $x^2 - (a^2 - d)y^2 = 1$ sera $x = \frac{2a^2}{d} - 1$, $y = \frac{2a}{d}$.

Toutefois, il existe des cas nombreux pour lesquels la possibilité de l'équation (3) entraîne celle des équations (2) et (1); ces cas sont compris dans la proposition suivante.

22. THÉORÈME. — *Si l'équation $x^2 - ab \dots ly^2 = -1$ admet des valeurs entières, et si $A, B, \dots, L$ représentent des nombres premiers $4n + 1$ non compris dans les diviseurs linéaires de $t^2 - ab \dots lu^2$, l'équation $x^2 - ab \dots lA^2B^2 \dots L^2y^2 = -1$ sera aussi soluble en nombres entiers.*

Considérons d'abord l'équation $x^2 - ab \dots lA^2y^2 = -1$; nous allons établir le théorème en démontrant que, si A satisfait aux conditions de l'énoncé, le développement de $\sqrt{ab \dots lA^2}$ en fraction con-

tinue ne peut pas présenter de terme du milieu dans la période des dénominateurs. Nous représenterons par la lettre μ le dénominateur du milieu de la période, et nous rappellerons que, lorsque ce terme μ se rencontre dans le développement de $\sqrt{N}$, il est toujours un diviseur des nombres $2N$ et $2H$.

Cela posé, les diviseurs de $2ab \dots l$ étant déterminés et inscrits les uns à la suite des autres, en multipliant successivement ces diviseurs par 1, ce qui les reproduira, ensuite par A et enfin par A^2 , on obtiendra tous les diviseurs de $2ab \dots lA^2$. Ainsi, en représentant par α un diviseur quelconque de $2ab \dots l$, les diviseurs de $2ab \dots lA^2$ se rattacheront à l'un des trois types suivants :

$$\alpha, \quad \alpha A, \quad \alpha A^2.$$

Or, il est facile de voir qu'aucun nombre de ces types ne pourra être égal à la valeur de μ dans le développement de $\sqrt{ab \dots lA^2}$ en fraction continue.

Si, dans ce développement, on pouvait avoir $\mu = \alpha$, il résulterait de l'égalité

$$H^2 - ab \dots l(A^2 H'^2) = \pm \alpha$$

que le même nombre α serait également admissible pour μ dans le développement de $\sqrt{ab \dots l}$, ce qui est contraire aux conditions de l'énoncé, puisque, par hypothèse, l'équation $x^2 - ab \dots ly^2 = -1$ admet des solutions entières.

La valeur $\mu = \alpha A$ ne peut pas être admise, d'après ce qui a été démontré (n° 18).

Enfin, si $\mu = \alpha A^2$ était admissible, nous aurions l'égalité

$$H^2 - ab \dots lA^2 H'^2 = \pm \alpha A^2,$$

et, comme $H = \alpha A^2 h$, cette égalité peut se mettre sous la forme

$$(\alpha A h)^2 - ab \dots lH'^2 = \pm \alpha,$$

relation qui prouve que, dans l'hypothèse où l'on s'est placé, $\mu = \alpha$ serait admissible dans le développement de $\sqrt{ab \dots l}$ en fraction con-

tinue, ce qui est impossible, ainsi qu'on l'a vu dans le cas précédent. Il est donc également impossible qu'on puisse avoir $\mu = \alpha A^2$ dans le développement de $\sqrt{ab \dots l A^2}$.

Il reste toutefois à prouver cette dernière impossibilité, dans le cas où α serait égal à 1, c'est-à-dire pour $\mu = A^2$. Nous aurions, dans cette hypothèse,

$$H^2 - ab \dots l A^2 H'^2 = \pm A^2.$$

Ici $H = A^2 h$, et, par suite,

$$A^2 h^2 - ab \dots l H'^2 = \pm 1,$$

A serait donc un diviseur de $t^2 \pm ab \dots l u^2$, ce qui est contraire aux conditions de l'énoncé. Le théorème est donc démontré dans le cas de l'équation $x^2 - ab \dots l A^2 y^2 = -1$.

En considérant l'équation $x^2 - ab \dots l A^2 B^2 y^2 = -1$, le théorème s'établirait de la même manière; car l'équation $x^2 - ab \dots l A^2 y^2 = -1$ admet des solutions entières, et, de plus, B n'est pas compris dans les diviseurs linéaires de $t^2 - abl \dots A^2 u^2$. La proposition s'étend donc à un nombre quelconque de facteurs A, B, ..., L, remplissant les conditions de l'énoncé.

COROLLAIRE. — Si l'équation $x^2 - ab \dots l y^2 = -1$ admet des solutions entières, et si les facteurs premiers A, B, ..., L, de la forme $4n + 1$, ne sont pas compris dans les diviseurs de $t^2 - ab \dots l u^2$, l'équation $x^2 - a^{2\alpha+1} b^{2\beta+1} \dots l^{2\lambda+1} A^{2a} B^{2b} \dots L^{2l} y^2 = -1$ admettra aussi des solutions entières (n° 19).

23. THÉORÈME. — Si A, B, C, ..., L représentent des nombres premiers de la forme $8n + 5$, les équations

$$\begin{aligned} x^2 - 2A y^2 &= -1, \\ x^2 - 2AB y^2 &= -1, \\ x^2 - 2A^2 B^2 C^2 \dots L^2 y^2 &= -1 \end{aligned}$$

sont toujours possibles en nombres entiers.

Nous démontrerons ce théorème en suivant la méthode du numéro précédent.

1° $x^2 - 2A y^2 = -1$. Les diviseurs du double du déterminant N inférieurs à $2\sqrt{N}$ sont 2 et 4. Or, comme $2A$ est de la forme $8n + 2$, $\mu = 4$ est inadmissible dans la période des dénominateurs (n° 14).

Il en est de même de $\mu = 2$; car, dans cette hypothèse, nous aurions

$$H^2 - 2AH'^2 = \pm 2,$$

relation impossible, parce que A , qui est de la forme $8n + 5$, serait diviseur linéaire de $t^2 \pm 2u^2$, ce qui n'a jamais lieu. Donc le développement de $\sqrt{2A}$ en fraction continue ne peut pas avoir de terme du milieu de la période, et, par suite (n° 4), l'équation $x^2 - 2A y^2 = -1$ admet toujours des solutions entières.

2° $x^2 - 2AB y^2 = -1$. Les douze diviseurs de $4AB$ sont :

$$1, 2, 4, A, 2A, 4A, B, 2B, 4B, AB, 2AB, 4AB.$$

Rejetant l'unité, le facteur 2 d'après ce qu'on a dit au cas précédent, les multiples de 4 (n° 13), et les nombres supérieurs à $2\sqrt{2AB}$, les seules valeurs, que pourrait prendre μ , parmi ces diviseurs, sont

$$(A, 2B), (B, 2A);$$

$\mu = A$ et $\mu = B$ sont inadmissibles (n° 15), il ne reste donc à considérer que les diviseurs conjugués de ces deux derniers $2A$ et $2B$. Or, en général, si un diviseur B n'est pas admissible pour μ , il en est de même de son diviseur conjugué $2A$. C'est ce que nous allons reconnaître dans ce cas particulier. Supposons, en effet, qu'on puisse avoir $\mu = 2A$, il en résulterait :

$$H^2 - 2ABH'^2 = \pm 2A,$$

ou bien, en vertu de la relation $H = 2Ah$,

$$2Ah^2 = BH'^2 \pm 1.$$

Dans cette relation H' est impair, puisque H et H' sont les termes d'une

même réduite, par suite BH'^2 est de la forme $8n + 5$ et $BH'^2 \pm 1$ de l'une des deux formes $8n + 4$, $8n + 6$. D'un autre côté, le premier membre $2Ah^2$ de la même relation ne peut être que de l'une des deux formes $8n$, $8n + 2$. Cette dernière relation est donc impossible en valeurs entières de h et de H' , et, par suite, $\mu = 2A$ est inadmissible.

Il en serait de même de $\mu = 2B$, ce qui démontre le théorème pour le second cas $x^2 - 2AB\gamma^2 = -1$.

3° $x^2 - 2A^2B^2C^2 \dots L^2\gamma^2 = -1$. On sait que l'équation $x^2 - 2\gamma^2 = -1$ admet toujours des solutions entières; on sait de plus que les nombres $A, B, \dots, L$, supposés premiers de la forme $8n + 5$, ne sont jamais compris dans les diviseurs linéaires de $t^2 - 2u^2$. Ce troisième cas est donc démontré, puisqu'il rentre dans le théorème établi (n° 22).

24. Il résulte immédiatement des théorèmes démontrés (n°s 20 et 23) que, si $A, B, C, \dots, L$ représentent des nombres premiers $8n + 5$, les équations.

$$x^2 - 2A^\alpha \gamma^2 = -1,$$

$$x^2 - 2A^{2\alpha+1} B^{2\beta+1} \gamma^2 = -1,$$

$$x^2 - 2A^{2\alpha} B^{2\beta} C^{2\gamma} \dots L^{2\lambda} \gamma^2 = -1$$

admettent toujours des solutions entières.

