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

P. TCHEBICHEF

Sur les formes quadratiques

Journal de mathématiques pures et appliquées 1re série, tome 16 (1851), p. 257-282.
<http://www.numdam.org/item?id=JMPA_1851_1_16__257_0>

SUR LES FORMES QUADRATIQUES;

PAR M. P. TCHEBICHEF.

I.

Euler nous a déjà donné plusieurs exemples du parti que l'on peut tirer de la représentation des nombres par des formes quadratiques à déterminants négatifs pour reconnaître s'ils sont premiers ou non. Je vais, à présent, montrer que, dans ces recherches, on peut aussi bien se servir de certaines formes à déterminants positifs, ce qui est nécessaire pour rendre cette méthode tout à fait générale et même avantageuse pour des nombres d'une grandeur considérable. En effet, quand on se borne seulement aux formes quadratiques à déterminants négatifs, les différents nombres exigent l'emploi de plusieurs différentes formes, et chacune d'elles demande des procédés particuliers pour trouver facilement la représentation du nombre donné. De plus, le nombre de ces formes propres à distinguer le cas d'un nombre premier de celui d'un nombre composé étant limité, on peut rencontrer des nombres qui ne peuvent prendre aucune de ces formes. On écarterait toutes ces difficultés si l'on pouvait considérer les nombres d'après leur représentation par des formes quadratiques à déterminants positifs; car alors, pour embrasser tous les cas possibles, il suffira d'un petit nombre de formes convenablement choisies, telles que, par exemple,

$$x^2+y^2, \quad x^2+2y^2, \quad x^2-2y^2,$$

ou

$$x^2+y^2, \quad x^2+3y^2, \quad 3y^2-x^2; \quad \text{etc.}$$

D'ailleurs il ne sera pas difficile, en traitant chacune d'elles, de construire des tables qui faciliteront considérablement ces recherches.

La totalité des représentations du nombre N par la forme Ax^2+By^2

étant limitée, on distingue le cas de N premier de celui où il est composé, en cherchant le nombre de résolutions de l'équation

$$Ax^2 + By^2 = N.$$

Nous verrons que la même chose a lieu par rapport à l'équation

$$x^2 - Dy^2 = \pm N,$$

si parmi ses solutions, qui sont en nombre infini, on ne compte que celles où x et y ne surpassent pas certaines limites, ce qui revient à ne compter que le nombre de certains groupes que présentent toutes les solutions possibles de l'équation

$$x^2 - Dy^2 = \pm N.$$

II.

Soient α, β les plus petites valeurs de x, y qui, étant au-dessus de zéro, vérifient l'équation

$$x^2 - Dy^2 = 1,$$

et a, b des nombres positifs qui vérifient celle-ci,

$$x^2 - Dy^2 = \pm N.$$

Par la multiplication des équations

$$\alpha^2 - D\beta^2 = 1, \quad a^2 - Db^2 = \pm N,$$

nous trouvons

$$(a\alpha - b\beta D)^2 - D(a\beta - b\alpha)^2 = \pm N,$$

ce qui prouve que les nombres

$$x = \pm(a\alpha - b\beta D), \quad y = \pm(a\beta - b\alpha),$$

vérifient aussi l'équation

$$x^2 - Dy^2 = \pm N.$$

De cette manière, on pourra toujours passer d'une solution de l'équation

$$x^2 - Dy^2 = \pm N$$

à une autre, et, par conséquent, trouver plusieurs valeurs de x et de y qui la vérifient. Examinons maintenant dans quel cas les nombres

positifs x, y, donnés par les formules

$$(1) \qquad x = \pm (a\alpha - b\beta D), \quad y = \pm (a\beta - b\alpha),$$

seront plus petits que les nombres a et b dont on est parti. Dans ces recherches, il faut faire attention aux signes $\pm$ qu'on doit prendre dans les formules (1) pour rendre x, y positifs, et pour cela nous traiterons séparément deux cas,

$$x^2 - Dy^2 = N, \quad x^2 - Dy^2 = -N.$$

Dans le premier cas, nous aurons

$$a^2 - Db^2 = N,$$

ce qui donne

$$a = \sqrt{Db^2 + N};$$

de plus, d'après l'équation

$$\alpha^2 - D\beta^2 = 1,$$

on trouve

$$\alpha = \sqrt{D\beta^2 + 1}.$$

En mettant ces valeurs de a et α dans l'équation

$$x = \pm (a\alpha - b\beta D),$$

on obtient

$$x = \pm (\sqrt{Db^2 + N} \cdot \sqrt{D\beta^2 + 1} - b\beta D),$$

d'où il est clair que x sera positif quand on prendra la formule $\pm (a\alpha - b\beta D)$ avec le signe $+$. Mais, pour que cette valeur de $x = a\alpha - b\beta D$ soit plus petite que a, et, par conséquent, y plus petit que b, nous trouvons cette condition

$$a\alpha - b\beta D < a.$$

Cette inégalité donne

$$\frac{b\beta D}{a} > \alpha - 1, \quad \frac{b^2\beta^2 D^2}{a^2} > (\alpha - 1)^2,$$

et, en y mettant les valeurs de b et β tirées des équations

$$a^2 - Db^2 = N, \quad \alpha^2 - D\beta^2 = 1,$$

nous trouverons

$$\frac{(\alpha^2 - 1)(a^2 - N)}{a^2} > (\alpha - 1)^2,$$

et, par conséquent,

$$a > \sqrt{\frac{(\alpha+1)N}{2}}.$$

Donc les nouvelles valeurs de x et y seront toujours plus petites que celles dont on part si la valeur de x surpasse $\sqrt{\frac{(\alpha+1)N}{2}}$; par conséquent, en tirant à l'aide des formules (1) successivement d'une solution de l'équation

$$x^2 - Dy^2 = N$$

une autre, on parviendra nécessairement à de telles valeurs de x et y que la première ne surpasse pas $\sqrt{\frac{(\alpha+1)N}{2}}$. Quant à la limite de la valeur de y, nous la trouvons égale à $\sqrt{\frac{(\alpha+1)N}{2D}}$; car, pour

$$x = \sqrt{\frac{(\alpha+1)N}{2}},$$

l'équation

$$x^2 - Dy^2 = N$$

donne

$$y = \sqrt{\frac{(\alpha-1)N}{2D}}.$$

De cette manière se trouve établi le théorème suivant :

