[3] J. H. B. Kemperman, *On small sumsets in Abelian Groups*, Acta Math. 103 (1960), pp. 63–88.
[4] M. Kneser, *Abschätzung der asymptotischen Dichte von Summenmengen*, Math. Zeitschr. 58 (1953), pp. 459–484.
[5] – *Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen*, ibid. 61 (1955), pp. 429–434.

Received on 3.3.1981
and in revised form on 6.4.1983 (1244)

ACTA ARITHMETICA
XLIV (1984)

Sommes de puissances et d'irréductibles dans $F_q[X]$

par

MIREILLE CAR (Marseille)

I. Introduction. Soit F_q le corps fini à q éléments. De nombreuses analogies entre l'arithmétique de l'anneau $F_q[X]$ des polynômes à une indéterminée sur le corps F_q et l'anneau Z des entiers relatifs ont été mises en évidence, notemment en ce qui concerne l'arithmétique additive. Les problèmes de Goldbach, [5], et de Waring, [2], [8], ont été étudiés, et plus particulièrement le problème de Waring pour les carrés. Il est actuellement connu que tout polynôme $M \in F_q[X]$, de degré assez élevé, est représentable comme somme de trois polynômes irréductibles de degré au plus égal au degré de M, [5], et que, tout polynôme de degré $2n$ ou $2n-1$ assez élevé, est représentable comme somme de trois carrés de polynômes de degré au plus n, [3]. Nous nous intéressons ici à la représentation d'un polynôme de $F_q[X]$ comme somme d'une puissance k-ième et de deux polynômes irréductibles. Ce problème a déjà été étudié dans [9] pour les polynômes de degré multiples de k. On y démontre le théorème suivant:

THÉORÈME. *Soit k un entier de l'intervalle $[2, p[$, où p est la caractéristique du corps F_q. Alors, si n est un entier suffisamment grand, tout polynôme $K \in F_q[X]$ de degré nk est représentable comme somme*

$$K = a_1P_1 + a_2P_2 + a_3A^k,$$

P_1 et P_2 étant des polynômes irréductibles unitaires de degré nk, A étant un polynôme unitaire de degré n, a_1, a_2 et a_3 étant des éléments de F_q.

Il est possible d'avoir de telles représentations pour des polynômes de degré non multiple de k, et même d'avoir des représentations de la forme

$$K = P_1 + P_2 + A^k,$$

les polynômes P_1 et P_2 étant irréductibles, mais non nécessairement unitaires, A étant un polynôme, ces polynômes vérifiant de plus, des conditions de degré. On peut aussi exiger que le polynôme A intervenant dans une telle représentation soit irréductible. C'est ce qui est fait ici, où l'on démontre essentiellement le théorème suivant:

THÉORÈME. *Soit k un entier de l'intervalle $[2, p[$, où p est la*

caractéristique du corps F_q. Alors, il existe un entier $n(q, k)$, ne dépendant que de q et de k, tel que, pour tout entier $n \geqslant n(q, k)$, si M est un polynôme de $F_q[X]$ de degré $d^0M \in]kn-k, kn]$, l'équation

$$M = P_1 + P_2 + A^k \tag{E}$$

admet une solution (P_1, P_2, A) où P_1 et P_2 sont des polynômes irréductibles de degré d^0M, où A est

(i) *soit, un polynôme de $F_q[X]$ de degré $< n$,*

(ii) *soit, un polynôme de $F_q[X]$ tel que A^k soit de degré $\leqslant d^0M$,*

(iii) *soit, un polynôme irréductible de $F_q[X]$ de degré $< n$,*

(iv) *soit, un polynôme irréductible de $F_q[X]$ tel que A^k soit de degré $\leqslant d^0M$.*

Ce théorème est établi dans [4] dans le cas particulier $k = 2$. Le passage au cas général ne présente que des difficultés techniques supplémentaires.

Remarquons que les conditions (i) et (ii), ainsi que les conditions (iii) et (iv) sont équivalentes pour des polynômes M de degré non multiple de k.

Remarquons aussi que l'existence d'une solution satisfaisant à la condition (iii) assure l'existence de solutions satisfaisant aux autres conditions. Nous démontrerons toutefois les quatre parties du théorème, car la démonstration fournit une évaluation asymptotique du nombre de solutions de (E), nombre qui varie suivant les conditions exigées.

II. Notation. Nous reprenons les notations utilisées dans [4] et [5].

Soit H un polynôme non nul de $F_q[X]$, son degré sera noté d^0H, le nombre de ses diviseurs unitaires $d(H)$, le coefficient de son terme de plus haut degré $\operatorname{sgn}(H)$; l'ensemble des polynômes de degré strictement inférieur à d^0H, identifié à l'ensemble des classes de congruence inversibles modulo H, sera noté $\mathscr{C}_H$, et le groupe multiplicatif des classes de congruence modulo H sera noté $\mathscr{C}_H^*$, l'ordre de ce groupe sera noté $\Phi(H)$. La fonction Φ ainsi définie a les mêmes propriétés que la fonction d'Euler classique.

On désigne par $\mathscr{U}$ l'ensemble des polynômes unitaires. Sur $\mathscr{U}$ on définit la fonction de Möbius μ par

$$\mu(H) = \begin{cases} 1 & \text{si } H = 1, \\ 0 & \text{si } H \text{ est divisible par le carré d'un polynôme irréductible,} \\ (-1)^r & \text{si } H \text{ est produit de } r \text{ polynômes irréductibles distincts.} \end{cases}$$

L'ensemble des polynômes irréductibles sera noté $\mathscr{I}$, l'ensemble des polynômes de degré m sera noté D_m, l'ensemble des polynômes de degré strictement inférieur à m sera noté F_m. On pose $I_m = D_m \cap \mathscr{I}$.

Si A et B sont des polynômes, si H est un polynôme non nul, on note $A|B$ la relation A divise B, $A \nmid B$ la relation A ne divise pas B, $A \equiv B \pmod H$ la relation A est congru à B modulo H. Le plus grand commun diviseur unitaire de deux polynômes non nuls A et B sera noté (A, B).

Sur le corps $F_q(X)$ des fractions rationnelles, on définit une valuation v par

$$v(A/B) = d^0B - d^0A$$

si A et B sont des polynômes non nuls. Le complété de $F_q(X)$ pour cette valuation s'identifie au corps $\boldsymbol{K}$ des séries de Laurent formelles en $1/X$, à coefficients dans F_q, la valuation v se prolongeant à $\boldsymbol{K}$ par

$$v\Big(\sum_{s\in\boldsymbol{Z}} a_sX^s\Big) = -\operatorname{Sup}\{r \in \boldsymbol{Z} |\ a_r \neq 0\}.$$

A cette valuation v est associée la valeur absolue $|\ |_v$ définie par

$$|a|_v = q^{-v(a)} \quad \text{si } a \neq 0, \qquad |0|_v = 0.$$

Nous noterons simplement $|\ |$ cette valeur absolue, bien que ce dernier symbole soit aussi utilisé pour désigner la valeur absolue classique sur le corps $\boldsymbol{R}$ des nombres réels ou sur le corps $\boldsymbol{C}$ des nombres complexes, mais il y a peu de risque de confusion.

On désigne par $\mathscr{P}$ l'idéal de valuation, et, pour tout entier j, par $\mathscr{P}_j$ l'idéal

$$\{t \in \boldsymbol{K} |\ v(t) > j\}.$$

Les ensembles $\mathscr{P}_j$ sont des sous-groupes compacts du groupe additif localement compact $\boldsymbol{K}$. Désignons par dt la mesure de Haar sur $\boldsymbol{K}$ normalisée à 1 sur $\mathscr{P}$.

Tout élément $u \in \boldsymbol{K}$ s'écrit de façon unique

$$u = [u] + \{u\},$$

où $[u]$ est un polynôme de $F_q[X]$ et $\{u\}$ un élément de $\mathscr{P}$, $\{u\}$ sera appelée partie fractionnaire de u.

Soit e un caractère non principal du groupe additif de F_q. On définit un caractère non principal E du groupe additif de $\boldsymbol{K}$ en posant

$$E\Big(\sum_{s\in\boldsymbol{Z}} a_sX^s\Big) = e(a_{-1}).$$

Si $\mathscr{A}$ est un sous-ensemble de $\boldsymbol{K}$ contenant 0, l'ensemble des éléments non nuls de $\mathscr{A}$ sera noté $\mathscr{A}^0$.

III. Sommes de caractères. Les cinq propositions suivantes ont été établies dans [5] ou se démontrent par des méthodes analogues.

PROPOSITION III.1. *Pour tout entier j, $\mathscr{P}_j$ a pour mesure q^{-j}.*

PROPOSITION III.2. (i) *Pour tout polynôme A, $E(A) = 1$.*

(ii) *Pour tout polynôme H non nul, si A et B sont des polynômes congrus modulo H, $E(A/H) = E(B/H)$.*

(iii) *Si $u \in \mathscr{P}_1$, $E(u) = 1$.*

PROPOSITION III.3. *Soient un entier $j \geqslant 0$, $u \in \mathbf{K}$ et $b \in \mathscr{P}$. Alors,*

$$\int_{b+\mathscr{P}_j} E(ut)\,dt = \begin{cases} q^{-j}E(ub), & si \quad v(u) > -j, \\ 0, & si \quad v(u) \leqslant -j. \end{cases} \tag{III.1}$$

PROPOSITION III.4. *Soient $u \in \mathbf{K}$ et j un entier $\geqslant 0$. Alors on a*

$$\sum_{B \in F_j} E(uB) = \begin{cases} q^j, & si \quad v(\{u\}) > j, \\ 0, & si \quad v(\{u\}) \leqslant j. \end{cases} \tag{III.2}$$

De cette proposition on déduit un corollaire très souvent utilisé par la suite, et qui pourrait etre aisément démontré de façon directe.

COROLLAIRE. *Si G et H sont des polynômes premiers entre eux,*

$$\sum_{R \in \mathscr{C}_H} E\left(\frac{G}{H}R\right) = 0. \tag{III.3}$$

De la proposition III.4 on déduit aussi la "première formule de changement de variable".

PROPOSITION III.5. *Soient un entier $j \geqslant 0$, $u \in \mathscr{P}$ et $a \in \mathbf{K}$ tels que $j \geqslant v(a) \geqslant -v(u)$. Alors on a*

$$\sum_{B \in F_j} E(auB) = |a|^{-1} \sum_{B \in F_{j-v(a)}} E(uB). \tag{III.4}$$

Donnons maintenant la "deuxième formule de changement de variable".

