INSTYTUT MATEMATYCZNY POLSKIEJ AKADEMII NAUK

DISSERTATIONES MATHEMATICAE

(ROZPRAWY MATEMATYCZNE)

KOMITET REDAKCYJNY

KAROL BORSUK redaktor

ANDRZEJ BIAŁYNICKI-BIRULA, BOGDAN BOJARSKI,
ZBIGNIEW CIESIELSKI, JERZY ŁOŚ, ANDRZEJ MOSTOWSKI,
ZBIGNIEW SEMADENI, MARCELI STARK, WANDA SZMIELEW

XCV

GEORGES RHIN

Répartition modulo 1 dans un corps de séries formelles sur un corps fini

WARSZAWA 1972

PAŃSTWOWE WYDAWNICTWO NAUKOWE

5.7133

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

BUW—EO—73/193 /7

TABLE DES MATIÈRES

INTRODUCTION 5

CHAPITRE 0. Définitions et rappels. 7
1. Notations . . 7
2. Définitions et rappels . . 8

CHAPITRE 1. Majoration des sommes de Weyl $\sum_{n=M+1}^{M+N} e_0(Lf(P_n))$ lorsque $\deg Q \geqslant \log^3 \gamma$ 11
1. Notations 11
2. Etude de $D_1(\nu)$ et $D_2(\nu)$ . . . 12
3. Quelques lemmes arithmétiques sur $F_q[x]$ 18
4. Deux lemmes de préparation à la démonstration du théorème 1 . 23
5. Majoration du nombre de solutions de quelques équations diophantiennes sur $F_q[x]$ 28
6. Trois lemmes de préparation à la démonstration du théorème 2 38
7. Énoncés et démonstrations des théorèmes 1 et 2 48
8. Deux lemmes 53

CHAPITRE 2. Nombre de polynômes irréductibles dans une progression arithmétique . 57
1. Relations arithmétiques sur $\mathscr{M}$ 57
2. Etude des fonctions $L(\cdot, \chi)$ . . . 58
3. Isomorphisme entre $\mathscr{G}(\mathscr{R}_{(k)H})$ et un groupe quotient du groupe des idèles de $\mathscr{F}$ 59
4. Fonctions L_ω lorsque ω est un quasi caractère des classes d'idèles 61
5. Théorie du corps de classes et fonctions L_ω . 62
6. Nombre de polynômes irréductibles dans une progression arithmétique 63

CHAPITRE 3. Equirépartition modulo 1 des suites $(f(P_n))_{n\geqslant 1}$ 67

BIBLIOGRAPHIE . 75

Introduction

Un des problèmes classiques de la théorie des nombres est la détermination des réels α pour lesquels, étant donné une suite croissante d'entiers λ_n, la suite $(\lambda_n \alpha)_{n \in N}$ est équirépartie modulo 1. En 1916, H. Weyl a démontré qu'il en était ainsi pour la suite $(\alpha_1 n + \ldots + \alpha_k n^k)_{n \in N}$ sous la condition nécessaire et suffisante que l'un des α_i soit irrationnel. D'autre part, J. F. Koksma (1935) a prouvé que la suite $(\lambda_n \alpha)_{n \in N}$ est équirépartie pour presque tout α. Il est naturel de remplacer N par l'ensemble $\mathscr{P}$ des nombres premiers. Le théorème de C. L. Siegel [7] sur la répartition des nombres premiers dans une progression arithmétique et la découverte de nouvelles méthodes de majoration des sommes trigonométriques que nous serons amenés à généraliser, permirent à I. M. Vinogradov de démontrer que la suite $(p\alpha)_{p \in \mathscr{P}}$ est équirépartie quand α est irrationnel [15] (1947). Ce résultat avait été établi en 1937 par P. Turan sous l'Hypothèse de Riemann. Reprenant l'étude de la même question, I. M. Vinogradov a donné [16] des conditions d'irrationnalité sur les α_i $(i \geqslant 2)$ pour que la suite $(\alpha_1 p + \quad + \alpha_k p^k)_{p \in \mathscr{P}}$ soit équirépartie.

Une certaine analogie entre l'arithmétique de $\boldsymbol{Z}$ et celle des polynômes sur un corps fini F_q à q éléments, a conduit à généraliser ces problèmes dans le complété de $F_q(x)$ pour la valuation „0-adique", c'est-à-dire dans le corps $\mathscr{F}_0$ des séries formelles de la forme $\theta = \sum_{-h}^{+\infty} a_n x^{-n}$ à coefficients $a_n \in F_q$. Dans ce corps, la notion d'équirépartition modulo 1 pourrait être généralisée de plusieurs façons. La définition la plus fructueuse semble être celle de L. Carlitz (1952) [2] qui a démontré la validité d'un analogue du critère de Weyl. Le théorème de Koksma a été généralisé par B. de Mathan (1967) [11] et les premiers résultats de Weyl par A. Dijksma (1970) [5].

Nous désignons par $(P_n)_{n \in N}$ la suite croissante (au sens de la définition 2, p. 9) des polynômes irréductibles unitaires sur F_q. Notre résultat principal est le suivant:

La suite $(P_n \alpha)_{n \in N}$ est équirépartie modulo 1 dans $\mathscr{F}_0$ si et seulement si α n'est pas un élément de $F_q(x)$.

Nous donnons aussi des majorations du reste de la suite $(P_n \alpha)_{n \in N}$ et plus généralement d'une suite $(f(P_n))_{n \in N}$ lorsque f est un polynôme de $\mathscr{F}_0[X]$

de degré inférieur à p dont un coefficient α satisfait une condition d'irrationnalité.

La démonstration de ces théorémes requiert l'étude de l'arithmétique de $F_q[x]$ et la généralisation à $\mathscr{F}_0$ des méthodes des sommes trigonométriques de I. M. Vinogradov. Ceci est fait dans une première partie. Dans la seconde partie, nous étudions la répartition des polynômes irréductibles dans une progression arithmétique à l'aide des fonctions L introduites par Hayes [8]. Nous montrons que ces fonctions diffèrent peu des fonctions L définies par Weil [18] pour lesquelles celui-ci a démontré l'hypothèse de Riemann [19]. Ces résultats généralisent ceux de Artin [1], Carlitz [2] et Uchiyama [14].

Dans le chapitre 0, nous rappelons la définition de l'équirépartition modulo 1 dans $\mathscr{F}_0$ et le critère de Weyl. Nous définissons un ordre sur $F_q[x]$. Cet ordre se réduit à celui donné par Dijksma [4] sous la condition supplémentaire que 0 soit minimum dans F_q.

Dans les chapitres suivants, nous étudions les sommes de Weyl $\sum_{n=M+1}^{M+N} e_0\big(Lf(P_n)\big)$, le coefficient irrationnel α étant approché par une réduite A/Q.

Dans le chapitre 1, nous majorons ces sommes de Weyl lorsque degré de $Q \geqslant \log^3\gamma$ où γ est le degré du polynôme P_{M+N} mentionné ci-dessus. Dans les paragraphes 2, 3 et 5, nous démontrons quelques lemmes arithmétiques. En particulier, nous calculons les sommes

$$D_i(\nu) = \sum_{|F|_0 \leqslant q^\nu} d^i(F) \qquad (i = 1, 2)$$

où $d(F)$ désigne le nombre de diviseurs unitaires de F. Le lemme 19 généralise un résultat de I. M. Vinogradov amélioré par Hua [10]. Les paragraphes 4 et 6 donnent des majorations des sommes doubles $\sum_G \sum_H e_0\big(f(GH)\big)$ qui interviennent dans la démonstration des théorèmes 1 et 2. Dans le cas où le degré de f est supérieur ou égal à 2, nous obtenons une condition d'irrationnalité sur α moins exigeante que celle donnée par Vinogradov [16].

Dans le chapitre 2, le calcul du nombre de polynômes irréductibles de degré donné dans une progression arithmétique nous amène à déterminer les régions du plan complexe dans lesquelles les fonctions $L(\cdot\,,\chi)$, où χ est un caractère modulo une relation arithmétique $\mathscr{R}$, ne s'annulent pas.

Pour cela nous démontrons que le groupe des caractères modulo une relation arithmétique $\mathscr{R}_{(k)H}$ est isomorphe à un groupe de quasi-caractères sur le groupe des idèles de $F_q(x)$.

Le chapitre 3 regroupe les résultats des chapitres précédents et donne, outre le théorème 9 déjà cité, des majorations du reste des suites $\big(f(P_n)\big)_{n\in N}$.

CHAPITRE 0

Définitions et rappels

1. Notations. Si p est un nombre premier, f un entier positif, on désigne par F_q le corps fini à $q = p^f$ éléments.

$F_q[x]$ est l'anneau des polynômes à une indéterminée sur F_q et $F_q[x]^* = F_q[x] - \{0\}$.

$\mathscr{F} = F_q(x)$ est le corps des fractions rationnelles à une indéterminée sur F_q.

La valuation „0-adique" sur le corps $\mathscr{F}$ est la valuation w_0 définie par

$$w_0\left(\frac{A}{B}\right) = \deg(B) - \deg(A) \quad \text{où } A \in F_q[x]^*,\ B \in F_q[x]^*$$

et $\deg(A)$ désigne le degré du polynôme A. La valeur absolue associée à la valuation w_0 est

$$\left|\frac{A}{B}\right|_0 = q^{-w_0(A/B)}.$$

$\mathscr{F}_0$ désigne le complété de $\mathscr{F}$ pour cette valeur absolue. $\mathscr{F}_0$ s'identifie au corps $F_q\{x^{-1}\}$ des séries de Laurent formelles:

$$\theta = \sum_{-\infty}^{+\infty} a_n x^{-n} \text{ où } a_n \in F_q \quad \text{et} \quad a_n = 0 \text{ pour } n < n_\theta.$$

La valeur absolue sur $\mathscr{F}_0$ qui prolonge celle de $\mathscr{F}$ est définie par:

$$|\theta|_0 = q^{-n_\theta} \quad \text{si } a_{n_\theta} \neq 0.$$

$\mathscr{P} = x^{-1}F_q[[x^{-1}]]$ est l'idéal de valuation de $\mathscr{F}_0$, où $F_q[[T]]$ désigne l'anneau des séries formelles en T à coefficients dans F_q.

$\mathscr{H}_0$ est l'homomorphisme du groupe additif $\mathscr{F}_0^+$ sur le groupe additif $\mathscr{P}^+$ défini par

$$\mathscr{H}_0(\theta) = \mathscr{H}_0\left(\sum_{-\infty}^{+\infty} a_n x^{-1}\right) = \sum_{n=1}^{+\infty} a_n x^{-n}.$$

$d\theta$ désigne la mesure de Haar du groupe additif localement compact $\mathscr{F}_0^+$ normalisée à $\mathscr{P}$, c'est-à-dire telle que

$$\int_{\mathscr{P}} 1\cdot d\theta = 1.$$

Si ψ est un caractère différent de 1 de F_q^+, nous définissons le caractère e_0 de $\mathscr{F}_0^+$ par

$$e_0\Big(\sum_{-\infty}^{+\infty} a_n x^{-n}\Big) = \psi(a_1).$$

Si $H \in F_q[x]$ alors $e_0(H\theta) = e_0\big(H\mathscr{H}_0(\theta)\big)$ et $e_0(H) = 1$. Si $\theta \in \mathscr{P}^2$ alors $e_0(\theta) = 1$.

Soient $\mathscr{B} = a+\mathscr{P}^b$ une boule contenue dans $\mathscr{P}$ et $\Theta = (\theta_n)_{n\geqslant 1}$ une suite d'éléments de $\mathscr{F}_0$. Nous désignons par $F_N(\mathscr{B}, \Theta)$ le nombre d'entiers n tels que $1 \leqslant n \leqslant N$ et $\mathscr{H}_0(\theta_n) \in \mathscr{B}$. Nous posons

$$R_N(\mathscr{B}, \Theta) = F_N(\mathscr{B}, \Theta) - N \operatorname{mes} \mathscr{B} = F_N(\mathscr{B}, \Theta) - Nq^{1-b},$$

et

$$ND_N(\Theta) = \sup_{\mathscr{B}\subseteq\mathscr{P}} |R_N(\mathscr{B}, \Theta)|.$$

2. Définitions et rappels.

DÉFINITION 1 [3]. Une suite Θ d'éléments de $\mathscr{F}_1$ est dite *équirépartie modulo* 1 si et seulement si

$$\lim_{N\to+\infty} D_N(\Theta) = 0.$$

Nous obtenons alors le critère de Weyl [3] et [11]:

CRITÈRE DE WEYL. *Une suite Θ est équirépartie modulo* 1 *dans $\mathscr{F}_0$ si et seulement si pour tout $H \in F_q[x]^*$*

$$\lim_{N\to+\infty} \frac{1}{N} \sum_{n=1}^{N} e_0(H\theta_n) = 0.$$

Nous définissons sur $F_q[x]$ l'ordre total suivant:

DÉFINITION 2. Soit un *ordre total* arbitraire sur F_q. A cet ordre, sera associé l'ordre suivant sur $F_q[x]$:

$$G < H$$

si l'une des deux propriétés suivantes est vérifiée

(i) $$|G|_0 < |H|_0,$$

(ii) $$|G|_0 = |H|_0 = q^n$$

avec

$$G = g_0x^n + g_1x^{n-1} + \ldots + g_n,$$
$$H = h_0x^n + h_1x^{n-1} + \quad + h_n$$

et il existe un entier ν, $0 \leqslant \nu \leqslant n$, tel que

$$g_i = h_i \quad \text{si } 0 \leqslant i \leqslant \nu - 1$$

et

$$g_\nu < h_\nu \quad \text{pour l'ordre de } F_q.$$

PROPOSITION 1. *Soient G et H deux polynômes unitaires de degré n tels que*

$$|G-H|_0 > q^\omega \quad \textit{avec } 0 \leqslant \omega < n-1.$$

Alors quels que soient les polynômes unitaires X et Y tels que $|X-G|_0 \leqslant q^\omega$ et $|Y-H|_0 \leqslant q^\omega$ nous avons $X < Y$ si et seulement si $G < H$.

Démonstration. Supposons $G < H$. Il existe ν tel que $1 \leqslant \nu \leqslant n$ et

$$g_i = h_i \quad \text{pour } 0 \leqslant i \leqslant \nu - 1,$$
$$g_\nu < h_\nu.$$

Puisque $|G-H|_0 > q^\omega$, $|G-H|_0 = q^{n-\nu} > q^\omega$ et $\nu \leqslant n-1-\omega$. Si

$$X = x^n + a_1 x^{n-1} + \ldots + a_n,$$
$$Y = x^n + b_1 x^{n-1} + \quad + b_n$$

alors

$$a_i = g_i \quad \text{pour } 1 \leqslant i \leqslant n-1-\omega,$$
$$b_i = h_i \quad \text{pour } 1 \leqslant i \leqslant n-1-\omega,$$

donc

$$a_i = b_i \quad \text{pour } 1 \leqslant i \leqslant \nu - 1.$$

De plus $a_\nu < b_\nu$ car $a_\nu = g_\nu$ et $b_\nu = h_\nu$ donc $X < Y$.

Réciproquement si $X < Y$, puisque $|X-Y|_0 > q^\omega$, il existe ν tel que

$$\nu \leqslant n-1-\omega$$
$$a_i = b_i \qquad \text{pour } 1 \leqslant i \leqslant \nu - 1$$
$$a_\nu < b_\nu$$

et puisque $|X-G|_0 \leqslant q^\omega$ et $|Y-H|_0 \leqslant q^\omega$ on a $a_i = g_i$ et $b_i = h_i$ pour $1 \leqslant i \leqslant n-1-\omega$ donc $G < H$.

CHAPITRE 1

Majoration des sommes de Weyl $\sum_{n=M+1}^{M+N} e_0(Lf(P_n))$ lorsque $\deg Q \geqslant \log^3 \gamma$

1. Notations. On désigne par $\boldsymbol{N}$ l'ensemble des entiers naturels, par $\boldsymbol{N}^*$ l'ensemble des entiers naturels non nuls, par $\mathscr{M}$ l'ensemble des polynômes unitaires de $F_q[x]$

$\pi(\nu)$ est le nombre des polynômes irréductibles de $\mathscr{M}$ de degré ν.

Si G est un élément de $\mathscr{M}$, $d(G)$ désigne le nombre de polynômes de $\mathscr{M}$ qui divisent G.

On notera F divise G par $F \mid G$.

$\Phi(G)$ est le nombre d'éléments de $\mathscr{M}$ de même degré que G, premiers à G.

μ est la fonction de Möbius sur $\mathscr{M}$, c'est-à-dire

$$\mu(G) = \begin{cases} 1 & \text{si } G = 1, \\ 0 & \text{si } H^2 | G \text{ et } \deg H \geqslant 1, \\ (-1)^r & \text{si } G = \prod_{i=1}^{r} P_i \text{ où les } P_i \text{ sont des polynômes} \\ & \text{irréductibles distincts.} \end{cases}$$

$$\sigma_a(G) = \sum_{\substack{F|G \\ F \in \mathscr{M}}} |F|_0^a; \qquad D_a(\nu) = \sum_{\substack{|F|_0 \leqslant q^\nu \\ F \in \mathscr{M}}} d^a(F).$$

$\zeta(s)$ désigne la fonction zêta de $\mathscr{M}$ [6]: elle est définie par

$$\zeta(s) = \sum_{F \in \mathscr{M}} |F|_0^{-s} \quad \text{pour } s = \sigma + it,\ \sigma, t \in \boldsymbol{R},\ \sigma > 1.$$

Son prolongement analytique dans $\boldsymbol{C}$ est donné par

$$\zeta(s) = (1 - q^{1-s})^{-1}$$

et si $\sigma > 1$

$$\zeta(s) = \prod_P (1 - |P|_0^{-s})^{-1}$$

le produit infini étant étendu à tous les polynômes irréductibles de $\mathscr{M}$.

2. Etude de $D_1(\nu)$ et $D_2(\nu)$.

LEMME 1. *Soit $\varepsilon > 0$; il existe une constante positive $C(\varepsilon)$ telle que pour tout élément Q de $\mathcal{M}$*

$$d(Q) \leqslant C(\varepsilon)\, |Q|_0^{\varepsilon}.$$

Démonstration. Si P est irréductible et $|P|_0 > 2^{1/\varepsilon}$ alors

$$\frac{d(P^l)}{|P^l|_0^{\varepsilon}} = \frac{l+1}{|P^l|_0^{\varepsilon}} \leqslant \frac{l+1}{2^l} = \frac{l+1}{(1+1)^l} \leqslant \frac{l+1}{l+1} = 1.$$

Si P est irréductible et $|P|_0 \leqslant 2^{1/\varepsilon}$, puisque $|P|_0 \geqslant q \geqslant 2$

$$\frac{d(P^l)}{|P^l|_0^{\varepsilon}} = \frac{l+1}{|P^l|_0^{\varepsilon}} \leqslant \frac{l+1}{2^{l\varepsilon}} \leqslant \frac{l+1}{l\varepsilon \log 2} \leqslant \frac{2}{\varepsilon \log 2}.$$

Soit $Q = P_1^{l_1} \dots P_s^{l_s}$ où $P_1, \dots, P_s$ sont les facteurs irréductibles distincts de Q. Alors

$$\frac{d(Q)}{|Q|_0^{\varepsilon}} = \prod_{P|Q} \frac{d(P^l)}{|P^l|_0^{\varepsilon}} \leqslant \prod_{|P|_0 \leqslant 2^{1/\varepsilon}} \frac{2}{\varepsilon \log 2} = C(\varepsilon).$$

LEMME 2. *Soient f et g deux applications de $\mathcal{M}$ dans $\boldsymbol{C}$ telles que pour $G \in \mathcal{M}$*

$$f(G) = \sum_{\substack{F|G \\ F \in \mathcal{M}}} g(F)$$

Alors

$$\sum_{\substack{|F|_0 \leqslant q^\nu \\ F \in \mathcal{M}}} f(F) = \sum_{\substack{|F|_0 \leqslant q^\nu \\ F \in \mathcal{M}}} (1 + q + \quad + q^{\nu - \deg F}) g(F). \tag{1}$$

Démonstration.

$$\sum_{\substack{|F|_0 \leqslant q^\nu \\ F \in \mathcal{M}}} f(F) = \sum_{\substack{|F|_0 \leqslant q^\nu \\ F \in \mathcal{M}}} \sum_{\substack{G|F \\ G \in \mathcal{M}}} g(G) = \sum_{\substack{|G|_0 \leqslant q^\nu \\ G \in \mathcal{M}}} \sum_{\substack{G|F \\ |F|_0 \leqslant q^\nu \\ F \in \mathcal{M}}} g(G)$$

$$= \sum_{\substack{|G|_0 \leqslant q^\nu \\ G \in \mathcal{M}}} g(G) \sum_{\substack{|A|_0 \leqslant q^{\nu - \deg G} \\ A \in \mathcal{M} \\ F = AG}} 1 = \sum_{\substack{|G|_0 \leqslant q^\nu \\ G \in \mathcal{M}}} (1 + q + \dots + q^{\nu - \deg G}) g(G).$$

LEMME 3.

$$D_1(\nu) = q^{\nu+1}\left(\frac{\nu}{q-1} + \frac{q-2}{(q-1)^2}\right) + \frac{1}{(q-1)^2}. \tag{2}$$

Il suffit d'appliquer l'égalité (1) avec $g = 1$ et $f = d$.

LEMME 4 [6].

$$\pi(\nu) = \frac{1}{\nu} \sum_{\lambda|\nu} \mu\left(\frac{\nu}{\lambda}\right) q^\lambda$$

où μ désigne la fonction de Möbius sur $\boldsymbol{N}$.

LEMME 5. *Soient a et b deux réels et*

$$Z(s) = \frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)}.$$

Pour $\sigma > \sigma_0 = \max\left(1, 1+a, 1+b, 1+a+b, \frac{1}{2}(1+a+b)\right)$

$$Z(s) = \sum_{G\in\mathscr{M}} \frac{\sigma_a(G)\sigma_b(G)}{|G|_0^s}.$$

Démonstration. Supposons que $a \neq b$, $a \neq 0$, et $b \neq 0$. Pour $\sigma > \sigma_0$

$$Z(s) = \prod_P \frac{1-|P|_0^{a+b}|P|_0^{-2s}}{(1-|P|_0^{-s})(1-|P|_0^a|P|_0^{-s})(1-|P|_0^b|P|_0^{-s})(1-|P|_0^{a+b}|P|_0^{-s})}$$

$$= \prod_P \frac{1}{(1-|P|_0^a)(1-|P|_0^b)} \sum_{n=0}^{+\infty} |P|_0^{-ns}(1-|P|_0^{(n+1)a})(1-|P|_0^{(n+1)b}).$$

En séparant les différentes fractions et en les développant suivant les puissances de $|P|_0$, nous obtenons:

$$Z(s) = \sum_{G\in\mathscr{M}} \frac{\varrho(G)}{|G|_0^s} \quad \text{où } G = P_1^{a_1}\ldots P_r^{a_r},$$

$$\varrho(G) = \prod_{k=1}^{r} \frac{(1-|P_k|_0^{(a_k+1)a})(1-|P_k|_0^{(a_k+1)b})}{(1-|P_k|_0^a)(1-|P_k|_0^b)};$$

σ_a est une fonction multiplicative sur $\mathscr{M}$; en effet, si $(F, G) = 1$

$$\sigma_a(FG) = \sum_{\substack{H|FG\\ H\in\mathscr{M}}} |H|_0^a = \sum_{\substack{H_1|G\\ H_2|F}} |H_1H_2|_0^a$$

$$= \Big(\sum_{\substack{H|F\\ H\in\mathscr{M}}} |H|_0^a\Big)\Big(\sum_{\substack{K|G\\ K\in\mathscr{M}}} |K|_0^a\Big) = \sigma_a(F)\cdot\sigma_a(G).$$

Il suffit alors de calculer $\sigma_a(P^k)$ où P est irréductible,

$$\sigma_a(P^k) = \sum_{i=0}^{k} |P^i|_0^a = \sum_{i=0}^{k} |P|_0^{ia} = \frac{1-|P|_0^{(k+1)a}}{1-|P|_0^a}.$$

Ceci montre que $\varrho(G) = \sigma_a(G)\sigma_b(G)$.

En passant à la limite, la formule est aussi vérifiée pour $a = b$, $a = 0$ ou $b = 0$.

PROPOSITION 2.

$$D_2(\nu) = (A\nu^3 + B\nu^2 + C\nu + D)q^\nu + E$$

où

$$A = \tfrac{1}{6}, \quad B = \frac{2q-1}{2(q-1)}, \quad C = \frac{11q^2-19q+2}{6(q-1)^2},$$

$$D = 1+\frac{1}{(q-1)^3}, \quad E = -\frac{1}{(q-1)^3}.$$

Démonstration. D'après le lemme 5, en posant $a = b = 0$, nous avons

$$\frac{\zeta^4(s)}{\zeta(2s)} = \sum_{G\in\mathscr{M}} \frac{d^2(G)}{|G|_0^s} \quad \text{pour } \sigma > 1.$$

Cette série est uniformément convergente dans le demi-plan $\sigma \geqslant \sigma_0 > 1$ pour tout σ_0; il suffit en effet d'utiliser le lemme 1 avec $\varepsilon < (\sigma_0-1)/2$.

Pour $\nu \geqslant 0$

$$\frac{1}{2\pi i}\int_{(2)} \frac{q^{\nu s}}{s^2}\cdot\frac{\zeta^4(s)}{\zeta(2s)}\,ds = \frac{1}{2\pi i}\sum_{\substack{G\in\mathscr{M}\\ |G|_0=q^g}} d^2(G)\int_{(2)} \frac{q^{(\nu-g)s}}{s^2}\cdot ds$$

où (2) est la droite $s = 2+it$ parcourue de $t = -\infty$ à $t = +\infty$.

