NOUVELLES ANNALES DE MATHÉMATIQUES

E. DE JONQUIÈRES

Étude sur les décompositions en sommes de deux carrés, du carré d'un nombre entier composé de facteurs premiers de la forme $4n+1$, et de ce nombre lui-même. Formules et application à la résolution complète, en nombres entiers, des équations indéterminées, simultanées, $y = x^2 + (x+1)^2$ et $y^2 = z^2 + (z+1)^2$ (fin)

Nouvelles annales de mathématiques 2e série, tome 17 (1878), p. 289-310

<http://www.numdam.org/item?id=NAM_1878_2_17__289_0>

ÉTUDE SUR LES DÉCOMPOSITIONS EN SOMMES DE DEUX CARRÉS, DU CARRÉ D'UN NOMBRE ENTIER COMPOSÉ DE FACTEURS PREMIERS DE LA FORME $4n+1$, ET DE CE NOMBRE LUI-MÊME.

FORMULES ET APPLICATION A LA RÉSOLUTION COMPLÈTE, EN NOMBRES ENTIERS, DES ÉQUATIONS INDÉTERMINÉES, SIMULTANÉES, $y = x^2 + (x+1)^2$ ET $y^2 = z^2 + (z+1)^2$;

[FIN (*).]

PAR M. E. DE JONQUIÈRES.

V. Actuellement, pour passer du système de valeurs de x et de y qu'on vient d'écrire à un autre système du même groupe (E_n) qui nous occupe, il suffit de changer dans l'expression de x, et en même temps dans celle de y, le signe du produit $a_1 b_1$; on obtient ainsi un deuxième système de valeurs. Pour en obtenir un troisième, il suffit de changer le signe du produit $a_2 b_2$ dans les mêmes expressions de x et y, et ainsi de suite pour les suivants. On obtient donc d'abord, en procédant de la sorte, autant de systèmes nouveaux de valeurs de x et de y qu'il y a de produits tels que $a_1 b_1$, $a_2 b_2$, c'est-à-dire autant qu'il y a de facteurs $f_1, f_2, f_3, \ldots, f_n$; donc n.

Cela fait, pour obtenir d'autres valeurs conjuguées de x et de y, il faut changer *à la fois*, dans les deux formules (1), les signes de deux produits tels que $a_1 b_1$, $a_2 b_2$, et cette opération donne lieu à $\dfrac{n(n-1)}{2}$ systèmes nouveaux de valeurs correspondantes de x et de y.

(*) *Nouvelles Annales*, 2e série, t. XVII, p. 241.

On continue ces changements de signe, en les faisant porter successivement sur trois, sur quatre, etc., produits (ab) à la fois, jusqu'à ce qu'on soit arrivé à les prendre en nombre inclusivement égal à la moitié du nombre n. Seulement il y a deux cas à considérer, selon que n est pair ou impair.

Lorsque n est pair $(n = 2n')$, il arrive que, dans le dernier groupe de ces permutations, celui où les produits ab sont pris n' à n', les valeurs de x et de y ainsi obtenues se répètent deux fois chacune, de telle sorte que, pour avoir le nombre exact des solutions distinctes ajoutées de ce chef, il ne faut compter que la moitié de celles de ce groupe. D'après cela, le nombre total de ces combinaisons diverses, et par suite celui des systèmes de x et de y, sont donnés par la somme

$$
\begin{aligned}
& 1 + 2n' + \frac{2n'(2n'-1)}{1.2} + \frac{2n'(2n'-1)(2n'-2)}{1.2.3} + \ldots \\
& + \frac{1}{2}\,\frac{2n'(2n'-1)(2n'-2)\ldots(2n'-n'+1)}{1.2.3\ldots n'} \\
& = 2^{2n'-1} = 2^{n-1}.
\end{aligned}
$$

Lorsque n est impair $(n = 2n' + 1)$, la règle générale s'applique sans modification, jusques et y compris le groupe où les facteurs (ab) dont on change à la fois le signe primitif sont pris n' à n', et le nombre total des systèmes de x et de y est égal à

$$
\begin{aligned}
& 1 + (2n' + 1) + \frac{(2n'+1)2n'}{1.2} \\
& + \frac{(2n'+1)2n'(2n'-1)}{1.2.3} + \ldots \\
& \frac{(2n'+1)2n'(2n'-1)\ldots(2n'-n'-2)}{1.2.3\ldots n'} = 2^{2n'} = 2^{n-1},
\end{aligned}
$$

c'est-à-dire le même que dans l'autre cas, algébriquement parlant.

VI. Quant au nombre N lui-même, sa décomposition en une somme de deux carrés suit la loi suivante.

Si N_2 est le produit $f_1 f_2$ de deux facteurs

$$f_1 = a_1^2 + b_1^2 \quad \text{et} \quad f_2 = a_2^2 + b_2^2,$$

on a

$$N_2 = L_2^2 + P_2^2,$$

où L_2 et P_2 ont pour valeurs types

$$L_2 = a_1 a_2 - b_1 b_2 \quad \text{et} \quad P_2 = a_1 b_2 + a_2 b_1.$$

L'autre décomposition, dont N est susceptible dans ce cas, se déduit de la valeur type qu'on vient d'écrire, en changeant à la fois dans L_2 et dans P_2 le signe de $a_1 b_1$, ou, ce qui revient au même, de b_1 tout seul.

Si N_3 est le produit $f_1 f_2 f_3$ de trois facteurs, c'est-à-dire d'un facteur de plus f_3 ($f_3 = a_3^2 + b_3^2$) que dans le cas précédent, la décomposition est

$$N_3 = L_8^2 + P_3^2,$$

où L_3 et P_3 ont pour valeurs initiales, en fonction de L_2 et de P_2,

$$L_3 = a_3 L_2 - b_3 P_2 \quad \text{et} \quad P_3 = a_3 P_2 + b_2 P_2.$$

Les trois autres décompositions se déduisent de celles-ci, en y changeant successivement et à la fois, dans L_3 et P_3, les signes de b_1, de b_2 et de b_3.