PROPOSITION III.6. *Soient des entiers $j \geqslant 0$ et $k \geqslant 2$, soient un polynôme H tel que $d^0H \leqslant j$ et $u \in \mathscr{P}$ tel que $v(u) > (k-1)(j-1)+d^0H$. Alors on a*

$$\sum_{B \in F_{j-d^0H}} E(uH^kB^k) = |H|^{-1} \sum_{B \in F_j} E(uB^k). \tag{III.5}$$

Démonstration. On a

$$|H| \sum_{B \in F_{j-d^0H}} E(uH^kB^k) = \sum_{R \in \mathscr{C}_H} \sum_{B \in F_{j-d^0H}} E(uH^kB^k).$$

Si $v(u) > (k-1)(j-1)+d^0H$, si $B \in F_{j-d^0H}$, si $R \in \mathscr{C}_H$,

$$v\left(u([HB+R]^k - H^kB^k)\right) > 1,$$

et

$$E(u[HB+R]^k) = E(uH^kB^k).$$

Donc,

$$|H| \sum_{B \in F_{j-d^0H}} E(uH^kB^k) = \sum_{R \in \mathscr{C}_H} \sum_{B \in F_{j-d^0H}} E(u[HB+R]^k) = \sum_{B \in F_j} E(uB^k). \tag{III.6}$$

Terminons ce paragraphe par la "troisième formule de changement de variable" et son corollaire.

PROPOSITION III.7. *Soient des entiers $m \geqslant 0$ et $k \geqslant 2$. Soit $u \in \mathscr{P}$ tel que $v(u) > (k-1)m$. Alors, on a*

$$\sum_{B \in D_m} E(uB^k) = q^{m(1-k)} \sum_{b \in F_q^0} E(ub^kX^{km}) \sum_{V \in F_{km}} E(uV). \tag{III.7}$$

Démonstration. C'est la généralisation de la proposition III.8 de [4] où seul le cas $k = 2$ est traité.

Si $B \in D_m$, il existe $b \in F_q^0$ et $V \in F_{km}$ uniques tels que

$$B^k = b^{km}X^{km} + V,$$

b et V sont donc tels que

$$E(uB^k) = E(ub^kX^{km})E(uV).$$

D'autre part, il existe exactement q^{km-m} polynômes $W \in F_{km}$ tels que

$$d^0(B^k - b^kX^{km} - W) < km - m,$$

et, pour de tels polynômes

$$E(uV) = E(uW).$$

Enfin, si $b \in F_q^0$, si $V \in F_{km}$, il existe un et un seul polynôme B de degré m tel que

$$d^0(B^k - b^kX^{km} - W) < km - m.$$

En effet, cette relation détermine le degré de B, qui doit etre égal à m, le coefficient $\operatorname{sgn}(B)$, puis, par induction, tous les coefficients de B.

COROLLAIRE. *Sous les mêmes hypothèses,*

$$\sum_{B \in D_m} E(uB^k) = \begin{cases} q^m(q-1) & si \quad v(u) > km+1, \\ 0 & si \quad v(u) \leqslant km, \\ q^m \sum_{b \in F_q^0} e(ab^k) & si \quad v(u) = km+1, \text{ et si } a \in F_q \text{ est tel que} \\ & \quad v(u - aX^{-v(u)}) > v(u). \end{cases} \tag{III.8}$$

Démonstration. C'est une conséquence de (III.2) et de (III.7).

IV. La méthode du cercle. Soit un entier $k \geqslant 2$, strictement inférieur à la caractéristique du corps F_q.

Soit un nombre réel $h > 0$ lui aussi fixé. (Il sera choisi plus loin en fonction de k.)

Soit un entier n tel que

$$n \geqslant 11kh\log(n)/\log(q). \tag{IV.1}$$

Soit M un polynôme de degré $m \in \{kn, kn-1, \ldots, kn-k+1\}$. Soient, pour $i \in \{n, n+1\}$, f_i, f_i^* et g les applications de $\mathscr{P}$ dans $\mathbf{C}$ définies par

(IV.2) $$f_i(t) = \sum_{A \in F_i} E(tA^k),$$

(IV.3) $$f_i^*(t) = \sum_{P \in F_i \cap \mathscr{S}} E(tP^k),$$

(IV.4) $$g(t) = \sum_{P \in I_m} E(tP).$$

Soient

(IV.5) $$R_i(M) = \int_{\mathscr{P}} f_i(t) g^2(t) E(-Mt)\, dt,$$

(IV.6) $$R_i^*(M) = \int_{\mathscr{P}} f_i^*(t) g^2(t) E(-Mt)\, dt.$$

Alors, d'après (III.1), $R_i(M)$, respectivement $R_i^*(M)$, est égal au nombre de solutions de l'équation $M = P_1 + P_2 + A^k$ où P_1 et P_2 sont des polynômes irréductibles de degré m, où A est un polynôme de degré strictement inférieur à i, respectivement, un polynôme irréductible de degré strictement inférieur à i.

Les intégrales $R_n(M)$ et $R_n^*(M)$ nous donnent le nombre de solutions de l'équation (E) satisfaisant aux conditions (i) ou (iii). Dans le cas où d^0M est divisible par k, les intégrales $R_{n+1}(M)$ et $R_{n+1}^*(M)$ nous donnent le nombre de solutions de (E) satisfaisant aux conditions (ii) ou (iv).

Posons

(IV.7) $$s = [h \log(n)/\log(q)],$$

(IV.8) $$N = k(n - s + 1).$$

On appelle *fraction de Farey à l'ordre N* toute fraction rationnelle G/H telle que

(i) H est un polynôme unitaire de degré au plus N,
(ii) $G \in \mathscr{C}_H^*$.

Si G/H est une fraction de Farey à l'ordre N, la boule

$$\mathscr{U}_{G/H} = \{t \in \mathscr{P} |\ \nu(t - G/H) > d^0H + N\}$$

est appelée *arc de Farey* de centre G/H.

Lorsque G/H décrit l'ensemble des fractions de Farey à l'ordre N, les arcs de Farey $\mathscr{U}_{G/H}$ forment une partition de $\mathscr{P}$. C'est le théorème 4.3 de [5].

Sur les arcs de Farey $\mathscr{U}_{G/H}$ tels que $d^0H \leqslant ks$, on sait calculer $f_i(t)$ et on a une bonne approximation de $f_i(t)$ et de $g(t)$. Ces arcs sont dits majeurs. Soit $\mathscr{A}$ leur réunion, et $\mathscr{A}'$ la réunion des arcs restants. Si G/H est une fraction de Farey à l'ordre N, soient

(IV.9) $$I_{G/H}(M) = \int_{\mathscr{U}_{G/H}} f_i(t) g^2(t) E(-Mt)\, dt,$$

(IV.10) $$I_{G/H}^*(M) = \int_{\mathscr{U}_{G/H}} f_i^*(t) g^2(t) E(-Mt)\, dt.$$

Les sommes

$$\int_{\mathscr{A}} f_i(t) g^2(t) E(-Mt)\, dt = \sum_{\substack{H \in \mathscr{U} \\ d^0H \leqslant ks}} \sum_{G \in \mathscr{C}_H^*} I_{G/H}(M),$$

$$\int_{\mathscr{A}} f_i^*(t) g^2(t) E(-Mt)\, dt = \sum_{\substack{H \in \mathscr{U} \\ d^0H \leqslant ks}} \sum_{G \in \mathscr{C}_H^*} I_{G/H}^*(M)$$

donneront de bonnes approximations de $R_i(M)$ et $R_i^*(M)$. Le calcul de ces sommes fait apparaitre les premiers termes de séries singulières $\mathfrak{S}(M)$ et $\mathfrak{S}^*(M)$ qui seront étudiées au paragraphe suivant.

Lorsque t est dans $\mathscr{A}'$, on a seulement une majoration de $f_i(t)$ et de $f_i^*(t)$. La majoration de $f_i(t)$ se fait comme dans [8]. La majoration de $f_i^*(t)$ nécessite la majoration de sommes doubles qui sera faite au paragraphe VI.

Dans tous les paragraphes suivants, les constantes impliquées par les symboles $\ll$ ne dépendront que de q et de k.

V. Les séries singulières. Dans ce paragraphe, M est un polynôme de $F_q[X]$, fixé. Si G et H sont des polynômes premiers entre eux, on pose

(V.1) $$S(G, H) = \sum_{A \in \mathscr{C}_H} E\left(\frac{G}{H} A^k\right),$$

(V.2) $$S^*(G, H) = \sum_{A \in \mathscr{C}_H^*} E\left(\frac{G}{H} A^k\right).$$

Si H est un polynôme non nul, on pose

(V.3) $$C(M, H) = \sum_{G \in \mathscr{C}_H^*} S(G, H) E\left(-M \frac{G}{H}\right),$$

(V.4) $$C^*(M, H) = \sum_{G \in \mathscr{C}_H^*} S^*(G, H) E\left(-M \frac{G}{H}\right).$$

Les propositions V.1 et V.2 se démontrent comme les théorèmes 8.4 et 8.8 de [1].

PROPOSITION V.1. *Les fonctions $H \mapsto C(M, H)$ et $H \mapsto C^*(M, H)$ sont multiplicatives.*

PROPOSITION V.2. *Si G et H sont des polynômes premiers entre eux,*

(V.5) $$|S(G, H)| \ll |H|^{1 - 1/k}.$$

PROPOSITION V.3. *Soient $P \in \mathscr{S}$ et $u(P)$, respectivement $u^*(P)$, le nombre de solutions de la congruence*

$$L^k \equiv M \pmod{P},$$

respectivement, le nombre des solutions $L \not\equiv 0 \pmod P$ *de cette congruence. Alors, on a*

$$C(M, P) = (u(P)-1)|P|, \tag{V.6}$$

$$C^*(M, P) = (u^*(P)-1)|P|. \tag{V.7}$$

Démonstration. Immédiate, avec (III.3).

COROLLAIRE. *Si* H *est un polynôme non nul, sans facteur carré,*

$$|C(M, H)| \leqslant (k-1)^{\omega(H)}|H|, \tag{V.8}$$

$$|C^*(M, H)| \leqslant k^{\omega(H)}|H|, \tag{V.9}$$

où $\omega(H)$ *est le nombre de facteurs irréductibles de* H.

PROPOSITION V.4. *Pour tout polynôme* H *de degré* $d^0H \geqslant 2$, *on a*

$$\Phi(H) \gg |H|(\log d^0H)^{-1}. \tag{V.10}$$

Démonstration. Comme pour le théorème 5.1, chapitre I de [6]. (Ici, la constante impliquée par le symbole $\gg$ ne dépend que de q.)