Si $\nu-g \geqslant 0$,

$$\frac{1}{2\pi i}\int_{(2)} \frac{q^{(\nu-g)s}}{s^2}\cdot ds = (\nu-g)\log q.$$

Si $\nu-g < 0$,

$$\int_{(2)} \frac{q^{(\nu-g)s}}{s^2}\cdot ds = 0.$$

On a donc

$$D_2(\nu) = \frac{1}{2\pi i\log q}\int_{(2)} \frac{q^{(\nu+1)s}-q^{\nu s}}{s^2}\cdot\frac{\zeta^4(s)}{\zeta(2s)}\,ds.$$

Intégrons la fonction

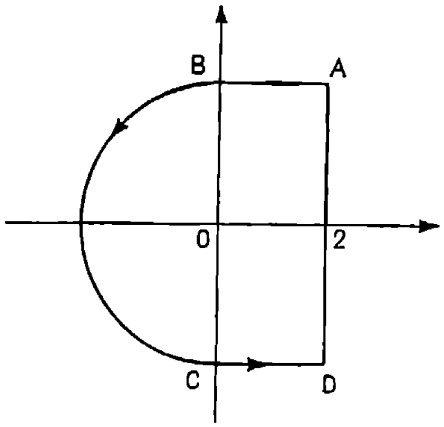
$$u(s) = \frac{q^{(\nu+1)s}-q^{\nu s}}{s^2}\cdot\frac{\zeta^4(s)}{\zeta(2s)}$$

sur le contour $\widehat{ABCDA}$ suivant:

$$A = 2+i\frac{(2k+1)\pi}{\log q}, \quad k \geqslant 1,$$

$$D = 2-i\frac{(2k+1)\pi}{\log q},$$

$\widehat{BC}$ est le demi cercle de centre O et de rayon $(2k+1)\pi/\log q$



$$\left| D_2(\nu) - \frac{1}{2\pi i \log q} \int_{DA} u(s)\,ds \right| \leqslant \frac{2}{2\pi \log q} \int_{\frac{(2k+1)\pi}{\log q}}^{+\infty} \frac{2q^{2(\nu+1)}}{4+t^2} \cdot \frac{(1-q^{-1})^{-4}}{(1-q^{-3})^{-1}}\,dt$$
$$\leqslant \frac{c(q,\nu)}{k}$$

où $c(q,\nu)$ ne dépend pas de k. Alors

$$\lim_{k\to+\infty} \frac{1}{2\pi i \log q} \int_{DA} u(s)\,ds = D_2(\nu).$$

Démontrons que sur AB et CD, $|u(s)| \leqslant C(q,\nu)/k^2$. Sur CD nous aurons, en posant $t_k = (2k+1)\pi/\log q$,

$$u(s) = u(\sigma+it_k) = \frac{q^{(\nu+1)s}-q^{\nu s}}{(\sigma+it_k)^2} \cdot \left[\frac{q^{s-1}}{1-q^{\sigma-1+it_k}}\right]^4 \cdot \frac{1-q^{2s-1}}{q^{2s-1}}$$

d'où

$$|u(s)| \leqslant \frac{2q^{(\nu+1)\sigma}}{t_k^2} \cdot q^{4\sigma-1} \cdot \frac{1+q^{2\sigma-1}}{q^{2\sigma-1}}.$$

Puisque $0 \leqslant \sigma \leqslant 2$, on a $|u(s)| \leqslant C(q,\nu)/k^2$ où $C(q,\nu)$ ne dépend pas de k.

Nous aurons le même résultat sur AB, donc

$$\lim_{k\to+\infty} \left[\int_{AB} u(s)\,ds + \int_{CD} u(s)\,ds \right] = 0.$$

Sur l'arc $\widehat{BC}$, puisque $\sigma \leqslant 0$, nous aurons

$$\left| \frac{\zeta^4(s)}{\zeta(2s)} \right| \leqslant \frac{q^{1-2\sigma}+1}{(q^{1-\sigma}-1)^4} \leqslant \frac{q^{1+2\sigma}+q^{4\sigma}}{(q-q^{\sigma})^4} \leqslant q+1$$

et

$$|q^{(\nu+1)s} - q^{\nu s}| \leqslant 2$$

donc

$$|u(s)| \leqslant \frac{2(q+1)}{|s|^2} = \frac{2(q+1)}{t_k^2}$$

et

$$\left| \int\limits_{\widehat{BC}} u(s)\,ds \right| \leqslant \frac{2\pi(q+1)}{t_k}.$$

Nous avons donc $\lim\limits_{k\to+\infty} \int\limits_{\widehat{BC}} u(s)\,ds = 0$ et par conséquent

$$D_2(\nu) = \lim_{k\to+\infty} \frac{1}{2\pi i \log q} \int\limits_{\widehat{ABCDA}} u(s)\,ds.$$

D'autre part, nous avons

$$\frac{1}{2\pi i \log q} \int\limits_{\widehat{ABCDA}} u(s)\,ds$$

$$= \frac{1}{\log q}\left[\operatorname{Res}(u, 0) + \operatorname{Res}(u, 1) + \sum_{l=1}^{k} \operatorname{Res}\left(u, 1 + \frac{2l\pi i}{\log q}\right) + \right.$$

$$\left. + \sum_{l=1}^{k} \operatorname{Res}\left(u, 1 - \frac{2l\pi i}{\log q}\right)\right].$$

Calculons le résidu en 0 de u:

$$q^{(\nu+1)s} - q^{\nu s} = q^{\nu s}\big(s \log q + o(s)\big)$$

donc $\operatorname{Res}(u, 0) = \zeta^3(0) \log q = \log q/(1-q)^3$. Calculons le résidu de u en $\omega = 1 + 2l\pi i/\log q$. Posons $s = \omega + z$,

$$q^{\nu s} = q^{\nu\omega} \cdot q^{\nu z} = q^{\nu}\big(1 + \nu z \log q + \tfrac{1}{2}\nu^2 z^2 \log^2 q + \tfrac{1}{6}\nu^3 z^3 \log^3 q + o(z^3)\big),$$

$$s^{-2} = \omega^{-2}\left(1 + \frac{z}{\omega}\right)^{-2} = \omega^{-2}\left(1 - \frac{2z}{\omega} + \frac{3z^2}{\omega^2} - \frac{4z^3}{\omega^3} + o(z^3)\right),$$

$$(q^{s-1} - 1)^{-4} = (q^z - 1)^{-4} = z^{-4}\log^{-4} q\left(1 + \frac{z}{2}\log q + \frac{z^2}{6}\log^2 q + \frac{z^3}{24}\log^3 q + o(z^3)\right)^{-4}$$

$$= z^{-4}\log^{-4} q\big(1 - 2z\log q + \tfrac{11}{6}z^2\log^2 q - z^3\log^3 q + o(z^3)\big),$$

$$1 - q^{1-2s} = 1 - q^{-1}\big(1 - 2z\log q + 2z^2\log^2 q - \tfrac{4}{3}z^3\log^3 q + o(z^3)\big).$$

Donc le développement en série de Laurent de $u(s)$ au voisinage de $s = \omega$ est

$$u(\omega + z) = \frac{a_0}{z^4} + \frac{a_1}{z^3} + \frac{a_2}{z^2} + \frac{a_3}{z} + f(z)$$

et

$$\operatorname{Res}(u, \omega) = a_3 = \left(\frac{P_1(\nu)}{\omega^2} + \frac{P_2(\nu)}{\omega^3} + \frac{P_3(\nu)}{\omega^4} + \frac{P_4(\nu)}{\omega^5}\right) q^{\nu} \log q$$

où les P_i $(i = 1, \ldots, 4)$ sont des polynômes de degré 3 dont les coefficients sont réels et ne dépendent que de q. Donc

$$D_2(\nu) = \frac{1}{(1-q)^3} + q^\nu \sum_{l\in Z}\left(\frac{P_1(\nu)}{\omega_l^2} + \frac{P_2(\nu)}{\omega_l^3} + \frac{P_3(\nu)}{\omega_l^4} + \frac{P_4(\nu)}{\omega_l^5}\right)$$

et donc

$$D_2(\nu) = q^\nu(A\nu^3 + B\nu^2 + C\nu + D) - \frac{1}{(q-1)^3}$$

où A, B, C, D sont réels et ne dépendent que de q.

Pour calculer ces coefficients nous calculerons $D_2(\nu)$ pour $\nu = 0, 1, 2, 3$,

$$D_2(0) = 1 \Rightarrow D = 1 + \frac{1}{(q-1)^3}.$$

$D_2(1) - D_2(0) = 4q$ car il y a q polynômes unitaires de degré 1 et ils sont tous irréductibles et ont exactement deux diviseurs distincts.

Les polynômes unitaires de degré 2 se répartissent en trois classes:

1° $\frac{1}{2}(q^2 - q)$ irréductibles,

2° q carrés,

3° $q(q-1)/2$ qui ont deux facteurs distincts de degré 1. Donc

$$D_2(2) - D_2(1) = \tfrac{1}{2}(q^2 - q) \times 4 + 9q + 16q(q-1)/2.$$

Les polynômes unitaires de degré 3 se répartissent en cinq classes:

1° $\frac{1}{3}(q^3 - q)$ irréductibles,

2° q cubes,

3° $q \times q(q-1)/2$ polynômes produits d'un polynôme de degré 2 et d'un polynômes de degré 1,

4° $q(q-1)$ polynômes produits d'un carré d'un polynôme de degré 1 par un autre polynôme de degré 1,

5° $q(q-1)(q-2)/6$ polynômes produits de trois polynômes distincts de degré 1. Donc

$$D_2(3) - D_2(2) = \tfrac{1}{3}(q^3 - q) \times 4 + 16q + \tfrac{1}{2}q^2(q-1) \times 16 + 36q(q-1) + \\ + \tfrac{64}{6}q(q-1)(q-2).$$

Nous obtenons alors le système d'équations:

$$Aq + Bq + Cq + \left(1 + \frac{1}{(q-1)^3}\right)q - 1 = 4q,$$

$$A(8q^2 - q) + B(4q^2 - q) + C(2q^2 - q) + \left(1 + \frac{1}{(q-1)^3}\right)(q^2 - q) = 10q^2 - q,$$

$$A(27q^3 - 8q^2) + B(9q^3 - 4q^2) + C(3q^3 - 2q^2) + \left(1 + \frac{1}{(q-1^3)}\right)(q^3 - q^2) \\ = 20q^3 - 4q^2$$

BU W

qui donne

$$A = \tfrac{1}{6}, \quad B = 1+\frac{1}{2}\cdot\frac{1}{q-1} = \frac{2q-1}{2(q-1)},$$

$$C = \frac{11}{6}+\frac{1}{2}\cdot\frac{1}{q-1}-\frac{1}{(q-1)^2} = \frac{11q^2-19q+2}{6(q-1)^2}.$$

Donc

$$\sum_{|G|_0=q^\nu} d^2(G) = (A_1\nu^3+B_1\nu^2+C_1\nu+D_1)q^\nu+E_1$$

où

$$A_1 = \frac{1}{6}\left(1-\frac{1}{q}\right) = \frac{1}{6\zeta(2)}.$$

Dans le cas réel, nous avons une formule analogue [17]

$$\sum_{n\leqslant x} d^2(n) = x(a\log^3 x+b\log^2 x+c\log x+d)+O(x^{1/2+\varepsilon})$$

où

$$a = \frac{1}{\pi^2} = \frac{1}{6\zeta_{\boldsymbol{R}}(2)},$$

et $\zeta_{\boldsymbol{R}}$ désigne la fonction zeta de Riemann.

Corollaire. *Pour* $\nu\geqslant 2$, $D_1(\nu)-D_1(\nu-1)\leqslant 2\nu q^\nu$ *et* $D_2(\nu)\leqslant 2\nu^3 q^\nu$.

Démonstration.

$$D_1(\nu)-D_1(\nu-1) = q^\nu(\nu+1)\leqslant 2\nu q^\nu.$$

Comme $q\geqslant 2$, nous avons $D_2(\nu)\leqslant(\frac{1}{6}\nu^3+\frac{3}{2}\nu^2+\frac{7}{3}\nu+2)q^\nu$ et il est facile de voir que pour $\nu\geqslant 2$

$$\tfrac{1}{6}\nu^3+\tfrac{3}{2}\nu^2+\tfrac{7}{3}\nu+2\leqslant 2\nu^3.$$

3. Quelques lemmes arithmétiques sur $F_q[x]$.

Lemme 6. *Soit $\mathscr{A}$ un ensemble fini de A polynômes distincts de $F_q[x]$ et soit $\beta\in\mathscr{F}_0$. Alors, si r est un entier* $(r\geqslant 1)$

$$I = \int_{\mathscr{F}} |S(\beta)|^{2r}d\beta\leqslant A^{2r-1}$$

où

$$S(\beta) = \sum_{H\in\mathscr{A}} e_0(\beta H).$$

Démonstration. Nous avons:

$$I = \int_{\mathscr{F}} \sum_{\substack{(n_1,\ldots,n_r)\\(m_1,\ldots,m_r)\\1\leqslant n_i\leqslant A;\,1\leqslant m_i\leqslant A}} e_0\big(\beta(H_{n_1}+\ldots+H_{n_r}-H_{m_1}-\quad -H_{m_r})\big)d\beta$$

et

$$\int_{\mathscr{P}} e_0(H\beta)\,d\beta = \begin{cases} 0 & \text{si } H \neq 0, \\ 1 & \text{si } H = 0, \end{cases}$$

cette intégrale étant l'intégrale du caractère $\beta \to e_0(\beta H)$ sur le groupe compact $\mathscr{P}^+$.

I est donc égal au nombre de solutions de l'équation

$$H_{n_1} + \quad + H_{n_r} = H_{m_1} + \quad + H_{m_r}$$

où $1 \leqslant n_i \leqslant A$, $1 \leqslant m_i \leqslant A$, $H_{n_i} \in \mathscr{A}$, $H_{m_i} \in \mathscr{A}$.

$H_{n_1}, \ldots, H_{n_r}, H_{m_1}, \ldots, H_{m_{r-1}}$ étant fixés, il y a au plus un polynôme H_{m_r} de $\mathscr{A}$ vérifiant l'équation ci-dessus. Donc $I \leqslant A^{2r-1}$.

LEMME 7. *Soient A et Q deux polynômes tels que $(A, Q) = 1$, L un polynôme non nul et ν un entier positif. Le nombre de polynômes G de $F_q[x]$ tels que*

$$\left|\mathscr{H}_0\left(\frac{LAG}{Q}\right)\right|_0 \leqslant q^\delta |Q|_0^{-1}$$

et

$$|G|_0 \leqslant q^{\nu-1}$$

est majoré par

$$(q^{\delta+1} + |L|_0)(q^\nu |Q|_0^{-1} + 1).$$

Démonstration. Cherchons le nombre de polynômes G tels que

$$0 \leqslant |G|_0 \leqslant |Q|_0 \text{ et } |\mathscr{H}_0(AG/Q)|_0 \leqslant q^\delta |Q|_0^{-1}.$$

Si $\delta < 0$, la seule solution est $G = 0$.

Si $1 \leqslant q^\delta < |Q|_0$, soit $R \in F_q[x]$ tel que $0 \leqslant |R|_0 \leqslant q^\delta$, alors il existe un couple (G_0, K_0) unique tel que $G_0, K_0 \in F_q[x]$, $|G_0|_0 < |Q|_0$ et $AG_0 + K_0 Q = R$.

Nous avons $\mathscr{H}_0(AG_0/Q) = \mathscr{H}_0(R/Q) = R/Q$. G_0 est donc l'unique solution du système

$$0 \leqslant |G|_0 < |Q|_0, \qquad \mathscr{H}_0\left(\frac{AG}{Q}\right) = \frac{R}{Q}.$$

Il y a donc autant de solutions que de polynômes R, soit au plus $q^{\delta+1}$.

Examinons maintenant l'équation du lemme.

Si $D = (L, Q)$, $L = DL_1$ et $Q = DQ_1$ alors

$$\frac{LA}{Q} = \frac{L_1 A}{Q_1} \quad \text{avec } (L_1 A, Q_1) = 1.$$

Si $G = KQ_1 + G_1$ avec $|G_1|_0 < |Q_1|_0$, l'équation devient

$$\left|\mathscr{H}_0\left(\frac{L_1 A G_1}{Q_1}\right)\right|_0 \leqslant q^\delta \frac{|Q_1|_0}{|Q|_0} \cdot |Q_1|_0^{-1}.$$

Si $q^\delta|Q_1|/|Q|_0 < 1$, il n'y a que la solution $G_1 = 0$.

Sinon, il y a au plus $q^{\delta+1}\ |Q_1|_0/|Q|_0$ solutions pour K fixé. Il suffit donc maintenant de compter le nombre des polynômes K.

Si $q^{\nu-1} < |Q_1|_0$ alors seul $K = 0$ convient.

Si $q^{\nu-1} \geqslant |Q_1|_0$ alors $0 \leqslant |K|_0 \leqslant q^{\nu-1}|Q_1|_0^{-1}$.

Il y a donc toujours au plus $(q^\nu|Q_1|_0^{-1}+1)$ polynômes K. Le nombre total des solutions de l'équation du lemme est majoré par

$$\left(q^{\delta+1}\frac{|Q_1|_0}{|Q|_0}+1\right)(q^\nu|Q_1|_0^{-1}+1)$$

ce qui donne en multipliant le membre de gauche par $|D|_0$ et en divisant celui de droite par $|D|_0$:

$$\left(q^{\delta+1}\frac{|Q_1D|_0}{|Q|_0}+|D|_0\right)(q^\nu|Q_1D|_0^{-1}+|D|_0^{-1}\leqslant (q^{\delta+1}+|L|_0)(q^\nu|Q|_0^{-1}+1).$$

Lemme 8.

(i) *Soient $F\in\mathscr{M}$, $\mathscr{G}$ un sous-ensemble fini quelconque de $\mathscr{M}$, f une fonction numérique arbitraire sur $\mathscr{G}$. Alors si $S = \sum_{\substack{(G,F)=1\\ G\in\mathscr{G}}} f(G)$ et si $S_D = \sum_{\substack{G\equiv 0 \bmod D\\ G\in\mathscr{G}}} f(G)$ où $D\in\mathscr{M}$, nous aurons*

$$S = \sum_{\substack{D|F\\ D\in\mathscr{M}}} \mu(D)S_D.$$

(ii) *Soient $\mathscr{R}$ un sous-ensemble fini de $\mathscr{M}^2$ et f une fonction numérique arbitraire sur $\mathscr{R}$. Alors*

$$\sum_{\substack{(G,H)\in\mathscr{R}\\ (G,H)=1}} f(G,H) = \sum_{D\in\mathscr{M}}\mu(D)\sum_{(DG',DH')\in\mathscr{R}} f(DG',DH').$$

(iii) *$\Omega(D)$ désigne le nombre de facteurs irréductibles distincts de $D\in\mathscr{M}$. Soient m un entier positif pair, $\mathscr{G}$ une partie finie de $\mathscr{M}$ et f une fonction réelle positive ou nulle sur $\mathscr{G}$. Alors, si $F\in\mathscr{M}$*

$$\sum_{\substack{(G,F)=1\\ G\in\mathscr{G}}} f(G) \leqslant \sum_{\substack{D|F\\ D\in\mathscr{M}\\ \Omega(D)\leqslant m}} \mu(D)S_D$$

où S_D est défini comme dans (i).

Démonstration. Nous avons

$$\sum_{D|F}\mu(D)S_D = \sum_{D|F}\sum_{G\equiv 0 \bmod D}\mu(D)f(G).$$

Le coefficient de $f(G)$ est $\sum_{D|(F,G)}\mu(D)$ qui est égal à 1 si $(F,G)=1$ et à 0 sinon; ceci démontre (i).

(ii) est évident car le coefficient de $f(G, H)$ dans le membre de droite est $\sum \mu(D)$, la sommation étant étendue à tous les D unitaires qui divisent à la fois G et H.

Pour (iii), il suffit de démontrer que si $Z = (F, G) \neq 1$, alors $\sum_{\substack{D|Z \\ \Omega(D)\leqslant m}} \mu(D) \geqslant 0$ pour tout entier positif pair.

Si $\Omega(Z) = g$, nous n'avons besoin de considérer que le cas $m < g$.

Si nous regroupons les diviseurs D de Z qui ont le même nombre de facteurs irréductibles, la somme ci-dessus est

$$1-\binom{g}{1}+\binom{g}{2}+\ldots+\binom{g}{m} = \binom{g-1}{m} \geqslant 0.$$

LEMME 9. *Soient γ et γ_1 deux entiers tels que $1 \leqslant \gamma_1 < \gamma$, c un réel tel que $0 < c \leqslant 1$, $\mathscr{M}(\gamma, \gamma_1)$ l'ensemble des polynômes unitaires de degré inférieur ou égal à γ qui sont produits de polynômes irréductibles distincts de degré inférieur ou égal à γ_1.*

Alors il existe une partition $(\mathscr{D}_t)$ de $\mathscr{M}(\gamma, \gamma_1)$ en au plus

$$h = \exp\left(\left(\frac{\log\gamma_1}{\log(1+c)}+2\right)\log\gamma\right)$$

éléments telle que

(i) *pour tout t il existe un réel φ_t positif ou nul tel que*

$$\forall D \in \mathscr{D}_t, \quad q^{\varphi_t} \leqslant |D|_0 \leqslant q^{\varphi_t(1+c)},$$

(ii) *étant donné un réel γ_2 tel que $0 < \gamma_2 \leqslant \gamma - \gamma_1$ et $\varphi_t > \gamma_2$, il existe deux sous-ensembles $\mathscr{H}$ et $\mathscr{K}$ de $\mathscr{M}$ vérifiant les propriétés suivantes:*

(a) *il existe un réel ψ tel que $\gamma_2 < \psi \leqslant \gamma_1 + \gamma_2$ et $q^{\psi} \leqslant |K|_0 \leqslant q^{\psi(1+c)}$ pour tout $K \in \mathscr{K}$,*

(b) *si $\mathscr{C} = \{KH$ où $K \in \mathscr{K}, H \in \mathscr{H}, (H, K) = 1$ et $|KH|_0 \leqslant q^{\gamma}\}$ il existe une surjection $f\colon \mathscr{D}_t \to \mathscr{C}$ telle que le cardinal de $f^{-1}(KH)$ soit constant.*

Démonstration. Soit φ la fonction définie sur N par $\varphi(0) = 0$, $\varphi(1) = 1$ et $\varphi(t+1) = (1+c)\varphi(t)$ pour tout $t \in N^*$. Soit τ le plus grand entier tel que $\varphi(\tau) \leqslant \gamma_1$. Alors

$$(1+\tau)^{\tau-1} \leqslant \gamma_1 \quad \text{soit } \tau \leqslant 1+\frac{\log\gamma_1}{\log(1+c)}.$$

Tout polynôme $D \in \mathscr{M}(\gamma, \gamma_1)$ peut s'écrire

$$D = P_1 \cdot P_2 \ldots P_{\gamma}$$

où P_i est irréductible ou égal à 1 et

$$q^{\gamma_1} \geqslant |P_1|_0 \geqslant |P_2|_0 \geqslant \ldots \geqslant |P_{\gamma}|_0 \geqslant 1.$$

Soit $t_j = t_j(D)$ l'entier tel que

$$q^{\varphi(t_j)} \leqslant |P_j|_0 < q^{\varphi(t_j+1)}.$$

Si $|P_j|_0 = 1$, alors $t_j = 0$. Chaque polynôme D de $\mathscr{M}(\gamma, \gamma_1)$ définit ainsi une suite $\tau \geqslant t_1 \geqslant t_2 \geqslant \ldots \geqslant t_\gamma \geqslant 0$.

Soit $\mathscr{D}_t$ l'ensemble des polynômes D qui donnent la même suite $(t_1, \ldots, t_\gamma) = t$.

Soit $B(\tau+1, \gamma)$ le nombre de suites $(t_1, \ldots, t_\gamma)$ distinctes. Comme $B(\tau+1, \gamma) = B(\tau, \gamma) + B(\tau+1, \gamma-1)$, $B(1, \gamma) = 1$ et $B(\tau+1, 1) = \tau+1$, nous avons:

$$B(\tau+1, \gamma) = \binom{\gamma+\tau}{\tau} \leqslant \gamma^{\tau+1} \leqslant h.$$

Il y a donc au plus h ensembles $\mathscr{D}_t$.

Soit une suite $t = (t_1, \ldots, t_\gamma)$ et soit φ_t l'entier défini par $\varphi_t = \varphi(t_1) + \ldots + \varphi(t_\gamma)$.

Pour tous les polynômes D de $\mathscr{D}_t$, nous avons $|D|_0 \geqslant q^{\varphi_t}$.

Si $t_j > 0$ et $t_{j+1} = 0$, nous avons $D = P_1 \ldots P_j$, ce qui entraine

$$|D|_0 \leqslant q^{\varphi(1+t_1)+\ldots+\varphi(1+t_j)} \leqslant q^{(1+c)(\varphi(t_1)+\ldots+\varphi(t_j))}$$

soit $|D|_0 \leqslant q^{\varphi_t(1+c)}$.

La propriété (i) est donc vérifiée.

Soient γ_2 et φ_t tels que $0 < \gamma_2 < \varphi_t$. Il existe un entier s $(1 \leqslant s \leqslant \gamma)$ tel que

$$\varphi(t_1) + \ldots + \varphi(t_{s-1}) \leqslant \gamma_2 < \varphi(t_1) + \quad + \varphi(t_s).$$

Si $\psi = \varphi(t_1) + \ldots + \varphi(t_s)$, nous avons

$$q^\psi \leqslant |P_1 \ldots P_s|_0 < q^{(1+c)\psi}$$

et

$$\gamma_2 < \psi \leqslant \varphi(t_1) + \quad + \varphi(t_{s-1}) + \gamma_1 \leqslant \gamma_2 + \gamma_1.$$

Soit $\mathscr{K}$ l'ensemble des produits de polynômes distincts $P_1 \ldots P_s$ pour lesquels

$$q^{\varphi(t_j)} \leqslant |P_j|_0 < q^{\varphi(1+t_j)} \quad \text{pour } j = 1, \ldots, s,$$

$$|P_s|_0 \leqslant \ldots \leqslant |P_2|_0 \leqslant |P_1|_0 \leqslant q^{\gamma_1}.$$

La propriété (a) est vérifiée.

Soit $\mathscr{H}$ l'ensemble des produits distincts $P_{s+1} \ldots P_\gamma$ pour lesquels

$$q^{\varphi(t_j)} \leqslant |P_j|_0 < q^{\varphi(1+t_j)} \quad \text{pour } j = s+1, \ldots, \gamma,$$

$$|P_{s+1}|_0 \geqslant \ldots \geqslant |P_\gamma|_0.$$

Tous les produits KH avec $K \in \mathscr{K}$, $H \in \mathscr{H}$, $(H, K) = 1$ et $|KH|_0 \leqslant q^\gamma$ appartiennent à $\mathscr{D}_t$.

Etant donné $D \in \mathscr{D}_t$, il reste à déterminer de combien de façons D s'écrit sous forme d'un produit KH.

Si $t_s > t_{s+1}$ le couple (K, H) est unique car K est nécessairement le produit des facteurs irréductibles P de D tels que $|P|_0 \leqslant q^{\varphi(t_s)}$ et H est le produit des autres.

