110. Sur les Polynômes Irréductibles dans un Corps Fini. I

Par Saburô UCHIYAMA
Institut Mathématique, Université Métropolitaine, Tokyo
(Comm. by Z. SUETUNA, M.J.A., July 12, 1954)

0. Introduction. Soit F_q un corps fini à $q=p^n$ éléments, où p est un nombre premier impair et $u>1$: en particulier, F_p sera considéré comme l'anneau quotient $Z/(p)$, Z étant l'anneau des entiers rationels. On dit qu'un polynôme $M(X)=\sum_{j=0}^{m}c_jX^{m-j}$ à coefficients dans F_q est *unitaire* si le coefficient dominant c_0 est égal à 1, et les coefficients $c_1,\ldots,c_r$ et les coefficients $c_{m-t+1},\ldots,c_m$ sont respectivement appelés les premiers r et les derniers t coefficients du polynôme $M(X)$. Nous désignerons par $\pi_q(m;\ r,\ t)$ $(0\leqslant r+t\leqslant m)$ le nombre des polynômes unitaires irréductibles dans $F_q[X]$, de degré m, tels que chacun des premiers r et derniers t coefficients en est fixe dans F_q: on peut admettre ici que le dernier coefficient de tels polynômes ne soit pas égal à 0, lorsque $t>0$. Il est bien connu que

$$\frac{\varphi(m)}{m-1}\frac{q^m-q}{m}\ll\pi_q(m;\ 0,\ 0)\ll\frac{q^m-q}{m},$$

et M. L. Carlitz a démontré que l'on a[1]

$$\pi_q(m;\ 1,\ 1)=\frac{1}{m}q^{m-2}+O(q^{m/2})\qquad(m\to\infty).$$

Nous considérons dans cette note le problème de déterminer la valeur de $\pi_q(m;\ r,\ t)$ principalement dans le cas où $n=1$, c'est-à-dire où $q=p$, pour quelques valeurs particulières de r, t. Mais, quel que soit $n\geqslant 1$, il est à peu près evident qu'on aura le

Théorème 1. *On a*

$$\pi_q(m;\ 0,\ 2)=\frac{1}{m}q^{m-2}+O(q^{m/2})\qquad(m\to\infty).$$

Ensuite de cela, nous démontrons le résultat suivant:

Théorème 2. *Si* $r+t\geqslant 2$ *on a*

$$\pi_p(m;\ r,\ t)=\frac{1}{m}p^{m-r-t}+O(p^{\theta m})\qquad(p>\max(r,\ t);\ m\to\infty),$$

où θ, $\frac{1}{2}\leqslant\theta<1$, *est une constante indépendante de* p, m.

Pour démontrer ces théorèmes, nous employons quelques fonctions L plus générales que celles introduites par M. Carlitz.[2]

1. Préliminaires. Soit $q=p^n$, p premier impair. Dans ce §,

1) L. Carlitz: A theorem of Dickson on irreducible polynomials, Proc. Amer. Math. Soc., **3**, 693-700 (1952). Il a aussi déterminé la valeur de π_q $(m;\ 1,0)$ etc.

2) Loc. cit., §§ 2 et 3.