ACTA ARITHMETICA
L (1988)

Un problème de diviseurs dans $F_q[X]$

par

MIREILLE CAR (Marseille)

I. Introduction. Il était tentant de formuler pour l'anneau $F_q[X]$ des polynômes à coefficients dans le corps fini à q éléments une conjecture analogue à celle d'Erdös sur les diviseurs d'un entier qui dit que presque tous les entiers possèdent des diviseurs d et d' tels que $d < d' < 2d$, cette conjecture prenant alors la forme suivante:

Presque tous les polynômes de $F_q[X]$ ont deux diviseurs distincts de même degré.

On démontre que cette conjecture est vraie en suivant la méthode utilisée par H. Maier et G. Tenenbaum dans [5] pour démontrer le théorème suivant dont la conjecture d'Erdös est un simple corollaire.

THÉORÈME. *Soit $E(n)$ le minimum des nombres $\log(d'/d)$ pour d et d' divisant n, $d < d'$. Alors, si $n \mapsto \xi(n)$ est une fonction tendant vers $+\infty$ avec n, on a*

$$E(n) \ll (\log n)^{1-\log 3} \exp\left(\xi(n)\sqrt{\log(\log n)}\right) \tag{†}$$

presque partout.

Contrairement à H. Maier et G. Tenenbaum qui, s'intéressant à la majoration de $E(n)$ ont négligé l'ensemble exceptionnel des entiers n ne vérifiant pas (†), on donnera ici une majoration du nombre des polynômes de degré n qui n'ont pas deux diviseurs distincts de même degré. On établira le théorème suivant:

THÉORÈME. *Soit $h(n)$ le nombre de polynômes de degré n de $F_q[X]$ ne possédant pas deux diviseurs distincts de même degré. Alors, pour tout $a \in]1/\log(3), 1[$ on a*

$$h(n) \in O\left(q^n [\log(\log n)(\log n)^{-1/4}]^{g(a)}\right),$$

où

$$g(a) = 1 - a + a\log(a),$$

les constantes impliquées par le symbole O ne dépendant que de q et de a.

On déduit de ce théorème que pour tout nombre réel $\varepsilon > 0$, on a

$$h(n) \in O\left(q^n (\log n)^{-b+\varepsilon}\right),$$

avec

$$b = \frac{1}{4}\left(1 - \frac{1+\log(\log 3)}{\log 3}\right) = 0{,}00103\ldots,$$

les constantes impliquées par le O ne dépendant que de q et de ε.

II. Notations et conventions. Le mot polynôme désignera un polynôme unitaire de $F_q[X]$. L'ensemble des polynômes sans facteur carré sera noté $\mathcal{M}$, l'ensemble des polynômes de degré n de $\mathcal{M}$ sera noté $\mathcal{M}_n$. On notera $\mathcal{I}$ l'ensemble des polynômes irréductibles. Le symbole

$$\sum{}^*, \quad \text{resp. } \sum{}' \quad \text{et} \quad \prod{}'$$

signifie que la somme porte sur des polynômes de $\mathcal{M}$, resp. que la somme ou le produit portent sur des polynômes de $\mathcal{I}$.

Soit H un polynôme. On note $d^\circ H$ le degré de H, $\omega(H)$ le nombre de facteurs irréductibles distincts de H et on pose

$$|H| = q^{d^\circ H}.$$

Si P est un polynôme irréductible divisant H, on dira que P est facteur de H et le mot facteur ne sera utilisé que dans ce cas.

Si E est un ensemble fini de polynômes, on pose

$$\sigma_{-1}(E) = \sum_{H \in E} |H|^{-1},$$

et on note ${}^{\#}E$ le nombre d'éléments de E.

Une application f de $\mathcal{M}$ dans l'ensemble des nombres réels est dite multiplicative si

$$f(AB) = f(A)f(B)$$

pour tout couple de polynômes premiers entre eux.

Les constantes contenues dans les symboles O_α, $\ll_\alpha$, resp. O, $\ll$, ne dépendent que de q et du paramètre α, resp. ne dépendent que de q ou sont absolues.

III. Théorèmes auxilliaires.

III.1. Le théorème Π et ses conséquences.