Si $t_s = t_{s+1}$, soient s_1 et s_2 les entiers tels que $t_j = t_s$ si et seulement si $s_1 \leqslant j \leqslant s_2$. Les polynômes irréductibles $(P_{t_j})_{s_1 \leqslant j \leqslant s_2}$ peuvent être des facteurs de K ou de H. On peut donc parmi ces $(s_2 - s_1 + 1)$ polynômes en choisir $(s - s_1 + 1)$ arbitraires pour figurer dans K.

Il y a donc

$$n = \binom{s_2 - s_1 + 1}{s - s_1 + 1}$$

façons de choisir K.

Comme n ne dépend que de la suite $t = (t_1 \ldots t_\gamma)$, la propriété (b) est démontrée.

4. Deux lemmes de préparation à la démonstration du théorème 1.

LEMME 10. *Soient: γ un entier tel que $\gamma \geqslant 10$; χ un entier positif tel que $\chi < \gamma$; y un entier tel que $\gamma/2 \leqslant y < \gamma$; ϱ_0 le réel égal à: $\chi/5$ si $\chi \leqslant \gamma/4$, $\gamma/20$ si $\gamma/4 \leqslant \chi \leqslant 3\gamma/4$, $(\gamma - \chi)/5$ si $3\gamma/4 \leqslant \chi < \gamma$; $\Delta_0 = \gamma^{2,5} q^{-\varrho_0}$; $Q \in \mathscr{M}$, $T \in \mathscr{M}$, $A \in F_q[x]^*$, $\theta \in \mathscr{P}$, $\tau \in \mathscr{F}_0$ tels que $(A, Q) = 1$, $|T|_0 = q^t$, $|Q|_0 = q^\chi$, $|\tau|_0 = q^y$; $L \in F_q[x]^*$ tel que $|L|_0 \leqslant q^{\varrho_0}$; r et ω des entiers tels que $\gamma - \varrho_0 \leqslant \omega < \gamma$, $r = \gamma$ ou $\gamma - 1$ et si $r = \gamma - 1$ alors $\omega = \gamma - 1$; R un polynôme unitaire de degré r; $\mathscr{G}$ et $\mathscr{H}$ deux parties de $\mathscr{M}$; ε un réel tel que $|\varepsilon| \leqslant 0{,}01\gamma$; ψ une application de $\mathscr{G}$ dans le corps $\mathbf{C}$ des complexes vérifiant la propriété suivante: si ν est un entier tel que $\gamma/4 - t - \varepsilon \leqslant \nu \leqslant \gamma/2 - t$ alors*

$$\sum_{\substack{|G|_0 = q^\nu \\ G \in \mathscr{G}}} |\psi(G)| \leqslant c_1 \gamma q^\nu, \qquad \sum_{\substack{|G|_0 = q^\nu \\ G \in \mathscr{G}}} |\psi(G)|^2 \leqslant c_2 \gamma^3 q^\nu$$

On pose

$$S = \sum_G \psi(G) \sum_H e_0(LT^2GHa) \quad \text{où } a = \frac{A}{Q} + \frac{\theta}{Q\tau},$$

la sommation étant faite sur couples (G, H) de $\mathscr{G} \times \mathscr{H}$ tels que $|T^2GH - R|_0 \leqslant q^\omega$, $|G|_0 = q^\nu$ et $\gamma/4 - t - \varepsilon \leqslant \nu \leqslant \gamma/2 - t$. Alors

$$|S| \leqslant C_3 q^{\omega+1} \cdot q^{-1,1t} \cdot \Delta_0 \quad \text{où } C_3 = \max(C_1,\ 2\sqrt{C_2}).$$

Démonstration. Supposons que $t > 1{,}2\,\varrho_0$. Pour G_0 fixé de degré ν, soit H_0 (s'il existe) dans $\mathscr{H}$ tel que $|T^2G_0H_0 - R|_0 \leqslant q^\omega$. Tous les polynômes $H \in \mathscr{H}$ tels que $|T^2G_0H - R|_0 \leqslant q^\omega$ sont tels que $|H - H_0|_0 \leqslant q^{\omega - 2t - \nu}$

Soit (H_0) la boule dans $F_q[x]$ de centre H_0 et de rayon $q^{\omega - 2t - \nu}$. Alors

$$|S| \leqslant \sum_\nu \sum_{|G_0|_0 = q^\nu} |\psi(G_0)| \sum_{H \in (H_0)} 1$$

ce qui entraîne

$$|S| \leqslant \sum_{\nu} \sum_{|G_0|_0 = q^\nu} |\psi(G_0)| \cdot q^{\omega-2t-\nu+1} \leqslant \sum_{\nu} c_1 \gamma q^{\omega-2t+1}$$
$$\leqslant c_1 \gamma^2 q^{\omega+1} q^{-1,1t} \cdot q^{-1,08\varrho_0} \leqslant c_1 q^{\omega+1} \cdot q^{-1,1t} \cdot \Delta_0 .$$

Nous pouvons donc supposer maintenant que $t \leqslant 1,2\varrho_0$. Soit $G_0 \in \mathscr{G}$ de degré ν et (G_0) l'ensemble des $G \in \mathscr{G}$ tels que

$$|G - G_0|_0 \leqslant q^v \quad \text{où } v = \nu + \omega - \gamma \ (v+1 \geqslant 0{,}13\gamma \geqslant 0).$$

Les polynômes de $\mathscr{G}$ de degré ν sont partagés en $q^{\nu-v-1}$ ensembles (G_0). Soit $H_0 \in \mathscr{H}$ tel qu'il existe $G_1 \in (G_0)$ vérifiant

$$|T^2 G_1 H_0 - R|_0 \leqslant q^\omega .$$

L'ensemble des $H \in \mathscr{H}$ tels que $|T^2 GH - R|_0 \leqslant q^\omega$ pour $G \in (G_0)$ est l'ensemble des $H \in \mathscr{H}$ tels que

$$|G(H - H_0) + (G - G_1) H_0|_0 = |GH - G_1 H_0|_0 \leqslant q^{\omega-2t}$$

c'est-à-dire l'ensemble des $H \in \mathscr{H}$ tels que $|H - H_0|_0 \leqslant q^{\omega-2t-\nu}$. Nous noterons (H_0) cet ensemble.

Si $H = H_0 + X$, $\beta_0 = \beta_0(G) = LT^2 Ga$ et

$$S_G = \sum_{\substack{|X|_0 \leqslant q^{\omega-2t-\nu} \\ H_0 + X \in (H_0)}} e_0(\beta_0 X)$$

alors

$$S = \sum_{\nu} \sum_{\substack{(G_0) \\ |G_0|_0 = q^\nu}} \sum_{G \in (G_0)} \psi(G) e_0(LT^2 GH_0 a) S_G .$$

Soit Ω_G l'ensemble des $\beta \in \mathscr{F}_0$ tels que $|\beta - \beta_0|_0 \leqslant q^{\nu+2t-\omega-2}$. Si $\beta \in \Omega_G$, $(\beta - \beta_0) X \in \mathscr{P}^2$ pour tout X tel que $|X|_0 \leqslant q^{\omega-2t-\nu}$ donc

$$e_0(\beta X) = e_0(\beta_0 X)$$

Si nous posons

$$S(\beta) = \sum_{\substack{|X|_0 \leqslant q^{\omega-2t-\nu} \\ H_0 + X \in (H_0)}} e_0(\beta X)$$

nous aurons pour $\beta \in \Omega_G$, $S_G = S(\beta)$.

Si η_G est la fonction caractéristique de $\mathscr{H}_0(\Omega_G)$,

$$\int_{\Omega_G} |S_G|^2 d\beta = \int_{\Omega_G} |S(\beta)|^2 d\beta = \int_{\mathscr{F}} |S(\beta)|^2 \eta_G(\beta) d\beta$$

ce qui entraîne

$$|S_G|^2 = \frac{1}{\operatorname{mes} \Omega_G} \int_{\mathscr{F}} |S(\beta)|^2 \eta_G(\beta) d\beta .$$

Nous avons donc

$$\sum_{G\in(G_0)} |S_G|^2 \leqslant q^{\omega-2t-\nu+1} \int_{\mathscr{P}} |S(\beta)|^2 \sum_{G\in(G_0)} \eta_G(\beta)\, d\beta.$$

Il suffit de démontrer que

$$\text{(1)} \qquad \forall \beta \in \mathscr{P}, \qquad \sum_{G\in(G_0)} \eta_G(\beta) \leqslant 4\, q^{v+1+1,8t-2\varrho_0}.$$

En effet, si (1) est vérifié

$$\sum_{G\in(G_0)} |S_G|^2 \leqslant 4\, q^{2(\omega-2t-\nu+1)+v+1+1,8t-2\varrho_0}$$

et

$$\Big|\sum_{\substack{G,H\\|G|=q^\nu}} \psi(G)\, e_0(LT^2GH\,\alpha)\Big| \leqslant \Big(\sum_{|G|_0=q^\nu} |\psi(G)|^2\Big)\Big(\sum_{\substack{(G_0)\\|G_0|_0=q^\nu}} \sum_{G\in(G_0)} |S_G|^2\Big)$$
$$\leqslant 4\, C_2\gamma^3 q^\nu \cdot q^{\nu-v-1} \cdot q^{2(\omega-2t-\nu+1)+v+1+1,8t-2\varrho_0}$$
$$\leqslant 4\, C_2\gamma^3 q^{2(\omega+1)-2,2t-2\varrho_0}$$

ce qui entraîne $|S| \leqslant 2\sqrt{C_2}\,\gamma^{2,5} q^{\omega+1-1,1t-\varrho_0}$.

Pour démontrer (1), il suffit de démontrer qu'étant donné $\beta \in \mathscr{P}$ fixé, le nombre de polynômes $G' \in (G_0)$ pour lesquels $\Omega_{G'}$ contient un point β' tel que $\beta' - \beta \in F_q[x]$ est majoré par

$$\Lambda = 4\, q^{v+1-1,8t-2\varrho_0}.$$

Soient G et G' deux tels polynômes; alors

$$\text{(2)} \qquad \big|\mathscr{H}_0\big(\beta_0(G') - \beta_0(G)\big)\big|_0 \leqslant q^{\nu+2t-\omega-2}.$$

Il suffit donc de démontrer que pour G fixé cette équation admet au plus Λ solutions G' dans (G_0).

(2) s'écrit

$$\left|\mathscr{H}_0\left(\frac{LAT^2(G'-G)}{Q} + \frac{LT^2\,0(G'-G)}{Q\tau}\right)\right|_0 \leqslant q^{\nu+2t-\omega-2}$$

donc G' satisfait l'équation

$$\left|\mathscr{H}_0\left(\frac{LAT^2(G'-G)}{Q}\right)\right|_0 \leqslant q^a$$

où $a = \max(\nu+2t-\omega-2,\ \varrho_0+2t+v-\chi-y-1)$.

D'après le lemme (7), le nombre de solutions de cette équation est majoré par

$$\text{(3)} \qquad (q^{a+1-d+\chi}+1)(1+q^{v+1+d-\chi})$$

où d est défini par

$$(LT^2, Q) = D \quad \text{et} \quad |D|_0 = q^d.$$

Donc $d \leqslant \varrho_0 + 2t$.

L'expression (3) est majorée par $4q^{v+1+2t+\lambda}$ où $\lambda = \max(a+1-2t, \varrho_0-\chi, a+\chi-v-2t, -v-1-2t)$.

Il suffit donc de démontrer que $\lambda \leqslant -0,2t-2\varrho_0$:

$$a+1-2t \leqslant \max(\nu-\omega-1, \varrho_0+v-\chi-y) \leqslant -0,2t-2\varrho_0,$$

$$\varrho_0-\chi \leqslant -0,2t-2\varrho_0,$$

$$a+\chi-v-2t \leqslant \max(\nu-\omega-2+\chi-v, \varrho_0-1-y)$$

$$\leqslant \max(2\varrho_0+\chi-\gamma, \varrho_0-0,5\gamma) \leqslant -0,2t-2\varrho_0,$$

et

$$-v-1-2t \leqslant \varrho_0-t-0,24\gamma \leqslant -0,2t-2\varrho_0.$$

Lemme 11. *Les hypothèses étant celles du lemme* 10, *on suppose de plus que* $y \geqslant \max(\chi, \gamma-\chi)$. *Soit* $\mathscr{D}$ *une partie de* $\mathscr{M}$. *Posons*

$$S = \sum_D \sum_M e_0(LDMa)$$

a sommation étant faite sur les couples (D, M) *de* $\mathscr{D}\times\mathscr{M}$ *tels que*

$$|DM-R|_0 \leqslant q^\omega, \quad |M|_0 = q^\nu \quad \textit{avec } 0,2\gamma \leqslant \nu \leqslant \gamma-3\varrho_0.$$

Alors

$$|S| \leqslant 2\gamma q^{\omega+1}\cdot q^{-\varrho_0}.$$

Démonstration. De même que dans le lemme 10, nous partageons les polynômes de $\mathscr{M}$ de degré ν en $q^{\nu-v-1}$ sous-ensembles (M_0):

$$|M-M_0|_0 \leqslant q^v \quad \text{où } v = \nu+\omega-\gamma$$

auxquels correspondront les sous-ensembles (D_0) de $\mathscr{D}$:

$$|D-D_0|_0 \leqslant q^{\omega-\nu}.$$

Pour $D\in(D_0)$ posons $D = D_0+Y$. Soient

$$\beta_0 = \beta_0(M) = LMa, \quad S_M = \sum_{D_0+Y\in(D_0)} e_0(\beta_0 Y),$$

$$S_{(M_0)} = \sum_{M\in(M_0)} e_0(LD_0Ma)S_M.$$

Alors

$$S = \sum_\nu \sum_{\substack{(M_0)\\ |M_0|_0=q^\nu}} S_{(M_0)}.$$

Soit Ω_M l'ensemble des β de $\mathscr{F}_0$ tels que

$$|\beta-\beta_0|_0 \leqslant q^{\nu-\omega-2}.$$

Alors, si $\beta \in \Lambda_M$ et $|Y|_0 \leqslant q^{\omega-\nu}$, $(\beta-\beta_0)\,Y \in \mathscr{P}^2$ et

$$S(\beta) = \sum_{\substack{|Y|_0 \leqslant q^{\omega-\nu} \\ D_0+Y \in (D_0)}} e_0(\beta Y) = S_M.$$

Donc

$$\int_{\Lambda_M} |S_M|^2 d\beta = \int_{\Lambda_M} |S(\beta)|^2 d\beta$$

et si η_M est la fonction caractéristique de $\mathscr{H}_0(\Omega_M)$

$$|S_M|^2 \leqslant \frac{1}{\operatorname{mes} \Lambda_M} \int_{\mathscr{P}} |S(\beta)|^2 \eta_M(\beta)\, d\beta.$$

De même que dans le lemme 10, nous avons

$$\sum_{M \in (M_0)} |S_M|^2 \leqslant q^{2(\omega-\nu+1)} \cdot \Lambda$$

où Λ est le nombre maximum de solutions en M' de l'équation

$$M' \in (M_0) \quad \text{et} \quad \left|\mathscr{H}_0\big(L(M'-M)\,a\big)\right|_0 \leqslant q^{\nu-\omega-2}, \quad \text{pour } M \text{ dans } (M_0).$$

Ceci entraîne que

$$\left|\mathscr{H}_0\left(\frac{LA\,(M'-M)}{Q}\right)\right|_0 \leqslant q^a$$

où $a = \max(\nu-\omega-2,\ \varrho_0+v-\chi-y-1)$.

En utilisant la même démonstration que dans le lemme 10, on montre que l'on a $\Lambda \leqslant 4q^{v+1-2\varrho_0}$ et alors

$$\sum_{M \in (M_0)} |S_M|^2 \leqslant 4\, q^{2(\omega-\nu+1)+v+1-2\varrho_0}.$$

Mais nous avons

$$|S_{(M_0)}|^2 \leqslant q^{v+1}\Big(\sum_{M \in (M_0)} |S_M|^2\Big)$$

donc

$$|S_{(M_0)}| \leqslant 2\, q^{\omega-\nu+1+v+1-\varrho_0},$$

$$|S| \leqslant \sum_{\nu} 2\, q^{\omega+1-\varrho_0},$$

et

$$|S| \leqslant 2\gamma\, q^{\omega+1-\varrho_0}.$$

5. Majoration du nombre de solutions de quelques équations diophantiennes sur $F_q[x]$. Soient k un entier tel que $2 \leqslant k \leqslant p-1$, $a_0, a_1, \ldots, a_k \in \mathscr{F}_0$ et

$$f(X) = a_k X^k + \ldots + a_1 X + a_0, \qquad X \in F_q[x].$$

Soient v un entier de N^*, R un polynôme de $F_q[x]$

$$S(v) = \sum_{|X-R|_0 \leqslant qv} e_0\big(f(X)\big)$$

et

$$J(v, l) = \int_{\mathscr{P}} \ldots \int_{\mathscr{P}} |S(v)|^{2l} d\alpha_1 \ldots d\alpha_k, \qquad l \in N^*.$$

Nous avons

$$|S(v)| \leqslant q^{v+1}, \qquad J(v, l) \leqslant q^{2l(v+1)}$$

et

$$|S(v)|^{2l} = \sum_{\substack{X_1, \ldots, X_l \\ Y_1, \ldots, Y_l}} e_0\big(\alpha_k(X_1^k + \quad + X_l^k - Y_1^k - \ldots - Y_l^k) + \ldots\big).$$

$J(v, l)$ est donc égal au nombre de solutions du système

$$X_1^h + \ldots + X_l^h = Y_1^h + \ldots + Y_l^h, \qquad h = 1, \ldots, k,$$

$$|X_i - R|_0 \leqslant q^v \quad \text{et} \quad |Y_i - R|_0 \leqslant q^v.$$

$J(v, l)$ est indépendant de R, car en posant $X_i' = X_i - R$ et $Y_i' = Y_i - R$, nous obtenons le système

$$\sum_{j=1}^{l} (X_j' + R)^h = \sum_{j=1}^{l} (Y_j' + R)^h, \qquad h = 1, \ldots, k,$$

qui est équivalent au système

$$\sum_{j=1}^{l} X_j'^h = \sum_{j=1}^{l} Y_j'^h, \qquad h = 1, \ldots, k.$$

Il est clair que $J(v, l)$ est une fonction non décroissante de v. La méthode utilisée pour majorer $J(v, l)$ généralise celle de L. K. Hua ([10] et [13], p. 102–109).

LEMME 12. *Soient $X_1, \ldots, X_k, Y_1, \ldots, Y_k$ des polynômes de $F_q[x]$. Posons*

$$s_h = \sum_{j=1}^{k} X_j^h, \qquad s_h' = \sum_{j=1}^{k} Y_j^h$$

et soient σ_h et σ_h' les h-ièmes fonctions symétriques élémentaires des X_j et des Y_j respectivement. Si

$$|X_j|_0 \leqslant q^v \quad \textit{et} \quad |Y_j|_0 \leqslant q^v, \qquad j = 1, \ldots, k,$$

et

$$|s_h - s'_h|_0 \leqslant q^{v(h-1)}, \qquad h = 1, \ldots, k,$$

alors

$$|\sigma_h - \sigma'_h|_0 \leqslant q^{v(h-1)}, \qquad h = 1, \ldots, k.$$

Démonstration. $\sigma_1 = s_1$, $\sigma'_1 = s'_1$ donc on a bien $|\sigma_1 - \sigma'_1|_0 = |s_1 - s'_1|_0 \leqslant 1$. Supposons

$$|\sigma_j - \sigma'_j|_0 \leqslant q^{v(j-1)} \quad \text{pour } 1 \leqslant j \leqslant h-1.$$

D'après les formules de Newton, nous avons

$$s_h - \sigma_1 s_{h-1} + \sigma_2 s_{h-2} - \ldots + (-1)^h h \sigma_h = 0.$$

Puisque $1 \leqslant h \leqslant k \leqslant p-1$, $h \cdot 1 \neq 0$ dans $\mathscr{F}_0$; donc

$$|\sigma_h - \sigma'_h|_0 \leqslant \max(|s_h - s'_h|_0, |\sigma_1 s_{h-1} - \sigma'_1 s'_{h-1}|_0, \ldots)$$

et nous avons

$$\sigma_j s_{h-j} - \sigma'_j s'_{h-j} = (\sigma_j - \sigma'_j) s_{h-j} + \sigma'_j (s_{h-j} - s'_{h-j}).$$

Nous avons d'autre part

$$|\sigma_j|_0 \leqslant q^{vj} \quad \text{et} \quad |s_j|_0 \leqslant q^{vj}$$

donc

$$|\sigma_j s_{h-j} - \sigma'_j s'_{h-j}|_0 \leqslant q^{v(h-1)}$$

et

$$|\sigma_h - \sigma'_h|_0 \leqslant q^{v(h-1)}.$$

Lemme 13. *Soient g un entier tel que $0 < g < v$, $R_1, \ldots, R_k$, k polynômes de $F_q[x]$ tels que*

$$|R_i|_0 \leqslant q^v \quad \text{et} \quad |R_i - R_j|_0 \geqslant q^{v-g} \quad \text{si } i \neq j.$$

Soit, pour $1 \leqslant j \leqslant k$, un polynôme X_j tel que

$$|X_j - R_j|_0 \leqslant q^{v-g-1}.$$

Alors le nombre de k-uples $(X_1, \ldots, X_k)$ pour lesquels les valeurs de s_h $(h = 1, \ldots, k)$, différent en valeur absolue d'au plus $q^{v(h-1)}$ est majoré par

$$q^{gk(k-1)/2+k}.$$

Démonstration. Si $|X|_0 \leqslant q^v$

$$|(X - X_1) \ldots (X - X_k) - (X - Y_1) \ldots (X - Y_k)|_0$$
$$\leqslant \max_{1 \leqslant h \leqslant k} (|\sigma_h - \sigma'_h|_0 |X|_0^{k-h}) \leqslant q^{(k-1)v}.$$

Si les Y_i satisfont les mêmes conditions que les X_i, alors

$$|X_k - Y_j|_0 \geqslant q^{v-g}, \quad j = 1, 2, \ldots, k-1.$$

En posant $X = Y_k$, il vient

$$q^{(k-1)(v-g)}|X_k - Y_k|_0 \leqslant q^{(k-1)v}$$

soit

$$|X_k - Y_k|_0 \leqslant q^{(k-1)g}.$$

Donc le nombre de polynômes X_k qui satisfont les conditions du lemme, est majoré par $q^{(k-1)g+1}$. Pour une valeur donnée de X_k, les polynômes $X_1, \ldots, X_{k-1}$ satisfont des conditions analogues avec $k-1$ au lieu de k et donc le nombre de valeurs de X_{k-1} est au plus $q^{(k-2)g+1}$: Le nombre total des k-uples $(X_1, \ldots, X_k)$ n'excède donc pas

$$q^{(k-1+k-2+\ldots+1)g+k} = q^{k(k-1)g/2+k}.$$

Lemme 14. *Dans les mêmes conditions que celles du lemme* 13, *le nombre de k-uples $(X_1, \ldots, X_k)$ pour lesquels les s_h $(h = 1, \ldots, k)$ sont dans des boules de rayon $q^{vh(1-1/k)}$, est majoré par*

$$q^{(k-1)v/2+k(k-1)g/2+k}.$$

Démonstration. Nous partageons la h-ième boule en au plus $q^{v(1-h/k)}$ boules de rayon $q^{v(h-1)}$. Nous obtenons alors au plus

$$\prod_{h=1}^{k} q^{v(1-h/k)} = q^{(k-1)v/2}$$

ensembles de k boules satisfaisant les conditions du lemme 13. Pour chacun de ces ensembles de boules, nous avons au plus $q^{k(k-1)/2-g+k}$ solutions, ce qui donne le résultat.

Lemme 15. *Soit l un entier supérieur à k. Posons*

$$I = \int_{\mathscr{P}} \ldots \int_{\mathscr{P}} |\mathscr{Z}_{m,R_1} \ldots \mathscr{Z}_{m,R_k}|^2 \left|S\left(v(1-1/k)\right)\right|^{2(l-k)} d\alpha_1 \ldots d\alpha_k$$

où

$$\mathscr{Z}_{m,R_j} = \sum_{|X-R_j|_0 \leqslant q^{v-m-1}} e_0\left(f(X)\right)$$

et où les R_j sont des polynômes satisfaisant les conditions du lemme 13 *avec $g = m$. Alors*

$$I \leqslant q^{(3k-1)v/2+k(k-1)m/2-mk+k} \cdot J\left(v(1-1/k), l-k\right).$$

Démonstration. Nous avons

$$I = \sum_{N_1,\ldots,N_k} \psi(N_1, \ldots, N_k) \int_{\mathscr{P}} \ldots \int_{\mathscr{P}} e_0(N_k\alpha_k + \quad + N_1\alpha_1) \times$$
$$\times \left|S\left(v(1-1/k)\right)\right|^{2(l-k)} d\alpha_1 \ldots d\alpha_k,$$

$$I \leqslant \sum_{N_1,\ldots,N_k} \psi(N_1, \ldots, N_k) \int_{\mathscr{P}} \ldots \int_{\mathscr{P}} \left|S\left(v(1-1/k)\right)\right|^{2(l-k)} d\alpha_1 \ldots d\alpha_k,$$

où $\psi(N_1, \ldots, N_k)$ est le nombre de solutions de l'équation

$$X_1^h + \quad + X_k^h - Y_1^h - \ldots - Y_k^h = N_h, \quad h = 1, \ldots, k,$$

pour X_i et Y_i tels que

$$|X_i - R_i|_0 \leqslant q^{v-m-1} \quad \text{et} \quad |Y_i - R_i|_0 \leqslant q^{v-m-1}, \quad i = 1, \ldots, k,$$

et où

$$N_h = X_1'^h + \ldots + X_{l-k}'^h - Y_1'^h - \ldots - Y_{l-k}'^h, \quad h = 1, \ldots, k,$$

les X_i' et les Y_i' étant dans une boule de centre R et de rayon $q^{v(1-1/k)}$.