LEMME. *Pour tout réel* $\theta > 1$, *pour tout réel* $\varepsilon > 0$, *il existe une constante* $a = a(q, \theta, \varepsilon)$, *ne dépendant que de* q, θ *et* ε, *telle que, pour tout polynôme* H *sans facteur carré, on ait*

$$\theta^{\omega(H)} \leqslant a(q, \theta, \varepsilon)|H|^{\varepsilon}. \tag{V.11}$$

Démonstration. Soient $\theta > 1$ et $\varepsilon > 0$. Pour tout polynôme H,

$$\frac{\theta^{\omega(H)}}{|H|^{\varepsilon}} \leqslant \prod_{\substack{P\in\mathscr{S}\cap\mathscr{U}\\ P|H}} \left(\frac{\theta}{|P|^{\varepsilon}}\right) \leqslant \prod_{\substack{P\in\mathscr{S}\cap\mathscr{U}\\ P|H\\ d^0P<\log\theta/\varepsilon\log q}} \left(\frac{\theta}{|P|^{\varepsilon}}\right) \leqslant \prod_{\substack{P\in\mathscr{S}\cap\mathscr{U}\\ d^0P<\log\theta/\varepsilon\log q}} \left(\frac{\theta}{|P|^{\varepsilon}}\right).$$

PROPOSITION V.5. *La série*

$$\mathfrak{S}(M) = \sum_{H\in\mathscr{U}} \frac{\mu^2(H)C(M, H)}{|H|\Phi^2(H)} \tag{V.12}$$

est absolument convergente. De plus, pour tout entier $t \geqslant 2$,

$$\sum_{d^0H\geqslant t} \frac{\mu^2(H)|C(M, H)|}{|H|\Phi^2(H)} \ll q^{-t/2}. \tag{V.13}$$

Il existe une constante $a_1 = a_1(q)$, *ne dépendant que de* q, *telle que,*

$$\mathfrak{S}(M) \geqslant a_1 > 0. \tag{V.14}$$

Démonstration. Soit $H\in\mathscr{U}$ tel que $\mu^2(H) = 1$ et $d^0H \geqslant t \geqslant 2$. Alors, avec (V.8), (V.10) et (V.11),

$$\frac{|C(M, H)|}{|H|\Phi^2(H)} \ll (k-1)^{\omega(H)}|H|^{-2}(\log d^0H)^2 \ll |H|^{-7/4}(\log d^0H)^2,$$

d'où,

$$\sum_{\substack{H\in\mathscr{U}\\ d^0H\geqslant t}} \frac{\mu^2(H)|C(M, H)|}{|H|\Phi^2(H)} \ll \sum_{h=t}^{\infty} q^{-3h/4}(\log h)^2 \ll q^{-t/2}.$$

De (V.13) on déduit immédiatement la première assertion.

La série $\mathfrak{S}(M)$ s'écrit comme produit eulérien absolument convergent

$$\mathfrak{S}(M) = \prod_{P\in\mathscr{S}} \left(1 + \frac{C(M, P)}{|P|\Phi^2(P)}\right).$$

La proposition V.3 nous donne

$$\mathfrak{S}(M) \geqslant \prod_{\substack{P\in\mathscr{S}\\ P\nmid M}} (1-\Phi^{-2}(P)) \geqslant \prod_{P\in\mathscr{S}} (1-\Phi^{-2}(P)),$$

ce dernier produit est strictement positif, et ne dépend que de q.

PROPOSITION V.6. *La série*

$$\mathfrak{S}^*(M) = \sum_{H\in\mathscr{U}} \frac{\mu^2(H)C^*(M, H)}{\Phi^3(H)} \tag{V.15}$$

est absolument convergente. De plus, pour tout entier $t \geqslant 2$,

$$\sum_{\substack{H\in\mathscr{U}\\ d^0H\geqslant t}} \frac{\mu^2(H)|C^*(M, H)|}{\Phi^3(H)} \ll q^{-t/2}. \tag{V.16}$$

Enfin,

$$\mathfrak{S}^*(M) \geqslant a_1 > 0. \tag{V.17}$$

Démonstration. Identique à celle de la proposition précédente.

VI. Majoration de sommes de caractères. On pose

$$\varrho = 2^{-k} \quad \text{et} \quad \tau = 2^{-2k}. \tag{VI.1}$$

On prolonge la fonction d en 0 en posant $d(0) = 1$, ce qui permet de formuler les majorations de façon plus concise.

LEMME. *Soient des entiers* $r \geqslant 0$ *et* $j > 0$. *Alors, on a*

$$\sum_{A\in F_j} d(A)^r \leqslant j^{2r-1}q^r. \tag{VI.2}$$

Démonstration. La relation $d(AB) \leqslant d(A)d(B)$, vraie pour tout couple (A, B) de polynômes, permet de démontrer (VI.2) par récurrence sur r.

Dans ce qui suit, G et H sont des polynômes premiers entre eux.

PROPOSITION VI.1. *Pour tout entier* $j > 0$, *on a*

(VI.3) $$\left|\sum_{A\in F_j} E\left(\frac{G}{H}A^k\right)\right| \ll j^{1/4e} q^j \operatorname{Sup}\{|H|^{-e}, q^{-ej}, |H|q^{-kej}\}.$$

Démonstration. Comme pour le lemme 5, page 215 de [8], en appliquant $(k-1)$ fois l'inégalité de Schwarz, on obtient, en posant

$$S = \sum_{A\in F_j} E\left(\frac{G}{H}A^k\right),$$

$$|S|^{2^{k-1}} \leqslant q^{j(2^{k-1}-k+1)} \sum_{(A_1,\dots,A_{k-1})\in F_j^{k-1}} V(A_1 \dots A_{k-1}),$$

où, pour tout polynôme A,

$$V(A) = \begin{cases} 1, & \text{si} \quad v\left(\left\{\frac{G}{H}A\right\}\right) > j, \\ 0, & \text{sinon.} \end{cases}$$

On en déduit

$$|S|^{2^{k-1}} \leqslant (q-1)^{k-2} q^{j(2^{k-1}-k+1)} \sum_{A\in F_t} V(A) d(A)^{k-1},$$

avec

$$t = (k-1)(j-1)+1.$$

On a

$$\sum_{A\in F_t} V(A) \leqslant \begin{cases} q^t/|H| & \text{si} \quad d^0H \leqslant j, \\ q^{t-j} & \text{si} \quad j < d^0H \leqslant t, \\ |H|q^{-j} & \text{si} \quad t < d^0H. \end{cases}$$

L'inégalité de Schwarz et la majoration (VI.2) nous donnent

$$|S|^{2^k} \leqslant (q-1)^{2k-4} q^{j(2^k-2k+2)} t^{2^{2k-2}} q^t \operatorname{Sup}\{q^t/|H|, q^{t-j}, |H|q^{-j}\},$$

$$|S|^{2^k} \leqslant q^{k-2} q^{2^k j} t^{2^{2k-2}} \operatorname{Sup}\{|H|^{-1}, q^{-j}, |H|q^{-kj}\}.$$

Proposition VI.2. *Soient a et b des entiers strictement positifs, $\mathscr{A}$ une partie de F_a, $\mathscr{B}$ une partie de F_b, et*

(VI.4) $$\mathscr{S}(\mathscr{A}, \mathscr{B}) = \sum_{A\in\mathscr{A}} \sum_{B\in\mathscr{B}} E\left(\frac{G}{H}A^kB^k\right).$$

Alors, on a

(VI.5) $$|\mathscr{S}(\mathscr{A}, \mathscr{B})| \ll (a+b)^{1/4\tau} q^{a+b} \operatorname{Sup}\{|H|^{-\tau}, |H|q^{-k\tau(a+b)}, \operatorname{Inf}(q^{-\tau a}, q^{-\tau b})\}.$$

Démonstration. L'inégalité de Schwarz nous donne

$$|\mathscr{S}(\mathscr{A}, \mathscr{B})|^2 \leqslant q^a \sum_{A\in\mathscr{A}} \left|\sum_{B\in\mathscr{B}} E\left(\frac{G}{H}A^kB^k\right)\right|^2 \leqslant q^a \sum_{B_1\in\mathscr{B}} \sum_{B_2\in\mathscr{B}} \mathscr{S}_{B_1,B_2},$$

où, pour $B_1\in F_b$, $B_2\in F_b$,

$$S_{B_1,B_2} = \sum_{A\in F_a} E\left(\frac{G}{H}A^k[B_1^k - B_2^k]\right).$$

En utilisant k fois l'inégalité de Schwarz on obtient

$$|\mathscr{S}(\mathscr{A}, \mathscr{B})|^{2^{k+1}} \leqslant q^{2^k a + 2^{k+1} b - 2b} \sum_{B_1\in F_b} \sum_{B_2\in F_b} |S_{B_1,B_2}|^{2^k}.$$

En procédant encore comme pour le lemme 5 de [8], on obtient

$$|\mathscr{S}(\mathscr{A}, \mathscr{B})|^{2^{k+1}} \leqslant q^{2^{k+1}(a+b) - ka - 2b} \sum_{(A_1,\dots,A_k)\in F_a^k} \left|\sum_{B\in F_b} E\left(k!\frac{G}{H}A_1 \dots A_kB^k\right)\right|^2.$$

En utilisant à nouveau $k-2$ fois l'inégalité de Schwarz, on obtient

$$|\mathscr{S}(\mathscr{A}, \mathscr{B})|^{2^{2k-1}} \leqslant q^{(a+b)(2^{2k-1}-k)+b} \sum_{\substack{(A_1,\dots,A_k)\in F_a^k \\ (B_1,\dots,B_{k-1})\in F_b^{k-1}}} W(A_1 \dots A_kB_1 \dots B_{k-1}),$$

où, pour tout polynôme H,

$$W(H) = \begin{cases} 1, & \text{si} \quad v\left(\left\{\frac{G}{H}A\right\}\right) > b, \\ 0, & \text{sinon.} \end{cases}$$

En posant $t = k(a-1)+(k-1)(b-1)+1$, on a

$$|\mathscr{S}(\mathscr{A}, \mathscr{B})|^{2^{2k-2}} \leqslant (q-1)^{2k-2} q^{(a+b)(2^{2k-1}-k)+b} \sum_{A\in F_t} W(A)(d(A))^{2k-1}.$$

Comme précédemment, avec la majoration (VI.2) on a

$$|\mathscr{S}(\mathscr{A}, \mathscr{B})|^{2^{2k}} \leqslant q^{2k-2} k^{4k-2-1} (a+b)^{4k-2-1} q^{2^{2k}(a+b)} \operatorname{Sup}\{1/|H|, q^{-b}, |H|q^{-k(a+b)}\}.$$

On obtient (VI.5) en remarquant que les ensembles $\mathscr{A}$ et $\mathscr{B}$ jouent des rôles symétriques.

