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

# AU SUJET DES CONGRUENCES DE DEGRÉ SUPÉRIEUR A DEUX

par S. THOUVENOT et F. CHATELET

SOMMAIRE

La recherche des conditions pour qu'un polynôme d'une seule variable, à coefficients entiers rationnels, se décompose, dans le corps des restes des entiers suivant un module $N$ premier, en produit de facteurs linéaires (ou pour qu'une congruence de degré $n$, suivant le module $N$, ait $n$ solutions entières et distinctes), est un problème classique. La théorie des restes quadratiques en donne une solution complète pour les polynômes du second degré. Mais les solutions, qui ont été proposées jusqu'à présent pour les polynômes de degrés supérieurs à deux, ne sont pas entièrement satisfaisantes.

Dans une publication antérieure [1]), l'un des auteurs avait étudié ce problème pour les polynômes du troisième degré par une méthode particulièrement élémentaire. Après avoir résumé et complété les résultats ainsi obtenus, on généralise ici cette méthode aux polynômes de degrés arbitraires.

## I. CONGRUENCES DU TROISIEME DEGRÉ SANS SECOND TERME

On cherche les conditions que doivent vérifier les entiers $w$ et $t$ pour que la congruence:

$$\varphi_3(X) = X_3 - wX - t \equiv 0\,, \qquad (N)\,. \qquad (1)$$

où N est un entier premier, ait trois solutions entières et distinctes. Dans une publication antérieure [2]), on a exploré ce problème par trois voies conduisant à des résultats qui se complètent. On résume ici ces résultats en les présentant sous une forme légèrement différente et en y apportant quelques additions.

---

1) Cf. S. THOUVENOT: *Comptes rendus à l'Académie des Sciences*, t. 252 (1961), pp. 1890 et 2060 et *Publications scientifiques et techniques du Ministère de l Air* nº 388.

2) *Loc. cit.*, pp. 40 à 42, 42 à 44 et 59 à 63.

On désigne par $S_j$ la somme des puissances, d'exposant $j$ (entier positif), des racines du polynôme $\varphi_3(X)$. Il est classique que cette somme vérifie la relation de récurrence:

$$S_{j+3} = wS_{j+1} + tS_j , \qquad (2)$$

pour tous les entiers positifs $j$.

Le théorème de FERMAT montre que, si la congruence (1) a trois solutions entières, les sommes $S_j$ vérifient la relation:

$$S_{i+N-1} \equiv S_i , \qquad (N) , \qquad (3)$$

duel que soit l'entier positif $i$. On peut exprimer cette relation en fonction de $w$ et $t$, au moyen de la relation de récurrence (2) et montrer ensuite que les conditions obtenues pour les trois indices $i = 0$, 1 et 2 sont suffisantes pour l'existence de trois solutions entières et distinctes de la congruence (1).

Pour exprimer la relation (3) en fonction de $w$ et $t$, on peut en effet poser, pour un entier positif $i$ choisi arbitrairement:

$$S_i = u , \qquad S_{i+1} = 2x , \qquad S_{i+2} = 3y + uw . \qquad (4)$$

La formule de récurrence (2) montre alors que, pour tout entier positif $j$ supérieur ou égal à 2:

$$S_{i+j} = 3y\,K_{j-2} + 2x\,K_{j-1} + u\,K_j \qquad (5)$$

où $K_j$ est un polynôme en $w$ et $t$ qui se déduit des trois valeurs initiales:

$$K_0 = 1 , \qquad K_1 = 0 , \qquad K_2 = w , \qquad (6)$$

par la relation de récurrence:

$$K_{v+3} = w\,K_{v+1} + t\,K_v . \qquad (7)$$

On peut aussi calculer les coefficients du polynôme $K_j(w, t)$ par la formule:

$$K_j(w,t) = \sum \frac{(\lambda_2 + \lambda_3)!}{\lambda_2 !\,\lambda_3 !}\, w^{\lambda_2} t^{\lambda_3} , \qquad (8)$$

où la somme est étendue aux partitions de l'entier $j$ de la forme:

$$j = 2\lambda_2 + 3\lambda_3 , \qquad (9)$$

avec $\lambda_2$ et $\lambda_3$ entiers positifs ou nuls.

