A. DELTOUR

Continuants : applications à la théorie des nombres

Nouvelles annales de mathématiques 4e série, tome 11 (1911), p. 116-129

<http://www.numdam.org/item?id=NAM_1911_4_11__116_1>

[I23a]

CONTINUANTS : APPLICATIONS A LA THÉORIE DES NOMBRES;

Par M. A. DELTOUR.

(*Suite et fin*) (¹).

TROISIÈME PARTIE.

95. La considération des continuants fournit de nouvelles démonstrations de certains théorèmes relatifs à la décomposition des nombres entiers en somme de carrés.

Cet article contient deux de ces démonstrations : la première se rapporte à la décomposition d'un nombre premier de la forme $4h+1$ en une somme de deux carrés (théorème de Fermat); la seconde est celle de la formule de Liouville qui sert à déterminer dans cer-

(¹) Voir *Nouv. Ann.*, 4ᵉ série, t. I et VIII, 1908, p. 49, 172, 264, 481 et 535.

tains cas le nombre des décompositions d'un nombre donné en une somme de carrés.

96. *Démonstration du théorème de Fermat relatif à la décomposition d'un nombre premier* $p = 4h + 1$ *en une somme de deux carrés.* — Les formules indiquées au n° 41 montrent que :

1° Un continuant symétrique $(\alpha, \underline{\alpha})$ ayant un nombre pair d'éléments entiers représente un nombre entier de la forme x^2+y^2 (x, y premiers entre eux) et *vice versa;*

2° Un continuant symétrique positif réduit $(\alpha, m, \underline{\alpha})$ ayant un nombre impair d'éléments $\geqq 3$ représente un produit xy dont les facteurs sont > 1 et ne peut pas représenter un nombre premier.

Cela posé, on sait que pour un nombre premier $p = 4h + 1$, le nombre des continuants positifs réduits de valeur p est $\frac{p-1}{2}$ (50, Remarque 1°) et par conséquent pair.

Ces continuants sont symétriques ou non.

Dans ce dernier cas, l'un d'eux (β) et son inverse $(\underline{\beta})$ sont différents.

Les continuants non symétriques se correspondent ainsi deux à deux. Il y a donc un nombre pair de continuants symétriques.

Or, le continuant (p) de résidu 1 est symétrique. D'ailleurs, c'est évidemment le seul n'ayant qu'un élément.

Il y a donc au moins un continuant symétrique de valeur p dont le nombre d'éléments est $\geqq 2$ et par conséquent pair.

D'où résulte

$$p = x^2 + y^2.$$

Il ne peut pas y en avoir deux. Car, soient R_1, R_2 leurs résidus. Ceux-ci satisferaient, d'après la relation (VI) (n° 19), aux congruences

$$R_1^2 + 1 \equiv 0 \pmod{p},$$
$$R_2^2 + 1 \equiv 0 \pmod{p},$$

d'où

$$R_1^2 - R_2^2 \equiv 0 \pmod{p},$$

ce qui est impossible puisque $R_1 R_2$ sont $\leq \frac{p-1}{2}$.

97. Le théorème de Liouville, dont on trouvera plus loin l'énoncé, se présentera comme une conséquence de la formule (I) du n° 5 :

$$\text{(I)} \qquad (\alpha, \beta) = (\alpha)(\beta) + (\alpha_{0,1})(\beta_{1,0}).$$

Pour le démontrer, il faut d'abord comparer celle-ci aux diverses expressions d'un nombre positif donné N de la forme

$$(1) \qquad N = ab + a'b',$$

où a, a' sont premiers entre eux, ainsi que b, b', tous ces nombres étant entiers positifs et différents de zéro.

A cet effet, nous supposerons que dans la formule (I) tous les éléments sont positifs, le dernier de (α) ou le premier de (β) pouvant seuls être nuls.

98. Il s'agit de montrer que *toute expression* (1) *de* N *est identique à l'une de celles qui résultent de l'application de la formule* (I) *à chacun des continuants réduits* (α, β) *de valeur* N *ainsi définis et* vice versa.

En effet, considérons d'abord l'ensemble de celles où $a > a'$ et où, pour les valeurs particulières $a = a' = 1$, on a $b < b'$.