Si N_4 a un facteur de plus ($f_4 = a_4^2 + b_4^2$), la décomposition type est

$$N_4 = L_4^2 + P_4^2,$$

où L_4 et P_4 ont pour valeurs initiales, en fonction de L_3 et P_3,

$$L_4 = a_4 L_3 - b_4 P_3 \quad \text{et} \quad P_4 = a_4 P_3 + b_4 L_3.$$

Les sept autres décompositions dont N_4 est susceptible dans ce cas se déduisent de celle-ci en y changeant successivement, dans L_4 et P_4 à la fois, les signes de b_1, b_2, b_3, b_4, puis de $b_1 b_2$, $b_1 b_3$ et $b_1 b_4$.

En général, si N_n se compose de n facteurs (supposés, comme dans ce qui précède, à la première puissance), le $n^{\text{ième}}$ ayant pour expression $f_n = a_n^2 + b_n^2$, la décomposition type, parmi les 2^{n-1} dont N_n est alors susceptible, est

$$N_n = L_n^2 + P_n^2,$$

où L_n et P_n ont, en fonction de L_{n-1} et P_{n-1}, c'est-à-dire en fonction des valeurs de L et P dans la décomposition type de $\frac{N_n}{f_n} = L_{n-1}^2 + P_{n-1}^2$, les valeurs initiales suivantes :

$$L_n = a_n L_{n-1} - b_n P_{n-1} \quad \text{et} \quad P_n = a_n P_{n-1} + b_n L_{n-1}$$

Les $2^{n-1} - 1$ autres décompositions se déduisent de celle-ci, en y changeant successivement, dans L_n et P_n à la fois, les signes de $b_1, b_2, \ldots, b_n$, pris d'abord un à un, puis deux à deux, puis trois à trois, etc., et enfin n' à n', si $n = 2n' + 1$, et en ne prenant que la moitié du nombre de ces combinaisons n' à n', si $n = 2n'$, comme on l'a déjà dit pour le cas où le nombre à décomposer est N^2.

VII. Les formules des § IV et V donnent lieu à une autre remarque importante.

Toutes les décompositions de N^2, à quelque espèce qu'elles appartiennent, dérivent de celles de N (lesquelles sont au nombre de 2^{n-1}, toutes différentes entre elles), soit par la formule de décomposition simple

$$(2) \qquad N^2 = \overline{(L_i^2 - P_i^2)}^2 + \overline{2L_iP_i}^2,$$

soit par la formule double

$$(3) \qquad N^2 = \overline{(L_iL_{i'} \mp P_iP_{i'})}^2 + \overline{(L_iP_{i'} \pm L_{i'}P_i)}^2,$$

dans laquelle on doit prendre successivement les signes supérieurs et les signes inférieurs ensemble.

Or il est remarquable que les 2^{n-1} décompositions qui dérivent de la formule (2) composent *à elles seules* toutes les décompositions de la dernière espèce (E_n), et que les formules (3) n'en fournissent aucune de cette espèce. Pour le démontrer, il suffit de prouver :

1° Qu'elles sont toutes différentes entre elles, donc en nombre effectivement égal à 2^{n-1}, ainsi que le comporte l'espèce (E_n) ;

2° Que, dans chacune d'elles, les deux nombres composants n'ont aucun diviseur commun, ce qui est le caractère propre et distinctif des décompositions de cette espèce.

En premier lieu, si deux de ces décompositions, telles que $(L_1^2 - P_1^2)^2 + \overline{2L_1P_1}^2$ et $(L_2^2 - P_2^2)^2 + \overline{2L_2P_2}^2$, par exemple, étaient les mêmes, on aurait $L_2^2 - P_2^2 = L_2^2 - P_2^2$, car, $L_1^2P_1^2$ étant impair, on ne peut supposer qu'on eût $L_1^2 - P_1^2 = 2L_2P_2$ et $L_2^2 - P_2^2 = 2L_1P_1$. Mais, en considérant celles de N, toutes différentes entre elles, d'où elles dérivent respectivement, on a

$$N = L_1^2 + P_1^2 = L_2^2 + P_2^2,$$

d'où l'on conclurait, en combinant ces deux égalités par voie d'addition et ensuite de soustraction, $L_1 = L_2$ et $P_1 = P_2$, contrairement à l'hypothèse. Donc les deux décompositions dont il s'agit sont nécessairement différentes, comme celles d'où elles dérivent.

En second lieu, les deux nombres $L_i^2 - P_i^2$ et $2L_iP_i$ sont premiers entre eux; car, si L_i est pair, P_i est impair, ou inversement; donc $L_i^2 - P_i^2$ n'admet pas le facteur 2. En outre, L_i et P_i étant, à cause de la composition du nombre N, premiers entre eux dans la décomposition $N = L_i^2 + P_i^2$, tout diviseur de L_i P_i qui diviserait $L_i^2 - P_i^2$ devrait diviser L_i^2 et P_i^2; d'où il s'ensuivrait que L_i et P_i ne seraient pas premiers entre eux, contrairement à ce qui a lieu.

La proposition énoncée se trouve donc établie, et il en résulte que toutes les décompositions provenant de la formule double (3) font partie des $n - 1$ premières espèces, mais jamais de la dernière (E_n).

