62. *Sur les Polynômes Irréductibles dans un Corps Fini. II*

Par Saburô UCHIYAMA
Institut Mathématique, Université Métropolitaine, Tokyo
(Comm. by Z. SUETUNA, M.J.A., May 13, 1955)

Cet article est un prolongement de ma note précédente[1] au même titre et nous nous proposons dans ce qui suit de donner une généralisation du théorème 2 établi dans N-I, et y notons en même temps quelques conséquences de l'hypothèse de Riemann pour nos fonctions L.

5. Fonctions L. Soit $q=p^\nu$ ($\nu \geqq 1$) une puissance d'un nombre premier impair et soit F_q un corps fini d'ordre q. Nous considérons encore les fonctions

$$L(s, \lambda, \tilde{\lambda}, \chi)=\sum_M \lambda(M)\tilde{\lambda}(M)\chi(M)\,|M|^{-s},$$

où $s=\sigma+it$, $\sigma>1$, et $\lambda=\prod_{k=1}^{r}\lambda^{(k)}$, $\tilde{\lambda}=\prod_{k=1}^{t-1}\tilde{\lambda}^{(k)}$. La condition "$\lambda^{(k)}(M)=0$ si $X|M$" a été inessentielle pour la définition des fonctions $\lambda^{(k)}$, et nous ne mettons donc plus dans la suite cette convention sur les $\lambda^{(k)}$. Alors, si $\lambda\tilde{\lambda}\chi \neq \lambda_0\tilde{\lambda}_0\chi_0$, les fonctions L s'écrivent toujours sous forme

$$L(s, \lambda, \tilde{\lambda}, \chi)=1+\frac{\tau_1}{q^s}+\frac{\tau_2}{q^{2s}}+\cdots+\frac{\tau_{K-1}}{q^{(K-1)s}} \qquad (K=r+t),$$

où

$$\tau_j=\tau_j(\lambda, \tilde{\lambda}, \chi)=\sum_{\deg M=j}\lambda(M)\tilde{\lambda}(M)\chi(M)$$

et, comme on voit facilement,

$$\tau_n(\lambda, \tilde{\lambda}, \chi)=0 \qquad \text{pour } n \geqq K.$$

D'autre part on a

$$L(s, \lambda_0, \tilde{\lambda}_0, \chi)=(1-q^{-s})^{\varepsilon}(1-q^{1-s})^{-1},$$

où $\varepsilon=0$ ou 1 suivant que $t=0$ ou non.

6. Extension du corps F_q. Soit maintenant F_{q^u} une extension algébrique de degré u du corps F_q. Nous dirons que les fonctions λ', $\tilde{\lambda}'$, et χ', définies dans F_{q^u}, sont les *fonctions induites* des λ, $\tilde{\lambda}$, et χ de F_q, s'il existe les relations suivantes entre eux:

$$\left.\begin{aligned} \lambda&=\prod_{k=1}^{r}\lambda^{(k)}_{\beta_k}, & \lambda'&=\prod_{k=1}^{r}\lambda'^{(k)}_{\beta_k} \\ \tilde{\lambda}&=\prod_{k=1}^{t-1}\tilde{\lambda}^{(k)}_{\tilde{\beta}_k}, & \tilde{\lambda}'&=\prod_{k=1}^{t-1}\tilde{\lambda}'^{(k)}_{\tilde{\beta}_k} \end{aligned}\right\} \quad (\beta_k, \tilde{\beta}_k \in F_q),$$

et

1) S. Uchiyama: Sur les polynômes irréductibles dans un corps fini. I, Proc. Japan Acad., **30**, 523-527 (1954). Dans ce qui va suivre nous renverrons à cette note par N-I.

$$\left.\begin{array}{ll}\chi=\chi_\gamma & (\mathrm{Ind}=\mathrm{Ind}_w)\\ \chi'=\chi'_{\gamma'} & (\mathrm{Ind}=\mathrm{Ind}_{w'})\end{array}\right\}\ (\gamma\equiv\gamma'\ (\mathrm{mod}\ q-1),\ w=\text{norme } w').$$

Soient donnés un polynôme unitaire irréductible P de $F_q[X]$ et un polynôme unitaire irréductible P' de $F_{q^u}[X]$, tel que $P'\mid P$. Posons $d=(\deg P, u)$: on a alors $\deg P'=\deg P/d$ et $\lambda'(P')=\lambda(P)^{u/d}$, $\tilde{\lambda}'(P')=\tilde{\lambda}(P)^{u/d}$, $\chi'(P')=\chi(P)^{u/d}$.

Proposition 1. *Si les fonctions λ', $\tilde{\lambda}'$, et χ' de F_{q^u} sont les fonctions induites des λ, $\tilde{\lambda}$, et χ de F_q, on a*

$$L(s,\lambda',\tilde{\lambda}',\chi')=\prod_{\rho=0}^{u-1}L\left(s-\frac{\rho}{u}\frac{2\pi i}{\log q},\lambda,\tilde{\lambda},\chi\right).$$

En effet, si l'on écrit par P et P' des polynômes unitaires irréductibles respectivement de $F_q[X]$ et de $F_{q^u}[X]$, on a

$$\begin{aligned}L(s,\lambda',\tilde{\lambda}',\chi')&=\prod_{P'}(1-\lambda'(P')\tilde{\lambda}'(P')\chi'(P')\mid P'\mid^{-s})^{-1}\\&=\prod_{P}\prod_{P'\mid P}\\&=\prod_{P}(1-(\lambda(P)\tilde{\lambda}(P)\chi(P))^{u/d}\mid P\mid^{-su/d})^{-d}\qquad (d=(\deg P,u))\\&=\prod_{P}\prod_{\rho=0}^{u-1}(1-\lambda(P)\tilde{\lambda}(P)\chi(P)\zeta^{\rho\deg P}\mid P\mid^{-s})^{-1}\qquad (\zeta=e^{2\pi i/u})\\&=\prod_{\rho=0}^{u-1}L\left(s-\frac{\rho}{u}\frac{2\pi i}{\log q},\lambda,\tilde{\lambda},\chi\right).\end{aligned}$$