25. Remarque. — On voit, d'après le théorème précédent, que si deux facteurs premiers A et B de la forme $8n + 5$ sont combinés avec le facteur 2, l'équation $x^2 - 2A^m B^n \gamma^2 = -1$ est toujours possible en nombres entiers, lorsque les exposants m et n sont de même parité. Mais, si les exposants de A et de B sont de parité différente, l'équation correspondante peut ne pas être soluble en valeurs entières de x et de γ . On en voit un exemple dans l'équation $x^2 - 2 \cdot 5 \cdot 13^2 \gamma^2 = -1$, qui n'est jamais vérifiée par des valeurs entières.

Toutefois, il résulte du théorème (n° 20) que si les nombres premiers A et B de la forme $8n + 5$ sont tels, que B ne soit pas compris dans les diviseurs linéaires de $t^2 - 2Au^2$, l'équation $x^2 - 2A^{2\alpha+1} B^{2\beta} \gamma^2 = -1$ admettra toujours des solutions entières.

Cette dernière proposition peut d'ailleurs (n°s 20 et 22) être généralisée de la manière suivante :

THÉOREME. — Si $B, C, \dots, L$ représentent des nombres premiers $8n + 5$, et $a, b, \dots, l$ des nombres premiers $8n + 1$, qui ne soient compris ni les uns ni les autres dans les diviseurs linéaires du nombre quadratique $t^2 - 2Au^2$, dans lequel A représente aussi un facteur premier $8n + 5$, l'équation

$$x^2 - 2A^{2\alpha+1} B^{2\beta} \dots L^{2\lambda} a^{2m} b^{2n} \dots l^{2p} y^2 = -1$$

admet toujours des solutions entières.

26. THÉOREME. — Si A, B, C désignent des nombres premiers de la forme $8n + 5$, et si B et C ne sont pas compris dans les diviseurs linéaires de $t^2 - 2Au^2$, les équations

$$x^2 - 2ABC y^2 = -1,$$

$$x^2 - 2A^2 BC y^2 = -1$$

sont toujours possibles en nombres entiers.

1° $x^2 - 2ABC y^2 = -1$. Les diviseurs de $4ABC$ sont au nombre de 24; en excluant : 1° le facteur 2, 2° ceux qui sont des multiples de 4 (n° 14), 3° ceux qui sont de la forme $8n + 5$ (n° 15) et les facteurs conjugués de ces derniers, tels que $2AB, 2AC, 2BC$, 4° ceux qui sont plus grands que $2\sqrt{2ABC}$; et en ne considérant qu'une fois ceux qui sont symétriques, tels que $2B$ et $2C, AB$ et AC , ces 24 diviseurs se réduisent aux quatre suivants :

$$(2A, BC), (2B, AC),$$

et ces diviseurs peuvent s'assembler deux à deux en groupes de facteurs conjugués dont le produit est égal à $2ABC$.

Pour établir le théorème, il suffira donc de démontrer que le nombre, que nous avons désigné par μ , ne peut être égal à aucun de ces quatre diviseurs.

Dans l'une des hypothèses $\mu = 2A, \mu = BC$, nous aurions, après la réduction connue consistant en ce que μ est toujours un diviseur de $2H$, la relation

$$(\mu = 2A, BC). 2Ah^2 - BCH'^2 = \pm 1.$$

Or, cette relation est impossible en valeurs entières de h et de H' , puisque, d'après l'énoncé, B et C ne sont pas compris dans les diviseurs linéaires de $t^2 \pm 2Au^2$. L'hypothèse $\mu = 2A$ ou $\mu = BC$ est donc inadmissible.

Supposons en deuxième lieu qu'on puisse avoir $\mu = 2B$ ou $\mu = AC$, il en résulterait, après la réduction connue, la relation

$$(\mu = 2B, AC), \quad 2Bh^2 - ACH'^2 = \pm 1.$$

Si, dans cette relation, h et H' admettaient des valeurs entières, A serait un diviseur de $t^2 \pm 2Bu^2$. Or, comme les nombres premiers A et B sont de la forme $8n + 5$, il est facile de prouver que *si B ne divise pas la formule $t^2 + 2Au^2$, réciproquement A ne divisera pas la formule $t^2 + 2Bu^2$.*

En conservant la notation de Legendre $\left(\frac{N}{C}\right)$ pour exprimer le reste de la division du nombre $N \frac{C-1}{2}$ par le facteur premier C , reste qui, d'après le théorème de Fermat, est toujours égal à $+1$ ou à -1 , nous aurons en effet, puisque, d'après l'énoncé, B ne divise pas $t^2 + 2Au^2$, l'égalité

$$\left(\frac{2A}{B}\right) = -1;$$

mais comme B est de la forme $8n + 5$, on sait que $\left(\frac{2}{B}\right) = -1$; par suite $\left(\frac{A}{B}\right) = 1$. Donc, d'après la loi de réciprocité, $\left(\frac{B}{A}\right) = 1$, et comme $\left(\frac{2}{A}\right) = -1$, nous aurons enfin $\left(\frac{2B}{A}\right) = -1$, égalité qui prouve que A n'est pas compris dans les diviseurs linéaires de $t^2 + 2Bu^2$.

Il n'est pas nécessaire de rappeler d'ailleurs que tout nombre premier $4n + 1$, qui ne divise pas la formule $t^2 + au^2$, ne divise pas non plus la formule $t^2 - au^2$. L'hypothèse $(\mu = 2B, AC)$ est donc inadmissible et le premier cas du théorème est démontré.

2° $x^2 - 2A^2BCy^2 = -1$. D'après l'énoncé du théorème les nombres premiers B et C de la forme $8n + 5$ ne sont pas diviseurs de $t^2 + 2Au^2$; il est facile de prouver par suite que réciproquement A

n'est pas diviseur de $t^2 + 2BCu^2$. Puisque B et C ne divisent pas $t^2 + 2Au^2$, nous avons, en effet,

$$\left(\frac{2A}{B}\right) = -1, \quad \left(\frac{2A}{C}\right) = -1;$$

mais comme $\left(\frac{2}{B}\right) = \left(\frac{2}{C}\right) = -1$, il en résulte $\left(\frac{A}{B}\right) = \left(\frac{A}{C}\right) = 1$, d'où, en vertu de la loi de réciprocité, $\left(\frac{BC}{A}\right) = 1$, et finalement $\left(\frac{2BC}{A}\right) = -1$, égalité qui prouve que A n'est pas diviseur de $t^2 + 2BCu^2$.

Cela posé, on sait (n° 25) que l'équation $x^2 - 2BCy^2 = -1$ admet toujours des solutions entières. Donc (n° 22) il en sera de même de l'équation $x^2 - 2BCA^2y^2 = -1$.

27. Des théorèmes, qui viennent d'être démontrés, on déduit comme conséquence la proposition suivante :

THÉORÈME. — Si A, B, C, ..., L représentent des nombres premiers $8n+5$, et si B, C, ..., L ne sont pas compris dans les diviseurs linéaires de $t^2 - 2Au^2$, les équations

$$x^2 - 2A^\alpha B^{2^6+1} C^{2^7+1} y^2 = -1,$$

$$x^2 - 2A^\alpha B^{2^6} C^{2^7} \dots L^{2^\lambda} y^2 = -1$$

sont toujours solubles en nombres entiers.

28. En donnant à A diverses valeurs particulières, on peut déduire du théorème précédent une série de corollaires.

Corollaire I. — Si B, C, ..., L désignent des nombres premiers de l'une des formes $40x+21$, $40x+29$, les équations

$$x^2 - 2.5^\alpha B^{2^6+1} C^{2^7+1} y^2 = -1,$$

$$x^2 - 2.5^\alpha B^{2^6} C^{2^7} \dots L^{2^\lambda} y^2 = -1$$

admettent toujours des solutions entières.

Corollaire II. — Si B, C, ..., L désignent des nombres premiers de l'une des formes $104x+29$, $104x+53$, $104x+61$, $104x+69$,

$104x + 77$, $104x + 101$, les équations

$$x^2 - 2.13^\alpha B^{26+\alpha} C^{27+\alpha} y^2 = -1,$$

$$x^2 - 2.13^\alpha B^{26} C^{27} \dots L^{2\lambda} y^2 = -1$$

sont toujours solubles en nombres entiers.

29. Remarque. — D'après le théorème (n° 26), l'équation $x^2 - 2ABCy^2 = -1$, dans laquelle A, B, C représentent des nombres premiers $8n + 5$, admet des solutions entières, si les deux conditions $\left(\frac{A}{B}\right) = 1$, $\left(\frac{A}{C}\right) = 1$ sont satisfaites. Or, les facteurs premiers A, B, C du déterminant peuvent être permutés dans ces égalités symboliques; nous pouvons donc généraliser la première partie du théorème n° 26 de la manière suivante :

L'équation $x^2 - 2ABCy^2 = -1$ admet toujours des solutions entières, lorsque deux des trois quantités $\left(\frac{A}{B}\right)$, $\left(\frac{A}{C}\right)$, $\left(\frac{B}{C}\right)$ sont égales à $+1$.