Comme a, a' sont premiers entre eux, ainsi que b, b', toute égalité (1) est susceptible de s'identifier avec la formule (I) en posant

$$(\alpha) = a, \qquad (\beta) = b,$$
$$(\alpha_{0,1}) = a', \qquad (\beta_{1,0}) = b',$$

d'où l'on déduit

$$(\alpha, \beta) = \mathrm{N}.$$

On satisfait à ces égalités en prenant pour (α) le continuant positif court correspondant à la fraction $\frac{a}{a'}$ (n° 50); de même pour (β) celui de $\frac{b}{b'}$ si $b > b'$, ou pour $(\beta_{1,0})$ celui de $\frac{b'}{b}$ si $b < b'$, en faisant alors $(\beta) = (0, \beta_{1,0})$.

Dans le premier cas $(b > b')$, le continuant (α, β) est positif réduit. Dans le second, le premier élément de β est zéro.

L'égalité (1) est donc toujours représentée, et d'une seule façon, par la formule (I) dans laquelle (α, β) est un continuant réduit de valeur N où le premier élément de (β) peut seul être nul.

D'ailleurs, à deux systèmes différents de valeurs de a, a'; b, b' correspondent deux systèmes distincts de suites α, β.

Inversement, en mettant un continuant positif réduit de N sous l'une des formes (α, β), $(\alpha, 0, \beta_{1,0})$, dans lesquelles (α), (β), $(\beta_{1,0})$ sont des continuants positifs, la formule (I) représente évidemment une certaine décomposition (1) de N.

En outre, quel que soit le continuant de N considéré, à deux systèmes différents de suites α, β ou α, $\beta_{1,0}$ correspondent deux systèmes distincts de valeurs de a, a'; b, b'.

On reproduit donc ces systèmes de valeurs, c'est-à-dire toutes les expressions (1) au moyen de la formule (I) appliquée de toutes les manières possibles à chacun des continuants positifs réduits de N.

Remarque. — Pour former les différentes suites partielles α qui correspondent à un continuant donné de N, si n, n_1 désignent respectivement la somme des éléments de (α) et celle des éléments du continuant, il faut donner à n successivement toutes les valeurs de 1 à $n_1 - 1$.

Exemple :

$$N = (2, 1, 3),$$
$$(\alpha) = (1), (2), (2, 1), (2, 1, 1), (2, 1, 2).$$

Dans les conditions admises, le nombre des décompositions de N sous la forme $ab + a'b'$ est donc $\Sigma(n_1 - 1)$, Σ se rapportant à tous les continuants positifs réduits de N.

99. *Lorsqu'on prend l'ensemble des expressions* (1) *pour lesquelles on a* $a < a'$ *et* $b > b'$ *pour* $a = a' = 1$ *au lieu de* $a > a'$ *et* $b < b'$ *pour* $a = a' = 1$, *on trouve un mode de représentation semblable.*

Il suffit de remplacer (α) par $(\alpha, 0)$ dans les formules. Chacune des nouvelles expressions s'obtient, en effet, en permutant dans chacune des précédentes a avec a' et b avec b'.

Ainsi $(\alpha)(0, \beta)$ deviennent $(\alpha, 0), (\beta)$; $(\alpha), (\beta)$ deviennent $(\alpha, 0), (0, \beta)$.

On voit d'ailleurs que le premier continuant (α) est (1) pour la série $a > a'$ et $(1, 0)$ pour la série $a < a'$; dans les deux cas, on a

$$a = a' = 1$$

et

$$N = b + b'.$$

Pour $(\alpha) = (1)$, on a en effet $b < b'$ et pour $(\alpha) = (1, 0)$, $b > b'$.

100. *Représentation des expressions* (1) *du n° 97, dans lesquelles on a*

$$N = 2m, \qquad ab = m', \qquad a'b' = m'',$$

m, m', m'' étant des nombres impairs.

En conservant la notation déjà employée, l'ensemble de ces expressions est représenté de la même manière qu'aux nos 98, 99 ; seulement, de tous les systèmes de suites α, β, on ne retient que ceux dans lesquels (α), $(\alpha_{0,1})$, c'est-a-dire a et a' sont impairs. Cette dernière condition suffit d'ailleurs pour que (β), $\beta_{1,0})$, c'est-à-dire b, b', soient aussi impairs, puisque ces nombres sont premiers entre eux et que (α, β) est pair.