Proposition VI.3. *Soient x, a et b des entiers strictement positifs, $\mathscr{A}$ un ensemble de polynômes A tels que $a \leqslant d^0A < a+x$, $\mathscr{B}$ un ensemble de polynômes B tels que $b \leqslant d^0B < b+x$. Soit*

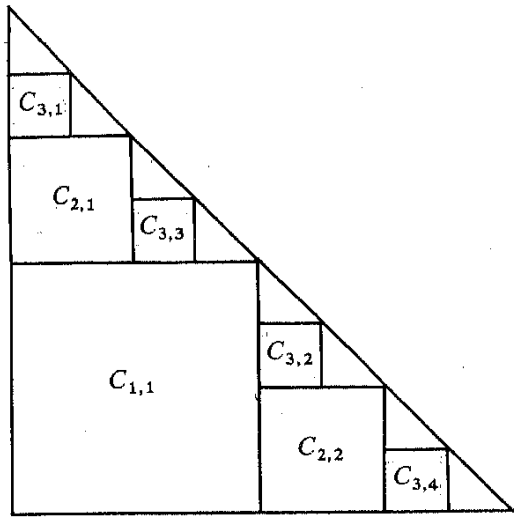
(VI.6) $$\mathscr{T}(\mathscr{A}, \mathscr{B}) = \sum_{A\in\mathscr{A}} \sum_{\substack{B\in\mathscr{B} \\ d^0(AB) < a+b+x}} E\left(\frac{G}{H}A^kB^k\right).$$

Alors, on a

(VI.7) $$|\mathscr{T}(\mathscr{A}, \mathscr{B})| \ll x(a+b+x)^{1/4\tau} q^{a+b+x} \operatorname{Sup}\{|H|^{-\tau}, q^{-(a+b+x)\tau/2}, |H|q^{-k\tau(a+b+x)}\}.$$

Démonstration. Désignons par T l'ensemble des couples d'entiers (α, β) tels que $a \leqslant \alpha < a+x$ et $b \leqslant \beta < a+b+x-\alpha$.

Partageons l'ensemble T en ensembles élémentaires $C_{i,j}$ définis de la façon suivante: i est un entier de l'intervalle $[1, \log(x)/\log(2)+1]$, j varie de 1 à 2^{i-1}.



$$C_{1,1} = [a, a+x/2[\times [b, b+x/2[\cap \mathbf{Z} \times \mathbf{Z}.$$

Si $i \geqslant 2$, si

$$j-1 = \sum_{r=0}^{i-2} d_{j,r} 2^r, \quad d_{j,r} \in \{0, 1\},$$

est le développement de $j-1$ en base 2,

$$C_{i,j} = [a_{i,j}, a_{i,j}+x2^{-i}[\times [b_{i,j}, b_{i,j}+x2^{-i}[\cap \mathbf{Z} \times \mathbf{Z},$$

où,

$$a_{i,j} = a + \sum_{r=0}^{i-2} d_{j,r} 2^{-r-1}, \quad b_{i,j} = b + \sum_{r=0}^{i-2} e_{j,r} 2^{-r-1},$$

les coefficients $d_{j,r}$ et $e_{j,r}$ étant liés par la relation

$$d_{j,r} + e_{j,r} = 1.$$

De ce fait, lorsque j varie de 1 à 2^{i-1}, on a

$$(*) \qquad a_{i,j} + b_{i,j} + x2^{1-i} = a+b+x.$$

Le plus grand des nombres $a_{i,j}+x2^{-i}$ est $a+x-x2^{-K}$, le plus grand des nombres $b_{i,j}+x2^{-i}$ est $b+x-x2^{-K}$, où $K = [\log(x)/\log(2)]+1$. Il n'y a pas

d'entier dans les intervalles $[a+x-x2^{-K}, a+x[$, $[b+x-x2^{-K}, b+x[$. Les ensembles $C_{i,j}$ $(1 \leqslant i \leqslant K, 1 \leqslant j \leqslant 2^{i-1})$ forment une partition de T, et, si on pose

$$S_{i,j} = \sum_{(\alpha,\beta)\in C_{i,j}} \sum_{\substack{A\in\mathscr{A} \\ d^0A=\alpha}} \sum_{\substack{B\in\mathscr{B} \\ d^0B=\beta}} E\left(\frac{G}{H} A^k B^k\right),$$

$$\mathscr{T}(\mathscr{A}, \mathscr{B}) = \sum_{i=1}^{K} \sum_{j=1}^{2^{i-1}} S_{i,j}.$$

La proposition précédente permet de majorer chacune des sommes $S_{i,j}$. Compte tenu de l'égalité (*), on obtient

$$|S_{i,j}| \ll (a+b+x)^{1/4\tau} q^{a+b+x} \operatorname{Sup}(|H|^{-\tau}, |H| q^{-k\tau(a+b+x)}, q^{-\tau(a+b+x)/2}).$$

Il y a $2^K - 1 < 2x$ sommes $S_{i,j}$.

Proposition VI.4. *Soient x, a, b et c des entiers strictement positifs avec $b \leqslant c$, $\mathscr{A}$ un ensemble de polynômes A tels que $a \leqslant d^0A < a+x$ et $\mathscr{B}$ un ensemble de polynômes B tels que $b \leqslant d^0B < c+x$. Soit*

$$(VI.8) \qquad \mathscr{U}(\mathscr{A}, \mathscr{B}) = \sum_{A\in\mathscr{A}} \sum_{\substack{B\in\mathscr{B} \\ d^0(AB) < a+c+x}} E\left(\frac{G}{H} A^k B^k\right).$$

Alors, on a

$$(VI.9) \qquad |\mathscr{U}(\mathscr{A}, \mathscr{B})| \ll x(a+c+x)^{1/4\tau} q^{a+c+x} \operatorname{Sup}\{|H|^{-\tau}, q^{-(a+c+x)\tau/2}, |H| q^{-k\tau(a+c+x)}\}.$$

Démonstration. On partage la somme $\mathscr{U}(\mathscr{A}, \mathscr{B})$ en deux sommes

$$\sum_{A\in\mathscr{A}} \sum_{B\in F_c\cap\mathscr{B}} E\left(\frac{G}{H} A^k B^k\right) \quad \text{et} \quad \sum_{A\in\mathscr{A}} \sum_{\substack{B\in\mathscr{B} \\ c \leqslant d^0B < a+c+x-d^0A}} E\left(\frac{G}{H} A^k B^k\right)$$

que l'on majore à l'aide des relations (VI.5) et (VI.7).

VII. Majoration de la somme $\sum_{P\in\mathscr{P}\cap F_a} E\left(\frac{G}{H} P^k\right)$. On conserve les hypothèses du paragraphe précédent. On suppose de plus que $d^0H \in [2kr, ka-2kr]$, les entiers a et r étant tels que

$$r > 0, \quad a > 4kr.$$

On pose

$$(VII.1) \qquad S = \sum_{P\in\mathscr{P}\cap F_a} E\left(\frac{G}{H} P^k\right),$$

$$(VII.2) \qquad B = \prod_{\substack{P\in\mathscr{P}\cap\mathscr{U} \\ d^0P < a/2}} P.$$

On désigne par $\mathscr{D}$ l'ensemble des diviseurs unitaires de B, par $\mathscr{D}'$ l'ensemble des polynômes $D\in\mathscr{D}$ dont tous les facteurs irréductibles sont de degré strictement inférieur à $2r$ et par $\mathscr{D}''$ le complémentaire de $\mathscr{D}'$ dans $\mathscr{D}$. On désigne par $\mathscr{D}_0$, respectivement $\mathscr{D}_1$, l'ensemble des $D\in\mathscr{D}$ tels que $\mu(D)=1$, respectivement, tels que $\mu(D)=-1$.

Si $D\in\mathscr{D}$ est tel que $d^0D<a$, on pose

$$S_D=\sum_{A\in F_{a-d^0D}^0} E\left(\frac{G}{H}A^kD^k\right). \tag{VII.3}$$

Proposition VII.1. *On a*

$$\left|S-\sum_{\substack{D\in\mathscr{D}\\ d^0D<a}}\mu(D)S_D\right|\leqslant q^{(a+1)/2}. \tag{VII.4}$$

Démonstration. On a

$$\left|S-\sum_{\substack{P\in\mathscr{P}\\ a/2\leqslant d^0P<a}} E\left(\frac{G}{H}P^k\right)\right|\leqslant q^{(a+1)/2},$$

et, avec (VII.2),

$$\sum_{\substack{P\in\mathscr{P}\\ a/2\leqslant d^0P<a}} E\left(\frac{G}{H}P^k\right)=\sum_{\substack{U\in F_a\\ (U,B)=1}} E\left(\frac{G}{H}U^k\right).$$

D'autre part, l'identité de Möbius nous donne

$$\sum_{\substack{U\in F_a\\ (U,B)=1}} E\left(\frac{G}{H}U^k\right)=\sum_{U\in F_a}\sum_{\substack{D\in\mathscr{U}\\ D|(U,B)}}\mu(D)E\left(\frac{G}{H}U^k\right)=\sum_{\substack{D\in\mathscr{U}\\ D|B\\ d^0D<a}}\mu(D)\sum_{\substack{U\in F_a\\ D|U}}E\left(\frac{G}{H}U^k\right);$$

et (VII.4) se déduit alors de (VII.3).

Proposition VII.2. *Pour $j\in\{0,1\}$, on a*

$$\left|\sum_{\substack{D\in\mathscr{D}_j\\ d^0D<r}}S_D\right|\ll ra^{1/4\varrho}q^{a-k\varrho r}. \tag{VII.5}$$

Démonstration. Soit $D\in\mathscr{D}_j\cap F_r$. Posons

$$H'=H/(H,D^k)\quad\text{et}\quad G'=GD^k/(H,D^k).$$

Les polynômes H' et G' sont premiers entre eux, et,

$$S_D=\sum_{A\in F_{a-d^0D}^0}E(G'A^k/H').$$

Avec (VI.3) il vient

$$|S_D|\ll 1+(a-d^0D)^{1/4\varrho}q^{a-d^0D}\operatorname{Sup}(|H'|^{-\varrho},\,q^{-\varrho(a-d^0D)},\,|H'|^{\varrho}q^{-k\varrho(a-d^0D)}).$$

D'autre part,

$$kr\leqslant d^0H-kd^0D\leqslant d^0H'\leqslant d^0H\leqslant ka-2kr,$$

donc

$$|S_D|\ll a^{1/4\varrho}q^{a-k\varrho r-d^0D},$$

d'où, (VII.5).

Proposition VII.3. *Pour $j\in\{0,1\}$, on a*

$$\left|\sum_{\substack{D\in\mathscr{D}_j\\ r\leqslant d^0D<a-r}}S_D\right|\ll a^{1+1/\tau}q^{a-2k\tau r}. \tag{VII.6}$$

Démonstration. On applique la proposition VI.4. Les inégalités vérifiées par a, r et d^0H donnent (VII.6).