Nous pouvons remplacer les X_i' par $X_i' - R$ et les X_i par $X_i - R$ et de même pour les Y. Nous obtenons de nouveaux polynômes R_i qui satisfont encore les conditions du lemme 13. Alors N_h se trouve dans la boule de centre 0 et de rayon $q^{vh(1-1/k)}$. D'après le lemme 14, pour un k-uple $(Y_1, \ldots, Y_k)$ donné, le nombre de k-uples $(X_1, \ldots, X_k)$ possibles est majoré par

$$q^{(k-1)v/2+k(k-1)m/2+k}.$$

De plus, $(Y_1, \ldots, Y_k)$ prend au plus $q^{(v-m)k}$ valeurs. Donc

$$\sum_{N_1, \ldots, N_k} \psi(N_1, \ldots, N_k) \leqslant q^{(k-1)v/2+k(k-1)m/2+k+(v-m)k}$$
$$\leqslant q^{(3k-1)v/2+k(k-1)m/2-mk+k}.$$

Lemme 16. *Le résultat du lemme* 15 *est encore vrai, que les R_i vérifient les conditions du lemme* 13 *ou non, si m prend la valeur*

$$\mu = \left[\frac{v}{k}\right] + 2.$$

Démonstration. Puisque

$$|\mathscr{Z}_{\mu, R_i}| \leqslant q^{v-\mu+1},$$
$$|\mathscr{Z}_{\mu, R_1} \ldots \mathscr{Z}_{\mu, R_k}|^2 \leqslant q^{(v-\mu+1)2k}.$$

Il suffit alors de démontrer que

$$q^{(v-\mu+1)2k} \leqslant q^{(3k-1)v/2+k(k-1)\mu/2-\mu k+k}$$

soit

$$\tfrac{1}{2}(k+1)v + k \leqslant \tfrac{1}{2}k(k-1)\mu + \mu k$$

et

$$\frac{v}{k} + \frac{2}{k+1} \leqslant \mu,$$

ce qui est vérifié.

Lemme 17. *Soit $l > k$. L'ensemble des polynômes $(T_1, \ldots, T_l)$ est dit bien espacé s'il contient au moins k polynômes distincts.*

Le nombre de l-uples $(T_1, \ldots, T_l)$ *tels que* $|T_i|_0 \leqslant q^g$ *qui ne sont pas bien espacés, est au plus*

$$l!\,q^{l-1+(g+1)(k-1)}.$$

Démonstration. Si $(T_1, \ldots, T_l)$ n'est pas bien espacé, les polynômes $T_1, \ldots, T_l$ prennent h valeurs distinctes $T'_1, \ldots, T'_h$. La valeur T'_i est prise l_i fois. Nous avons $l_1+l_2+\quad+l_h = l$. Il y a donc $\binom{l-1}{h-1}$ l-uples $(T_1, \ldots, T_l)$ qui ne sont pas bien espacés et dont les polynômes prennent les valeurs $T'_1, \ldots, T'_h$. Il y a $\binom{q^{g+1}}{h}$ façons de choisir $T'_1, \ldots, T'_h$ et il y a au plus

$$l!\sum_{h=1}^{k-1}\binom{q^{g+1}}{h}\binom{l-1}{h-1},$$

l-uples qui ne sont pas bien espacés. Ce nombre est majoré par

$$l!\sum_{h=1}^{k-1}\binom{l-1}{h-1}q^{(k-1)(g+1)} \leqslant l!\,q^{l-1}q^{(k-1)(g+1)}.$$

Lemme 18. *Soient* $\mu = [v/k]+2$ *et* $l \in \boldsymbol{N}$ *tel que* $l \geqslant \frac{1}{4}k^2+\frac{5}{4}k$, *alors*

$$J(v, l) \leqslant (l!)^2\cdot\mu\cdot q^{6l-k}q^{v(2(l-k)/k+3k/2-1/2)}\,J\left(v\left(1-\frac{1}{k}\right), l-k\right).$$

Démonstration. Soit a un entier tel que $1 \leqslant a \leqslant \mu-1$; alors

$$q^{a+1} \leqslant q^{v/k+2}.$$

Soit

$$S(v) = \sum_{R\in E(a,v)}\ \sum_{|X-R|_0\leqslant q^{v-a-1}} e_0\big(f(X)\big) = \sum_{R\in E(a,v)} \mathscr{Z}_{a,R}$$

où $E(a, v) = \{R \in F_q[x]$ tels que $R = x^{v-a}T$, avec $|T|_0 \leqslant q^a\}$. Nous avons

$$\big(S(v)\big)^l = \sum_{(R_1,\ldots,R_l)\in E^l(a,v)} \mathscr{Z}_{a,R_1}\cdots\mathscr{Z}_{a,R_l}.$$

Cette somme a $q^{(a+1)l}$ termes. Nous notons $\mathscr{Z}'_a$ les produits $\mathscr{Z}_{a,R_1}\cdots\mathscr{Z}_{a,R_l}$ tels que les polynômes $T_1, \ldots, T_l$ soient bien espacés. Il y a $\mathscr{N}_a \leqslant q^{(a+1)l}$ produits $\mathscr{Z}'_a$. Dans les autres produits, chaque facteur $\mathscr{Z}_{a,R_i}$ peut s'écrire $\sum_{R'\in E(a+1,v)} \mathscr{Z}_{a+1,R'}$. Nous obtenons donc des produits du type $\mathscr{Z}_{a+1,R_1}\cdots$ $\cdots\mathscr{Z}_{a+1,R_l}$ où $R_i \in E(a+1, v)$ pour $1 \leqslant i \leqslant l$. Nous notons $\mathscr{Z}'_{a+1}$ les produits ci-dessus tels que les polynômes $T_1, \ldots, T_l$ soient bien espacés. Il y a $\mathscr{N}_{a+1}$ produits $\mathscr{Z}'_{a+1}$. En réitérant ce procédé, on obtient des produits de la forme $\mathscr{Z}_{\mu,R_1}\cdots\mathscr{Z}_{\mu,R_l}$ où $R_i \in E(\mu, v)$ pour $1 \leqslant i \leqslant l$. Nous notons

$\mathscr{Z}'_\mu$ tous ces produits et soit $\mathscr{N}_\mu$ leur nombre. Nous avons alors

$$(S(v))^l = \sum_{m=a}^{\mu}\Big(\sum \mathscr{Z}'_m\Big)$$

et

$$|S(v)|^{2l} \leqslant \mu \sum_{m=a}^{\mu}\Big|\sum \mathscr{Z}'_m\Big|^2 \leqslant \mu \sum_{m=a}^{\mu}\mathscr{N}_m \sum |\mathscr{Z}'_m|^2.$$

D'après le lemme 17

$$\mathscr{N}_m \leqslant l!\, q^{2l-1+(k-1)m} \quad \text{dès que } m > a.$$

Considérons la somme $\sum|\mathscr{Z}'_m|^2$. Le terme général peut s'écrire

$$\mathscr{Z}'_m = \mathscr{Z}_{m,R_1}\ldots\mathscr{Z}_{m,R_k}\cdot\mathscr{Z}_{m,R_{k+1}}\ldots\mathscr{Z}_{m,R_l}$$

où les polynômes $R_1,\ldots,R_k$ satisfont les conditions du lemme 13 avec $g = m$. Puisque la moyenne arithmétique majore la moyenne géométrique

$$|\mathscr{Z}_{m,R_{k+1}}\ldots\mathscr{Z}_{m,R_l}|^2 \leqslant \frac{1}{l-k}\sum_{j=k+1}^{l}|\mathscr{Z}_{m,R_j}|^{2(l-k)}.$$

Partageons la boule de rayon q^{v-m-1} en boules de rayon $q^{v(1-1/k)-1}$. Le nombre de ces boules est au plus $q^{v-m-1-v(1-1/k)+2} = q^{v/k-m+1}$. Chaque somme obtenue est de la forme $S\big(v(1-1/k)-1\big)$. D'après l'inégalité de Hölder

$$|\mathscr{Z}_{m,R_j}|^{2(l-k)} \leqslant q^{(v/k-m+1)(2(l-k)-1)}\sum\big|S\big(v(1-1/k)-1\big)\big|^{2(l-k)},$$

et

$$\sum|\mathscr{Z}'_m|^2$$
$$\leqslant \frac{1}{l-k}q^{(v/k-m+1)(2(l-k)-1)}\sum|\mathscr{Z}_{m,R_1}\ldots\mathscr{Z}_{m,R_k}|^2\sum_{j=k+1}^{l}\big|S\big(v(1-1/k)\big)-1\big|^{2(l-k)}.$$

D'après les lemmes 15 et 16:

$$\int_{\mathscr{P}}\int_{\mathscr{P}}\sum|\mathscr{Z}'_m|^2\,da_k\ldots da_1 \leqslant q^{(v/k-m+1)(2(l-k)-1)}\times$$
$$\times\mathscr{N}_m\cdot q^{(v/k-m+1)}\cdot q^{v(3k-1)/2+k(k-1)m/2-mk+k}J\big(v(1-1/k),\,l-k\big)$$
$$= q^{m(k^2/2+k/2-2l)+2l-k}\times\mathscr{N}_m\times q^{v(2(l-k)/k+3k/2-1/2)}J\big(v(1-1/k),\,l-k\big).$$

Donc

$$J(v,l) \leqslant \sum_{m=a}^{\mu} q^{(k^2/2+k/2-2l)m}\cdot\mathscr{N}_m^2\cdot q^{2l-k+v(2(l-k)/k+3k/2-1/2)}J\big(v(1-1/k)-1,\,l-k\big).$$

Nous avons

$$\sum_{m=a}^{\mu} q^{(k^2/2+k/2-2l)m} \mathcal{N}_m^2$$

$$\leqslant q^{(k^2/2+k/2-2l)a+2(a+1)l} + \sum_{m=a+1}^{\mu} (l!)^2 q^{(k^2/2+k/2-2l)m+4l-2} q^{(2k-2)m}$$

$$= q^{(k^2+k)a/2+2l} + (l!)^2 q^{4l-2} \sum_{m=a+1}^{\mu} q^{(k^2/2+5/2k-2l-2)m}$$

$$\leqslant q^{2(a+1)l} + (l!)^2 q^{4l-2} \leqslant (l!)^2 q^{4l} \quad \text{si nous posons } a = 1.$$

Donc

$$J(v, l) \leqslant (l!)^2 \mu q^{6l-k} q^{v(2(l-k)/k+3k/2-1/2)} J\big(v(1-1/k)-1, l-k\big)$$

qui est l'inégalité du lemme.

Lemme 19. *Si r est un entier positif ou nul et l un entier tel que $l \geqslant \frac{1}{4}k^2 + \frac{1}{4}k + kr$, alors pour v entier $v \geqslant 4$*

$$J(v, l) \leqslant K^r v^r q^{2l+v(2l-k(k+1)/2+\delta_r)}$$

où $K = (l!)^2 q^{6l-3k}$ et $\sigma_r = \frac{1}{2}k(k+1)(1-1/k)^r$.

Démonstration. Si $r = 0$, puisque $\delta_0 = \frac{1}{2}k(k+1)$ et que $J(v, l) \leqslant q^{2l(v+1)}$, le résultat est vrai. Supposons que le résultat soit vrai jusqu'à $r-1$, alors en utilisant le lemme 18, nous obtenons, sachant que

$$v \geqslant 4 \quad \text{et} \quad k \geqslant 2 \Rightarrow \mu \leqslant \tfrac{1}{2}v + 2 \leqslant v,$$

$$J(v, l) \leqslant (l!)^2 q^{6l-k} v q^{v(2(l-k)/k+3k/2-1/2)} K^{r-1} \big(v(1-1/k)-1\big)^{r-1} \times$$
$$\times q^{2(l-k)} q^{(v(1-1/k)-1)(2(l-k)-k(k+1)/2+\delta_{r-1})}.$$

Le coefficient de v est alors exactement

$$2l - \tfrac{1}{2}k(k+1) + \delta_r$$

et nous obtenons

$$J(v, l) \leqslant K^r v^r q^{2l} q^{v(2l-k(k+1)/2+\delta_r)} q^{2k-2l+k(k+1)/2}.$$

Puisque $2k - 2l + \frac{1}{2}k(k+1) \leqslant 2k(1-r) \leqslant 0$ pour $r \geqslant 1$, nous obtenons la majoration du lemme.

Lemme 20. *Pour tout $n \in \mathbf{N}^*$ nous avons*

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

Démonstration. Soient m un réel strictement positif et $(p_i)_{i \geqslant 1}$ une suite croissante de nombres premiers distincts.

Si

$$H(m, p_1, \ldots, p_s) = \sum_{l=0}^{s} (-1)^l \sum_{\substack{(i_1, \ldots i_l) \\ 1 \leqslant i_j \leqslant s \\ i_j \neq i_k \text{ si } j \neq k}} q^{m/p_{i_1} \ldots p_{i_l}}$$

et si $n = p_1^{a_1} \ldots p_t^{a_t}$ alors $n\pi(n) = H(n, p_1, \ldots, p_t)$ et $t \leqslant \dfrac{\log n}{\log 2}$. Comme

$$H(m, p_1, \ldots, p_{s+1}) = H(m, p_1, \ldots, p_s) + \sum_{l=1}^{s+1} (-1)^l \sum_{\substack{(i_1, \ldots, i_l) \\ 1 \leqslant i_j \leqslant s \\ i_j \neq i_k \text{ si } j \neq k}} q^{m/p_{i_1} \ldots p_{i_{l-1}} p_{s+1}}$$

nous avons

$$(1) \qquad H(m, p_1, \ldots, p_{s+1}) = H(m, p_1, \ldots, p_s) - H\left(\frac{m}{p_{s+1}}, p_1, \ldots, p_s\right).$$

Nous allons démontrer que si $m \geqslant 12$ et $s \leqslant \dfrac{\log m}{\log 2}$ alors

$$(2) \qquad 0 \leqslant q^m - q^{m/2} - \quad - q^{m/(s+1)},$$

$$(3) \qquad q^m - q^{m/2} - \ldots - q^{m/(s+1)} \leqslant H(m, p_1, \ldots, p_s) \leqslant q^m.$$

(2) est équivalente à (4) : $1 + q^{m/3 - m/2} + \ldots + q^{m/(s+1) - m/2} \leqslant q^{m/2}$,

$$1 + q^{m/3 - m/2} + \ldots + q^{m/(s+1) - m/2} \leqslant 1 + 2^{-2} + s \cdot 2^{-m/4} \leqslant 1 + \tfrac{1}{4} + 2^{-m/4} \frac{\log m}{\log 2}.$$

La fonction

$$f(x) = \frac{\log x}{\log 2} \cdot 2^{-x/4}$$

est décroissante pour $x \geqslant 12$ donc

$$1 + q^{m/3 - m/2} + \ldots + q^{m/s+1 - m/2} \leqslant 1 + \frac{1}{4} + \frac{1}{8} \frac{\log 12}{\log 2} \leqslant 2 \leqslant q^{m/2}$$

ce qui démontre (4).

Pour démontrer (3), il suffit de raisonner par récurrence sur s en utilisant (1) et (2).

(4) entraine que

$$q^m - 2q^{m/2} \leqslant H(m, p_1, \ldots, p_s) \leqslant q^m \quad \text{pour } s \leqslant \frac{\log m}{\log 2}.$$

Il suffit donc, pour démontrer le lemme, de vérifier la relation directement pour $1 \leqslant n \leqslant 11$.

LEMME 21. *Soit $Q \in \mathcal{M}$ de degré $\chi \geqslant 2$. Le nombre r de polynômes irréductibles qui divisent Q vérifie l'inégalité*

$$r \leqslant \frac{3\chi \log q}{\log \chi}.$$

Démonstration.

(a) Si $2 \leqslant \chi \leqslant q^3$ alors $r \leqslant \chi \leqslant \dfrac{3\chi \log q}{\log \chi}$;

(b) Si $q^3 \leqslant \chi \leqslant q^6$, $r \leqslant \pi(1) + \pi(2) + \dfrac{\chi - (\pi(1) + 2\pi(2))}{3}$ soit $r \leqslant q^2/6 - q/2 + \chi/3$.

Comme $\dfrac{\chi}{2} \leqslant \dfrac{3\chi \log q}{\log \chi}$ il suffit de démontrer que

$$\frac{q^2}{6} - \frac{q}{2} + \frac{\chi}{3} \leqslant \frac{\chi}{2}$$

ce qui est équivalent à $q^2 - 3q \leqslant \chi$, ce qui est vérifié.

(c) Supposons maintenant $\chi > q^6$.

Il existe un entier et un seul $k = k(\chi)$ tel que

$$\pi(1) + 2\pi(2) + \ldots + (k-1)\pi(k-1) < \chi \leqslant \pi(1) + \ldots + k\pi(k).$$

Alors $r \leqslant \pi(1) + \quad + \pi(k)$.

Puisque, d'après le lemme 20, $n\pi(n) \geqslant q^n - 2q^{n/2}$, k est majoré par tout réel λ tel que

$$\chi \leqslant q^\lambda - 2q^{\lambda/2} + q^{\lambda-1} - 2q^{(\lambda-1)/2}.$$

Nous allons montrer que $\lambda = \dfrac{\log \chi}{\log q}$ convient. En effet, l'inégalité ci-dessus devient

$$\chi \leqslant \chi - 2\chi^{1/2} + \frac{\chi}{q} - 2\frac{\chi^{1/2}}{\sqrt{q}} \Leftrightarrow 4(q^2 + 2q\sqrt{q} + q) \leqslant \chi$$

ce qui est vérifié puisque $4(q^2 + 2q\sqrt{q} + q) \leqslant 16q^2 \leqslant q^6 < \chi$. Puisque

$$\frac{q^k}{k} \leqslant \frac{q^\lambda}{\lambda} = \frac{\chi \log q}{\log \chi}$$

il suffit de démontrer que

$$\pi(1) + \quad + \pi(k) \leqslant \frac{3q^k}{k} \quad \text{pour } k \geqslant 1. \tag{1}$$

Supposons que (1) soit vérifiée pour $k \geqslant 3$. Alors

$$\pi(1) + \ldots + \pi(k+1) \leqslant \frac{3q^k}{k} + \frac{q^{k+1}}{k+1} \leqslant \frac{3q^{k+1}}{k+1}.$$

Il suffit donc de vérifier (1) pour $k = 1, 2, 3$.

LEMME 22. *Soient Q un polynôme de degré $\chi \geqslant 2$, A un polynôme premier à Q, $C \in F_q[x]$, $L \in F_q[x]^*$ et u un entier $1 \leqslant u < p$.*

Le nombre de solutions de l'équation

$$LAG^u \equiv C \bmod Q \quad \textit{avec } 0 \leqslant |G|_0 < |Q|_0, (G, Q) = 1$$

est majoré par:

$$|L|_0 q^{\frac{3\chi \log u}{\log \chi}}$$

Démonstration.

(a) Examinons l'équation (1), $G^u \equiv C \bmod Q$.

Nous avons $Q = Q_1 \ldots Q_r$ où $Q_i = P_i^{a_i}$ et où les P_i sont premiers entre eux.

(1) s'écrit $G^u \equiv C \bmod Q_i \ \forall i \ 1 \leqslant i \leqslant r$.

Si G_i est une solution de $G^u \equiv C \bmod Q$, on a $G \equiv G_i \bmod Q_i$. Nous allons montrer qu'étant donné $(G_1, \ldots, G_r)$ tel que, pour tout i, G_i soit solution de $G^u \equiv C \bmod Q_i$, il existe un seul polynôme G tel que $0 \leqslant |G|_0 < |Q|_0$ satisfaisant (1).

Si $Q = Q_i R_i$, il existe $T_1, \ldots, T_r$ tels que

$$T_i R_i \equiv 1 \bmod Q_i \quad \text{pour } 1 \leqslant i \leqslant r$$

et si $G_0 = \sum_{i=1}^{r} G_i T_i R_i$ on a bien $G_0 \equiv G_i \bmod Q_i$ pour tout i $1 \leqslant i \leqslant r$.

Si $G' \equiv G_i \bmod Q_i$ pour $1 \leqslant i \leqslant r$ alors $G_0 \equiv G' \bmod Q$, ce qui démontre le résultat annoncé.

Il suffit donc de majorer le nombre de solutions d'une équation

$$(2) \qquad G^u \equiv C \bmod P^a \quad 0 \leqslant |G|_0 < |P^a|_0, \quad (P, G) = 1$$

où P désigne un polynôme irréductible.

Si $a = 1$, il y a au plus u solutions au plus.

Supposons que pour $a - 1 \geqslant 1$ il y ait u solutions au plus.

Si G est une solution de (2), $G^u \equiv C \bmod P^{a-1}$ et $G = G_0 + HP^{a-1}$ où $0 \leqslant |H|_0 < |P|_0$ et $G_0^u \equiv C \bmod P^{a-1}$ avec $0 \leqslant |G_0|_0 < |P^{a-1}|_0$, $(G_0, P) = 1$.

Nous avons donc $G^u \equiv C + K_0 P^{a-1} \bmod P^a$ et $G^u \equiv G_0^u + uG_0^{u-1} H P^{a-1} \bmod P^a$.

Nous obtenons alors l'équation

$$K_0 + uG_0^{u-1} H \equiv 0 \bmod P, \quad 0 \leqslant |H|_0 < |P|_0.$$

uG_0^{u-1} est inversible modulo P donc l'équation ci-dessus a une seule solution en H.

Le nombre de solutions de (2) est donc majoré par u, ce qui entraîne que le nombre de solutions de (1) est majoré par u^r, donc par

$$u^{\frac{3\chi\log q}{\log\chi}} = q^{\frac{3\chi\log u}{\log\chi}}$$

(b) Examinons maintenant l'équation

$$ALG^u \equiv C \bmod Q, \qquad 0 \leqslant |G| < |Q|.$$

Nous posons $Q = Q_1 D$, $L = L_1 D$ où $D = (Q, L)$.

L'équation n'est possible que si D divise C. Nous avons alors

$$AL_1G^u \equiv C_1 \bmod Q_1, \qquad 0 \leqslant |G|_0 < |Q|_0.$$

Il existe V tel que $(V, Q_1) = 1$ et $AVL_1 = 1 \bmod Q_1$. L'équation devient alors

$$G^u \equiv C_1 V \bmod Q_1 \qquad \text{avec } 0 \leqslant |G|_0 < |Q|_0$$

qui a au plus $\dfrac{|Q|_0}{|Q_1|_0} u^r$ solutions.

Le nombre de solutions de l'équation proposée est donc majoré par $|L|_0 q^{\frac{3\chi\log u}{\log\chi}}$

6. Trois lemmes de préparation à la démonstration du théorème 2.

LEMME 23. *Soient: k un entier tel que $2 \leqslant k < p$; s un entier tel que $1 \leqslant s \leqslant k$; γ un entier tel que $\log\gamma \geqslant k^{100}$; y un entier tel que $[\frac{1}{2}s\gamma + \frac{1}{4}\gamma] \leqslant y < s\gamma$; χ un entier tel que $\log^3\gamma \leqslant \chi \leqslant \frac{1}{2}s\gamma + \frac{1}{4}\gamma$; ϱ_0 le réel égal à*

$$\gamma/\big(20k^2(2+\log k)\big) \quad \textit{si } \tfrac{1}{4}\gamma \leqslant \chi \leqslant \tfrac{1}{2}s\gamma + \tfrac{1}{4}\gamma,$$
$$\chi/\Big(5k^2\big(2+\log(k\sqrt{\gamma/\chi})\big)\Big) \quad \textit{si } \chi < \tfrac{1}{4}\gamma;$$

$\Delta_0 = \gamma^{2,75} q^{-\varrho_0}$; $Q \in \mathscr{M}$, $T \in \mathscr{M}$, $A \in F_q[x]^*$, $\theta \in \mathscr{P}$, $\tau \in \mathscr{F}_0$ tels que $(A, Q) = 1$, $|T|_0 = q^t$, $|Q|_0 = q^\chi$ et $|\tau|_0 = q^y$; $a_0, \ldots, a_k$, $k+1$ éléments de $\mathscr{F}_0$ avec $a_s = A/Q + \theta/Q\tau$ et $f(X)$ le polynôme

$$f(X) = a_k X^k + \ldots + a_1 X + a_0 \qquad \textit{pour } X \in F_q[x];$$

$L \in F_q[x]^*$ tel que $|L|_0 \leqslant q^{\varrho_0}$; r et ω des entiers tels que $\gamma - \varrho_0 \leqslant \omega < \gamma$, $r = \gamma$ ou $\gamma - 1$ et si $r = \gamma - 1$ alors $\omega = \gamma - 1$; R un polynôme unitaire de degré r; $\mathscr{G}$ et $\mathscr{H}$ deux parties de $\mathscr{M}$ telles que si $G \in \mathscr{G}$: $(G, Q) = 1$; ε un réel tel que $|\varepsilon| \leqslant 0{,}01\gamma$; ψ vérifiant les mêmes conditions que celles du lemme 10.

On pose $S = \sum_G \psi(G) \sum_H e_0\big(Lf(T^2GH)\big)$, la sommation étant faite sur les couples (G, H) de $\mathscr{G} \times \mathscr{H}$ tels que

$$|T^2GH - R|_0 \leqslant q^\omega, \qquad |G|_0 = q^\nu \qquad \textit{et} \qquad \tfrac{1}{4}\gamma - t - \varepsilon \leqslant \nu \leqslant \tfrac{1}{2}\gamma - t.$$

Alors

$$|S| \leqslant c_3 q^{\omega+1} q^{-1,1t} \Delta_0$$

où c_3 est une constante qui ne dépend que de c_1, c_2 et q.

