Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 13 (1967)

Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: AU SUJET DES CONGRUENCES DE DEGRÉ SUPÉRIEUR A DEUX

Autor: Thouvenot, S. / Chatelet, F.

Kapitel: II. Sommes des puissances des racines d'une équation algébrique

DOI: https://doi.org/10.5169/seals-41529

L'une ou l'autre des deux congruences:

$$w^3 + 7t^2 \equiv 0 \qquad ou \qquad w^3 + 8t^2 \equiv 0, \qquad (17)$$

entraîne que:

$$K_{16}(w, t) = w^8 + 21\,w^5 t^2 + 15\,w^2 t^4 \equiv 1, \qquad (17)$$

Pour l'entier premier $N = 31$, le quotient:

$$K_{28}(w, t)/w = w^{12} + 3.26\,w^9 t^2 + 5.99\,w^6 t^4 + 7.66\,w^3 t^6 + 9.5\,t^8$$

se décompose, dans le corps des restes d'entiers suivant le module 31 en le produit:

$$(w^3 + 12t^2)(w^3 + 16t^2)(w^3 + 18t^2)(w^3 + 25t^2).$$

II. Sommes des puissances des racines d'une équation algébrique

Pour généraliser facilement les résultats précédents, il est commode d'utiliser les sommes S_j des puissances des racines d'une équation algébrique:

$$X^{n+1} - v_1 X^n - v_2 X^{n-1} - \dots - v_{n+1} = 0, \qquad (16)$$

pour les exposants entiers j, tant positifs que négatifs ou nuls, et les combinaisons linéaires de ces sommes S_j.

Si on considère la puissance θ^j d'une racine θ de l'équation (16), d'exposant j entier positif, négatif ou nul, comme une fonction $f(j)$ de l'exposant j, cette fonction vérifie la relation de récurrence:

$$f(j) = \Sigma(v_i f(j-i)), \qquad (17)$$

où la somme est étendue aux valeurs entières de i de 1 à $n + 1$. Toute combinaison linéaire de plusieurs solutions de la relation de récurrence (17) vérifie aussi cette relation; en particulier, les sommes S_j des puissances d'exposant j des racines de l'équation (16) vérifie la relation:

$$S_j = \Sigma(v_i S_{j-i}).$$

De façon plus précise, on peut déterminer de manière unique une solution de la relation (17) qui prend des valeurs données pour n valeurs de la variable j; elle peut être exprimée comme combinaison linéaire de n solutions particulières de la relation (17), pourvu que ces solutions soient linéairement indépendantes.

En particulier, on peut déterminer une combinaison linéaire:

$$K_j(v_1, v_2, \ldots, v_{n+1}) = a_1\,\theta_1^j + a_2\,\theta_2^j + \ldots + a_{n+1}\,\theta_{n+1}^j$$

des puissances d'exposant j des racines de l'équation (16) telle que:

$$K_0 = 1\,, \quad K_{-1} = 0\,, \quad K_{-2} = 0\,, \ldots, \quad K_{-n} = 0\,. \qquad (18)$$

La fonction K_j est déterminée de manière unique, pourvu que l'équation (16) n'ait pas de racine multiple. Inversement, les fonctions $f(j) = \theta^j$, pour chaque racine θ de l'équation (16), peuvent être exprimées comme combinaisons linéaires de $n + 1$ fonctions K_{i+j}, par exemple pour les valeurs $0, 1, \ldots, n$ de l'indice i.

Les fonctions $K_j(v_1, v_2, \ldots, v_{n+1})$ peuvent être calculées, à partir des valeurs initiales (18), au moyen de la formule de récurrence (17). Elles peuvent aussi, pour les valeurs positives des indices j, être exprimées en fonction de $v_1, v_2, \ldots, v_{n+1}$ par la formule:

$$K_j(v_1, v_2, \ldots, v_{n+1}) = \Sigma\left(\frac{(j_1 + j_2 + \ldots + j_{n+1})\,!}{j_1\,!\,j_2\,!\ldots j_{n+1}\,!}\,v_1^{j1}\,v_2^{j2}\ldots v_{n+1}^{jn+1}\right) \qquad (19)$$

où la somme est étendue à toutes les décompositions de l'entier j en sommes de la forme:

$$j = j_1 + 2j_2 + 3j_3 + \ldots + (n+1)\,j_{n+1} \qquad (20)$$

avec $j_1, j_2, \ldots, j_{n+1}$ entiers positifs ou nuls.

Les sommes S_j, ou plus généralement les fonctions S_{i+j} de l'indice j, pour i fixe, peuvent être exprimées comme combinaisons linéaires des fonctions K_j par la formule:

$$S_{i+j} = u_0\,K_j + u_1\,K_{j-1} + \ldots + u_n\,K_{j-n}$$

où les coefficients $u_0, u_1, \ldots, u_n$ sont déterminés par les relations:

$$S_i = u_0\,, \quad S_{i+1} = u_0\,K_1 + u_1\,, \quad S_{i+2} = u_0\,K_2 + u_1\,K_1 + u_2\,,$$
$$\ldots, \quad S_{i+n} = u_0\,K_n + u_1\,K_{n-1} + \ldots + u_n\,.$$

Elles peuvent aussi être calculées, pour les entiers positifs j, en fonction de $v_1, v_2, \ldots, v_{n+1}$ par la formule:

$$S_j = j\,\Sigma\left(\frac{(j_1 + j_2 + \ldots + j_{n+1} - 1)\,!}{j_1\,!\,j_2\,!\ldots j_{n+1}\,!}\,v_1^{j1}\,v_2^{j2}\ldots v_{n+1}^{jn+1}\right) \qquad (21)$$

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:

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

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).