Functiones et Approximatio
XXXV (2006), 91–115

POINTS ENTIRES AU VOISINAGE D'UNE COURBE PLANE DE CLASSE C^n, II

Martin N. Huxley & Patrick Sargos

Dedicated to Professor Eduard Wirsing
on the occasion of his 75th birthday

Résumé: Dans la méthode des différences divisées pour majorer le nombre de points entiers au voisinage d'une courbe, Filaseta et Trifonov (1996) ont introduit un argument de divisibilité qui s'applique lorsque le voisinage considéré est très fin.

Nous approfondissons cet argument et l'adaptons au cas plus général où le voisinage n'est plus nécessairement aussi fin. Le problème se complique alors par l'apparition des arcs majeurs, déjà rencontrés par les auteurs dans un article précédent (1995).
Mots clés: points entiers, différences divisées.

Abstract: Filaseta and Trifonov (1996) introduced a divisibility argument into the divided differences method for bounding the number of integer points in a narrow strip close to a curve; their result is useful when the strip is very narrow.

We sharpen their argument, and extend it to allow broader strips. An immediate complication is the possible appearance of major arcs, which were first encountered in our earlier paper (1995).
Keywords: lattice points (integer points), divided differences.

1. Introduction et énoncé des résultats

Soient M un entier grand et δ un réel positif petit, et soit $f : [M, 2M] \to \mathbb{R}$ une fonction régulière. Le problème considéré consiste à majorer le nombre:

$$\mathcal{R}(f, \delta) = \sharp\,\{m \in [M, 2M] \cap \mathbb{Z} \mid \|f(m)\| \leqslant \delta\}, \tag{1.1}$$

où $\|x\|$ désigne la distance du réel x à l'ensemble $\mathbb{Z}$ des entiers relatifs. L'hypothèse minimum revient à supposer que f est de classe C^n pour un certain $n \geqslant 1$, et que:

$$|f^{(n)}(x)| \asymp \lambda_n, \quad \text{pour } M \leqslant x \leqslant 2M, \tag{1.2}$$

où λ_n est un réel positif petit.

2001 Mathematics Subject Classification: 11P21, 11J25.

Le problème des points entiers au voisinage d'une courbe apparaît naturellement dans certains problèmes de théorie analytique des nombres (voir par exemple [3] et la bibliographie de [3]). Il intervient également dans les majorations de sommes d'exponentielles (cf [4], [9], [11]), et on peut s'attendre à ce que le champ des applications s'étende à de nombreux autres problèmes d'arithmétique.

Il peut être traité par des méthodes de sommes d'exponentielles (sommes simples [5], sommes avec paramètre [8] ou sommes doubles [7]), avec des résultats de la forme:

$$\mathcal{R}(f,\delta) \ll M\delta + E, \tag{1.3}$$

où E dépend de l'ordre de grandeur des dérivées de f, mais non de δ.

Lorsque δ est suffisamment petit, la méthode plus simple des différences divisées (cf [6], [10], [3]) donne de meilleurs résultats. Par exemple, le Théorème 1 de [10] s'applique sous la seule hypothèse (1.2) et s'écrit:

$$\mathcal{R}(f,\delta) \ll M\lambda_n^{\frac{2}{n(n+1)}} + M\delta^{\frac{2}{n(n-1)}} + \Big(\frac{\delta}{\lambda_n}\Big)^{\frac{1}{n}} + 1. \tag{1.4}$$

Le terme $(\delta/\lambda_n)^{1/n}$ est optimal et le terme $M\lambda_n^{2/(n(n+1))}$ est, pour $n \geqslant 3$ (et surtout pour $n \geqslant 4$), meilleur que le terme E dans (1.3) déduit des résultats actuels sur les sommes d'exponentielles. Dans cette méthode, l'objectif prioritaire est de réduire le terme $M\delta^{2/n(n-1)}$.

Un progrès dans ce sens a été réalisé par Filaseta et Trifonov (cf [3], Théorème 6) lorsque la dérivée $(n-1)^e$ de f vérifie

$$|f^{(n-1)}(x)| \asymp \lambda_{n-1} := M\lambda_n, \quad \text{pour } M \leqslant x \leqslant 2M, \tag{1.5}$$

avec λ_{n-1} suffisamment petit, et lorsque $\delta \ll \lambda_{n-1}$. Leur idée essentielle est un argument de divisibilité tout à fait remarquable obtenu en introduisant une relation de récurrence classique sur les différences divisées [12].

Dans cet article, nous approfondissons et nous combinons le Lemme de réduction de [6], l'étude des "arcs majeurs" de [10] et l'argument de divisibilité de [3]. L'hypothèse commune à tous nos résultats est la suivante:

$$f \text{ est de classe } C^n \text{et vérifie (1.2) et (1.5), et on suppose } M \geqslant 4,\ \delta \leqslant 1/4. \tag{1.6}$$

Nous commençons par énoncer l'analogue du Théorème 6 de [3], qui ne fait pas intervenir les arcs majeurs.

Théorème 1. *On se place sous l'hypothèse (1.6) et on suppose en outre $\delta \ll \lambda_{n-1}$. Alors, pour $n \geqslant 3$, on a:*

$$\mathcal{R}(f,\delta) \ll M\lambda_n^{\frac{2}{n(n+1)}} + M(\delta\lambda_{n-1})^{\frac{2}{n^2-n+2}} + 1. \tag{1.7}$$

Sous des hypothèses similaires, Filaseta et Trifonov ont obtenu:

$$\mathcal{R}(f,\delta) \ll M\lambda_n^{\frac{2}{n(n+1)}} + M\delta^{\frac{2}{(n-1)(n-2)}} + M(\delta\lambda_{n-1})^{\frac{1}{n^2-3n+4}}. \tag{1.8}$$

Dans le membre de droite de (1.8), le deuxième terme disparaît par une simplification de démonstration, alors que l'amélioration du troisième terme, pour $n \geqslant 4$, provient du renforcement de l'argument de divisibilité; mais le fond de la démonstration reste inchangé par rapport à [3].

L'objectif suivant est de supprimer l'hypothèse $\delta \ll \lambda_{n-1}$ qui est d'autant plus contraignante que le Théorème 1 n'est intéressant que si λ_{n-1} est suffisamment petit. Soit S l'ensemble des entiers $m \in [M, 2M]$ tels que $\|f(m)\| \leqslant \delta$. Il se trouve que les points de S auxquels on ne peut pas appliquer l'argument de divisibilité sont précisément ceux qui forment les arcs majeurs et ils peuvent être étudiés à part par la méthode de [10]. On arrive ainsi au Théorème suivant.

Théorème 2. *Sous l'hypothèse (1.6), on a, pour $n \geqslant 3$:*

$$\begin{aligned}\mathcal{R}(f,\delta) \ll M\lambda_n^{\frac{2}{n(n+1)}} + M(\delta\lambda_{n-1})^{\frac{2}{n^2-n+2}} + M\delta^{\frac{2}{(n-1)(n-2)}} \\ + \Big(\frac{\delta}{\lambda_{n-1}}\Big)^{\frac{1}{n-1}} + 1.\end{aligned} \tag{1.9}$$

La contribution des arcs majeurs longs peut être majorée plus efficacement par l'utilisation du Théorème de Branton et Ramaré [1]. L'élimination des arcs majeurs courts coûte alors un facteur M^ε, ce qui donne le Théorème suivant.