THÉORÈME. *Si l'équation*

$$x^2 - Dy^2 = N$$

est possible, on trouvera dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha+1)N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha-1)N}{2D}}$$

des valeurs entières de x et y qui la vérifient, $x = \alpha$ étant la plus petite solution, supérieure à l'unité, de l'équation

$$x^2 - Dy^2 = 1.$$

En passant au cas de

$$x^2 - Dy^2 = -N,$$

nous remarquons que, d'après les équations

$$a^2 - Db^2 = -N, \quad \alpha^2 - D\beta^2 = 1,$$

on aura

$$a = \sqrt{Db^2 - N}, \quad \alpha = \sqrt{D\beta^2 + 1},$$

et, par conséquent, la valeur de

$$y = \pm (a\beta - b\alpha)$$

pourra être mise sous cette forme,

$$y = \pm (\beta\sqrt{Db^2 + N} - b\sqrt{D\beta^2 + 1}),$$

ou, ce qui revient au même,

$$y = \pm \frac{\beta^2(Db^2 - N) - b^2(D\beta^2 + 1)}{\beta\sqrt{Db^2 - N} + b\sqrt{D\beta^2 + 1}} = \pm \frac{-\beta^2 N - b^2}{\beta\sqrt{Db^2 - N} + b\sqrt{D\beta^2 + 1}}.$$

De là nous concluons que y est positif quand on prend la formule $\pm(a\beta - b\alpha)$ avec le signe $-$, et que, par conséquent, pour rendre y inférieur à b, nous devons vérifier cette condition

$$-(a\beta - b\alpha) < b.$$

Cette inégalité donne

$$\alpha - 1 < \frac{a\beta}{b}, \quad (\alpha - 1)^2 < \frac{a^2\beta^2}{b^2},$$

et, en y mettant les valeurs de a^2 et β^2 d'après les équations

$$a^2 - Db^2 = -N, \quad \alpha^2 - D\beta^2 = 1,$$

nous trouvons

$$(\alpha - 1)^2 < \frac{(Db^2 - N)(\alpha^2 - 1)}{Db^2},$$

ce qui donne définitivement

$$b > \sqrt{\frac{(\alpha + 1)N}{2D}}.$$

Donc, toutes les fois que, dans la solution connue de l'équation

$$x^2 - Dy^2 = -N,$$

la valeur de y surpasse $\sqrt{\frac{(\alpha+1)N}{2D}}$, on pourra en tirer, à l'aide des formules (1), une solution plus simple, et, par conséquent, on par-

viendra nécessairement à une solution telle que y ne surpassera pas $\sqrt{\frac{(\alpha+1)N}{2D}}$; cela suppose, d'après l'équation

$$x^2 - Dy^2 = -N,$$

que x ne dépassera pas la limite $\sqrt{\frac{(\alpha-1)N}{2}}$. De cette manière nous parvenons à ce théorème :

THÉORÈME. *Si l'équation*

$$x^2 - Dy^2 = -N$$

est possible, on trouvera dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha-1)N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha+1)N}{2D}},$$

des valeurs entières de x et y qui la vérifient, $x = \alpha$ étant la plus petite solution, supérieure à l'unité, de l'équation

$$x^2 - Dy^2 = 1.$$

III.

Les limites entre lesquelles, d'après les théorèmes qui viennent d'être démontrés, on est sûr de trouver des nombres x et y qui vérifient l'équation

$$x^2 - Dy^2 = \pm N$$

quand elle est possible, jouissent de cette propriété remarquable :

Si $x = a$, $y = b$, $x = a_1$, $y = b_1$ sont deux systèmes de valeurs de x et y qui ne surpassent pas les limites trouvées plus haut et vérifient l'une des équations

$$x^2 - Dy^2 = N, \quad x^2 - Dy^2 = -N,$$

les nombres $ab_1 + a_1 b$, $ab_1 - a_1 b$ ne seront pas divisibles par N, tandis que leur produit $(ab_1 + a_1 b)(ab_1 - a_1 b)$ sera un multiple de N.

Pour établir cette propriété, observons d'abord que le produit des

deux équations

$$a^2 - Db^2 = \pm N, \quad a_1^2 - Db_1^2 = \pm N,$$

peut être mis sous la forme

$$(aa_1 \pm Dbb_1)^2 - D(ab_1 \pm a_1 b)^2 = N^2.$$

Cela posé, si nous admettons que $ab_1 \pm a_1 b$ pris avec l'un des signes + ou − soit divisible par N, le nombre $aa_1 \pm Dbb_1$ pris avec le même signe devra nécessairement, d'après l'équation précédente, être également divisible par N; on aurait donc, dans cette hypothèse,

$$\left(\frac{aa_1 \pm Dbb_1}{N}\right)^2 - D\left(\frac{ab_1 \pm a_1 b}{N}\right)^2 = 1,$$

$\frac{aa_1 \pm Dbb_1}{N}$, $\frac{ab_1 \pm a_1 b}{N}$ étant des nombres entiers. Mais, comme nous supposons que α est la plus petite valeur de x, autre que l'unité, satisfaisant à l'équation

$$x^2 - Dy^2 = 1,$$

la formule précédente se trouvera être impossible si l'on établit l'inégalité

$$\left(\frac{aa_1 \pm Dbb_1}{N}\right)^2 < \alpha^2.$$

Or nous allons démontrer que ceci a toujours lieu quand on prend pour a et a_1 des nombres qui ne surpassent pas $\sqrt{\frac{(\alpha \pm 1)N}{2}}$, et pour b, b_1 des valeurs non au-dessus de $\sqrt{\frac{(\alpha \mp 1)N}{2D}}$. (Les signes supérieurs se rapportent au cas de $x^2 - Dy^2 = N$, et les signes inférieurs à celui de $x^2 - Dy^2 = -N$.) Pour prouver notre assertion, nous remarquerons que, a et a_1 étant compris entre les limites o et $\sqrt{\frac{(\alpha \pm 1)N}{2}}$, b et b_1 entre o et $\sqrt{\frac{(\alpha \mp 1)N}{2D}}$, la valeur de $\left(\frac{aa_1 \pm Dbb_1}{N}\right)^2$ ne pourra surpasser celle qu'on trouverait en admettant le signe + dans la formule, et en y supposant de plus

$$a = a_1 = \sqrt{\frac{(\alpha \pm 1)N}{2}}, \quad b = b_1 = \sqrt{\frac{(\alpha \mp 1)N}{2D}}.$$

Or, comme dans cette hypothèse la valeur de $\left(\frac{aa_1 \pm Dbb_1}{N}\right)^2$ se réduit à α^2, nous en concluons que, dans les limites données plus haut, le *maximum* de $\left(\frac{aa_1 \pm Dbb_1}{N}\right)^2$ est α^2, et que ce *maximum* n'a lieu que pour $a = a_1$, $b = b_1$. Donc, dans le cas que nous examinons, où a et b sont différents de a_1, b_1, on aura nécessairement

$$\left(\frac{aa_1 \pm Dbb_1}{N}\right)^2 < \alpha^2,$$

ce qu'il s'agissait de démontrer.

