We recall that $f(i) = \lfloor i^{1+\varepsilon/2} \rfloor$ and that $i_0 = i_0(q)$ is the smallest integer for which $f(i_0+1) \geqslant q$. A simple calculation shows $c_8 \cdot i_0/q \leqslant q^{-\varepsilon/4}$ for $q \geqslant c_9$. Choosing $t = \max\left\{c_9, \frac{12}{\lfloor \varepsilon \rfloor}+1\right\}$, by (26) and (28) we have

$$\begin{aligned}\text{Prob}\left\{\left|\left|\{\xi_i\colon 1 \leqslant i \leqslant k,\ \xi_i \equiv h \pmod q\}\right| - k/q\right| > t \text{ for some } h, q, k\right\}\\ \leqslant \sum_{q \geqslant c_9} \sum_{h=1}^{q} \text{Prob}\left\{\left|\{\xi_i\colon 1 \leqslant i \leqslant i_0(q),\ \xi_i \equiv h \pmod q\}\right| \geqslant t\right\}\\ \leqslant \sum_{q \geqslant c_9} \sum_{h=1}^{q} q^{-3} = \sum_{q \geqslant c_9} q^{-2} \leqslant 1/2.\end{aligned}$$

Thus the proof of Theorem 3 is complete.

References

[1] J. Beck, *Roth's estimate of the discrepancy of integer sequences is nearly sharp*, Combinatorica 1(4) (1981), pp. 319–325.

[2] — *Balanced two-colorings of finite sets in the square, I*, ibid. 1(4) (1981), pp. 327–335.

[3] J. Beck and T. Fiala, *"Integer-Making" theorems*, Discrete Applied Math. 3 (1981), pp. 1–8.

[4] J. H. Halton, *On the efficiency of certain quasirandom sequences of points in evaluating multi-dimensional integrals*, Num. Math. 2 (1960), pp. 84–90.

[5] K. F. Roth, *Remark concerning integer sequences*, Acta Arith. 9 (1964), pp. 257–260.

[6] W. M. Schmidt, *Irregularities of distribution, IV*, Inv. Math. 7 (1969), pp. 55–82.

[7] — *Irregularities of distribution, VII*, Acta Arith. 21 (1972), pp. 45–50.

[8] — *Lectures on irregularities of distribution*, Tata Institute of Fundamental Research, Lectures on Math. and Phys. 56 (1977).

MATHEMATICAL INSTITUTE
OF THE HUNGARIAN ACADEMY OF SCIENCES
H-1053 Budapest, Reáltanoda u. 13-15
Hungary

Received on 27. 11. 1981
and in revised form on 26. 7. 1982 (1280)

ACTA ARITHMETICA
XLIII (1984)

Polynômes de $F_q[X]$ ayant un diviseur de degré donné

par

MIREILLE CAR (Marseille)

1. Introduction. Soit F_q le corps fini à q éléments et $F_q[X]$ l'anneau des polynômes à une indéterminée sur le corps F_q.

Si -1 n'est pas carré dans le corps F_q, il y a une similitude parfaite entre l'étude des sommes de deux carrés dans $F_q[X]$ et l'étude des sommes de deux carrés dans l'anneau Z, comme le montrent la caractérisation des sommes de deux carrés donnée dans [7] ou l'estimation du nombre $A(n)$ de polynômes unitaires de degré n qui sont sommes de deux carrés obtenue dans [1].

Si -1 est carré dans le corps F_q, cette similitude disparait, et, le cas de la caractéristique 2 excepté, le problème des sommes de deux carrés devient trivial puisque tout polynôme de $F_q[X]$ est alors somme de deux carrés. On rend ce problème moins trivial en exigeant dans les sommes de deux carrés les conditions de degré les plus restrictives possibles, conditions qui sont automatiquement réalisées dans le cas où -1 n'est pas carré dans le corps F_q. Les polynômes de degré $2n$ ou $2n-1$ sommes de deux carrés

$$A^2 + B^2$$

où A et B sont des polynômes de degré au plus égal à n sont les polynômes de degré $2n$ ou $2n-1$ admettant un diviseur de degré n.

Par une méthode semblable à celle qu'ont utilisée Erdös [4] et Tenenbaum [9], on obtient dans [2] une estimation asymptotique du nombre $A(N)$ de polynômes unitaires de degré N de $F_q[X]$ ayant un facteur de degré égal à la partie entière de $N/2$, estimation donnée par le théorème suivant:

THÉORÈME. *Pour tout réel $\varepsilon > 0$, il existe un entier $N(q, \varepsilon)$ ne dépendant que de q et de ε, tel que, pour tout entier $N \geqslant N(q, \varepsilon)$ on ait*

$$\frac{q^N}{N^{a+\varepsilon}} \leqslant A(N) \ll \frac{q^N}{N^a}\,(\log N)^{-1/2},$$

où

$$\alpha = 1 - \frac{1+\log(\log 2)}{\log 2},$$

la constante impliquée par le symbole $\ll$ *ne dépendant que de* q.

Sous la forme d'un problème de diviseur, le problème étudié en [2] n'est qu'un cas particulier du problème suivant: Etant donnés deux entiers $0 \leqslant n \leqslant N$, peut-on estimer le nombre de polynômes de degré N de $\boldsymbol{F}_q[X]$ ayant un diviseur de degré n? Ce problème peut se poser que -1 soit ou ne soit pas carré dans le corps $\boldsymbol{F}_q$. C'est ce problème que nous étudions ici, en nous limitant aux polynômes unitaires, et, pour des raisons de symétrie, au cas où $N \geqslant 2n$. On supposera aussi $n \neq 0$ pour que le problème ne soit pas trivial.

Notons que si -1 est carré dans le corps $\boldsymbol{F}_q$, et si celui-ci n'est pas de caractéristique 2, ce dernier problème peut encore s'interpréter comme un problème de sommes de deux carrés. En effet, tout polynôme de degré N ayant un diviseur de degré n s'écrit comme somme de deux carrés A^2+B^2, où A et B sont des polynômes de degré au plus égal à $\mathrm{Sup}(n, N-n)$. Cette limitation des degrés étant moins naturelle que celle imposée en [2], nous ne nous intéresserons pas à cette interprétation.

On désigne par $F(N, n)$ le nombre de polynômes unitaires de degré N de $\boldsymbol{F}_q[X]$ admettant un diviseur de degré n. Si l'on impose au rapport N/n de rester borné, l'estimation des nombres $F(N, n)$ peut se faire comme celle des nombres $A(N)$ qui est faite en [2]. Lorsqu'on n'impose pas cette condition, l'estimation des nombres $F(N, n)$ se fait par une méthode légèrement différente, méthode utilisée dans [9] pour résoudre un problème analogue sur les entiers. Les résultats établis ici généralisent les résultats obtenus en [2] avec une minoration meilleure, semblable à la minoration obtenue en [11]. Ils peuvent etre résumés par le théorème suivant:

THÉORÈME. *Soit*

$$\alpha = 1 - \frac{1+\log(\log 2)}{\log 2}.$$

Alors,

(1) *si* n *et* N *sont des entiers tels que* $2 \leqslant n \leqslant N$, *on a*

$$F(N, n) \ll \frac{q^N}{n^\alpha} (\log n)^{-1/2},$$

(2) *il existe une constante absolue* $c > 0$, *effectivement calculable, et un entier* $n_0 \geqslant 1$, *tels que, pour tout entier* $n \geqslant n_0$, *pour tout entier* $N \geqslant 2n$, *on ait*

$$F(N, n) \geqslant \frac{q^N}{n^\alpha} \exp\left(-c\left(\log(n)\log(\log n)\right)^{1/2}\right)$$

les constantes impliquées par les symboles $\ll$ *ne dépendant que de* q.

Remarquons que ce théorème ne donne pas d'information pour tous les entiers n possibles. On n'a aucun résultat général pour les petites valeurs de n. Toutefois, on peut faire un calcul direct de $F(N, n)$ dans certains cas particuliers. Par exemple, on a sans difficulté que

$$F(N, 1) = \begin{cases} q^N\left[1 - \left(1 - \frac{1}{q}\right)^q\right] & \text{si} \quad N \geqslant q, \\ q^N\left[1 - \sum_{k=0}^{N} \left(-\frac{1}{q}\right)^k\right] & \text{si} \quad N < q. \end{cases}$$

2. Notations and conventions. Soit $\mathscr{U}$ l'ensemble des polynômes unitaires de $\boldsymbol{F}_q[X]$. Le mot polynôme désignera toujours un polynôme de $\mathscr{U}$. Soit A un tel polynôme. On note

$d^\circ A$ le degré de A,

$|A|$ le nombre $q^{d^\circ A}$.