101. Dans ce mode de représentation, les nombres impairs a, a' jouissent des trois propriétés suivantes :

1° *Si a, a' et a_1, a'_1 sont deux couples consécutifs de valeurs impaires,*

$$\begin{aligned} a &= (\alpha), & a_1 &= (\alpha, \varphi), \\ a' &= (\alpha_{0,1}), & a'_1 &= (\alpha, \varphi_{0,1}), \end{aligned}$$

correspondant à deux suites α, $\alpha\varphi$, d'un continuant donné $N = (\alpha, \beta) = (\alpha, \varphi, \beta')$ (n° 98, Remarque) et tels que $(a - a')$ et $(a_1 - a'_1)$ soient de même signe, on a

$$a + a' = [a_1 - a'_1]. \tag{2}$$

2° *Si a, a' correspondent à la première suite α de ce continuant, on a*

$$a - a' = 0. \tag{3}$$

3° *Si a, a' correspondent à la dernière suite α, on a*

$$a + a' = N. \tag{4}$$

Pour démontrer la première, supposons d'abord $(a - a')$, $(a_1 - a'_1)$ positifs.

Puisqu'on a

$$a_1 = (\alpha, \varphi),$$
$$a'_1 = (\alpha, \varphi_{0,1}),$$

le dernier élément de φ est différent de zéro; autrement on aurait $a_1 < a'_1$.

Cette suite peut donc s'écrire

$$\varphi = (1, \psi, 1) \qquad \text{ou} \qquad \varphi = (0, 1, \psi, 1),$$

suivant qu'elle commence ou non par un terme différent de zéro, la suite ψ contenant ou non des éléments nuls.

On a ainsi dans le premier cas

$$a_1 = (\alpha, 1, \psi, 1) = a(1, \psi, 1) + a'(\psi, 1),$$
$$a'_1 = (\alpha, 1, \psi) = a(1, \psi) + a'(\psi)$$

et, dans le second cas, des expressions analogues.

Pour que les deux couples a, a' et a_1, a'_1 soient consécutifs, il faut prendre pour ψ la suite la plus réduite qui donne pour a_1, a'_1 des valeurs impaires. Comme on le voit facilement, c'est celle où ψ ne contient qu'un seul élément $k \geqq 0$.

On a alors soit

$$\varphi = (1, k, 1)$$

et

$$a_1 = a(k+2) + a'(k+1),$$
$$a'_1 = a(k+1) + a'k;$$

soit

$$\varphi = (0, 1, k, 1)$$

et

$$a_1 = a(k+1) + a'(k+2),$$
$$a'_1 = ak + a'(k+1),$$

relations d'où résulte

$$a + a' = a_1 - a'_1.$$

En particulier, lorsque $k = 0$, (φ) devient (2) ou $(0, 2)$.

Démonstration analogue lorsqu'on suppose $(a - a')$ et $(a - a'_1)$ négatifs, en remplaçant dans les expressions précédentes

$$(1, \psi, 1) \quad \text{par} \quad (1, \psi, 1, 0)$$

ou

$$(0, 1, \psi, 1) \quad \text{par} \quad (0, 1, \psi, 1, 0).$$

On a donc, dans tous les cas,

$$a + a' = [a_1 - a'_1].$$

La seconde proposition est évidente si l'on remarque que le premier continuant partiel (α) est (1) ou $(1, 0)$ pour lequel on a

$$\begin{aligned} a &= (\alpha) = 1, \\ a' &= (\alpha_{0,1}) = 1. \end{aligned}$$

Pour démontrer la troisième, mettons le continuant donné de N sous la forme $(\lambda, 0, 1)$.

Les nombres (λ) et $(\lambda_{0,1}) = (\lambda, 0)$ sont premiers avec $N = 2m = (\lambda, 0, 1)$, par conséquent impairs, et représentent le dernier couple de valeurs a, a' puisque λ est la dernière suite pouvant être prise pour α.

On a dans l'expression de N correspondante

$$b = b' = 1,$$

et par suite

$$N = a + a'.$$

102. Théorème de Liouville [1]. — *Soit m un nombre positif impair tel que $2m = m' + m''$ (m', m'' positifs impairs); si l'on pose*

$$S = \Sigma[f(d' - d'') - f(d' + d'')],$$

---

[1] *Journal de Mathématiques pures et appliquées*, 2e série, t. III, 1858, p. 143.

où f est une fonction paire quelconque, d' un diviseur de m', d'' un diviseur de m'', et où Σ s'étend, pour toutes les valeurs de m' et de m'', à tous les couples de diviseurs d', d'', on trouve

$$S = \Sigma d[f(0) - f(2d)],$$

où d parcourt tous les diviseurs de m.

