NOUVELLES ANNALES DE MATHÉMATIQUES

A. DELTOUR

Continuants : applications à la théorie des nombres

Nouvelles annales de mathématiques 4e série, tome 8 (1908), p. 535-542

<http://www.numdam.org/item?id=NAM_1908_4_8__535_1>

[I23a]

CONTINUANTS : APPLICATIONS A LA THÉORIE DES NOMBRES;

PAR M. A. DELTOUR.

(SUITE.)

CONGRUENCES.

87. *Objet et définitions.* — Lorsque les valeurs des continuants, des adjoints et de leurs éléments sont déterminées par des congruences et exprimées par des nombres congrus suivant un certain module, les procédés de transformation employés jusqu'ici subsistent encore.

être un *maximum* entre celles de tous les polygones isopérimètres.

En effet, chaque polygone concave a une diagonale HK (au moins) hors du polygone; or, il suffit de tourner l'une des parties du contour, dont les extrêmes sont H et K, autour de la droite HK, pour augmenter l'aire du polygone donné sans changer son périmètre.

Il faut y ajouter ceux qui reposent sur l'existence de continuants définis comme les unitaires (n° 75), à cela près que les égalités sont remplacées par des congruences.

Ces continuants ainsi que leurs adjoints et les suites d'éléments qui les constituent seront dits unitaires par congruences ou, par abréviation, *unitaires congr.*

Il est évident que les unitaires (n° 75) sont des unitaires congr. par rapport à tous les modules.

Nous nous occuperons d'abord du mode de formation de ces unitaires congr., puis de leur application à la transformation des continuants ou des adjoints dont les valeurs sont définies par des congruences.

L'indication du module (mod t), à la suite des congruences, sera supprimée lorsqu'il n'y aura pas ambiguïté.

88. *Unitaires congr.* — Malgré la similitude des définitions des deux sortes d'unitaires et l'analogie de propriétés qui en résulte, certaines différences sont à noter.

Ainsi les conditions nécessaires et suffisantes pour qu'un continuant (λ) soit unitaire sont, comme on sait,

$$(\lambda_{0,1}) = (\lambda_{1,0}) = 0,$$

puisque la relation (VI) donne

$$(\lambda)(\lambda_{1,1}) = \pm 1.$$

Mais pour que (λ) soit unitaire congr., les conditions semblables

$$(\lambda_{0,1}) \equiv (\lambda_{1,0}) \equiv 0$$

doivent être complétées par l'une des congruences

$$(\lambda) \equiv \pm 1, \qquad (\lambda_{1,1}) \equiv \pm 1.$$

89. — Les propositions suivantes, dont il suffit de donner l'énoncé, s'établissent par des moyens analogues à ceux employés au n° 31 :

I. *Le nombre congru à la valeur absolue d'un continuant ou d'un adjoint n'est pas modifié par l'introduction d'une suite unitaire congr. entre deux éléments* (*Syst. alt.*)

Le facteur par lequel la valeur relative est multipliée est ± 1, $\pm i$, suivant le type auquel appartient la suite.

II. *Toute permutation circulaire d'un unitaire congr. forme un unitaire congr. de même type* (*Syst. alt.*).

En outre, on remarquera que, si (λ) est un unitaire congr., $(-\lambda)$ l'est aussi.

90. — *Si*

$$(\lambda) = (a, \alpha, b, \beta)$$

est un unitaire congr. et si l'on pose

$$(\lambda) \equiv u i^{n_\lambda^2} \equiv u_1 \qquad (\text{pour } u = \pm 1),$$

on a la relation (*Syst. alt.*)

$$u_1[-1]^{n_\alpha}(\alpha) \equiv (\beta).$$

En effet, (β) peut s'écrire

$$(\beta) = (0, -b, -\underline{\alpha}, -a, 0, a, \alpha, b, \beta$$

et devient, par suppression de la suite λ,

$$\begin{aligned}(\beta) &\equiv u_1(0, -b, -\underline{\alpha}, -a, 0)\\ &\equiv u_1[-1]^{n_\alpha}(\alpha).\end{aligned}$$

Cette relation prend une forme symétrique par rapport à α et β.

