I. CONGRUENCES DU TROISIEME DEGRÉ SANS SECOND TERME

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 λ_2 et λ_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 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.