Théorème 3. *Sous l'hypothèse (1.6), on a, pour $n \geqslant 4$ et pour tout $\varepsilon > 0$:*

$$\begin{aligned}\mathcal{R}(f,\delta) \ll_\varepsilon M^{1+\varepsilon}\lambda_n^{\frac{2}{n(n+1)}} + M^{1+\varepsilon}(\delta\lambda_{n-1})^{\frac{2}{n^2-n+2}} \\ + M^{1+\varepsilon}\Big(\delta^2 + \frac{\delta^2}{M\lambda_{n-1}}\Big)^{\frac{2}{n^2-3n+4}} + \Big(\frac{\delta}{\lambda_{n-1}}\Big)^{\frac{1}{n-1}} + 1.\end{aligned} \tag{1.10}$$

La relation de divisibilité peut être exploitée différemment, comme expliqué à la section 6. En ne modifiant qu'une partie de la démonstration, on obtient une variante des Théorèmes 1, 2, 3 dans lesquels le terme $M(\delta\lambda_{n-1})^{2/(n^2-n+2)}$ est remplacé par

$$M(\delta\lambda_n^{\frac{1}{3}})^{\frac{2}{n^2-n+2}} + M\delta^{\frac{4}{(n^2-3n+6)}}$$

Il n'est maintenant plus nécessaire de supposer λ_{n-1} très petit, et la condition $\delta \ll \lambda_{n-1}$ est moins restrictive. Nous commençons par l'analogue du Théorème 1:

Théorème 4. *On se place sous l'hypothèse (1.6) et on suppose en outre $\delta \ll \lambda_{n-1}$. Alors, pour $n \geqslant 3$, on a:*

$$\mathcal{R}(f,\delta) \ll M\lambda_n^{\frac{2}{n^2+n}} + M(\delta\lambda_n^{\frac{1}{3}})^{\frac{2}{n^2-n+2}} + M\delta^{\frac{4}{n^2-3n+6}} + 1. \tag{1.11}$$

L'analogue du Théorème 2 s'écrit:

Théorème 5. *Sous l'hypothèse (1.6), on a, pour* $n = 3$*:*

$$\mathcal{R}(f,\delta) \ll M\lambda_3^{1/6} + M\delta^{1/4}\lambda_3^{1/12} + M\delta^{2/3} + \Big(\frac{\delta}{\lambda_2}\Big)^{1/2} + 1. \tag{1.12}$$

Pour $n = 4$*, on a:*

$$\mathcal{R}(f,\delta) \ll M\lambda_4^{1/10} + M\delta^{1/7}\lambda_4^{1/21} + M\delta^{1/3} + \Big(\frac{\delta}{\lambda_3}\Big)^{1/3} + 1. \tag{1.13}$$

Pour $n \geqslant 5$*, on a:*

$$\mathcal{R}(f,\delta) \ll M\lambda_n^{\frac{2}{n(n+1)}} + M\delta^{\frac{2}{(n-1)(n-2)}} + \Big(\frac{\delta}{\lambda_{n-1}}\Big)^{\frac{1}{n-1}} + 1. \tag{1.14}$$

L'analogue du Théorème 3 est notre dernier résultat.

Théorème 6. *Sous l'hypothèse (1.6), on a, pour* $n \geqslant 4$ *et pour tout* $\varepsilon > 0$*:*

$$\begin{aligned} \mathcal{R}(f,\delta) \ll_\varepsilon M^{1+\varepsilon}\lambda_n^{\frac{2}{n(n+1)}} + M^{1+\varepsilon}(\delta\lambda_n^{\frac{1}{3}})^{\frac{2}{n^2-n+2}} \qquad (1.15) \\ + M^{1+\varepsilon}\delta^{\frac{4}{n^2-3n+6}} + M^{1+\varepsilon}\Big(\frac{\delta^2}{M\lambda_{n-1}}\Big)^{\frac{2}{n^2-3n+4}} + \Big(\frac{\delta}{\lambda_{n-1}}\Big)^{\frac{1}{n-1}} + 1. \end{aligned}$$

En particulier, si on suppose $M\lambda_{n-1} \gg 1$*, alors:*

$$\mathcal{R}(f,\delta) \ll_\varepsilon M^{1+\varepsilon}\Big(\lambda_n^{\frac{2}{n(n+1)}} + (\delta\lambda_n^{\frac{1}{3}})^{\frac{2}{n^2-n+2}} + \delta^{\frac{4}{n^2-3n+6}}\Big). \tag{1.16}$$

Le reste de l'article est consacré à la démonstration des Théorèmes 1 à 6.

Notations. Toutes les constantes sous-entendues dans les symboles classiques 0, $\ll$, $\gg$, $\asymp$, ne dépendent que de n et des constantes sous-entendues dans (1.2) et (1.5); dans le symbole $\ll_\varepsilon$, la constante dépend en outre de ε. On rappelle que $u \ll v$ signifie que v est positif et que $|u| \leqslant Bv$ pour une certaine constante positive B ; $u \gg v$ signifie que v est positif et que $v \ll u$; $u \asymp v$ signifie qu'on a à la fois $u \ll v$ et $u \gg v$.

L'écriture $u \ll v$ signifie que $|u| \leqslant v/B$, où B est une constante positive suffisamment grande, en un sens défini par le contexte. Par exemple, la phrase "$u \ll v$ implique $u_1 \ll v_1$" signifie: "pour toute constante positive B_1, il existe une constante positive B telle que $|u| \leqslant v/B$ implique $|u_1| \leqslant v_1/B_1$".

2. Compléments sur les arcs majeurs

Les arcs majeurs correspondent à des groupements de points entiers proches de la courbe $y = f(x)$ qui sont tous sur une même courbe polynomiale de degré $< r$ (où r est égal à n dans [10] et égal à $n-1$ ici). Comme ils annulent certaines différences divisées, certains raisonnements ne leur sont plus applicables et ils doivent être traités à part.

L'étude faite dans [10] est suffisante pour presque tous les besoins de cet article et est résumée dans le Lemme 1. Le cas $n = 4$ nécessite un travail supplémentaire (cf Lemme 2), qui généralise une démonstration de [2].

Dans ce paragraphe, nous faisons tous les rappels nécessaires à une lecture autonome; nous établissons les résultats dans leur plus grande généralité, en traitant les arcs majeurs relatifs à la dérivée r^e d'une fonction C^r vérifiant seulement (2.1); dans le problème initial, on prendra r égal à $n-1$.

2.1. Préliminaires. Soit $f : [M, 2M] \to \mathbb{R}$ une fonction de classe C^r, avec $r \geqslant 2$, vérifiant:

$$|f^{(r)}(x)| \asymp \lambda_r, \quad \text{pour } M \leqslant x \leqslant 2M, \tag{2.1}$$

où λ_r est un réel positif petit. Soit δ positif, $\delta \leqslant 1/4$. Soit un ensemble S tel que:

$$S \subset \{m \in [M, 2M] \cap \mathbb{N} \mid \|f(m)\| < \delta\} \tag{2.2}$$

(avec le signe "$<$" au lieu de "$\leqslant$" pour appliquer sans modification le Lemme 3 de [10]). Pour $m \in S$, on définit:

$$\tilde{f}(m) = \text{l'entier le plus proche de } f(m). \tag{2.3}$$

Nous modifions légèrement la définition des arcs majeurs de [10]:

Définition. Un arc majeur est un ensemble maximal $\mathcal{A} = \{m_1, \ldots, m_N\}$ de points consécutifs de S, avec $N \geqslant r^2 + 1$, tel qu'on ait $\tilde{f}(m_i) = P(m_i)$ pour $i = 1, \ldots, N$, où P est un polynôme de degré $< r$.