Nous venons donc d'établir qu'aucun des deux nombres $ab_1 + a_1 b$, $ab_1 - a_1 b$ n'est divisible par N. Quant à leur produit

$$(ab_1 + a_1 b)(ab_1 - a_1 b) = a^2 b_1^2 - a_1^2 b^2,$$

il est évidemment divisible par N; en effet, en substituant dans la formule $a^2 b_1^2 - a_1^2 b^2$ les valeurs de a^2, a_1^2, tirées des équations

$$a^2 - Db^2 = \pm N, \quad a_1^2 - Db_1^2 = \pm N,$$

nous trouvons de suite

$$a^2 b_1^2 - a_1^2 b^2 = \pm (b_1^2 - b^2) N.$$

Donc, si a, a_1, b, b_1 sont des valeurs entières de x et de y comprises dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha \pm 1)N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha \mp 1)N}{2D}},$$

et qui vérifient l'équation

$$x^2 - Dy^2 = \pm N,$$

on trouvera nécessairement deux diviseurs de N en cherchant les facteurs communs à N et aux nombres $ab_1 + a_1 b$, $ab_1 - a_1 b$. De là nous tirons ce théorème :

THÉORÈME. *Si l'équation*

$$x^2 - Dy^2 = \pm N,$$

dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha \pm 1)N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha \pm 1)N}{2D}}.$$

peut être vérifiée par deux systèmes différents de valeurs de x et y, le nombre N *est composé.*

Quant à α, ce nombre a ici la même signification que dans les théorèmes précédents.

IV.

D'après les théorèmes que nous venons de prouver, la représentation du nombre N par la formule $\pm(x^2 - Dy^2)$ nous conduit à reconnaître que N est un nombre composé dans les deux cas suivants :

1°. Si, N étant de la forme des diviseurs linéaires de $x^2 - Dy^2$ susceptibles d'être représentés par la forme $\pm(x^2 - Dy^2)$, on ne trouve pas dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha \pm 1)N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha \mp 1)N}{2D}},$$

des valeurs entières de x, y qui rendent l'expression $\pm(x^2 - Dy^2)$ égale à N; car alors, d'après l'un des deux premiers théorèmes, l'équation

$$\pm(x^2 - Dy^2) = N$$

sera impossible, et ceci n'aura lieu que pour N composé;

2°. Si, dans ces limites, on trouve deux représentations différentes du nombre N; d'après le dernier théorème, ceci suppose que N est composé.

Donc, le nombre N ne peut être premier que dans le cas où l'équation

$$x^2 - Dy^2 = \pm N,$$

dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha \pm 1)N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha \mp 1)N}{2D}},$$

n'a qu'une seule solution dans laquelle évidemment x doit être premier à y et à D. Mais toutes les fois que ceci a lieu, peut-on en conclure que le nombre N soit nécessairement premier ?

En examinant sous ce rapport les formes

$$= x^2 - Dy^2,$$

nous remarquons qu'elles se divisent en deux espèces. Les unes, dans les limites énoncées et x étant premier à y et à D, ne donnent une seule représentation de N que dans le cas où ce nombre est premier; telles sont, par exemple, les formes

$$\pm(x^2 - 2y^2), \quad \pm(x^2 - 3y^2), \quad \pm(x^2 - 5y^2), \quad \text{etc.}$$

Les autres, au contraire, donnent une seule représentation non-seulement pour des nombres premiers, mais aussi pour plusieurs nombres composés quand on prend les nombres x, y dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha \pm 1)N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha \mp 1)N}{2D}},$$

x étant premier à y et à D. Par exemple, en cherchant la représentation du nombre composé 371 par la forme $x^2 - 37y^2$, nous trouvons que les limites de x et de y sont

$$x = 0, \quad x = \sqrt{\frac{(73+1).371}{2}}; \quad y = 0, \quad y = \sqrt{\frac{(73-1).371}{2.73}};$$

car la solution la plus simple de l'équation

$$x^2 - 37y^2 = 1$$

est la suivante :

$$x = 73, \quad y = 12.$$

Or, dans ces limites, nous observons que l'équation

$$x^2 - 37y^2 = 371$$

ne peut être vérifiée qu'en prenant

$$x = 36, \quad y = 5.$$

Nous ne donnerons pas ici une méthode générale pour distinguer à laquelle des deux espèces appartient une formule donnée $\pm(x^2 - Dy^2)$, comme Euler l'a fait par rapport aux formes $Ax^2 + By^2$; nous nous bornerons quant à présent à assigner plusieurs formes de la première espèce, qu'on reconnaît très-aisément.

V.

Nous avons vu, dans le § II, que si l'équation

$$x^2 - Dy^2 = \pm N$$

est possible, on trouvera au moins une solution dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha \pm 1)N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha \mp 1)N}{2D}}.$$

Nous allons démontrer maintenant que, dans ces limites, l'équation

$$x^2 - Dy^2 = \pm N$$

aura au moins deux solutions si, étant susceptible d'être vérifiée par

$$x = l, \quad y = m, \quad x = l', \quad y = m',$$

les nombres $lm' + l'm$, $lm' - l'm$ ne sont pas divisibles par N.

Pour parvenir à cette conclusion, nous remarquons d'abord qu'en général, si x, y, X, Y vérifient l'équation

$$x^2 - Dy^2 = \pm N,$$

et que les nombres $xY + yX$, $xY - yX$ ne soient pas divisibles par N, la même chose aura lieu quand on aura remplacé x, y par les nombres x_1, y_1 tirés des équations

$$(2) \qquad x_1 = \pm(\alpha x - \beta y D), \quad y_1 = \pm(\beta x - \alpha y),$$

dont nous nous sommes servi dans le § II. En effet, nous avons prouvé dans ce paragraphe que les valeurs de x_1, y_1, déterminées par les formules (2), vérifieront l'équation

$$x_1^2 - Dy_1^2 = \pm N,$$

et comme

$$X^2 - DY^2 = \pm N,$$

nous trouverons

$$(x_1^2 - Dy_1^2)(X^2 - DY^2) = N^2,$$

ou bien, ce qui revient au même,

$$(x_1 X \pm y_1 Y)^2 - D(x_1 Y \pm y_1 X)^2 = N^2;$$

de là il est clair que si $x_1 Y \pm y_1 X$, pris avec l'un des deux signes $\pm$, était divisible par N, le nombre $x_1 X \pm D y_1 Y$, pris avec le même signe, serait également divisible par N. Mais cela ne peut avoir lieu; pour le faire voir, observons que $xY + yX$, $xY - yX$, d'après les formules (2), peuvent être mis sous la forme

$$\pm (x_1 Y \pm y_1 X)\alpha \pm \beta (x_1 X \pm y_1 YD).$$

Or, si les nombres $x_1 Y \pm y_1 X$, $x_1 X \pm y_1 YD$, pris avec l'un des deux signes $\pm$, étaient divisibles par N, il s'ensuivrait aussi qu'un des nombres $xY + yX$, $xY - yX$ serait également divisible par N, ce qui n'est pas. Donc aussi les nombres $x_1 Y + y_1 X$, $x_1 Y - y_1 X$ ne pourront pas être divisibles par N.