Théorème Π. *Soit, pour tout entier $n \geq 1$, π_n le nombre de polynômes irréductibles unitaires de degré n. Alors, on a*

$$\text{(III.1)} \qquad n\pi_n = \sum_{j|n} \mu(j)\, q^{n/j},$$

d'où,

$$\text{(III.2)} \qquad q^n - 2q^{n/2} \leq n\pi_n \leq q^n.$$

On trouvera une démonstration élémentaire de ce résultat dans [6]. On en déduit la relation

$$\text{(III.3)} \qquad \left(1 - \frac{1}{q}\right) q^n \ll n\pi_n \ll q^n,$$

ainsi que les propositions suivantes.

Proposition III.1. *Soient des nombres réels $y \geq x \geq 1$. Alors, on a*

$$\text{(III.4)} \qquad y/x \ll \prod_{x \leq d^\circ P \leq y}{}' (1 + |P|^{-1}) \ll y/x.$$

Démonstration. C'est une conséquence de la proposition A.6 de [1].

Proposition III.2. *Soient un entier $n > 0$, $t \in]1/n, \pi - 1/n[$, et*

$$\text{(III.5)} \qquad T_{t,n} = \sum_{1/t < d^\circ P \leq n}{}' \frac{\left(1 + 2\cos(t d^\circ P)\right)^2}{|P|}.$$

Soit

$$\text{(III.6)} \qquad K = 3 + 4/\sin(1/2) + 2/\sin(1).$$

Alors, on a

$$\text{(III.7)} \qquad T_{t,n} \leq \begin{cases} 3\log(tn) & \text{si } t \leq 1, \\ 3\log(n) + K & \text{si } 1 < t \leq \pi - 1, \\ 3\log(n) + \dfrac{2}{(n+1)\sin t} - 2\log(\sin t) + K & \text{si } t > \pi - 1. \end{cases}$$

Démonstration. On majore $T_{t,n}$ à l'aide du théorème Π et on obtient (III.7) par des calculs élémentaires à partir des relations

$$\sum_{j=1}^{\infty} \frac{\cos(jt)}{j} = -\log(2\sin(t/2)), \qquad \left|\sum_{j=m+1}^{n} \frac{\cos(jt)}{j}\right| \leq \frac{1}{(m+1)\sin(t/2)}.$$

III.2. Fonctions multiplicatives.

Proposition III.3. *Soit f une fonction multiplicative définie sur $\mathcal{M}$ à valeurs réelles positives vérifiant la condition suivante: Il existe un nombre réel $B \geq 0$ tel que pour tout polynôme irréductible P on ait*

$$\text{(III.8)} \qquad f(P) < B.$$

Alors, pour tout nombre réel $x > 0$, on a

$$\text{(III.9)} \qquad \sum_{d^\circ H \leq x}{}^* f(H) \ll_B q^x \prod_P{}' \left(1 - \frac{1}{|P|}\right)\left(1 + \frac{f(P)}{|P|}\right).$$

Démonstration. Il suffit d'adapter à $F_q[X]$ la démonstration du théorème 1, [3], sur les fonctions sous-multiplicatives.

III.3. Le théorème de Turán.

Proposition III.4. *Soit $\mathscr{P}$ un ensemble fini de polynômes irréductibles. Pour tout polynôme M, soit*

$$f(M) = \sum_{\substack{P \in \mathscr{P} \\ P \mid M}} 1.$$

Soit d le plus grand des nombres $d^\circ P$ lorsque P décrit $\mathscr{P}$. Soit, pour $y > 0$, pour tout entier $n \geqslant 1$, $e_n(y)$ le nombre de polynômes H de degré n tels que

$$|f(H) - \sigma_{-1}(\mathscr{P})| \geqslant y \sigma_{-1}(\mathscr{P}). \tag{III.10}$$

Alors, pour $n \geqslant d$ on a

$$e_n(y) \leqslant q^n y^{-2} \big(\sigma_{-1}(\mathscr{P})\big)^{-1}. \tag{III.11}$$

Démonstration. La proposition III.4 est un corollaire d'un résultat qui est l'analogue pour $F_q[X]$ du lemme 7, p. 279 de [4] et qui se démontre de façon similaire.

III.4. Polynômes dont les facteurs sont soumis à des conditions de degré.