Proposition VII.4. *Soit, pour tout entier $j>0$, $h(j)$ le nombre de polynômes $D\in\mathscr{D}'$ tels que $d^0D<j$. Alors, on a*

$$h(j)\leqslant q^{j(1-(1/2r))+2qr(\log q)^{-2}}. \tag{VII.7}$$

Démonstration. Posons

$$v=1-(1/2r).$$

Si $D\in\mathscr{D}'$, D est sans facteur carré, et tous ses facteurs irréductibles sont de degré strictement inférieur à $2r$. On a donc

$$h(j)\leqslant\sum_{D\in\mathscr{D}'\cap F_j}(q^j|D|^{-1})^v\leqslant q^{jv}\prod_{P\in F_{2r}\cap\mathscr{P}\cap\mathscr{U}}(1+|P|^{-v}),$$

$$\log\left(h(j)q^{-jv}\right)\leqslant\sum_{P\in F_{2r}\cap\mathscr{P}\cap\mathscr{U}}\log(1+|P|^{-v})\leqslant\sum_{P\in F_{2r}\cap\mathscr{P}\cap\mathscr{U}}|P|^{-v}\leqslant\sum_{j=1}^{2r-1}q^{(1-v)j},$$

$$\log\left(h(j)q^{-jv}\right)\leqslant\frac{q^{2r(1-v)}}{(1-v)\log(q)}\leqslant 2rq/\log(q).$$

La majoration de $h(j)$ s'en déduit.

Proposition VII. 5. *Pour $j\in\{0,1\}$, on a*

$$\left|\sum_{\substack{D\in\mathscr{D}'\cap\mathscr{D}_j\\ a-r\leqslant d^0D<a}}S_D\right|\ll rq^{2rq(\log q)^{-2}+a(1-(1/2r))}. \tag{VII.8}$$

Démonstration. On a

$$\left|\sum_{\substack{D\in\mathscr{D}'\cap\mathscr{D}_j\\ a-r\leqslant d^0D<a}}S_D\right|=\left|\sum_{A\in F_r^0}\sum_{\substack{D\in\mathscr{D}'\cap\mathscr{D}_j\\ a-r\leqslant d^0D<a-d^0A}}E\left(\frac{G}{H}A^kD^k\right)\right|\leqslant\sum_{A\in F_r^0}h(a-d^0A),$$

d'où, avec (VII.7),

$$\Big|\sum_{\substack{D\in\mathscr{D}''\cap\mathscr{P}_j\\ a-r\leqslant d^0D<a}} S_D\Big| \leqslant q^{2rq(\log q)^{-2}} q^{(r-a)/2r} \sum_{A\in F_r^0} |A|^{-1}.$$

PROPOSITION VII.6. *Pour $j\in\{0,1\}$, on a*

$$\Big|\sum_{\substack{D\in\mathscr{D}''\cap\mathscr{P}_j\\ a-r\leqslant d^0D<a}} S_D\Big| \ll a^{1+1/4\tau}(\log a) r q^{a-k\tau r}. \tag{VII.9}$$

Démonstration. On pose

$$T=\sum_{\substack{D\in\mathscr{D}''\cap\mathscr{P}_j\\ a-r\leqslant d^0D<a}} S_D.$$

Alors,

$$T=\sum_{A\in F_r^0}\sum_{\substack{D\in\mathscr{D}''\cap\mathscr{P}_j\\ a-r<d^0D<a-d^0A}} E\left(\frac{G}{H}A^kD^k\right).$$

Si $D\in\mathscr{D}''$, D a un facteur irréductible unitaire P tel que $d^0P>2r$, et D a $\omega(D)<a$ facteurs irréductibles unitaires. Si $b\in\{1,\dots,a-1\}$, on pose

$$T_b=\sum_{A\in F_r^0}\sum_{\substack{D\in\mathscr{D}''\cap\mathscr{P}_j\\ a-r\leqslant d^0D<a-d^0A\\ \omega(D)=b}} E\left(\frac{G}{H}A^kD^k\right).$$

Posons, pour $A\in F_r$,

$$\Theta_b(A)=\sum_{\substack{P\in\mathscr{S}\cap\mathscr{U}\\ 2r\leqslant d^0P<a/2}}\sum_{\substack{V\in\mathscr{Q}_{|j-1|}\\ a-r\leqslant d^0(VP)<a-d^0A\\ \omega(V)=b-1}} E\left(\frac{G}{H}A^kP^kV^k\right).$$

Alors,

$$T_b=\frac{1}{b}\sum_{A\in F_r^0}\Theta_b(A).$$

La somme $\Theta_b(A)$ s'écrit comme différence $\Theta^{(1)}-\Theta^{(2)}$ où

$$\Theta^{(1)}=\sum_{\substack{P\in\mathscr{S}\cap\mathscr{U}\\ 2r\leqslant d^0P<a/2}}\sum_{\substack{V\in\mathscr{Q}_{|j-1|}\\ d^0(VP)<a-d^0A\\ \omega(V)=b-1}} E\left(\frac{G}{H}A^kP^kV^k\right),$$

$$\Theta^{(2)}=\sum_{\substack{P\in\mathscr{S}\cap\mathscr{U}\\ 2r\leqslant d^0P<a/2}}\sum_{\substack{V\in\mathscr{Q}_{|j-1|}\\ d^0(VP)<a-r\\ \omega(V)=b-1}} E\left(\frac{G}{H}A^kP^kV^k\right).$$

La proposition VI.4 permet de majorer ces sommes. Si

$$H'=H/(H,A^k)\quad\text{et}\quad G'=GA^k/(H,A^k),$$

$$|\Theta^{(1)}|\ll a(a-d^0A)^{1/4\tau}q^{a-d^0A}\operatorname{Sup}\{|H'|^\tau, q^{-(a-d^0A)\tau}, |H'|^\tau q^{-k\tau(a-d^0A)}\},$$

$$|\Theta^{(2)}|\ll a(a-r)^{1/4\tau}q^{a-r}\operatorname{Sup}\{|H'|^\tau, q^{-(a-r)\tau}, |H'|^\tau q^{-k\tau(a-r)}\}.$$

Les relations vérifiées par a, r, d^0H et d^0A nous donnent

$$|\Theta^{(1)}-\Theta^{(2)}|\ll a^{1+1/4\tau}q^{a-k\tau r}|A|^{-1},$$

d'où,

$$|T|\ll a^{1+1/4\tau}q^{a-k\tau r}\left(\sum_{b=1}^{a-1}\frac{1}{b}\right)\left(\sum_{A\in F_r^0}\frac{1}{|A|}\right).$$

Nous pouvons maintenant conclure.

PROPOSITION VII.7. *Soient des entiers*

$$r>0\quad\text{et}\quad a>\operatorname{Sup}\{4kr, 4qr^2/(\log q)^2+2kr^2\}.$$

Si H est un polynôme tel que $d^0H\in[2kr, ka-2kr]$, si G est un polynôme premier à H,

$$\left|\sum_{P\in\mathscr{S}\cap F_a} E\left(\frac{G}{H}P^k\right)\right|\ll r(\log a)a^{1+1/4\tau}q^{a-k\tau r}. \tag{VII.10}$$

Démonstration. Immédiate avec (VII.4)–(VII.6), (VII.8) et (VII.9).

VIII. Évaluation de $f_i(t)$.

PROPOSITION VIII.1. *Soit $u\in\mathscr{P}$ de valuation $v(u)>(k-1)i$. Alors,*

(α) *si $v(u)>k(i-1)+1$, $f_i(u)=q^i$,*
(β) *si $v(u)=kj-r$, avec $1\leqslant j<i$ et $0\leqslant r<k$, $f_i(u)=q^j$,*
(γ) *si $v(u)=kj+1$, avec $0\leqslant j<i$, si $a\in F_q^0$ est tel que $v(u-aX^{-v(u)})>v(u)$,*

$$f_i(u)=q^j\sum_{b\in F_q}e(ab^k).$$

Démonstration. (α) est immédiat. Pour avoir (β) et (γ) on écrit

$$f_i(u)=1+\sum_{r=0}^{i-1}\sum_{A\in D_r}E(uA^k),$$

et on applique le corollaire de la proposition III.7.

Si $v(u)=kj-r$, avec $1\leqslant j<i$ et $0\leqslant r<k$,

$$f_i(u)=1+\sum_{r=0}^{i-1}(q-1)q^r=q^j,$$

si $v(u)=kj+1$, avec $0\leqslant j<i$, si $a\in\mathbf{F}_q^0$ est tel que $v(u-aX^{-v(u)})>kj+1$,

$$f_i(u)=1+\sum_{r=0}^{i-1}(q-1)q^r+q^j\sum_{b\in\mathbf{F}_q^0}e(ab^k).$$

On remarque que, pour tout entier $j>(k-1)i$, si $a\in\mathbf{F}_q^0$, si $v\in\mathscr{P}_j$, $f(v+aX^{-j})$ ne dépend que de a et de j. Posons

$$f(v+aX^{-j})=\varphi(a,j). \tag{VIII.1}$$

PROPOSITION VIII.2. *Soit $t=G/H+u$ appartenant à l'arc de Farey $\mathscr{U}_{G/H}$ où $d^0H\leqslant i$. Alors, on a*

$$f_i(t)=|H|^{-1}S(G,H)f_i(u). \tag{VIII.2}$$

Démonstration. On a

$$f_i\left(u+\frac{G}{H}\right)=\sum_{R\in\mathscr{C}_H}\sum_{L\in\mathbf{F}_{i-d^0H}}E\left(\left[u+\frac{G}{H}\right][R+LH]^k\right),$$

$$f_i\left(u+\frac{G}{H}\right)=\sum_{R\in\mathscr{C}_H}E\left(\frac{G}{H}R^k\right)\sum_{L\in\mathbf{F}_{i-d^0H}}E(uL^kH^k)E\left(u\left\{[R+LH]^k-L^kH^k\right\}\right).$$

Les relations (IV.1), (IV.7) et (IV.8) assurent que, si $R\in\mathscr{C}_H$, si $L\in\mathbf{F}_{i-d^0H}$,

$$v\left(u\left\{[R+LH]^k-L^kH^k\right\}\right)>1$$

et, par suite,

$$E\left(u\left\{[R+LH]^k-L^kH^k\right\}\right)=1.$$

On conclut avec (V.1) et la "deuxième formule de changement de variable".

PROPOSITION VIII.3. *Soit G/H une fraction de Farey telle que $ks<d^0H$. Soit $t\in\mathscr{U}_{G/H}$. Alors, on a*

$$|f_i(t)|\ll i^{1/4\varrho}q^{i-k\varrho s}.$$

Démonstration. Pour $ks<d^0H\leqslant i$, (VIII.2), (V.5) et la proposition précédente nous donnent

$$|f_i(t)|\ll|H|^{-1/k}q^i\leqslant q^{i-s}.$$

Si $i<d^0H$, les relations (IV.1), (IV.7) et (IV.8) assurent que

$$f_i(t)=f_i\left(\frac{G}{H}\right).$$

La majoration (VI.3) nous donne

$$|f_i(t)|\ll i^{1/4\varrho}q^iq^{k\varrho(1-s)}.$$

IX. Approximation de $g(t)$ sur les arcs majeurs. Les théorèmes de répartition des nombres premiers dans les progressions arithmétiques se

généralisent aux polynômes de $\mathbf{F}_q[X]$. On a les théorèmes suivants, conséquences immédiates de résultats établis dans [7].