Si A s'écrit comme produit

$$A = P_1^{u_1} \dots P_r^{u_r},$$

où $P_1, \dots, P_r$ sont des polynômes irréductibles deux à deux distincts, où $u_1, \dots, u_r$ sont des entiers strictement positifs, on pose

$$\omega(A) = r, \qquad \Omega(A) = u_1 + \dots + u_r.$$

Soit alors $i(n, A)$ l'ensemble des indices $i \in \{1, \dots, r\}$ tels que $d^\circ P_i \leqslant n$. On pose

$$\omega_n(A) = \mathrm{Card}\left(i(n, A)\right), \qquad \Omega_n(A) = \sum_{j \in i(n, A)} u_j.$$

Le polynôme A est dit sans facteur carré si $\omega(A) = \Omega(A)$. On désigne par $\mathscr{Q}$ l'ensemble des polynômes sans facteur carré.

Soient A et B deux polynômes. On note

$A \vee B$ le plus grand diviseur commun de A et de B,

$A \mid B$ la relation A divise B.

On désigne par $\mathscr{I}$ l'ensemble des polynômes irréductibles. Si n et N sont des entiers tels que $0 \leqslant n \leqslant N/2$, on désigne par $\mathscr{F}(N, n)$ l'ensemble

des polynômes de degré N de $\mathscr{U}$ admettant un diviseur de degré n. Si $\mathscr{B}$ est un ensemble fini de polynômes, on note $\|\mathscr{B}\|$ le cardinal de $\mathscr{B}$ et, pour tout nombre réel y, on note

$$\sigma_y(\mathscr{B}) \text{ la somme } \sum_{B\in\mathscr{B}} |B|^y.$$

3. Estimation des nombres $q_0(N,n)$, $p_k(N,n)$ et $P_k(N,n)$. Soient k, n, N des entiers positifs. Soient

$q_k(N,n)$ le nombre de polynômes $H\in\mathscr{Q}$ tels que $\omega_n(H)=k$, $d^\circ H=N$,

$p_k(N,n)$ le nombre de polynômes $H\in\mathscr{U}$ tels que $\omega_n(H)=k$, $d^\circ H=N$,

$P_k(N,n)$ le nombre de polynômes $H\in\mathscr{U}$ tels que $\Omega_n(H)=k$, $d^\circ H=N$.

On pose

$$q_k(N)=q_k(N,N),\quad p_k(N)=p_k(N,N),\quad P_k(N)=P_k(N,N).$$

Ces nombres ont été étudiés dans [3]. On y démontre le

THÉORÈME F. *Soit un nombre réel $A>0$. Si k et N sont des entiers tels que $1\leqslant k\leqslant A\log(N)$,*

$$q_k(N)\ll\frac{q^N(\log N)^{k-1}}{N(k-1)!},\quad p_k(N)\ll\frac{q^N(\log N)^{k-1}}{N(k-1)!},$$

les constantes impliquées par les symboles $\ll$ ne dépendant que de q et de A.

Soit un nombre réel $A\in]0,q[$. Si k et N sont des entiers tels que $1\leqslant k\leqslant A\log(N)$,

$$P_k(N)\ll\frac{q^N(\log N)^{k-1}}{N(k-1)!},$$

la constante impliquée par le symbole $\ll$ ne dépendant que de q et de A.

On désigne par $\pi(N)$ le nombre de polynômes irréductibles de degré N. On a

$$q_1(N)=p_1(N)=P_1(N)=\pi(N).$$

Il est bien connu que les polynômes irréductibles de $\boldsymbol{F}_q[X]$ ont une répartition analogue à celle des nombres premiers. Cette répartition est donnée par le théorème suivant dont on peut trouver une démonstration très simple dans [8].

THÉORÈME H. *Pour tout entier $k\geqslant 2$,*

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

On obtient une estimation des nombres $p_k(N,n)$ et $P_k(N,n)$ à partir de l'estimation des nombres $P_0(N,n)$. Cette dernière estimation fournit en outre une minoration de $q_0(N,n)$ qui sera utilisée au paragraphe 5.

3.1. Estimation des nombres $q_0(N,n)$ et $P_0(N,n)$. Du théorème H on déduit la relation

$$q_0(N,n)\leqslant P_0(N,n)\leqslant q_0(N,n)+\frac{q^{N-n}}{(q-1)(n+1)}. \tag{1}$$

Soit un nombre réel $x\geqslant 1$. On note $\mathscr{U}(N,x)$ l'ensemble des polynômes de degré N dont tous les facteurs irréductibles sont de degré strictement supérieur à x. On pose

$$P(N,x)=\|\mathscr{U}(N,x)\|. \tag{2}$$

Soit

$$V(x)=\prod_{\substack{p\in\mathscr{I}\\ d^\circ p\leqslant x}}\left(1-\frac{1}{|p|}\right). \tag{3}$$

Comme pour le théorème 1, p. 201 de [5], on démontre que le rapport

$$\frac{P(N,x)}{q^N V(x)}$$

reste borné par deux constantes strictement positives. La démonstration nécessite quelques notations supplémentaires. On choisit sur $\mathscr{I}$ une relation d'ordre total notée $\preceq$ telle que

$$d^\circ P\leqslant d^\circ Q\Rightarrow P\preceq Q.$$

Si $Q\in\mathscr{I}$, on note $[Q$, resp. $Q[$, l'ensemble des polynômes irréductibles P tels que $Q\preceq P$, resp. $P\preceq Q$ et $P\neq Q$. On note $\overline{\mathscr{U}}(N;Q)$ l'ensemble des polynômes de degré N dont tous les facteurs irréductibles sont dans $[Q$. On pose

$$\overline{P}(N,Q)=\|\overline{\mathscr{U}}(N,Q)\|, \tag{4}$$

$$\overline{V}(Q)=\prod_{p\in Q[}\left(1-\frac{1}{|p|}\right). \tag{5}$$

PROPOSITION 1. *Il existe des constantes absolues $a_1>0$ et $a_2>0$, telles que*

(a) *pour tout polynôme irréductible Q, pour tout entier $N\geqslant d^\circ Q$,*

$$a_1\overline{V}(Q)q^N\leqslant\overline{P}(N,Q)\leqslant a_2\overline{V}(Q)q^N, \tag{6}$$

(b) *pour tout nombre réel $x\geqslant 1$, pour tout entier $N>x$,*

$$a_1 V(x)q^N\leqslant P(N,x)\leqslant a_2 V(x)q^N. \tag{7}$$

Démonstration. Le théorème H remplaçant le théorème des nombres premiers, comme pour le théorème 429 de [6], on démontre qu'il

existe des constantes absolues $a_1 > 0$ et $a_2 > 0$ telles que, pour tout $x \geqslant 1$, on ait

$$a_1 \leqslant xV(x) \leqslant a_2. \tag{8}$$

Le théorème II nous donne aussi, pour tout polynôme irréductible P,

$$1 - \frac{\log 4}{d^\circ P} \leqslant \frac{V(d^\circ P)}{\overline{V}(P)} \leqslant 1. \tag{9}$$

Soit un nombre réel $x \geqslant 1$. Soit Q un polynôme irréductible. Soit un entier N.

Si $x < N \leqslant 2x$, resp. si $d^\circ Q \leqslant N < 2d^\circ Q$, et si $H \in \mathscr{U}(N, x)$, resp. si $H \in \overline{\mathscr{U}}(N, Q)$, H est irréductible, et

$$P(N, x) = \pi(N), \quad \text{resp.} \quad \overline{P}(N, Q) = \pi(N).$$

Le théorème II et les relations (8) et (9) nous donnent

$$\frac{29}{200a_2} \leqslant \frac{P(N, x)}{q^N V(x)} \leqslant \frac{1}{a_1}, \qquad \frac{29}{200a_2} \leqslant \frac{\overline{P}(N, Q)}{q^N \overline{V}(Q)} \leqslant \frac{1}{a_1(1-\log 2)}.$$

On pose $a_1 = 29/200a_2$ et $a_2 = 1/a_1(1-\log 2)$. La proposition est établie sous les hypothèses

$$(\mathrm{H}_1)\ x < N \leqslant 2x, \quad \text{resp.} \quad (\overline{\mathrm{H}}_1)\ d^\circ Q \leqslant N < 2d^\circ Q.$$

Soit un entier $v \geqslant 1$. On dira que x et N vérifient l'hypothèse (H_v) si $x < N \leqslant (v+1)x$; on dira que Q et N vérifient l'hypothèse $(\overline{\mathrm{H}}_v)$ si $d^\circ Q \leqslant N < (v+1)d^\circ Q$. On suppose que sous l'hypothèse $(\overline{\mathrm{H}}_v)$, resp. (H_v), (6), resp. (7), est vérifiée. Soient alors $Q \in \mathscr{S}$ et un entier N vérifiant $(\overline{\mathrm{H}}_{v+1})$. On peut supposer que $N \geqslant (v+1)d^\circ Q$. On a

$$\overline{P}(N, Q) = P(N, N/v+1) + \sum_{\substack{R \in [Q \\ d^\circ R \leqslant N/v+1}} \overline{P}(N - d^\circ R, R),$$

$N/v+1$ et N vérifient (H_v), et, pour tout polynôme $R \in [Q$ tel que $d^\circ R \leqslant N/v+1$, R et $(N - d^\circ R)$ vérifient $(\overline{\mathrm{H}}_v)$. On applique les relations (6) et (7) aux nombres $\overline{P}(N - d^\circ R, R), P(N, N/v)$. Après simplifications on obtient

$$a_1 \leqslant \overline{P}(N, Q)/\overline{V}(Q)q^N \leqslant a_2.$$

Le point (a) est établi sous l'hypothèse $(\overline{\mathrm{H}}_{v+1})$.