Proposition III.5. *Soient un entier n, des nombres réels u et v tels que $1 \leqslant u \leqslant v \leqslant n$ et $\mathscr{B}(n, u, v)$ l'ensemble des polynômes $M \in \mathscr{M}_n$ tels que*

$$\sum_{\substack{P \mid M \\ d^\circ P \leqslant u}}' d^\circ P \geqslant v.$$

Alors, pour tout $a \in]0, 1[$, on a

$$^{\#}\mathscr{B}(n, u, v) \ll_a \frac{u}{v} q^{n - av/u}. \tag{III.12}$$

Démonstration. Comme les lemmes 10 et 11 de [2].

Proposition III.6. *Soient un entier $n > 0$, un nombre réel $y \geqslant 1$ et $\mathscr{C}(n, y)$ l'ensemble des polynômes $M \in \mathscr{M}_n$ dont tous les facteurs sont de degré $> y$. Alors, pour $n > y$, on a*

$$1 \ll y q^{-n}\, {}^{\#}\mathscr{C}(n, y) \ll 1. \tag{III.13}$$

Démonstration. Comme en arithmétique classique (III.13) se démontre par une méthode de crible. Pour celà, on ordonne $\mathscr{I}$ par une relation d'ordre compatible avec les degrés, procédé déjà utilisé en [1]. Puis, on procède comme pour le théorème 1, p. 201 de [4].

IV. Démonstration du théorème. Soit $a \in]1/\log(3), 1[$. Soit un entier $n > \exp(\exp(3))$. On pose

$$\varepsilon = \varepsilon(n) = \big(\log(\log n)\big)^{-1}, \tag{IV.1}$$

$$l = l(n) = \big(1 - 2\varepsilon(n)\big)\log n, \qquad m = m(n) = \big(1 - \varepsilon(n)\big)\log n, \tag{IV.2}$$

$$\lambda = \lambda(n) = \tfrac{1}{4}\log(\log n) - \log\big(\log(\log n)\big). \tag{IV.3}$$

Soit un entier $k \in [l, m]$. Pour tout polynôme M on pose

$$M_k = \prod_{\substack{P \mid M \\ d^\circ P < \exp(k)}}' P. \tag{IV.4}$$

Proposition IV.1. *Soit $\mathscr{Y} = \mathscr{Y}(n, k)$ l'ensemble des polynômes $M \in \mathscr{M}_n$ tels qu'il existe un entier $s \in [\lambda, k]$ vérifiant*

$$\omega(M_k) - \omega(M_{k-s}) < as. \tag{IV.5}$$

Alors, on a

$$^{\#}\mathscr{Y} \ll_a q^n \exp\big(-\lambda g(a)\big), \tag{IV.6}$$

où

$$g(a) = 1 - a + a\log(a). \tag{IV.7}$$

Démonstration. Comme pour le lemme 4 de [5], en appliquant la proposition III.3 aux fonctions multiplicatives

$$M \mapsto a^{\omega(M_k) - \omega(M_{k-s})},$$

s décrivant les entiers de $[\lambda, k]$.

Proposition IV.2. *Soit $\mathscr{Z} = \mathscr{Z}(n, k)$ l'ensemble des polynômes $M \in \mathscr{M}_n$ tels que*

$$\omega(M_k) < (1 - \varepsilon) k. \tag{IV.8}$$

Alors, on a

$$^{\#}\mathscr{Z} \ll q^n \log^2(\log n)(\log n)^{-1}. \tag{IV.9}$$

Démonstration. On applique la proposition III.4 à l'ensemble $\mathscr{P}$ des polynômes irréductibles P tels que $d^\circ P < \exp(k)$.