Le polynôme P est alors unique; on pose

$$P(x) = \frac{1}{q} \sum_{j=0}^{r-1} b_j x^j,$$

avec q entier $\geqslant 1$, $b_j \in \mathbb{Z}$, $b_0, b_1, \ldots, b_{r-1}$, q, étant premiers dans leur ensemble. On dira que q est le *dénominateur* de $\mathcal{A}$ et que $y = P(x)$ est l'*équation* de $\mathcal{A}$.

On pose $\Gamma_\delta = \{(x, y) \mid M \leqslant x \leqslant 2M, |y - f(x)| < \delta\}$ et on désigne par γ la courbe $\{(x, y) \mid x \in \mathbb{R}, y = P(x)\}$. Le Lemme 3 de [10] montre que $\gamma \cap \Gamma_\delta$ possède au plus r composantes connexes. On en choisit une qui contient le maximum de points $\{(m_{h+1}, \tilde{f}(m_{h+1})), \ldots, (m_{h+k}, \tilde{f}(m_{h+k}))\}$, avec $k \geqslant r+1$. On dira que l'ensemble $\overline{\mathcal{A}} = \{m_{h+1}, \ldots, m_{h+k}\}$ est l'*arc majeur propre* extrait de $\mathcal{A}$. Alors $\overline{\mathcal{A}}$ est un arc majeur au sens de [10] et on peut lui appliquer les résultats de [10].

La *longueur* de $\overline{\mathcal{A}}$ est le nombre $L = m_{h+k} - m_{h+1}$ et on a:

$$L \ll \Big(\frac{\delta}{\lambda_r}\Big)^{\frac{1}{r}} \qquad \text{(cf [10], Lemme 4).} \tag{2.4}$$

Son nombre d'éléments vérifie:

$$\sharp \overline{\mathcal{A}} \ll L q^{-\frac{2}{r(r-1)}} \qquad \text{(cf [10], Lemme 5).} \tag{2.5}$$

Si $\overline{\mathcal{A}}$ a un dénominateur $q \ll \delta^{-1}$, alors tout point $m \in S$ tel que $\tilde{f}(m) \neq P(m)$, est à une distance D de $\overline{\mathcal{A}}$, avec:

$$D \gg \min\Big\{ L(q\delta)^{-\frac{1}{r-1}}, (q\lambda_r)^{-\frac{1}{r}} \Big\} \qquad \text{(cf [10], Lemme 8).} \tag{2.6}$$

2.2. Contribution des arcs majeurs. On désigne par $\mathcal{P}$ l'ensemble des arcs majeurs, par S_0 l'ensemble des points de S qui proviennent des arcs majeurs, et on pose $R_0 = \sharp\, S_0$.

Lemme 1. *Pour* $r \geqslant 2$, *on a:*

$$R_0 \ll M \delta^{\frac{2}{r(r-1)}} + \max_{\mathcal{A} \in \mathcal{P}} (\sharp\, \mathcal{A}). \tag{2.7}$$

Démonstration. Rappelons que, pour chaque arc majeur $\mathcal{A} \in \mathcal{P}$, nous avons choisi un arc majeur propre, noté $\overline{\mathcal{A}}$. On a ainsi

$$R_0 \leqslant \sum_{\mathcal{A} \in \mathcal{P}} (\sharp\, \mathcal{A}).$$

On choisit un entier $Q \asymp \delta^{-1}$, suffisamment petit pour que, si $q \leqslant Q$, alors tout arc majeur propre $\overline{\mathcal{A}}$ de dénominateur q vérifie (2.6) et ne possède aucun point en commun avec n'importe quel autre arc majeur propre. On divise alors $\mathcal{P}$ en deux parties $\mathcal{P}_1$ et $\mathcal{P}_2$; $\mathcal{P}_1$ est l'ensemble des arcs majeurs dont le dénominateur et strictement supérieur à q et $\mathcal{P}_2$ désigne l'ensemble des autres arcs majeurs. On pose alors

$$S_i = \cup_{\mathcal{A} \in \mathcal{P}_i} \overline{\mathcal{A}}, \qquad R_i = (\sharp\, S_i), \qquad \text{pour } i = 1, 2,$$

et on a

$$R_0 \leqslant r(R_1 + R_2).$$

a) **Majoration de** R_1. On considère $2r-1$ points consécutifs de S_1. On peut en extraire r points consécutifs, $m_1, \ldots, m_r$, qui proviennent d'un même arc majeur propre de dénominateur $q > Q$. Reprenant la démonstration du Lemme 5 de [10], on remarque qu'on a $m_r - m_1 \geqslant q^{2/r(r-1)}$. On a donc prouvé

$$R_1 \leqslant (2r-1)(M Q^{-\frac{2}{r(r-1)}} + 1). \tag{2.8}$$

b) **Majoration de** R_2. On note $\overline{\mathcal{A}}_1, \dots, \overline{\mathcal{A}}_J$ la suite des arcs majeurs propres de dénominateur au plus égal à Q, dans l'ordre où ils interviennent. Par chaque arc majeur propre $\overline{\mathcal{A}}_j$ $(1 \leqslant j \leqslant J)$, on désigne respectivement par m_j, q_j et L_j le premier point de $\overline{\mathcal{A}}_j$, son dénominateur et sa longeur. On choisit également un réel D_j tel que

$$D_j \gg \min(L_j(q_j\delta)^{-\frac{2}{r(r-1)}}, (q_j\lambda_r)^{-\frac{1}{r}}),$$

de sorte que le segment $[m_j, m_j + D_j]$ contienne $\overline{\mathcal{A}}_j$ et ne contienne aucun élément de $\overline{\mathcal{A}}_{j+1}$; cela est toujours possible d'après (2.6) et d'après le choix de Q. On pose

$$\rho_j = \frac{(\sharp\overline{\mathcal{A}}_j)}{D_j}.$$

On a ainsi

$$R_2 \leqslant \sum_{j=1}^{J-1} \rho_j D_j + (\sharp\overline{\mathcal{A}}_J) \leqslant M(\max_j \rho_j) + (\sharp\overline{\mathcal{A}}_J),$$

cette dernière inégalité provenant du fait que les intervalles $[m_j, m_j + D_j]$ sont deux à deux disjoints et contenus dans un intervalle de longeur M.

Par (2.4), (2.5) et par le choix de D_j, on obtient en outre

$$\rho_j \ll \delta^{\frac{2}{r(r-1)}} \text{ si } r \geqslant 3, \text{ et } \rho_j \ll \delta^{\frac{1}{2}} \text{ si } r = 2.$$

On en déduit

$$R_2 \ll M\delta^{\frac{2}{r(r-1)}} + (\sharp\overline{\mathcal{A}}_J), \text{ pour } r \geqslant 3. \tag{2.9}$$

On a donc obtenu (2.7) pour $r \geqslant 3$. Le cas particulier $r = 2$ est implicitement contenu dans [2] (ou encore dans le Lemme 2 ci-après). Le Lemme 1 est entièrement démontré.