Observons encore que les décompositions de cette dernière provenance sont en nombre double de celui des combinaisons deux à deux des nombres composants L_i ou P_i, à cause des doubles signes de la formule (3); donc il y en a $2\,\frac{2^{n-1}(2^{n-1}-1)}{2}$. Or il en existe, comme on l'a vu, 2^{n-1} autres, provenant de la formule (2). Par conséquent, les formules (2) et (3) ensemble en fournissent $2^{n-1} + 2\,\frac{2^{n-1}(2^{n-1}-1)}{2} = 2^{2(n-1)} = 4^{n-1}$, c'est-à-dire autant qu'il y a d'unités dans le carré de 2^{n-1}, nombre des décompositions de N.

On sait d'ailleurs que le nombre effectif des décompositions de N^2 est $\frac{3^n-1}{2}$, et, comme on a $\frac{3^n-1}{2} < 4^{n-1}$, dès que $n > 2$, il s'ensuit nécessairement que quelques-unes des décompositions fournies par les formules (2) et (3) se répètent; mais cette répétition se présente seulement parmi celles qui dérivent de la formule (3), et jamais parmi celles qui dérivent de la formule (2), puisque celles-ci, toutes différentes entre elles, sont en nombre précisément égal à 2^{n-1}, c'est-à-dire n'excédant pas le nombre de celles qui composent l'espèce (E_n) qu'elles concourent seules à former.

Par exemple, dans le cas où $N = f_1 f_2 f_3$ se compose de trois facteurs simples, les formules

$$N^2 = (\overline{L_2 L_3 - P_2 P_3})^2 + (\overline{L_2 P_3} + \overline{P_2 L_3})^2,$$

$$N^2 = (\overline{L_2 L_4} + \overline{P_2 P_4})^2 + (\overline{L_2 P_4} - \overline{P_2 L_4})^2,$$

$$N^2 = (\overline{L_3 L_4} + \overline{P_3 P_4})^2 + (\overline{L_3 P_4} - \overline{P_3 L_4})^2,$$

ne font que répéter respectivement celles que fournissent les formules

$$N^2 = (L_1 L_4 - P_1 P_4)^2 + (\overline{L_1 P_4 + P_1 L_4})^2,$$

$$N^2 = (L_1 \overline{L_3} - P_1 P_3)^2 + (\overline{L_1 P_3} - \overline{P_1 L_3})^2,$$

$$N^2 = (\overline{L_1 L_2} - \overline{P_1 P_2})^2 + (L_1 \overline{P_2} - \overline{P_1} L_2)^2,$$

les quatre valeurs de N en fonction de L_1, P_1; L_2, P_2; L_3, P_3; L_4, P_4 étant d'ailleurs supposées écrites dans l'ordre symétrique qui se présente le plus naturellement.

VIII. Afin de rendre plus clair tout ce qui précède, notamment la règle indiquée (V) pour les permutations de signes, nous allons en faire quelques applications algébriques et numériques, en ayant soin de prendre les deux cas de n pair et de n impair.

Soit d'abord n pair et $N = f_1 f_2 f_3 f_4$.

Les formules (1) développées donnent

$$
\begin{aligned}
x = {} & (a_1^2 - b_1^2)(a_2^2 - b_2^2)(a_3^2 - b_3^2)(a_4^2 - b_4^2) \\
& - 4\,a_1 b_1 . a_2 b_2 (a_3^2 - b_3^2)(a_4^2 - b_4^2) \\
& - 4\,a_1 b_1 . a_3 b_3 (a_2^2 - b_2^2)(a_4^2 - b_4^2) \\
& - 4\,a_1 b_1 . a_4 b_4 (a_2^2 - b_2^2)(a_3^2 - b_3^2) \\
& - 4\,a_2 b_2 . a_3 b_3 (a_1^2 - b_1^2)(a_4^2 - b_4^2) \\
& - 4\,\alpha_2 b_2 . a_4 b_4 (a_1^2 - b_1^2)(a_3^2 - b_3^2) \\
& - 4\,a_3 b_3 . a_4 b_4 (a_1^2 - b_1^2)(a_2^2 - b_2^2) \\
& + 16\,a_1 b_1 . a_2 b_2 . a_3 b_3 . a_4 b_4 .
\end{aligned}
$$

$$
\begin{aligned}
y = {} & 2\,a_1 b_1 (a_2^2 - b_2^2)(a_3^2 - b_3^2)(a_4^2 - b_4^2) \\
& + 2\,a_2 b_2 (a_1^2 - b_1^2)(a_3^2 - b_3^2)(a_4^2 - b_4^2) \\
& + 2\,a_3 b_3 (a_1^2 - b_1^2)(a_2^2 - b_2^2)(a_4^2 - b_4^2) \\
& + 2\,a_4 b_4 (a_1^2 - b_1^2)(a_2^2 - b_2^2)(a_3^2 - b_3^2) \\
& - 8\,a_1 b_1 . a_2 b_2 . a_3 b_3 (a_4^2 - b_4^2) \\
& - 8\,a_1 b_1 . a_2 b_2 . a_4 b_4 (a_3^2 - b_3^2) \\
& - 8\,a_1 b_1 . a_3 b_3 . a_4 b_4 (a_2^2 - b_2^2) \\
& - 8\,a_2 b_2 . a_3 b_3 . a_4 b_4 (a_1^2 - b_1^2).
\end{aligned}
$$

Si nous désignons par les lettres romaines A, B, C, D, E, F, G, H, dans la valeur de x, et par les mêmes lettres accentuées A′, B′, ..., H′, dans la valeur de y, les huit termes dont ces valeurs se composent respectivement, pris dans l'ordre symétrique où ils y sont écrits, ces indices mnémotechniques nous permettront de présenter sous une forme plus brève et plus claire le tableau ci-après des systèmes de valeurs conjuguées de x et de y, qui sont ici au nombre de $2^{4-1} = 8$, savoir :