En examinant les huit combinaisons de signe que peuvent présenter les trois quantités $\left(\frac{A}{B}\right)$, $\left(\frac{A}{C}\right)$, $\left(\frac{B}{C}\right)$, le dernier énoncé prouve que, pour quatre d'entre elles, l'équation considérée admet toujours des solutions entières. Mais la méthode ne permet aucune affirmation pour les quatre combinaisons restantes. Si deux quantités $\left(\frac{A}{C}\right)$, $\left(\frac{B}{C}\right)$ sont égales à -1 , nous aurions en effet la relation

$$(\mu = 2C, AB) \quad 2Ch^2 - ABH'^2 = \pm 1$$

qui peut admettre des valeurs entières pour h et H' .

La deuxième partie du même théorème peut s'énoncer ainsi qu'il suit :

L'équation $x^2 - 2BCA^2y^2 = -1$ admet toujours des solutions entières, lorsque $\left(\frac{B}{A}\right) = \left(\frac{C}{A}\right) = \pm 1$ (nos 22 et 23).

On voit, d'après ces deux énoncés, que si, $\left(\frac{B}{C}\right)$ étant égal à -1 , on considère une équation toujours possible en nombres entiers, dont le déterminant $2BC$ soit égal au produit du facteur 2 par deux facteurs premiers $8n + 5$, et que si on introduit dans ce déterminant un facteur

premier A de la même forme, la probabilité de la possibilité en valeurs entières ne sera pas la même pour les deux équations suivantes :

$$x^2 - 2BCA y^2 = -1,$$

$$x^2 - 2BCA^2 y^2 = -1.$$

Pour qu'on puisse affirmer que la première équation admet forcément des valeurs entières, il faut en effet les deux conditions $\left(\frac{B}{A}\right) = 1$, $\left(\frac{C}{A}\right) = 1$, tandis que la seconde sera toujours soluble en entiers non-seulement dans le cas qui précède $\left(\frac{B}{A}\right) = 1$, $\left(\frac{C}{A}\right) = 1$, mais encore dans le cas suivant $\left(\frac{B}{A}\right) = -1$, $\left(\frac{C}{A}\right) = -1$. Pour fixer les idées, considérons les deux équations

$$(1) \quad x^2 - 2.5.13.37 y^2 = -1,$$

$$(2) \quad x^2 - 2.5.13.37^2 y^2 = -1,$$

dans lesquelles $\left(\frac{5}{13}\right) = -1$, nous avons $\left(\frac{5}{37}\right) = -1$, $\left(\frac{13}{37}\right) = -1$. Par suite, l'équation (2) admet toujours des solutions entières, tandis que nous ne pouvons rien affirmer pour l'équation (1). On reconnaîtrait d'ailleurs, par une autre voie, que cette équation (1) est impossible en valeurs entières de x et de y .

30. Avant d'examiner le cas dans lequel les facteurs premiers $8n+5$ et $8n+1$ sont mêlés dans leur combinaison avec le nombre 2, recherchons d'une manière générale les conditions de possibilité en nombres entiers d'une équation $x^2 - 2AB...KLy^2 = -1$, qui contient un nombre quelconque de facteurs premiers $8n+5$ dans son déterminant.

A cet effet, considérons encore un cas particulier, *et déterminons analytiquement les conditions de possibilité en nombres entiers de l'équation*

$$x^2 - 2ABCD y^2 = -1,$$

dans laquelle A, B, C, D représentent des nombres premiers de la forme $8n+5$.

Nous déterminerons ces conditions en écrivant que, dans la période des dénominateurs des quotients complets provenant du développement de $\sqrt{2ABCD}$ en fraction continue, il ne peut pas y avoir de terme du milieu, terme que nous avons désigné jusqu'ici par la lettre μ .

Or, en inscrivant les quarante-huit diviseurs de $4ABCD$, on constate que, pour trente-six de ces diviseurs, les relations analogues à la suivante :

$$H^2 - 2ABCDH'^2 = \pm \mu,$$

dans lesquelles μ doit non-seulement diviser $4ABCD$, mais encore $2H$, sont naturellement impossibles en valeurs entières de H et de H' . Tous les diviseurs impairs de $2N$, qui contiendraient un nombre impair de facteurs premiers A, B, C, D , seraient de la forme $8n + 5$, et seraient ainsi inadmissibles pour μ (n° 15); le diviseur impair $ABCD$ est supérieur à $2\sqrt{N}$, et doit être rejeté. Il ne restera donc à considérer que les six diviseurs impairs AB, AC , etc., provenant de la combinaison deux à deux des facteurs A, B, C, D , ainsi que les facteurs conjugués de ces diviseurs impairs, en tout douze diviseurs, qui pourraient correspondre à la valeur de μ , savoir :

$(AB, 2CD), (AC, 2BD), (BC, 2AD), (AD, 2BC), (CD, 2AB), (BD, 2AC)$.

Par suite, les conditions de possibilité de l'équation considérée en nombres entiers s'obtiendront en écrivant qu'aucune des six relations suivantes ne peut admettre de solutions entières :

$$(a) \quad \begin{cases} (\mu = AB, 2CD) & ABh^2 - 2CDH'^2 = \pm 1, \\ (\mu = AC, 2BD) & AC h^2 - 2BDH'^2 = \pm 1, \\ (\mu = BC, 2AD) & BC h^2 - 2ADH'^2 = \pm 1, \\ (\mu = AD, 2BC) & AD h^2 - 2BCH'^2 = \pm 1, \\ (\mu = CD, 2AB) & CD h^2 - 2ABH'^2 = \pm 1, \\ (\mu = BD, 2AC) & BD h^2 - 2ACH'^2 = \pm 1. \end{cases}$$

Il est facile de reconnaître que ces relations ne peuvent être vérifiées par aucune valeur entière de h ou de H' , si l'on a les cinq égalités symboliques suivantes :

$$(b) \quad \left(\frac{A}{C}\right) = 1, \quad \left(\frac{B}{C}\right) = 1, \quad \left(\frac{A}{D}\right) = 1, \quad \left(\frac{B}{D}\right) = 1, \quad \left(\frac{C}{D}\right) = 1.$$

Car, en examinant la première des relations (α), nous aurons, en combinant la première et la troisième des égalités (6) avec l'égalité connue $\left(\frac{2}{A}\right) = -1$, l'égalité nouvelle $\left(\frac{2CD}{A}\right) = -1$, qui prouve que A n'est pas compris dans les diviseurs linéaires de $t^2 \pm 2CDu^2$, ou, en d'autres termes, que la relation considérée n'admet pas de valeurs entières pour h et H' . On prouverait d'une manière analogue que l'existence des cinq égalités symboliques (6) entraîne l'impossibilité en valeurs entières de h et de H' pour les autres relations (α).

Ainsi, en traduisant en langage ordinaire les conditions représentées par les égalités symboliques (6), nous aurons les conditions de possibilité en nombres entiers de l'équation considérée, dont le déterminant est $2ABCD$. Remarquons à cet effet que la première et la deuxième des égalités (6) expriment que A et B ne sont pas compris dans les diviseurs linéaires de $t^2 - 2Cu^2$, ou, en d'autres termes, qu'elles expriment (n° 26) que l'équation $x^2 - 2ABCy^2 = -1$ admet des solutions entières. Remarquons de même que les troisième, quatrième et cinquième égalités (6) expriment que A, B et C ne sont pas compris dans les diviseurs de $t^2 - 2Du^2$.

Nous arrivons ainsi à formuler la proposition suivante :

THÉORÈME. — *Si A, B, C, D représentent des nombres premiers $8n + 5$ l'équation*

$$x^2 - 2ABCDy^2 = -1$$

admet toujours des solutions entières, lorsque l'équation

$$x^2 - 2ABCy^2 = -1$$

est soluble en nombres entiers, et lorsque, de plus, les facteurs premiers A, B, C, qui entrent dans le déterminant de cette dernière équation, ne sont pas compris dans les diviseurs linéaires de $t^2 - 2Du^2$.

La loi relative au cas de quatre facteurs premiers $8n + 5$, combinés avec le nombre 2, est donc analogue à celle qui a été déterminée pour le cas de trois facteurs. Hâtons-nous d'ajouter cependant que les égalités symboliques (6) ne comprennent pas tous les cas d'impossibilité en nombres entiers des relations (α), ou, en d'autres termes,

que les conditions restrictives du dernier théorème peuvent être modifiées. Mais, avant de développer cette considération, nous allons démontrer que la loi, qui vient d'être remarquée, est susceptible d'être généralisée.

31. *Recherchons à cet effet les conditions de possibilité en nombres entiers de l'équation*

$$(1) \quad x^2 - 2AB...FKLy^2 = -1,$$

dans laquelle un nombre quelconque de facteurs premiers $8n + 5$ est combiné avec 2 dans le déterminant.

Commençons par déterminer d'une manière générale le nombre des équations de condition analogues aux relations (α) du numéro précédent. Comme chaque diviseur impair de $2N$ aura son conjugué dans les diviseurs pairs, le nombre de ces relations sera égal au nombre des diviseurs impairs admissibles pour μ . Or (n° 15), les valeurs impaires à assigner à μ contiendront toujours un nombre pair de facteurs premiers de N . Par suite, dans le cas où le nombre m de facteurs premiers $8n + 5$, qui entrent dans le déterminant, est pair, on pourra assigner à μ les valeurs suivantes :

1° Les diviseurs $AB, AC, \text{ etc.}$, provenant des combinaisons deux à deux des facteurs premiers du déterminant, c'est-à-dire $\frac{m(m-1)}{2}$ valeurs.