2.3. Contribution des arcs majeurs longs. Nous allons maintenant remplacer la majoration (2.5) par le résultat de Branton et Ramaré concernant le nombre de points entiers sur une courbe polynomiale de degré $\leqslant r - 1$, qui est plus efficace lorsque L est assez grand. Sous les hypothèses de (2.5), on a:

$$\sharp\,\overline{\mathcal{A}} \leqslant (r-1)^{\omega(q)} + 0\Big(Lq^{-\frac{1}{r-1}}\Big) \qquad \text{(cf [1], Théorème 2)}, \tag{2.10}$$

où $\omega(q)$ désigne le nombre de facteurs premiers de q comptés sans multiplicité. En relation avec (2.10), on pose:

$$H = r^2 + 2r \max_{1 \leqslant q \leqslant Q_0} (r-1)^{\omega(q)}, \tag{2.11}$$

où Q_0 est choisi assez grand pour inclure tous les dénominateurs possibles, tout en assurant la majoration:

$$H \ll_\varepsilon M^\varepsilon, \quad \text{pour tout } \varepsilon > 0. \tag{2.12}$$

D'après la formule d'interpolation de Lagrange, on peut prendre $Q_0 = M^{r(r+1)/2}$ (cf [10]). Si $\mathcal{A}$ est un arc majeur ayant au moins H éléments, on a alors, sous les hypothèses de (2.5):

$$\sharp\overline{\mathcal{A}} \ll Lq^{-\frac{1}{r-1}}. \tag{2.13}$$

On désigne par $\mathcal{P}_H$ l'ensemble des arcs majeurs ayant au moins H éléments, par S_H l'ensemble des points de S qui proviennent d'un arc majeur $\mathcal{A} \in \mathcal{P}_H$ et on pose $R_H = \sharp S_H$. Si on reprend mot pour mot la démonstration du Lemme 1 en remplaçant (2.5) par (2.13), on obtient seulement:

$$R_H \ll M\delta^{1/r} + \max_{\mathcal{A}\in\mathcal{P}} (\sharp\,\mathcal{A}), \tag{2.14}$$

ce qui est suffisant dans notre problème initial, sauf pour $n = 4$ (i.e. $r = 3$). On peut améliorer (2.14) en généralisant la démonstration de [2]:

Lemme 2. *Avec les notations précédentes, on a, pour $r \geqslant 2$:*

$$R_H \ll M\delta^{\frac{1}{r-1}} + \max_{\mathcal{A}\in\mathcal{P}} (\sharp\,\mathcal{A}). \tag{2.15}$$

Démonstration. On sépare les arcs majeurs de $\mathcal{P}_H$ en trois groupes $\mathcal{P}_1$, $\mathcal{P}_2$ et $\mathcal{P}_3$ selon que l'on a:

$$q \ll \frac{1}{\delta} \quad \text{et} \quad \frac{1}{(q\lambda_r)^{1/r}} \ll \frac{L}{(q\delta)^{1/(r-1)}} \tag{2.16}$$

$$q \ll \delta^{-1} \quad \text{et} \quad \frac{1}{(q\lambda_r)^{1/r}} \gg \frac{L}{(q\delta)^{1/(r-1)}} \tag{2.17}$$

ou

$$q \gg \frac{1}{\delta}. \tag{2.18}$$

Appelons R_1, R_2 et R_3 la contribution de $\mathcal{P}_1$, $\mathcal{P}_2$ et $\mathcal{P}_3$. Pour majorer R_2 et R_3, on reprend exactement la démonstration du Lemme 1, sauf que la majoration (2.5) doit être remplacée par (2.13). On obtient ainsi la majoration annoncée en (2.15) pour R_2 et R_3. Il reste donc à majorer R_1.

On commence par éliminer une situation extrême. Soit q_0 le plus petit entier tel qu'il existe $\mathcal{A} \in \mathcal{P}_1$ de dénominateur q_0. Si $(q_0\lambda_r)^{-1/r} \gg M$, deux arcs majeurs propres $\overline{\mathcal{A}}_1$ et $\overline{\mathcal{A}}_2$ sont séparés par une distance $\gg (q_0\lambda_r)^{-1/r} \gg M$, d'après (2.6) et (2.16), ce qui est impossible. On a alors $R_1 \ll \max_{\mathcal{A}\in\mathcal{P}_1} (\sharp\,\mathcal{A})$, et (2.15) est démontré dans ce cas. On peut donc supposer:

$$(q_0\lambda_r)^{-\frac{1}{r}} \ll M. \tag{2.19}$$

On définit maintenant le coefficient directeur de l'arc majeur $\mathcal{A}$, de dénominateur q et d'équation $y = P(x)$, comme étant le coefficient $\alpha = p/q$ de x^{r-1} dans l'écriture de $P(x)$ (p et q ne sont pas nécessairement premiers entre eux). On note $\mathcal{P}_1(\alpha)$ l'ensemble des arcs majeurs $\mathcal{A} \in \mathcal{P}_1$ de coefficient directeur α, et $R_1(\alpha)$ la contribution des arcs majeurs de $\mathcal{P}_1(\alpha)$.

a) Dans un premier temps, on démontre les deux propriétés suivantes:

$$\text{Pour tout } \alpha,\ \mathcal{P}_1(\alpha) \text{ possède au plus un élément,} \tag{2.20}$$

et

$$\text{si la distance de } \alpha \text{ à } f^{(r-1)}([M,2M]) \text{ est } \gg M\lambda_r, \text{ alors } \mathcal{P}_1(\alpha) = \emptyset. \tag{2.21}$$

Pour simplifier, on prolonge f en une fonction sur $\mathbb{R}$, notée encore f, qui vérifie: $|f^{(r)}(x)| \asymp \lambda_r$ pour $x \in \mathbb{R}$. Pour tout rationnel α, on désigne par $z = z(\alpha)$ le réel qui vérifie $f^{(r-1)}(z) = \alpha(r-1)!$.

Soit $\mathcal{A} \in \mathcal{P}_1(\alpha)$, d'équation $y = P(x)$, de dénominateur q. Soit $\overline{\mathcal{A}}$ l'arc majeur propre extrait de $\mathcal{A}$, de longueur L. Soit enfin D la distance de z à $\overline{\mathcal{A}}$. Alors on a:

$$D \ll (q\lambda_r)^{-\frac{1}{r}}. \tag{2.22}$$

En effet, si on pose $\varphi(x) = f(x) - P(x)$, on a $\varphi^{(r-1)}(z) = 0$, et si $z+h \in \overline{\mathcal{A}}$, alors $|\varphi^{(r-1)}(z+h)| = |hf^{(r)}(\xi)| \gg D\lambda_r$; d'autre part, sur un intervalle de longueur L, on a $|\varphi(x)| < \delta$. Alors la démonstration du Lemme 4 de [10] montre que $L \ll (\delta/D\lambda_r)^{1/(r-1)}$. Compte tenu de (2.16), cette dernière inégalité implique (2.22).

Supposons maintenant que $\mathcal{A}_1$ et $\mathcal{A}_2$ soient dans $\mathcal{P}_1(\alpha)$; soient $\overline{\mathcal{A}}_1$ et $\overline{\mathcal{A}}_2$ les arcs majeurs propres extraits de $\mathcal{A}_1$ et $\mathcal{A}_2$, de dénominateur q_1 et q_2. Posons $q = \min\{q_1, q_2\}$. Alors, d'après (2.22), $\overline{\mathcal{A}}_1$ et $\overline{\mathcal{A}}_2$ sont dans un même intervalle de longueur $\ll (q\lambda_r)^{-1/r}$, alors que, d'après (2.6) et (2.16), ils sont séparés entre eux par une distance $\gg (q\lambda_r)^{-1/r}$. Cette contradiction prouve (2.20).