Démonstration. Si $t > 1{,}2\varrho_0$, en décomposant la somme S de la même façon que dans le lemme 10, nous obtenons

$$|S| \leqslant c_1 \cdot \gamma^2 \cdot q^{\omega+1} \cdot q^{-1,1t} \cdot q^{-\varrho_0}.$$

Nous supposerons donc maintenant que $t \leqslant 1{,}2\varrho_0$. De même que dans le lemme 10, nous partageons les polynômes de $\mathscr{G}$ de degré ν en $q^{\nu-v-1}$ sous-ensembles (G_0):

$$|G - G_0|_0 \leqslant q^v \quad \text{où } v = \nu + \omega - \gamma$$

auxquels correspondent les sous-ensembles (H_0) de $\mathscr{H}$:

$$|H - H_0|_0 \leqslant q^{\omega-2l-\nu}.$$

Posons

$$S_G = \sum_{H \in (H_0)} e_0\big(Lf(T^2GH)\big), \qquad S_{(G_0)} = \sum_{G \in (G_0)} \varphi(G) S_G,$$

$$S_\nu = \sum_{\substack{(G_0) \\ |G_0|_0 = q^\nu}} S_{(G_0)}, \qquad S'_G = e_0\big(-Lf(T^2GH_0)\big) S_G$$

et

$$\beta'_j = \beta'_j(G) = \frac{Lf^{(j)}}{j!}(T^2GH_0)T^{2j}G^j, \qquad 1 \leqslant j \leqslant k.$$

Nous avons

$$S = \sum_\nu S_\nu \quad \text{et} \quad S'_G = \sum_{H_0 + X \in (H_0)} e_0(\beta'_k X^k + \ldots + \beta'_1 X).$$

Soit Ω_G l'ensemble des $\beta = (\beta_k, \ldots, \beta_1)$ tels que

$$|\beta_j - \beta'_j|_0 \leqslant q^{-2-j(\omega-2l-\nu)}, \qquad 1 \leqslant j \leqslant k.$$

Si $\beta \in \Omega_G$ nous avons

$$S'_G = S(\beta) = \sum_{H_0 + X \in (H_0)} e_0(\beta_k X^k + \quad + \beta_1 X),$$

$$\int_{\Omega_G} |S'_G|^{2l} d\beta_1 \ldots d\beta_k = \int_{\Omega_G} |S(\beta)|^{2l} d\beta_1 \ldots d\beta_k$$

et

$$|S'_G|^{2l} \leqslant \frac{1}{\operatorname{mes} \Omega_G} \int_{\mathscr{P}} \int_{\mathscr{P}} |S(\beta)|^{2l} \eta_G(\beta) d\beta_1 \ldots d\beta_k$$

où $\eta_G(\beta)$ est la fonction caractéristique de $\mathscr{H}_0^k(\Omega_G)$,

$$\sum_{G\in(G_0)} |S'_G|^{2l} \leqslant \frac{1}{\operatorname{mes}\Omega_G} \int_{\mathscr{P}} \int_{\mathscr{P}} |S(\beta)|^{2l} \sum_{G\in(G_0)} \eta_G(\beta)\, d\beta_1 \ldots d\beta_k.$$

$\sum_{G\in(G_0)} \eta_G(\beta)$ est majoré par le nombre de polynômes G' de (G_0) pour lesquels $\Omega_{G'}$ contient un point β' dont les coordonnées diffèrent de celles d'un point β de Ω_G par des polynômes de $F_q[x]$. Il suffit donc de majorer, pour G dans (G_0), le nombre des solutions G' du système

$$(1) \qquad |\beta_j(G') - \beta_j(G) - K_j|_0 \leqslant q^{-2-j(\omega-2t-\nu)}, \quad 1 \leqslant j \leqslant k,$$

où $K_j \in F_q[x]$.

(a) **Etude du système (1).**

Le système (1) est équivalent à

$$1 \leqslant j \leqslant k, \quad \sum_{u=j}^{k} \binom{u}{j} a_u L T^{2u} H_0^{u-j}(G'^u - G^u) = K_j + \theta_j,$$

$$K_j \in F_q[x], \quad \theta_j \in \mathscr{F}_0 \quad \text{et} \quad |\theta_j|_0 \leqslant q^{-2-j(\omega-2t-\nu)}.$$

Nous obtenons, en posant $G_u = a_u L T^{2u}(G'^u - G^u)$

$$(2) \qquad \sum_{u=j}^{k} \binom{u}{j} H_0^{u-j} G_u = K_j + \theta_j, \quad 1 \leqslant j \leqslant k.$$

En particulier, $G_k = K_k + \theta_k$. En multipliant les deux membres de cette équation par $\binom{k}{j} H_0^{k-j}$ et en les soustrayant successivement aux $k-1$ autres équations de (2), nous obtenons:

$$1 \leqslant j \leqslant k-1, \quad \sum_{u=j}^{k-1} \binom{u}{j} H_0^{u-j} G_u = K_j + \theta_j - \binom{k}{j} H_0^{k-j} K_k - \binom{k}{j} H_0^{k-j} \theta_k$$
$$= K_j^1 + \theta_j^1$$

où $K_j^1 \in F_q[x]$ et $|\theta_j^1|_0 \leqslant q^{-2-j(\omega-2t-\nu)+(k-j)(r-\omega)}$. En particulier $G_{k-1} = K_{k-1}^1 + \theta_{k-1}^1$.

Nous obtenons comme ci-dessus

$$1 \leqslant j \leqslant k-2, \quad \sum_{u=j}^{k-2} \binom{u}{j} H_0^{u-j} G_u = K_j^2 + \theta_j^2$$

où

$$K_j^2 \in F_q\ [x] \quad \text{et} \quad |\theta_j^2|_0 \leqslant q^{-2-j(\omega-2t-\nu)+(k-j)(r-\omega)}.$$

Par récurrence, nous obtenons

$$L T^{2s} a_s (G'^s - G^s) = K'_s + \theta'_s$$

soit

$$\left|\mathscr{H}_0\left(LT^{2s}\frac{A}{Q}(G'^s-G^s)+LT^{2s}\frac{\theta(G'^s-G^s)}{Q\tau}\right)\right|_0 \leqslant q^{-2-s(\omega-2t-\nu)+(k-s)(r-\omega)}.$$

Le nombre de solutions de (1) est majoré par le nombre Λ des solutions G' de l'équation

$$\left|\mathscr{H}_0\left(LT^{2s}\frac{A}{Q}(G'^s-G^s)\right)\right|_0 \leqslant q^{a-\varkappa} \tag{3}$$

où

$$a = \max\big(-2-s(\omega-2t-\nu)+(k-s)(r-\omega)+\chi,\ \varrho_0+2st-1+v+ \\ +(s-1)\nu-y\big).$$

(b) Majoration de Λ.

D'après le lemme 22, le nombre de solutions G' de l'équation

$$LT^{2s}AG'^s \equiv C' \bmod Q, \qquad 0 \leqslant |C'|_0 < |Q|_0,$$

est majoré par

$$(q^{v+1-\chi}+1)\,q^{\varrho_0+2st}\cdot q^{\frac{3\chi\log s}{\log\chi}}$$

Le nombre de polynômes C' qui conviennent est majoré par $(q^{a+1}+1)$. Nous avons donc

$$\Lambda \leqslant (q^{v+1-\chi}+1)(q^{a+1}+1)\,q^{\varrho_0+2st}q^{\frac{3\chi\log s}{\log\chi}}$$

Posons

$$\varrho = 0,05\gamma \quad \text{si } \tfrac{1}{4}\gamma \leqslant \chi \leqslant \tfrac{1}{2}s\gamma+\tfrac{1}{4}\gamma,$$
$$\varrho = 0,2\chi \quad \text{si } \chi < \tfrac{1}{4}\gamma.$$

Alors, $\varrho_0 \leqslant \varrho/10$. Démontrons que

$$\Lambda \leqslant 4q^{v+1+(3k+1)t-4,41\varrho},$$

$$\begin{aligned} a+1 &\leqslant s\nu+2st+\max\left(-1-s\omega+(k-s)(\gamma-\omega)+\chi,\ \varrho_0-\tfrac{1}{2}s\gamma\right) \\ &\leqslant s(\nu-\tfrac{1}{2}\gamma+t)+st+\max(k\varrho_0-\tfrac{1}{2}s\gamma+\chi,\ \varrho_0) \\ &\leqslant kt+k\varrho_0+\tfrac{1}{4}\gamma+s(\nu-\tfrac{1}{2}\gamma+t). \end{aligned}$$

D'autre part

$$\begin{aligned} a+1 &\leqslant s(\nu-\tfrac{1}{2}\gamma+t)+st+\chi+\max(k\varrho_0-s\tfrac{1}{2}\gamma,\ \varrho_0-\chi) \\ &\leqslant kt+s(\nu-\tfrac{1}{2}\gamma+t)+\chi-4,9\varrho. \end{aligned}$$

Nous aurons donc

$$\begin{aligned} a+1 &\leqslant v+1-\nu-\omega+\gamma+s(\nu-\tfrac{1}{2}\gamma+t)+st+k\varrho_0+\tfrac{1}{4}\gamma \\ &\leqslant v+1+(k+1)t+(k+1)\varrho_0-\tfrac{1}{4}\gamma \\ &\leqslant v+1+(k+1)t-4,7\varrho, \qquad \text{car } (k+1)\varrho_0 \leqslant 0,3\varrho, \end{aligned}$$

$$v+1-\chi \leqslant v+1-5\varrho, \qquad a+1+v+1-\chi \leqslant v+1+kt-4,9\varrho,$$

et

$$0 \leqslant v+1-\nu-\omega+\gamma \leqslant v+1+t-0,235\gamma \leqslant v+1+t-4,7\varrho.$$

Donc

$$\Lambda \leqslant 4q^{v+1+(3k+1)t+\varrho_0+\frac{3\chi\log k}{\log\chi}-4,7\varrho}$$

Puisque $\chi \geqslant \log^3\gamma$, $\log\chi \geqslant 300\log k$ donc

$$\frac{3\chi\log k}{\log\chi} \leqslant 0,01\chi \leqslant 0,05\varrho \qquad \text{si } \chi \leqslant 0,25\gamma$$

et si $\chi \geqslant 0,25\gamma$

$$\frac{3\chi\log k}{\log\chi} \leqslant \frac{3k\gamma\log k}{k^{300}+\log\frac{1}{4}} \leqslant 0,0025\gamma \leqslant 0,05\varrho.$$

Donc $\Lambda \leqslant 4\ q^{v+1+(3k+1)t-4,41\varrho}$.

(c) Majoration de $|S_\nu|^{2l}$.

D'après le lemme 19, si $l \geqslant \frac{1}{4}k(k+1)+kh$

$$\sum_{G\in(G_0)} |S_G|^{2l} \leqslant 4q^{k+\frac{1}{2}k(k+1)(\omega-2t-\nu)}\cdot K^h\cdot(\omega-2t-\nu)^h \times$$
$$\times\, q^{2l(\omega-2t-\nu+1)-\frac{1}{2}k(k+1)(\omega-2t-\nu)+(\omega-2t-\nu)\delta_h+v+1+(3k+1)t-4,41\varrho}$$

où $K=(l!)^2q^{6l-3k}$ et $\delta_h=\frac{1}{2}k(k+1)(1-1/k)^h$. Donc

$$\sum_{G\in(G_0)} |S_G|^{2l} \leqslant 4K^h(\omega-2t-\nu)^h q^{k+(\omega-2t-\nu)(2l+\delta_h)+2l}\times q^{v+1+(3k+1)t-4,41\varrho}.$$

Nous avons

$$|S_\nu|^2 \leqslant \Big(\sum_{|G|_0=q^\nu}|\psi(G)|^2\Big)\Big(\sum_{\substack{(G_0)\\|G_0|_0=q^\nu}}\ \sum_{G\in(G_0)}|S_G|^2\Big),$$

$$\Big(\sum_{\substack{(G_0)\\|G_0|_0=q^\nu}}\ \sum_{G\in(G_0)}|S_G|^2\Big)^l \leqslant q^{(\nu-v-1)(l-1)}\sum_{\substack{(G_0)\\|G_0|_0=q^\nu}}\Big(\sum_{G\in(G_0)}|S_G|^2\Big)$$

et

$$\Big(\sum_{G\in(G_0)}|S_G|^2\Big)^l \leqslant q^{(v+1)(l-1)}\Big(\sum_{G\in(G_0)}|S_G|^2\Big).$$

Donc

$$|S_\nu|^{2l} \leqslant 4C_2^l\gamma^{3l}K^h(\omega-2t-\nu)^h q^{2l(\omega-2t+1)+(3k+1)t+(\omega-2t-\nu)\delta_h-4,41\varrho}.$$

(d) Majoration de S lorsque $\chi \geqslant 0,25\gamma$.

Nous prendrons $l=[\frac{1}{4}k(k+1)+kh+\frac{1}{2}]$ avec

$$h=\left[\frac{\log 25k(k+1)}{-\log(1-1/k)}+1\right].$$

Alors

$$(\omega-2t-\nu)\,\delta_h \leqslant \gamma\cdot\tfrac{1}{2}k(k+1)(1-1/k)^h \leqslant 0,02\gamma = 0,4\varrho.$$

Démontrons que $l \leqslant 2k^2(2+\log k)$. Il suffit de démontrer que

$$\frac{1}{2k}+\tfrac{1}{4}(k+1)+\frac{\log 25\,k(k+1)}{-\log(1-1/k)}+1 \leqslant 2k(2+\log k).$$

Puisque $-\log(1-1/k) \geqslant 1/k+1/2k^2$ et que $\log(1+1/k) \leqslant 1/k$, il suffit de démontrer que

$$\log 25+2\log k+\frac{1}{k} \leqslant \left(3{,}75\,k+2\,k\log k-\frac{1}{2k}-1{,}25\right)\left(\frac{1}{k}+\frac{1}{2k^2}\right)$$

et

$$\log 25+\frac{1}{k} \leqslant 3{,}75+\left(\frac{3{,}75}{2}-1{,}25\right)\frac{1}{k}.$$

L'inégalité ci-dessus est vérifiée car

$$\log 25+\frac{3}{8k} < 3{,}3+0{,}2 < 3{,}75.$$

Nous avons

$$|S_\nu|^{2l} \leqslant C_1' C_2^l \gamma^{3l} \gamma^{l/k} q^{2l(\omega+1)-3lt-2l\varrho_0}$$

car

$$l \geqslant \tfrac{1}{4}k(k+1)+3k \geqslant 3k+1 \quad \text{et} \quad 4\varrho \geqslant 2l\varrho_0.$$

Donc

$$|S_\nu| \leqslant C_1'^{1/2l}\cdot\sqrt{C_2}\,\gamma^{1,75}\, q^{\omega+1-1,5t-\varrho_0}$$

et

$$|S| \leqslant C_3 \gamma^{2,75} q^{\omega+1-1,1t-\varrho_0}$$

où C_3 ne dépend que de q (car $k < p \leqslant q$) et de C_2.

(e) Majoration de S lorsque $\chi < 0{,}25\gamma$.

Nous prendrons $l = [\tfrac{1}{4}k(k+1)+kh+\tfrac{1}{2}]$ avec

$$h = \left[\frac{\log 8k(k+1)\gamma/\chi}{-\log(1-1/k)}+1\right].$$

Alors

$$(\omega-2t-\nu)\,\delta_h \leqslant \frac{\gamma}{2}\,k(k+1)\left(1-\frac{1}{k}\right)^h \leqslant 0{,}08\,\chi = 0{,}4\varrho.$$

Démontrons que

$$l \leqslant 2k^2(2+\log k\sqrt{\gamma/\chi}).$$

De même que dans (d), il suffit de démontrer que $\log 8+3/8k \leqslant 3{,}75$ ce qui est vérifié.

Nous avons

$$|S_\nu|^{2l} \leqslant C_4 C_2^l \gamma^{3l+l/k} K^h q^{2l(\omega+1)-3lt-2l\varrho_0-0{,}01\varrho}$$

car $l \geqslant 3k+1$ et $4\varrho \geqslant 2l\varrho_0$. Démontrons que

$$K^h \leqslant q^{0{,}01\varrho}.$$

Puisque $\log\gamma \geqslant k^{100}$

$$\log k\sqrt{\gamma/\chi}+2 \leqslant \tfrac{1}{2}\log\gamma + k + 2 \leqslant \log\gamma$$

donc $l \leqslant 2k^2\log\gamma$ et

$$(l!)^2 \leqslant \exp(4k^2\log\gamma \times 2k^2\log\log\gamma) \leqslant q^{16k^4\log\gamma\log\log\gamma}.$$

Ceci entraîne

$$K^h \leqslant \big((l!)^2 q^{6l}\big)^h \leqslant q^{32k^5\log^2\gamma\log\log\gamma + 24k^3\log^2\gamma} \leqslant q^{64k^5\log^2\gamma\log\log\gamma}.$$

Il suffit maintenant de démontrer que $64k^5\log^2\gamma\log\log\gamma \leqslant 0{,}01\,\varrho$ soit

$$64k^5\log^2\gamma\log\log\gamma \leqslant 0{,}002\log^3\gamma, \qquad 32000\,k^5 \leqslant \frac{\log\gamma}{\log\log\gamma}.$$

Puisque $\log\gamma \geqslant k^{100}$, la fonction du second membre est croissante. Il suffit de vérifier que

$$32000\,k^5 \leqslant \frac{k^{100}}{100\log k}$$

soit $32\cdot 10^5\cdot\log k \leqslant k^{95}$ ce qui est vérifié.

De même que dans (d)

$$|S_\nu| \leqslant C_2'^{1/2l}\sqrt{C_2}\,\gamma^{1,75}\,q^{\omega+1-1,5t-\varrho_0} \qquad \text{et} \qquad |S| \leqslant C_3\gamma^{2,75}q^{\omega+1-1,1t-\varrho_0}$$

où C_3 ne dépend que de q et de C_2.

Lemme 24. *Les hypothèses sont celles du lemme 23.*

Soient $\mathscr{D}$ et $\mathscr{H}$ deux parties de $\mathscr{M}$ telles que si $D \in \mathscr{D}$

$$(D, Q) = 1 \qquad \textit{et} \qquad |D|_0 \leqslant q^{0,25\gamma-1}.$$

Posons

$$S = \sum_D \sum_M e_0\big(Lf(DM)\big)$$

la sommation étant faite sur les couples (D, M) de $\mathscr{D}\times\mathscr{H}$ tels que

$$|DM|_0 \leqslant q^{\gamma-1}, \qquad |M|_0 = q^\nu,$$

avec $0{,}5\gamma < \nu < 0{,}75\gamma$.

Alors

$$|S| \leqslant C_4\gamma^{2,75}\cdot q^{\gamma-\varrho_0}$$

où C_4 ne dépend que de q.

Démonstration. Nous avons:

$$S = \sum_{\substack{|D|_0 \leqslant q^{0,24\gamma} \\ D\in\mathscr{D}}} \sum_{M\in\mathscr{H}} e_0\big(Lf(DM)\big) + \sum_{|D|_0 > q^{0,24\gamma}} \sum_{M\in\mathscr{H}} e_0\big(Lf(DM)\big).$$

En appliquant le lemme 23 à la deuxième somme, nous obtenons

$$|S| \leqslant \gamma q^{0,99\gamma} + C_3\gamma^{2,75}\cdot q^{\gamma-\varrho_0}$$

et puisque $\varrho_0 \leqslant 0{,}01\gamma$

$$|S| \leqslant C_4 \gamma^{2,75} q^{\gamma-\varrho_0}.$$

Lemme 25. *Les hypothèses sont celles du lemme 23 et on suppose de plus que* $2 \leqslant s$, $T|Q$ *et*

$$kt \leqslant 0{,}042\chi \quad si \ \chi < 0{,}25\gamma,$$

$$kt \leqslant 0{,}0105\gamma \quad si \ \chi \geqslant 0{,}25\gamma.$$

Soit $\mathscr{D}$ *une partie de* $\mathscr{M}$ *telle que, si* $D \in \mathscr{D}$, $(D, Q) = 1$. *Posons*

$$S = \sum_D \sum_M e_0\big(Lf(DTM)\big)$$

la sommation étant faite sur les couples (D, M) *de* $\mathscr{D} \times \mathscr{M}$ *tels que*

$$|DTM - R|_0 \leqslant q^{\omega}, \qquad |M|_0 = q^{\nu} \qquad avec \ 0{,}75\gamma - t \leqslant \nu \leqslant r - t.$$

Alors

$$|S| \leqslant C_5 \gamma^{1,5} q^{\omega+1-t-\varrho_0}$$

où C_5 *est une constante qui ne dépend que de* q.

Démonstration. De même que dans le lemme 10, nous partageons les polynômes de $\mathscr{M}$ de degré ν en $q^{\nu-v-1}$ sous-ensembles (M_0)

$$|M - M_0|_0 \leqslant q^{v} \qquad \text{avec } v = \nu + \omega - \gamma$$

associés à un polynôme D de $\mathscr{D}$ de degré inférieur ou égal à $r - \nu - t$. Posons

$$S_D = \sum_{M \in (M_0)} e_0\big(Lf(DTM)\big).$$

Puisque (M_0) est la boule de $\mathscr{M}$ de centre M_0 et de rayon q^{v}

$$S_D = q^{-v-1} \sum_{\substack{|X|_0 \leqslant q^{v} \\ X \in F_q[x]}} e_0\big(Lf\big(DT(M+X)\big)\big).$$

Posons

$$S_X = \sum_{M \in (M_0)} e_0\big(Lf\big(DT(M+X)\big)\big),$$

$$\beta'_j = \beta'_j(X) = \frac{Lf^{(j)}(DTX)}{j!} \cdot D^j T^j$$

et

$$S'_X = \sum_{M \in (M_0)} e_0\Big(\sum_{j=1}^{k} \beta'_j M^j\Big)$$

Nous avons

$$S_D = q^{-v-1} \sum_{|X|_0 \leqslant q^{v}} S_X \qquad \text{et} \qquad |S_X| = |S'_X|.$$

Soit Ω_X l'ensemble des $\beta = (\beta_k, \ldots, \beta_1)$ tels que

$$|\beta_j - \beta'_j|_0 \leqslant q^{-2-j\nu}, \quad 1 \leqslant j \leqslant k.$$

Posons

$$S(\beta) = \sum_{M \in (M_0)} e_0\Big(\sum_{j=1}^{k} \beta_j M^j\Big).$$

De même que dans le lemme 23, nous avons

$$|S'_X|^{2l} \leqslant q^{k+\frac{1}{2}k(k+1)\nu} \int_{\mathscr{P}} \int_{\mathscr{P}} |S(\beta)|^{2l} \eta_X(\beta)\, d\beta_k \ldots d\beta_1$$

où $\eta_X(\beta)$ est la fonction caractéristique de $\mathscr{H}_0^k(\Omega_X)$.

$$\sum_{|X|_0 \leqslant q^\nu} |S'_X|^{2l} \leqslant q^{k+\frac{1}{2}k(k+1)\nu} \cdot \int_{\mathscr{P}} \int_{\mathscr{P}} |S(\beta)|^{2l} \sum_{|X|_0 \leqslant q^\nu} \eta_X(\beta)\, d\beta_k \ldots d\beta_1$$

et $\sum_{|X|_0 \leqslant q^\nu} \eta_X(\beta)$ est majoré par le nombre de solutions X' du système

$$(1) \qquad |\beta_j(X') - \beta_j(X) - K_j|_0 \leqslant q^{-2-j\nu}, \quad K_j \in F_q[x], \quad 1 \leqslant j \leqslant k.$$

(a) Etude du système (1).

En posant $G_u = a_u L T^u D^u$ le système (1) est équivalent à

$$\sum_{u=j}^{k} \binom{u}{j} G_u(X'^{u-j} - X^{u-j}) = K_j + \theta_j, \quad 1 \leqslant j \leqslant k,$$

où $K_j \in F_q[x]$ et $|\theta_j| \leqslant q^{-2-j\nu}$. En particulier

$$kG_k(X' - X) = K_{k-1} + \theta_{k-1}.$$

Pour $1 \leqslant j \leqslant k-2$ multiplions les deux membres de la j-ième équation par $(k-j)!$ et soustrayons membre à membre l'équation ci-dessus multipliée par

$$\frac{(k-1)!}{j!} \frac{X'^{k-j} - X^{k-j}}{X' - X} \quad \text{lorsque } X' \neq X.$$

Nous obtenons

$$1 \leqslant j \leqslant k-2, \qquad \sum_{u=j}^{k-1} (k-j)! \binom{u}{j} G_u(X'^{u-j} - X^{u-j}) = K_j^1 + \theta_j^1$$

où $K_j^1 \in F_q[x]$ et $|\theta_j^1|_0 \leqslant \max(q^{-2-j\nu}, q^{-2-(k-1)\nu+(k-j-1)\nu})$ donc $|\theta_j^1|_0 \leqslant q^{-2-j\nu}$. En particulier

$$2(k-1)G_{k-1}(X' - X) = K_{k-2}^1 + \theta_{k-2}^1.$$

Nous obtenons par récurrence

$$2!\,3! \ldots (k-s+1)!\, sG_s(X' - X) = K'_{s-1} + \theta'_{s-1}$$

où $K'_{s-1} \in F_q[x]$ et $|\theta'_{s-1}|_0 \leqslant q^{-2-(s-1)\nu}$, soit

$$\left|\mathscr{H}_0\left(\frac{A}{Q} LT^s D^s(X'-X) + \frac{L\theta}{Q\tau} T^s D^s(X'-X)\right)\right|_0 \leqslant q^{-2-(s-1)\nu}.$$

Le nombre des solutions G' de l'équation (1) est majoré par le nombre Λ des solutions G' de l'équation

$$\left|\mathscr{H}_0\left(LT^s \frac{A}{Q} D^s(X'-X)\right)\right|_0 \leqslant q^{a-\chi} \tag{2}$$

où $a = \max(-2-(s-1)\nu+\chi,\ \varrho_0-1+st+s(r-\nu-t)+v-y)$.

(b) Majoration de Λ.

D'après le lemme 7

$$\Lambda \leqslant (q^{a+1}+q^{\varrho_0+st})(q^{v+1-\chi}+1).$$

ϱ est défini comme dans le lemme 23 (b); alors

$$kt \leqslant 0{,}21\,\varrho.$$

Démontrons que

$$\Lambda \leqslant 4\, q^{v+1-4{,}69\varrho}.$$

Nous avons

$$\begin{aligned} a+1 &\leqslant v+1+\max\big(\varrho_0-s\nu+\chi,\ \varrho_0+s(\gamma-\nu)-s\gamma/2-\gamma/4\big) \\ &\leqslant v+1+\varrho_0+st+\max(-\gamma/4,\ -\gamma/2) \leqslant v+1-4{,}69\,\varrho, \\ v+1-\chi+\varrho_0+st &\leqslant v+1+\varrho_0+st-5\varrho \leqslant v+1-4{,}69\,\varrho, \\ \varrho_0+st &\leqslant 0{,}31\,\varrho \leqslant v+1-4{,}69\,\varrho. \end{aligned}$$

(c) Majoration de $|S_D|^{2l}$.

D'après le lemme 19, si $l \geqslant \frac{1}{4}k(k+1)+kh$

$$\sum_{|X|_0 \leqslant q^v} |S_X|^{2l} \leqslant 4\, q^{k+\frac{1}{2}k(k+1)\nu} K^h v^h q^{(v+1)2l-\frac{1}{2}k(k+1)v} \times q^{v\delta_h+v+1-4{,}69\varrho}$$

où

$$K = (l!)^2 q^{6l-3k} \quad \text{et} \quad \delta_h = \tfrac{1}{2}k(k+1)(1-1/k)^h.$$

De plus

$$|S_D|^{2l} \leqslant q^{-2l(v+1)+(v+1)(2l-1)} \sum_{|X|_0 \leqslant q^v} |S_X|^{2l} \leqslant 4\, q^k K^h \gamma^h q^{2l(v+1)+\frac{1}{2}k(k+1)\varrho_0+v\delta_h-4{,}69\varrho}.$$

(d) Majoration de S.

De même que dans le lemme 23 (d) et (e) nous obtenons

$$|S_D|^{2l} \leqslant C'_3 \gamma^{l/k} q^{2l(v+1)-2l\varrho_0+\frac{1}{2}k(k+1)\varrho_0-0{,}28\varrho}$$

car $4\varrho \geqslant 2l\varrho_0$, $v\delta_h \leqslant 0{,}4\varrho$ et $K^h \leqslant 0{,}01\varrho$.