	$x =$								$y =$								
	A	B	C	D	E	F	G	H	A′	B′	C′	D′	E′	F′	G′	H′	
1er système (type)	+	−	−	−	−	−	−	+	+	+	+	+	−	−	−	−	Formules (1).
2e » . . .	+	+	+	+	−	−	−	−	−	+	+	+	+	+	+	−	Obtenu par le changement de signe de a_1b_1.
3	+	+	−	−	+	+	−	−	+	−	+	+	+	+	−	+	Id. de a_2b_2.
4e » . .	+	[illegible]	+	−	+	−	+	−	+	+	−	+	+	−	+	+	Id. de a_3b_3.
5e »	+	−	−	+	−	+	+	−	+	+	+	−	−	+	+	+	Id. de a_4b_4.
6e »	+	−	+	+	+	+	−	[illegible]	−	−	+	+	−	−	+	+	Id. de a_1b_1 et $a\ b$
7e »	+	+	−	+	+	−	+	+	−	+	−	+	−	+	−	+	Id. de a_1b_1 et a_3b_3
8e » .	+	[illegible]	+	−	−	+	+	+	−	+	+	−	[illegible]	−	−	+	Id. de a_1b_1 et a_4b_4.

Conformément à la règle donnée (V) pour le cas de n pair, on n'a eu égard ici qu'aux changements de signes simultanés des produits a_1b_1, a_2b_2: a_1b_1, a_3b_3; a_1b_1, a_4b_4, ceux des trois autres combinaisons a_2b_2, a_3b_3; a_2b_2, a_4b_4; a_3b_3, a_4b_4, ne faisant que répéter les trois premières, comme on peut s'en assurer.

Comme exemple numérique, prenons

$$\begin{aligned} N = 32045 &= 5.13.17.29 \\ &= (2^2+1^2)(3^2+2^2)(4^2+1^2)(5^2-2^2). \end{aligned}$$

On a ici

$$\begin{array}{llll} a_1 = 2, & b_1 = 1, & a_1^2 - b_1^2 = 3, & a_1b_1 = 2, \\ a_2 = 3, & b_2 = 2, & a_2^2 - b_2^2 = 5, & a_2b_2 = 6; \\ a_3 = 4, & b_3 = 1, & a_3^2 - b_3^2 = 15, & a_3b_3 = 4; \\ a_4 = 5, & b_4 = 2, & a_4^2 - b_4^2 = 21, & a_4b_4 = 10. \end{array}$$

Le premier système du tableau donne, tous calculs faits, les valeurs

$$\begin{aligned} x &= A - B - C - D - E - F - G + H = 31323, \\ y &= A' + B' + C' + D' - E' - F' - G' - H' = -6764, \end{aligned}$$

et

$$\begin{aligned} x^2 + y^2 = \overline{31323}^2 + \overline{6764}^2 &= 981130329 \\ &+ 45751696 = 1026882025 = \overline{32045}^2. \end{aligned}$$

Si l'on prend les valeurs du huitième système, par exemple, on trouve, tous calculs effectués,

$$\begin{aligned} x &= A + B + C - D - E + F + G + H = 32037, \\ y &= -A' + B' + C' - D' + E' - F' - G' + H' = -716; \end{aligned}$$

d'où

$$\begin{aligned} x^2 + y^2 = \overline{32037}^2 + \overline{716}^2 &= 1026369369 + 512656 \\ &= 1026882025 = \overline{32045}^2. \end{aligned}$$

IX. Actuellement, prenons n impair et N égal à $f_1f_2f_3f_4f_5$.

Les formules (1) développées donnent

$$
\begin{aligned}
1 = {} & (a_1^2 - b_1^2)(a_2^2 - b_2^2)(a_3^2 - b_3^2)(a_4^2 - b_4^2)(a_5^2 - b_5^2) \\
& - 4a_1b_1.a_2b_2(a_3^2 - b_3^2)(a_4^2 - b_4^2)(a_5^2 - b_5^2) \\
& - 4a_1b_1.a_3b_3(a_2^2 - b_2^2)(a_4^2 - b_4^2)(a_5^2 - b_5^2) \\
& - 4a_1b_1.a_4b_4(a_2^2 - b_2^2)(a_3^2 - b_3^2)(a_5^2 - b_5^2) \\
& - 4a_1b_1.a_5b_5(a_2^2 - b_2^2)(a_3^2 - b_3^2)(a_4^2 - b_4^2) \\
& - 4a_2b_2.a_3b_3(a_1^2 - b_1^2)(a_4^2 - b_4^2)(a_5^2 - b_5^2) \\
& - 4a_2b_2.a_4b_4(a_1^2 - b_1^2)(a_3^2 - b_3^2)(a_5^2 - b_5^2) \\
& - 4a_2b_2.a_5b_5(a_1^2 - b_1^2)(a_3^2 - b_3^2)(a_4^2 - b_4^2) \\
& - 4a_3b_3.a_4b_4(a_1^2 - b_1^2)(a_2^2 - b_2^2)(a_5^2 - b_5^2) \\
& - 4a_3b_3.a_5b_5(a_1^2 - b_1^2)(a_2^2 - b_2^2)(a_4^2 - b_4^2) \\
& - 4a_4b_4.a_5b_5(a_1^2 - b_1^2)(a_2^2 - b_2^2)(a_3^2 - b_3^2) \\
& + 16\,a_1b_1.a_2b_2.a_3b_3.a_4b_4(a_5^2 - b_5^2) \\
& + 16.a_1b_1.a_2b_2.a_3b_3.a_5b_5(a_4^2 - b_4^2) \\
& + 16.a_1b_1.a_2b_2.a_4b_4.a_5b_5(a_3^2 - b_3^2) \\
& + 16\,a_1b_1.a_3b_3.a_4b_4.a_5b_5(a_2^2 - b_2^2) \\
& + 16.a_2b_2.a_3b_3.a_4b_4.a_5b_5(a_1^2 - b_1^2)
\end{aligned}
$$