THÉORÈME A. *Soit, pour tout entier $r>0$, $\pi(r)$ le nombre de polynômes irréductibles unitaires de degré r de $\mathbf{F}_q[X]$. Alors,*

$$q^r-2q^{r/2}\leqslant r\pi(r)\leqslant q^r.$$

THÉORÈME B. *Soit, pour tout entier $r>0$, pour tout polynôme unitaire $H\neq1$, pour tout polynôme K premier à H, $\Pi(r;H,K)$ le nombre de polynômes irréductibles de degré r de $\mathbf{F}_q[X]$ congrus à K modulo H. Alors,*

$$\left|\Pi(r;H,K)-\frac{q^r(q-1)}{r\Phi(H)}\right|\leqslant(q-1)(1+d^0H)q^{r/2}.$$

THÉORÈME C. *Soit, pour tout entier $r>0$, pour tout polynôme unitaire H, pour tout entier $k\geqslant0$ tel que $k+d^0H\geqslant1$, pour tout polynôme K premier à H, $\prod(r;H,k,K)$ le nombre de polynômes irréductibles P de $\mathbf{F}_q[X]$ de degré r, congrus à K modulo H et tels que*

$$d^0(X^{d^0P}K-X^{d^0K}P)<d^0P+d^0K-k.$$

Alors,

$$\left|\prod(r;H,k,K)-\frac{q^{r-k}}{r\Phi(H)}\right|\leqslant(k+1+d^0H)q^{r/2}.$$

Ce dernier théorème correspond à une partition des polynômes irréductibles suivant les différents restes modulo H, et les différents systèmes $(a_r,\ldots,a_{r-k})$ possibles, pour les coefficients des k termes de plus haut degré. Définissons d'une autre façon une telle partition.

DÉFINITION. Soit H un polynôme non nul. Les polynômes A et B sont dits *équivalents modulo $\mathscr{R}_H$* si

(1) A et B sont congrus modulo H,

(2) $d^0(A-B)<N$.

La proposition suivante donne un système de représentants des classes modulo $\mathscr{R}_H$.

PROPOSITION IX.1. *Soit H un polynôme non nul de degré $d^0H\leqslant ks$, soit $w=N-d^0H$, et, pour tout entier $r\geqslant N$, soit $\mathscr{A}_r$ l'ensemble des polynômes*

$$A=X^wHB+R$$

où B décrit D_{r-N}, où R décrit $\mathscr{C}_H$.

Alors, la réunion de $\mathscr{C}_H$ et des différents ensembles $\mathscr{A}_r$ ($r\geqslant N$), constitue un système de représentants des classes d'équivalence modulo $\mathscr{R}_H$.

Démonstration. Remarquons que des polynômes A et B de degrés différents au moins égaux à N, sont distincts modulo $\mathscr{R}_H$ et que des

polynômes A et B de degrés strictement inférieurs à N, congrus modulo H, sont congrus modulo $\mathscr{R}_H$.

Soit un entier $r \geqslant N$. Les polynômes de $\mathscr{A}_r$ sont de degré r. Soient

$$A = X^w HB + R \quad \text{et} \quad A' = X^w HB' + R'$$

des polynômes de $\mathscr{A}_r$. S'ils sont équivalents modulo $\mathscr{R}_H$, alors,

$$R = R' \quad \text{et} \quad d^0(A - A') < N,$$

d'où,

$$|X^w HB - X^w HB'| < q^N \quad \text{et} \quad |B - B'| < 1.$$

Chaque ensemble $\mathscr{A}_r$ contient au plus un représentant de chaque classe modulo $\mathscr{R}_H$, de plus,

$$\text{Card}(\mathscr{A}_r) = (q-1)q^{r-N}|H|.$$

Or, les polynômes de D_r se répartissent en exactement $(q-1)q^{r-N}|H|$ classes modulo $\mathscr{R}_H$, $\mathscr{A}_r$ est donc un système complet de représentants modulo $\mathscr{R}_H$, des polynômes de degré r.

PROPOSITION IX.2. *Soit t appartenant à l'arc de Farey $\mathscr{U}_{G/H}$. Alors, si A et A' sont des polynômes équivalents modulo $\mathscr{R}_H$,*

$$E(tA) = E(tA').$$

Démonstration. Immédiate.

PROPOSITION IX.3. *Soit $t = u + G/H$ appartenant à l'arc majeur $\mathscr{U}_{G/H}$. Alors,*

$$\left| g(t) - \frac{\mu(H)}{\Phi(H)} G(v(u)) \right| \leqslant (q-1)(2ks+1)q^{m/2+2ks}, \tag{IX.1}$$

où,

$$G(v(u)) = \begin{cases} (q-1)q^m/m, & \text{si} \quad v(u) > m+1, \\ -q^m/m, & \text{si} \quad v(u) = m+1, \\ 0, & \text{si} \quad v(u) \leqslant m. \end{cases} \tag{IX.2}$$

Démonstration. Utilisons le système de représentants des classes modulo $\mathscr{R}_H$ donné par la proposition IX.1. Si $A \in \mathscr{A}_m$, notons provisoirement $P(m; H, A)$ le nombre de polynômes irréductibles de degré m, équivalents à A modulo $\mathscr{R}_H$. Alors,

$$g(t) = \sum_{P \in I_m} E(tP) = \sum_{A \in \mathscr{A}_m} E(tA) P(m; H, A).$$

Si A et H ne sont pas premiers entre eux, et si P est un polynôme

irréductible congru à A modulo H, P divise H. Ceci ne peut se produire pour des polynômes P de degré $m > k(n-1) > ks \geqslant d^0 H$, d'où,

$$g(t) = \sum_{\substack{A \in \mathscr{A}_m \\ (A,H)=1}} E(tA) P(m; H, A).$$

Si les polynômes A et H sont premiers entre eux, le nombre $P(m; H, A)$ est le nombre $\prod(m; H, m-N, A)$ intervenant au théorème C, d'où,

$$\left| g(t) - \frac{q^N}{m\Phi(H)} \sum_{\substack{A \in \mathscr{A}_m \\ (A,H)=1}} E(At) \right| \leqslant (q-1)(m-N+1+d^0 H) q^{m-N} q^{m/2},$$

et, par définition de $\mathscr{A}_m$ et des arcs majeurs,

$$\left| g(t) - \frac{q^N}{m\Phi(H)} \sum_{R \in \mathscr{C}_H^*} E\left(\frac{G}{H} R\right) E(uR) \sum_{B \in D_{m-N}} E(uX^w HB) \right|$$
$$\leqslant (q-1)(2ks+1) q^{2ks} q^{m/2}.$$

Si $R \in \mathscr{C}_H$, $v(uR) > 1$ et $E(uR) = 1$. Comme pour le théorème 3.1, chapitre VI, de [6], on a

$$\sum_{R \in \mathscr{C}_H^*} E\left(\frac{G}{H} R\right) = \mu(H),$$

d'où,

$$\text{(i)} \qquad \left| g(t) - \frac{q^N \mu(H)}{m\Phi(H)} \sum_{B \in D_{m-N}} E(uX^w HB) \right| \leqslant (q-1)(2ks+1) q^{2ks} q^{m/2}.$$

On a

$$m+1-N > m-N > -N = v(X^w H) > -v(u).$$

On applique la "première formule de changement de variable". Il vient

$$\sum_{B \in D_{m-N}} E(uX^w HB) = |X^w H|^{-1} \sum_{B \in D_m} E(uB)$$
$$= \begin{cases} (q-1)q^{m-N}, & \text{si} \quad v(u) > m+1, \\ -q^{m-N}, & \text{si} \quad v(u) = m+1, \\ 0, & \text{si} \quad v(u) \leqslant m. \end{cases}$$

On pose

$$G(v(u)) = \frac{1}{m} \sum_{B \in D_m} E(uB),$$

d'où, (IX.2); (IX.1) se déduit alors de (i).

COROLLAIRE. *Sous les mêmes hypothèses,*

$$\text{(IX.3)} \qquad \left| g^2(t) - \frac{\mu^2(H)}{\Phi^2(H)} G^2(v(u)) \right| \leqslant 2(q-1)^2(2ks+1)q^{2ks}q^{3m/2}m^{-1}.$$

Démonstration. Immédiate avec le théorème A, (IX.1) et (IX.2).

X. Estimation de $f_i^*(t)$. L'étude de $f_i^*(t)$ sur les arcs majeurs nécessite une équivalence $\mathscr{R}_{i,H}$ donnant une partition de $\mathscr{I}$ plus fine que celle donnée par $\mathscr{R}_H$.

DÉFINITION. Soit H un polynôme non nul. Les polynômes A et B seront dits *équivalents modulo* $\mathscr{R}_{i,H}$ si

(1) A et B sont congrus modulo H,

(2) $d^0A < i-s$ et $d^0B < i-s$, ou, $d^0A \geqslant i-s$ et $d^0(A-B) < ki-ks-(k-1)d^0A$.

PROPOSITION X.1. *Soit H un polynôme non nul tel que $d^0H \leqslant ks$. Soient, pour tout entier $r \in \{i-s, \ldots, i-1\}$, $w(i,r) = k(i-r-s)+r-d^0H$, et $\mathscr{A}_i(r)$ l'ensemble des polynômes $A = X^{w(i,r)}HB+R$, où R décrit $\mathscr{C}_H$, où B décrit $D_{k(r+s-i)}$.*

Alors, la réunion de $\mathscr{C}_H$ et des ensembles $\mathscr{A}_i(r)$ $(i-s \leqslant r < i)$, constitue un système de représentants des classes modulo $\mathscr{R}_{i,H}$ des polynômes de F_i.

Démonstration. Comme pour la proposition IX.1.

PROPOSITION X.2. *Soit t appartenant à l'arc majeur $\mathscr{U}_{G/H}$. Si A et B sont des polynômes équivalents modulo $\mathscr{R}_{i,H}$, on a*

$$E(tA^k) = E(tB^k).$$

Démonstration. Immédiate.