En posant

$$m' = d'e', \qquad m'' = d''e'',$$

on a

$$2m = d'e' + d''e'',$$

où d', d'', e', e'' peuvent avoir des facteurs communs.

Pour ramener ces expressions au cas du n° 100, décomposons S en parties et désignons par $S_{p,q}$ la somme relative à tous les couples d', d'' pour lesquels p et q sont respectivement les plus grands communs diviseurs de d', d'' et de e', e''.

Occupons-nous d'abord de $S_{1,1}$. Les égalités $2m = d'e' + d'e''$ peuvent être représentées, dans la notation du n° 98, au moyen des continuants (α, β) de $2m$, puisque d', d'' sont premiers entre eux, ainsi que e', e''.

Groupons les termes de $S_{1,1}$ dont les couples d', d'' proviennent d'un même continuant (α, β) et rangeons ces termes dans l'ordre des suites α correspondantes, comme au n° 98 (*Remarque*).

Soit T l'un de ces groupes.

Posons enfin $T = T' + T''$, les termes de T qui composent chacune des parties T', T'' étant caractérisés par le signe de $(d' - d'')$ ou par celui de $e' - e''$, lorsque $d' = d'' = 1$ (n° 99).

Puis cherchons séparément les expressions de T' et T''.

La somme

$$T' = \Sigma[f(d' - d'') - f(d' + d'')]$$

des termes de T correspondant aux expressions (1), pour lesquelles on a

$$d' > d''$$

ou

$$d' = d'' = 1 \quad \text{et} \quad e' < e'',$$

se réduit à

$$T' = f(0) - f(2m).$$

Soient, en effet, d', d'' et d'_1, d''_1 deux couples *consécutifs* quelconques provenant des deux continuants partiels (α), $(\alpha') = (\alpha, \varphi)$.

Le terme $-f(d' + d'')$ est détruit par le suivant $f(d'_1 - d''_1)$ à cause de la relation (2) (n° 101). Restent donc seulement les deux termes extrêmes où figurent la différence des premières valeurs de d', d'' et la somme des dernières qui sont connues par les relations (3) et (4) (n° 101).

On trouve donc

$$T' = f(0) - f(2m).$$

La somme T'' est l'ensemble des termes de T correspondant aux expressions (1) pour lesquelles on a

$$d' < d''$$

ou

$$d' = d'' = 1 \quad \text{et} \quad e' > e''.$$

Or, celles-ci se déduisent des précédentes, relatives au groupe T', en permutant les nombres d' et d'' et, pour les premiers termes où $d' = d'' = 1$, en permutant e' et e''.

Par suite, la somme T'' s'obtient en permutant dans T' les nombres d' et d''. *Comme f est une fonction paire*, l'expression ne change pas.

On a donc

$$T'' = T'.$$

La valeur de T est, par conséquent,

$$T = 2T' = 2[f(0) - f(2m)].$$

Cette formule est indépendante du continuant (α, β) auquel se rapporte le groupe T.

Valeur de $S_{1,1}$. — Pour trouver $S_{1,1}$, il faut totaliser les sommes T relatives à tous les continuants réduits (α, β) de $2m$.

Elles ont même valeur, et leur nombre est $\frac{\varphi(2m)}{2}$ (n° 50, *Remarque*).

On a donc

$$S_{1,1} = \varphi(2m)[f(0) - f(2m)].$$

Valeur de $S_{p,q}$. — Pour un couple de diviseurs d', d'' appartenant à $S_{p,q}$, l'égalité $2m = d'e' + d''e''$, où pq est facteur commun dans le second membre, et par conséquent diviseur de m, peut s'écrire

$$2\frac{m}{pq} = \frac{d'}{p}\frac{e'}{q} + \frac{d''}{p}\frac{e''}{q}.$$

$\frac{d'}{p}$, $\frac{d''}{p}$ sont premiers entre eux, ainsi que $\frac{e'}{q}$, $\frac{e''}{q}$.

On est donc ramené au cas de $S_{1,1}$ lorsqu'on remplace m par $\frac{m}{pq}$.