Si $M \in \mathscr{M}$, on désigne par $\varrho(M)$ le nombre d'éléments de l'ensemble des différences $d^\circ D - d^\circ D'$ lorsque D et D' sont des polynômes tels que DD' divise M et on pose pour tout nombre réel t

$$S(M, t) = \sum_{DD' \mid M}^{*} \exp\big(it(d^\circ D - d^\circ D')\big) = \prod_{P \mid M}' \big(1 + 2\cos(t d^\circ P)\big). \tag{IV.10}$$

Proposition IV.3. *Soit $M \in \mathscr{M}$. Alors, on a*

$$3^{2\omega(M)} \leqslant \frac{\varrho(M)}{2\pi} \int_{-\pi}^{\pi} S^2(M, t)\, dt. \tag{IV.11}$$

Démonstration. On pose

$$S(M, t) = \sum_{k=-\infty}^{+\infty} a_k \exp(kit).$$

Avec (IV.10), on a

$$3^{\omega(M)} = S(M, 0) = \sum_{k=-\infty}^{+\infty} a_k.$$

L'inégalité (IV.11) s'obtient alors à l'aide de l'inégalité de Cauchy–Schwarz et de la formule de Parseval.

Soit $\mathscr{H} = \mathscr{H}(n, k)$ l'ensemble des polynômes de $\mathscr{M}_n$ n'appartenant pas à la réunion $\mathscr{Y} \cup \mathscr{Z}$. Pour $t \in [-\pi, +\pi]$, on pose

(IV.12) $$\Psi(t) = \Psi(n, k, t) = \sum_{M \in \mathscr{H}} S^2(M_k, t)\, 3^{-2\omega(M_k)}.$$

Proposition IV.4. *Si* $\exp(\lambda+1-k) < |t| \leqslant 1$, *on a*

(IV.13) $$\Psi(t) \ll_a q^n \big(\exp(k)|t|\big)^{-a\log(3)},$$

si $1 < |t| \leqslant \pi - \exp(\lambda - k)$, *on a*

(IV.14) $$\Psi(t) \ll_a q^n (\pi - t)^{-2/3}\, 3^{(\varepsilon-1)k}.$$

Démonstration. Pour des raisons de symétrie, on peut supposer

(1) $$\exp(\lambda+1-k) < t \leqslant \pi - \exp(\lambda-k).$$

On définit la fonction multiplicative f_t en posant pour $M \in \mathscr{M}$

(2) $$f_t(M) = S^2(M_k, t)\, 3^{-\omega(M_k)-\omega_t(M)},$$

où

(3) $$\omega_t(M) = \sum_{\substack{P|M \\ d^\circ P \leqslant 1/t}}' 1.$$

Les propositions III.3 et III.1 permettent d'écrire

(4) $$\sum_{d^\circ H = n}^{*} f(t) \ll q^n \exp(-k) \exp(\tfrac{1}{3}\Sigma_1) \exp(\tfrac{1}{3}\Sigma_2),$$

où

(5) $$\Sigma_1 = \sum_{d^\circ P < 1/t}' S^2(P, t)|P|^{-1} \leqslant \sum_{d^\circ P \leqslant 1/t}' 9|P|^{-1},$$

(6) $$\Sigma_2 = \sum_{1/t \leqslant d^\circ P < \exp(k)}' S^2(P, t)|P|^{-1} \leqslant \sum_{1/t \leqslant d^\circ P < \exp(k)}' \big(1 + 2\cos(td^\circ P)\big)^2 |P|^{-1}.$$

Avec le théorème II et la proposition III.2, on a, pour $t \leqslant 1$,

$$\sum_{M \in \mathscr{H}} S^2(M_k, t)\, 3^{-\omega(M_k)-\omega_t(M)} \ll q^n,$$

et pour $t > 1$,

$$\sum_{M \in \mathscr{H}} S^2(M_k, t)\, 3^{-\omega(M_k)} \ll q^n (\pi - t)^{-2/3}.$$

On achève la démonstration comme pour le lemme 5 de [5].

Proposition IV.5. *Soit* $\mathscr{T} = \mathscr{T}(n, k)$ *l'ensemble des polynômes* $M \in \mathscr{M}_n$ *tels que*

(IV.15) $$\varrho(M_k) < \exp(k - 2\lambda).$$

Alors, on a

(IV.16) $$^{\#}\mathscr{T} \ll_a q^n \exp(-\lambda g(a)).$$

Démonstration. On pose

(1) $$^{\#}\mathscr{T} = \mathscr{T}_1 + \mathscr{T}_2,$$

où les polynômes comptés dans $\mathscr{T}_1$ appartiennent à $\mathscr{H}$. Comme pour le lemme 5 de [5], on a

(2) $$2\pi \mathscr{T}_1 \leqslant \exp(k - 2\lambda) \int_{-\pi}^{+\pi} \Psi(t)\, dt.$$

Avec la proposition précédente et la majoration triviale

$$\Psi(t) \leqslant q^n,$$

on obtient

$$\int_{-\pi}^{+\pi} \Psi(t)\, dt \ll_a q^n \exp(\lambda - k),$$

et (IV.16) se déduit alors de (1), (2), et des propositions IV.1 et IV.2.