2° Les diviseurs $ABCD, ABCE, \text{ etc.}$, provenant des combinaisons quatre à quatre des mêmes facteurs, c'est-à-dire $\frac{m(m-1)(m-2)(m-3)}{1.2.3.4}$ valeurs.

3° Les diviseurs $ABCDEF, ABCDEG, \text{ etc.}$, provenant des combinaisons six à six des facteurs de N , c'est-à-dire $\frac{m(m-1)...(m-5)}{1.2...6}$ valeurs.

Et ainsi de suite jusqu'aux combinaisons $m - 2$ à $m - 2$ des facteurs de N , c'est-à-dire $\frac{m(m-1)}{2}$ valeurs.

Le nombre total de ces valeurs de μ sera évidemment égal à la

somme des coefficients des termes de rang impair de la formule du binôme de Newton diminuée des coefficients du premier et du dernier terme, qui sont l'un et l'autre égaux à l'unité. Or, on sait que, dans cette formule du binôme, la somme des coefficients des termes de rang impair est égale à 2^{m-1} . Ainsi, dans le cas de m pair, le nombre des équations de condition analogues aux relations (α) sera égal à $2^{m-1} - 2$. Pour $m = 4$, cette formule nous donne six relations, ainsi que nous l'avons constaté dans le numéro précédent. Pour $m = 2$, la même formule indique qu'il n'y a pas d'équations de condition pour la possibilité en nombres entiers de l'équation

$$x^2 - 2AB y^2 = -1,$$

ou, en d'autres termes, elle confirme le théorème consistant en ce que cette équation admet toujours des solutions entières, lorsque A et B sont des nombres premiers de la forme $8n + 5$.

Si le nombre m de facteurs premiers qui entrent dans le déterminant est impair, le nombre des valeurs impaires à assigner à μ s'obtiendra, comme ci-dessus, en additionnant le nombre des combinaisons deux à deux, quatre à quatre, etc., jusqu'au nombre des combinaisons $m - 1$ à $m - 1$ des facteurs premiers de N . Comme dans ce cas le dernier terme de la formule du binôme est de rang pair, le nombre total des valeurs impaires, qui pourront être assignées à μ , sera égal à la somme des coefficients des termes de rang impair de la formule du binôme diminuée du coefficient du premier terme, c'est-à-dire de l'unité. Pour m impair, les équations de condition seront donc au nombre de $2^{m-1} - 1$. Pour $m = 1$, il n'y a donc pas d'équation de condition, et l'équation

$$x^2 - 2A y^2 = -1$$

admet toujours des solutions entières pour tout nombre A premier $8n + 5$.

Après cette digression, revenons à la recherche des conditions de possibilité de l'équation (1), et remarquons que les équations de condition se ramèneront aux types suivants :

$$(7) \left\{ \begin{array}{ll} (\mu = \text{type AB}) & ABh^2 - 2CD \dots LH'^2 = \pm 1, \\ (\mu = \text{type ABCD}) & ABCDh^2 - 2E \dots LH'^2 = \pm 1; \\ \dots\dots\dots & \dots\dots\dots \\ \text{et, enfin, pour } m \text{ pair} & \\ (\mu = \text{type } 2AB) & CD \dots Lh^2 - 2ABH'^2 = \pm 1, \\ \text{et, dans le cas de } m \text{ impair} & \\ (\mu = \text{type } 2A) & CD \dots Lh^2 - 2AH'^2 = \pm 1. \end{array} \right.$$

Toutes ces relations seront impossibles en valeurs entières de h et de H' si, $\left(\frac{A}{B}\right)$ restant arbitraire, nous avons les $\frac{m(m-1)}{2} - 1$ égalités symboliques suivantes, que l'on obtient en combinant deux à deux les facteurs premiers $8n + 5$ qui entrent dans le déterminant, savoir :

$$(8) \left\{ \begin{array}{l} \left(\frac{A}{C}\right) = \left(\frac{B}{C}\right) = 1, \\ \left(\frac{A}{D}\right) = \left(\frac{B}{D}\right) = \left(\frac{C}{D}\right) = 1, \\ \left(\frac{A}{E}\right) = \left(\frac{B}{E}\right) = \left(\frac{C}{E}\right) = \left(\frac{D}{E}\right) = 1, \\ \dots\dots\dots \\ \left(\frac{A}{L}\right) = \left(\frac{B}{L}\right) = \left(\frac{C}{L}\right) = \dots = \left(\frac{K}{L}\right) = 1. \end{array} \right.$$

Il est clair, en effet, que si, dans l'hypothèse où nous venons de nous placer, nous considérons un type quelconque des relations (7), le type AB par exemple, nous aurons $\left(\frac{2CD \dots L}{B}\right) = -1$ pour toutes les combinaisons AB, et que, par cela même, les diverses égalités de ce type seront impossibles en valeurs entières de h et de H' . La même impossibilité s'établit facilement pour les relations (7) des autres types.

Il reste à établir nettement que, dans le cas particulier où l'on s'est placé, $\left(\frac{A}{B}\right)$ peut rester arbitraire, et que les $\frac{m(m-1)}{2} - 1$ égalités (8) concourent toutes à l'impossibilité des relations (7). En premier lieu,

A n'entrera jamais seul (n° 15) dans un coefficient impair de h^2 de ces relations; dès lors, en examinant l'une quelconque d'entre elles

$$(2) \quad A n h'^2 - 2 p H'^2 = \pm 1,$$

et en considérant un facteur premier quelconque n_i de n , il est évident qu'en vertu des relations (δ) nous arriverons toujours à établir l'égalité $\left(\frac{2p}{n_i}\right) = -1$, qui assure l'impossibilité de cette relation (2) en valeurs entières de h et de H' , sans que nous soyons obligés d'avoir égard au signe de $\left(\frac{A}{B}\right)$. Nous arriverions à une conséquence analogue pour les relations dans lesquelles A entrerait dans un coefficient pair. Le signe de $\left(\frac{A}{B}\right)$ peut donc rester arbitraire.

En deuxième lieu, en admettant que $\left(\frac{A}{B}\right)$ soit arbitraire, c'est-à-dire égal à $+1$ ou à -1 , il est facile de voir que l'une quelconque des égalités (δ), telle que $\left(\frac{D}{E}\right) = 1$, concourt à l'impossibilité des relations (γ). Il résulte en effet de ce qui précède que le diviseur AE du déterminant sera l'une des valeurs susceptibles d'être assignées à μ , les relations (γ) comprendront donc la suivante

$$AE h^2 - 2 BCD \dots K L H'^2 = \pm 1.$$

Or, l'impossibilité de cette relation en valeurs entières de h et de H' se prouve par l'égalité $\left(\frac{2 BCD \dots K L}{E}\right) = -1$, à l'établissement de laquelle concourt l'égalité considérée $\left(\frac{D}{E}\right) = 1$.

Ainsi, en résumé, sans affirmer que l'équation

$$x^2 - 2 ABCD \dots F K L y^2 = -1$$

ne soit possible en nombres entiers que dans le cas où les égalités (δ) sont remplies, il est certain que si ces $\frac{m(m-1)}{2} - 1$ égalités sont satisfaites, l'équation considérée admettra des solutions entières.

Pour formuler une loi de possibilité, il suffira de traduire en langage ordinaire les égalités (δ). Or, les deux premières expriment que A et B ne sont pas compris dans les diviseurs de $t^2 - 2Cu^2$, les trois suivantes signifient que A, B et C ne sont pas compris dans les diviseurs linéaires de $t^2 - 2Du^2$, et ainsi de suite, suivant une loi évidente jusqu'aux égalités de la dernière ligne qui expriment que les $m - 1$ facteurs premiers A, B, C, ..., F, K ne sont pas compris dans les diviseurs linéaires de $t^2 - 2Lu^2$. Nous arrivons ainsi à la proposition suivante :

THÉOREME. — *L'équation $x^2 - 2ABC...FKLy^2 = -1$, dans laquelle A, B, C, ..., L représentent des nombres premiers $8n + 5$, admet toujours des solutions entières, lorsque l'équation $x^2 - 2ABC...FKy^2 = -1$ a des solutions de même nature, et lorsque de plus les facteurs A, B, C, ..., K, qui entrent dans le déterminant de cette dernière équation, ne sont pas compris dans les diviseurs linéaires de $t^2 - 2Lu^2$.*

32. Dans l'énoncé précédent, on a traduit en langage ordinaire les conditions qui dérivent des égalités symboliques (δ); par cela même, la condition relative à la possibilité en nombres entiers de l'équation $x^2 - 2ABC...FKy^2 = -1$ doit être entendue dans ce sens que l'équation $x^2 - 2ABC...Fy^2 = -1$ admet à son tour des solutions entières, et que de plus A, B, C, ..., F ne sont pas compris dans les diviseurs linéaires de $t^2 - Ku^2$, et ainsi de suite, en passant par une série d'équations dans lesquelles le nombre des facteurs premiers du déterminant diminue successivement d'une unité jusqu'à ce qu'on arrive à l'équation $x^2 - 2ABy^2 = -1$, qui admet toujours des solutions entières aussi bien dans le cas de $\left(\frac{A}{B}\right) = 1$ que dans le cas contraire $\left(\frac{A}{B}\right) = -1$.