Démontrons que $\frac{1}{2}k(k+1)\varrho_0 \leqslant 0{,}28\,\varrho$. Il suffit de démontrer que

$$\tfrac{1}{2}k(k+1)\frac{\varrho}{k^2(2+\log k)} \leqslant 0{,}28\,\varrho$$

soit

$$\frac{k+1}{k(2+\log k)} \leqslant 0{,}56,$$

$$1 \leqslant (0{,}12+0{,}56\log k)\,k \quad \text{et} \quad 1 \leqslant 0{,}24+1{,}12\log 2.$$

$$\log 2 > 0{,}69 \quad \text{donc} \quad 0{,}24+1{,}12\log 2 > 1{,}01.$$

Nous avons

$$|S| \leqslant \sum_{\nu} \sum_{|D|_0=q^{r-\nu-t}} |S_D| \leqslant C_5\gamma^{1,5}q^{\omega+1-t-\varrho_0}.$$

7. Enoncés et démonstrations des théorèmes 1 et 2.

THÉORÈME 1. *Soient: γ un entier tel que $\gamma \geqslant 10$; χ un entier tel que $0<\chi<\gamma$; y un entier tel que $\max(\chi, \gamma-\chi) \leqslant y < \gamma$; ϱ_0 le réel défini par: $0{,}2\,\chi$ si $\chi \leqslant \gamma/4$, $0{,}05\,\gamma$ si $\gamma/4 \leqslant \chi \leqslant 3\,\gamma/4$, $0{,}2\,(\gamma-\chi)$ si $3\,\gamma/4 \leqslant \chi < \gamma$; $\Delta_1 = \exp(110\log^2\gamma)\cdot q^{-\varrho_0}$; $A, L \in F_q[x]^*$, $Q \in \mathscr{M}$, $\theta \in \mathscr{P}$ et $\alpha, \tau \in \mathscr{F}_0$ tels que $|L|_0 \leqslant q^{\varrho_0}$, $(A, Q) = 1$, $|Q|_0 = q^{\chi}$, $|\tau|_0 = q^{y}$ et $\alpha = A/Q+\theta/Q\tau$; r et ω des entiers tels que $\gamma-\varrho_0 \leqslant \omega < \gamma$, $r = \gamma$ ou $\gamma-1$ et si $r = \gamma-1$, $\omega = \gamma-1$; $R \in \mathscr{M}$ de degré r.*

Si $S = \sum e_0(PL\alpha)$ où la sommation est faite sur les polynômes irréductibles P de $\mathscr{M}$ tels que $|P-R|_0 \leqslant q^{\omega}$ alors $|S| \leqslant C_6\Delta_1 q^{\omega+1}$ où C_6 est une constante positive qui ne dépend que de q.

THÉORÈME 2. *Soient: k un entier tel que $2 \leqslant k \leqslant p-1$; γ un entier tel que $\operatorname{Log}\gamma \geqslant k^{100}$; $\alpha_0, \alpha_1, \ldots, \alpha_k \in \mathscr{F}_0$ tels qu'il existe un entier s, $2 \leqslant s \leqslant k$, pour lequel $\alpha_s = A/Q+\theta/Q\tau$, où $Q \in \mathscr{M}$, $A \in F_q[x]^*$, $(A, Q) = 1$, $|Q|_0 = q^{\chi}$, $\theta \in \mathscr{P}$, $|\tau|_0 = q^{y}$, $s\,\gamma > y \geqslant [s\gamma/2+\gamma/4]$ et $\log^3\gamma \leqslant \chi \leqslant s\gamma/2+\gamma/4$; ϱ_0 le réel défini par*

$$\frac{0{,}05\gamma}{k^2(2+\log k)} \quad \text{si } \tfrac{1}{4}\gamma \leqslant \chi \leqslant \tfrac{1}{2}s\gamma+\tfrac{1}{4}\gamma,$$

$$\frac{0{,}2\gamma}{k^2\big(2+\log(k\sqrt{\gamma/\chi})\big)} \quad \text{si } \chi < \tfrac{1}{4}\gamma;$$

$\Delta_1 = \exp(110\log^2\gamma)\,q^{-\varrho_0}$; r, ω et R sont définis comme dans le théorème 1.

Si $S = \sum_P e_0\big(Lf(P)\big)$ où $f(P) = \alpha_k P^k + \quad + \alpha_1 P + \alpha_0$ et où la sommation est faite sur les polynômes irréductibles P de $\mathscr{M}$ tels que $|P-R|_0 \leqslant q^{\omega}$, alors

$$|S| \leqslant C_6\Delta_1 q^{\omega+1}.$$

Démonstration des théorèmes 1 et 2. Les démonstrations des théorèmes 1 et 2 ont une partie commune dans laquelle $f(X)$ désigne

aX pour le théorème 1, $a_kX^k+\ldots+a_0$ pour le théorème 2, et V désigne le polynôme 1 pour le théroème 1, le polynôme Q pour le théorème 2.

Soit F le produit de tous les polynômes irréductibles de $\mathscr{M}$ de degré inférieur ou égal à $\gamma/4$ ne divisant pas V, et soit $W = F\cdot V$. Nous désignons par $\mathscr{U}$ l'ensemble des polynômes U de $\mathscr{M}$ premiers à W et tels que $|U-R|_0 \leqslant q^{\omega}$. Si $\mathscr{U}_j$ est l'ensemble des polynômes de $\mathscr{U}$ ayant j facteurs irréductibles, nous avons

$$\mathscr{U} = \bigcup_{j=1}^{3} \mathscr{U}_j.$$

Par convention, si $1\in\mathscr{U}$, nous posons $1\in\mathscr{U}_1$ et $\mathscr{U}_1^* = \mathscr{U}_1-\{1\}$. Si $\mathscr{S} = \sum_{U\in\mathscr{U}} e_0\big(Lf(U)\big)$, le lemme 8 (i) entraine

$$\mathscr{S} = \sum_{\substack{D|F\\ D\in\mathscr{M}}} \mu(D) \sum_{\substack{|DM-R|_0\leqslant q^{\omega}\\ (M,V)=1}} e_0\big(Lf(DM)\big).$$

Si $S_i = \sum_{U\in\mathscr{U}_i} e_0\big(Lf(U)\big)$ $(i = 1, 2, 3)$, nous avons les relations

$$\mathscr{S} = S_1+S_2+S_3, \qquad |S_1-S| \leqslant q^{1+\gamma/4}.$$

Pour majorer S, il suffit de majorer $\mathscr{S}$, S_2 et S_3. Dans la démonstration, C désigne une constante qui ne dépend que de q.

(a) Majoration de S_2.

Si

$$\mathscr{S}_2 = \sum_{\substack{|UU'-R|_0\leqslant q^{\omega}\\ U,U'\in\mathscr{U}_1^*}} e_0\big(Lf(UU')\big)$$

nous avons

$$|S_2-\tfrac{1}{2}\mathscr{S}_2| \leqslant \tfrac{1}{2}\cdot\frac{q}{q-1}\cdot q^{\gamma/2} \leqslant q^{\gamma/2}.$$

Comme

$$\mathscr{S}_2 = \sum_{\substack{|UU'-R|_0\leqslant q^{\omega}\\ U,U'\in\mathscr{U}_1^*\\ |U|_0\leqslant q^{\gamma/2}}} e_0\big(Lf(UU')\big) + \sum_{\substack{|UU'-R|_0\leqslant q^{\omega}\\ U,U'\in\mathscr{U}_1^*\\ |U|_0>q^{\gamma/2}\\ |U'|_0\leqslant q^{\gamma/2}}} e_0\big(Lf(UU')\big)$$

en appliquant les lemmes 10 et 23, à la première somme avec $T = 1$, $G = U, H = U'$ et $\psi(G) = 1$ et à la deuxième somme avec $T = 1$, $G = U', H = U$, nous obtenons

$$|\mathscr{S}_2| \leqslant C\, q^{\omega+1}\cdot\Delta_0 \qquad \text{où } \Delta_0 = \gamma^3 q^{-\varrho_0}$$

et

$$|S_2| \leqslant q^{\gamma/2}+C\cdot q^{\omega+1}\cdot\Delta_0.$$

(b) Majoration de S_3.

Si

$$\mathscr{S}_3 = \sum_{\substack{|UU'-R|_0 \leqslant q^\omega \\ U \in \mathscr{U}_1^* \\ U' \in \mathscr{U}_2}} e_0\big(Lf(UU')\big)$$

alors

$$S_3 - \tfrac{1}{3}\mathscr{S}_3 = -\tfrac{1}{3} \sum_{\substack{|U^2U'-R|_0 \leqslant q^\omega \\ U \in \mathscr{U}_1^* \\ U' \in \mathscr{U}_1^*}} e_0\big(Lf(U^2U')\big)$$

et

$$|S_3 - \tfrac{1}{3}\mathscr{S}_3| \leqslant \tfrac{2}{3} \sum_{\substack{q^{\gamma/2} < |UU'|_0 \leqslant q^{3\gamma/4} \\ U, U' \in \mathscr{U}_1^*}} 1 \leqslant \tfrac{2}{3} q^{1+3\gamma/4}.$$

Dans l'expression de $\mathscr{S}_3$, comme $U' \in \mathscr{U}_2$, $|U'|_0 > q^{\gamma/2}$ et les valeurs prises par U dans $\mathscr{U}_1^*$ sont soumises à la condition $q^{\gamma/4} < |U|_0 < q^{\gamma/2}$; nous pouvons donc appliquer les lemmes 10 et 23 en posant $T = 1$, $G = U$, $H = U'$ et $\psi(G) = 1$, ce qui donne

$$|\mathscr{S}_3| \leqslant C \cdot q^{\omega+1} \cdot \Delta_0.$$

(c) Majoration de $\mathscr{S}$.

Nous pouvons écrire $\mathscr{S} = \mathscr{A}_0 - \mathscr{A}_1$ où

$$\mathscr{A}_i = \sum_{\substack{D|F \\ \mu(D)=(-1)^i}} \sum_{\substack{|DM-R|_0 \leqslant q^\omega \\ (M,V)=1}} e_0\big(Lf(DM)\big) \quad (i = 0,1).$$

Nous majorerons $\mathscr{A}_0$; $\mathscr{A}_1$ se majore de la même manière. Soit ν le degré de M.

(α) Si $0 \leqslant \nu < \gamma/4 - \varepsilon\gamma$ (où $\varepsilon = 0{,}01$), d'après le lemme 9, nous pouvons répartir les diviseurs du polynôme F dans au plus

$$\exp\left(\left(2 + \frac{\log\gamma/4}{\log(1+\varepsilon)}\right)\log\gamma\right)$$

ensembles disjoints; nous noterons $\mathscr{A}_0'$ la partie de $\mathscr{A}_0$ qui correspond à un ensemble de cette partition. Nous allons montrer que $\mathscr{A}_0'$ est majoré par $C \cdot q^{\omega+1} \cdot \Delta_0$. Ceci entrainera que la partie de $\mathscr{A}_0$ correspondant à $0 \leqslant \nu < \gamma/4 - \varepsilon\gamma$ est majorée par

$$C \cdot q^{\omega+1} \cdot \Delta_0 \cdot \exp\left(\left(2 + \frac{\log\gamma/4}{\log(1+\varepsilon)}\right)\log\gamma\right)$$
$$\leqslant C \cdot q^{\omega+1} \cdot \Delta_0 \cdot \exp(110\log^2\gamma - 10\log\gamma) \leqslant C \cdot q^{\omega+1} \cdot \Delta_1.$$

Il reste donc à démontrer que $\mathscr{A}_0'$ est majoré par $C \cdot q^{\omega+1} \cdot \Delta_0$, φ étant défini par le lemme 9, si $\varphi \leqslant \gamma/4 - \nu - \varepsilon\gamma$ alors $|\mathscr{A}_0'| \leqslant 2q^\nu q^{(\gamma/4-\nu-\varepsilon\gamma)(1+\varepsilon)} \leqslant 2q^{\gamma/4}$

et si $\varphi > \gamma/4 - \nu - \varepsilon\gamma$, $\mathscr{A}_0'$ se met sous la forme

$$\mathscr{A}_0' = \frac{1}{n} \sum_M \sum_K \sum_X e_0\big(Lf(MKX)\big)$$

la sommation étant étendue à des éléments de $\mathscr{M}$ satisfaisant à

$$|M|_0 = q^\nu, \quad q^{\gamma/4-\nu-\varepsilon\gamma} < |K|_0 \leqslant q^{(\gamma/4-\nu-\varepsilon\gamma)(1+\varepsilon)} \leqslant q^{\gamma/2-\nu}$$
$$|MKX - R|_0 \leqslant q^\omega \quad \text{et} \quad (K, X) = 1$$

chaque polynôme $D = KX$ étant pris n fois.

Nous avons

$$\mathscr{A}_0' = \frac{1}{n} \sum_{\substack{T|F \\ T\in\mathscr{M}}} \mu(T)\, \mathscr{A}_T'$$

où

$$\mathscr{A}_T' = \sum_M \sum_{K_1} \sum_{X_1} e_0\big(Lf(T^2MK_1X_1)\big)$$

la sommation étant étendue à des éléments de $\mathscr{M}$ tels que.

$$|M|_0 = q^\nu, \quad q^{\gamma/4-\nu-t-\varepsilon\gamma} < |K_1|_0 \leqslant q^{\gamma/2-\nu-t} \quad \text{et} \quad |T^2MK_1X_1 - R|_0 \leqslant q^\omega.$$

Le nombre $\psi(G)$ des solutions de l'équation $MK_1 = G$ est au plus $d(G)$ donc ψ satisfait les conditions des lemmes 10 et 23 avec $C_1 = C_2 = 2$. Nous avons donc

$$\mathscr{A}_T' = \frac{1}{n} \sum_G \psi(G) \sum_H e_0\big(Lf(T^2GH)\big)$$

la sommation étant étendue à des polynômes tels que

$$q^{\gamma/4-t-\varepsilon\gamma} < |G|_0 \leqslant q^{\gamma/2-t} \quad \text{et} \quad |T^2GH - R|_0 \leqslant q^\omega.$$

En appliquant les lemmes 10 et 23, nous obtenons

$$|\mathscr{A}_T'| \leqslant C q^{\omega+1} \cdot q^{-1,1t} \cdot \Delta_0$$

et donc

$$|\mathscr{A}_0'| \leqslant C \cdot q^{\omega+1} \cdot \Delta_0 \sum_{t\geqslant 0} q^{-0,1t} \leqslant C \cdot q^{\omega+1} \cdot \Delta_0.$$

(β) Si $\nu \geqslant 0{,}24\gamma$, les démonstrations sont différentes pour le théorème 1 et le théorème 2.

Avec les hypothèses du théorème 1, si $\nu \leqslant \gamma - 3\varrho_0$, nous appliquons le lemme 11 à la partie correspondante $\mathscr{A}_0''$ de $\mathscr{A}_0$, ce qui donne

$$|\mathscr{A}_0''| \leqslant 2\gamma q^{\omega+1} \cdot q^{-\varrho_0} \leqslant q^{\omega+1} \cdot \Delta_0$$

et si $\gamma - 3\varrho_0 < \nu \leqslant r$, la partie correspondante $\mathscr{A}_0'''$ de $\mathscr{A}_0$ s'écrit sous la forme

$$\mathscr{A}_0''' = \sum_{\nu} \sum_{|M_1|_0 = q^\nu} \sum_{D \in (D_0)} S_D$$

où les boules (M_1) sont définies par:

$$M \in (M_1) \Leftrightarrow \begin{cases} |M - M_1|_0 \leqslant q^{\chi-1}, \\ M \in \mathscr{M}. \end{cases}$$

Chaque boule (M_0) associée à (D_0) est réunion de $q^{\nu-\chi+1}$ boules (M_1). Si $|Y|_0 \leqslant q^{\chi-1}$, $LDY\theta/Q\tau \in \mathscr{P}^2$ donc

$$S_D = e_0(LM_1Da) \sum_{|Y|_0 \leqslant q^{\chi-1}} e_0\left(\frac{LADY}{Q}\right);$$

Q ne divise pas LAD puisque $(A, Q) = 1$ et $|LD|_0 \leqslant q^{4\varrho_0} < q^\chi$ donc $S_D = 0$ et $\mathscr{A}_0''' = 0$.

Avec les hypothèses du théorème 2, si $\nu \leqslant 0{,}5\gamma$, en appliquant le lemme 23 avec $T = 1$, $G = M$, $H = D$ à la partie correspondante $\mathscr{A}_{0,1}$ de $\mathscr{A}_0$, nous obtenons

$$|\mathscr{A}_{0,1}| \leqslant C \cdot \Delta_0 \cdot q^{\omega+1}.$$

Si $0{,}5\gamma < \nu < 0{,}75\gamma$ et $r = \gamma$ en appliquant le lemme 23 avec $T = 1$, $G = D$ et $H = M$ à la partie correspondante $\mathscr{A}_{0,2}$ de $\mathscr{A}_0$ nous obtenons

$$|\mathscr{A}_{0,2}| \leqslant C \cdot \Delta_0 \cdot q^{\omega+1}$$

si $0{,}5\gamma < \nu < 0{,}75\gamma$ et $r = \gamma - 1$,

$$\mathscr{A}_{0,2} = \sum_{\substack{D \\ |D|_0 > q^{0,25\gamma-1}}} \sum_M e_0\big(Lf(DM)\big) + \sum_{\substack{D \\ |D|_0 \leqslant q^{0,25\gamma-1}}} \sum_M e_0\big(Lf(DM)\big).$$

En appliquant le lemme 23 à la première partie et le lemme 24 à la deuxième partie, nous obtenons

$$|\mathscr{A}_{0,2}| \leqslant C \cdot \Delta_0 q^{\omega+1}.$$

Si $0{,}75\gamma \leqslant \nu \leqslant r$, la partie correspondante $\mathscr{A}_{0,3}$ de $\mathscr{A}_0$ s'écrit

$$\mathscr{A}_{0,3} = \sum_{T|Q} \mu(T) S(T) \quad \text{où} \quad S(T) = \sum_D \sum_M e_0\big(Lf(DTM)\big)$$

la sommation étant faite sur les couples (D, M) tels que $D \mid F$, $|M|_0 = q^r$, $0{,}75\gamma - t \leqslant \nu \leqslant r - t$, et $|DTM - R|_0 \leqslant q^\omega$.

Si t satisfait la condition du lemme 25, nous obtenons

$$|S(T)| \leqslant C\gamma^{1,5} q^{\omega+1-t-\varrho_0}.$$

Sinon

$$|S(T)| \leqslant \gamma q^{\omega+1-t}.$$

Si ϱ est défini comme dans le lemme 23 (b), nous avons alors

$$t > 0{,}21\,\varrho/k, \qquad 0{,}2\,\varrho/k \geqslant \varrho_0 \qquad \text{et} \qquad \delta\chi \leqslant 0{,}01\,\varrho/k \qquad \text{où } \delta = 5/(100k)^2.$$

Donc

$$|S(T)| \leqslant \gamma q^{\omega+1-\varrho_0} q^{-\delta\chi}.$$

En utilisant le lemme 1, nous obtenons

$$|\mathscr{A}_{0,3}| \leqslant \sum_{t\leqslant\gamma} \sum_{|T|_0=q^t} C\gamma^{1,5} q^{\omega+1-t-\varrho_0} + \sum_{T|Q} \gamma q^{\omega+1-\varrho_0} q^{-\delta\chi}$$

et $|\mathscr{A}_{0,3}| \leqslant C\gamma^{2,5} q^{\omega+1-\varrho_0} \leqslant C\Delta_0 q^{\omega+1}$.

Nous avons donc dans tous les cas

$$|\mathscr{S}| \leqslant C\Delta_1 q^{\omega+1}.$$

Puisque $S_1 - S$, S_2 et S_3 vérifient l'inégalité ci-dessus, nous avons

$$|S| \leqslant C_6 \Delta_1 q^{\omega+1}$$

où C_6 est une constante qui ne dépend que de q.

8. Deux lemmes.

LEMME 26. *Soient $Q \in \mathscr{M}$, $A \in F_q[x]^*$ tels que $(A, Q) = 1$. Alors*

$$\sum_{\substack{H\in F_q[x]\\(H,Q)=1\\0\leqslant|H|_0<|Q|_0}} e_0\left(\frac{AH}{Q}\right) = \mu(Q).$$

Démonstration. Posons

$$\psi(A) = \sum_{\substack{H\in F_q[x]\\(H,Q)=1\\0\leqslant|H|_0<|Q|_0}} e_0\left(\frac{AH}{Q}\right).$$

Pour tout $H \in F_q[x]$ tel que $(H, Q) = 1$, et $0 \leqslant |H|_0 < |Q|_0$, il existe $K = K(H)$ unique tel que $0 \leqslant |AH + KQ|_0 < |Q|_0$. L'application $H \to U(H) = AH + KQ$ ainsi définie, est injective et $\big(U(H), Q\big) = 1$. Nous avons donc

$$\psi_A(Q) = \sum_{\substack{0\leqslant|U|_0<|Q|_0\\(U,Q)=1}} e_0\left(\frac{U}{Q}\right) = \psi_1(Q),$$

$\psi_A(Q)$ est donc indépendante de A.

Montrons que ψ_1 est multiplicative. Soient $Q_1, Q_2 \in F_q[x]$ tels que $(Q_1, Q_2) = 1$. Pour tout $H \in F_q[x]$ tel que $0 \leqslant |H|_0 < |Q_1 Q_2|_0$ et $(H, Q_1 Q_2) = 1$,

il existe (H_1, H_2) unique tel que

$$0 \leqslant |H_1|_0 < |Q_1|_0, \qquad (H_1, Q_1) = 1,$$
$$0 \leqslant |H_2|_0 < |Q_2|_0, \qquad (H_2, Q_2) = 1,$$

et $H_1Q_2 + H_2Q_1 = H$,

$$\psi_1(Q_1Q_2) = \sum_{\substack{0 \leqslant |H|_0 < |Q_1Q_2|_0 \\ (H, Q_1Q_2)=1}} e_0\left(\frac{H}{Q_1Q_2}\right)$$
$$= \sum_{\substack{0 \leqslant |H_1|_0 < |Q_1|_0 \\ 0 \leqslant |H_2|_0 < |Q_2|_0 \\ (H_1, Q_1)=1 \\ (H_2, Q_2)=1}} e_0\left(\frac{H_1Q_2 + H_2Q_1}{Q_1Q_2}\right) = \psi_1(Q_1)\cdot\psi_1(Q_2).$$

Il suffit donc de calculer $\psi_1(P^m)$ où m est un entier positif et P un polynôme de $\mathscr{M}$ irréductible,

$$\psi_1(P^m) = \sum_{\substack{0 \leqslant |H|_0 < |P^m|_0 \\ (H, P^m)=1}} e_0\left(\frac{H}{P^m}\right)$$

donc

$$\psi_1(P^m) = \sum_{0 \leqslant |H|_0 < |P^m|_0} e_0\left(\frac{H}{P^m}\right) - \sum_{0 \leqslant |H|_0 < |P^{m-1}|_0} e_0\left(\frac{HP}{P^m}\right),$$

or

$$\sum_{0 \leqslant |H|_0 < |P^n|_0}' e_0\left(\frac{H}{P^n}\right) = \begin{cases} |P|_0^n & \text{si } n = 0, \\ 0 & \text{si } n > 0. \end{cases}$$

Nous avons donc

$$\psi_1(P^m) = \begin{cases} -1 & \text{si } m = 1, \\ 0 & \text{si } m \geqslant 2, \end{cases}$$

et comme $\psi_1(1) = 1$, ψ_1 est la fonction de Möbius sur $\mathscr{M}$.

Lemme 27. *Soit ν un entier tel que $\nu \geqslant 1$. Alors*

$$\frac{e^{-2}}{\nu} \leqslant \prod_P \left(1 - \frac{1}{|P|_0}\right) \leqslant \frac{e}{\nu+1}$$

le produit étant fait sur l'ensemble des polynômes P de $\mathscr{M}$ irréductibles et de degré inférieur ou égal à ν.

Démonstration.

$$\prod_P \left(1 - \frac{1}{|P|_0}\right) = \prod_{k=1}^{\nu} \left(1 - \frac{1}{q^k}\right)^{\pi(k)}$$

D'après le lemme 20, pour $\nu \geqslant 1$

$$\prod_P \left(1-\frac{1}{|P|_0}\right) \leqslant \exp\left[q\log\left(1-\frac{1}{q}\right)+\sum_{2\leqslant k\leqslant \nu}\frac{q^k-2q^{k/2}}{k}\log(1-q^{-k})\right]$$

$$\leqslant \exp\left[\sum_{1\leqslant k\leqslant \nu}\left(-\frac{1}{k}\right)+\sum_{2\leqslant k}\frac{2q^{-k/2}}{k}\right].$$

Comme

$$\sum_{k\geqslant 2}\frac{2q^{-k/2}}{k} \leqslant \frac{1}{2}+\frac{1}{3\sqrt{2}}+\frac{1}{2}\sum_{k\geqslant 4}2^{-k/2} \leqslant 1{,}3,$$

$$\sum_{1\leqslant k\leqslant \nu}\frac{1}{k} \geqslant \log(\nu+1)+0{,}3$$

nous avons bien

$$\prod_P \left(1-\frac{1}{|P|_0}\right) \leqslant \frac{e}{\nu+1}.$$

D'autre part, nous avons

$$\prod_P \left(1-\frac{1}{|P|_0}\right) \geqslant \exp\left(\sum_{1\leqslant k\leqslant \nu}\frac{q^k}{k}\log(1-q^{-k})\right).$$

Puisque $\log(1-x) \geqslant -x-x^2$ pour $0 \leqslant x \leqslant \frac{1}{2}$

$$\prod_P \left(1-\frac{1}{|P|_0}\right) \geqslant \exp\left[\sum_{1\leqslant k\leqslant \nu}\left(-\frac{1}{k}\right)-\sum_{k\geqslant 1}\frac{q^{-k}}{k}\right].$$

Comme

$$\sum_{k\geqslant 1}\frac{q^{-k}}{k} \leqslant \frac{1}{q-1} \leqslant 1,$$

$$\sum_{1\leqslant k\leqslant \nu}\frac{1}{k} \leqslant 1+\log\nu,$$

nous avons bien

$$\prod_P \left(1-\frac{1}{|P|_0}\right) \geqslant \frac{e^{-2}}{\nu}.$$

CHAPITRE 2

Nombre de polynômes irréductibles dans une progression arithmétique

1. Relations arithmétiques sur $\mathscr{M}$.

DÉFINITION 3 [8]. Une relation d'équivalence sur $\mathscr{M}$ est dite *relation de congruence* si elle est compatible avec la structure de demi-groupe multiplicatif de $\mathscr{M}$.