On trouve encore les relations

$$(2') \qquad d' + d'' = [d'_1 - d''_1],$$

pour deux couples consécutifs de diviseurs et

$$(3') \qquad d' - d'' = 0,$$

$$(4') \qquad d' + d'' = \frac{2m}{q},$$

pour les couples extrêmes.

On déduit de là, comme pour $S_{1,1}$,

$$S_{p,q} = \varphi\left(\frac{2m}{pq}\right)\left[f(0) - f\left(\frac{2m}{q}\right)\right].$$

Valeur de S. — En faisant parcourir à p tous les diviseurs de $\frac{m}{q}$, q restant constant, on a pour total

$$\Sigma_q(S_{p,q}) = \left[\Sigma\,\varphi\left(\frac{2m}{pq}\right)\right]\left[f(0) - f\left(\frac{2m}{q}\right)\right].$$

Or, on sait que

$$\Sigma\,\varphi\left(\frac{2m}{pq}\right) = \frac{m}{q}.$$

On a donc

$$\Sigma_q(S_{p,q}) = \frac{m}{q}\left[f(0) - f\left(\frac{2m}{q}\right)\right].$$

Puis, faisant parcourir à q ou à $\frac{m}{q}$ tous les diviseurs d de m et ajoutant, on a finalement

$$S = \Sigma d[f(0) - f(2d)].$$

Remarque. — Les raisonnements qui précèdent s'appliquent encore si, au lieu de $N = 2m$, on fait $N = 2^h m$.

On trouve dans ce cas

$$S = 2^{h-1}\Sigma d[f(0) - f(2^h d)].$$

103. Rappelons maintenant comment la formule de Liouville permet de déterminer le nombre de décompositions d'un nombre donné $4m$, m étant impair, en une somme de quatre carrés impairs et de $8m$ en une somme de huit carrés impairs.

On sait d'abord que $\Sigma(-1)^{\frac{d-1}{2}}$, où le signe Σ s'applique à tous les diviseurs d de m, est égal au nombre de décompositions de $2m$ en une somme de deux carrés impairs, en comptant comme distinctes celles qui ne diffèrent que par l'ordre des termes.

Cela posé, soit

$$4m = X^2 + Y^2 + Z^2 + T^2.$$

Ces carrés étant impairs, on peut écrire

$$2m' = X^2 + Y^2,$$
$$2m'' = Z^2 + T^2,$$

d'où

$$4m = 2m' + 2m'',$$

où m, m', m'' sont impairs.

Pour avoir toutes les décompositions de $4m$, il suffit d'avoir toutes celles de $2m'$ et de $2m''$ pour toutes les valeurs de m' et de m''.

Or, si dans la formule de Liouville on pose $f(x) = \cos xt$, t étant une constante quelconque, on trouve l'égalité

$$\Sigma[\Sigma \sin d't \,\Sigma \sin d''t] = \Sigma[d \sin^2 dt],$$

et pour $t = \frac{\pi}{2}$

$$\Sigma\left[\Sigma(-1)^{\frac{d'-1}{2}} \Sigma(-1)^{\frac{d''-1}{2}}\right] = \Sigma d.$$

Dans celle-ci, $\Sigma(-1)^{\frac{d'-1}{2}}$, où le signe Σ s'applique à tous les diviseurs d' de m', est égal au nombre de décompositions de $2m'$ en une somme de deux carrés impairs. De même $\Sigma(-1)^{\frac{d''-1}{2}}$ pour $2m''$.

La somme de leurs produits pour toutes les valeurs de m' et de m'' qui forme le premier membre est donc égal au nombre de décompositions de $4m$ en une somme de quatre carrés impairs.

En désignant par $Z_p(m)$ la somme des puissances p de tous les diviseurs de m, ce nombre est Σd ou $Z_1(m)$.

Faisant ensuite successivement $f(x) = x^2$ et x^4, on trouve

$$Z_3(m) = \Sigma\, Z_1(n)\, Z_1(2m - n)$$

et

$$Z_5(m) = \Sigma\, Z_1(n)\, Z_3(2m - n),$$

n variant, sous le signe Σ, de 1 à $2m - 1$.

De la première de ces égalités, on déduit, par un raisonnement analogue au précédent, que le nombre $8m$ se décompose en une somme de huit carrés impairs de $Z_3(m)$ façons.