D'après cela, nous concluons que si les nombres $lm' + l'm$, $lm' - l'm$ ne sont pas divisibles par N, et que $x = a$, $y = b$ soit une solution de l'équation

$$x^2 - Dy^2 = \pm N$$

dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha \pm 1)N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha \mp 1)N}{2D}},$$

qu'on trouve, d'après le § II, en partant de $x = l$, $y = m$, et en passant successivement d'une solution à une autre à l'aide des équations (2), les nombres $am' + bl'$ de même ne seront pas divisibles par N. De la même manière nous conclurons que si a_1, b_1 est une solution de l'équation

$$x^2 - Dy^2 = \pm N,$$

dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha \pm 1)N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha \mp 1)N}{2D}},$$

qu'on trouvera en partant de $x = l'$, $y = m'$, on ne rendra pas les nombres $am' + bl'$, $am' - bl'$ divisibles par N, en remplaçant l', m' par a_1, b_1. Mais ceci suppose évidemment que les nombres a_1, b_1 ne sont pas respectivement égaux aux nombres a, b; car, autrement, $am' - bl'$ se réduisant à

$$ab - ba = 0,$$

deviendrait divisible par N. Donc, dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha \pm 1)N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha \mp 1)N}{2D}},$$

on trouvera nécessairement deux solutions de l'équation

$$x^2 - Dy^2 = \pm N,$$

si elle est susceptible d'être vérifiée par deux systèmes de valeurs

$$x = l, \quad y = m, \quad x = l', \quad y = m',$$

et que les nombres $lm' + l'm$, $lm' - l'm$ ne soient pas divisibles par N.

VI.

D'après ce que nous venons de prouver, nous allons montrer que toutes les formes $\pm(x^2 - Dy^2)$, dont les diviseurs quadratiques ne sont que de la forme $\lambda x^2 - \mu y^2$, peuvent servir pour examiner si un nombre donné est premier ou non.

THÉORÈME. *Soient $x^2 - Dy^2$ une forme dont les diviseurs quadratiques ne sont que de la forme $\lambda x^2 - \mu y^2$, N un nombre premier par rapport à D et de la forme des diviseurs linéaires contenus dans une seule forme quadratique $\pm(x^2 - Dy^2)$. Le nombre N sera premier si, α étant la plus petite valeur de x supérieure à l'unité parmi les solutions de l'équation*

$$x^2 - Dy^2 = 1,$$

on trouve, dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha \pm 1)N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha \mp 1)N}{2D}},$$

une seule représentation du nombre N par la forme $\pm(x^2 - Dy^2)$, et que, dans cette représentation, x et y n'aient point de facteur commun. Dans tous les autres cas le nombre N sera composé.

Démonstration. Pour établir le théorème énoncé, nous allons faire voir que lorsque N est un nombre composé, l'un des trois cas suivants aura nécessairement lieu :

1°. On ne trouvera pas de représentation du nombre N par la forme

$\pm (x^2 - Dy^2)$ dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha \pm 1)N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha \mp 1)N}{2D}};$$

2°. On trouvera dans ces limites une représentation de N pour laquelle x, y ne seront pas premiers entre eux;

3°. On trouvera dans ces limites plusieurs représentations du nombre N.

Si parmi les facteurs du nombre N on trouve des nombres qui ne soient pas diviseurs de $x^2 - Dy^2$, l'équation

$$x^2 - Dy^2 = \pm N$$

ne sera pas possible, à moins que ces facteurs ne divisent x^2 et y^2. Donc, dans ce cas, ou bien la représentation du nombre N par la forme $\pm (x^2 - Dy^2)$ sera impossible, ou bien dans la représentation du nombre N les nombres x et y ne seront pas premiers entre eux.

En passant au cas où tous les facteurs de N sont diviseurs de $x^2 - Dy^2$, supposons que

$$N = N_1 . N_2.$$

Tous les diviseurs quadratiques de $x^2 - Dy^2$ étant, par supposition, de la forme $\lambda x^2 - \mu y^2$, nous concluons que les nombres N_1, N_2 pourront être représentés ainsi :

$$(3) \qquad N_1 = \lambda_1 x_1^2 - \mu_1 y_1^2, \quad N_2 = \lambda_2 x_2^2 - \mu_2 y_2^2,$$

et comme leur produit N est de la forme $\pm (x^2 - Dy^2)$, on trouvera

$$\lambda_2 = \lambda_1, \quad \mu_2 = \mu_1$$

dans le cas de

$$N = x^2 - Dy^2,$$

et

$$\lambda_2 = -\lambda_1, \quad \mu_2 = -\mu_1$$

dans le cas de

$$N = -(x^2 - Dy^2).$$

Donc

$$N_1 N_2 = \pm (\lambda_1 x_1^2 - \mu_1 y_1^2)(\lambda_1 x_2^2 - \mu_1 y_2^2),$$

ou bien, ce qui revient au même,

$$N_1 N_2 = \pm [(\lambda_1 x_1 x_2 \pm \mu_1 y_1 y_2)^2 - \lambda_1 \mu_1 (x_1 y_2 \pm y_1 x_2)^2].$$

D'après cette équation et en remarquant que

$$N_1 N_2 = N, \quad \lambda_1 \mu_1 = D,$$

nous concluons que l'équation

$$x^2 - D y^2 = \pm N$$

sera vérifiée par deux systèmes de valeurs de x, y,

$$(4) \qquad \begin{cases} X = \lambda_1 x_1 x_2 + \mu_1 y_1 y_2, & X_1 = \lambda_1 x_1 x_2 - \mu_1 y_1 y_2, \\ Y = x_1 y_2 + y_1 x_2, & Y_1 = x_1 y_2 - y_1 x_2. \end{cases}$$

En cherchant, d'après ces formules, les valeurs de $XY_1 + YX_1$, $XY_1 - YX_1$, nous trouvons

$$\begin{aligned} XY_1 + YX_1 &= (\lambda_1 x_1 x_2 + \mu_1 y_1 y_2)(x_1 y_2 - y_1 x_2) \\ &\quad + (\lambda_1 x_1 x_2 - \mu_1 y_1 y_2)(x_1 y_2 + y_1 x_2) \\ &= 2 x_2 y_2 (\lambda_1 x_1^2 - \mu_1 y_1^2) = 2 x_2 y_2 N_1, \\ XY_1 - YX_1 &= (\lambda_1 x_1 x_2 + \mu_1 y_1 y_2)(x_1 y_2 - y_1 x_2) \\ &\quad - (\lambda_1 x_1 x_2 - \mu_1 y_1 y_2)(x_1 y_2 + y_1 x_2) \\ &= 2 x_1 y_1 (\lambda_1 x_2^2 - \mu_1 y_2^2) = \pm 2 x_1 y_1 N_2. \end{aligned}$$

