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.

n ($\geqslant 1$) peut être un nombre naturel quelconque mais fixe.

Posons

$$\xi^{(k)}(x_0, x_1, x_2, \ldots, x_m) = k(-1)^k \sum_{\substack{\mu_j \geqslant 0 \\ \mu_0+\mu_1+\mu_2+\cdots+\mu_m=k \\ \mu_1+2\mu_2+\cdots+m\mu_m=k}} \frac{(-1)^{\mu_0}(k-\mu_0-1)!}{\mu_1!\,\mu_2!\cdots\mu_m!} x_0^{\mu_0}x_1^{\mu_1}x_2^{\mu_2}\cdots x_m^{\mu_m}$$

$$(1 \leqslant k < p,\ m=1, 2, \ldots).$$

Si $M=M(X)=\sum_{j=0}^{m} c_j X^{m-j}$ est un polynôme unitaire dans $F_q[X]$, nous allons définir pour $1 \leqslant k < p$ et $0 \leqslant \beta \leqslant q-1$

$$\lambda^{(k)}(M)=\lambda_\beta^{(k)}(M)=\begin{cases} 1 & (\deg M=0), \\ \exp\dfrac{2\pi i}{p} S(\beta\xi^{(k)}(M)) & (\deg M \geqslant 1,\ c_m \neq 0), \\ 0 & (\deg M \geqslant 1,\ c_m=0), \end{cases}$$

où S désigne la trace absolue et $\tilde{\lambda}^{(k)}(M)$ de la même manière avec $\tilde{\xi}^{(k)}(M)$ au lieu de $\xi^{(k)}(M)$ dans la définition de $\lambda^{(k)}(M)$, où

$$\xi^{(k)}(M)=\xi^{(k)}(1, c_1, \ldots, c_m),$$

$$\tilde{\xi}^{(k)}(M)=\xi^{(k)}\left(1, \frac{c_{m-1}}{c_m}, \ldots, \frac{c_0}{c_m}\right) \qquad (c_m \neq 0).$$

Il y a donc q fonctions $\lambda^{(k)}$ ou $\tilde{\lambda}^{(k)}$ pour chaque k, $1 \leqslant k < p$. D'autre part, l'indice étant défini par rapport à un élément primitif fixe dans F_q, nous posons pour $0 \leqslant \gamma \leqslant q-2$

$$\chi(M)=\chi_\gamma(M)=\begin{cases} \exp\dfrac{2\pi i}{p-1}\gamma \operatorname{Ind} c_m & (c_m \neq 0), \\ 0 & (c_m=0): \end{cases}$$

alors, il y a $q-1$ fonctions χ.

Lemme 1.1. Soient $A(X)$ et $B(X)$ deux polynômes unitaires quelconques dans $F_q[X]$. On a

$$\lambda^{(k)}(AB)=\lambda^{(k)}(A)\lambda^{(k)}(B),\ \tilde{\lambda}^{(k)}(AB)=\tilde{\lambda}^{(k)}(A)\tilde{\lambda}^{(k)}(B);\quad \chi(AB)=\chi(A)\chi(B).$$

Lemme 1.2. On a

$$\left.\begin{matrix} \sum_{\lambda^{(k)}} \lambda^{(k)}(M) \\ \sum_{\tilde{\lambda}^{(k)}} \tilde{\lambda}^{(k)}(M) \end{matrix}\right\} = \begin{cases} q \\ 0 \end{cases} \quad \left.\begin{matrix} \xi^{(k)}(M) \\ \tilde{\xi}^{(k)}(M) \end{matrix}\right\} = \begin{cases} 0 \\ \text{non } 0 \end{cases}, \ 1 \leqslant k < p\Big);$$

$$\sum_{\chi} \chi(M)=\begin{cases} q-1 & (c_m=1), \\ 0 & (c_m \neq 1). \end{cases}$$

