III. CONGRUENCES DE DEGRÉ ARBITRAIRE

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **13 (1967)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **12.07.2024**

où la somme est étendue aux décompositions de l'entier j de la forme (20) [1]).

Exemples : Pour $n = 4$, les fonctions K_4, K_5 et K_6 sont:

$$K_4 = v_1^4 + 3v_1^2 v_2 + 2v_1 v_3 + v_2^2 + v_4$$
$$K_5 = v_1^5 + 4v_1^3 v_2 + 3v_1^2 v_3 + 3v_1 v_2^2 + 2v_1 v_4 + 2v_1 v_4 + 2v_2 v_3$$
$$K_6 = v_1^6 + 5v_1^4 v_2 + 4v_1^3 v_3 + 6v_1^2 v_2^2 + 3v_1^2 v_4 + 6v_1 v_2 v_3 + v_2^3 + 2v_2 v_4 + v_3^2 .$$

Pour $n = 5$, la fonction K_{12} (avec $v_1 = 0$) est:

$$K_{12} = v_4^3 + 12v_2 v_3^2 v_4 + 6v_2^2 v_4^2 + 5v_2^4 v_4 + v_3^4 + v_2^6 + 10v_2^3 v_3^2 + 3v_5^2 v_2 + 6v_5 v_3 v_4 + 12v_5 v_3 v_2^2 .$$

III. Congruences de degré arbitraire

On cherche les conditions que doivent vérifier les entiers $v_1, v_2, ..., v_{n+1}$ pour que la congruence:

$$X^{n+1} - v_1 X^n - v_2 X^{n-1} - ... - v_{n+1} \equiv 0 , \qquad (N) , \qquad (22)$$

où N est un entier premier, ait $n + 1$ solutions entières et distinctes.

Le théorème de Fermat montre que, si les racines θ de cette congruence sont entières, elles vérifient la congruence:

$$\theta^{N-1} \equiv \theta , \qquad (N) . \qquad 23)$$

Les fonctions K_j vérifient alors, pour toutes les valeurs entières positives, négatives ou nulles de j, les congruences:

$$K_{j+N-1} \equiv K_j , \qquad (N) . \qquad (24)$$

Inversement, si $n + 1$ fonctions K_{i+j} vérifient la congruence (24), les racines θ de la congruence (22), vérifient toutes la congruence de Fermat (23) et par suite sont entières. Les fonctions K_j ont d'ailleurs été choisies de manière que les conditions les plus simples correspondent aux valeurs entières de i de $- n$ à 0.

Ainsi, les congruences:

$$K_{N-n} \equiv 0 , \quad K_{N-n-1} \equiv 0 , \quad \dots , \quad K_{N-2} \equiv 0 , \quad K_{N-1} , \quad (N) , \qquad (25)$$

1) *Loc. cit.*, p. 135, où la formule est établie seulement pour $v1 = 0$, mais peut être généralisée facilement. Voir aussi Glenisson et Derdvidue, *Mathesis* (1960).

sont des conditions nécessaires et suffisantes pour que la congruence (22) ait $n + 1$ solutions entières et distinctes.

Il est facile de constater, d'un côté que n des relations (25) entraînent la $(n + 1)^{\text{me}}$, de l'autre que l'éventualité $\nu_1 = 0$ apporte de notables simplifications dans ces relations [1]).

Le cas de $n + 1 = 2$ présente un intérêt particulier. Dans le cas général, les relations (25) se réduisent alors à deux expressions identiques. C'est ainsi que, pour $N = 7$, ces deux relations sont:

$$4_1^4 + 4v_1^2 v_2 + 3v_2^2 \equiv 0 \,, \qquad (7)\,.$$

D'autre part, si $\nu_1 \equiv 0, (N)$, la relation $K_{N-2} \equiv 0, (N)$, est toujours vérifiée, parce qu'elle contient ν_1 en facteur, tandis que la relation $K_{N-1} \equiv 1, (N)$, se réduit à:

$$v_2{}^{(N-1)/2} \equiv 1 \,, \qquad (N)\,.$$

Ce qui est la relation classique de Gauss, pour les restes quadratiques suivant le module N, dont les formules (25) apparaissent ainsi comme une généralisation aux congruences d'une variable de degré quelconque.