Soient $x \geqslant 1$ et un entier N vérifiant (H_{v+1}). Il existe un et un seul polynôme irréductible Q tel que $\mathscr{U}(N, x) = \overline{\mathscr{U}}(N, Q)$. Mais alors, $V(x) = \overline{V}(Q)$, $d^\circ Q > x$ et $d^\circ Q \leqslant N < (v+1)d^\circ Q$. D'après ce qui précède,

$$a_1 \leqslant P(N, x)/V(x)q^N \leqslant a_2,$$

ce qui établit le point (b).

COROLLAIRE. *Il existe une constante absolue a_3 telle que pour tout entier $n \geqslant 1$, pour tout entier $N \geqslant n$, on ait*

$$nq_0(N, n) \leqslant nP_0(N, n) \leqslant a_3 q^N. \tag{10}$$

THÉORÈME Q. *Il existe une constante absolue $a_4 > 0$, un entier $n_1 > 0$ tels que, pour tout entier $n \geqslant n_1$, pour tout entier $N > n$, on ait*

$$nq_0(N, n) \geqslant a_4 q^N.$$

3.2. Majoration des nombres $p_k(N, n)$ et $P_k(N, n)$. On suppose $k \geqslant 1$. On conserve les notations du paragraphe 1.

On désigne par $\mathscr{H}(n)$ l'ensemble des polynômes de $\mathscr{U}$ dont tous les facteurs irréductibles sont de degré au plus égal à n, et par $\mathscr{H}(n, k)$, resp. $h(n, k)$, l'ensemble des polynômes $H \in \mathscr{H}(n)$ tels que $\Omega(H) = k$, resp. tels que $\omega(H) = k$.

PROPOSITION 2. *Soit un nombre réel $A > 0$. Si k et n sont des entiers tels que $1 \leqslant k \leqslant -A\log(V(n))$, on a*

$$\sigma_{-1}(h(n, k)) \ll \frac{(-\log V(n))^k}{k!}, \tag{11}$$

la constante impliquée par le symbole $\ll$ ne dépendant que de q et de A.

Soit un nombre réel $A \in]0, q[$. Si k et n sont des entiers tels que $1 \leqslant k \leqslant -A\log(V(n))$, on a

$$\sigma_{-1}(\mathscr{H}(n, k)) \ll \frac{(-\log V(n))^k}{k!}, \tag{12}$$

la constante impliquée par le symbole $\ll$ ne dépendant que de q et de A.

Démonstration. Posons, pour tout nombre complexe z de module strictement inférieur à 1,

$$f(z) = \sum_{H \in \mathscr{H}(n)} z^{\omega(H)} |H|^{-1}. \tag{i}$$

On remarque que

$$f(z) = \sum_{k=0}^{\infty} \sigma_{-1}(h(n, k)) z^k. \tag{ii}$$

Dans le disque $|z| < 1$ cette série est absolument convergente et s'écrit comme produit eulérien absolument convergent

$$f(z) = \prod_{\substack{P \in \mathscr{P} \\ d^\circ P \leqslant n}} \left(1 + \frac{z}{|P|}\left(1 - \frac{1}{|P|}\right)^{-1}\right).$$

On pose

$$g(z)=\prod_{\substack{P\in\mathscr{P}\\ d^\circ P\leqslant n}}\left(1+\frac{z}{|P|}\left(1-\frac{1}{|P|}\right)^{-1}\right)\left(1-\frac{1}{|P|}\right)^{z},$$

alors,

(iii) $$f(z)=g(z)V(n)^{-z}.$$

Le produit $g(z)$ admet un prolongement analytique à tout le plan complexe. Pour tout réel $A>0$, les fonctions g et g'' sont uniformément bornées dans le disque fermé $|z|\leqslant A$, les bornes ne dépendant que de q et de A. Soit un entier $k\leqslant -A\log\big(V(n)\big)$, soit $\varepsilon=k/-\log\big(V(n)\big)$. La formule de Cauchy nous donne

$$\sigma_{-1}\big(h(n,k)\big)=\frac{1}{2\pi i}\int_{|z|=\varepsilon}g(z)V(n)^{-z}z^{-k-1}dz,$$

$$\left|\sigma_{-1}\big(h(n,k)\big)-g(\varepsilon)\frac{1}{2\pi i}\int_{|z|=\varepsilon}\frac{V(n)^{-z}}{z^{k+1}}dz-\right.$$

$$\left.-\frac{1}{2\pi i}\int_{|z|=\varepsilon}\frac{g(z)-g(\varepsilon)-g'(\varepsilon)(z-\varepsilon)}{z^{k+1}V(n)^{z}}dz\right|\ll\int_{|z|=\varepsilon}\frac{|z-\varepsilon|^2|V(n)^{-z}|}{|z|^{k+1}}dz,$$

$$\left|\sigma_{-1}\big(h(n,k)\big)-g(\varepsilon)\frac{\big(-\log\big(V(n)\big)\big)^k}{k!}\right|\ll\frac{\big(-\log\big(V(n)\big)\big)^{k-1}}{(k-1)!},$$

les constantes impliquées par les symboles $\ll$ ne dépendant que de q et de A. La majoration (11) s'en déduit.

Pour la majoration (12) on procède de façon similaire. Le prolongement analytique n'est possible que dans le disque $|z|<q$, d'où la condition $A\in\,]0,q[$ exigée pour la relation (12).

THÉORÈME F_n. *Soit un nombre réel $A>0$. Alors, si k et n sont des entiers tels que $0\leqslant k\leqslant A\log(n)$, pour tout entier $N>0$, on a*

$$p_k(N,n)\ll\frac{q^N(\log n)^k}{n(k!)},$$

la constante impliquée par le symbole $\ll$ ne dépendant que de q et de A. Soit un nombre réel $A\in\,]0,q[$. Alors, si k et n sont des entiers tels que $0\leqslant k\leqslant A\log(n)$, pour tout entier $N>0$, on a

$$P_k(N,n)\ll\frac{q^N(\log n)^k}{n(k!)},$$

la constante impliquée par le symbole $\ll$ ne dépendant que de q et de A.

Démonstration. Si $k=0$, et si $N>n$, le corollaire de la proposition 1 donne les résultats annoncés. Si $k=0$, et si $N\leqslant n$, le théorème F_n est trivial. On suppose $k\geqslant 1$. Soit $U\in\mathscr{U}$ tel que $\Omega_n(U)=k$, U s'écrit comme produit HR où $H\in\mathscr{H}(n,k)$, où R est un polynôme tel que $\Omega_n(R)=0$. On a la majoration

$$P_k(N,n)\leqslant\sum_{\substack{H\in\mathscr{H}(n,k)\\ d^\circ H\leqslant N}}P_0(N-d^\circ H,n).$$

Si $n\geqslant N-d^\circ H$, $P_0(N-d^\circ H,n)=0$, si $n<N-d^\circ H$, on applique le corollaire de la proposition 1, d'où,

$$P_k(N,n)\leqslant a_3q^Nn^{-1}\sum_{\substack{H\in\mathscr{H}(n,k)\\ d^\circ H\leqslant N}}|H|^{-1}\leqslant a_3q^Nn^{-1}\sigma_{-1}\big(\mathscr{H}(n,k)\big).$$

Les relations (8) et (13) donnent le résultat annoncé. L'autre majoration s'obtient de façon identique.

4. Majoration de $F(N,n)$. Dans ce paragraphe, les constantes impliquées par les symboles $\ll$ ne dépendent que de q ou sont absolues.

LEMME. *Soient a et b des nombres réels tels que $0<b<1<a$. Alors, pour tout x réel strictement positif,*

(1) $$\sum_{h\geqslant ax}\frac{x^h}{h!}\ll\left(\frac{e}{a}\right)^{ax}x^{-1/2},$$

(2) $$\sum_{h\leqslant bx}\frac{x^h}{h!}\ll\left(\frac{e}{b}\right)^{bx}x^{-1/2}.$$

Démonstration. C'est le lemme 1 de [10].