En donnant cette interprétation à l'énoncé du théorème du n° 31, il est évident que les équations qui auraient pour déterminant le facteur 2 multiplié par une combinaison quelconque n à n des facteurs premiers $8n + 5$, qui entrent dans le déterminant de l'équation primitive, seraient aussi toujours possibles en nombres entiers.

Ainsi, pour fixer les idées, considérons l'équation

$$x^2 - 2.29.61.5.109y^2 = -1;$$

nous pouvons affirmer (n° 31) qu'elle admet des solutions entières, puisque nous avons les $\frac{m(m-1)}{2} - 1 = 5$ égalités symboliques suivantes :

$$\left(\frac{29}{5}\right) = \left(\frac{61}{5}\right) = 1, \quad \left(\frac{29}{109}\right) = \left(\frac{61}{109}\right) = \left(\frac{5}{109}\right) = 1,$$

et nous pouvons affirmer de plus que des nombres entiers peuvent également vérifier les équations qui auraient pour déterminant les nombres qu'on obtiendrait en multipliant 2 par les combinaisons trois à trois des facteurs premiers $8n+5$ qui entrent dans l'équation primitive, savoir :

$$2. 5.29. 61 = 17690,$$

$$2. 5.29.109 = 31610,$$

$$2. 5.61.109 = 66490,$$

$$2.29.61.109 = 385642.$$

Dans l'équation dont le déterminant serait 17690, nous aurions en effet $\left(\frac{2.5}{29}\right) = -1$, $\left(\frac{2.5}{61}\right) = -1$, conditions qui suffisent (n° 26) pour assurer la possibilité de cette équation en valeurs entières. On reconnaîtrait de la même manière que les trois équations suivantes sont dans le même cas.

35. Nous avons dit ci-dessus, à la suite de l'énoncé du théorème du n° 30, que tous les cas de possibilité de l'équation $x^2 - 2ABCDy^2 = -1$ en nombres entiers n'étaient pas compris dans ce théorème; pour légitimer cette assertion, supposons que les égalités symboliques (6), inscrites au numéro précité, soient remplacées par les égalités suivantes :

$$(6') \quad \left(\frac{A}{C}\right) = \left(\frac{B}{C}\right) = -1, \quad \left(\frac{A}{D}\right) = \left(\frac{B}{D}\right) = \left(\frac{C}{D}\right) = -1.$$

En suivant la marche habituelle, on reconnaîtra sans difficulté que

si ces cinq conditions (6') sont remplies, les équations de condition (α), inscrites (n° 30), sont impossibles en valeurs entières de h et de H' , ou, en d'autres termes, que, dans cette hypothèse, l'équation

$$x^2 - 2ABCDy^2 = -1$$

admet des solutions entières.

En traduisant en langage ordinaire les conditions (6'), nous aurons la proposition suivante :

THÉORÈME. — *L'équation $x^2 - 2ABCDy^2 = -1$, dans laquelle A, B, C, D représentent des nombres premiers $8n + 5$, est toujours possible en nombres entiers, si A et B ne sont pas compris dans les diviseurs de $t^2 - Cu^2$, et si de plus A, B, C ne sont pas compris dans les diviseurs de $t^2 - Du^2$.*

34. Il est facile de constater que le théorème précédent, dans lequel la loi relative aux conditions de possibilité apparaît clairement, peut être étendu à un nombre pair quelconque de facteurs premiers $8n + 5$ combinés avec 2. Dans ce cas, en effet, les valeurs, qu'on pourra assigner au nombre que nous avons désigné par μ , contiendront toujours un nombre pair des facteurs premiers $8n + 5$, aussi bien pour les valeurs impaires de μ que pour les valeurs conjuguées de ces dernières. Dès lors les équations de condition (γ) du n° 31 seront impossibles en valeurs entières de h et de H' non-seulement dans le cas où les égalités symboliques (δ) seraient satisfaites, mais encore dans le cas où l'on changerait le signe du deuxième membre de ces égalités, ce qui donnerait les $\frac{m(m-1)}{2} - 1$ conditions :

$$(\delta') \quad \left\{ \begin{array}{l} \left(\frac{A}{C}\right) = \left(\frac{B}{C}\right) = -1, \\ \left(\frac{A}{D}\right) = \left(\frac{B}{D}\right) = \left(\frac{C}{D}\right) = -1, \\ \left(\frac{A}{E}\right) = \left(\frac{B}{E}\right) = \left(\frac{C}{E}\right) = \left(\frac{D}{E}\right) = -1, \\ \dots\dots\dots \\ \left(\frac{A}{L}\right) = \left(\frac{B}{L}\right) = \left(\frac{C}{L}\right) = \dots = \left(\frac{K}{L}\right) = -1. \end{array} \right.$$

Nous aurons ainsi la proposition suivante :

THÉORÈME. — L'équation $x^2 - 2ABCD...FKLy^2 = -1$, dont le déterminant contient un nombre pair de facteurs premiers $A, B, \dots, K, L$, de la forme $8n + 5$, est toujours possible en nombres entiers, lorsque les conditions suivantes sont remplies :

1° Si A et B ne sont pas compris dans les diviseurs linéaires de $t^2 - Cu^2$;

2° Si A, B et C ne sont pas compris dans les diviseurs linéaires de $t^2 - Du^2$;

.....

$(m - 2)^\circ$ Si $A, B, C, \dots, F, K$ ne sont pas compris dans les diviseurs linéaires de $t^2 - Lu^2$.

Il est facile de voir qu'il ne serait plus exact de dire, dans le cas du théorème qui vient d'être énoncé, que les équations, qui auraient pour déterminant le nombre 2 multiplié par une combinaison quelconque n à n des nombres premiers $8n + 5$ qui entrent dans l'équation primitive, seraient toujours possibles en nombres entiers. Cette proposition ne serait vraie que dans le cas de n pair. Pour fixer les idées, considérons l'équation

$$x^2 - 2.5.109.13.37y^2 = -1,$$

nous aurons les cinq égalités symboliques

$$\left(\frac{5}{13}\right) = \left(\frac{109}{13}\right) = -1, \quad \left(\frac{5}{37}\right) = \left(\frac{109}{37}\right) = \left(\frac{13}{37}\right) = -1,$$

qui permettent d'affirmer que cette équation admet toujours des solutions entières; si nous multiplions ensuite le facteur 2 successivement par les quatre combinaisons trois à trois des facteurs premiers $8n + 5$ qui entrent dans la même équation, les conditions déterminées (n° 29) ne seraient pas remplies pour les équations dont les déterminants seraient égaux aux nombres :

$$2.5.13.37, \quad 2.5.13.109, \quad 2.5.37.109, \quad 2.13.37.109.$$

Nous ne pourrions donc pas affirmer que ces équations admettraient des solutions entières; on peut constater d'ailleurs par une autre voie qu'aucune d'elles n'est soluble en nombres entiers. On reconnaît, par exemple, que la décomposition du déterminant $2.5.13.37$ en deux carrés ne peut s'effectuer que des quatre manières suivantes :

$$2.5.13.37 = 69^2 + 7^2 = 63^2 + 29^2 = 51^2 + 47^2 = 33^2 + 61^2,$$

et l'examen de ces carrés composants suffit (nos **8, 15, 16**) pour permettre d'affirmer que l'équation correspondante serait impossible en valeurs entières.

55. On ne peut pas dire que les théorèmes énoncés (nos **51** et **54**) comprennent tous les cas de possibilité en valeurs entières des équations auxquelles ils se rapportent. On a seulement démontré en effet que, si les égalités symboliques (δ) ou (δ') étaient satisfaites, les équations de condition (γ) ne pouvaient pas être vérifiées par des valeurs entières de h ou de H' . Mais la réciproque de cette proposition n'est nullement exacte. Pour compléter ce qui se rattache aux équations qui ne contiennent que des facteurs premiers $8n + 5$ combinés avec le nombre 2 dans le déterminant, nous serions donc conduits à rechercher tous les cas pour lesquels on peut affirmer, d'après les principes qui précèdent, que ces équations admettent forcément des valeurs entières.