Avant de démontrer (2.21), on remarque que, dans la définition de $\mathcal{P}_1$, on aurait pu éliminer les arcs majeurs qui sont au bord de l'intervalle $[M, 2M]$ et qui chevauchent le point M ou le point $2M$; il y en a au plus deux et leur contribution est comptée dans le terme max $(\sharp\,\mathcal{A})$. Dans ce cas, avec les notations de (2.22), si la distance de z à $[M, 2M]$ est $\gg M$, alors on a $D \gg M \gg (q_0\lambda_r)^{-1/r}$ (d'après (2.19)) $\geqslant (q\lambda_r)^{-1/r}$, ce qui contredit (2.22). On a donc prouvé (2.21).

b) Nous continuons la démonstration du Lemme 2 par un calcul indépendant:

Lemme 3. *Soit J un intervalle de $\mathbb{R}$. Pour chaque $\alpha = p/q \in J$, avec $1 \leqslant q \leqslant Q$ et $(p,q) = 1$, soit $R_1(\alpha)$ un réel positif tel que $R_1(\alpha) \leqslant Bq^{-\theta}$, avec $\theta < 2$. Alors on a:*

$$\sum_{\alpha \in J} R_1(\alpha) \ll_\theta B|J|Q^{2-\theta} + \max_{\alpha \in J} R_1(\alpha), \tag{2.23}$$

où $|J|$ désigne la longueur de J.

Démonstration du Lemme 3. Choisissons un réel Q_1 tel que $|J|Q_1^2 \asymp 1$. Le nombre des $\alpha = p/q \in J$ tels que $q \leqslant Q_1$ est $0(1)$, puisqu'ils sont distants entre eux d'au moins Q_1^{-2}; la contribution de ces α est majorée par le terme max $R_1(\alpha)$.

Les $\alpha = p/q \in J$ avec $q \asymp Q_2 := 2^k Q_1$ sont en nombre $\ll |J| Q_2^2$ et ont une contribution $\ll B|J|Q_2^{2-\theta}$. Il ne reste plus qu'à sommer sur k pour obtenir (2.23). c.q.f.d.

c) Pour finir la démonstration du Lemme 2, on se ramène à la situation du Lemme 3.

Par (2.4), (2.5) et (2.20), on a: $R_1(\alpha) \ll (\delta/\lambda_r)^{1/r} q^{-1/(r-1)}$, lorsque $\alpha = p/q$ et $(p,q) = 1$.

D'autre part, d'après (2.21), l'intervalle J peut être pris de longueur $\asymp M\lambda_r$. Il ne reste plus qu'à montrer que Q peut être choisi égal à:

$$Q = \min\Big\{\delta^{-1}, (\delta/\lambda_r)^{1-1/r}\Big\}. \tag{2.24}$$

En effet, d'après (2.16), on ne doit considérer que des dénominateurs $q \ll \delta^{-1}$. D'autre part, on a toujours

$$1 \ll \sharp\overline{\mathcal{A}} \ll Lq^{-\frac{1}{r-1}} \ll \Big(\frac{\delta}{\lambda_r}\Big)^{\frac{1}{r}} \times q^{-\frac{1}{r-1}},$$

et par suite $q \ll (\delta/\lambda_r)^{1-1/r}$, ce qui prouve (2.24).

On reporte les valeurs ci-dessus dans (2.23), ce qui donne:

$$R_1 \ll \max_{\alpha} R_1(\alpha) + M\lambda_r \Big(\frac{\delta}{\lambda_r}\Big)^{\frac{1}{r}} Q^{2-\frac{1}{r-1}}.$$

Il suffit alors d'écrire:

$$Q^{2-\frac{1}{r-1}} = Q \times Q^{\frac{r-2}{r-1}} \ll \Big(\frac{\delta}{\lambda_r}\Big)^{1-\frac{1}{r}} \delta^{-\frac{r-2}{r-1}},$$

d'après (2.24), pour obtenir (2.15).

Le Lemme 2 est entièrement démontré.

3. Le Lemme de réduction

Pour faire apparaître les différences divisées de f, nous reprenons et nous précisons le Lemme 1 de [6]. Nous en présentons trois variantes, dont deux en association avec les arcs majeurs.

Soit $f : [M, 2M] \to \mathbb{R}$ une fonction C^r vérifiant (2.1); on pose $R = \sharp S$, où S est défini en (2.2). Si $m \in S$, $\tilde{f}(m)$ est défini en (2.3).

Étant donné les entiers $a_1, \ldots, a_r \geqslant 1$, on pose systématiquement:

$$\underline{a} = (a_1, \ldots, a_r) \in (\mathbb{N} \setminus \{0\})^r, \quad \text{et} \quad a = a_1 + \cdots + a_r \tag{3.1}$$

$$d_0 = 0,\ d_1 = a_1,\ d_2 = a_1 + a_2, \ldots, d_r = a_1 + \cdots + a_r. \tag{3.2}$$

Dans le résultat suivant, la fonction f n'intervient pas et l'ensemble $S \subset [M, 2M] \cap \mathbb{N}$ peut être pris quelconque:

Lemme 4. *On suppose $r \geqslant 1$. Etant donné un entier A $(1 \leqslant A \leqslant M)$, il existe une famille d'ensembles $S(\underline{a})$, $\underline{a} \in [1, A]^r$, de sorte que les trois propriétés suivantes soient satisfaites:*

$$S(\underline{a}) \subset \{m \mid m + d_i \in S \text{ pour } i = 0, 1, \ldots, r\} \tag{3.3}$$

$$\text{si } m \text{ et } m + b \in S(\underline{a}), \text{ alors } b > a \tag{3.4}$$

$$R \leqslant (r+1) \sum_{a_1=1}^{A} \cdots \sum_{a_r=1}^{A} R(\underline{a}) + (r+1)\frac{M}{A} + r, \tag{3.5}$$

avec la notation $R(\underline{a}) = \sharp\, S(\underline{a})$.

Démonstration. On décompose l'ensemble S en groupes $G = \{m_0, m_1, \ldots, m_r\}$ formés de $(r+1)$ points consécutifs de S. Les points qui ne rentrent dans aucun groupe sont en nombre $\leqslant r$ et sont comptés dans le dernier terme de (3.5).

Les groupes qui contiennent deux points consécutifs m_{i-1} et m_i avec $m_i - m_{i-1} > A$ sont en nombre $\leqslant M/A$ et leur contribution est alors $\leqslant (r+1)M/A$.

Soit enfin $G = \{m_0, m_1, \ldots, m_r\}$ un groupe tel que $m_i - m_{i-1} \leqslant A$ pour chaque $i = 1, \ldots, r$. On pose $a_i = m_i - m_{i-1}$ pour $i = 1, \ldots, r$. On dit alors que $m_0 \in S(\underline{a})$ et que $S(\underline{a})$ est constitué de ces m_0. Les ensembles $S(\underline{a})$ ainsi construits répondent à la question.

Lemme 5. *On suppose $r \geqslant 2$. Etant donné un entier A $(1 \leqslant A \leqslant M)$, il existe une famille $S(\underline{a})$, $\underline{a} \in [1, A]^r$, vérifiant (3.3) et (3.4), ainsi que les deux propriétés suivantes:*

$$\textit{Si } m \in S(\underline{a}), \textit{ alors aucun polynôme } P \textit{ de degré} < r \textit{ ne vérifie:} \tag{3.6}$$
$$P(m + d_i) = \tilde{f}(m + d_i) \text{ pour } i = 0, 1, \ldots, r,$$

$$R \leqslant (r^2+1) \sum_{a_1=1}^{A} \cdots \sum_{a_r=1}^{A} R(\underline{a}) + (r^2+1)\frac{M}{A} + r^2 + 0(M\delta^{\frac{2}{r(r-1)}}) + 0\left(\left(\frac{\delta}{\lambda_r}\right)^{\frac{1}{r}}\right). \tag{3.7}$$

Démonstration. Soit S_0 l'ensemble des points de S qui proviennent des arcs majeurs, et soit $S_1 = S \setminus S_0$. On pose $R_0 = \sharp\, S_0$ et $R_1 = \sharp\, S_1$. Par le Lemme 1, on a

$$R_0 \ll M\delta^{\frac{2}{r(r-1)}} + \left(\frac{\delta}{\lambda_r}\right)^{\frac{1}{r}}.$$

Il reste à majorer R_1.