*Exemples :* Les partitions de l'entier 14 de la forme (9) sont:

$$14 = 2.7 = 2.4 + 3.2 = 2.1 + 3.4$$

et le polynôme $K_{14}(w, t)$ est:

$$K_{14}(w, t) = w^7 + 15\, w^4 t^2 + 5wt^4 .$$

Les partitions de l'entier 15 de la forme (9) sont:

$$15 = 2.6 + 3.1 = 2.3 + 3.3 = 3.5$$

et le polynôme $K_{15}(w, t)$ est:

$$K_{15}(w, t) = 7w^6 t + 20w^3 t^3 + t^5 .$$

En choisissant en particulier $j = N - 1$, les relations (3) et (5) montrent que:

$$S_{i+N-1} \equiv S_i \equiv 3y\, K_{N-3} + 2x\, K_{N-2} + u\, K_{N-1} , \qquad (N) , \tag{10}$$

ou encore:

$$(S_{i+2} - wS_i)\, K_{N-3} + S_{i+1}\, K_{N-2} + S_i\, K_{N-1} \equiv S_i , \qquad (N) . \tag{11}$$

Et, en utilisant les valeurs classiques des sommes des premières puissances des racines du polynôme $\varphi_3(X)$:

$$S_0 = 3 , \qquad S_1 = 0 , \qquad S_2 = 2w , \qquad S_3 = 3t , \qquad S_4 = 2w^2 , \tag{12}$$

les relations (11), correspondant aux indices $i = 0$, 1 et 2, s'écrivent:

$$\begin{aligned} - w\, K_{N-3} + 3\, K_{N-1} &\equiv 3 \\ 3t\, K_{N-3} + 2w\, K_{N-2} &\equiv 0 , \qquad (N) . \\ 3t\, K_{N-2} + 2w\, K_{N-1} &\equiv 2w \end{aligned} \tag{13}$$

L'ensemble de ces trois congruences forme un système linéaire, dans le corps des restes suivant le module premier $N$, en $K_{N-3}, K_{N-2}, K_{N-1}$, dont le déterminant est égal à $27\, t^2 - 4w^3$. Si ce déterminant n'est pas divisible par $N$, donc si la congruence (1) n'a pas de racine double, le système (13) a pour seule solution:

$$K_{N-3} \equiv 0 , \qquad K_{N-2} \equiv 0 , \qquad K_{N-1} \equiv 1 , \qquad (N) . \tag{14}$$

L'une quelconque de ces conditions entraîne d'ailleurs les autres, sauf peut-être si $w$ ou $t$ est nul — cf. (13).

D'autre part, la relation de récurrence (7) montre que, si $N - 5$ est divisible par 6, les quotients $K_{N-2}(w, t)/t$ et $K_{N-3}(w, t)/w$ sont des polynômes homogènes en $w^3$ et $t^2$ de degrés $(N - 5)/6$. Si $N - 7$ est divisible par 6, les quotients $K_{N-2}(w, t)/wt$ et $K_{N-3}(w, t)/w^2$ sont des polynômes homogènes en $w^3$ et $t^2$ de degrés $(N - 7)/6$.

L'étude directe des congruences (1) conduit à grouper celles de ces congruences pour lesquelles le rapport $\alpha = w^3/t^2$ est le même. En particulier, les congruences (1) qui ont trois solutions entières, non nulles et distinctes se répartissent en $(N - 5)/6$, ou $(N - 7)/6$ groupes de cette espèce, suivant le reste de $N$ pour le module 6 [1]). Il en résulte que les quotients $K_{N-3}(w, t)/w$ et $K_{N-2}(w, t)/t$, ou $K_{N-3}(w, t)/w^2$ et $K_{N-2}(w, t)/w^2$, se décomposent en produits de $(N - 5)/6$, ou de $(N - 7)/6$, facteurs de la forme:

$$w^3 - \alpha_i t^2$$

correspondants aux groupes précédents.