Pour effectuer cette recherche, on ne saurait songer, pour une équation qui contiendrait m facteurs premiers $8n + 5$ dans son déterminant, à faire toutes les combinaisons possibles des signes des $\frac{m(m-1)}{2}$

quantités $\left(\frac{A}{B}\right)$, $\left(\frac{A}{C}\right)$, etc., et à examiner ensuite si, pour chaque série (δ) d'égalités symboliques, les équations de condition (γ) admettraient ou n'admettraient pas de valeurs entières pour h et H' . Le nombre de séries d'égalités symboliques serait en effet égal à $2^{\frac{m(m-1)}{2}}$, ou $2^{\frac{m(m-1)}{2} - 1}$, en ne fixant pas, comme il est souvent possible de le

faire, le signe de l'une des quantités $\left(\frac{A}{B}\right)$. Ce procédé serait imprati-

Pour l'équation (2),

$$(\alpha_2) \left\{ \begin{array}{ll} (\mu = \text{type AB}) & ABh^2 - 2C...KLPQH'^2 = \pm 1, \\ (\mu = \text{type ABCD}) & ABCDh^2 - 2C...KLPQH'^2 = \pm 1, \\ \dots\dots\dots & \dots\dots\dots \\ (\mu = \text{type 2AB}) & CD...PQh^2 - 2ABH'^2 = \pm 1. \end{array} \right.$$

Par hypothèse, les relations (α_1) relatives à l'équation (1) ne peuvent pas admettre de valeurs entières pour h et H' , et il faut démontrer que, les autres conditions de l'énoncé étant remplies, les relations (α_2) n'admettront pas non plus de valeurs entières pour les mêmes quantités.

Ces dernières relations se divisent en trois séries :

1° Celles qui ne contiennent ni P ni Q au coefficient de h^2 , relations qui reproduiront exactement les égalités (α_1) relatives à l'équation (1), avec cette seule différence que le produit PQ sera introduit au coefficient de H'^2 . Toutefois, dans ces relations qui ne contiennent ni P ni Q au coefficient de h^2 , on trouve encore la suivante, unique de son espèce :

$$(3_2) \quad ABC...KLh^2 - 2PQH'^2 = \pm 1.$$

2° Celles qui contiennent soit P soit Q au coefficient de h^2 .

3° Celles qui contiennent à la fois P et Q audit coefficient de h^2 , et qui sont analogues aux relations de la première série, puisqu'elles n'en diffèrent que par le déplacement du produit PQ d'un coefficient à l'autre.

Prouvons d'abord que les relations de la première série ne peuvent pas admettre de valeurs entières de h et de H' . En considérant l'une quelconque de ces relations :

$$(4_2) \quad AB...EFh^2 - 2C...KLPQH'^2 = \pm 1,$$

et en la rapprochant de la relation

$$(4_1) \quad AB...EFh^2 - 2C...KLH'^2 = \pm 1,$$

qui lui correspond dans les égalités (α_1) , nous observerons que, d'après l'énoncé, cette relation (4_1) ne peut pas admettre de valeurs entières

pour h et H' ; par suite, en désignant par M un facteur particulier du coefficient de H'^2 de cette dernière relation, et par N un coefficient particulier de h^2 , nous avons l'une ou l'autre des deux égalités

$$\left(\frac{AB...EF}{M}\right) = -1, \quad \left(\frac{2C...KL}{N}\right) = -1.$$

Dans le premier cas, la relation (4_2) ne peut pas admettre de valeurs entières pour h et H' ; dans le deuxième cas, nous remarquerons que, d'après les conditions (a) de l'énoncé, $\left(\frac{PQ}{N}\right) = 1$, d'où il résultera $\left(\frac{2C...KL PQ}{N}\right) = -1$. La relation (4_2) est donc toujours impossible en valeurs entières de h et de H' .

La relation (3_2) , qui se rattache à la même série, est aussi dans ce cas; nous aurons en effet, d'après l'énoncé, $\left(\frac{2PQ}{A}\right) = -1$.

Passons aux relations de la deuxième série, et considérons l'une quelconque d'entre elles :

$$(5_2) \quad AB...EFP h^2 - 2BC...KLQH'^2 = \pm 1.$$

Les facteurs premiers autres que P et Q , qui entrent dans les coefficients de h^2 et de H'^2 de cette dernière relation, sont en nombre impair (n° 31). Nous avons donc, d'après les conditions (a) :

$$\left(\frac{AB...EF}{Q}\right) = \left(\frac{A}{Q}\right), \quad \left(\frac{2BC...KL}{P}\right) = -\left(\frac{B}{P}\right) = -\left(\frac{A}{Q}\right).$$

d'où il résulte

$$\left(\frac{AB...EFP}{Q}\right) = \left(\frac{AP}{Q}\right), \quad \left(\frac{2BC...KLQ}{P}\right) = -\left(\frac{AP}{Q}\right).$$

Or, comme $\left(\frac{AP}{Q}\right) = \pm 1$, ces dernières inégalités prouvent que la relation (5_2) est impossible en valeurs entières de h et de H' .

Considérons enfin les relations de la troisième série, qui rentrent dans le type suivant :

$$(6_2) \quad AB...PQ h^2 - 2CD...KLH'^2 = \pm 1.$$

Les facteurs C, D, ..., K, L du coefficient de H'^2 sont évidemment en nombre pair, nous avons donc, en vertu des conditions (a),

$$\left(\frac{CD \dots KL}{P}\right) = 1, \quad \text{et par suite,} \quad \left(\frac{2CD \dots KL}{P}\right) = -1,$$

ce qui prouve que la relation (6₂) ne peut pas admettre de valeurs entières de h et de H' . Le théorème est donc démontré.

Pour démontrer que les relations de la première série sont impossibles en valeurs entières de h et de H' , nous nous sommes reportés aux relations correspondantes de l'équation (1) dont le déterminant contient deux facteurs premiers de moins. On pourrait se demander, par suite, si le théorème est applicable au cas de l'équation $x^2 - 2ABPQ\gamma^2 = -1$, pour lequel les relations (α_1) relatives à l'équation $x^2 - 2AB\gamma^2 = -1$ n'existent pas. Mais, sans entrer dans les détails de la question, il est facile de voir, en appliquant la marche suivie dans la démonstration précédente, que le théorème est aussi vrai dans ce cas particulier.

37. Réciproquement, on peut démontrer que si les conditions

$$(a) \quad \left(\frac{A}{P}\right) = \left(\frac{B}{P}\right) = \dots = \left(\frac{L}{P}\right) = \left(\frac{A}{Q}\right) = \left(\frac{B}{Q}\right) = \dots = \left(\frac{L}{Q}\right) = \pm 1$$

sont satisfaites, ce n'est qu'en réunissant ces conditions à un groupe d'égalités en vertu desquelles l'équation

$$(1) \quad x^2 - 2AB \dots KL\gamma^2 = -1$$

admettrait des valeurs entières, qu'on pourra établir que l'équation $x^2 - 2AB \dots KLPQ\gamma^2 = -1$ admet aussi des valeurs entières.

Reprenons la relation de la première série, considérée dans le numéro précédent, et rapprochons-la de celle qui lui correspond dans les relations (α_1) relatives à l'équation (1). Ces relations, déjà inscrites ci-dessus, sont :

$$(4_2) \quad AB \dots EFh^2 - 2C \dots KLPQH'^2 = \pm 1,$$

$$(4_1) \quad AB \dots EFh^2 - 2C \dots KLH'^2 = \pm 1.$$

Si les égalités qu'on doit grouper avec les conditions (a) n'expriment

pas que l'équation (1) admet des valeurs entières, nous ne pourrons pas établir, au moyen de ces égalités, que l'une des quantités

$$\left(\frac{AB \dots EF}{M}\right), \quad \text{ou} \quad \left(\frac{2C \dots KL}{N}\right),$$

dans lesquelles M et N désignent comme ci-dessus un facteur premier quelconque des coefficients de H'^2 et de h^2 de la relation (4₁), est égale à -1 . Mais comme, en vertu des conditions, (a) $\left(\frac{PQ}{N}\right) = 1$, il sera, par suite, également impossible d'établir que la relation (4₂) n'admet pas de valeurs entières pour h et H' . La réciproque est donc démontrée.

58. THÉORÈME. — *Si l'équation*

$$(1) \quad x^2 - 2AB \dots KLA_1 B_1 \dots K_1 L_1 y^2 = -1,$$

dans laquelle les facteurs premiers $8n+5$ sont en nombre pair dans chacune des deux séries $A, B, \dots, K, L$ et $A_1, B_1, \dots, K_1, L_1$, admet des solutions entières, il en sera de même de l'équation

$$(2) \quad x^2 - 2AB \dots KLA_1 B_1 \dots K_1 L_1 PQ y^2 = -1,$$

dans le cas où les facteurs premiers P et Q de la forme $8n+5$ satisfont aux conditions suivantes :

$$(a) \quad \begin{cases} \left(\frac{A}{P}\right) = \left(\frac{B}{P}\right) = \dots = \left(\frac{L}{P}\right) = \left(\frac{A}{Q}\right) = \left(\frac{B}{Q}\right) = \dots = \left(\frac{L}{Q}\right) = \pm 1, \\ \left(\frac{A_1}{P}\right) = \left(\frac{B_1}{P}\right) = \dots = \left(\frac{L_1}{P}\right) = \left(\frac{A_1}{Q}\right) = \left(\frac{B_1}{Q}\right) = \dots = \left(\frac{L_1}{Q}\right) = \mp 1. \end{cases}$$

Imaginons que l'on ait écrit, comme dans le théorème précédent, les équations de condition (α_1) et (α_2) relatives aux équations (1) et (2). Nous supposons, d'après l'énoncé, que les facteurs premiers, qui entrent dans le déterminant de l'équation (1), sont tels que les relations (α_1) ne peuvent pas admettre de valeurs entières pour h et H' , et il faut démontrer que, si les conditions (a) sont satisfaites, il en sera de même pour les relations (α_2).