Lemme 1.3. Soient $A(X)=\sum_{j=0}^{m} a_j X^{m-j}$ $(a_m \neq 0)$ et $B(X)=\sum_{j=0}^{m} b_j X^{m-j}$ deux polynômes unitaires dans $F_q[X]$. Alors: pour que soient $a_j=b_j$ $(j=1, \ldots, r;\ r<p)$, il faut et il suffit que l'on ait $\sum_{\lambda}^{(\kappa)} \lambda^{(k)}(A)\overline{\lambda^{(k)}}(B) \neq 0$ $(k=1, \ldots, r)$; pour que soient $a_j=b_j$ $(j=m-t+1, \ldots, m;\ t<p)$, il faut et il suffit que l'on ait $\sum_{\tilde{\lambda},\chi}^{(\kappa)} \tilde{\lambda}^{(k)}(A)\overline{\tilde{\lambda}^{(k)}}(B)\chi(A)\overline{\chi(B)} \neq 0$ $(k=1, \ldots, t-1)$.[3]

3) Dans ce qui suit, $\overline{\ }$ désigne le conjugué complexe.

Démonstration. On sait qu'il y a les formules suivantes:

$$a_j = \sum_{\substack{\mu_i \geqslant 0 \\ \mu_1+2\mu_2+\cdots+j\mu_j=j}} \prod_{i=1}^{j} (-\xi^{(i)}(A)/i)^{\mu_i}/\mu_i! \qquad (1 \leqslant j \leqslant r),$$

$$\frac{a_{m-j-1}}{a_m} = \sum_{\mu_i} \prod_{i=1}^{j-1} (-\tilde{\xi}^{(i)}(A)/i)^{\mu_i}/\mu_i! \qquad (a_m \neq 0;\ 2 \leqslant j \leqslant t).$$

On en déduit immédiatement notre lemme.

Écrivons maintenant pour un polynôme unitaire $M(X)$ dans $F_q[X]$, que $\lambda(M)=\prod_{k=1}^{r} \lambda^{(k)}(M)$, $\tilde{\lambda}(M)=\prod_{k=1}^{t-1} \tilde{\lambda}^{(j)}(M)$: en particulier, $\lambda_0(M) = \prod \lambda_0^{(k)}(M)$, $\tilde{\lambda}_0(M)=\prod \tilde{\lambda}_0^{(k)}(M)$.

Lemme 1.4. Si $m>r+t$ on a

$$\tau_m(\lambda, \tilde{\lambda}, \chi) = \sum_{\deg M = m} \lambda(M)\tilde{\lambda}(M)\chi(M) = 0,$$

sauf au cas où $\lambda=\lambda_0$, $\tilde{\lambda}=\tilde{\lambda}_0$ et $\chi=\chi_0$.

Nous posons

$$L(s, \lambda, \tilde{\lambda}, \chi) = \sum_{M \in F_q[X],\ \text{unitaire}} \lambda(M)\tilde{\lambda}(M)\chi(M)|M|^{-s} \qquad (s>1),$$

où $|M|=q^{\deg M}$. Alors, en vertu du lemme 1.4, on obtient

$$L(s, \lambda, \tilde{\lambda}, \chi) = 1 + \sum_{j=1}^{r+t} \frac{\tau_j(\lambda, \tilde{\lambda}, \chi)}{q^{js}} \qquad (\lambda \neq \lambda_0,\ \tilde{\lambda} \neq \tilde{\lambda}_0 \text{ ou } \chi \neq \chi_0).$$

2. Démonstration du théorème 1. Nous considérons les fonctions $L(s, \tilde{\lambda}^{(1)}, \chi)=L(s, \lambda_0, \tilde{\lambda}^{(1)}, \chi)$. Il résulte du lemme 1.1 qu'on a la décomposition d'Euler

$$L(s, \tilde{\lambda}^{(1)}, \chi) = \prod_P (1-\tilde{\lambda}^{(1)}(P)\chi(P)|P|^{-s})^{-1},$$

où P produit tous polynômes unitaires irréductibles dans $F_q[X]$.