$$
\begin{aligned}
0 = {} & 2a_1b_1(a_2^2 - b_2^2)(a_3^2 - b_3^2)(a_4^2 - b_4^2)(a_5^2 - b_5^2) \\
& + 2a_2b_2(a_1^2 - b_1^2)(a_3^2 - b_3^2)(a_4^2 - b_4^2)(a_5^2 - b_5^2) \\
& + 2a_3b_3(a_1^2 - b_1^2)(a_2^2 - b_2^2)(a_4^2 - b_4^2)(a_5^2 - b_5^2) \\
& + 2a_4b_4(a_1^2 - b_1^2)(a_2^2 - b_2^2)(a_3^2 - b_3^2)(a_5^2 - b_5^2) \\
& + 2a_5b_5(a_1^2 - b_1^2)(a_2^2 - b_2^2)(a_3^2 - b_3^2)(a_4^2 - b_4^2) \\
& - 8\,a_1b_1.a_2b_2.a_3b_3(a_4^2 - b_4^2)(a_5^2 - b_5^2) \\
& - 8\,a_1b_1.a_2b_2.a_4b_4(a_3^2 - b_3^2)(a_5^2 - b_5^2) \\
& - 8\,a_1b_1.a_2b_2.a_5b_5(a_3^2 - b_3^2)(a_4^2 - b_4^2) \\
& - 8.a_1b_1.a_3b_3.a_4b_4(a_2^2 - b_2^2)(a_5^2 - b_5^2) \\
& - 8.a_1b_1.a_3b_3.a_5b_5(a_2^2 - b_2^2)(a_4^2 - b_4^2) \\
& - 8.a_1b_1.a_4b_4.a_5b_5(a_2^2 - b_2^2)(a_3^2 - b_3^2) \\
& - 8.a_2b_2.a_3b_3.a_4b_4(a_1^2 - b_1^2)(a_5^2 - b_5^2) \\
& - 8.a_2b_2.a_3b_3.a_5b_5(a_1^2 - b_1^2)(a_4^2 - b_4^2) \\
& - 8.a_2b_2.a_4b_4.a_5b_5(a_1^2 - b_1^2)(a_3^2 - b_3^2) \\
& - 8\,a_3b_3.a_4b_4.a_5b_5(a_1^2 - b_1^2)(a_2^2 - b_2^2) \\
& + 32\,a_1b_1.a_2b_2.a_3b_3.a_4b_4.a_5b_5
\end{aligned}
$$

Si nous représentons, comme ci-dessus (VIII), par les premières lettres de l'alphabet romain, les seize termes dont se compose la valeur de x, en les prenant successivement dans l'ordre symétrique où ils sont écrits, et si nous faisons de même pour les seize termes de y, avec les mêmes lettres accentuées, nous pourrons écrire le système type des valeurs de x et y ci-dessus, sous la forme

$$\begin{aligned} x &= A - B - C - D - E - F - G - H - I - J - K \\ &\quad + L + M + N + O + P. \\ y &= A' + B' + C' + D' + E' - F' - G' - H' - I' - J' \\ &\quad - K' - L' - M' - N' - O' + P'. \end{aligned}$$

Effectuant ensuite sur ce système type, qui résulte directement de l'application des formules (1), les permutations de signe indiquées au § V, on forme le tableau suivant, qui comprend les $2^{5-1} = 16$ systèmes de valeurs conjuguées de x et de y, dont se compose le cinquième groupe ou la dernière espèce (E_5) parmi les cinq espèces formant en totalité les

$$\frac{3^5 - 1}{2} = 121$$

systèmes de décomposition dont N^2 est ici susceptible.

	$x =$															
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1er syst.	+	−	−	−	−	−	−	−	−	−	−	+	+	+	+	+
2e »	+	+	+	+	+	−	−	−	−	−	−	−	−	−	−	+
3e »	+	+	−	−	−	+	+	+	−	−	−	−	−	−	+	−
4e »	+	−	+	−	−	+	−	−	+	+	−	−	−	+	−	−
5e »	+	−	−	+	−	−	+	−	+	−	+	−	+	−	−	−
6e »	+	−	−	−	+	−	−	+	−	+	+	+	−	−	−	−
7e »	+	−	+	+	+	+	+	+	−	−	−	+	+	+	−	−
8e »	+	+	−	+	+	+	−	−	+	+	−	+	+	−	+	−
9e »	+	+	+	−	+	−	+	−	+	−	−	+	−	+	+	−
10e »	+	+	+	+	−	−	−	+	−	+	+	−	+	+	+	−
11e »	+	+	+	−	−	−	+	+	+	+	−	+	+	−	−	+
12e »	+	+	−	+	−	+	−	+	+	−	+	+	−	+	−	+
13e »	+	+	−	−	+	+	+	−	−	+	+	−	+	+	−	+
14e »	+	−	+	+	−	+	+	−	−	+	+	+	−	−	+	+
15e »	+	−	+	−	+	+	−	+	+	−	+	−	+		+	+
16e »	+	−	−	+	+	−	+	+	+	+	−	−	−	+	+	+