Ainsi, si $w$ et $t$ ne sont pas divisibles par $N$, l'une des trois congruences équivalentes:

$$K_{N-3}(w, t)/w \equiv 0, \qquad K_{N-2}(w, t)/t \equiv 0, \qquad K_{N-1}(w, t) \equiv 1, \qquad (N)$$

si $\qquad N - 5 \equiv 0, \qquad (6) \qquad (15)$

ou

$$K_{N-3}(w, t)/w^2 \equiv 0, \qquad K_{N-2}(w, t)/wt \equiv 0, \qquad K_{N-1}(w, t) \equiv 1, \qquad (N)$$

si $\qquad N - 7 \equiv 0, \qquad (6), \qquad (15\,bis)$

est une condition nécessaire et suffisante pour que la congruence (1) ait trois solutions entières, non nulles et distinctes.

*Exemples:* Pour l'entier premier $N = 17$, les conditions

$$K_{14}(w, t)/w = w^6 + 15\,w^3 t^2 + 5\,t^4 \equiv 0, \qquad (17)$$
$$K_{15}(w, t)/t = 7\,w^6 + 20\,w^2 t^2 + t^4 \equiv 0, \qquad (17)$$

sont équivalentes et leurs premiers membres se décomposent, dans le corps des restes des entiers suivant le module 17, à un facteur constant près en le produit:

$$(w^3 + 7\,t^2)(w^3 + 8\,t^2).$$

1) *Loc. cit.*, p. 45.

L'une ou l'autre des deux congruences:

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

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:

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

## 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:

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

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 $\theta^j$ d'une racine $\theta$ 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:

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

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

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

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 $\theta$ de l'équation (16), peuvent être exprimées comme combinaisons linéaires de $n + 1$ fonctions $K_{i+j}$, par exemple pour les valeurs 0, 1, ..., $n$ 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:

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

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

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

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:

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

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 $v_1, v_2, \ldots, v_{n+1}$ pour que la congruence:

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

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

Le théorème de Fermat montre que, si les racines $\theta$ 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 $\theta$ 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:

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

---

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 $(n + 1)^{me}$, de l'autre que l'éventualité $v_1 = 0$ 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 $v_1 \equiv 0, (N)$, la relation $K_{N-2} \equiv 0, (N)$, est toujours vérifiée, parce qu'elle contient $v_1$ 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:

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

$$K_9 = v_1^9 + 8v_1^7 v_2 + 7v_1^6 v_3 + 21v_1^5 v_2^2 + 30v_1^4 v_2 v_3 + 20v_1^3 v_2^3 + 10v_1^3 v_3^2 + 30v_1^2 v_2^2 v_3 + 5v_1 v_2^4 + 12v_1 v_2 v_3^2 + 4v_2^3 v_3 + v_3^3 \equiv 0 , \qquad (11)$$

1) Si $n + 1 = 3$ et $v1 = 0$, 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 $\lambda$ 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 $K_j (v_1, v_2, ..., v_{n+1})$, 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 $j - i$.

TABLEAU T

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | | | | | | | | | |
| 2 | 1 | 1 | | | | | | | | |
| 3 | 1 | 1 | 1 | | | | | | | |
| 4 | 1 | 2 | 1 | 1 | | | | | | |
| 5 | 1 | 2 | 2 | 1 | 1 | | | | | |
| 6 | 1 | 3 | 3 | 2 | 1 | 1 | | | | |
| 7 | 1 | 3 | 4 | 3 | 2 | 1 | 1 | | | |
| 8 | 1 | 4 | 5 | 5 | 3 | 2 | 1 | 1 | | |
| 9 | 1 | 4 | 7 | 6 | 5 | 3 | 2 | 1 | 1 | |
| 10 | 1 | 5 | 8 | 9 | 7 | 5 | 3 | 2 | 1 | 1 |

(Reçu le 15 mars 1967)

S. Thouvenot
17, rue Raynouard
Paris (16)

Prof. F. Châtelet
11, rue Jules Haag
Besançon