On décompose S_1 en groupes de r^2+1 points consécutifs. Soit $G = \{m_0, m_1, \ldots, m_{r^2}\}$ un tel groupe. On pose $M_i = \big(m_i, \tilde{f}(m_i)\big) \in \mathbb{Z}^2$. Soit P l'unique polynôme de degré $< r$ tel que la courbe $y = P(x)$ passe par les points $M_0, M_1, \ldots, M_{r-1}$. Par construction, G n'est contenu dans aucun arc majeur, ce qui implique que l'un au moins des M_k n'est pas sur la courbe $y = P(x)$. On fixe un tel M_k, et on pose: $a_1 = m_1 - m_0, a_2 = m_2 - m_1, \ldots, a_r = m_k - m_{r-1}$; on dit que m_0 est dans $S(\underline{a})$, ce qui définit les ensembles $S(\underline{a})$.

En raisonnant comme au Lemme 4, il est facile de vérifier que les ensembles $S(\underline{a})$ ainsi construits répondent à la question.

Lemme 6. *On suppose $r \geqslant 2$ et on définit l'entier H comme en (2.11). Étant donné un entier $A (1 \leqslant A \leqslant M)$, il existe une famille d'ensembles $S(\underline{a})$, $\underline{a} \in [1, A]^r$, vérifiant (3.3), (3.4) et (3.6), ainsi que la propriété suivante:*

$$R \leqslant H \sum_{a_1=1}^{A} \cdots \sum_{a_r=1}^{A} R(\underline{a}) + \frac{HM}{A} + H + 0(M\delta^{\frac{1}{r-1}}) + 0\biggl(\Bigl(\frac{\delta}{\lambda_r}\Bigr)^{\frac{1}{r}}\biggr). \tag{3.8}$$

Pour la démonstration de ce Lemme, il suffit d'adapter celle du Lemme 5, en utilisant le Lemme 2 à la place du Lemme 1, et en considérant des groupes de H points consécutifs de S_1. Nous ne donnerons pas les détails.

4. Différences divisées et Lemme de divisibilité

Nous rappelons les notations et les propriétés des différences divisées qui nous seront utiles dans la suite, renvoyant à [12] pour les démonstrations, puis nous nous plaçons dans le cadre de l'ensemble $S(\underline{a})$ défini à la section 3 pour formuler le Lemme de divisibilité.

4.1. Généralités sur les différences divisées. Soit E un sous-ensemble de $\mathbb{R}$, $f : E \to \mathbb{R}$ une fonction quelconque, $x_0, x_1, \ldots, x_r$, $(r+1)$ points distincts de E (avec $r \geqslant 1$) et $M_i = \bigl(x_i, f(x_i)\bigr) \in \mathbb{R}^2$. Soit P l'unique polynôme de degré $\leqslant r$ tel que la courbe $y = P(x)$ passe par les points M_i, $i = 0, 1, \ldots, r$. Le coefficient de x^r dans l'écriture de P se note $f[x_0, x_1, \ldots, x_r]$ et est égal à:

$$f[x_0, x_1, \ldots, x_r] = \frac{1}{D} \sum_{k=0}^{r} (-1)^{r-k} D_k f(x_k), \tag{4.1}$$

où on a posé:

$$D = \prod_{0 \leqslant i < j \leqslant r} \prod (x_j - x_i) \quad \text{et} \quad D_k = \prod_{\substack{i \,\mathrm{et}\, j \;\neq k \\ 0 \leqslant i < j \leqslant r}} \prod (x_j - x_i). \tag{4.2}$$

Si on suppose que E est un intervalle et si f est de classe C^r, alors:

$$f[x_0, \ldots, x_r] = \frac{1}{r!} f^{(r)}(\xi) \tag{4.3}$$

pour un certain ξ intérieur à l'intervalle engendré par les x_i.

Les différences divisées d'ordre r et d'ordre $r-1$ sont liées par la relation de récurrence:

$$f[x_0, \ldots, x_r] = \frac{f[x_0, \ldots, \widehat{x_k}, \ldots, x_r] - f[x_0, \ldots, \widehat{x_\ell}, \ldots, x_r]}{x_\ell - x_k} \quad (k \neq \ell), \tag{4.4}$$

avec la notation $f[x_0, \ldots, \widehat{x_k}, \ldots, x_r] = f[x_0, \ldots, x_{k-1}, x_{k+1} \ldots, x_r]$.

4.2. Le Lemme de divisibilité.

a) On fixe $\underline{a} = (a_1, \ldots, a_r) \in (\mathbb{N} \setminus \{0\})^r$. Avec la notation (3.2), on pose:

$$D = \prod_{0 \leqslant i < j \leqslant r} \prod (d_j - d_i), \tag{4.5}$$

$$D_k = \prod_{\substack{i \text{ et } j \neq k \\ 0 \leqslant i < j \leqslant r}} (d_j - d_i), \quad \text{pour } 0 \leqslant k \leqslant r, \tag{4.6}$$

$$D_{k\ell} = \prod_{\substack{i \text{ et } j \neq k \text{ et } \ell \\ 0 \leqslant i < j \leqslant r}} (x_j - x_i), \quad \text{pour } 0 \leqslant k, \ell \leqslant r, k \neq \ell. \tag{4.7}$$

Alors, pour toute fonction f définie sur un ensemble convenable, on a:

$$f[x+d_0, \ldots, x+d_r] = \frac{1}{D} \sum_{i=0}^{r} (-1)^{r-i} D_i f(x+d_i), \tag{4.8}$$

$$\begin{aligned} &f[x+d_0, \ldots, \widehat{x+d_k}, \ldots, x+d_r] \\ &= \frac{1}{D_k} \left\{ \sum_{i=0}^{k-1} (-1)^{r-i-1} D_{ki} f(x+d_i) + \sum_{j=k+1}^{r} (-1)^{r-j} D_{kj} f(x+d_k) \right\}. \end{aligned} \tag{4.9}$$

D'autre part, si f est de classe C^{r+s} dans un certain intervalle, et si x est dans un intervalle convenable, alors, d'après (4.3), on a:

$$\frac{d^s}{dx^s} f[x+d_0, \ldots, x+d_r] = f^{(s)}[x+d_0, \ldots, x+d_r] = \frac{1}{r!} f^{(r+s)}(\xi), \tag{4.10}$$

avec $x < \xi < x+d_r$, et s entier $\geqslant 0$.

b) Soit $E = \{m+d_0, \ldots, m+d_r\} \cup \{m+b+d_0, \ldots, m+b+d_r\}$, où m et b sont deux entiers, et soit $\tilde{f} : E \to \mathbb{Z}$ une fonction quelconque. On pose $\tilde{g}(x) = \tilde{f}(x+b) - \tilde{f}(x)$, et:

$$L_k = D_k \tilde{g}[m+d_0, \ldots, \widehat{m+d_k}, \ldots, m+d_r] \quad (0 \leqslant k \leqslant r). \tag{4.11}$$

Il résulte de (4.9) que L_k est un entier. On pose enfin:

$$e = \text{p.g.c.d.}(D_0, D_1, \ldots, D_r). \tag{4.12}$$

Lemme 7. *On suppose que* $\tilde{f}[m+d_0, \ldots, m+d_r] = \tilde{f}[m+b+d_0, \ldots, m+b+d_r]$. *Alors, pour chaque* $k = 0, \ldots, r$, L_k *est divisible par* D_k/e.