Soit $\mathscr{Q} = \mathscr{Q}(n, k)$ l'ensemble des polynômes $Q \in \mathscr{M}$ dont les facteurs sont de degré $< \exp(k)$ et qui vérifient les conditions suivantes:

(a) $$d^\circ Q \leqslant \exp(k + \lambda),$$

(b) $$\varrho(Q) \geqslant \exp(k - 2\lambda),$$

(c) si les polynômes D et D' sont tels que DD' divise Q, alors

$$d^\circ D \neq d^\circ D'.$$

Soit $\mathscr{E} = \mathscr{E}(n, k)$, resp. $\mathscr{G} = \mathscr{G}(n, k)$, l'ensemble des polynômes $M \in \mathscr{M}_n$ tels que M_k vérifie (c), resp. $M_k \in \mathscr{Q}(n, k)$.

PROPOSITION IV.6. *On a*

(IV.17) $$\#\mathcal{E}-\#\mathcal{G} \ll_a q^n \exp(-\lambda g(a)),$$

(IV.18) $$\#\mathcal{G} \ll q^n \exp(-k)\sigma_{-1}(\mathcal{Q}).$$

Démonstration. Si $M\in\mathcal{E}$ est tel que M_k ne vérifie pas (b), $M\in\mathcal{T}$, si $M\in\mathcal{E}$ est tel que M_k ne vérifie pas (a), $M\in\mathcal{B}(n, \exp(k), \exp(k+\lambda))$, ensemble défini à la proposition III.5, et (IV.17) se déduit alors de (IV.16) et (III.12). Tout $M\in\mathcal{G}$ s'écrit comme produit $M = QB$ où $Q\in\mathcal{Q}$, où B est premier à

$$H = H_k = \prod_{d^\circ P<\exp(k)}{}' P.$$

On a (IV.18) avec la proposition III.6.

Si $M\in\mathcal{M}$, on désigne par $I(M) = I(n, k, M)$ l'ensemble des couples (P, Q) de polynômes irréductibles tels que

(d) $$\exp(k+\lambda) < d^\circ P < 2\exp(k+\lambda),$$

(e) $$d^\circ P < d^\circ Q,$$

(f) $$d^\circ Q-d^\circ P \in \{d^\circ D'-d^\circ D,\ DD' \mid M\}.$$

Soit $\mathcal{F} = \mathcal{F}(n, k)$ l'ensemble des polynômes $M\in\mathcal{G}(n, k)$ ayant deux facteurs P et Q tels que $(P, Q)\in I(M_k)$.

PROPOSITION IV.7. *On a*

(IV.19) $$\#\mathcal{F} \gg q^n \exp(-k-4\lambda)\sigma_{-1}(\mathcal{Q}).$$

Démonstration. L'ensemble $\mathcal{F}$ contient les polynômes $M\in\mathcal{M}_n$ s'écrivant comme produit

$$M = M_k P_1 P_2 B$$

où $M_k\in\mathcal{Q}$, $(P_1, P_2)\in I(M_k)$, où B est premier à

$$U = U_k = \prod_{d^\circ P<3\exp(k+\lambda)}{}' P,$$

et, pour ces polynômes M, cette écriture est unique. La proposition III.6 nous donne

(1) $$\#\mathcal{F} \gg q^n \exp(-k-\lambda)\sum_{M\in\mathcal{Q}}|M|^{-1}\sum_{(P,Q)\in I(M)}|P|^{-1}|Q|^{-1}.$$