D'où il est clair que si $x_1 y_1$ est premier par rapport à N_1, et $x_2 y_2$ est premier par rapport à N_2, les nombres $XY_1 + YX_1$, $XY_1 - YX_1$ ne seront pas divisibles par

$$N = N_1 N_2,$$

ce qui, d'après le § V, suppose deux solutions de l'équation

$$x^2 - D y^2 = \pm N,$$

dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha \pm 1) N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha \mp 1) N}{2D}}.$$

Quant au cas où $x_1 y_1$ aurait un commun diviseur avec N_1, ou bien $x_2 y_2$ avec N_2, il n'est pas difficile de s'assurer que les solutions (4)

de l'équation

$$x^2 - Dy^2 = \pm N$$

ainsi que toutes les autres qu'on en pourrait tirer à l'aide des formules (2), contiendront des valeurs de x, y divisibles par un même nombre.

C'est ainsi que nous nous convainquons que, dans les suppositions énoncées plus haut, on ne trouvera jamais un nombre composé N qui puisse avoir, dans les limites

$$x = 0, \quad x = \sqrt{\frac{(\alpha \pm 1)N}{2}}, \quad y = 0, \quad y = \sqrt{\frac{(\alpha \mp 1)N}{2D}},$$

une seule représentation par la forme $\pm(x^2 - Dy^2)$, pour des nombres x, y premiers entre eux. Donc ceci ne peut avoir lieu que pour N premier; dans le cas contraire, d'après ce que nous avons vu dans le § V, on conclura que N est composé.

VII.

C'est de cette manière qu'on pourra reconnaître la nature d'un nombre donné d'après sa représentation par la forme quadratique $x^2 - Dy^2$ ou $-(x^2 - Dy^2)$ si tous les diviseurs quadratiques de $x^2 - Dy^2$ sont de la forme $\lambda x^2 - \mu y^2$. Nous allons maintenant présenter une Table de ces formes les plus simples, avec les limites de x, y, déterminées par les formules

$$x = \sqrt{\frac{(\alpha \pm 1)N}{2}}, \quad y = \sqrt{\frac{(\alpha \mp 1)N}{2D}},$$

ainsi que des formes linéaires des nombres qui peuvent être examinés au moyen de ces formes.

FORMES quadratiques de N.	LIMITES DE x, y.	FORMES LINÉAIRES DE N.
x^2-2y^2	$x=\sqrt{2\mathrm{N}},\quad y=\sqrt{\frac{\mathrm{N}}{2}}$	$\mathrm{N}=8n+1,\ 7$
$-(x^2-2y^2)$	$x=\sqrt{\mathrm{N}},\quad y=\sqrt{\mathrm{N}}$	
x^2-3y^2	$x=\sqrt{\frac{3}{2}\mathrm{N}},\quad y=\sqrt{\frac{\mathrm{N}}{6}}$	$\mathrm{N}=12n+1$
$-(x^2-3y^2)$	$x=\sqrt{\frac{1}{2}\mathrm{N}},\quad y=\sqrt{\frac{1}{2}\mathrm{N}}$	$\mathrm{N}=12n+11$
x^2-5y^2	$x=\sqrt{5\mathrm{N}},\quad y=\sqrt{\frac{4}{5}\mathrm{N}}$	$\mathrm{N}=20n+1,\ 9,\ 11,\ 19$
$-(x^2-5y^2)$	$x=\sqrt{4\mathrm{N}},\quad y=\sqrt{\mathrm{N}}$	
x^2-6y^2	$x=\sqrt{3\mathrm{N}},\quad y=\sqrt{\frac{\mathrm{N}}{3}}$	$\mathrm{N}=24n+1,\ 19$
$-(x^2-6y^2)$	$x=\sqrt{2\mathrm{N}},\quad y=\sqrt{\frac{1}{2}\mathrm{N}}$	$\mathrm{N}=24n+5,\ 23$
x^2-7y^2	$x=\sqrt{\frac{9}{2}\mathrm{N}},\quad y=\sqrt{\frac{1}{2}\mathrm{N}}$	$\mathrm{N}=28n+1,\ 9,\ 25$
$-(x^2-7y^2)$	$x=\sqrt{\frac{7}{2}\mathrm{N}},\quad y=\sqrt{\frac{9}{14}\mathrm{N}}$	$\mathrm{N}=28n+3,\ 19,\ 27$
x^2-10y^2	$x=\sqrt{10\mathrm{N}},\quad y=\sqrt{\frac{9}{10}\mathrm{N}}$	$\mathrm{N}=40n+1,\ 9,\ 31,\ 39$
$-(x^2-10y^2)$	$x=\sqrt{9\mathrm{N}},\quad y=\sqrt{\mathrm{N}}$	
x^2-11y^2	$x=\sqrt{\frac{11}{2}\mathrm{N}},\quad y=\sqrt{\frac{9}{22}\mathrm{N}}$	$\mathrm{N}=44n+1,\ 5,\ 9,\ 27$
$-(x^2-11y^2)$	$x=\sqrt{\frac{9}{2}\mathrm{N}},\quad y=\sqrt{\frac{1}{2}\mathrm{N}}$	$\mathrm{N}=44n+3,\ 19,\ 35,\ 39,\ 43$
x^2-13y^2	$x=\sqrt{325\,\mathrm{N}},\quad y=\sqrt{\frac{324}{13}\mathrm{N}}$	$\mathrm{N}=52n+\begin{cases}1,\ 3,\ 9,\ 17,\ 23,\ 25,\ 27,\ 29,\ 35,\\ 43,\ 49,\ 51\end{cases}$
$-(x^2-13y^2)$	$x=\sqrt{324\,\mathrm{N}},\quad y=\sqrt{25\,\mathrm{N}}$	
x^2-14y^2	$x=\sqrt{8\mathrm{N}},\quad y=\sqrt{\frac{1}{2}\mathrm{N}}$	$\mathrm{N}=56n+1,\ 9,\ 11,\ 25,\ 43,\ 51$
$-(x^2-14y^2)$	$x=\sqrt{7\mathrm{N}},\quad y=\sqrt{\frac{8}{7}\mathrm{N}}$	$\mathrm{N}=56n+5,\ 13,\ 31,\ 45,\ 47,\ 55$
x^2-15y^2	$x=\sqrt{\frac{5}{2}\mathrm{N}},\quad y=\sqrt{\frac{1}{10}\mathrm{N}}$	$\mathrm{N}=60n+1,\ 49$
$-(x^2-15y^2)$	$x=\sqrt{\frac{3}{2}\mathrm{N}},\quad y=\sqrt{\frac{1}{6}\mathrm{N}}$	$\mathrm{N}=60n+11,\ 59$