Il est facile de voir que:

$$L(s, \tilde{\lambda}_0^{(1)}, \chi^0) = (1-q^{-s})(1-q^{1-s})^{-1},$$

$$L(s, \tilde{\lambda}_0^{(1)}, \chi) = 1 \qquad (\chi \neq \chi_0),$$

$$L(s, \tilde{\lambda}_0^{(1)}, \chi_0) = 1-q^{-s} \qquad (\tilde{\lambda}^{(1)} \neq \tilde{\lambda}_0^{(1)}),$$

et puis

$$|\tau_1(\tilde{\lambda}^{(1)}, \chi)| = |\tau_1(\lambda^{(1)}, \overline{\chi})| = q^{1/2} \qquad (\tilde{\lambda}^{(1)} \neq \tilde{\lambda}_0^{(1)},\ \chi \neq \chi_0).$$

On peut achever la démonstration du théorème 1 d'une manière très semblable au raisonnement de M. Carlitz,[4] selon les lemmes 1.2 et 1.3.

3. Lemmes auxiliaires sur quelques sommes trigonométriques Dans ce qui va suivre, nous nous bornerons au cas où $n=1$.

Lemme 3.1. Soient $f_1(X)$ et $f_2(X)$ deux polynômes à coefficients entiers respectivements de degrés m_1 et m_2 modulo p, p étant un premier impair. Si $m=m_1+m_2 \geqslant 2$, on a alors

4) Loc. cit., § 4.

$$\sum_{k=1}^{p-1} e^{2\pi i(f_1(k)+f_2(k^{-1}))/p} = O(p^{1-\frac{1}{m_3}}),$$

où $m_3=m$ *ou* $2m$ *suivant que* $m_1m_2=0$ *ou non, et* k^{-1} *est défini par rapport au module* p.

Ce lemme est essentiellement le résultat dû à M. L. J. Mordell.[5]

Posons maintenant $\chi(a)=\chi(X+a)$.

Lemme 3.2. Sous la condition du lemme 3.1 on a

$$\sum_{k=1}^{p-1} e^{2\pi i(f_1(k)+f_2(k^{-1}))/p}\chi(k) = O(p^{1-\frac{1}{2m_3}}) \quad (\chi \neq \chi_0).$$

Démonstration. On a evidemment

$$\sum_{k=1}^{p-1} e^{2\pi i g(k)/p}\chi(k) = \frac{1}{p-1}\sum_{k=1}^{p-1}\sum_{k_1=1}^{p-1} e^{2\pi i g(kk_1)/p}\chi(k)\chi(k_1),$$

où $g(X)=f_1(X)+f_2(X^{-1})$. Or, en vertu du lemme 3.1, on obtient immédiatement notre lemme selon l'inégalité de Cauchy.

4. Démonstration du théorème 2. Supposons maintenant que $r+t \geqslant 2$. Comme dans la démonstration du théorème 1, nous considérons les fonctions $L(s, \lambda, \tilde{\lambda}, \chi)$.

Encore, il est facile de vérifier que

$$L(s, \lambda_0, \tilde{\lambda}_0, \chi_0)=(1-p^{-s})(1-p^{1-s})^{-1}.$$

D'autre part nous avons déjà montré que l'on a

$$L(s, \lambda, \tilde{\lambda}, \chi)=1+\sum_{j=1}^{r+t}\frac{\tau_j(\lambda, \tilde{\lambda}, \chi)}{p^{js}} \qquad (\lambda \neq \lambda_0,\ \tilde{\lambda} \neq \lambda_0 \text{ ou } \chi \neq \chi_0),$$

où

$$\tau_j(\lambda, \tilde{\lambda}, \chi)=O(p^{j-1+\theta}),$$

comme on le déduit sans paine des lemmes 3.1, 3.2.