	$y =$																
	A′	B′	C′	D′	E′	F′	G′	H′	I′	J′	K′	L′	M′	N′	O′	P′	
1er syst.	+	+	+	+	+	−	−	−	−	−	−	−	−	−	−	+	Type initial.
2e »	−	+	+	+	+	+	+	+	+	+	+	−	−	−	−	−	a_1b_1.
3e »	+	−	+	+	+	+	+	+	−	−	−	+	+	+	−	−	a_2b_2.
4e »	+	+	−	+	+	+	−	−	+	+	−	+	+	−	+	−	a_3b_3.
5e »	+	+	+	−	+	−	+	−	+	−	+	+	−	+	+	−	a_4b_4.
6e »	+	+	+	+	−	−	−	+	−	+	+	−	+	+	+	−	a_5b_5.
7e »	−	−	+	+	+	−	−	−	+	+	+	+	+	+	−	+	a_1b_1, a_2b_2.
8e »	−	+	−	+	+	−	+	+	−	−	+	+	+	−	+	+	a_1b_1, a_3b_3.
9e »	−	+	+	−	+	+	−	+	−	+	−	+	−	+	+	+	a_1b_1, a_4b_4.
10e »	−	+	+	+	−	+	+	−	+	−	−	−	+	+	+	+	a_1b_1, a_5b_5.
11e »	+	−	−	+	+	−	+	+	+	+	−	−	−	+	+	+	a_2b_2, a_3b_3.
12e »	+	−	+	−	+	+	−	+	+	−	+	−	+	−	+	+	a_2b_2, a_4b_4.
13e »	+	−	+	+	−	+	+	−	−	+	+	+	−	−	+	+	a_2b_2, a_5b_5.
14e »	+	+	−	−	+	+	+	−	−	+	+	−	+	+	−	+	a_3b_3, a_4b_4.
15e »	+	+	−	+	−	+	−	+	+	−	+	+	−	+	−	+	a_3b_3, a_5b_5.
16e »	+	+	+	−	−	−	+	+	+	+	−	+	+	−	−	+	a_4b_4, a_5b_5.

Obtenu par le changement de signe du ou des produits (rows 2e–16e of the last column).

Soit, comme exemple numérique,

$$N = 1185665 = 5.13.17.29.37$$
$$= (2^2 + 1^2)(3^2 + 2^2)(4^2 + 1^2)(5^2 + 2^2)(6^2 + 1^2),$$

d'où

$$\begin{array}{llll} a_1^2 - b_1^2 = 3 & \text{et} & a_1 b_1 = 2, \\ a_2^2 - b_2^2 = 5 & & a_2 b_2 = 6, \\ a_3^2 - b_3^2 = 15 & & a_3 b_3 = 4, \\ a_4^2 - b_4^2 = 21 & & a_4 b_4 = 10, \\ a_5^2 - b_5^2 = 35 & & a_5 b_5 = 6. \end{array}$$

Les valeurs conjuguées données par le onzième système, par exemple, sont

$$x = A + B + C - D - E - F + G - H + I - J - K$$
$$+ L + M - N - O + P = 1112703,$$
$$y = A' - B' - C' - D' + E' - F' - G' + H' - I' + J' - K'$$
$$- L' - M' + N' - O' + P' = 409504.$$

et, par suite,

$$x^2 + y^2 = \overline{1112703}^2 + \overline{409504}^2$$
$$= 1405801492225 = \overline{1185665}^2.$$

X. Si l'on voulait obtenir l'une des décompositions de N^2 qui, dans l'exemple numérique précédent, appartiennent à l'une des autres espèces, à la quatrième par exemple, et qu'on voulût avoir, parmi celles-ci, l'une de celles (au nombre de huit) dans lesquelles x^2 et y^2 ont le facteur commun $\overline{37}^2$, il suffirait d'écrire

$$x^2 = \overline{37}^2 . U^2, \quad y^2 = \overline{37}^2 . V^2,$$

$U^2 + V^2$ représentant l'une des huit décompositions de dernière espèce du nombre $N = 5.13.17.29$ dont nous avons donné le tableau au § VIII.

Il n'est pas nécessaire de s'étendre là-dessus davantage.

XI. Examinons en second lieu le cas où le nombre N est de la forme $f_1^\alpha . f_2^\beta . f_3^\gamma \dots f_n^\nu$, les facteurs premiers, de la forme $4n + 1$, y entrant aux puissances respectives, α, β, γ, ..., ν, et non plus à la première.

Les formules ci-dessus, notamment la formule fondamentale (1), sont encore applicables à ce cas, à la seule condition qu'on écrive $N = f_1 f_1 f_1 \dots f_2 f_2 f_2 \dots f_3 f_3 f_3 \dots$ et qu'on le considère ainsi comme composé de

$$n = \alpha + \beta + \gamma + \dots$$

facteurs du premier degré, comme précédemment. Mais alors, comme plusieurs des nombres $a_1, a_2, a_3, \dots$ et $b_1, b_2, b_3, \dots$ sont égaux entre eux, respectivement, cette égalité entraîne des simplifications dans la forme des expressions résultantes, et des réductions dans le nombre des termes dont ces expressions se composent. En outre, il y a des réductions dans le nombre total des décompositions qui composent le groupe (E_n), ainsi que dans tous les autres. On sait, en effet, que dans ce cas le nombre des décompositions de N est donné par la formule

$$I = \frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)\dots$$

et celui de N^2 par

$$I' = \frac{1}{2}[(2\alpha+1)(2\beta+1)(2\gamma+1)\dots - 1],$$

au lieu de

$$I = 2^{(\alpha+\beta+\gamma+\dots)-1} \quad \text{et} \quad I' = \frac{1}{2}[3^{(\alpha+\beta+\gamma+\dots)} - 1],$$

qu'on avait dans le cas où les facteurs, en même nombre effectif d'ailleurs, étaient tous différents et du premier degré. Quant à ces réductions qui se produisent alors, elles tiennent à l'une des deux causes suivantes ;

Tantôt deux ou plusieurs décompositions, qui sont distinctes dans le cas général, deviennent identiques d'une espèce à l'autre ;

Tantôt elles se réduisent à la décomposition illusoire $N^2 + 0$.

