196. Sur le Nombre des Valeurs Distinctes d'un Polynôme à Coefficients dans un Corps Fini

Par Saburô UCHIYAMA
Institut Mathématique, Université Métropolitaine, Tokyo
(Comm. by Z. SUETUNA, M.J.A., Dec. 13, 1954)

Étant donnés un polynôme $f(X)$ de degré $n \geqq 2$ à coefficients entiers rationnels et un nombre m entier positif, nous désignerons par $W(m)$ le nombre des valeurs $f(k)$ $(k=0, 1, \ldots, m-1)$, incongrues par rapport au module m. Comme on voit facilement la fonction $W(m)$ peut s'écrire sous la forme

$$W(m)=m\sum_{u=0}^{m-1}\left(\sum_{t=0}^{m-1}\sum_{v=0}^{m-1}\exp\left\{2\pi i\frac{t}{m}(f(u)-f(v))\right\}\right)^{-1}$$

et elle est multiplicative, c'est-à-dire pour deux nombres m_1 et m_2 entiers positifs, $(m_1, m_2)=1$ entraîne $W(m_1m_2)=W(m_1)W(m_2)$.

Dans la théorie des nombres il serait intéressant de déterminer en général la valeur de $W(m)$ pour les polynômes donnés à coefficients entiers. MM. R. D. von Sterneck et R. Kantor ont résolu complètement ce problème pour les polynômes cubiques, aussi bien pour ceux qui sont quadratiques,[1] mais on ne sait pas encore suffisamment trouver la valeur de $W(m)$ au cas particulier où m est un nombre premier,[2] pour tels polynômes de degré au moins 4.

p étant un nombre premier impair, nous étudierons dans la suite la valeur de la fonction $W(p)$ pour quelques polynômes, en établissant une borne inférieure pour $W(p)$ quand p tend à l'infinité, et considérons en même temps, dans les corps de nombres algébriques finis, un tel problème analogue dont les modules sont des idéaux premiers de ces corps algébriques.

1. A l'aide de la notion des *corps finis* on peut simplifier et unifier toute la considération dans ce qui suit.

Soit maintenant F_q un corps fini à $q=p^\nu$ éléments, où p est un nombre premier impair et $\nu \geqq 1$. Étant donné un polynôme $f(X)$ de degré n dont les coefficients appartiennent à un corps F_q fixe, nous désignerons par $V(q)$ le nombre des valeurs distinctes $f(x)$, $x \in F_q$. Sans rien perdre de la généralité on peut supposer ici que le polynôme soit unitaire, c'est-à-dire que son coefficient dominant soit égal à l'unité.

1) R. Kantor: Ueber die Anzahl incongruenter Werte ganzer rationaler Funktionen, Monatshefte Math. Phys., **26**, 24-39 (1915).

2) Cf. S. Chowla: The Riemann zeta and allied functions, Bull. Amer. Math. Soc., **58**, 301 (1952). On a trivialement $W(p)>p/n$.