PROPOSITION 4.1. *Soit*

$$a=1-\frac{1+\log(\log 2)}{\log 2}.$$

Alors, si n et N sont des entiers tels que $2\leqslant n\leqslant N$,

$$F(N,n)\ll q^Nn^{-a}(\log n)^{-1/2}.$$

Démonstration. Posons

$$a=\frac{\log n}{\log 2},\qquad b=\frac{13}{10}a,\qquad c=\frac{11}{10}a.$$

On partage l'ensemble $\mathscr{F}(N,n)$ en cinq sous-ensembles $\mathscr{F}_i(N,n)$, $1\leqslant i\leqslant 5$, déterminés par les conditions suivantes.

$$H \in \mathscr{F}_1(N,n) \Leftrightarrow \Omega_n(H) \leqslant a,$$

$$H \in \mathscr{F}_2(N,n) \Leftrightarrow a < \Omega_n(H) \leqslant b,$$

$$H \in \mathscr{F}_3(N,n) \Leftrightarrow b < \Omega_n(H) \text{ et } \omega_n(H) \leqslant c,$$

$$H \in \mathscr{F}_4(N,n) \Leftrightarrow b < \Omega_n(H) \text{ et } c < \omega_n(H) \leqslant e^2\log(n),$$

$$H \in \mathscr{F}_5(N,n) \Leftrightarrow b < \Omega_n(H) \text{ et } e^2\log(n) < \omega_n(H).$$

On pose

$$F_i(N,n) = \|\mathscr{F}_i(N,n)\|.$$

1° Si $H \in \mathscr{F}(N,n)$, H s'écrit comme produit UV avec $d^\circ U = n$, $d^\circ V = N-n$ et $\Omega_n(H) = \Omega_n(U) + \Omega_n(V) = \Omega(U) + \Omega_n(V)$, d'où la majoration,

$$F_1(N,n) \leqslant \sum_{i+j\leqslant a} P_i(n)P_j(N-n,n).$$

Pour $1 \leqslant i \leqslant a$, $j \leqslant a$, on peut appliquer les théorèmes F et F_n, d'où,

$$F_1(N,n) \leqslant \frac{q^N}{n^2} \sum_{\substack{i+j\leqslant a \\ i\geqslant 1}} \frac{(\log n)^{i+j-1}}{(i-1)!\,j!} = \sum_{0\leqslant h\leqslant a-1} \frac{(2\log n)^h}{h!},$$

et, avec (2),

$$F_1(N,n) \ll \frac{q^N}{n^2}(\log n)^{-1/2}\big(2e\log(2)\big)^{\log n/\log 2},$$

(a) $$F_1(N,n) \ll q^N n^{-a}(\log n)^{-1/2}.$$

2° On a

$$F_2(N,n) \ll \sum_{a<k\leqslant b} P_k(N,n).$$

Pour $k \leqslant b = \dfrac{13\log n}{10\log 2}$, le théorème F_n s'applique, et,

$$F_2(N,n) \ll q^N n^{-1} \sum_{a<k\leqslant b} \frac{(\log n)^k}{k!},$$

la majoration (1) donne alors

$$F_2(N,n) \ll q^N n^{-1}(\log n)^{-1/2}\big(e\log(2)\big)^{\log n/\log 2},$$

(b) $$F_2(N,n) \ll q^N n^{-a}(\log n)^{-1/2}.$$

3° Si $H \in \mathscr{F}_3(N,n)$, H est divisible par le carré d'un polynôme K tel que $\Omega_n(K) > a/10$ et donc tel que $d^\circ K > a/10$. Par suite,

$$F_3(N,n) \leqslant \sum_{\substack{d^\circ K\leqslant N/2 \\ d^\circ K>a/10}} q^{N-2d^\circ K} \ll q^{N-a/10}.$$

Or,

$$q^{a/10} \geqslant 2^{a/10} = n^{1/10},$$

d'où,

(c) $$F_3(N,n) \ll q^N n^{-1/10}.$$

4° On a

$$F_4(N,n) \leqslant \sum_{11a/10<j\leqslant e^2\log(n)} p_j(N,n),$$

on applique le théorème F_n,

$$F_4(N,n) \ll q^N n^{-1} \sum_{11a/10<j\leqslant e^2\log(n)} \frac{(\log n)^j}{j!}.$$

Avec (1) on a alors,

$$F_4(N,n) \ll q^N n^{-1}(\log n)^{-1/2}\left(\frac{10}{11}e\log(2)\right)^{\frac{11\log n}{10\log 2}}$$

$$= q^N n^{\frac{-11a}{10}+\frac{\frac{1}{10}-\frac{11}{10}\log\frac{11}{10}}{\log 2}}(\log n)^{-1/2},$$

(d) $$F_4(N,n) \ll q^N n^{-11a/10}.$$

5° Si $H \in \mathscr{F}_5(N,n)$, il existe un entier $k \geqslant e^2\log(n)$, un polynôme $K \in q(n,k) = h(n,k) \cap \mathscr{Q}$, tel que H soit divisible par K, l'ensemble $h(n,k)$ ayant été défini au paragraphe précédent. Donc

$$F_5(N,n) \leqslant \sum_{k\geqslant e^2\log(n)} \sum_{K\in q(n,k)} q^{N-d^\circ K}.$$

On a

$$\sigma_{-1}\big(q(n,k)\big) \leqslant \frac{1}{k!}\Big(\sum_{\substack{P\in\mathscr{P} \\ d^\circ P\leqslant n}} |P|^{-1}\Big)^k.$$

On applique le théorème II

$$F_5(N,n) \leqslant q^N \sum_{k\geqslant e^2\log(n)} \frac{(1+\log n)^k}{k!},$$

d'où, avec (2),

$$F_5(N,n) \ll q^N(\log n)^{-1/2}\big((1+\log n)/e\log n\big)^{e^2\log n},$$

$$F_5(N,n) \ll q^N n^{-e^2}(\log n)^{-1/2}. \tag{e}$$

Comme $\alpha < 1/10$, les relations (a), (b), (c), (d) et (e) donnent le résultat annoncé.

5. Minoration de $F(N,n)$. Suivant la méthode utilisée dans [9] et améliorée dans [11], on construit un ensemble contenu dans $\mathscr{F}(N,n)$ dont on minorera le nombre d'éléments.

Les constantes impliquées par les symboles 0 et $\ll$ que nous utiliserons ici ne dépendront que de q ou seront absolues.

On pose, lorsque ces expression ont un sens,

$$L(x) = \log(x), \quad L_2(x) = \log\big(\log(x)\big).$$

5.1. Construction des ensembles $\mathscr{X}(N,n)$ et $\mathscr{Y}(N,n)$. Soit un entier $n \geqslant 3$ tel que

$$n > \sup\left\{2^{4[L(n)/L_2(n)]^{1/2}}, \frac{2[L(n)L_2(n)]^{1/2}}{L(2)}\left(1+n^{-\left(\frac{L_2(n)}{L(n)}\right)^{1/2}}\right)\left(\frac{L(n)}{L_2(n)}\right)^{1/2}\right\}. \tag{1}$$

Posons

$$K = \big[\big(L(n)L_2(n)^{-1}\big)^{1/2}\big], \tag{2}$$

$$t = \left[\frac{L(n)}{2KL(2)}\right]. \tag{3}$$

Pour $h \in \{1,\dots,K-2\}$, soit $\mathscr{P}_h$ l'ensemble des polynômes irréductibles P tels que

$$n^{h/K} \leqslant d^\circ P < n^{(h+1)/K}. \tag{4}$$

Soit $\mathscr{B}$ l'ensemble des polynômes sans facteur carré, ayant exactement t facteurs irréductibles dans chaque ensemble $\mathscr{P}_h$ et n'ayant pas d'autres facteurs irréductibles. La condition (1) assure que l'ensemble $\mathscr{B}$ n'est pas vide. En outre, on a la

PROPOSITION 5.1. *Soient*

$$\beta(n) = \left(\frac{L(n)}{2KL(2)} - 1\right)n^{1-2/K}, \tag{5}$$

$$b(n) = \frac{L(n)}{2KL(2)}\,n^{1-2/K}(1+2n^{-1/K}). \tag{6}$$

Alors, si $B \in \mathscr{B}$,

$$\beta(n) \leqslant d^\circ B \leqslant b(n), \tag{7}$$

et, en conséquence,

$$\|\mathscr{B}\| \leqslant q^{b(n)+1}/(q-1). \tag{8}$$

Démonstration. Immédiate, avec le théorème II.

Pour tout entier $j \geqslant n$, soit $\mathscr{H}_j$ l'ensemble des polynômes de degré j s'écrivant comme produit PB où $B \in \mathscr{B}$, où P est un polynôme irréductible. Les relations (1) et (7) montrent que la décomposition

$$H = PB, \quad P \in \mathscr{I}, \quad B \in \mathscr{B},$$

des polynômes de $\mathscr{H}_j$ est unique. On pose alors,

$$P = p(H) \quad \text{et} \quad B = B(H).$$

Pour tout entier $j \geqslant n$, soit $\mathscr{V}_j$ l'ensemble des polynômes de degré j s'écrivant comme produit QB où $B \in \mathscr{B}$, où Q est un polynôme sans facteur carré tel que $\omega_n(Q) = 0$.