Par exemple, dans le cas particulier où N a la forme $f_1 f_2^2$, c'est-à-dire $f_1 f_2 f_3$, où $f_2 = f_3$, le nombre des décompositions de N^2 s'abaisse de

$$\frac{1}{2}(3^3 - 1) = 13 \text{ à } \frac{1}{2}(3.5 - 1) = 7,$$

savoir deux de première espèce, trois de seconde et deux de troisième, et si $f_1 = f_2 = f_3$, ou $N = f_1^3$, le nombre des solutions n'est plus que de $\frac{1}{2}[(2.3+1) - 1] = 3$, dont une de chaque espèce.

Mais il y a à faire sur ces décompositions d'autres remarques plus importantes, dont la démonstration ne présente pas de difficulté.

Bien que le nombre $N = f_1^\alpha f_2^\beta f_3^\gamma \ldots f_n^\nu$, composé de n facteurs (de la forme $4h + 1$) élevés respectivement à des puissances marquées par les exposants $\alpha, \beta, \ldots, \nu$, se décompose de I manières différentes en une somme de deux carrés (I étant égal à

$$\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1) \ldots (\nu + 1),$$

et le $\frac{1}{2}$ qui est en excédant quand le produit est impair comptant pour 1), il n'existe, parmi ces I décompositions, que 2^{n-1} décompositions dans chacune desquelles les deux carrés soient premiers entre eux, et elles existent toujours, de telle sorte que, sous ce rapport, le nombre N se trouve exactement dans le même cas que si tous les facteurs $f_1, f_2, \ldots, f_n$ n'y entraient qu'à la première puissance.

Par exemple, le nombre $5^3.13^2.17$, qui comporte douze décompositions, n'en a que quatre, c'est-à-dire le même nombre que $5.13.17$, dans chacune desquelles les deux carrés soient premiers entre eux, et ce sont celles qu'on obtient en regardant comme simples les trois facteurs composés, mais premiers entre eux, 5^3, 13^2 et 17, savoir

$$\begin{aligned} 5^3.13^2.17 &= 599^2 + 18^2 = 567^2 + 194^2 \\ &= 537^2 + 266^2 = 409^2 + 438^2, \end{aligned}$$

Dans les $I - 2^{n-1}$ autres décompositions de N, les carrés composants ont pour facteur commun l'un des produits qu'on obtient en combinant un à un, deux à deux, trois à trois, etc., et enfin n à n, les facteurs $f_1, f_2, f_3, \ldots, f_n$, affectés chacun d'un exposant pair, respectivement moindre que celui α, β, ... ou ν dont ils sont affectés dans N.

Dans l'exemple numérique ci-dessus, les huit décompositions qui n'ont pas été écrites sont : 1° les quatre qui ont 5^2 pour facteur commun et dont la partie décomposée correspond au produit des trois facteurs $5.13^2.17$, savoir

$$\begin{gathered} 5^2(54^2 + 107^2), \quad 5^2(98^2 + 69^2), \\ 5^2(114^2 + 37^2), \quad 5^2(118^2 + 21^2); \end{gathered}$$

2° les deux qui proviennent de $13^2(5^3.17)$ et qui sont

$$13^2(42^2 + 19^2), \quad 13^2(46^2 + 3^2);$$

3° enfin les deux qui proviennent de $5^2.13^2(5.17)$, qui ont $5^2.13^2$ en facteur commun et sont

$$5^2.13^2(7^2 + 6^2), \quad 5^2.13^2(9^2 + 2^2).$$

En conséquence, les décompositions de N^2, dont le nombre total est

$$P' = \frac{1}{2}[\,2\alpha+1\quad 2\beta+1\,\ldots\,2\nu+1\ -1\,],$$

ne contiennent, comme faisant partie de la dernière espèce (E_n), que celles qui dérivent des 2^{n-1} décompositions de N où les carrés sont premiers entre eux, par la formule fondamentale $(L_i^2 - P_i^2)^2 + \overline{2L_iP_i}^2$, absolument comme dans le cas (VII) où il n'entrait dans N que n facteurs à la première puissance, et toutes les autres appartiennent aux $n-1$ premières espèces, dans chacune desquelles les deux carrés composants ont un diviseur commun.

En résumé, que N soit composé de n facteurs du premier degré, de la forme $4h+1$, ou de n de ces facteurs élevés chacun à une puissance quelconque, il y a toujours 2^{n-1} décompositions de ce nombre dans chacune desquelles les deux carrés sont premiers entre eux, et pas davantage, et ces 2^{n-1} décompositions donnent naissance, par la formule $(L_i - P_i^2)^2 + \overline{2L_iP_i}^2$, à un pareil nombre de décompositions du carré N^2 de ce nombre, lesquelles jouissent seules de la même propriété parmi toutes les autres décompositions dont N^2 est susceptible et composent exclusivement la dernière espèce (E_n) de ces décompositions ; ce qui est assurément un fait digne de remarque.

XI. Entre autres conséquences de la théorie qui vient d'être exposée, on en déduit une réponse précise à cette question :

Quels sont les nombres entiers dont chacun jouit de la propriété d'être égal à la somme des carrés de deux nombres entiers consécutifs, et d'avoir pour carré la *somme des carrés de deux autres nombres entiers consécutifs.*

En d'autres termes, *elle fournit une solution complète du système des équations indéterminées*

$$y = x^2 + (x+1)^2, \quad y^2 = z^2 + (z+1)^2,$$

en nombres entiers.

Observons d'abord que y est impair et ne peut avoir pour diviseurs premiers que des facteurs de la forme $4k+1$. En effet, s'il en avait d'autres de la forme $4k+3$, il faudrait, comme on sait, pour que la décomposition de y en une somme de deux carrés fût possible d'une manière quelconque, que ces facteurs fussent chacun en nombre pair, c'est-à-dire que leurs produits M^2 fût un carré; on aurait donc, en appelant, comme ci-dessus, N le produit de tous les autres facteurs de forme $4k+1$,

$$y = M^2 N.$$

On sait d'ailleurs aussi que, ni M, ni M^2 ne sont en aucune façon décomposables en une somme de deux carrés; donc, si $\alpha^2 + \beta^2$ représente l'une quelconque des décompositions de N, la décomposition correspondante de y aurait la forme $y = M^2(\alpha^2 + \beta^2)$, ou $y = M^2\alpha^2 + M^2\beta^2$.