Si $\mathscr{R}_H$ est la restriction à $\mathscr{M}$ de la relation „modulo H" sur $F_q[x]$ alors $\mathscr{R}_H$ est une relation de congruence sur $\mathscr{M}$ pour tout H de $\mathscr{M}$.

DÉFINITION 4 [8]. Un polynôme A de $\mathscr{M}$ est dit *inversible modulo* $\mathscr{R}$ s'il existe B de $\mathscr{M}$ tel que AB et 1 soient équivalents modulo $\mathscr{R}$ et on notera

$$AB \equiv 1 \bmod \mathscr{R}.$$

On appelle $\mathscr{G}(\mathscr{R})$ le *groupe commutatif* des classes d'équivalences inversibles du demi-groupe quotient $\mathscr{M}/\mathscr{R}$. Si $\mathscr{M}/\mathscr{R}$ est fini, on dit que $\mathscr{R}$ est *finie* et on note $g(\mathscr{R})$ l'ordre de $\mathscr{G}(\mathscr{R})$.

Nous supposons connue la théorie des caractères sur un groupe fini commutatif [9].

DÉFINITION 5 [8]. Soit $\mathscr{R}$ une relation de congruence finie sur $\mathscr{M}$. A tout caractère χ de $\mathscr{G}(\mathscr{R})$ nous associons la fonction χ à valeurs complexes définie sur $\mathscr{M}$ par:

Si A est inversible modulo $\mathscr{R}$, $\chi(A) = \chi(\bar{A})$ où $\bar{A}$ désigne la classe de A modulo $\mathscr{R}$.

Si A n'est pas inversible $\chi(A) = 0$. La fonction χ est appelée *caractère modulo* $\mathscr{R}$:

L'ensemble des caractères modulo $\mathscr{R}$ est un groupe multiplicatif isomorphe à $\mathscr{G}(\mathscr{R})$, dont l'élément neutre est noté par χ_0. χ_0 est appelé le *caractère principal modulo* $\mathscr{R}$.

DÉFINITION 6 [8]. Une relation de congruence finie $\mathscr{R}$ sur $\mathscr{M}$ est dite *arithmétique*:

s'il n'existe qu'un nombre fini de polynômes irréductibles de $\mathscr{M}$ qui ne sont pas inversibles modulo $\mathscr{R}$;

s'il existe un entier $m = m(\mathscr{R})$ tel que pour tout entier $r \geqslant m$, le nombre de polynômes de $\mathscr{M}$ de degré r soit le même dans chaque classe d'équivalence de $\mathscr{G}(\mathscr{R})$.

Dans la suite $m(\mathscr{R})$ désigne le plus petit entier m satisfaisant la propriété ci-dessus.

Soient $\mathscr{R}_1$ et $\mathscr{R}_2$ deux relations arithmétiques, alors $\mathscr{R} = \mathscr{R}_1 \cap \mathscr{R}_2$ définie par

$$A \equiv B \bmod \mathscr{R} \Leftrightarrow A \equiv B \bmod \mathscr{R}_i, \quad i = 1, 2,$$

est une relation arithmétique. Si χ_i est un caractère modulo $\mathscr{R}_i$ $(i = 1, 2)$, alors $\chi_1 \cdot \chi_2$ est un caractère modulo $\mathscr{R}$.

DÉFINITION 7 [8]. Soient $\mathscr{R}_1$ et $\mathscr{R}_2$ deux relations arithmétiques. $\mathscr{R}_1$ et $\mathscr{R}_2$ sont dites *indépendantes* si $\mathscr{G}(\mathscr{R})$ est isomorphe à $\mathscr{G}(\mathscr{R}_1) \times \mathscr{G}(\mathscr{R}_2)$ avec $\mathscr{R} = \mathscr{R}_1 \cap \mathscr{R}_2$.

Il résulte de cette définition que si $\mathscr{R}_1$ et $\mathscr{R}_2$ sont deux relations arithmétiques indépendantes, le groupe des caractères modulo $\mathscr{R}_1 \cap \mathscr{R}_2$ est l'ensemble des produits $\chi_1 \cdot \chi_2$ où χ_i est un caractère modulo $\mathscr{R}_i$ $(i = 1, 2)$.

PROPOSITION 3 [8]. *Soit k un élément de $\mathbf{N}$. Soit $\mathscr{R}_{(k)}$ la relation définie par*

$$A \equiv B \bmod \mathscr{R}_{(k)} \Leftrightarrow |x^{\deg B} \cdot A - x^{\deg A} \cdot B|_0 < q^{\deg AB - k}.$$

Les relations $\mathscr{R}_{(k)}$ et $\mathscr{R}_H$ où est un polynôme de $\mathscr{M}$ degré h sont deux relations arithmétiques indépendantes et si

$$\mathscr{R}_{(k)H} = \mathscr{R}_{(k)} \cap \mathscr{R}_H$$

nous avons

$$m(\mathscr{R}_{(k)H}) \leqslant k + h \quad \text{et} \quad g(\mathscr{R}_{(k)H}) = q^k \cdot \Phi(H).$$

2. Etude des fonctions $L(\cdot, \chi)$.

DÉFINITION 8 [8]. Soit $\mathscr{R}$ une relation arithmétique et soit χ un caractère modulo $\mathscr{R}$. La fonction $L(\cdot, \chi)$ est définie par

$$L(s, \chi) = \sum_{F \in \mathscr{M}} \chi(F) |F|_0^{-s}$$

où $s = \sigma + it$ et $\sigma > 1$.

Si $\sigma > 1$

$$L(s, \chi) = \prod_P \left(1 - \frac{\chi(P)}{|P|_0^s}\right)^{-1}$$

le produit étant étendu à tous les polynômes irréductibles de $\mathscr{M}$. La fonction $L(\cdot, \chi)$ est périodique, de période $2\pi i/\log q$.

PROPOSITION 4 [8]. *Soient $\mathscr{R}$ une relation arithmétique et χ un caractère modulo $\mathscr{R}$.*

Si $\chi \neq \chi_0$, la fonction $L(\cdot, \chi)$ est analytique dans tout le plan complexe et

$$L(s, \chi) = \sum_{\substack{|F|_0 \leqslant q^{m(\mathscr{R})-1} \\ F \in \mathscr{M}}} \chi(F)\,|F|_0^{-s}.$$

Si $\chi = \chi_0$, la fonction $L(\cdot, \chi)$ est méromorphe dans le plan complexe et ses pôles (tous d'ordre 1) sont

$$s = 1 + \frac{2l\pi i}{\log q}, \qquad l \in \boldsymbol{Z}.$$

Quel que soit χ, $L(s, \chi)$ est non nul pour $\sigma \geqslant 1$.

On peut utiliser la méthode de Siegel [7] pour donner dans le cas général une estimation uniforme du nombre de polynômes irréductibles dans une même classe d'équivalence modulo une relation arithmétique $\mathscr{R}$.

Les fonctions L ci-dessus sont à peu prés, celles pour lesquelles A. Weil a démontré l'hypothèse de Riemann. Pour la commodité du lecteur, nous précisons cette connexion dans les paragraphes qui suivent.

Je remercie ici J. P. Serre qui m'a fourni de précieuses indications pour cette démonstration.

3. Isomorphisme entre $\mathscr{G}(\mathscr{R}_{(k)H})$ et un groupe quotient du groupe des idèles de $\mathscr{F}$. Nous utiliserons les notations de Weil [18].

Soit E l'ensemble des places du corps $\mathscr{F}$. Si $v \in E$ nous noterons $\mathscr{F}_v$ le complété de $\mathscr{F}$ pour v et U_v le groupe des unités de $\mathscr{F}_v$. Si $H = P_1^{k_1} \ldots$ $\ldots P_r^{k_r}$ où les P_i sont des polynômes irréductibles unitaires distincts et où les nombres entiers k_i sont positifs, nous noterons S l'ensemble des places $v_0, v_1, \ldots, v_r$ où v_0 est la place associée à la valuation w_0 et v_i $(1 \leqslant i \leqslant r)$ est la place associée au polynôme irréductible P_i. Nous poserons $v_i(P_i) = 1$ et nous noterons $U_{v_i}^n$ $(n \in \boldsymbol{N})$ l'ensemble des éléments z de $\mathscr{F}_{v_i}$ tels que $v_i(z-1) \geqslant n$. Nous noterons $\mathscr{F}_A^*$ le groupe des idèles de $\mathscr{F}$. Nous définissons pour tout v le groupe I_v par

$$I_{v_0} = x^{\boldsymbol{Z}} \cdot U_{v_0}^{k+1},$$

$$I_v = U_v^{k_v} \quad \text{si } v \in S - \{v_0\},$$

$$I_v = U_v \quad \text{si } v \in E - S.$$

Soit $I = \prod_{v \in E} I_v \cdot I$ est alors un sous-groupe ouvert de $\mathscr{F}_A^*$.

PROPOSITION 5. *Le groupe $\mathscr{F}_A^*/\mathscr{F}^* \cdot I$ est isomorphe à $\mathscr{G}(\mathscr{R}_{(k)H})$.*

Démonstration. Notons $\mathscr{M}_i$ $(1 \leqslant i \leqslant r)$ le demi-groupe multiplicatif des polynômes de $\mathscr{M}$ premiers à P_i.

Nous définissons

$$G_0 = \mathscr{M}/\mathscr{R}_{(k)}, \qquad G_i = \mathscr{M}_i/\mathscr{R}_{P_i}k_i \quad \text{pour } 1 \leqslant i \leqslant r.$$

Nous avons alors

$$G_0 = \mathscr{G}(\mathscr{R}_{(k)}) \quad \text{et} \quad G_i = \mathscr{G}(\mathscr{R}_{P_i} k_i), \quad 1 \leqslant i \leqslant r,$$

par définition. Il est facile de vérifier que $\mathscr{G}(\mathscr{R}_{(k)H})$ est isomorphe au produit direct des groupes G_i $(0 \leqslant i \leqslant r)$. Nous noterons par θ l'isomorphisme de $\prod_{i=0}^{r} G_i$ dans $\mathscr{G}(\mathscr{R}_{(k)H})$ tel que si A est un élément de $\mathscr{M}$ premier à H alors l'image par θ^{-1} de la classe de A est le produit des classes de A dans les groupes G_i.

Soit z un élément de U_{v_i} $(1 \leqslant i \leqslant r)$. Alors z s'écrit

$$z = \sum_{n=0}^{+\infty} K_n P_i^n, \quad K_n \in F_q[x], \quad |K_n|_0 < |P_i|_0$$

et $K_0 \neq 0$. On posera $\psi_i(z)$ égal à la classe du polynôme

$$\sum_{n=0}^{k_i-1} K_n P_i^n + P_i^{k_i} \quad \text{dans } G_i.$$

Il est facile de vérifier que ψ_i est un homomorphisme surjectif dont le noyau est égal à $U_{v_i}^{k_i}$. Soit z un élément de $U_{v_0}^1$ alors z s'écrit

$$z = 1 + \sum_{n=1}^{\infty} a_n x^{-n}, \quad a_n \in F_q.$$

On posera $\psi_0(z)$ égal à la classe du polynôme $x^{k+1} + \sum_{n=1}^{k} a_n x^{k+1-n}$ dans G_0.

Alors ψ_0 est un homomorphisme surjectif dont le noyau est $U_{v_0}^{k+1}$. Pour tout v de E nous définissons une application φ_v de $\mathscr{F}_A^*$ dans $\prod_{i=0}^{r} G_i$ de la façon suivante:

Soit $z = (z_v)_{v \in E}$ un élément de $\mathscr{F}_A^*$. Nous posons

$$z_v = P_v^{n_v} \cdot z_v', \quad z_v' \in U_v \quad \text{pour } v \neq v_0,$$

$$z_{v_0} = a \cdot x^{-n_0} \cdot z_{v_0}', \quad a \in F_q^* \quad \text{et} \quad z_{v_0}' \in U_{v_0}^1, \quad \text{et} \quad y^{-1} = a \prod_{v=v_0} P_v^{n_v}.$$

Nous définissons φ_v par

$$\varphi_v(z) = \prod_{i=0}^{r} \psi_i(P_v^{n_v}) \quad \text{pour } v \notin S,$$

$$\varphi_{v_i}(z) = [\psi_i(y \cdot z_{v_i})]^{-1} \quad \text{pour } 1 \leqslant i \leqslant r,$$

$$\varphi_{v_0}(z) = [\psi_0(y \cdot z_{v_0} \cdot x^{n_0 + w_0(y)})]^{-1}.$$

Nous avons plongé ici canoniquement G_i dans $\prod_{\nu=0}^{r} G_\nu$. Puisqu'il n'y a qu'un

nombre fini de n_v différents de zéro nous poserons:

$$\varphi(z) = \prod_{v \in E} \varphi_v(z).$$

Il est clair que φ est un homomorphisme de $\mathscr{F}_A^*$ dans $\prod_{i=0}^{r} G_i$. De plus φ est surjectif car les applications ψ_i le sont. Il reste à démontrer que le noyau de φ est $\mathscr{F}^* I$. Démontrons d'abord que $\varphi(\mathscr{F}^*) = 1$. Soit $a \in \mathscr{F}^*$ alors

$$a = aP_1^{n_1} \dots P_r^{n_r} Q_1^{l_1} \dots Q_h^{l_h}$$

où les Q_i $(1 \leqslant i \leqslant h)$ sont des polynômes irréductibles unitaires distincts des P_i $(1 \leqslant i \leqslant r)$ et où $a \in F_q^*$.

Nous avons donc

$$\prod_{v \notin S} \varphi_v(a) = \prod_{i=0}^{r} \psi_i(Q_1^{l_1} \dots Q_h^{l_h}),$$

$$\prod_{1 \leqslant i \leqslant r} \varphi_{v_i}(a) = \prod_{i=1}^{r} \psi_i(Q_1^{l_1} \dots Q_h^{l_h})^{-1}$$

et

$$\varphi_{v_0}(a) = \psi_0(Q_1^{l_1} \dots Q_h^{l_h} x^t)^{-1} \qquad \text{où } t = \deg(Q_1^{l_1} \dots Q_h^{l_h}).$$

Nous avons donc $\varphi(a) = 1$.

Soit $z \in \mathscr{F}_A^*$ tel que $\varphi(z) = 1$. De même que précédemment nous avons

$$z_v = P_v^{n_v} \cdot z_v', \qquad v \neq v_0,\ z_v' \in U_v$$

et

$$z_{v_0} = a \cdot x^{-n_0} \cdot z_{v_0}' \qquad a \in F_q^*,\ z_{v_0}' \in U_{v_0}^1.$$

Posons $a = a \cdot \prod_{v \neq v_0} P_v^{n_v}$ et $u = z \cdot a^{-1}$.

Nous avons donc $U_v \in u_v$ si $v \neq v_0$ et $u_{v_0} \in x^{\mathbf{Z}} \cdot U_{v_0}^1$.

Puisque $\varphi(a) = 1$ nous avons $\varphi(u) = 1$.

De plus $\prod_{v \notin S} \varphi_v(u) = 1$ donc $\prod_{v \in S} \varphi_v(u) = 1$.

Nous devons donc avoir $u_v \in I_v$ pour tout v de S puisque le produit $\prod_{i=0}^{r} G_i$ est direct ce qui termine la démonstration.

4. Fonctions L_ω lorsque ω est un quasi caractère des classes d'idèles.

DÉFINITION 10 [18]. Un quasi-caractère ω du groupe des classes d'idèles $\mathscr{F}_A^*/\mathscr{F}^*$ est une représentation continue de $\mathscr{F}_A^*/\mathscr{F}^*$ dans C^* (On l'identifie avec une représentation continue de $\mathscr{F}_A^*$ dans C^* triviale sur $\mathscr{F}^*$.) ω est dit *principal* s'il est trivial sur le sous-groupe compact maximal de $\mathscr{F}_A^*/\mathscr{F}^*$. ω induit sur $\mathscr{F}_v^*$ un quasi-caractère ω_v. On note $f(v)$ le plus petit entier f tel que ω_v soit trivial sur U_v^f. Si $f(v) = 0$, ω est dit

non ramifié en v. Le diviseur $D_\omega = \sum_v f(v)\cdot v$ est appelé le *conducteur* de ω. On pose $\omega(v) = \omega_v(P_v)$ et l'on définit la fonction L_ω par

$$L_\omega(s) = \prod_v \left(1-\omega(v)q^{-s\deg v}\right)^{-1}$$

avec $s = \sigma+it$, $\sigma > 1$, où le produit est effectué sur toutes les places v où ω n'est pas ramifié. $\deg(v) = \deg(P_v)$ si $v \neq v_0$ et $\deg(v_0) = 1$.

THÉORÈME 3. *Soit χ un caractère non principal modulo $\mathscr{R}_{(k)H}$ alors il existe un quasi-caractère ω non principal de $\mathscr{F}_A^*$ trivial sur $\mathscr{F}^*\cdot I$ tel que:*

$$L(s,\chi) = L_\omega(s)\prod_{v\in S}(1-\varepsilon_v q^{-s\deg v})$$

où $|\varepsilon_v| = 0$ *ou* 1.

Démonstration. Posons $\psi = \theta\circ\varphi$. Si χ est un caractère de $\mathscr{G}(\mathscr{R}_{(k)H})$ nous posons $\omega = \chi\circ\psi$. L'application $\chi \to \chi\circ\psi$ est alors un isomorphisme entre le groupe des caractères de $\mathscr{G}(\mathscr{R}_{(k)H})$ et le groupe des quasi-caractères de $\mathscr{F}_A^*$ dont le noyau contient $\mathscr{F}^*\cdot I$. Nous remarquons que tout quasi-caractère de $\mathscr{F}_A^*$ dont le noyau contient $\mathscr{F}^*\cdot I$ et qui n'est pas le caractère unité ne peut être principal. En effet soit ω un quasi-caractère tel que $\omega(\mathscr{F}^*\cdot I) = 1$. Si ω est principal $\omega(\mathscr{F}^*\cdot\prod U_v) = 1$ donc $\omega(\mathscr{F}^*\cdot I\cdot\prod U_v) = 1$.

Mais le groupe $\mathscr{F}^*\cdot I\cdot\prod U_v$ est égal au groupe $\mathscr{F}^*\cdot\mathscr{F}_0^*\prod_{v\neq v_0} U_v$ qui est égal à $\mathscr{F}_A^*$. Donc ω est le caractère unité.

Si $v\notin S$ nous avons $\chi(P_v) = \omega(v)$. L'égalité du théorème est vraie avec $\varepsilon_v = 0$ si $v\in S$ et si ω est ramifié en v et $\varepsilon_v = \omega(v)$ si ω est ramifié en v.

5. Théorie du corps de classes et fonctions L_ω. Soit $\overline{\mathscr{F}}$ une clôture algébrique de $\mathscr{F}$ et $\mathscr{F}_{ab}$ l'extension abélienne maximale de $\mathscr{F}$ dans $\overline{\mathscr{F}}$. Soit L une extension de $\mathscr{F}$ et posons:

$$N(L) = \mathscr{F}^*\cdot N_{L/\mathscr{F}}(L_A^*)$$

où L_A^* désigne le groupe des idèles de L et $N_{L/\mathscr{F}}$ la norme de L_A^* dans $\mathscr{F}_A^*$. Alors d'après [18] (corollaire 2 du théorème 7, p. 276) l'application $L\mapsto N(L)$ est une bijection de l'ensemble des sous-corps de $\mathscr{F}_{ab}$ de degré fini sur $\mathscr{F}$ sur les sous-groupes ouverts de $\mathscr{F}_A^*$ d'indice fini dans $\mathscr{F}_A^*$ et contenant $\mathscr{F}^*$. Il existe donc un sous-corps L de $\mathscr{F}_{ab}$ de degré fini sur $\mathscr{F}$ tel que:

$$N(L) = \mathscr{F}^*\cdot I.$$

Le corps de base F_q peut a priori s'agrandir dans E. Soit $F_{q'}$ ce nouveau corps et K le corps $F_{q'}\mathscr{F}$. Nous avons alors $\mathscr{F}\subset K\subset L$. Puisque le groupe des quasi-caractères de $\mathscr{F}_A^*$ triviaux sur $\mathscr{F}^*I$ et principaux est réduit

au quasi-caractère unité cela signifie qu'il n'y a pas d'extension du corps des constantes F_q donc $F_{q'} = F_q$ et $K = \mathscr{F}$.

Soit ζ_L et $\zeta_{\mathscr{F}}$ les fonctions zeta de Dedekind des corps L et $\mathscr{F}$ respectivement. Puisqu'il n'y a pas d'extension du corps des constantes, d'après [18] (théorème 4, p. 130) les fonctions ζ_L et $\zeta_{\mathscr{F}}$ ont les mêmes pôles. Soit Γ le groupe des quasi-caractères de $\mathscr{F}_A^*$ triviaux sur $\mathscr{F}^* \cdot I = N(L)$ et soit ω_0 le quasi-caractère unité. Alors $L_{\omega_0} = \zeta_{\mathscr{F}}$. D'après [18] (théorème 10, p. 180)

$$\zeta_L(s) = \prod_{\omega \in \Gamma} L_\omega(s).$$

D'après [19] (p. 64 et p. 70) ζ_L vérifie l'hypothèse de Riemann c'est-à-dire que ses zéros α vérifient $|\alpha| \leqslant \frac{1}{2}$. Nous avons

$$\prod_{\substack{\omega \in \Gamma \\ \omega \neq \omega_0}} L_\omega(s) = \zeta_L(s)\zeta_{\mathscr{F}}^{-1}(s).$$

ζ_L et $\zeta_{\mathscr{F}}$ ayant les mêmes pôles il est clair que chaque fonction L_ω ($\omega \neq \omega_0$) vérifie l'hypothèse de Riemann et il en est de même pour les fonctions $L(\cdot, \chi)$.

6. Nombre de polynômes irréductibles dans une progression arithmétique. Nous supposons dans ce paragraphe que $k+h \geqslant 1$ ($h = \deg H$).

Soit K un polynôme de $\mathscr{M}$ inversible modulo la relation $\mathscr{R}_{(k)H}$ et posons

$$f(G) = 1 \quad \text{si } G \in \mathscr{M} \text{ et } G \equiv K \bmod \mathscr{R}_{(k)H},$$
$$f(G) = 0 \quad \text{sinon.}$$

Si $\pi(\gamma, H, k; K)$ désigne le nombre de polynômes irréductibles unitaires de degré γ qui sont congrus à K modulo $\mathscr{R}_{(k)H}$ nous avons:

$$\pi(\gamma, H, k; K) = \sum_{|P|_0 = q^\gamma} f(P).$$

Soient χ_i ($0 \leqslant i \leqslant g(\mathscr{R}_{(k)H}) - 1$) les caractères modulo $\mathscr{R}_{(k)H}$, χ_0 étant le caractère principal.

Posons $\pi(\gamma, \chi_i) = \sum_{|P|_0 = q^\gamma} \chi_i(P)$. Il vient:

$$\pi(\gamma, H, k; K) = \frac{1}{q^k \Phi(H)} \sum_{i=0}^{g(\mathscr{R})-1} \overline{\chi_i}(K)\pi(\gamma, \chi_i).$$

D'après la proposition 3 et le paragraphe précédent nous pouvons écrire si $\chi_i \neq \chi_0$

$$L(s, \chi_i) = \prod_{j=1}^{k+h-1} (1 - a_j T) \quad \text{avec } T = q^{-s}$$

et $|a_j| \leqslant q^{1/2}$.

Nous obtenons alors en prenant la différentielle du logarithme

$$d\big(\operatorname{Log} L(s, \chi_i)\big) = -\sum_{n=1}^{\infty}\sum_{j=1}^{k+h-1} a_j^n \cdot T^n \frac{dT}{T},$$

$$d\big(\operatorname{Log} L(s, \chi_i)\big) = \sum_{n=1}^{\infty}\sum_{|G|_0=q^n} \Lambda_0(G)\,\chi_i(G)\cdot T^n \frac{dT}{T}$$

avec

$$\begin{aligned}\Lambda_0(G) &= \deg(P) \qquad \text{si } G = P^l \text{ et } P \text{ irréductible},\\ &= 0 \qquad\qquad \text{sinon}.\end{aligned}$$

Nous en déduisons par identification:

$$\Big|\sum_{\substack{|G|_0=q^\gamma\\ G\in M}} \Lambda_0(G)\,\chi_i(G)\Big| = \Big|\sum_{j=1}^{k+h-1} a_j^\gamma\Big|$$

donc

$$\begin{aligned}\Big|\gamma \sum_{|P|_0=q^\gamma} \chi_i(P)\Big| &\leqslant (k+h-1)\,q^{\gamma/2} + \sum_{\substack{j|\gamma\\ j\geqslant 2}} \frac{\gamma}{j} \sum_{|P|_0=q^{\gamma/j}} 1\\ &\leqslant (k+h-1)\,q^{\gamma/2} + \sum_{\substack{j|\gamma\\ j\geqslant 2}} q^{\gamma/j}\end{aligned}$$

d'après le lemme 20.

Nous avons donc pour $i \neq 0$

$$|\pi(\gamma, \chi_i)| \leqslant \frac{k+h-1+\gamma-1}{\gamma}\, q^{\gamma/2},$$

donc

$$\left|\pi(\gamma, H, k;\ K) - \frac{\pi(\gamma, \chi_0)}{q^k \Phi(H)}\right| \leqslant \frac{k+h-1+\gamma-1}{\gamma}\, q^{\gamma/2}.$$

Mais nous avons $|\pi(\gamma, \chi_0) - \pi(\gamma)| \leqslant r$. Il vient alors:

$$\begin{aligned}&\left|\pi(\gamma, H, k;\ K) - \frac{q^\gamma}{\gamma q^k \Phi(H)}\right|\\ &\qquad\leqslant \frac{k+h-1+\gamma-1}{\gamma}\, q^{\gamma/2} + \frac{r}{q^k \Phi(H)} + \frac{q^\gamma}{\gamma} - \pi(\gamma).\end{aligned}$$

Nous avons:

$$\Phi(H) = \prod_{i=1}^{r} |P_i|_0^{k_i-1}(|P_i|_0 - 1) \geqslant 2^{r-2}$$

car $|P_i|_0 - 1 \geqslant 2$ sauf si $q = 2$ et $P_i = x$ ou $x+1$.