Proposition 2. *Sous la même condition de la proposition 1 on a*

$$\tau'_1(\lambda',\tilde{\lambda}',\chi')=\xi^{(u)}(1,\tau_1,\tau_2,\dots,\tau_{K-1}),$$

où

$$\tau'_j(\lambda',\tilde{\lambda}',\chi')=\sum_{\substack{M\in P'_{q^u}[X]\\ \deg M=j}}\lambda'(M)\tilde{\lambda}'(M)\chi'(M).$$

C'est un corollaire simple de la proposition 1.

7. Généralisation du théorème 2. Or, on peut démontrer en général le

Théorème 3. *Si $r+t\geqq 2$ et $p>\max(r,t-1)$ on a*

$$\pi_q(m;r,t)=\frac{1}{m}q^{m-r-t}+O(q^{\theta m})\qquad (m\to\infty),$$

où θ ($\frac{1}{2}\leqq\theta<1$) est une constante indépendante de q et m.

En effet, pour démontrer ce théorème il suffit evidemment de montrer comme on a déjà vu dans N-I, § 4, qu'il existe une constante θ ($\frac{1}{2}\leqq\theta<1$) indépendante de q et m, telle que

$$\tau_j(\lambda,\tilde{\lambda},\chi)=O(q^{\theta j})\qquad (\lambda\tilde{\lambda}\chi\neq\lambda_0\tilde{\lambda}_0\chi_0)$$

pour $j=1,2,\dots,K-1$, où λ, $\tilde{\lambda}$, et χ sont les fonctions définies dans F_q. Cette estimation est une conséquence immédiate de la proposition 2 et des lemmes suivants:

Lemme 7.1. Soient $f_1(X)$ et $f_2(X)$ deux polynômes de $F_q[X]$ respectivement de degré m_1 et m_2. Si $m=m_1+m_2\geqq 2$, on a alors, en posant $g(x)=f_1(x)+f_2(x^{-1})$,

$$\sum_{\substack{x\in F_q \\ (x\neq 0 \text{ si } m_2\neq 0)}} \exp\frac{2\pi i}{p} S(g(x)) = O(q^{1-\frac{1}{m_3}}),$$

où $m_3=m$ *ou* $2m$ *suivant que* $m_1m_2=0$ *ou non, et* S *désigne la trace absolue.*

Lemme 7.2. Sous la même condition du lemme précédent on a

$$\sum_{x} \exp\frac{2\pi i}{p} S(g(x))\cdot\chi(x) = O(q^{1-\frac{1}{2m_3}}),$$

où $\chi(x)=\chi(X+x)$, $x\in F_q$.

Le lemme 7.2 peut être vérifié sans peine du lemme 7.1,[2] et il suffit donc de démontrer ce lemme-ci. Mais il est aisé de voir que tout le raisonnement de M. Mordell[3] fait dans les corps premiers, est aussi applicable sans rien changement aux cas de corps finis généraux. Ces lemmes seront ainsi démontrés.

Or, en vertu du lemme 7.1 ou 7.2, on a

$$\tau_1 = O(q^{\theta}), \qquad \tau_1' = O(q^{\theta u}),$$

où $\theta=1-\dfrac{1}{K_1}$, $K\leqq K_1\leqq 4(K-1)$, et par suite, de la proposition 2 on obtient $(u=j)$

$$\xi^{(j)}(1,\tau_1,\ldots,\tau_j) = O(q^{\theta j}).$$

Il s'en suit immédiatement, par récurrence sur j, que

$$\tau_j(\lambda,\tilde{\lambda},\chi) = O(q^{\theta j})$$

pour $j=1,\ldots,K-1$, c. q. f. d.

8. Sur l'hypothèse de Riemann pour les fonctions *L*. Il est facile de voir que, si l'hypothèse de Riemann pour les fonctions L est vraie, les constantes θ impliquées dans les théorèmes 2 et 3 deviennent être égales à $\frac{1}{2}$ toutes les deux. Comme M. Carlitz a noté dans son mémoire,[4] cette hypothèse est certainement vraie au cas de $(r=1,\ t=1)$. On sait que l'hypothèse est réelle aussi bien au cas de $(r=0,\ t=2)$. Mais il ne me paraît pas très facile de confirmer cette hypothèse en général.

Il serait encore intéressant de noter ici la

Proposition 3. *Soit* $f(X)\in F_q[X]$ *un polynôme de degré* m. *Si l'hypothèse de Riemann pour les fonctions* L *est vraie, on a*

$$\left|\sum_{x\in F_q} \exp\frac{2\pi i}{p} S(f(x))\right| \leqq (m-1)q^{\frac{1}{2}},$$

où S *désigne la trace absolue.*

Cette proposition peut être confrontée à une inégalité citée par M. Mordell.[5]

2) Voir N-I, § 3.

3) L. J. Mordell: On a sum analogous to a Gauss's sum, Oxford Quarterly Journal, **3**, 161–167 (1932).

4) L. Carlitz: A theorem of Dickson on irreducible polynomials, Proc. Amer. Math. Soc., **3**, 693–700 (1952).

5) Cf. L. J. Mordell: Thoughts on number theory, Journal London Math. Soc., **21**, 67 (1946).