Ces dernières relations étant divisées en trois séries analogues à celles que nous avons définies dans le théorème précédent, les relations de chaque série se ramènent aux types suivants :

$$\begin{aligned}
 1^{\text{re}} \text{ série } & \begin{cases} AB \dots KLA_1 B_1 \dots K_1 h^2 - 2 CD \dots C_1 D_1 \dots L_1 PQH'^2 = \pm 1 & (3_2), \\ AB \dots KLA_1 B_1 \dots K_1 L_1 h^2 - 2 PQH'^2 = \pm 1 & (4_2), \end{cases} \\
 2^{\text{e}} \text{ série } & \begin{cases} AB \dots LA_1 B_1 \dots K_1 P h^2 - 2 CD \dots KC_1 D_1 \dots L_1 QH'^2 = \pm 1 & (5_2), \\ AB \dots LA_1 B_1 \dots K_1 Q h^2 - 2 CD \dots KC_1 D_1 \dots L_1 PH'^2 = \pm 1 & (6_2), \end{cases} \\
 3^{\text{e}} \text{ série } & \begin{cases} AB \dots LA_1 B_1 \dots K_1 PQ h^2 - 2 CD \dots KC_1 D_1 \dots L_1 H'^2 = \pm 1 & (7_2), \\ PQ h^2 - 2 AB \dots KLA_1 B_1 \dots K_1 L_1 H'^2 = \pm 1 & (8_2). \end{cases}
 \end{aligned}$$

Établissons d'abord que les relations de la première série ne peuvent pas admettre de valeurs entières pour h et H' . D'après les conditions (α), nous avons pour tout facteur premier N qui entre dans le déterminant de l'équation (1) $\left(\frac{PQ}{N}\right) = 1$, et partant $\left(\frac{2PQ}{N}\right) = -1$, ce qui prouve que la relation (4₂) est impossible en valeurs entières de h et de H' . Il en est de même de la relation (3₂); car, en rapprochant l'une quelconque des relations de ce type (3₂) de celle qui lui correspond dans les relations (α_1) ou (3₁), nous aurons, en conservant à M et à N la signification définie au théorème précédent, l'une des égalités suivantes :

$$\left(\frac{AB \dots KLA_1 B_1 \dots K_1}{M}\right) = -1, \quad \left(\frac{2CD \dots C_1 D_1 L_1}{N}\right) = -1.$$

Ainsi, comme nous venons de voir que $\left(\frac{PQ}{N}\right) = 1$, il en résulte que l'ensemble des relations (3₂) est impossible en valeurs entières de h et de H' .

Considérons maintenant les relations de la deuxième série; dans le type (5₂), les facteurs $A, B, \dots, L$, qui entrent dans le coefficient de h^2 , seront en nombre pair ou impair, mais, quel que soit le cas qui se présente, le nombre des facteurs $C, D, \dots, K$, qui entrent dans le coefficient de H'^2 , sera de même parité; de même, les chiffres qui représentent le nombre de facteurs $A_1, B_1, \dots, K_1$ qui entrent dans le coefficient de h^2 d'une part, et le nombre de facteurs $C_1, D_1, \dots, L_1$ qui entrent dans

le coefficient de H'^2 d'autre part, seront tous les deux pairs ou tous les deux impairs. Nous aurons donc, en vertu des conditions (a), les deux égalités,

$$\left(\frac{AB \dots L}{Q}\right) = \left(\frac{CD \dots K}{P}\right), \quad \left(\frac{A_1 B_1 \dots K_1}{Q}\right) = \left(\frac{C_1 D_1 \dots L_1}{P}\right);$$

en rapprochant ces deux égalités de la suivante $\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right)$ et multipliant membre à membre les trois égalités, nous aurons finalement

$$\left(\frac{AB \dots LA_1 B_1 \dots K_1 P}{Q}\right) = \left(\frac{CD \dots KC_1 D_1 \dots L_1 Q}{P}\right),$$

ce qui prouve, en tenant compte de l'égalité $\left(\frac{2}{p}\right) = -1$, que l'une quelconque des relations représentées par le type (5₂) est impossible en valeurs entières de h et de H' . La même démonstration est applicable aux relations (6₂), et elle s'appliquerait aussi, avec une légère modification, au cas où l'un des coefficients de h^2 ou de H'^2 ne contiendrait pas de facteurs premiers de l'une des séries $A, B, \dots, L$ ou $A_1, B_1, \dots, L_1$.

Examinons enfin les relations de la troisième série, et commençons par la relation (8₂), qui est unique de son espèce. Les facteurs premiers $A, B, \dots, K, L$ entrent en nombre pair dans le coefficient de H'^2 , et les facteurs $A_1, B_1, \dots, K_1, L_1$ sont dans le même cas; nous avons donc, en vertu des conditions (a),

$$\left(\frac{AB \dots KL}{P}\right) = 1, \quad \left(\frac{A_1 B_1 \dots K_1 L_1}{P}\right) = 1,$$

ce qui nous donne l'égalité $\left(\frac{2AB \dots KLA_1 B_1 \dots K_1 L_1}{P}\right) = -1$, qui prouve que la relation (8₂) est impossible en valeurs entières de h et de H' .

En ce qui concerne les relations de cette troisième série dont le type est représenté par l'égalité (7₂) inscrite ci-dessus, considérons le type (7₁) qui lui correspond dans les relations (a₁)

$$(7_1) \quad AB \dots LA_1 B_1 \dots K_1 h^2 - 2CD \dots KC_1 D_1 - L_1 H'^2 = \pm 1$$

et observons que, puisque l'équation (1) est soluble en nombres entiers,

cette relation (7₁) n'admet pas de valeurs entières pour h et H' . Nous avons donc l'une des égalités suivantes :

$$\left(\frac{AB \dots LA_1 B_1 \dots K_1}{M}\right) = -1, \quad \left(\frac{2CD \dots KC_1 D_1 \dots L_1}{N}\right) = -1;$$

mais, en vertu des conditions (a), $\left(\frac{PQ}{M}\right) = 1$. Les relations de la troisième série dont le type est représenté par l'égalité (7₂) sont donc impossibles en valeurs entières de h et H' , ce qui démontre le théorème.

59. Remarque. — Dans le cas où les signes des seconds membres des conditions (a) sont différents, il est essentiel que les facteurs premiers $A, B, \dots, K, L$ et $A_1, B_1, K_1, \dots, L_1$ soient en nombre pair dans chacune des séries. Dans la démonstration on s'est en effet appuyé sur cette condition; mais, pour ne laisser aucun doute à cet égard, partons de l'équation

$$(1) \quad x^2 - 2AA_1 y^2 = -1,$$

et essayons d'établir la possibilité de l'équation

$$(2) \quad x^2 - 2AA_1 PQ y^2 = -1$$

dans le cas suivant :

$$(a) \quad \left(\frac{A}{P}\right) = \left(\frac{A}{Q}\right) = 1, \quad \left(\frac{A_1}{P}\right) = \left(\frac{A_1}{Q}\right) = -1;$$

parmi les six équations de condition (α_2) relatives à l'équation (2), nous trouverons la suivante :

$$PQ h^2 - 2AA_1 H'^2 = \pm 1.$$

Or, d'après les conditions (a), $\left(\frac{PQ}{A}\right) = 1$, $\left(\frac{PQ}{A_1}\right) = 1$, $\left(\frac{2AA_1}{P}\right) = 1$, $\left(\frac{2AA_1}{Q}\right) = 1$, il serait donc impossible d'établir que la relation, qui vient d'être inscrite, n'admet pas de valeurs entières pour h et H' , et par

suite de prouver que l'équation (2) admet toujours des valeurs entières pour x et y . On arriverait à la même conséquence dans le cas où les conditions (a) seraient remplacées par les suivantes :

$$(a_1) \quad \left(\frac{A}{P}\right) = \left(\frac{A}{Q}\right) = -1, \quad \left(\frac{A_1}{P}\right) = \left(\frac{A_1}{Q}\right) = 1.$$

Ainsi, on ne peut rien conclure sur la possibilité en valeurs entières de l'équation $x^2 - 2AA_1PQy^2 = -1$, dans le cas où les conditions (a) ou (a₁) sont remplies. Mais il est facile de voir que cette conséquence a une portée plus générale. Entrons dans quelques détails.

40. Lorsque les conditions (a), inscrites dans les énoncés des théorèmes (n^{os} 36 et 38), sont satisfaites, ces théorèmes permettent de rattacher les conditions de possibilité en valeurs entières de l'équation

$$(2) \quad x^2 - 2AB \dots KLA_1B_1 \dots K_1L_1PQy^2 = -1$$

à celles de l'équation analogue (1), qui ne contient pas le produit PQ dans son déterminant.

