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 $W(p)>p/n$.

Il est facile de montrer que:

1° si $n=2$ et $f(X)=X^2+aX+b$, a, $b \in F_q$ $(p \neq 2)$. on a

$$V(q)=\frac{q+1}{2},$$

et

2° si $n=3$ et $f(X)=X^3+aX^2+bX+c$, a, b et $c \in F_q$ $(p \neq 2, 3)$, on a

$$V(q)=\begin{cases} q & (a^2-3b=0 \text{ et } q \equiv -1 \pmod 3), \\ \dfrac{q+2}{3} & (a^2-3b=0 \text{ et } q \equiv 1 \pmod 3), \\ \dfrac{2q-1}{3} & (a^2-3b \neq 0 \text{ et } q \equiv -1 \pmod 3), \\ \dfrac{2q+1}{3} & (a^2-3b \neq 0 \text{ et } q \equiv 1 \pmod 3). \end{cases}$$

2. Pour le cas où $n \geqq 4$ nous démontrons le résultat que voici:

Théorème. *Soit $f(X) \in F_q[X]$ un polynôme de degré $n \geqq 4$ pour lequel le polynôme $f^*(u, v)=(f(u)-f(v))/(u-v)$ est absolument irréductible.*[3] *Alors, on a l'inégalité*

$$V(q) > \frac{q}{2}$$

pour tout nombre premier p assez grand.

Remarque 1. Si un polynôme $P(u, v)$ à coefficients dans un corps de nombres algébriques fini est absolument irréductible, il est aussi absolument irréductible modulo un idéal premier du corps algébrique, sauf au cas d'un nombre fini d'idéaux premiers.[4]

Remarque 2. Si nous faisions tomber l'hypothèse dans le théorème que le polynôme $f^*(u, v)$ soit absolument irréductible, nous ne pourrions conclure en général que $V(q)>q/2$ pour *tout* nombre premier p assez grand. En effet, pour $f(X)=X^4-X^2+1$ on a $f^*(u, v)=(u+v)(u^2+v^2-1)$ et il y a une infinité de nombres premiers p tels que $V(q) \leqq (q-1)/2$. Il existe encore un autre exemple plus critique. Considérons le polynôme $f(X)=X^3+aX^2+bX+c$ (a, b et $c \in F_q$): on aura

$$f^*(u, v)=u^2+uv+v^2+a(u+v)+b.$$

La condition nécessaire et suffisante pour ce $f^*(u, v)$ soit absolument irréductible est naturellement que $a^2-3b \neq 0$ dans l'F_q. Par conséquent, si $a^2-3b=0$ le polynôme $f^*(u, v)$ se réduit en deux facteurs linéaires et, comme on a déjà vu, on aura $V(q)=(q+2)/3$ pour tout $q \equiv 1 \pmod 3$.

3) C'est-à-dire, irréductible dans le corps de tous nombres algébriques par rapport à F_q.

4) A. Ostrowski: Zur arithmetischen Theorie der algebraischen Grössen, Gött. Nachr., 296 (1919). Cf. E. Noether: Ein algebraisches Kriterium für absolute Irreduzibilität, Math. Ann., **85**, 26-33 (1922).

3. Or, nous allons tirer brièvement une seule esquisse de notre démonstration pour le théorème mentionné au-dessus, car son raisonnement détaillé se paraîtra ailleurs.

Soit $q=p^{\nu}$ une puissance d'un nombre premier impair, et soit $f(X)\in F_q[X]$ un polynôme de degré $n\geqq 4$: si M_r $(1\leqq r\leqq n)$ désigne le nombre des $m\in F_q$ pour lesquels l'equation $f(x)=m$ ait exactement r racines dans l'F_q, on a alors par definition

$$V(q)=\sum_{r=1}^{n} M_r \tag{3.1}$$

et

$$q=\sum_{r=1}^{n} rM_r. \tag{3.2}$$

Si, en outre, on désigne par N_1 et N_2 les nombres des solutions (x, y) et (u, v), dans l'F_q, respectivement des équation

$$f(x)-f(y)=0 \text{ et } f^*(u, v)=0,$$

on a evidemment

$$N_1=\sum_{r=1}^{n} r^2M_r=q+N_2+O(1). \tag{3.3}$$

D'après un résultat dû à M. A. Weil[5] on obtient

$$N_2=q+O(q^{\frac{1}{2}}), \tag{3.4}$$

quand le polynôme $f^*(u, v)$ est absolument irréductible. Par conséquent, de l'inégalité

$$2(N_1\cdot V(q)-q^2)\geqq(\sum_{r=1}^{n} M_r)^2-\sum_{r=1}^{n} M_r^2 \tag{3.5}$$

il résulte aussitôt que, si le polynôme $f^*(u, v)$ est absolument irréductible, il y a deux constantes c_1 et c_2 (>0) indépendantes de q telles que

$$V(q)>\frac{q}{2}-c_1q^{\frac{1}{2}} \tag{3.6}$$

pour tout nombre premier $p>c_2$, puisque l'on a $(\sum M_r)^2-\sum M_r^2\geqq 0$.

4. Il est obligatoire d'apporter un lemme auxiliaire:

Lemme. Si l'on a $V(q)<q/2$ pour $p>c_2$, il y a alors une constante $\delta(>0)$ indépendante de q telle que $M_2<(1/2-\delta)q$.

Pour démontrer ce lemme nous utilisons les fonctions L[6] spécialement définies dans le corps F_q.

5. Nous allons maintenant conclure la démonstration de notre théorème.

Faisons la supposition que $V(q)<q/2$ pour quelque nombre premier p assez grand. Nous posons $M_{r_0}=\max_{1\leqq r\leqq u} M_r$: il convient de

5) A. Weil: Sur les courbes algébriques et les variétés qui s'en déduisent, Actual. Scientif. Industr. 1041, Paris, 1948. Voir aussi: H. Hasse: Ueber die Kongruenzzetafunktionen, Sitzungsberichte Berlin, 1934, § 9.

6) Voir S. Uchiyama: Sur les polynômes irréductibles dans un corps fini. I, Proc. Japan Acad., **30**, 523-527 (1954).

distinguer le cas de $r_0 \neq 2$ et celui de $r_0 = 2$.

i) $r_0 \neq 2$. Selon (3.1) et (3.2) on a

$$M_{r_0} < \left(\frac{1}{2} - \frac{1}{2n}\right)q,$$

et l'inégalité (3.5) devient, avec (3.6),

$$\begin{aligned} 2(N_1 \cdot V(q) - q^2) &\geqq (\sum M_r)^2 - M_{r_0}(\sum M_r) \\ &> \left(\frac{q}{2} - c_1 q^{\frac{1}{2}}\right)\left(\frac{q}{2n} - c_1 q^{\frac{1}{2}}\right) \end{aligned}$$

pour $p > c_2$. Mais cette dernière inégalité entraîne nettement $V(q) > q/2$ pour tout p assez grand, ce qui est en contradiction avec l'assomption.

ii) $r_0 = 2$. Dans ce cas, en vertu du lemme précédent, on arrivera encore à une contradiction par un raisonnement analogue à celui pour le cas où $r_0 \neq 2$.

Notre théorème se trouve ainsi démontré.