Exemples : Pour $n = 3$ et $N = 7$, la congruence (22) a pour solutions 1, 2 et 3 si ses coefficients sont égaux à:

$$v_1 \equiv 1 \,, \qquad v_2 \equiv 3 \,, \qquad v_3 \equiv 3 \,, \qquad (7)\,.$$

Ces coefficients vérifient les congruences:

$$K_4 \equiv 0 \,, \qquad K_5 \equiv 0 \,, \qquad K_6 \equiv 1 \,, \qquad (7)\,.$$

Pour $n = 3$ et $N = 11$, la congruence (22) a pour solutions 1, 2 et 3 si:

$$v_1 \equiv 5 \,, \qquad v_2 \equiv 0 \,, \qquad v_3 \equiv 5 \,, \qquad (11)\,.$$

Ces coefficients vérifient les congruences:

$$\begin{aligned} K_8 = {} & v_1^8 + 7v_1^6 v_2 + 6v_1^5 v_3 + 15v_1^4 v_2^2 + 20\,v_1^3 v_2 v_3 + 10v_1^2 v_2^3 + 6v_1^2 v_3^2 \\ & + 12v_1 v_2^2 v_3 + v_2^4 + 3v_2 v_3^2 \equiv 0 \,, \qquad (11) \end{aligned}$$

$$\begin{aligned} K_9 = {} & v_1^9 + 8v_1^7 v_2 + 7v_1^6 v_3 + 21v_1^5 v_2^2 + 30v_1^4 v_2 v_3 + 20v_1^3 v_2^3 + 10v_1^3 v_3^2 \\ & + 30v_1^2 v_2^2 v_3 + 5v_1 v_2^4 + 12v_1 v_2 v_3^2 + 4v_2^3 v_3 + v_3^3 \equiv 0 \,, \quad (11) \end{aligned}$$

---

1) Si $n + 1 = 3$ et $\nu 1 = 0$, il n'y a plus dans le cas général qu'une seule relation pour en entraîner les deux autres, cf. (13) et (14).

$$K_{10} = v_1^{10} + 9v_1^8 v_2 + 8v_1^7 v_3 + 28v_1^6 v_2^2 + 42v_1^5 v_2 v_3 + 35v_1^4 v_2^3 + 15v_1^4 v_3^2$$
$$+ 60v_1^3 v_2^2 v_3 + 15v_1^2 v_2^4 + 20v_1 v_2^3 v_3 + 4v_1 v_3^3$$
$$+ 30v_1^2 v_2 v_3^2 + v_2^5 + 6v_2^2 v_3^2 \equiv 1 \,. \qquad (11)$$

Pour $n = 4$ et $N = 17$, la congruence:

$$X^5 - v_2 x^3 - v_3 X^2 - v_4 X - v_5 \equiv 0 \,, \qquad (17) \,,$$

a 5 solutions entières et distinctes dans les deux seuls cas suivants:

$$v_2 \equiv 14\lambda^2 \,, \qquad v_3 \equiv 11\lambda^3 \,, \qquad v_4 \equiv 0 \,, \qquad v_5 \equiv 2\lambda^5 \,, \qquad (17) \,,$$

ou

$$v_2 \equiv 12\lambda^2 \,, \qquad v_3 \equiv 16\lambda^3 \,, \qquad v_4 \equiv 12\lambda^4 \,, \qquad v_5 \equiv 7\lambda^5 \,, \qquad (17) \,,$$

où λ est un entier arbitraire. Ces systèmes de coefficients vérifient notamment la relation donnée au paragraphe II ci-dessus (exemples).

VI. Remarques sur les partitions de l'indice j

Il peut être utile de contrôler le nombre total de termes dans l'expression de la fonction $K_j\,(v_1, v_2, \ldots, v_{n+1})$, lorsqu'on la calcule par la formule (19). Ce nombre est égal au nombre de partitions de l'indice j de la forme (20).

On peut pour celà construire un tableau triangulaire T, défini de la façon suivante:

On fait correspondre à la colonne de rang i le coefficient v_i de l'équation (16) d'indice i. A la ligne de rang j, on fait correspondre l'indice j de la fonction K_j considérée.

A l'intersection de la ligne de rang j et de la colonne de rang i, on porte le nombre de termes de l'expression de K_j ayant v_i comme facteur d'indice maximum.

Le nombre de termes de la fonction K_j, d'indice j, correspondant à une équation (16) de degré $n + 1$, est alors la somme des $n + 1$ premiers termes de la ligne de rang j.

On peut construire le tableau T par récurrence, ligne par ligne: l'élément appartenant à la ligne de rang j et à la colonne de rang i est égal à la somme des i premiers termes de la ligne de rang $j - i$.