Soit $M\in\mathcal{Q}$. Soit $P\in\mathcal{I}$ vérifiant (d). Soit $J = J(M, P)$ l'ensemble des entiers $d^\circ P+|d^\circ D-d^\circ D'|$ lorsque DD' divise M, $DD'\neq 1$. L'ensemble J contient $(\varrho(M)-1)/2$ éléments; de plus, si $j\in J$, on a

$$j \leqslant d^\circ P+d^\circ M \leqslant 3\exp(k+\lambda),$$

et si $Q\in\mathcal{I}$ est de degré j, le couple (P, Q) est dans $I(M)$. On a donc avec (III.3)

$$\sum_{(P,Q)\in I(M)}|Q|^{-1} \geqslant \sum_{j\in J}\pi_j q^{-j} \gg \sum_{j\in J} j^{-1},$$

d'où, avec la condition (b),

(2) $$\sum_{(P,Q)\in I(M)}|Q|^{-1} \gg \exp(-3\lambda).$$

On conclut avec (1) et le théorème II.

Soit $\mathcal{V}(n)$, resp. $\mathcal{V}^*(n)$, l'ensemble des polynômes de degré n, resp. l'ensemble des polynômes de $\mathcal{M}_n$ n'ayant pas deux diviseurs distincts de même degré.

PROPOSITION IV.8. *On a*

(IV.20) $$\#\mathcal{V}^*(n)\in O_a\big(q^n[\log(\log n)(\log n)^{-1/4}]^{g(a)}\big),$$

(IV.21) $$\#\mathcal{V}(n)\in O_a\big(q^n[\log(\log n)(\log n)^{-1/4}]^{g(a)}\big).$$

Démonstration. On a les inclusions

(1) $$\mathcal{V}^*(n)\subset\mathcal{E}(n, m)\subset\mathcal{E}(n, k)\subset\mathcal{E}(n, l).$$

Soit $M\in\mathcal{F}(n, k)$. Si j est un entier tel que $\exp(k+j)\geqslant 3\exp(k+\lambda)$, $M\notin\mathcal{E}(n, k+j)$. Posons

(2) $$j = j(n) = [\lambda+\log(3)]+1.$$

Alors,

(3) $$\#\mathcal{F}(n, k) \leqslant \#\mathcal{E}(n, k)-\#\mathcal{E}(n, k+j).$$

On suppose que tous les ensembles $\mathcal{Q}(n, k)$ sont non vides. Les propositions IV.6 et IV.7 nous donnent l'existence de constantes $K_1>0$, $K_2>0$ ne dépendant que de q et de a telles que

$$\#\mathcal{F}(n, k) \geqslant K_1\exp(-4\lambda)\,\#\mathcal{E}(n, k)-K_2 q^n\theta(n),$$

où

(4) $$\theta(n) = \exp(-4\lambda-g(a)\lambda),$$

d'où, avec (3),

$$\#\mathcal{E}(n, k+j) \leqslant \#\mathcal{E}(n, k)\big(1-K_1\exp(-4\lambda)\big)+K_2 q^n\theta(n).$$

En itérant cette relation, on obtient avec (1)

$$\#\mathcal{V}^*(n) \leqslant \#\mathcal{E}(n, l)\big(1-K_1\exp(-4\lambda)\big)^r+K_2 q^n\theta(n)\big(1+\big(1-K_1\exp(-4\lambda)\big)+\ldots+\big(1-K_1\exp(-4\lambda)\big)^{r-1}\big),$$

où

$$r = r(n) = \left[\frac{m-l}{j}\right].$$

On majore $^{\#}\mathscr{E}(n, l)$ par q^n et, pour n assez grand, on a

$$^{\#}\mathscr{V}^*(n) \ll_{K_1,K_2} q^n\left[\left(1-K_1\exp(-4\lambda)\right)^r+\frac{K_2}{K_1}\exp(-\lambda g(a))\right]$$
$$\ll_a q^n\exp(-\lambda g(a)).$$

La majoration

$$^{\#}\mathscr{V}^*(n) \ll_a q^n\exp(-\lambda g(a))$$

reste vraie si l'un des ensembles $\mathscr{Q}(n, k)$ est vide. On déduit la majoration de $^{\#}\mathscr{V}(n)$ de cette relation et de la relation

$$^{\#}\mathscr{V}(n) \leqslant \sum_{0\leqslant 2j\leqslant n} q^{j\,\#}\mathscr{V}^*(n-2j).$$

V. Remarques. La proposition précédente donne le théorème annoncé. La méthode utilisée au paragraphe IV peut conduire à une majoration de $^{\#}\mathscr{V}(n)$ où la fonction

$$n \mapsto \log(\log n)$$

est remplacée par une fonction

$$n \mapsto L(n)$$

tendant vers $+\infty$ avec n, moins vite que $\log(\log n)$.