Soit j un entier $\geqslant 2$. On pose

$$\text{(X.1)} \qquad \sigma_j = (q-1)\sum_{r=1}^{j-1} q^r/r.$$

On note ψ_i l'application de $\mathscr{P}_N$ dans C définie par

$$\text{(X.2)} \qquad \psi_i(u) = \begin{cases} \sigma_i, & \text{si} \quad v(u) > k(i-1)+1, \\ \sigma_j, & \text{si} \quad v(u) \in \{kj+2, \ldots, kj+k\}, \text{ avec } j < i-1, \\ \sigma_j + q^j\Big(\sum\limits_{b \in F_q^0} e(ab^k)\Big)/j, & \text{si} \quad v(u) = kj+1, \text{ avec } j < i, \\ & \text{et si } a \in F_q^0 \text{ est tel que} \\ & v(u-aX^{-v(u)}) > v(u). \end{cases}$$

On remarque que si $u = aX^{-v(u)}+v$, avec $a \in F_q^0$ et $v(v) > v(u)$, $\psi_i(u)$ ne dépend que de a et de $v(u)$. On pose alors

$$\text{(X.3)} \qquad \psi_i(u) = \varphi_i(a, v(u)).$$

PROPOSITION X.3. *Si $t = G/H+u$ appartient à l'arc majeur $\mathscr{U}_{G/H}$, on a*

$$\text{(X.4)} \qquad |f_i^*(t) - S^*(G,H)\Phi(H)^{-1}\psi_i(u)| \ll sq^{2ks}q^{i/2}.$$

Démonstration. On a

$$\text{(i)} \qquad f_i(t) = \sum_{r=1}^{i-1} S_r(t) \quad \text{où} \quad S_r(t) = \sum_{P \in I_r} E(tP^k).$$

Si $r \in \{i-s, \ldots, i-1\}$, si $A \in \mathscr{A}_i(r)$, notons $P_i(r; H, A)$ le nombre de polynômes $P \in I_r$ équivalents à A modulo $\mathscr{R}_{i,H}$. Si $r \in \{1, \ldots, i-s-1\}$, si $R \in \mathscr{C}_H$, soit $p_i(r; H, R)$ le nombre de polynômes $P \in I_r$ équivalents à R modulo $\mathscr{R}_{i,H}$. Alors, pour $r \in \{i-s, \ldots, i-1\}$,

$$S_r(t) = \sum_{\substack{A \in \mathscr{A}_i(r) \\ (A,H)=1}} E(tA^k)P_i(r; H, A),$$

pour $r \in \{1, \ldots, i-s-1\}$,

$$S_r(t) = \sum_{R \in \mathscr{C}_H^*} E(tR^k)p_i(r; H, R).$$

Si $r \in \{i-s, \ldots, i-1\}$, si $A \in \mathscr{A}_i(r)$ est premier à H, le nombre $P_i(r; H, A)$ est egal au nombre $\prod(r; H, kr+ks-ki, A)$ du théorème C, si $r \in \{1, \ldots, i-s-1\}$, si $R \in \mathscr{C}_H^*$, $p_i(r; H, R)$ est égal au nombre $\Pi(r; H, R)$ du théorème B. En procédant comme pour la fonction g, on obtient, pour $r \in \{i-s, \ldots, i-1\}$,

$$\left| S_r(t) - \sum_{R \in \mathscr{C}_H^*} E\left(\frac{G}{H}R^k\right) \sum_{B \in D_{k(r+s-i)}} E(u[R+X^{w(i,r)}HB]^k) \frac{q^{ki-ks-(k-1)r}}{r\Phi(H)} \right| \leqslant 2(q-1)ksq^{k(r+2s-i)}q^{r/2}.$$

Si $R \in \mathscr{C}_H$, si $B \in D_{k(r+s-i)}$,

$$E(u[R+X^{w(i,r)}HB]^k) = E(uX^{kw(i,r)}H^kB^k).$$

On applique la "deuxième formule de changement de variable". Il vient

$$\text{(ii)} \qquad \left| S_r(t) - \frac{S^*(G,H)}{r\Phi(H)} \sum_{B \in D_r} E(uB^k) \right| \leqslant 2(q-1)ksq^{k(r+2s-i)}q^{r/2}.$$

De la même façon, pour $r \in \{1+d^0H, \ldots, i-s-1\}$,

$$\text{(iii)} \qquad \left| S_r(t) - \frac{(q-1)q^r}{r\Phi(H)} S^*(G,H) \right| \leqslant (q-1)(ks+1)q^{ks}q^{r/2},$$

et, pour $r \in \{1, \ldots, d^0H\}$,

$$\text{(iv)} \qquad \left| S_r(t) - \frac{(q-1)q^r}{r\Phi(H)} S^*(G,H) \right| \leqslant (q-1)(ks+1)q^{ks}q^{r/2} + \Delta_r(H),$$

où $\Delta_r(H)$ désigne le nombre de diviseurs irréductibles de degré r de H. Notons que pour $r \in \{1, \dots, i-s-1\}$, on a

$$\sum_{B \in D_r} E(uB^k) = \mathrm{Card}\,(D_r) = (q-1)q^r.$$

On majore la somme des $\Delta_r(H)$ par d^0H. Les relations (i), (ii), (iii) et (iv), le corollaire de la proposition III.8, les relations (X.1) et (X.2) donnent alors le résultat annoncé.

PROPOSITION X.4. *Si $t \in \mathscr{A}'$, on a*

$$|f_i^*(t)| \ll s\log(i)\, i^{1+1/4\tau} q^{i-k\tau s/2}. \tag{X.5}$$

Démonstration. Si $t \in \mathscr{A}'$, il existe un arc de Farey $\mathscr{U}_{G/H}$ tel que $t \in \mathscr{U}_{G/H}$ et $ks < d^0H \leqslant N = k(n+1-s)$. Si $A \in F_i$, $E(tA^k) = E(GA^k/H)$, d'où,

$$f_i^*(t) = \sum_{P \in \mathscr{P} \cap F_i} E\left(\frac{G}{H} P^k\right).$$

Mais, $i \in \{n, n+1\}$, n et s vérifient les conditions (IV.1) et (IV.7). On peut donc appliquer la proposition VII.7 avec $r = \left[\dfrac{s-1}{2}\right]$, ce qui nous donne le résultat annoncé.

XI. Approximation de $R_i(M)$ et de $R_i^*(M)$. Posons

$$J_i(M) = \int_{\mathscr{A}} f_i(t) g^2(t) E(-Mt)\, dt, \tag{XI.1}$$

$$J_i'(M) = \int_{\mathscr{A}'} f_i(t) g^2(t) E(-Mt)\, dt, \tag{XI.2}$$

$$J_i^*(M) = \int_{\mathscr{A}} f_i^*(t) g^2(t) E(-Mt)\, dt, \tag{XI.3}$$

$$J_i^{*\prime}(M) = \int_{\mathscr{A}'} f_i^*(t) g^2(t) E(-Mt)\, dt. \tag{XI.4}$$

PROPOSITION XI.1. *On a les majorations*

$$|J_i'(M)| \ll i^{1/4\tau} q^{i-ks+m} m^{-1}, \tag{XI.5}$$

$$|J_i'(M)| \ll i^{1+1/4\tau} q^{i+m-(k\tau s/2)} m^{-1}. \tag{XI.6}$$

Démonstration. D'après la proposition VII.3, si $t \in \mathscr{A}'$,

$$|f_i(t)| \ll i^{1/4\tau} q^{i-ks},$$

d'où,

$$|J_i'(M)| \ll i^{1/4\tau} q^{i-ks} \int_{\mathscr{A}'} |g^2(t)|\, dt \leqslant i^{1/4\tau} q^{i-ks} \int_{\mathscr{P}} |g^2(t)|\, dt,$$

$$|J_i'(M)| \ll i^{1/4\tau} q^{i-ks} \mathrm{Card}\,(I_m),$$

(XI.5) se déduit alors du théorème A.

De même, d'après (X.5), si $t \in \mathscr{A}'$,

$$|f_i^*(t)| \ll s\log(i)\, i^{1+1/4\tau} q^{i-(k\tau s/2)},$$

le même procédé conduit à (XI.6).

PROPOSITION XI.2. *Soient*

$$K_n(M) = (q-2)q^n |M| m^{-2}, \tag{XI.7}$$

$$K_n^*(M) = (q-2)\sigma_n |M| m^{-2}, \tag{XI.8}$$

et, si k divise d^0M, soient

$$K_{n+1}(M) = q^n |M| \left(q^2 - 2q + r(M)\right) m^{-2}, \tag{XI.9}$$

$$K_{n+1}^*(M) = \left((q-2)\sigma_n + q^n\left(q - 3 + r(M) + \frac{2}{q}\right) n^{-1}\right) |M| m^{-2}, \tag{XI.10}$$

où $r(M)$ est le nombre de solutions $b \in \mathbf{F}_q$ de l'équation

$$\mathrm{sgn}(M) = b^k.$$

Alors, si $i \in \{n, n+1\}$, si G/H est le centre d'un arc majeur,

$$\left| I_{i,G/H}(M) - K_i(M) \frac{\mu^2(H) S(G, H)}{|H| \Phi^2(H)} E\left(-M\frac{G}{H}\right)\right| \ll \frac{s}{m} q^{i+3ks+m/2}, \tag{XI.11}$$

$$\left| I_{i,G/H}^*(M) - K_i^*(M) \frac{\mu^2(H) S^*(G, H)}{\Phi^3(H)} E\left(-M\frac{G}{H}\right)\right| \ll \frac{s}{m^2} q^{3ks+kn+i/2}. \tag{XI.12}$$

Démonstration. Soit $t = G/H + u$ appartenant à l'arc majeur $\mathscr{U}_{G/H}$. Alors, avec (VIII.2) et (IX.3), on a

$$\left| f_i(t) g^2(t) - \frac{\mu^2(H) S(G, H)}{|H| \Phi^2(H)} f_i(u) G^2(v(u))\right| \ll 2(q-1)^2 (2ks+1) q^{2ks+i+(3m/2)}/m,$$

avec (X.1), (X.2), (X.4) et (IX.3), on a

$$\left| f_i^*(t) g^2(t) - \frac{\mu^2(H) S^*(G, H)}{\Phi^3(H)} \psi_i(u) G^2(v(u))\right|$$

$$\ll s \cdot q^{2ks+2m(i/2)} m^{-2} + \frac{s}{m} q^{i+2ks+(3m/2)} \ll s \cdot q^{2ks+2m+(i/2)} m^{-2}.$$

Posons

$$L_i(M) = \int_{v(u) > N + d^0H} f_i(u) G(v(u))^2 E(-Mu)\, du, \tag{i}$$

$$L_i^*(M) = \int_{v(u) > N + d^0H} \psi_i(u) G^2(v(u)) E(-Mu)\, du. \tag{ii}$$

Alors, on a

$$\left|I_{i,G/H}(M)-L_i(M)\frac{\mu^2(H)S(G,H)}{|H|\Phi^2(H)}E\left(-M\frac{G}{H}\right)\right| \ll \frac{s}{m}q^{i+3ks+m/2},$$

$$\left|I^*_{i,G/H}(M)-L^*_i(M)\frac{\mu^2(H)S^*(G,H)}{\Phi^3(H)}E\left(-M\frac{G}{H}\right)\right| \ll \frac{s}{m^2}q^{3ks+kn+i/2}.$$