Elle peut, en effet, s'écrire, en remplaçant n_λ par $n_\alpha + n_\beta + 2$ dans l'expression de u_1,

$$(C_1) \qquad u[-1]^{n_\alpha n_\beta} i^{3n_\alpha^2}(\alpha) \equiv i^{3n_\beta^2}(\beta).$$

(α), (β) étant écrits dans le système alterné, les quantités $i^{3n_\alpha^2}(\alpha)$, $i^{3n_\beta^2}(\beta)$ sont réelles (n° 30, *remarque*).

Remarque. — Comme conséquence de la deuxième proposition du n° 89, on a une relation semblable pour toutes les combinaisons a, b distinctes qu'on peut former avec les éléments de λ pris deux à deux.

91. *Lorsqu'une suite d'éléments α est telle que le plus grand commun diviseur* S*, pris en valeur absolue, de* (α) *et du module t divise* $(\alpha_{1,0}) - u_1$

$$(u_1 = u i^{(n_\alpha - 1)^2};\ u = \pm 1),$$

on peut former un unitaire congr. de S *manières différentes en ajoutant à α trois nouveaux éléments* (*Syst. alt.*).

Cherchons à déterminer b_1, b_2, b_3 de telle sorte que

$$(\lambda) = (b_1, b_2, b_3, \alpha)$$

soit un unitaire congr.

Ces quantités doivent remplir les trois conditions

$$(b_1, b_2, b_3, \alpha_{0,1}) \equiv 0, \qquad (b_2, b_3, \alpha) \equiv 0,$$
$$(\lambda) \equiv (b_3, \alpha) \equiv u_1.$$

Il résulte de l'hypothèse que la dernière congruence qui s'écrit

$$(b_3)(\alpha) + (\alpha_{1,0}) - u_1 \equiv 0$$

est satisfaite pour S valeurs de b_3 distinctes. Soit b_3 l'une d'elles.

La deuxième devient alors

$$(b_2)u_1 + (\alpha) \equiv 0$$

et donne la valeur de b_2.

Pour déterminer b_1, on déduit de la relation (VI) appliquée à (b_2, b_3, α)

$$u_1(b_2, b_3, \alpha_{0,1}) \equiv [-1]^{n_\alpha - 1}.$$

Par suite, la première congruence devient

$$[-1]^{n_\alpha - 1}(b_1) + u_1(b_3, \alpha_{0,1}) \equiv 0$$

et donne la valeur de b_1.

92. *Avec une suite quelconque d'éléments β on peut toujours former un unitaire congr. en ajoutant quatre éléments (Syst. alt.).*

En effet, pour que

$$(\lambda) = (a_1, a_2, a_3, a_4, \beta)$$

soit un unitaire congr., il suffit (n° 91) que le plus grand commun diviseur S, en valeur absolue, de (a_4, β) et du module t divise

$$(\beta) - u_1 \qquad [u_1 = ui^{n_\beta}, \; u = \pm 1];$$

en d'autres termes, que a_4 admette au moins une valeur telle que cette condition soit satisfaite.

Donnons à a_4 la composition suivante :

$$a_4 = \text{APQ},$$

dans laquelle :

A représente un nombre premier avec t;

P, un produit formé avec tous les facteurs premiers de t qui n'appartiennent pas à $(\beta_{1,0})$, affectés d'exposants quelconques, $\geqq 0$ si ces facteurs appartiennent aussi à (β), > 0 dans le cas contraire;

Q, un produit formé avec tous les facteurs communs à t, $(\beta_{1,0})$, $(\beta) - u_1$, affectés d'un exposant plus petit que ceux qu'ils ont dans chacun des deux derniers nombres.

Dans l'égalité

$$(a_4, \beta) = (a_4)(\beta) + (\beta_{1,0}),$$

tout facteur de t premier avec Q divise une seule des deux parties du second nombre et, par suite, est premier avec (a_4, β).

Tout facteur de Q entre dans (a_4, β) avec l'exposant qu'il a dans Q et qui est plus petit que dans $(\beta) - u_1$.

Pour une telle valeur de a_4, la question se trouve par conséquent résolue, puisque le plus grand commun diviseur S de (a_4, β) et de t n'est autre que Q et divise $(\beta) - u_1$.