Or le plus petit facteur premier de la forme $4k+3$ étant 3, il est impossible que la différence entre $M\alpha$ et $M\beta$ ne soit que d'une unité, comme l'exige la première condition de l'énoncé.

Cela posé, si un nombre y satisfait aux équations proposées, son carré ne peut donner lieu à une décomposition telle que $y^2 = z^2 + (z+1)^2$, que si cette décomposition fait partie de la dernière espèce (E_n) parmi toutes celles que y^2 est susceptible de recevoir; car, pour toute décomposition $y^2 = u^2 + v^2$ qui ferait partie de l'une quelconque des autres espèces (E_1), (E_2), ..., (E_{n-1}), les deux nombres u, v auraient pour diviseur commun, comme on l'a démontré plus haut, l'un φ des facteurs de y, simples ou multiples, premiers ou composés. Or le plus petit de ces facteurs, de forme $4h+1$, étant 5, la différence entre u et v, qui est de la forme $\varphi(u'-v')$, est au moins égale à φ, donc *a fortiori* au moins égale à 5, et ne peut, en aucun cas, être égale à l'unité comme l'énoncé de la question l'exige.

C'est donc parmi les décompositions de l'espèce (E_n) seules qu'on peut rencontrer la décomposition

$$y^2 = z^2 + (z+1)^2.$$

Or, toutes les décompositions de l'espèce (E_n) sont, d'après (VII) et (XI), de la forme $(L_i^2 - P_i^2)^2 + \overline{2L_iP_i}^2$, les nombres entiers L_i, P_i, dont l'un est pair, et l'autre impair, étant tels qu'on ait $y = L_i^2 + P_i^2$. Soit L_i le plus grand de ces deux nombres, et posons, α étant un nombre entier positif, $L_i = P_i + \alpha$; d'où

$$y^2 = (2\alpha P_i + \alpha^2)^2 + (2P_i^2 + 2\alpha P_i)^2.$$

La seconde condition du problème consiste en ce que

$$(4)\quad \begin{cases} (2\alpha P_i + \alpha^2) - (2P_i^2 + 2\alpha P_i) = \pm 1 \\ \text{ou} \\ \alpha^2 - 2P_i^2 = \pm 1. \end{cases}$$

Il en résulte, comme on sait, que les deux nombres entiers α, P_i sont, l'un α le numérateur, l'autre P_i le dénominateur d'une quelconque des réduites de la fraction continue suivant laquelle se développe la racine carrée de 2, savoir d'une réduite de rang impair $\left(\text{la première étant } \frac{1}{0}\right)$ si l'on prend le signe $+$ dans le second membre de l'équation (4), et d'une réduite de rang pair si l'on prend le signe —

Ces réduites consécutives sont

$$(5) \qquad \frac{1}{0},\ \frac{1}{1},\ \frac{3}{2},\ \frac{7}{5},\ \frac{17}{12},\ \frac{41}{29},\ \frac{99}{70},\ \frac{239}{169},\ \ldots \text{ etc.}$$

Actuellement, la première condition du problème exige que dans la décomposition $L_\iota^2 + P_\iota^2$ de y, d'où dérive directement celle $y^2 = (L_\iota^2 - P_\iota^2)^2 + \overline{2L_\iota P_\iota}^2$ que nous venons de considérer, les nombres composants L_ι, P_ι ne diffèrent entre eux que d'une unité; en d'autres termes, il faut, non-seulement que α soit le numérateur de l'une des réduites ci-dessus, dont P_ι serait le dénominateur, mais encore que ce numérateur soit égal à l'unité.

Or, si l'on exclut dans la suite (5) la première réduite qui donne la solution illusoire $P_\iota = 0$, on voit que la suivante $\frac{1}{1}$ est la seule qui remplisse les conditions exigées. On a donc

$$P_\iota \text{ ou } x = 1, \quad \alpha \quad 1, \quad L_\iota = 2,$$

d'où

$$z = 1 + 2 \quad 5$$

et ensuite

$$y^2 = L_\iota^2 - P_\iota^2\ ^2 + \overline{2L_\iota P_\iota}^2 = 3^2 + 4^2 = 5^2.$$

Ainsi le système des valeurs $x = 1$, $z = 3$, $y = 5$ est *le seul* qui résolve la question proposée.

Remarque. — On conclut aussi de là que l'équation indéterminée du quatrième degré

$$x^4 + 2x^3 + 2x^2 \quad x = \frac{1}{2} z \quad z + 1$$

n'est pareillement satisfaite que par les valeurs conjuguées $x = 1$, $z = 3$;

Et encore que, parmi l'infinité des systèmes de deux nombres entiers consécutifs u et $(u+1)$, dont le produit $u(u+1)$ est égal à un nombre triangulaire $\frac{1}{2}z(z+1)$, il n'y en a qu'un seul, savoir 2 et 3, dans lequel le plus petit des deux nombres soit égal au carré d'un nombre entier augmenté de ce nombre lui-même, $2 = 1^2 + 1$, et l'on a $2.3 = \frac{3.4}{2}$.

Nota.—Le lecteur, se référant à la page 242 (*voir* la livraison de juin), ligne 2 en remontant, est prié d'intercaler la parenthèse suivante entre le mot « espèce » et le mot « dans » et avant la virgule :

(c'est l'espèce désignée par E_{n-1}, selon la notation adoptée).