Pour $\gamma \geqslant 4$, $\dfrac{r}{q^k \Phi(H)} \leqslant 2 \leqslant \frac{1}{2} q^{\gamma/2}$ et $\dfrac{q^\gamma}{\gamma} - \pi(\gamma) \leqslant \dfrac{2}{\gamma} q^{\gamma/2}$ d'après le lemme 20. Pour $1 \leqslant \gamma \leqslant 3$ nous avons:

$$\pi(1) = q, \quad \frac{q^2}{2} - \pi(2) = \tfrac{1}{2} q \quad \text{et} \quad \frac{q^3}{3} - \pi(3) = \tfrac{1}{3} q.$$

Nous obtenons alors le théorème

THÉORÈME 4. *Si* $k+h \geqslant 1$

$$\left| \pi(\gamma, H, k;\ K) - \frac{q^\gamma}{\gamma q^k \Phi(H)} \right| \leqslant (k+h+1)\, q^{\gamma/2}.$$

CHAPITRE 3

Equirépartition modulo 1 des suites $(f(P_n))_{n\geqslant 1}$

PROPOSITION 6. *Soit a un élément de $\mathscr{F}_0-\mathscr{F}$. Il existe alors un entier $r(a)$ tel que pour tout entier $r\geqslant r(a)$ on ait*

$$a=\frac{A}{Q}+\frac{\theta}{Q\tau}$$

avec $A\in F_q[x]^*$, $Q\in\mathscr{M}$, $\theta\in\mathscr{P}$ tels que

$$(A,Q)=1,\qquad |\tau|_0=q^r\qquad \text{et}\qquad q\leqslant |Q|_0\leqslant|\tau|_0.$$

De plus, le couple (A,Q) est unique pour r fixé.

Démonstration. D'après la théorie des fractions continues dans $\mathscr{F}_0$ [11]

$$a=\frac{A_n}{Q_n}+\frac{(-1)^n}{Q_n(Q_{n+1}+\theta_{n+1}Q_n)},\qquad n\geqslant 0,$$

où $\theta_{n+1}\in\mathscr{P}$, $A_n, Q_n\in F_q[x]^*$, $(A_n,Q_n)=1$ et $|Q_n|_0<|Q_{n+1}|_0$. Il existe donc (si $|Q_1|_0=q^{r(a)}$) un entier n unique tel que $|Q_n|_0\leqslant q^r<|Q_{n+1}|_0$. Nous prenons alors

$$\tau=x^r,\qquad Q=\frac{1}{a}Q_n,\qquad A=\frac{1}{a}A_n\qquad\text{et}\qquad \theta=\frac{(-1)^n x^r}{Q_{n+1}+\theta_{n+1}Q_n}$$

(a étant le coefficient du monôme de plus haut degré de Q_n).

Puisque le développement en fraction continue de a est unique, le couple (A,Q) est unique pour r fixé.

LEMME 28. *Soit $Q\in\mathscr{M}$ de degré $\chi\geqslant 1$, alors*

$$\Phi(H)\geqslant\frac{|H|_0}{\chi e^2}.$$

Démonstration. Soit $H=P_1^{k_1}\dots P_r^{k_r}$ où les P_i sont irréductibles distincts. Alors

$$\frac{\Phi(H)}{|H|_0}=\prod_{i=1}^{r}\left(1-\frac{1}{|P_i|_0}\right).$$

D'après le lemme 27

$$\prod_{|P|_0 \leqslant q^\chi} \left(1 - \frac{1}{|P|_0}\right) \geqslant \frac{e^{-2}}{\chi},$$

donc

$$\frac{\Phi(H)}{|H|_0} \geqslant \prod_{|P|_0 \leqslant q^\chi} \left(1 - \frac{1}{|P|_0}\right) \geqslant \frac{e^{-2}}{\chi},$$

ce qui démontre le lemme.

LEMME 29 [12]. *Soit* $\Theta = (\theta_n)$, $n \geqslant 1$, *une suite d'éléments de* $\mathscr{F}_0$ *telle que*

$$\left|\sum_{n=1}^{N} e_0(H\theta_n)\right| \leqslant a(N)N$$

pour tout $H \in F_q[x]$ *et* $0 < |H|_0 \leqslant q^{b(N)}$.

Alors

$$D_N(\Theta) \leqslant q^{1-b(N)} + a(N).$$

Démonstration. Soit $\mathscr{B} = a + \mathscr{P}^b$ une boule contenue dans $\mathscr{P}$. Il est facile de vérifier que

$$\eta_{\mathscr{B}}(\mathscr{H}_0(\theta)) = q^{1-b} \sum_{\substack{|H|_0 \leqslant q^{b-2} \\ H \in F_q[x]}} e_0(H(\theta - a))$$

où $\eta_{\mathscr{B}}$ est la fonction caractéristique de $\mathscr{B}$.

Nous avons donc

$$R_N(\mathscr{B}, \Theta) = q^{1-b} \sum_{\substack{0 < |H|_0 \leqslant q^{b-2} \\ H \in F_q[x]}} \sum_{n=1}^{N} e_0(H(\theta_n - a))$$

et

$$|R_N(\mathscr{B}, \Theta)| \leqslant q^{1-b} \sum_{0 < |H|_0 \leqslant q^{b-2}} \left|\sum_{n=1}^{N} e_0(H\theta_n)\right|.$$

Si $b \leqslant b(N) + 2$, nous obtenons

$$|R_N(\mathscr{B}, \Theta)| \leqslant q^{1-b} \sum_{0 < |H|_0 \leqslant q^{b-2}} N \cdot a(N) \leqslant Na(N).$$

Si $b > b(N) + 2$, la boule $\mathscr{B}$ est contenue dans la boule $\mathscr{B}_0 = a + \mathscr{P}^{b_0}$ où $b_0 = [b(N) + 2]$. Nous avons

$$R_N^2(\mathscr{B}, \Theta) - R_N^2(\mathscr{B}_0, \Theta) = F_N^2(\mathscr{B}, \Theta) - F_N^2(\mathscr{B}_0, \Theta) + N^2 \operatorname{mes}^2 \mathscr{B} - \\ - N^2 \operatorname{mes}^2 \mathscr{B}_0 - 2N \operatorname{mes} \mathscr{B} \cdot F_N(\mathscr{B}, \Theta) + 2N \operatorname{mes} \mathscr{B}_0 F_N(\mathscr{B}_0, \Theta).$$

Puisque

$$0 \leqslant F_N(\mathscr{B}, \Theta) \leqslant F_N(\mathscr{B}_0, \Theta) \leqslant |R_N(\mathscr{B}_0, \Theta)| + N \operatorname{mes} \mathscr{B}_0,$$

$$0 < \operatorname{mes} \mathscr{B} \leqslant \operatorname{mes} \mathscr{B}_0, \quad \text{et} \quad |R_N(\mathscr{B}_0, \Theta)| \leqslant Na(N),$$

nous obtenons

$$R_N^2(\mathscr{B}, \Theta) \leqslant N^2 a^2(N) + 2N \operatorname{mes} \mathscr{B}_0 \big(Na(N) + N \operatorname{mes} \mathscr{B}_0\big)$$

donc

$$|R_N(\mathscr{B}, \Theta)| \leqslant N\big(a(N) + 2q^{-1-[b(N)]}\big) \leqslant N\big(a(N) + q^{1-b(N)}\big).$$

Nous avons donc

$$|R_N(\mathscr{B}, \Theta)| \leqslant N\big(a(N) + q^{1-b(N)}\big)$$

pour toute boule $\mathscr{B} \subset \mathscr{P}$, ce qui démontre le lemme.

PROPOSITION 9. *Soit (G_n), $n \geqslant 1$, la suite croissante des éléments de $\mathscr{M}$. Alors la suite $(G_n a)$, $n \geqslant 1$, est équirépartie modulo 1 dans $\mathscr{F}_0$ si et seulement si $a \in \mathscr{F}_0 - \mathscr{F}$.*

Ce résultat a été démontré par une autre méthode par Dijksma [4].

Démonstration. Si $a \in \mathscr{F}$, $a = A/Q$ avec $Q \in F_q[x]^*$. En prenant $H = Q$ dans le critère de Weyl, nous obtenons

$$\sum_{n=1}^{N} e_0\left(\frac{A}{Q} G_n Q\right) = N$$

donc la suite $(G_n a)$, $n \geqslant 1$, n'est pas équirépartie modulo 1. Si $a \notin \mathscr{F}$, alors $Ha = \beta \notin \mathscr{F}$ quand $H \in F_q[x]^*$. Montrons que pour tout $\varepsilon > 0$, il existe $N_0(\beta, \varepsilon)$ tel que si $N \geqslant N_0$, alors

$$\Big|\sum_{n=1}^{N} e_0(\beta G_n)\Big| \leqslant \varepsilon N.$$

Il existe $N_0(\beta)$ tel que si $N \geqslant N_0(\beta)$, en posant $\omega = [\gamma/2]$:

$$|G_N|_0 = q^\gamma, \qquad \beta = \frac{A}{Q} + \frac{\theta}{Q\tau}$$

avec $\theta \in \mathscr{P}$, $A, Q \in F_q[x]^*$, $|\tau|_0 = q^\omega$, $|Q|_0 = q^\chi$ et $1 \leqslant \chi \leqslant \omega$ et $(A, Q) = 1$. Pour $\omega + 1 \leqslant \nu \leqslant \gamma$, nous partageons les polynômes de $\mathscr{M}$ de degré ν en $q^{\nu-\omega-1}$ boules disjointes de centre R et de rayon q^ω. Nous avons alors

$$\Big|\sum_{n=1}^{N} e_0(\beta G_n)\Big| \leqslant \sum_{|G|_0 \leqslant q^\omega} 1 + \sum_{\omega+1 \leqslant \nu \leqslant \gamma-1} q^{\nu-\omega-1} \max_{|R|_0 = q^\nu} \Big|\sum_{|G-R|_0 \leqslant q^\omega} e_0(\beta G)\Big| + \\ + \sum_{i=1}^{l-1} \Big|\sum_{|G-R_i|_0 \leqslant q^\omega} e_0(\beta G)\Big| + q^{\omega+1}$$

où $R_1, \ldots, R_{l-1}$ et R_l sont les centres des boules contenant des polynômes G_n de degré γ avec $n \leqslant N$. Nous avons $l \leqslant q^{\gamma-\omega-1}$ et

$$\Big|\sum_{|G-R| \leqslant q^\omega} e_0(\beta G)\Big| = \Big|\sum_{|X|_0 \leqslant q^\omega} e_0\left(\frac{AX}{Q}\right)\Big| = 0$$

car

$$\left|\frac{\theta(G-R)}{Q\tau}\right|_0 \leqslant q^{-2} \quad \text{si } |G-R|_0 \leqslant q^{\omega}.$$

Nous obtenons

$$\left|\sum_{n=1}^{N} e_0(\beta G_n)\right| \leqslant 2q^{\omega+1} \leqslant 2q\sqrt{N}$$

Il suffit donc de prendre $N_0(\beta, \varepsilon)$ tel que

$$N_0(\beta, \varepsilon) > N_0(\beta) \quad \text{et} \quad 2q^2 \leqslant \varepsilon\sqrt{N_0(\beta, \varepsilon)}$$

THÉORÈME 5. *Soient: N un entier positif; γ un entier tel que $|P_N|_0 = q^{\gamma}$: χ un entier tel que $\max(\chi, \gamma-\chi) \leqslant y < \gamma$; ϱ_0 le réel défini par $0,2\chi$ si $\chi \leqslant \gamma/4$, $0,05\gamma$ si $\gamma/4 \leqslant \chi \leqslant 3\gamma/4$, $0,2(\gamma-\chi)$ si $3\gamma/4 \leqslant \chi < \gamma$; $\Delta_1 = \exp(110\log^2\gamma)q^{-\varrho_0}$; $A \in F_q[x]^*$, $Q \in \mathscr{M}$, $\theta \in \mathscr{P}$ et $a, \tau \in \mathscr{F}_0$ tels que $(A, Q) = 1$, $|Q|_0 = q^{\chi}$, $|\tau|_0 = q^{y}$ et $a = \dfrac{A}{Q} + \dfrac{\theta}{Q\tau}$.*

Alors $D_N\big((P_n a)_{n\geqslant 1}\big) \leqslant c_7\gamma\Delta_1$, où c_7 est une constante qui ne dépend que de q.

THÉORÈME 6. *Soient: N un entier positif; k un entier tel que $2 \leqslant k \leqslant p-1$; γ un entier tel que $|P_N|_0 = q^{\gamma}$; $a_0, a_1, \ldots, a_k \in \mathscr{F}_0$ tels qu'il existe un entier s, $2 \leqslant s \leqslant k$, pour lequel $a_s = \dfrac{A}{Q} + \dfrac{\theta}{Q\tau}$, où $Q \in \mathscr{M}$, $A \in F_q[x]^*$, $(A, Q) = 1$, $|Q|_0 = q^{\chi}$, $\theta \in \mathscr{P}$, $|\tau|_0 = q^{y}$, $s\gamma > y \geqslant [s\gamma/2 + \gamma/4]$ et $\log^3\gamma \leqslant \chi \leqslant s\gamma/2 + \gamma/4$; ϱ_0 le réel défini par $\dfrac{0,05\gamma}{k^2(2+\log k)}$ si $\gamma/4 \leqslant \chi \leqslant s\gamma/2 + \gamma/4$, $\dfrac{0,2\chi}{k^2\big(2+\log(k\sqrt{\gamma/\chi})\big)}$ si $\chi < \gamma/4$; $\Delta_1 = \exp\,(110\,\log^2\gamma)q^{-\varrho_0}$.*

Alors si $f(X) = a_k X^k + \quad + a_1 X + a_0$

$$D_N\big((f(P_n))_{n\geqslant 1}\big) \leqslant c_7\gamma\Delta_1.$$

Démonstration des théorèmes 5 et 6. Prenons $\omega = \gamma - [\varrho_0]$ $L \in F_q[x]^*$, $|L|_0 \leqslant q^{\varrho_0}$. Il existe l polynômes de $\mathscr{M}$ de degré γ, $R_1, \ldots, R_l$ tels que $R_1 < R_2 < \ldots < R_l$, $|R_i - R_{i+1}|_0 > q^{\omega}$ et tels que la réunion des boules de centre R_i et de rayon q^{ω} contiennent tous les polynômes P_n tels que $1 \leqslant n \leqslant N$ et $|P_n|_0 = q^{\gamma}$. En outre, $|P_N - R_l|_0 \leqslant q^{\omega}$. En utilisant les théorèmes 1 et 2 et en posant dans le cas du théorème 5 $f(X) = aX$, nous obtenons si $\log\gamma \geqslant k^{100}$:

$$\left|\sum_{n=1}^{N} e_0\big(Lf(P_n)\big)\right| \leqslant \left|\sum_{|P_n|_0 \leqslant q^{\gamma-1}} e_0\big(Lf(P_n)\big)\right| + \\ + \sum_{i=1}^{l-1}\left|\sum_{|P-R_i|_0 \leqslant q^{\omega}} e_0\big(Lf(P)\big)\right| + \sum_{\substack{|P_n-R_l|_0 \leqslant q^{\omega} \\ n\leqslant N}} 1$$

soit

$$\Big|\sum_{n=1}^{N} e_0(Lf(P_n))\Big| \leqslant c_6 \Delta_1 q^{\gamma} + c_6 \Delta_1 q^{\gamma} + q^{\omega+1} \leqslant c_6' \gamma N \Delta_1$$

car $\pi(\gamma-1) \leqslant N$. Nous obtenons donc le résultat en utilisant le lemme 51.

COROLLAIRE. *Soit f un polynôme à coefficients dans $\mathscr{F}_0$, de degré k $(2 \leqslant k < p)$*

$$f(X) = a_0 + a_1 X + \ldots + a_k X^k.$$

S'il existe un entier s $(2 \leqslant s \leqslant k)$ tel que $a_s \notin \mathscr{F}$ et tel que, si $(A_i)_{i \geqslant 1}$ désigne le développement en fraction continue de a_s, la suite A_i soit bornée, alors la suite $(f(P_n))_{n \geqslant 1}$ est équirépartie modulo 1 dans $\mathscr{F}_0$.

THÉORÈME 7. *La suite $(P_n a)$, $n \geqslant 1$, est équirépartie modulo 1 si et seulement si $a \notin \mathscr{F}$.*

Démonstration. Si $a \in \mathscr{F}$ il est clair que la suite $(P_n a)_{n \geqslant 1}$ n'est pas équirépartie modulo 1. Si $a \notin \mathscr{F}$ et si $L \notin F_q[x]^*$ alors $La \notin \mathscr{F}$. Il suffit de montrer que si $a \notin \mathscr{F}$

$$\lim_{N \to +\infty} \frac{1}{N} \Big| \sum_{n=1}^{N} e_0(aP_n) \Big| = 0.$$

Soit ε tel que $0 < \varepsilon < 1$. Nous montrerons qu'il existe $N_0(a, \varepsilon)$ tel que pour $N \geqslant N_0(a, \varepsilon)$ on ait

$$\frac{1}{N} \Big| \sum_{n=1}^{N} e_0(aP_n) \Big| < \varepsilon.$$

Il existe $\gamma_1(a, \varepsilon) \geqslant 10$ tel que si $\gamma \geqslant \gamma_1(a, \varepsilon)$ les propriétés suivantes sont vérifiées:

(1) $$a = \frac{A}{Q} + \frac{\theta}{Q\tau}, \quad A \in F_q[x]^*, \quad Q \in \mathscr{M}, \quad (A, Q) = 1, \quad \theta \in \mathscr{P},$$

$$|\tau|_0 = q^{\gamma - [\gamma^{0,01}]}, \ |Q|_0 = q^{\chi} \quad \text{avec } 1 < \chi \leqslant \gamma - [\gamma^{0,01}],$$

(2) $$1 \leqslant 0{,}2\gamma^{0,01} \leqslant 0{,}05\gamma,$$

(3) $$\pi(\gamma-1) \geqslant \frac{q^{\gamma-1}}{2\gamma}$$

(ceci est possible car d'après le lemme 20 $\pi(\gamma-1) \geqslant \dfrac{1}{\gamma-1}(q^{\gamma-1} - 2q^{(\gamma-1)/2})$);

(4) $$2(2C_6+1)\gamma q^{3+110\log^2\gamma - 0{,}2\gamma^{0,01}} < \varepsilon$$

(où C_6 est la constance du théorème 1)

$$(5) \qquad 4\gamma q^{3-\gamma^{0,01}} + \frac{(1+2q)e^2\chi}{|Q|_0} + 6q\cdot\gamma^3\cdot q^{\gamma^{0,01}-0,5\gamma} < \varepsilon$$

(ceci est possible car $\lim\limits_{\gamma\to+\infty} |Q|_0 = +\infty$).

Nous supposerons que N est tel que $|P_N|_0 = q^\gamma$ et $\gamma \geqslant \gamma_1(\alpha, \varepsilon)$.

(a) Supposons que

$$\gamma^{0,01} \leqslant \chi \leqslant \gamma - [\gamma^{0,01}].$$

Posons $\omega = \gamma - [0{,}2\gamma^{0,01}]$. D'après (2)

$$\gamma - \varrho_0 \leqslant \omega < \gamma.$$

De même que dans la démonstration des théorèmes 5 et 6 nous obtenons:

$$\Big|\sum_{n=1}^{N} e_0(\alpha P_n)\Big| \leqslant 2C_6\Delta_1 q^\gamma + q^{\omega+1} \leqslant (2C_6+1)q^{\gamma+2-0,2\gamma^{0,01}+110\log^2\gamma}.$$

D'après (3)

$$N \geqslant \pi(\gamma-1) \geqslant \frac{q^{\gamma-1}}{2\gamma}$$

donc

$$\Big|\sum_{n=1}^{N} e_0(\alpha P_n)\Big| \leqslant 2(2C_6+1)\gamma q^{3+110\log^2\gamma-0,2\gamma^{0,01}}\cdot N < \varepsilon N$$

d'après (4).

(b) Supposons que

$$\chi < \gamma^{0,01}.$$

Posons:

$$\omega = \gamma - [\gamma^{0,01}].$$

Nous avons

$$\gamma - \gamma^{1-0,02} \leqslant \omega < \gamma.$$

Nous effectuons sur les polynômes unitaires de degré ν $(\omega < \nu \leqslant \gamma)$ une partition en boules de rayon q^ω. Si R est de degré ν, $\omega < \nu \leqslant \gamma$ et si $|P-R|_0 \leqslant q^\omega$, nous avons

$$e_0(P\alpha) = e_0\left(\frac{AP}{Q}\right) e_0\left(\frac{R\theta}{Q\tau}\right)$$

car $\dfrac{\theta(P-R)}{Q\tau} \in \mathscr{P}^2$. Nous avons alors

$$\Big|\sum_{|P-R|_0\leqslant q^\omega} e_0(aP)\Big| = \Big|\sum_{|P-R|_0\leqslant q^\omega} e_0\Big(\frac{AP}{Q}\Big)\Big|$$
$$= \Big|\sum_{\substack{(L,Q)=1\\ |L|_0<|Q|_0}} \pi(R, Q, [\gamma^{0,01}]; L)\, e_0\Big(\frac{AL}{Q}\Big)\Big|$$

où $\pi(R, Q, k; L)$ désigne le nombre de polynômes irréductibles P tels que $|P-R|_0 \leqslant q^{\nu-k}$ et $P \equiv L \bmod Q$.

D'après le théorème 4

$$\Big|\pi(R, Q, \nu-\omega-1, L) - \frac{\pi(\nu)}{\Phi(Q)\, q^{\nu-\omega-1}}\Big| \leqslant 3\gamma\cdot q^{\nu/2}.$$

D'après le lemme 26

$$\Big|\sum_{|P-R|_0\leqslant q^\omega} e_0(aP)\Big| \leqslant \frac{\pi(\nu)}{\Phi(Q)\, q^{\nu-\omega-1}} + 3\,\Phi(Q)\,\gamma\cdot q^{\nu/2}$$

et

$$\Big|\sum_{n=1}^{N} e_0(aP_n)\Big| \leqslant 2q^{\omega+1} + \sum_{\omega<\nu\leqslant\gamma} \frac{\pi(\nu)}{\Phi(Q)} + 3\gamma\,\Phi(Q)\, q^{0,5\gamma+\gamma^{0,01}}).$$

Nous avons

$$\sum_{\omega<\nu\leqslant\gamma-1} \pi(\nu) < N \quad \text{et} \quad \pi(\gamma) \leqslant \frac{q^\gamma}{\gamma} \leqslant 2qN$$

donc

$$\Big|\sum_{n=1}^{N} e_0(aP_n)\Big| \leqslant (4\gamma q^{3-\gamma^{0,01}} + \frac{1+2q}{\Phi(Q)} + 6q\gamma^3 q^{\gamma^{0,01}-0,5\gamma})\, N$$

soit

$$\Big|\sum_{n=1}^{N} e_0(aP_n)\Big| < \varepsilon N$$

d'après le lemme 28 et la condition (5).

Remarque. Dans le théorème 6, nous ne pouvons pas supprimer la condition $k \leqslant p-1$. En effet, d'après Dijksma [5], il existe $a \in \mathscr{F}_0 - \mathscr{F}$ tel que pour toute suite $(H_n)_{n\geqslant 1}$ d'éléments de $F_q[x]$, la suite $(H_n^p a)_{n\geqslant 1}$ ne soit pas équirépartie modulo 1 dans $\mathscr{F}_0$.

Prenons $a = \sum_{j=1}^{\infty} x^{-p^j}$ Alors a est algébrique et satisfait l'équation $x^p Y^p - x^p Y + 1 = 0$. Cette équation n'a pas de solutions dans $\mathscr{F}$. a est

donc irrationnel. Soit $H \in F_q[x]$, $H = \sum_{k=0}^{n} a_k x^k$, alors $H^P = \sum_{k=0}^{n} (a_k)^p \times x^{kp}$ et $aH^p = \sum_{j=1}^{\infty} \sum_{k=0}^{n} (a_k)^p x^{-p^j+kp}$. Puisque $-p^j + kp \equiv 0 \mod p$ pour tout $j \geqslant 1$ et tout $k \geqslant 0$, le coéfficient de x^{-1} de aH^p est toujours nul, donc

$$e_0(aH_n^p) = 1$$

et la suite $(aH_n^p)_{n \geqslant 1}$ n'est pas équirépartie modulo 1.

Bibliographie

[1] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen II*, Math. Z. 19 (1924), p. 207–246.

[2] L. Carlitz, *Theorem of Dickson on irreducible polynomials*, Proc. Amer. Math. Soc. 3 (1952), p. 693–700.

[3] — *Diophantine approximations in fields of characteristic p*, Amer. Math. Soc. 72 (1952), p. 187–208.

[4] A. Dijksma, *Uniform distribution of polynomials over $GF\{q, x\}$ in $GF[q, x]$*, part I, Nederl. Akad. Wetensch. Proc. Ser. A. 72, 4 (1969), p. 376–383.

[5] — *Uniform distribution of polynomials over $GF\{q, x\}$ in $GF[q, x]$*, part II, ibidem 73, 3 (1970), p. 187–195.

[6] F. Dress, *Fonctions arithmétiques sur l'anneau des polynômes à coefficients dans un corps fini*, Séminaire Delange — Pisot — Poitou (Théorie des Nombres) (1962/63) n° 13, 9 p.

[7] T. Estermann, *Introduction to modern prime number theory*, Cambridge, at the University Press (1952) (Cambridge Tracts in Mathematics and mathematical Physics, 41).

[8] D. R. Hayes, *The distribution of irreducibles in $GF[q, x]$*, Trans. Amer. Math. Soc. 117 (1965), p. 101–127.

[9] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Akademische Verlag, Leipzig 1923.

[10] L. K. Hua, *Additive theory of prime numbers*, Translations of Mathematical Monographs 13 (1965).

[11] B. de Mathan, *Approximations diophantiennes dans un corps local*, Bull. Soc. Math. France, Mémoire 21 (1970) 93 pages (Thèse Sci. Math. Caen (1968)).

[12] G. Rhin, Thèse de 3ème cycle (1967) Caen.

[13] Titchmarsh, *The theory of the Riemann Zeta function*, Oxford 1951.

[14] S. Uchiyama, *Sur les polynômes irréductibles dans un corps fini*, II, Proc. Japan Acad. 31 (1955), p. 267–269.

[15] I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers* (Translated from russian), London, Interscience Publishers (1954).

[16] I. M. Vinogradov, *Sur l'évaluation de sommes trigonométriques avec des nombres premiers*, Izv. Akad. Nauk. SSSR Serija. Math. 12 (1948), p. 225–248 (en russe).

[17] B. M. Wilson, *Proofs of some formulae enunciated by Ramanujan*, Proc. London Math. Soc. 2, Vol. 21 (1921), p. 235–255.

[18] A. Weil, *Basic number theory*, Springer, 1967.

[19] — *Courbes algébriques et variétés abéliennes*, Hermann, 1971.