Pour $N \geqslant 2n$, soit $\mathscr{X}(N,n)$ l'ensemble des produits UV où $U \in \mathscr{H}_n$, où $V \in \mathscr{H}_{N-n}$, pour $N > 2n + b(n)$, soit $\mathscr{Y}(N,n)$ l'ensemble des produits UV où $U \in \mathscr{H}_n$, où $V \in \mathscr{V}_{N-n}$. On a

$$\|\mathscr{X}(N,n)\| \leqslant F(N,n), \tag{9}$$

$$\|\mathscr{Y}(N,n)\| \leqslant F(N,n). \tag{10}$$

D'autre part, on a la

PROPOSITION 5.2. *Soit $S(N,n)$, resp. $T(N,n)$, le nombre de solutions de l'équation*

$$UV' = U'V \tag{E}$$

telles que $(U, U', V, V') \in \mathscr{H}_n \times \mathscr{H}_n \times \mathscr{H}_{N-n} \times \mathscr{H}_{N-n}$, resp. telles que $(U, U', V, V') \in \mathscr{H}_n \times \mathscr{H}_n \times \mathscr{V}_{N-n} \times \mathscr{V}_{N-n}$. Alors, on a

$$\|\mathscr{H}_n \times \mathscr{H}_{N-n}\|^2 \leqslant S(N,n)\,\|\mathscr{X}(N,n)\|, \tag{11}$$

$$\|\mathscr{H}_n \times \mathscr{V}_{N-n}\|^2 \leqslant T(N,n)\,\|\mathscr{Y}(N,n)\|. \tag{12}$$

Démonstration. Avec l'inégalité de Cauchy–Schwarz.

5.2. Estimations auxilliaires. Ces estimations se déduisent du théorème II.

PROPOSITION 5.3. *Si $h \in \{1,\dots,K-2\}$, soit $\mathscr{J}_h$ la réunion des ensembles $\mathscr{P}_1,\dots,\mathscr{P}_h$, si $h \in \{1,\dots,K-3\}$, soit $\mathscr{J}'_h$ la réunion des ensembles $\mathscr{P}_{h+1},\dots,\mathscr{P}_{K-2}$. Alors, si $1 \leqslant h \leqslant K-2$, on a*

$$\frac{L(n)}{K} - n^{-h/K}\left(1 + 2q^{-8}\,\frac{\sqrt{q}}{\sqrt{q}-1}\right) \leqslant \sigma_{-1}(\mathscr{P}_h) \leqslant \frac{L(n)}{K} + n^{-h/K}, \tag{13}$$

$$\frac{hL(n)}{K}-n^{-1/K}\left(1+2q^{-8}\frac{\sqrt{q}}{\sqrt{q}-1}\right)\leqslant\sigma_{-1}(\mathscr{J}_h)\leqslant\frac{hL(n)}{K}+n^{-1/K}, \tag{14}$$

$$\sigma_{-2}(\mathscr{P}_h)\leqslant\frac{q}{q-1}q^{-n^{h/K}}n^{-h/K}, \tag{15}$$

$$\frac{\{\sigma_{-1}(\mathscr{J}_h)\}^{2ht}}{\{[ht/2]!\}^4}\leqslant t^{-2}\big(4eL(2)\big)^{2ht}e^{2K}\quad \textit{si } ht \textit{ est pair}, \tag{16}$$

$$\frac{\{\sigma_{-1}(\mathscr{J}_h)\}^{2ht}}{\{r!(r+1)!\}^2}\leqslant t^{-2}\big(4eL(2)\big)^{2ht}e^{2K}\quad \textit{si } ht \textit{ est impair} \tag{17}$$

$$\textit{et si } ht=2r+1,$$

si $1\leqslant h\leqslant K-3$, *on a*

$$\frac{(K-2-h)L(n)}{K}-n^{-(h+1)/K}\left(1+2q^{-8}\frac{\sqrt{q}}{\sqrt{q}-1}\right)\leqslant\sigma_{-1}(\mathscr{J}'_h)\leqslant\frac{(K-2-h)L(n)}{K}+n^{-(h+1)/K}, \tag{18}$$

$$\frac{\{\sigma_{-1}(\mathscr{J}'_h)\}^{2(K-2-h)t}}{\{[(K-2-h)t]!\}^2}\leqslant t^{-1}\big(2eL(2)\big)^{2(K-2-h)t}e^{2K}. \tag{19}$$

Démonstration. Les relations (13), (14), (15) et (18) sont des conséquences immédiates de (1), (4) et du théorème II.

Les relations (16), (17) et (19) se déduisent des relations (2), (3), (14) et (18) et de la formule de Stirling.

Proposition 5.4. *On a*

$$\sigma_{-1/2}(\mathscr{B})\leqslant q^{(b(n)+1)/2}, \tag{20}$$

$$\sigma_{-1}(\mathscr{B})\geqslant t^{\frac{2-K}{2}}n^{\left(1-\frac{\alpha}{2}\right)\left(1-\frac{2}{K}\right)}, \tag{21}$$

où

$$\alpha=1-\big(1+L_2(2)\big)/L(2).$$

Démonstration. Avec (7) il vient

$$\sigma_{-1/2}(\mathscr{B})\leqslant\sum_{\substack{B\in\mathscr{B}\\ \beta(n)\leqslant d^\circ B\leqslant b(n)}}|B|^{-1/2}\leqslant\sum_{\beta(n)\leqslant r\leqslant b(n)}q^{r/2},$$

d'où (20).

Désignons par $\mathscr{B}_i$ $(1\leqslant i\leqslant K-2)$, l'ensemble des polynômes sans facteur carré, produits de t facteurs irréductibles de $\mathscr{P}_i$ et n'ayant pas d'autres facteurs irréductibles. Tout polynôme $B\in\mathscr{B}$ s'écrit de façon

unique comme produit $B_1\dots B_{K-2}$ où $B_i\in\mathscr{B}_i$, d'où,

$$\sigma_{-1}(\mathscr{B})=\sum_{(B_1,\dots,B_{K-2})\in\mathscr{B}_1\times\dots\times\mathscr{B}_{K-2}}|B_1\dots B_{K-2}|^{-1},$$

$$(*)\qquad \sigma_{-1}(\mathscr{B})=\prod_{i=1}^{K-2}\sigma_{-1}(\mathscr{B}_i).$$

Le lemme 13, p. 147 de [5] nous donne

$$\sigma_{-1}(\mathscr{B}_i)\geqslant\frac{1}{t!}\{\sigma_{-1}(\mathscr{P}_i)\}^t\left\{1-\binom{t}{2}[\sigma_{-1}(\mathscr{P}_i)]^{-2}\sigma_{-2}(\mathscr{P}_i)\right\}.$$

Les relations (13), (15) et (1) nous donnent

$$\binom{t}{2}\{\sigma_{-1}(\mathscr{P}_i)\}^{-2}\sigma_{-2}(\mathscr{P}_i)\leqslant\frac{t^2K^2}{2L(n)^2}\left(1+\frac{12K}{L(n)}n^{-i/K}\right)^2\frac{q}{q-1}n^{-i/K}q^{-n^{i/K}}$$
$$\leqslant\frac{q^{-15}}{32(q-1)}\left(1+\frac{3}{4L(2)}\right)^2t^2K^2L(n)^{-2}.$$

Avec (3) il vient

$$\binom{t}{2}\{\sigma_{-1}(\mathscr{P}_i)\}^{-2}\sigma_{-2}(\mathscr{P}_i)\leqslant\frac{q^{-15}}{32(q-1)}\left(1+\frac{3}{4L(2)}\right)^2\big(4L(2)\big)^{-2},$$

et,

$$\sigma_{-1}(\mathscr{B}_i)\geqslant\frac{1}{t!}\{\sigma_{-1}(\mathscr{P}_i)\}^t.$$

La relation (13) nous donne

$$\sigma_{-1}(\mathscr{B}_i)\geqslant\frac{1}{t!}\left\{\frac{L(n)}{K}\right\}^t\left\{1-\frac{6}{5}n^{-1/K}\frac{K}{L(n)}\right\}^t\geqslant\frac{1}{t!}\left\{\frac{L(n)}{K}\right\}^t.$$

Avec (3) et la formule de Stirling, il vient

$$\sigma_{-1}(\mathscr{B}_i)\geqslant t^{-1/2}\left(\frac{eL(n)}{tK}\right)^t\geqslant t^{-1/2}\big(2eL(2)\big)^{L(n)/2KL(2)},$$

et, avec (*),

$$\sigma_{-1}(\mathscr{B})\geqslant t^{-(K-2)/2}n^{(1-\alpha/2)(1-2/K)}.$$

5.3. Minoration de $\|\mathscr{H}_j\|$ *et de* $\|\mathscr{V}_{N-n}\|$.

Proposition 5.5. *Soit un entier* $j\geqslant n$. *Alors, on a*

$$\|\mathscr{H}_j\|\geqslant q^jj^{-1}t^{(2-K)/2}n^{(1-\alpha/2)(1-2/K)}. \tag{22}$$

Si $n \geqslant n_1$, *si* $N > 2n+b(n)$, *on a*

$$\|\mathscr{V}_{N-n}\| \geqslant q^{N-n} t^{(2-K)/2} n^{-a/2-(2-a)/K}. \tag{23}$$

Démonstration. Le théorème II nous donne

$$\|\mathscr{H}_j\| = \sum_{B\in\mathscr{B}} \pi(j-d^\circ B) \geqslant \sum_{B\in\mathscr{B}} \frac{q^{j-d^\circ B} - 2q^{(j-d^\circ B)/2}}{j-d^\circ B}$$

$$\geqslant q^j j^{-1} \sum_{B\in\mathscr{B}} |B|^{-1} - 2q^{j/2} \sum_{B\in\mathscr{B}} \frac{|B|^{-1/2}}{j-d^\circ B}.$$

Avec (1), (6) et (7) il vient

$$\|\mathscr{H}_j\| \geqslant q^j j^{-1} \sigma_{-1}(\mathscr{B}) - \frac{4}{j}\sigma_{-1/2}(\mathscr{B}),$$

et (22) se déduit alors de la proposition précédente et des relations (2) et (3).