Le théorème démontré ici admet un corollaire intéressant concernant les partitions d'un entier en entiers formant une suite pseudo-géométrique. Avant d'énoncer ce corollaire, précisons quelques définitions.

DÉFINITION V.1. Une suite $(n_j)_{1\leqslant j\leqslant k}$ d'entiers strictement positifs est dite *pseudo-géométrique* si l'égalité entre les sommes partielles

$$\sum_{j=1}^{k} \varepsilon_j n_j = \sum_{j=1}^{k} \delta_j n_j, \quad \varepsilon_j \in \{0, 1\},\ \delta_j \in \{0, 1\},$$

n'a lieu que si $\varepsilon_j = \delta_j$ pour tout $j = 1, \ldots, k$.

DÉFINITION V.2. Soit un entier $n > 0$. On désigne par $P.G(n)$ l'ensemble des suites finies $(n_1, \ldots, n_k)$, strictement croissantes telles que

(1) $$n = n_1 + \ldots + n_k,$$

(2) $$(n_1, \ldots, n_k) \text{ est pseudo-géométrique.}$$

On a alors le résultat suivant:

THÉORÈME. *Pour tout nombre réel* $a \in]1/\log(3), 1[$, *on a*

$$\sum_{\substack{k\\(n_1,\ldots,n_k)\in P.G(n)}} (n_1\times\ldots\times n_k)^{-1} \in O_a\left([\log(\log n)(\log n)^{-1/4}]^{g(a)}\right),$$

où

$$g(a) = 1-a+a\log(a).$$

En particulier,

$$\lim_{n\to+\infty}\Big(\sum_{\substack{k\\(n_1,\ldots,n_k)\in P.G(n)}} (n_1\times\ldots\times n_k)^{-1}\Big) = 0.$$

Démonstration. On utilise les notations du paragraphe IV. Soit $H \in \mathscr{M}_n$, $P_1, \ldots, P_k$ ses facteurs qui sont deux à deux distincts. Alors, $H \in \mathscr{V}^*(n)$ si et seulement si la suite $(d^\circ P_1, \ldots, d^\circ P_k)$ appartient à $P.G(n)$, d'où

$$^{\#}\mathscr{V}^*(n) = \sum_{\substack{k\\(n_1,\ldots,n_k)\in P.G(n)}} \pi_{n_1}\times\ldots\times\pi_{n_k}.$$

Supposons $q \geqslant 5$. Avec (III.2) on a

$$^{\#}\mathscr{V}^*(n) \geqslant \sum_{\substack{k\\(n_1,\ldots,n_k)\in P.G(n)}} \prod_{j=1}^{k}\left(\frac{q^{n_j}(1-2q^{-n_j/2})}{n_j}\right).$$

Si $(n_1, \ldots, n_k) \in P.G(n)$, les entiers $n_1, \ldots, n_k$ sont distincts, d'où

$$\prod_{j=1}^{k}(1-2q^{-n_j/2}) \geqslant \prod_{j=1}^{\infty}(1-2q^{-j/2}).$$

Notons $b(q)$ ce dernier produit qui est strictement positif. On a alors

$$\sum_{\substack{k\\(n_1,\ldots,n_k)\in P.G(n)}} (n_1\times\ldots\times n_k)^{-1} \leqslant b(q)^{-1}q^{-n\,\#}\mathscr{V}^*(n).$$

La majoration annoncée se déduit de (IV.20).

A titre de comparaison, notons que l'on a

$$\lim_{n\to+\infty}\Big(\sum_{\substack{k\\0<n_1<\ldots<n_k\\n_1+\ldots+n_k=n}} (n_1\times\ldots\times n_k)^{-1}\Big) = \exp(-\gamma),$$

où γ désigne la constante d'Euler.