En examinant dans les énoncés de ces théorèmes les conditions (a), on constate qu'elles rentrent dans les suivantes :

$$\left(\frac{PQ}{A}\right) = \left(\frac{PQ}{B}\right) = \dots = \left(\frac{PQ}{L}\right) = \left(\frac{PQ}{A_1}\right) = \left(\frac{PQ}{B_1}\right) = \dots = \left(\frac{PQ}{L_1}\right) = 1,$$

les quantités $\left(\frac{P}{A}\right), \left(\frac{Q}{A}\right), \left(\frac{P}{B}\right), \left(\frac{Q}{B}\right), \dots$, étant toutes égales à +1 ou à -1 dans le théorème (n^o 36), tandis que dans le théorème (n^o 38), lorsque le signe des seconds membres des égalités (a) n'est pas le même, c'est-à-dire pour le cas où ce théorème diffère en réalité du théorème (n^o 36), les quantités $\left(\frac{P}{A}\right)$ et $\left(\frac{Q}{A}\right)$, relatives à un facteur premier quelconque du déterminant de l'équation (1), sont bien toujours de même signe, mais ce signe commun n'est plus le même que le signe des quantités $\left(\frac{P}{A_1}\right)$ et $\left(\frac{Q}{A_1}\right)$.

Cela posé, lorsque les deux séries A, B, ..., L et A₁, B₁, ..., L₁, considérées dans le théorème (n^o 38), contiennent chacune un nombre pair

de termes, conformément à la condition posée dans l'énoncé, on prouverait, en suivant la marche indiquée (n° 37), que réciproquement ce ne serait qu'en réunissant les conditions (a) à un groupe d'égalités (δ_i), en vertu duquel l'équation (1) serait possible en valeurs entières, qu'on pourrait établir que l'équation (2) admettrait aussi des solutions de même nature. Pour la recherche indiquée (n° 35), il suffira donc, relativement à l'équation (2), dans le cas où les égalités (a) seraient remplies, de grouper ces égalités (a) des théorèmes (nos 36 et 38) avec les égalités qui expriment la possibilité de l'équation (1) en valeurs entières, sans s'inquiéter des autres permutations de signes qu'on pourrait faire subir aux quantités $\left(\frac{A}{B}\right)$, $\left(\frac{A}{C}\right)$, ..., provenant des combinaisons deux à deux des facteurs premiers qui entrent dans le déterminant de l'équation (1).

De plus, et c'est là l'extension de la conséquence constatée à la fin de la remarque précédente, si les deux séries A, B, ..., L et $A_1, B_1, \dots, L_1$ renferment chacune un nombre impair de termes, contrairement à ce qu'on a supposé (n° 38), et si les conditions

$$(a) \begin{cases} \left(\frac{A}{P}\right) = \left(\frac{B}{P}\right) = \dots = \left(\frac{L}{P}\right) = \left(\frac{A}{Q}\right) = \left(\frac{B}{Q}\right) = \dots = \left(\frac{L}{Q}\right) = +1 \text{ ou } -1 \\ \left(\frac{A_1}{P}\right) = \left(\frac{B_1}{P}\right) = \dots = \left(\frac{L_1}{P}\right) = \left(\frac{A}{Q}\right) = \left(\frac{B}{Q}\right) = \dots = \left(\frac{L}{Q}\right) = -1 \text{ ou } +1 \end{cases}$$

sont remplies, on peut démontrer qu'il ne sera pas possible de rien affirmer sur la possibilité de l'équation (2) en valeurs entières, soit que l'équation (1) admette des solutions de même nature, soit qu'elle n'en admette pas.

Parmi les équations de condition (α_2), relatives à l'équation (2), nous aurons, en effet, la suivante :

$$(r) \quad PQh^2 - 2AB \dots KLA_1B_1 \dots K_1L_1H'^2 = \pm 1;$$

pour un facteur quelconque M du coefficient de H'^2 , nous aurions $\left(\frac{PQ}{M}\right) = 1$, en vertu des conditions (a). En outre, comme les facteurs premiers des deux séries, A, B, ..., L et $A_1, B_1, \dots, L_1$ sont en nombre

impair dans chacune d'elles, nous avons, d'après les conditions (a),

$$\left(\frac{AB \dots KL}{P}\right) = \left(\frac{A}{P}\right), \quad \left(\frac{A_1 B_1 \dots K_1 L_1}{P}\right) = \left(\frac{A_1}{P}\right);$$

par suite,

$$\left(\frac{AB \dots KLA_1 B_1 \dots K_1 L_1}{P}\right) = \left(\frac{AA_1}{P}\right) = -1,$$

ce qui prouve, eu égard à la symétrie qui existe entre P et Q, que la relation (r) peut admettre des valeurs entières pour h et H' , ou, en d'autres termes, qu'on ne peut pas affirmer que l'équation (2) admet, dans ce cas, des solutions entières.

Sans entrer dans d'autres détails, nous arrivons ainsi à la conséquence suivante : Lorsque pour une équation (1), qui contient un nombre pair de facteurs premiers $8n + 5$ combinés avec le nombre 2 dans son déterminant, on a obtenu toutes les séries d'égalités symboliques (∂_1) pour lesquelles on peut affirmer que l'équation considérée admet des solutions entières, les considérations précédentes permettent d'établir sans tâtonnement toutes les séries d'égalités symboliques (∂_2) pour lesquelles on peut affirmer que l'équation (2), qui contient deux facteurs premiers de plus de la forme $8n + 5$ dans son déterminant, admet aussi des valeurs entières pour le cas où les conditions suivantes, relatives aux deux nouveaux facteurs P et Q, sont remplies, savoir :

$$\left(\frac{PQ}{A}\right) = \left(\frac{PQ}{B}\right) = \dots = \left(\frac{PQ}{L}\right) = \left(\frac{PQ}{A_1}\right) = \left(\frac{PQ}{B_1}\right) = \dots = \left(\frac{PQ}{L_1}\right) = 1.$$

41. En conservant les notations précédentes, recherchons les conséquences auxquelles on peut arriver lorsque les quantités $\left(\frac{PQ}{A}\right)$, $\left(\frac{PQ}{B}\right)$, etc. sont toutes négatives, et supposons d'abord que les facteurs premiers, qui entrent dans le déterminant de l'équation (1), se partagent en deux séries A, B, ..., K, L et A_1 , B_1 , ..., K_1 , L_1 composées chacune d'un nombre pair de termes, et pour lesquelles on aurait les

conditions

$$(a) \quad \begin{cases} \left(\frac{A}{P}\right) = \left(\frac{B}{P}\right) = \dots = \left(\frac{L}{P}\right) = \left(\frac{A_1}{Q}\right) = \left(\frac{B_1}{Q}\right) = \dots = \left(\frac{L_1}{Q}\right) = \pm 1, \\ \left(\frac{A}{Q}\right) = \left(\frac{B}{Q}\right) = \dots = \left(\frac{L}{Q}\right) = \left(\frac{A_1}{P}\right) = \left(\frac{B_1}{P}\right) = \dots = \left(\frac{L_1}{P}\right) = \mp 1; \end{cases}$$

dans ces égalités, les signes supérieurs des seconds membres marchent ensemble, ainsi que les signes inférieurs, à cause des conditions $\left(\frac{PQ}{A}\right) = -1$, $\left(\frac{PQ}{B}\right) = -1$, etc.

Cela posé, dans les relations (α_2) , relatives à l'équation

$$(2) \quad x^2 - 2AB \dots KLA_1 B_1 \dots K_1 L_1 y^2 = -1,$$

nous trouverions la suivante :

$$(r) \quad AB \dots KLA_1 B_1 \dots K_1 L_1 h^2 - 2PQH'^2 = \pm 1.$$

Or, pour un facteur quelconque M qui entre dans le coefficient de h^2 , nous aurons l'égalité $\left(\frac{2PQ}{M}\right) = 1$. De plus, comme les facteurs de chacune des séries A, B, ..., K, L et $A_1, B_1, \dots, K_1, L_1$ entrent par hypothèse en nombre pair dans le déterminant de l'équation (1) à laquelle nous rattachons l'équation (2), nous aurons

$$\left(\frac{AB \dots KLA_1 B_1 \dots K_1 L_1}{P}\right) = \left(\frac{AB \dots KLA_1 B_1 \dots K_1 L_1}{Q}\right) = 1;$$

la relation (r) peut donc admettre des valeurs entières pour h et H' . Ainsi, dans les conditions où l'on s'est placé, on ne peut pas se prononcer sur la possibilité de l'équation (2) en valeurs entières de x et de y . Pour fixer les idées, partons de l'équation $x^2 - 2AB y^2 = -1$, et supposons que les facteurs premiers P et Q de la forme $8n + 5$, comme cela a lieu pour les nombres premiers A et B, satisfassent aux conditions suivantes :

$$(a_1) \quad \left(\frac{A}{P}\right) = \left(\frac{B}{P}\right) = 1, \quad \left(\frac{A}{Q}\right) = \left(\frac{B}{Q}\right) = -1;$$

on ne pourrait pas se prononcer sur la possibilité en valeurs entières de x et de y pour l'équation $x^2 - 2ABPQy^2 = -1$, et cette conséquence est indépendante de la nature des signes des expressions $\left(\frac{A}{B}\right)$ et $\left(\frac{C}{D}\right)$. On arriverait aussi à la même conséquence, en permutant les signes des seconds membres des égalités (a_1) .

(La suite prochainement.)