On suppose $n \geqslant n_1$ et $N > 2n+b(n)$. Tout élément de $\mathscr{V}_{N-n}$ s'écrit de façon unique comme produit QB où $Q \in \mathscr{Q}$ avec $\omega_n(Q) = 0$, où $B \in \mathscr{B}$ avec $d^\circ B \leqslant b(n) < n$, d'où,

$$\|\mathscr{V}_{N-n}\| = \sum_{B\in\mathscr{B}} q_0(N-n-d^\circ B, n).$$

On a $N-n-d^\circ B > n \geqslant n_1$. On peut appliquer le théorème Q

$$q_0(N-n-d^\circ B) \geqslant \frac{1}{n} q^{N-n-d^\circ B},$$

et,

$$\|\mathscr{V}_{N-n}\| \geqslant \frac{1}{n} q^{N-n} \sigma_{-1}(\mathscr{B}).$$

(23) se déduit de la proposition précédente.

5.4. Majoration de $S(N,n)$ *et de* $T(N,n)$.

Proposition 5.6. *Si* $N \leqslant 2n+b(n)$, *on a*

$$S(N,n) \ll \|\mathscr{H}_n \times \mathscr{H}_{N-n}\| t^{K-2} L_2(n)^{-2} e^{4K+3t/2}. \tag{24}$$

Démonstration. Les solutions (U, U', V, V') de l'équation

$$UV' = U'V \tag{E}$$

considérées ici appartiendront toutes à $\mathscr{H}_n \times \mathscr{H}_n \times \mathscr{H}_{N-n} \times \mathscr{H}_{N-n}$. Soit (U, U', V, V') une telle solution. Il existe des polynômes irréductibles P, P', Q, Q', des polynômes B, B', C, C' de $\mathscr{B}$ tels que

$$PBQ'C' = UV' = U'V = P'B'QC,$$

et, d'après la proposition 5.1,

$$PQ' = P'Q. \tag{E'}$$

Si $P = Q'$, alors $P = P' = Q = Q'$. Si $P \neq Q'$, l'équation (E') n'est satisfaite que dans les cas suivants

(i) $P = P'$ et $Q = Q'$,

(ii) $P = Q$ et $P' = Q'$.

On partage les $S(N,n)$ solutions (U, U', V, V') de (E) en cinq classes:

(1) les solutions telles que $p(U) = p(U') = p(V) = p(V')$,

(2) les solutions telles que $p(U) \neq p(V)$ et $U \vee V = 1$,

(3) les solutions telles que $p(U) \neq p(U')$ et $U \vee U' = 1$,

(4) les solutions telles que $p(U) \neq p(V)$ et $U \vee V \neq 1$

(5) les solutions telles que $p(U) \neq p(U')$ et $U \vee U' \neq 1$.

On note $S_1, \ldots, S_5$ le nombre d'éléments de ces classes.

Si (U, U', V, V') est compté dans S_2, V divise V', mais V et V' sont unitaires et de même degré, donc $V = V'$ et $U = U'$. Par suite

$$S_2 = \|\mathscr{H}_n \times \mathscr{H}_{N-n}\|. \tag{a}$$

Si (U, U', V, V') est compté dans S_3, U divise V, $p(U) = p(V)$ et $B(U)$ divise $B(V)$. Les polynômes $B(U)$ et $B(V)$ sont construits de façon à avoir même nombre de facteurs irréductibles, ils sont donc égaux. Ceci ne peut se produire que si $N = 2n$, d'où,

$$S_3 = \begin{cases} 0 & \text{si} \quad N > 2n, \\ \|\mathscr{H}_n\|^2 & \text{si} \quad N = 2n. \end{cases} \tag{b}$$

Si $S_1 \neq 0$, il existe un polynôme irréductible P tel que

$$N-n-b(n) \leqslant d^\circ P < n,$$

et dans ce cas il y a moins de $q^n \|\mathscr{B}\|^4$ solutions dans la première classe, d'où,

$$S_1 \begin{cases} = 0 & \text{si} \quad N \geqslant 2n+b(n), \\ \leqslant q^{n+4b(n)} & \text{si} \quad N < 2n+b(n). \end{cases} \tag{c}$$

Si D est un polynôme sans facteur carré, dont tous les facteurs irréductibles sont dans les ensembles $\mathscr{P}_1, \ldots, \mathscr{P}_{K-2}$, soit $h(D)$ le plus petit entier h tels que tous les facteurs irréductibles de D soient dans $\mathscr{J}_h = \mathscr{P}_1 \cup \ldots \cup \mathscr{P}_h$. On a alors,

$$\omega(D) \leqslant th(D).$$

Notons $\mathscr{D}_{h,k}$, $1 \leqslant h \leqslant K-2$, $1 \leqslant k \leqslant ht$, l'ensemble des polynômes D sans facteur carré, dont tous les facteurs irréductibles sont dans $\mathscr{P}_1 \cup \ldots \cup \mathscr{P}_h$ tels que $h(D) = h$ et $\omega(D) = k$. Notons $S_4(h,k)$, resp. $S_5(h,k)$ le nombre de solutions (U, U', V, V') de (E) appartenant à la quatrième, resp.

à la cinquième, classe, telles que $h(U \vee V) = h$ et $\omega(U \vee V) = k$, resp. telles que $h(U \vee U') = h$ et $\omega(U \vee U') = k$.

On a

$$S_4 = \sum_{h=1}^{K-2} \sum_{k=1}^{ht} S_4(h, k), \tag{d}$$

$$S_5 = \sum_{h=1}^{K-2} \sum_{k=1}^{ht} S_5(h, k). \tag{e}$$

Considérons maintenant un polynôme $D \in \mathscr{D}_{h,k}$. Pour $j \in \{n, N-n\}$, soit $H_{D,j}$ le nombre de solutions $Y \in \mathscr{H}_j$ de la congruence

$$Y \equiv 0 \pmod{D}.$$

Il y a au plus $H_{D,n} \times H_{D,N-n}$ couples $(Y, Z) \in \mathscr{H}_n \times \mathscr{H}_{N-n}$ tels que $Y \vee Z = D$.

LEMME 1. 1° *Soient* $U \in \mathscr{H}_n$, $V \in \mathscr{H}_{N-n}$ *tels que* $U \vee V = D$. *Alors, il y a au plus* $q_k(d^\circ D)$ *solutions* (U, U', V, V') *de l'équation* (E).

2° *Soient* $U \in \mathscr{H}_n$, $U' \in \mathscr{H}_n$ *tels que* $U \vee U' = D$. *Alors, il y a au plus* $q_k(N-2n+d^\circ D)$ *solutions de l'équation* (E).

Démonstration. 1° Si (U, U', V, V') est solution de (E),

$$V' \equiv 0 \left(\mathrm{mod}\, \frac{V}{D}\right). \tag{*}$$

Réciproquement, si $V' \in \mathscr{H}_{N,n}$ vérifie (*), l'équation $UV' = U'V$ a au plus une solution $U' \in \mathscr{H}_n$.

Si $V' \in \mathscr{H}_{N-n}$ vérifie (*), il existe un polynôme W tel que

$$V' = W \frac{V}{D},$$

le polynôme W est sans facteur carré et vérifie les relations

$$d^\circ W = d^\circ D, \qquad \omega(W) = \omega(D) = k.$$

2° Le deuxième point se démontre de façon identique.

LEMME 2. *Posons* $l = ht-k$, $r = (K-2-h)t$. *Alors, pour* $j \in \{n, N-n\}$, *on a*

$$H_{D,j} \leqslant \frac{q^j}{j\,|D|} \left(1 + \frac{2b(n)}{j}\right) \frac{\{\sigma_{-1}(\mathscr{J}_h)\}^l}{l!} \frac{\{\sigma_{-1}(\mathscr{J}'_h)\}^r}{r!},$$

le dernier facteur étant pris égal à 1 *lorsque* $h = K-2$.