Soient $a_1, \ldots, a_r$ et $b_1, \ldots, b_t$ $r+t$ nombres entiers fixes (mod p) ($b_t \not\equiv 0 \pmod p$ lorsque $t>0$). Si $\lambda^{(k)}=\lambda_{\beta_k}^{(k)}$ $(k=1, \ldots, r)$, $\tilde{\lambda}^{(k)}=\tilde{\lambda}_{\tilde{\beta}_k}^{(k)}$ $(k=1, \ldots, t-1)$ et $\chi=\chi_\gamma$, nous posons

$$C(\lambda, \tilde{\lambda}, \chi)=\prod_{k=1}^{r}\exp\frac{2\pi i}{p}\beta_k\xi^{(k)}(1, a_1, \ldots, a_r)\cdot\prod_{k=1}^{t-1}\exp\frac{2\pi i}{p}\tilde{\beta}_k\xi^{(k)}\left(1, \frac{b_{t-1}}{b_t}, \ldots, \frac{b_1}{b_t}\right)$$
$$\cdot\exp\frac{2\pi i}{p-1}\gamma \operatorname{Ind} b_t.$$

Or, par construction, il résulte aussitôt que

$$\sum_{\lambda, \tilde{\lambda}, \chi} C(\bar{\lambda}, \bar{\tilde{\lambda}}, \bar{\chi}) \log L(s, \lambda, \tilde{\lambda}, \chi)=p^{r+t-\varepsilon}(p-1)^{\varepsilon}\sum_{d=1}^{\infty}\sum_{P\in E_d}\frac{1}{d}|P|^{-ds},$$

où $\varepsilon=0$ ou 1 suivant que $t=0$ ou $t \geqslant 1$ et E_d est l'ensemble de tous polynômes unitaires irréductibles (mod p) à coefficients entiers, dont les d$^{\text{ième}}$ puissances ont les premiers r coefficients $a_1, \ldots, a_r$ et

5) L. J. Mordell: On a sum analogous to a Gauss' sum, Oxford Quarterly Journal, **3**, 161-167 (1932). Voir aussi: H. Davenport: On certain exponential sums, J. für reine u. angew. Math., **169**, 158-176 (1933).

les derniers t coefficients $b_1, \ldots, b_t$: nous désignerons par $\pi(m, d)$ le nombre de tels polynômes irréductibles (mod p) de degré m/d, lorsque $d \mid m$. En conséquence de cela, on aura

$$p^{r+t-\varepsilon}(p-1)^{\varepsilon} \sum_{d \mid m} \pi(m, d) = \frac{1}{m} W_m,$$

où

$$W_m = p^m \sum_{\lambda \neq \lambda_0, \tilde{\lambda} \neq \tilde{\lambda}_0, \chi \neq \chi_0} C(\bar{\lambda}, \bar{\tilde{\lambda}}, \bar{\chi}) \cdot \sum_{\substack{\mu_i \geqslant 0 \\ \mu_1 + 2\mu_2 + \cdots + (r+t)\mu_{r+t} = m}} \frac{(-1)^{\mu_1+\mu_2+\cdots+\mu_{r+t}-1}(\mu_1+\mu_2+\cdots+\mu_{r+t}-1)!}{\mu_1!\mu_2!\cdots\mu_{r+t}!} \cdot \tau_1^{\mu_1} \tau_2^{\mu_2} \cdots \tau_{r+t}^{\mu_{r+t}}$$

$$= p^m + O(p^{\theta m + r + t}),$$

c'est-à-dire

$$\sum_{d \mid m} \frac{1}{d} \pi(m, d) = \frac{1}{m} p^{m-r-t} + O(p^{\theta m}).$$

Il est immédiat que

$$\pi_p(m; r, t) = \pi(m, 1), \qquad \sum_{\substack{d \mid m \\ d > 1}} \frac{1}{d} \pi(m, d) = O(p^{m/2}),$$

et on a donc à la fin

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

c. q. f. d.