93. *Cas particuliers. Unitaires congr.* (λ) *pour lesquels* $n_\lambda \leqq 5$ (*Syst. alt.*). — On trouve facilement que :

1° Les seuls unitaires congr. composés de *deux* ou de *trois* éléments sont les unitaires $(0,0)$, $(1,1,1)$, $(-1,-1,-1)$.

2° Ceux de *quatre* éléments sont de l'une des deux formes suivantes :

$$(a,\ b,\ -a,\ -b) \quad \text{avec} \quad ab \equiv 0,$$
$$(a,\ b,\ \ a,\ \ b) \quad \text{avec} \quad ab \equiv 2.$$

Ces unitaires congr. se ramènent d'ailleurs par transformation (T_{10}) (n° 16) aux unitaires

$$(0,\ m,\ 0,\ -m),$$
$$(1,\ 2,\ 1,\ \ 2).$$

3° Ceux de *cinq* éléments sont de l'une des trois formes suivantes :

$$(a,\ a,\ a,\ a,\ a),$$
$$(a,\ a,\ b,\ c,\ b),$$
$$(a,\ b,\ c,\ d,\ e),$$

les éléments a, b, c, d, e n'étant pas congrus entre eux.

Si l'on représente l'un de ces unitaires congr. par $(a_1,\ a_2,\ a_3,\ a_4,\ a_5)$, la relation (C_1) (n° 90) montre que les éléments sont liés par cinq congruences semblables à celle-ci :

$$a_2 \equiv u(-a_4 a_5 + 1).$$

Lorsque tous les éléments sont égaux, c'est le cas de la première forme ; on a

$$a \equiv u(-a^2 + 1),$$

d'où

$$(2a + u)^2 \equiv 5.$$

5 est résidu quadratique du module.

Soit, par exemple, $t = 41$.

$$(6,\ 6,\ 6,\ 6,\ 6),$$
$$(5,\ 5,\ 7,\ 17,\ 7),$$
$$(4,\ 7,\ 32,\ 14,\ 23)$$

sont des unitaires congr. (mod 41).

Remarque. — Les unitaires congr. dont certains éléments sont égaux à 0, ± 1 se réduisent à de plus simples par les procédés précédemment indiqués.

94. *Réduction des continuants et des adjoints*

(*Syst. alt.*). — Il reste à montrer comment s'opère la réduction d'un continuant quelconque, c'est-à-dire sa transformation en un autre de valeur absolue congrue à celle du premier et composé avec un nombre moindre d'éléments.

La même opération s'applique aussi aux adjoints.

Soit (α, β, γ) le continuant donné, dans lequel β est composé de trois éléments au moins.

Formons, comme au n° 92, au moyen de cette suite, un unitaire congr. $(\lambda) = (a_1, a_2, a_3, a_4, \beta)$.

On peut écrire

$$(\alpha, \beta, \gamma) = (\alpha, 0, -a_4, -a_3, -a_2, -a_1, 0, a_1, a_2, a_3, a_4, \beta, \gamma),$$

et, en supprimant λ, on a

$$(\alpha, \beta, \gamma) \equiv u_1(\alpha, 0, -a_4, -a_3, -a_2, -a_1, 0, \gamma).$$

Ce dernier continuant est congru au premier en valeur absolue et contiendra moins d'éléments que lui après élimination des deux zéros.

Remarques. — 1° La réduction s'obtient encore par un procédé semblable lorsque β est composé seulement de deux éléments et appartient à une suite unitaire congr. de cinq éléments.

2° Lorsque le continuant donné est (β) (α, γ s'évanouissant), sa valeur absolue se réduit à un nombre congru à (a_2, a_3), ainsi qu'il résulte de la dernière congruence.

Cette relation est aussi une conséquence de la formule (C_1) (n° 90), puisque $(a_1, a_2, a_3, a_4, \beta)$ est un unitaire congr.

Elle pourrait être prise comme point de départ pour la recherche des éléments a_1, a_2, a_3, a_4 qui, joints à une suite donnée β, forment un unitaire congru.

(*A suivre.*)