FORMES quadratiques de N.	LIMITES DE x, y.	FORMES LINÉAIRES DE N.
x^2-17y^2	$x=\sqrt{17\,\mathrm{N}}$, $y=\sqrt{\frac{16}{17}\mathrm{N}}$	$\mathrm{N}=68n+\begin{cases}1,\ 9,\ 13,\ 15,\ 19,\ 21,\ 25,\ 33,\ 35,\\ 43,\ 47,\ 49,\ 53,\ 55,\ 59,\ 67\end{cases}$
$-(x^2-17y^2)$	$x=\sqrt{16\,\mathrm{N}}$, $y=\sqrt{\mathrm{N}}$	
x^2-19y^2	$x=\sqrt{\frac{171}{2}\mathrm{N}}$, $y=\sqrt{\frac{169}{38}\mathrm{N}}$	$\mathrm{N}=76n+1,\ 5\ 9,\ 17,\ 25,\ 45,\ 49,\ 61,\ 73$
$-(x^2-19y^2)$	$x=\sqrt{\frac{169}{2}\mathrm{N}}$, $y=\sqrt{\frac{171}{38}\mathrm{N}}$	$\mathrm{N}=76n+3,\ 15,\ 27,\ 31,\ 51,\ 59,\ 67,\ 71,\ 75$
x^2-21y^2	$x=\sqrt{28\,\mathrm{N}}$, $y=\sqrt{\frac{9}{7}\mathrm{N}}$	$\mathrm{N}=84n+1,\ 25,\ 37,\ 43,\ 67,\ 79$
$-(x^2-21y^2)$	$x=\sqrt{27\,\mathrm{N}}$, $y=\sqrt{\frac{4}{3}\mathrm{N}}$	$\mathrm{N}=84n+5,\ 17,\ 41,\ 47,\ 59,\ 83$
x^2-22y^2	$x=\sqrt{99\,\mathrm{N}}$, $y=\sqrt{\frac{49}{11}\mathrm{N}}$	$\mathrm{N}=88n+1,\ 3,\ 9,\ 25,\ 27,\ 49,\ 59,\ 67,\ 75,\ 81$
$-(x^2-22y^2)$	$x=\sqrt{98\,\mathrm{N}}$, $y=\sqrt{\frac{9}{2}\mathrm{N}}$	$\mathrm{N}=88n+7,\ 13,\ 21,\ 29,\ 39,\ 61,\ 63,\ 79,\ 85,\ 87$
x^2-23y^2	$x=\sqrt{\frac{25}{2}\mathrm{N}}$, $y=\sqrt{\frac{1}{2}\mathrm{N}}$	$\mathrm{N}=92n+1,\ 9,\ 13,\ 25,\ 29,\ 41,\ 49,\ 73,\ 77,\ 81,\ 85$
$-(x^2-23y^2)$	$x=\sqrt{\frac{23}{2}\mathrm{N}}$, $y=\sqrt{\frac{25}{46}\mathrm{N}}$	$\mathrm{N}=92n+7,\ 11,\ 15,\ 19,\ 43,\ 51,\ 63,\ 67,\ 79,\ 83,\ 91$
x^2-26y^2	$x=\sqrt{26\,\mathrm{N}}$, $y=\sqrt{\frac{25}{26}\mathrm{N}}$	$\mathrm{N}=104n+\begin{cases}1,\ 9,\ 17,\ 23,\ 25,\ 49,\ 55,\ 79,\ 81,\\ 87,\ 95,\ 103\end{cases}$
$-(x^2-26y^2)$	$x=\sqrt{25\,\mathrm{N}}$, $y=\sqrt{\mathrm{N}}$	$\mathrm{N}=104n+\begin{cases}5,\ 11,\ 19,\ 21,\ 37,\ 45,\ 59,\ 67,\ 83,\\ 85,\ 93,\ 99\end{cases}$
x^2-29y^2	$x=\sqrt{4901\,\mathrm{N}}$, $y=\sqrt{\frac{4900}{29}\mathrm{N}}$	$\mathrm{N}=116n+\begin{cases}1,\ 3,\ 7,\ 9,\ 13,\ 23,\ 25,\ 35,\ 45,\\ 49,\ 51,\ 53,\ 57,\ 59,\ 63,\ 65,\ 67,\\ 71,\ 81,\ 83,\ 91,\ 93,\ 103,\ 107,\\ 109,\ 111,\ 115\end{cases}$
$-(x^2-29y^2)$	$x=\sqrt{4900\,\mathrm{N}}$, $y=\sqrt{\frac{4901}{29}\mathrm{N}}$	
x^2-30y^2	$x=\sqrt{6\,\mathrm{N}}$, $y=\sqrt{\frac{1}{6}\mathrm{N}}$	$\mathrm{N}=120n+1,\ 19,\ 49,\ 91$
$-(x^2-30y^2)$	$x=\sqrt{5\,\mathrm{N}}$, $y=\sqrt{\frac{1}{5}\mathrm{N}}$	$\mathrm{N}=120n+29,\ 71\ 101,\ 119$
x^2-31y^2	$x=\sqrt{\frac{1521}{2}\mathrm{N}}$, $y=\sqrt{\frac{1519}{62}\mathrm{N}}$	$\mathrm{N}=124n+\begin{cases}1,\ 5,\ 9,\ 25,\ 35,\ 41,\ 43,\ 45,\ 49,\\ 69,\ 81,\ 97,\ 101,\ 109,\ 103,\ 121\end{cases}$
$-(x^2-31y^2)$	$x=\sqrt{\frac{1519}{2}\mathrm{N}}$, $y=\sqrt{\frac{1521}{62}\mathrm{N}}$	$\mathrm{N}=124n+\begin{cases}3,\ 11,\ 15,\ 23,\ 27,\ 43,\ 55,\ 75,\ 79,\\ 83,\ 91,\ 99,\ 115,\ 119,\ 123\end{cases}$
x^2-33y^2	$x=\sqrt{12\,\mathrm{N}}$, $y=\sqrt{\frac{1}{3}\mathrm{N}}$	$\mathrm{N}=132n+\begin{cases}1,\ 25,\ 31,\ 37,\ 49,\ 67,\ 91,\ 97,\\ 103,\ 115\end{cases}$
$-(x^2-33y^2)$	$x=\sqrt{11\,\mathrm{N}}$, $y=\sqrt{\frac{4}{11}\mathrm{N}}$	$\mathrm{N}=132n+\begin{cases}17,\ 29,\ 35,\ 41,\ 65,\ 83,\ 95,\ 101,\\ 107,\ 131\end{cases}$

VIII.