Démonstration. Soit $U \in \mathscr{H}_j$ congru à 0 modulo D. Alors,

$$d^\circ U = j \text{ et } U = DPB', \text{ avec } P \in \mathscr{S},\ DB' \in \mathscr{R}.$$

Posons $B' = LR$ où tous les facteurs irréductibles de L, s'il en existe, sont dans $\mathscr{J}_h$, où tous les facteurs irréductibles de R, s'il en existe, sont dans $\mathscr{J}'_h$. On a

$$\omega(L) + \omega(D) = ht \quad \text{et} \quad \omega(R) = (K-2-h)t.$$

Notons $\mathscr{L}$, resp. $\mathscr{R}$, l'ensemble des polynômes sans facteur carré ayant l facteurs irréductibles dans $\mathscr{J}_h$, resp., ayant r facteurs irréductibles dans $\mathscr{J}'_h$. On a alors,

$$H_{D,j} \leqslant \sum_{L \in \mathscr{L}} \sum_{R \in \mathscr{R}} \pi\big(j - d^\circ(DLR)\big),$$

le théorème II nous donne

$$H_{D,j} \leqslant |D|^{-1} q^j \sum_{L \in \mathscr{L}} \sum_{R \in \mathscr{R}} \frac{1}{|LR|\,\big(j - d^\circ(DLR)\big)},$$

d'où, avec (7), (5) et (1),

$$H_{D,j} \leqslant \frac{q^j}{j\,|D|} \left(1 + \frac{2b(n)}{j}\right) \big(\sigma_{-1}(\mathscr{L})\big)\big(\sigma_{-1}(\mathscr{R})\big).$$

Les polynômes de L étant produits de l facteurs irréductibles de $\mathscr{J}_h$ deux à deux distincts, on a

$$\sigma_{-1}(\mathscr{L}) \leqslant \frac{\{\sigma_{-1}(\mathscr{J}_h)\}^l}{l!},$$

et, dans le cas où $h \neq K-2$, on a de même,

$$\sigma_{-1}(\mathscr{R}) \leqslant \frac{\{\sigma_{-1}(\mathscr{J}'_h)\}^r}{r!}.$$

Les lemmes 1 et 2 nous donnent

$$S_4(h, k) \leqslant \frac{q^N}{n(N-n)} \sum_{D \in \mathscr{D}_{h,k}} |D|^{-2} q_k(d^\circ D) \frac{\{\sigma_{-1}(\mathscr{J}_h)\}^{2l} \{\sigma_{-1}(\mathscr{J}'_h)\}^{2r}}{\{l!\}^2 \{r!\}^2}, \tag{f}$$

$$S_5(h, k) \leqslant \frac{q^N}{n(N-n)} \sum_{D \in \mathscr{D}_{h,k}} |D|^{-2} q_k(N-2n+d^\circ D) \frac{\{\sigma_{-1}(\mathscr{J}_h)\}^{2l} \{\sigma_{-1}(\mathscr{J}'_h)\}^{2r}}{\{l!\}^2 \{r!\}^2}. \tag{g}$$

Soit $D \in \mathscr{D}_{h,k}$. Alors,

$$k = \omega(D) \leqslant th \leqslant hL(n)/2KL(2),$$

$$d^\circ D + N - 2n \geqslant d^\circ D \geqslant n^{h/K},$$

$$L(d^\circ D + N - 2n) \geqslant L(d^\circ D) \geqslant \frac{h}{K} L(n) \geqslant 2kL(2).$$

On peut appliquer le théorème F

$$q_k(d^\circ D) \ll \frac{|D|}{d^\circ D}\,\frac{\big(L(d^\circ D)\big)^{k-1}}{(k-1)!},$$

$$q_k(N-2n+d^\circ D) \ll \frac{|D|}{N-2n+d^\circ D}\,\frac{\big(L(N-2n+d^\circ D)\big)^{k-1}}{(k-1)!}.$$

De l'hypothèse $N \leqslant 2n+b(n)$, on déduit que

$$q_k(N-2n+d^\circ D) \ll \frac{|D|}{d^\circ D}\,\frac{\big(L(d^\circ D)\big)^{k-1}}{(k-1)!}.$$

Les sommes $S_4(h,k)$ et $S_5(h,k)$ se majoreront de la même façon. On a

$$q_k(d^\circ D) \ll \frac{|D|}{d^\circ D}\,\frac{\big(L(d^\circ D)\big)^{k}}{k!}.$$

On a aussi

$$d^\circ D \leqslant htn^{(h+1)/K} \quad \text{et} \quad L(d^\circ D) \leqslant \frac{(h+1)L(n)}{K} + L(ht),$$

d'où, avec (14), (2) et (3),

$$L(d^\circ D) \leqslant \frac{h+1}{h}\,\sigma_{-1}(\mathscr{J}_h)\left(1+\frac{KL_2(n)}{2L(n)}\right)\left(1+\frac{12Kn^{-1/K}}{5L(n)}\right).$$

Pour $k \leqslant ht$,

$$\left(\frac{h+1}{h}\right)^k \leqslant e^t, \quad \left(1+\frac{KL_2(n)}{2L(n)}\right)^k \leqslant e^{t/2}, \quad \left(1+\frac{12Kn^{-1/K}}{5L(n)}\right)^k \ll 1,$$

d'où,

$$q_k(d^\circ D) \ll \frac{|D|}{d^\circ D}\,e^{3t/2}\cdot\frac{\{\sigma_{-1}(\mathscr{J}_h)\}^k}{k!},$$

la relation (f) nous donne alors,

$$S_4(h,k) \ll \frac{q^N}{n(N-n)}\,e^{3t/2}\cdot n^{-h/K}\,\frac{\{\sigma_{-1}(\mathscr{J}_h)\}^{2l+k}\{\sigma_{-1}(\mathscr{J}'_h)\}^{2r}}{\{k!\}\{l!\}^2\{r!\}^2}\,\sigma_{-1}(\mathscr{D}_{h,k}).$$

Les polynômes de $\mathscr{D}_{h,k}$ étant produits de k facteurs irréductibles distincts de $\mathscr{J}_h$, on a

$$\sigma_{-1}(\mathscr{D}_{h,k}) \leqslant \frac{\{\sigma_{-1}(\mathscr{J}_h)\}^k}{k!}.$$

On avait posé au lemme 2

$$l = ht-k \quad \text{et} \quad r = (K-2-h)t.$$

On a donc

$$S_4(h,k) \ll \frac{q^N}{n(N-n)}\,e^{3t/2}\cdot n^{-h/K}\,\frac{\{\sigma_{-1}(\mathscr{J}_h)\}^{2ht}\{\sigma_{-1}(\mathscr{J}'_h)\}^{2(K-2-h)t}}{\{[k!][(ht-k)!]\}^2\{[(K-2-h)t]!\}^2}.$$

Les relations (d) et (e) nous donnent alors

$$S_4+S_5 \ll \frac{q^N}{n(N-n)}\,e^{3t/2}\cdot\sum_{h=1}^{K-2} n^{-h/K}\sum_{k=1}^{ht}{}'\,\frac{\{\sigma_{-1}(\mathscr{J}_h)\}^{2ht}\{\sigma_{-1}(\mathscr{J}'_h)\}^{2(K-2-h)t}}{\{[k!][(ht-k)!]\}^2\{[(K-2-h)t]!\}^2}.$$

La fonction $k \mapsto k!(ht-k)!$ atteint son minimum pour $k = ht/2$ ou $k = (ht-1)/2$ suivant que ht est pair ou impair. Les majorations (16), (17) et (19) nous donnent

$$S_4+S_5 \ll \frac{q^N}{n(N-n)}\,e^{3t/2}\sum_{h=1}^{K-2} n^{-h/K}\cdot ht\cdot 2^{2ht}\cdot t^{-3}\big(2eL(2)\big)^{2(K-2)t}\cdot e^{4K},$$

$$S_4+S_5 \ll \frac{q^N}{n(N-n)}\,e^{4K+3t/2}\cdot t^{-2}\cdot K^2\cdot\big(2eL(2)\big)^{2(K-2)t}.$$

Avec (2) et (3) on a,

$$S_4+S_5 \ll \frac{q^N}{n(N-n)}\,e^{4K+3t/2}\cdot L_2(n)^{-2}\cdot n^{(2-\alpha)(1-2/K)}.$$

On conclut avec les relations (a), (b), (c) et (22).

PROPOSITION 5.7. *Si $n \geqslant n_1$ et si $N > 2n+b(n)$,*

$$T(N,n) \ll \|\mathscr{H}_n \times \mathscr{V}_{N-n}\|\,t^{K-2}L_2(n)^{-2}e^{4K+3t/2}. \tag{25}$$

Démonstration. Les solutions (U, U', V, V') de l'équation

$$UV' = U'V \tag{E}$$

considérées ici appartiendront toutes à $\mathscr{H}_n \times \mathscr{H}_n \times \mathscr{V}_{N-n} \times \mathscr{V}_{N-n}$. Si (U, U', V, V') est une de ces solutions, il existe des polynômes irréductibles P, P', des polynômes Q et Q' sans facteur carré tels que $\omega_n(Q) = \omega_n(Q') = 0$, des polynômes B, B', C, C' de $\mathscr{B}$ tels que

$$PBQ'C' = P'B'QC,$$

$$d^\circ(PB) = d^\circ(P'B') = n, \quad d^\circ(QC) = d^\circ(Q'C') = N-n.$$

D'après la proposition 5.1,

$$P = P' \quad \text{et} \quad Q = Q'.$$

On partage les $T(N,n)$ solutions de (E) en deux classes:

(1) les solutions (U, U', V, V') telles que $U \vee V = 1$,

(2) les solutions (U, U', V, V') telles que $U \vee V \neq 1$.