Démonstration. La relation de récurrence (4.4) appliquée à la fonction $\tilde{g}$ s'écrit:

$$\frac{L_k}{D_k} - \frac{L_j}{D_j} = (d_j - d_k)\tilde{g}[m+d_0, \ldots, m+d_r] = 0,$$

par hypothèse, d'où $D_k L_j = D_j L_k$ pour chaque k et j. Pour k fixé, on en déduit que D_k divise $D_j L_k$ pour chaque j; donc D_k divise eL_k. c.q.f.d.

5. Démonstration des Théorèmes 1, 2 et 3

Soient f vérifiant (1.6), et $0 < \delta < 1/4$; on fixe $r = n-1$ aux paragraphes 2, 3 et 4, et on définit S par (2.2). Étant donné $\underline{a}$ comme en (3.1) et $S(\underline{a})$ comme en (3.3), on veut, en premier lieu, majorer $R(\underline{a}) = \sharp\, S(\underline{a})$. A l'aide des Lemmes 4, 5 et 6, on en déduit les majorations cherchées de $R = \sharp\, S$ en optimisant le paramètre A selon le procédé du Lemme 2.4 de [5] (ce Lemme étant classique, nous l'appliquerons sans le signaler).

5.1. Décomposition en trois cas. Étant donné $\underline{a} = (a_1, \ldots, a_{n-1})$, on veut majorer $R(\underline{a})$; pour cela, on distingue trois cas qui donnent lieu à des démonstrations différentes.

(5.1) 1er cas: $D/D_s \gg \delta/\lambda_{n-1}$,

(5.2) 2ème cas: $D/D_s \ll \delta/\lambda_{n-1}$ et $\delta D_s/e \ll 1$,

(5.3) 3ème cas: $D/D_s \ll \delta/\lambda_{n-1}$ et $\delta D_s/e \gg 1$,

où D, D_i et e sont définis en (4.5), (4.6) et (4.12), et où on a posé

$$D_s = \max\{D_0, \ldots, D_{n-1}\}.$$

Tout au long de la démonstration, un rôle essentiel est joué par la fonction:

$$\varphi(x) = \frac{D}{e} f[x + d_0, \ldots, x + d_{n-1}]. \tag{5.4}$$

L'ordre de grandeur de φ et φ' se déduit de (4.10):

$$|\varphi(x)| \asymp \frac{D\lambda_{n-1}}{e} \quad \text{et} \quad |\varphi'(x)| \asymp \frac{D\lambda_n}{e}. \tag{5.5}$$

Pour $m \in S(\underline{a})$, on définit l'entier:

$$\widetilde{\varphi}(m) = \frac{D}{e} \tilde{f}[m + d_0, \ldots, m + d_{n-1}]. \tag{5.6}$$

On pose également:

$$\varphi(m) = \widetilde{\varphi}(m) + \eta(m), \quad \text{avec } \eta(m) \ll \eta := \frac{D_s \delta}{e}, \tag{5.7}$$

cette dernière inégalité découlant de (4.8). On achève ces préliminaires avec le Lemme suivant.

Lemme 8. (i) *On suppose* $\delta \ll \lambda_{n-1}$. *Alors dans le cas 2 et le cas 3,* $S(\underline{a})$ *est vide.*
(ii) *On suppose que* $S(\underline{a})$ *vérifie (3.6). Alors, dans le cas 2,* $S(\underline{a})$ *est vide.*
(iii) *On suppose que* $S(\underline{a})$ *vérifie (3.6) et que* $A \ll \delta^{-2/((n-1)(n-2))}$. *Alors, dans le cas 3,* $S(\underline{a})$ *est vide.*

Démonstration. La partie (i) est évidente. Pour les deux autres, on commence par établir la propriété intermédiaire suivante:

$$\text{On suppose (3.6). Alors, pour tout } m \in S(\underline{a}),\ \widetilde{\varphi}(m) \text{ est non nul.} \tag{5.8}$$

En effet, soit P le polynôme de degré $\leqslant n-1$ qui vérifie $P(m+d_i) = \tilde{f}(m+d_i)$ pour $i = 0, 1, \ldots, n-1$. Par définition, le coefficient de x^{n-1} de P est

$$\tilde{f}[m+d_0, \ldots, m+d_{n-1}] = \frac{e}{D}\widetilde{\varphi}(m);$$

son annulation contredirait (3.6).

Soit alors $\underline{a}$ vérifiant (5.2). Dans l'écriture (5.7), on a $\varphi(m) \ll 1$ par (5.2) et (5.5), et $\eta(m) \ll 1$ par (5.7) et (5.2), ce qui implique $\widetilde{\varphi}(m) \ll 1$; donc $\widetilde{\varphi}(m) = 0$, ce qui contredit (5.8) et prouve (ii).

Si $\underline{a}$ vérifie (5.3) et $A \ll \delta^{-2/((n-1)(n-2))}$ alors, à nouveau, on a $\eta(m) \ll 1$ (car $D_s \ll A^{(n-1)(n-2)/2} \ll \delta^{-1}$, et donc $\eta \ll 1/e \leqslant 1$), et $\varphi(m) \ll 1$ (car $\varphi(m) \asymp D\lambda_{n-1}/e \ll D_s\delta/e = \eta \ll 1$); la même conclusion s'applique, ce qui prouve (iii). c.q.f.d.

5.2. Majoration de $R(\underline{a})$ dans le 1er cas. Cette partie traite du cas où les a_i sont grands et constitue le coeur de la démonstration des théorèmes 1, 2 et 3.

Parallèlement à la fonction φ, on introduit la fonction ψ de la façon suivante. Étant donné l'entier b, on pose $g(x) = f(x+b) - f(x)$ et:

$$\psi(x) = D_s g[x+d_0, \ldots, \widehat{x+d_s}, \ldots, x+d_{n-1}], \tag{5.9}$$

où s est l'indice défini à la section 5.1. L'ordre de grandeur de ψ est

$$|\psi(x)| \asymp bD_s\lambda_{n-1}. \tag{5.10}$$

Si m et $m+b$ sont dans $S(\underline{a})$, on peut définir l'entier:

$$\widetilde{\psi}(m) = D_s\tilde{g}[m+d_0, \ldots, \widehat{m+d_s}, \ldots, m+d_{n-1}] \tag{5.11}$$

et poser:

$$\psi(m) = \widetilde{\psi}(m) + \beta(m), \quad \text{avec } \beta(m) \ll \beta := \delta D_{st}, \tag{5.12}$$

où l'indice t est choisi de sorte que $D_{st} = \max\{D_{si} \mid 0 \leqslant i \leqslant n-1, i \neq s\}$ (et D_{si} est défini en (4.7)), et où l'inégalité sur $\beta(m)$ découle de (4.9).