Il suffit d'établir les égalités

$$K_i(M)=L_i(M) \quad \text{et} \quad K^*_i(M)=L^*_i(M).$$

On a vu que $G(v(u))$ est nul si $m \geqslant v(u)$. D'autre part, si $v(u)>m$, $v(u)>k(n-1)+1$, d'après la proposition VIII.1 et la définition (X.2),

$$f_n(u)=q^n \quad \text{et} \quad \psi_n(u)=\sigma_n.$$

En remplaçant $G(v(u))$ par sa valeur on obtient

$$L_n(M)=q^n\left(\left(\frac{q^m(q-1)}{m}\right)^2\int_{\mathscr{P}_{1+m}}E(-Mu)\,du+ +(q^m/m)^2\sum_{b\in F_q^0}\int_{\mathscr{P}_{1+m}}E\left(-M(u+bX^{-m-1})\right)du\right),$$

$$L_n(M)=\frac{q^{m+n-1}}{m^2}\left((q-1)^2+\sum_{b\in F_q^0}e\left(-b\,\mathrm{sgn}(M)\right)\right)=\frac{q^{m+n-1}}{m^2}\left((q-1)^2-1\right),$$

$$L_n(M)=\frac{q^{m+n}}{m^2}(q-2);$$

et, de la même façon,

$$L^*_n(M)=\frac{\sigma_n q^m}{m^2}(q-2).$$

Le cas $i=n+1$ ne nous intéresse que si $m=d^0M=kn$. On a alors, avec la proposition VIII.1,

$$L_{n+1}(M)=\frac{(q-1)^2q^{2m+n+1}}{m^2}\int_{\mathscr{P}_{m+1}}E(-Mu)\,du+ +\sum_{b\in F_q^0}\int_{\mathscr{P}_{m+1}}\varphi(b,m+1)G^2(m+1)E\left(-M(u+bX^{-m})\right)du.$$

En remplaçant $\varphi(b,m+1)$ et $G(m+1)$ par leurs valeurs, on obtient

$$L_{n+1}(M)=\frac{(q-1)^2q^{m+n}}{m^2}+\sum_{b\in F_q^0}\frac{q^{m+n-1}}{m^2}\sum_{c\in F_q}e\left(b\left(c^k-\mathrm{sgn}(M)\right)\right).$$

Soit $r(M)$ le nombre de $c\in F_q$ tel que $\mathrm{sgn}(M)=c^k$. Alors,

$$L_{n+1}(M)=\frac{q^{m+n}}{m^2}\left((q-1)^2+\frac{1}{q}\left((q-1)r(M)\right)-\left(q-r(M)\right)\right),$$

$$L_{n+1}(M)=\frac{q^{m+n}}{m^2}(q^2-2q+r(M)).$$

Avec (X.2), on a

$$L^*_{n+1}(M)=\frac{(q-1)^2\sigma_{n+1}q^m}{m^2}\int_{\mathscr{P}_{m+1}}E(-Mu)du+ +\sum_{b\in F_q^0}\int_{\mathscr{P}_{m+1}}\varphi^*(b,m+1)G^2(m+1)E\left(-M(u+bX^{-m-1})\right)du,$$

d'où,

$$L^*_{n+1}(M)=\frac{(q-1)^2\sigma_{n+1}q^{m-1}}{m^2}+\sum_{b\in F_q^0}\left(\sigma_n+\frac{q^{m+n-1}}{nm^2}\sum_{c\in F_q^0}e(bc^k)\right)e\left(-\mathrm{sgn}(M)b\right),$$

$$L^*_{n+1}(M)=\frac{q^{m-1}}{m^2}\left((q-1)^2\sigma_{n+1}+\sigma_n\sum_{b\in F_q^0}e\left(-b\,\mathrm{sgn}(M)\right)\right)+ +\frac{q^n}{n}\sum_{\substack{b\in F_q^0\\ c\in F_q^0}}e\left(b\left(c^k-\mathrm{sgn}(M)\right)\right),$$

$$L^*_{n+1}(M)=\frac{q^{m-1}}{m^2}\left((q-1)^2\sigma_{n+1}-\sigma_n+q^nr(M)(q-1)-\left(q-1-r(M)\right)\right),$$

$$L^*_{n+1}(M)=\frac{q^m}{m^2}\left((q-2)\sigma_n+q^n\left(q-3+r(M)+\frac{2}{q}\right)\right).$$

On a les minorations.

(XI.13) $$K_{n+1}(M)\geqslant(q-2)q^{m+n+1}m^{-2},$$

(XI.14) $$K^*_n(M)\geqslant(q-1)(q-2)\,q^{m+n-1}n^{-1}m^{-q-2},$$

(XI.15) $$K^*_{n+1}(M)\geqslant(q-2)q^{m+n-1}n^{-1}m^{-2}.$$

Proposition XI.3. *Pour tout polynôme M de degré $d^0M\in]kn-k,\,kn]$, on a*

(XI.16) $$|R_n(M)-K_n(M)\mathfrak{S}(M)|\ll K_n(M)n^{1+(1/4q)-kqh},$$

(XI.17) $$|R^*_n(M)-K^*_n(M)\mathfrak{S}^*(M)|\ll K^*_n(M)n^{3+(1/4\tau)-(k\tau h/2)},$$

pour tout polynôme M de degré kn,

(XI.18) $$|R_{n+1}(M)-K_{n+1}(M)\mathfrak{S}(M)|\ll K_{n+1}(M)n^{1+(1/4q)-kqh},$$

(XI.19) $$|R^*_{n+1}(M)-K^*_{n+1}(M)\mathfrak{S}^*(M)| \ll K^*_{n+1}(M)n^{3+(1/4\tau)-(k\tau h/2)}.$$

Démonstration. On applique la proposition précédente. Avec (XI.5) et (V.13), il vient

$$|R_i(M)-K_i(M)\mathfrak{S}(M)|$$

$$\ll K_i(M)q^{-ks/2}+i^{1/4\varrho}q^{i-ks+m}m^{-1}+\frac{s}{m}q^{i+3ks+(m/2)}\sum_{\substack{H\in\mathfrak{A}\\ d^0H\leqslant ks}}\Phi(H),$$

d'où, avec (XI.7) et (XI.13),

$$|R_i(M)-K_i(M)\mathfrak{S}(M)| \ll K_i(M)\left[q^{-ks/2}+mi^{1/4\varrho}q^{-ks}+\frac{s}{m}q^{5ks-(m/2)}\right],$$

(XI.16) et (XI.18) se déduisent alors de (IV.1) et (IV.7).

On procède de même pour (XI.17) et (XI.19).

Cette démonstration achève la démonstration du théorème. Il suffit de choisir maintenant h suffisamment grand pour que $3+(1/4\tau)-(k\tau h/2)$ soit >0, c'est à dire $h>(3+2^{2k-2})2^{2k+1}/k$. Les nombres $R_i(M)$ et $R_i^*(M)$ sont alors asymptotiquement équivalents aux nombres $K_i(M)\mathfrak{S}(M)$ et $K_i^*(M)\mathfrak{S}^*(M)$ qui sont strictement positifs.

Références

[1] R. Ayoub, *An introduction to the analytic theory of numbers*, Mathematical Surveys, n°10, Amer. Math. Soc., Providence, R. I., 1963.

[2] M. Car, *Le problème de Waring pour l'anneau des polynômes sur un corps fini*, C.R.A.S., Paris, Série A et B, 273 (1971).

[3] — *Sommes de carrés dans* $\mathbf{F}_q[X]$, Dissertationes Mathematicae CCXV, Warszawa 1983, 40 pp.

[4] — *Sommes de carrés et d'irréductibles dans* $\mathbf{F}_q[X]$, Annales de la Faculté des Sciences de Toulouse, décembre 1981.

[5] D. R. Hayes, *The expression of a polynomial as sum of three irreducibles*, Acta Arith. 11 (1966), p. 461–488.

[6] K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin 1957.

[7] G. Rhin, *Répartition modulo* 1 *dans un corps de séries formelles sur un corps fini*, Dissertationes Mathematicae XCV, Warszawa 1972, 80 pp.

[8] W. Webb, *Waring's problem in* GF$[q, x]$, Acta Arith. 22 (1972), p. 207–220.

[9] — *On the representation of polynomials over finite fields as sums of powers and irreducibles*, Rocky Mountain J. Math. 3 (1973), p. 23–29.

Reçu le 9.4.1982
et dans la forme modifiée le 7.3.1983 (1299)

ACTA ARITHMETICA
XLIV (1984)

On elliptic units and class number of a certain dihedral extension of degree $2l$

by

HEIMA HAYASHI (Kumamoto)

0. Introduction. G. Gras and M.-N. Gras have introduced an effective method to compute the class number of the real abelian number field, utilizing cyclotomic units ([2]). K. Nakamula has introduced an effective method to compute the class number of a certain non-galois number field, utilizing its elliptic units ([6]). Nakamula also considered more general problems concerning the class number formulas related to elliptic units, and pointed out some essential issues ([7]). Our purpose is to establish the similar algorithms to those in [2] for any abelian extension over an imaginary quadratic number field, utilizing elliptic units instead of cyclotomic units. In the present note, as the first step of our purpose, we shall treat the following special case.

Let L be an abelian extension of degree l with an odd prime number l over an imaginary quadratic number field K such that L is a dihedral extension of degree $2l$ over rational number field Q. For each number field $\_$, we denote by $h_\_$, $E_\_$ and $\mu_\_$ the class number of $\_$, the unit group in $\_$ and the torsion part of $E_\_$ respectively. Then the index formula of the following form is well known (cf. [9]):

$$[E_L:\ \mu_L\eta^{Z[G]}] = M\frac{h_L}{h_K},$$

where G denotes the Galois group of L over K, $Z[G]$ the group ring of G over the ring Z of rational integers, η an element of E_L explicitly given by using the values of the Dedekind η-function and M a constant explicitly given depending on the choice of η (§ 1). Our problem treated here is how to give an effective algorithm for the numerical determination of $[E_L:\ \mu_L\eta^{Z[G]}]$. In this note we shall show a procedure to solve this problem. Especially we shall treat more precisely the case where $l=5$. The reason why we treat the case where $l=5$ is only that the case where $l=3$ has been partially treated by Nakamula (I of [6]), though his treatment is slightly different from ours.

It is also possible and interesting to establish the similar arguments in the treatment of the arithmetic of the maximal real subfield Ω of L. This