Ce résultat s'obtient facilement. Notons a_n la somme à étudier. Considérons pour $x \in [0, 1[$, la série génératrice

(1) $$f(x) = 1+\sum_{n=1}^{\infty} a_n x^n.$$

On a

$$(2) \qquad f(x) = \prod_{n=1}^{\infty} (1+x^n/n).$$

Posons alors

$$(3) \qquad g(x) = (1-x) f(x),$$

ce qui s'écrit aussi

$$(4) \qquad g(x) = f(x) \prod_{n=1}^{\infty} \exp(-x^n/n).$$

On montre que le développement en série de Taylor à l'origine de g converge normalement sur $[0, 1[$. Avec (2) et (4) on a

$$(5) \qquad g(1) = \exp(-\gamma).$$

Les relations (1) et (3) donnent alors le résultat annoncé.

Références

[1] M. Car, *Polynômes irréductibles de $F_q[X]$ de la forme $M+N$ où N est norme d'un polynôme de $F_{q^2}[X]$*, Dissertationes Mathematicae 238, Warszawa 1984.

[2] P. Erdős et G. Tenenbaum, *Sur les diviseurs consécutifs d'un entier*, Bull. Soc. Math. France 111 (1983), p. 125–145.

[3] H. Halberstam and H.-E. Richert, *On a result of R. R. Hall*, J. Number Theory 11 (1979), p. 76–89.

[4] H. Halberstam and K. F. Roth, *Sequences*, Clarendon Press, Oxford 1966.

[5] H. Maier and G. Tenenbaum, *On the set of divisors of an integer*, Invent. Math. 76 (1984), p. 121–128.

[6] M. Mignotte, *Statistiques sur $F_q[X]$*, Comptes rendus des journées de théorie analytique et élémentaire des nombres, Limoges, 10–11 mars, 1980.

LABORATOIRE DE THÉORIE DES NOMBRES
FACULTÉ DES SCIENCES DE SAINT-JÉRÔME
Avenue Escadrille Normandie Niemen
13397 Marseille Cedex 4, France

Reçu le 5.2.1986
et dans la forme modifiée le 17.9.1986 (1588)

ACTA ARITHMETICA
L (1988)

Note on an index formula of elliptic units in a ring class field II

by

HEIMA HAYASHI (Kumamoto, Japan)

This short note is a supplement to our previous note [1].

Let all of the notation and terminology be the same as in [1]. In [1] we have proved the following:

PROPOSITION 1 ([1], Prop. 1). *Let c_1 and c_2 be any two classes in* $\mathrm{Cl}(K/\Sigma)$ *and n the least positive rational integer such that* $n\big(l(c_1)-1\big)\big(l(c_2)-1\big) \equiv 0 \pmod{24}$. *Then*

$$\left\{\frac{\delta_K(c_1 c_2)}{\delta_K(c_1)\,\delta_K(c_2)}\right\}^n \in E_K^{24h}.$$

Our proof for this proposition (in [1]) contains somewhat incomplete parts. Indeed, in the arguments (in Steps 2 and 3 on pp. 208–209), some tedious verifications have been omitted. In this short note we shall give another simple and complete proof for the same proposition.

Proof of Proposition 1. It suffices to consider only the case where $K = K_f$. Moreover, since in the case where $(D, f) = (-3, 1), (-3, 2), (-3, 3), (-4, 1)$ or $(-4, 2)$, the assertion is trivial, we may exclude these cases throughout this proof.

Let C_1 and C_2 be any two classes in $\mathrm{Cl}(K_f/\Sigma)$ and let n be the least positive integer such that $n\big(l(C_1)-1\big)\big(l(C_2)-1\big) \equiv 0 \pmod{24}$. According to the arguments in [1] (Step 1 and the first half of Step 2, pp. 206–207), we have

$$(1.1) \qquad \left\{\frac{\delta_f(C_1 C_2)}{\delta_f(C_1)\,\delta_f(C_2)}\right\}^{2n} \in E_{K_f}^{24h},$$

and especially when none of three classes C_1^2, C_2^2 and $C_1^2 C_1^2$ is equal to the unit class C_0 in $\mathrm{Cl}(K_f/\Sigma)$,

$$(1.2) \qquad \left\{\frac{\delta_f(C_1 C_2)}{\delta_f(C_1)\,\delta_f(C_2)}\right\}^{n} \in E_{K_f}^{24h}.$$