On note T_1 et T_2 le nombre d'éléments de ces classes. Comme pour la proposition précédente,

(a) $$T_1 \leqslant \|\mathscr{H}_n \times \mathscr{V}_{N-n}\|.$$

Les ensembles $\mathscr{D}_{h,k}$ étant définis comme à la proposition précédente, soit $T_2(h,k)$ le nombre de solutions (U, U', V, V') de (E) comptées dans T_2 et telles que $h(U \vee V) = h$, $\omega(U \vee V) = k$. On a

(b) $$T_2 = \sum_{h=1}^{K-2} \sum_{k=1}^{ht} T_2(h,k).$$

Soit D un polynôme de $\mathscr{D}_{h,k}$.

Lemme 3. *Soient $U \in \mathscr{H}_n$, $V \in \mathscr{V}_{N-n}$ tels que $U \vee V = D$. Alors, il y a au plus $q_k(d^\circ D)$ solutions (U, U', V, V') de* (E).

Démonstration. Comme pour le lemme 1.

Lemme 4. *Soient $l = ht-k$, $r = (K-2-h)t$. Soit V_D le nombre de solutions $V \in \mathscr{V}_{N-n}$ de la congruence*

$$V \equiv 0 \pmod{D}.$$

Alors,

$$V_D \leqslant \frac{q^{N-n}}{n|D|}\left(1+\frac{2b(n)}{n}\right)\frac{\{\sigma_{-1}(\mathscr{J}_h)\}^l}{l!}\frac{\{\sigma_{-1}(\mathscr{J}'_h)\}^r}{r!}.$$

Démonstration. Semblable à celle du lemme 2, les nombres $\pi(j-d^\circ(DLR))$ étant remplacés par les nombres $q_0(N-n-d^\circ(DLR), n)$ et le théorème II par le théorème F_n.

Les nombres $H_{D,n}$ étant définis comme à la proposition précédente, il y a au plus $H_{D,n} \times V_D$ couples $(U, V) \in \mathscr{H}_n \times \mathscr{H}_{N-n}$ tels que $U \vee V = D$, d'où, avec les lemmes 2, 3 et 4,

$$T_2(h,k) \ll \frac{q^N}{n^2} \sum_{D \in \mathscr{D}_{h,k}} |D|^{-2} q_k(d^\circ D) \frac{\{\sigma_{-1}(\mathscr{J}_h)\}^{2l}}{[l!]^2} \frac{\{\sigma_{-1}(\mathscr{J}'_h)\}^{2r}}{[r!]^2}.$$

On majore $T_2(h,k)$ comme on a majoré $S_4(h,k)$. Avec (b) on obtient

$$T_2 \ll \frac{q^N}{n^2} e^{4K+3t/2} \cdot L_2(n)^{-2} n^{(2-\alpha)(1-2/K)}.$$

On conclut avec les relations (a), (22) et (23).

Proposition 5.8. *Soit $c = 7+3/4L(2)+1/e-2\alpha$. Alors, si $N \leqslant 2n+b(n)$, on a*

(26) $$\|\mathscr{X}(N,n)\| \geqslant \frac{q^N}{n^\alpha}\exp\left(-c\left(L(n)L_2(n)\right)^{1/2}\right).$$

Démonstration. Les propositions 5.2, 5.5 et 5.6 nous donnent

$$\|\mathscr{X}(N,n)\| \geqslant \frac{q^N}{n(N-n)} n^{2-\alpha} n^{2(\alpha-2)/K} t^{4-2K} L_2(n)^2 e^{-4K-3t/2},$$

d'où, avec (1), (2), (6) et la condition $N \leqslant 2n+b(n)$,

$$\|\mathscr{X}(N,n)\| \geqslant \frac{q^N}{n^\alpha} n^{2(\alpha-2)/K} t^{4-2K} L_2(n)^2 e^{-4K-3t/2}.$$

Les relations (1), (2) et (3) donnent alors

$$\|\mathscr{X}(N,n)\| \geqslant \frac{q^N}{n^\alpha}\exp\left(-\sqrt{L(n)L_2(n)}\left[7+\frac{3}{4L(2)}+\frac{1}{e}-2\alpha\right]\right).$$

Proposition 5.9. *Si $n \geqslant n_1$ et si $N > 2n+b(n)$,*

(27) $$\|\mathscr{Y}(N,n)\| \geqslant \frac{q^N}{n^\alpha}\exp\left(-c\left(L(n)L_2(n)\right)^{1/2}\right).$$

Démonstration. Les propositions 5.2, 5.5 et 5.7 nous donnent

$$\|\mathscr{Y}(N,n)\| \geqslant \frac{q^N}{n^\alpha} n^{(\alpha-2)/K} t^{4-2K} L_2(n)^2 e^{-4K-3t/2}.$$

On conclut comme précédemment.

Les relations (9), (10), (26) et (27) donnent la minoration annoncée valable lorsque n vérifie la condition (1) et que $N \in [2n, 2n+b(n)]$, ou lorsque n vérifie la condition (1), que $n \geqslant n_1$ et que $N \geqslant n+b(n)$.

Références

[1] M. Car, *Normes dans $\mathbf{F}_q[X]$ de polynômes de $\mathbf{F}_{q^h}[X]$*, C. R. Acad. Sci., Paris, 288, 9 avril 1979.

[2] — *Sommes de deux carrés dans $\mathbf{F}_q[X]$ et problèmes de diviseurs*, Ann. Fac. Sci. Univ. Toulouse (à paraitre).

[3] — *Factorisation dans $\mathbf{F}_q[x]$*, C. R. Acad. Sci., Paris, 294, 25 janvier 1982.

[4] P. Erdös, *Sur une inégalité asymptotique en théorie des nombres*, Vestnik Leningrad. Univ. 13 (1960), p. 41–49.

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

[6] G. H. Hardy and W. R. Wright, *An introduction to the theory of numbers*, Clarendon Press, Oxford 1938.

[7] W. Leahey, *Sums of squares of polynomials with coefficients in a finite field*, Amer. Math. Monthly 74 (1967), p. 816–819.

[8] M. Mignotte, *Statistiques sur $\mathbf{F}_q[X]$*, Comptes rendus des Journées de Théorie Analytique et Elémentaire des Nombres, Limoges, 10–11 mars 1980.

[9] G. Tenenbaum, *Estimations asymptotiques de fonctions arithmétiques liées aux diviseurs*, Thèse, Bordeaux, 30 avril 1976.
[10] — *Sur deux fonctions de diviseurs*, J. London Math. Soc. (2) 14 (1967), p. 521–526.
[11] — *Sur la probabilité qu'un entier possède un diviseur dans un intervalle donné*, preprint.

LABORATOIRE DE THÉORIE DES NOMBRES
Marseille, France

Reçu le 18. 1. 1982
et dans la forme modifiée le 5. 7. 1982 (1289)

ACTA ARITHMETICA
XLIII (1984)

Special values of the dilogarithm function

by

J. H. Loxton (Kensington, New South Wales, Australia)

1. Introduction. The *dilogarithm function* defined, for suitable z, by

$$\mathrm{Li}_2(z) = \sum_{n=1}^{\infty} z^n/n^2 = -\int_0^z \frac{\log(1-t)}{t}\,dt,$$

is one of the lesser transcendental functions. Nonetheless, as Lewin's treatise [3] demonstrates, it has a very respectable pedigree and a wealth of curious properties.

The present work will be concerned with some unexpected relations between the values of the dilogarithm function at certain algebraic integers. Lewin [4] has shown how interesting relations can be obtained by specializing Abel's functional equation for the dilogarithm function, but this technique does not seem to yield all the known results. Richmond and Szekeres [5] have introduced a different idea. They apply the circle method to obtain asymptotic formulae for the power series coefficients of the functions occurring on the two sides of a partition identity of Andrews and Gordon. A comparison of the two formulae then yields non-trivial numerical relations for the dilogarithm function. I shall exploit the same principle here. The investigation has produced some new partition identities of the same type as the celebrated Rogers–Ramanujan identities and some new relations between values of the dilogarithm function. In particular, I shall prove a formula conjectured by Lewin [4] which had apparently resisted more direct attacks. Despite this success, these ideas do not seem to touch the central problem here which is to explain the mechanism leading to such a profusion of identities.

2. The dilogarithm relations. It is most convenient to work with the function

$$L(z) = \mathrm{Li}_2(z) + \tfrac{1}{2}\log z \cdot \log(1-z)$$

instead of with the dilogarithm function itself. To avoid problems with complex logarithms, the argument z will be restricted to the interval