D'après ce que nous venons de trouver, on voit qu'il y a plusieurs formes à déterminants positifs dont on peut se servir pour examiner si un nombre donné est premier ou non. Quant aux limites de x, y, dans lesquelles on doit chercher la représentation du nombre examiné par la forme $\pm(x^2 - Dy^2)$, elles ne sont pas toujours plus étendues que celles qu'on trouve par rapport à la forme $x^2 + Dy^2$. Ainsi, d'après la Table précédente, on voit qu'en cherchant la représentation du nombre N par la forme $3y^2 - x^2$, on ne doit pas aller au delà de $y = \sqrt{\frac{N}{2}}$, et, comme y ne peut pas être évidemment plus petit que $\sqrt{\frac{N}{3}}$, on cherchera la valeur de y entre les limites $\sqrt{\frac{N}{3}}$, $\sqrt{\frac{N}{2}}$. De la même manière nous apercevons que, pour trouver la représentation du nombre N par la forme $x^2 - 3y^2$, on cherchera y entre les limites $\sqrt{N}$, $\sqrt{\frac{3}{2}N}$; pour la forme $x^2 - 2y^2$, ces limites sont $\sqrt{N}$, $\sqrt{2N}$, etc.

Nous allons maintenant montrer par un exemple qu'à l'aide de la forme $\pm(x^2 - Dy^2)$, convenablement choisie, il n'est pas difficile d'examiner si un nombre donné est premier ou non, même quand ce nombre est considérable. Nous choisissons le nombre 8520191; Legendre (*voyez* sa *Théorie des Nombres*, tome II, page 152), en cherchant deux nombres A et B, tels que chacun d'eux soit égal à la somme des diviseurs de l'autre, celui-ci non compris, a trouvé que

$$A = 2^8 . 520191, \quad B = 2^8 . 257 . 33023$$

vérifieront cette condition si le nombre 8520191 est premier. Mais jusqu'à présent on ne sait si ce nombre est premier ou non.

En remarquant que le nombre 8520191 est de la forme $12n + 11$, et que tous les nombres premiers de cette forme peuvent être représentés par $3y^2 - x^2$, nous allons chercher la représentation de 8520191 par la formule $3y^2 - x^2$. D'après le procédé exposé plus haut, nous

allons chercher la valeur y entre les limites

$$\sqrt{\frac{8520191}{3}}, \quad \sqrt{\frac{8520191}{3}},$$

c'est-à-dire entre les limites

$$1685, \quad 2065.$$

Pour que la forme $3y^2 - x^2$ représente un nombre impair, on prendra x impair et y pair, ou bien x pair et y impair. En faisant, dans le premier cas,

$$x = 2n + 1, \quad y = 2n,$$

nous trouvons que $3y^2 - x^2$ se réduit à

$$12n_1 - 8\frac{n(n+1)}{2} - 1,$$

ce qui ne peut être égal à 8520191, qui est de la forme $8m - 1$ si n_1 est impair. Donc

$$n_1 = 2l,$$

et, par conséquent, on aura, dans le premier cas,

$$y = 4l.$$

En passant au cas de x pair et y impair, faisons

$$x = 2n, \quad y = 2n_1 + 1.$$

Pour ces valeurs de x, y la forme $3y^2 - x^2$ devient

$$3 + 24\frac{n_1(n_1+1)}{2} - 4n^2,$$

et, en égalant cette quantité à 8520191, nous trouvons l'équation

$$3 + 24\frac{n_1(n_1+1)}{2} - 4n^2 = 8520191.$$

Or, comme cette équation se réduit à

$$6\frac{n_1(n_1+1)}{2} - n^2 = 2130047,$$

nous en concluons que n est impair.

Faisant donc

$$n = 2m + 1,$$

l'équation précédente devient

$$6\frac{n_1(n_1+1)}{2} - 8\frac{m(m+1)}{2} - 1 = 2130047,$$

et, par conséquent,

$$3\frac{n_1(n_1+1)}{2} - 4\frac{m(m+1)}{2} = 1060024,$$

ce qui suppose la divisibilité du nombre $\frac{n_1(n_1+1)}{2}$ par 4. Mais, pour que $\frac{n_1(n_1+1)}{2}$ soit divisible par 4, un des deux nombres n_1, n_1+1 doit être multiple de 8. Donc on aura

$$\text{ou} \quad n_1 = 8l' \quad \text{ou} \quad n_1 = 8l - 1.$$

En prenant la première valeur de n_1, nous trouvons

$$y = 16l' + 1,$$

et la seconde donne

$$y = 16l'' - 1.$$

Ainsi y ne peut être que de l'une de ces formes :

$$y = 4l, \quad y = 16l' + 1, \quad y = 16l' - 1.$$

De même, il n'est pas difficile de trouver les nombres auxquels y peut être congru suivant différents modules, et ensuite, au moyen de ces nombres, de trouver toutes les formes possibles de l, l', l''. Ainsi nous trouvons que pour

$$N = 5m + 1 = 7m' + 1 = 10m' + 9 = 13m''' + 4 = 17m^{IV} + 12,$$

ce qui est justement le cas de

$$N = 8520191,$$

l'équation

$$3y^2 - x^2 = N$$

suppose

$$y \equiv 0, \pm 2 \pmod 5,$$
$$y \equiv \pm 1, \pm 2 \pmod 7,$$
$$y \equiv \pm 1, \pm 2, 5 \pmod{11},$$
$$y \equiv 0, \pm 1, \pm 3, \pm 6 \pmod{13},$$
$$y \equiv \pm 1, \pm 2, \pm 3, \pm 4, \pm 7 \pmod{17}.$$

De là il est facile de conclure que les nombres l, l', l'', liés à y par les équations

$$y = 4l, \quad y = 16l' + 1, \quad y = 16l'' - 1$$

doivent avoir les formes :

$l = 5n + 0, 2, 3$	$l' = 5n + 1, 2, 4$	$l'' = 5n + 1, 3, 4$
$l = 7n + 2, 3, 4, 5$	$l' = 7n + 0, 2, 4, 6$	$l'' = 7n + 0, 1, 3, 5$
$l = 11n + 3, 4, 5, 6, 7, 8$	$l' = 11n + 0, 1, 3, 4, 6, 9$	$l'' = 11n + 0, 2, 5, 7, 8, 10$
$l = 13n + \begin{cases} 0, 3, 4, 5, 8, 9, \\ 10 \end{cases}$	$l' = 13n + \begin{cases} 0, 2, 3, 4, 5, \\ 6, 8 \end{cases}$	$l'' = 13n + \begin{cases} 0, 5, 7, 8, 9, 10, \\ 11 \end{cases}$
$l = 17n + \begin{cases} 1, 4, 5, 6, 8, 9, \\ 11, 12, 13, 16 \end{cases}$	$l' = 17n + \begin{cases} 0, 2, 3, 4, 5, 8, \\ 11, 14, 15, 16 \end{cases}$	$l'' = 17n + \begin{cases} 0, 1, 2, 3, 6, 9, \\ 12, 13, 14, 15 \end{cases}$

D'après ces formes de l, l', l'', il est très-facile de trouver toutes les solutions de l'équation

$$3y^2 - x^2 = 8520191$$

dans les limites

$$y > 1685, \quad y < 2065.$$

Dans le cas de

$$y = 4l,$$

nous trouvons que l doit être compris dans les limites 421 et 516. Si l'on prend, dans ces limites, tous les nombres de la forme

$$13n + 0, 3, 4, 5, 8, 9, 10,$$

et qu'on rejette, d'après l'équation

$$l = 5n + 0, 2, 3,$$

tous les nombres dont le dernier chiffre est 1, 4, 6, 9, on ne trouvera

que ces trente nombres :

425,	442,	455,	468,	485,	503,
432,	445,	458,	472,	490,	507,
433,	447,	460,	473,	497,	570,
437,	450,	463,	477,	498,	512,
438,	452,	465,	478,	502,	515.

D'après l'équation

$$l = 7n + 2,\ 3,\ 4,\ 5,$$

on supprimera de cette Table tous les nombres qui, divisés par 7, donnent des restes égaux à 0, 1, 4, 6, et l'on n'aura alors qu'à examiner dix-huit nombres parmi lesquels on reconnaîtra très-aisément ceux qui, divisés par 11, ne donnent pas les restes 3, 4, 5, 6, 7, 8; tous ces nombres, d'après l'équation

$$l = 11n + 3,\ 4,\ 5,\ 6,\ 7,\ 8,$$

doivent aussi être rejetés; alors il ne restera que les huit nombres suivants :

425,	437,	458,	478,
432,	445,	465,	502.

De plus, divisant ces nombres par 17, nous n'en trouverons que quatre :

$$437,\ 458,\ 465,\ 502,$$

qui s'accordent avec les formes

$$l = 17n + 1,\ 4,\ 5,\ 6,\ 8,\ 9,\ 11,\ 12,\ 13,\ 16;$$

d'ailleurs, comme ces nombres conduisent à des valeurs de y qui ne vérifient pas l'équation

$$3y^2 - x^2 = 8520191,$$

nous en concluons que, dans les limites énoncées plus haut, cette équation n'a point de solution pour laquelle y serait de la forme $4l$.

En passant au cas de

$$y = 16l' + 1,$$

nous trouvons que les limites de l' sont 105 et 129, et que, dans ces limites, les nombres de la forme

$$13n + 0,\ 2,\ 3,\ 4,\ 5,\ 6,\ 8,$$

qui, s'accordant avec les suivantes :

$$l' = 5n + 1,\ 2,\ 4,$$

se terminent par 1, 2, 4, 6, 7, 9, sont

$$106,\quad 109,\quad 117,\quad 121,$$
$$107,\quad 112,\quad 119,\quad 122.$$

En rejetant de là, d'après l'équation

$$l' = 7n + 0,\ 2,\ 4,\ 6,$$

tous les nombres qui, divisés par 7, donnent des restes différents de 0, 2, 4, 6, et, de plus, tous les nombres qui ne sont pas de l'une des formes

$$11n + 0,\ 1,\ 3,\ 4,\ 6,\ 9,$$

il ne reste que les deux suivants :

$$119,\quad 121.$$

En cherchant, d'après ces valeurs de l', celles de

$$y = 16l' + 1,$$

en substituant ces valeurs dans l'équation

$$3y^2 - x^2 = 8520191,$$

nous trouvons que la seconde donne

$$y = 1937,$$

qui vérifie l'équation

$$3y^2 - x^2 = 8520191,$$

en prenant

$$x = 1654.$$

Quant au dernier cas, c'est-à-dire celui de

$$y = 16l'' - 1,$$

nous trouvons 105 et 129 pour limites de l''; dans ces limites, d'après les équations

$$l'' = 13n + 0,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,$$
$$l'' = 5n + 1,\ 3,\ 4,$$

nous aurons les nombres suivants :

$$109,\quad 113,\quad 123,\quad 126,$$
$$111,\quad 114,\quad 124,\quad 128,$$

dont il ne restera qu'un seul,

$$126,$$

quand on aura rejeté tous les nombres qui ne s'accordent pas avec les formes

$$l'' = 7n + 0,\ 1,\ 3,\ 5,\quad l'' = 11n + 0,\ 2,\ 5,\ 7,\ 8,\ 10,$$

et comme le nombre 126 est de la forme

$$17n + 7,$$

et, par conséquent, ne s'accorde pas avec les formules

$$l'' = 17n + 0,\ 1,\ 2,\ 3,\ 6,\ 9,\ 12,\ 13,\ 14,\ 15,$$

nous concluons que ce nombre doit aussi être supprimé.

Ainsi nous ne trouvons qu'une seule représentation du nombre 8520191 par la forme $3y^2 - x^2$, en prenant y non supérieur à $\sqrt{\frac{8520191}{2}}$, et comme, dans cette représentation, les valeurs de x et y, nommément 1654 et 1937, n'ont point de commun diviseur, nous en concluons avec certitude que 8520191 est un nombre premier.

La méthode qui nous a servi à l'examen du nombre 8520191 à l'aide de la forme $3y^2 - x^2$ peut être étendue à tous les nombres, en faisant usage de certaines formes quadratiques. Ces recherches, comme on a pu le remarquer d'après l'exemple précédent, pourraient devenir très-expéditives, même pour des nombres considérables, si

l'on avait des Tables des solutions de la congruence

$$Ax^2 \pm By^2 \equiv C \pmod{p},$$

pour les valeurs les plus simples de p, telles que

$$p = 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29.$$

Ces Tables seraient peu nombreuses si l'on se servait des formes à déterminants négatifs et en même temps de celles à déterminants positifs, car alors on n'aurait pas besoin de recourir à plusieurs formes différentes. Ainsi, par exemple, on pourra examiner tous les nombres au moyen de ces trois formes

$$x^2 + y^2,\quad x^2 + 2y^2,\quad x^2 - 2y^2.$$

La première servira pour examiner tous les nombres de la forme

$$8n + 1,\ 5;$$

la seconde pourra être employée dans le cas du nombre

$$8n + 3;$$

et enfin la dernière pour ceux qui sont de la forme

$$8n + 7.$$

On verrait de la même manière que tous les cas possibles pourraient également être traités au moyen de ces trois formes

$$x^2 + y^2,\quad x^2 + 3y^2,\quad 3y^2 - x^2.$$