Avec ces notations, le Lemme de divisibilité s'énonce simplement:

$$\text{Si } \widetilde{\varphi}(m) = \widetilde{\varphi}(m+b), \text{ alors } \widetilde{\psi}(m) \text{ est divisible par } D_s/e. \tag{5.13}$$

Lemme 9. *Si $\underline{a}$ est dans le 1er cas, et si $S(\underline{a})$ vérifie (3.4), alors on a:*

$$R(\underline{a}) \ll M\lambda_n D + M\delta\lambda_{n-1}D_s. \tag{5.14}$$

Démonstration. a) Pour chaque entier k, on définit l'ensemble:

$$S_k(\underline{a}) = \{m \in S(\underline{a}) \mid \widetilde{\varphi}(m) = k\}. \tag{5.15}$$

Alors $S_k(\underline{a})$ est contenu dans un intervalle de longueur $L \ll D_s\delta/(D\lambda_n)$. En effet, si m et $m+b \in S_k(\underline{a})$, on a:

$$\varphi(m) - \eta(m) = \varphi(m+b) - \eta(m+b) = k, \quad \text{d'où: } \varphi(m+b) - \varphi(m) \ll \eta,$$

et on conclut par (5.5) et (5.7).

b) Soient maintenant m et $m+b \in S_k(\underline{a})$. On va montrer que:

$$b \gg (e\lambda_{n-1})^{-1}. \tag{5.16}$$

On utilise pour cela la fonction ψ définie en (5.9). D'après (5.10) et (3.4), on a:

$$\psi(m) \gg aD_s\lambda_{n-1} = \beta\frac{aD_s\lambda_{n-1}}{D_{st}\delta},$$

où β est défini en (5.12). Mais, par (5.1), on a $aD_s\lambda_{n-1}/(D_{st}\delta) \gg 1$, car

$$\frac{aD_s}{D_{st}} = \frac{D}{D_s} \times \frac{a}{|d_s - d_t|} \geqslant \frac{D}{D_s}.$$

Donc, $\psi(m) \gg \beta$, et par suite:

$$|\widetilde{\psi}(m)| \asymp |\psi(m)| \asymp bD_s\lambda_{n-1}. \tag{5.17}$$

En particulier, $\widetilde{\psi}(m)$ est non nul et la relation (5.13) montre que $|\widetilde{\psi}(m)| \gg D_s/e$; cette inégalité, combinée à (5.17), donne (5.16).

c) Les éléments de $S_k(\underline{a})$ sont en nombre $\ll 1+Le\lambda_{n-1} \ll 1+D_s\delta Me/D$. Le nombre des k possibles est $\leqslant \max\widetilde{\varphi}(m) - \min\widetilde{\varphi}(m) \ll \eta + D\lambda_{n-1}/e$ (d'après (5.5) et (5.7)) $\ll D\lambda_{n-1}/e$ (d'après (5.1)). On a donc:

$$R(\underline{a}) \ll \frac{D\lambda_{n-1}}{e}\Big(1 + \frac{D_s}{D}\delta Me\Big) = \frac{M\lambda_n D}{e} + M\delta\lambda_{n-1}D_s. \qquad \text{c.q.f.d.}$$

5.3. Démonstration du Théorème 1. On dispose de l'hypothèse $\delta \ll \lambda_{n-1}$, mais on peut se ramener, par un argument standard, à $\delta \ll \lambda_{n-1}$ (il suffit de décomposer la bande $\mathcal{B} = \{(x,y) \mid M \leqslant x \leqslant 2M, f(x) \leqslant y \leqslant f(x)+\delta\}$, d'épaisseur δ, en K bandes $\mathcal{B}_1, \ldots, \mathcal{B}_K$ d'épaisseur δ/K).

On applique le Lemme 4 à l'ensemble S:

$$R \ll \sum_{a_1=1}^{A} \cdots \sum_{a_{n-1}=1}^{A} R(\underline{a}) + \frac{M}{A} + 1, \tag{5.18}$$

oà A est un paramètre à déterminer, et où $S(\underline{a})$ vérifie (3.4). D'après la partie (i) du Lemme 8, ou bien $S(\underline{a})$ est vide, ou bien $\underline{a}$ est dans le premier cas. Dans tous les cas, on peut majorer $R(\underline{a})$ par (5.14). D'autre part, on a $D \ll A^{n(n-1)/2}$ et $D_s \ll A^{(n-1)(n-2)/2}$. On reporte ces inégalités dans (5.14), puis dans (5.18); on optimise sur A et on obtient finalement (1.7). c.q.f.d.

5.4. Démonstration du Théorème 2. On applique le Lemme 5 à l'ensemble S:

$$R \ll \sum_{a_1=1}^{A} \cdots \sum_{a_{n-1}=1}^{A} R(\underline{a}) + \frac{M}{A} + M\delta^{\frac{2}{(n-1)(n-2)}} + \Big(\frac{\delta}{\lambda_{n-1}}\Big)^{\frac{1}{n-1}} + 1, \tag{5.19}$$

où A est un paramètre libre, et où $S(\underline{a})$ vérifie (3.4) et (3.6).

On se restreint à $A \ll \delta^{-2/((n-1)(n-2))}$. Dans ce cas, la partie (ii) et la partie (iii) du Lemme 8 montrent que, ou bien $\underline{a}$ est dans le premier cas, ou bien $S(\underline{a})$ est vide. On peut donc toujours majorer $R(\underline{a})$ par (5.14). En reportant les inégalités $D \ll A^{n(n-1)/2}$ et $D_s \ll A^{(n-1)(n-2)/2}$ dans (5.14), puis dans (5.19), on obtient:

$$\begin{aligned} R \ll \min_{1 \leqslant A \ll \delta^{-2/((n-1)(n-2))}} & \Big\{ M\lambda_n A^{\frac{n(n+1)}{2}} - 1 + M\delta\lambda_{n-1} A^{\frac{(n^2-n+2)}{2}} - 1 + \frac{M}{A} \Big\} \\ & + M\delta^{\frac{2}{(n-1)(n-2)}} + \Big(\frac{\delta}{\lambda_{n-1}}\Big)^{\frac{1}{n-1}} + 1. \end{aligned} \tag{5.20}$$

Dans cette inégalité, la restriction $A \ll \delta^{-2/((n-1)(n-2))}$ peut être levée au prix d'un terme supplémentaire $M\delta^{2/(n-1)(n-2)}$ (mais ce terme existe déjà). En optimisant sur A, on obtient finalement (1.9). c.q.f.d.

5.5. Majoration de $R(\underline{a})$ dans le 3ème cas.

Lemme 10. *On suppose que $\underline{a}$ est dans le 3ème cas et que $S(\underline{a})$ vérifie (3.4). Alors on a:*

$$R(\underline{a}) \ll M\frac{D_s^2\delta^2}{D}\Big(1 + \frac{1}{M\lambda_{n-1}}\Big). \tag{5.21}$$

Démonstration. On reprend les notations concernant φ, ψ et $S_k(\underline{a})$.

a) Dans un premier temps, on veut établir la propriété suivante:

$$\text{Si } m \text{ et } m+b \in S_k(\underline{a}), \text{ alors ou bien } b \ll \frac{D_{st}\delta}{D_s\lambda_{n-1}}, \text{ ou bien } b \gg \frac{1}{e\lambda_{n-1}}, \tag{5.22}$$

où D_{st} est défini en (5.12). Pour cela, on fixe m et $m+b \in S_k(\underline{a})$.

On suppose d'abord $\widetilde{\psi}(m) = 0$. Alors, d'après (5.12), on a $\psi(m) \ll \delta D_{st}$, et, d'après (5.10), on a $\psi(m) \asymp bD_s\lambda_{n-1}$, d'où $b \ll D_{st}\delta/(D_s\lambda_{n-1})$.

On suppose maintenant $\widetilde{\psi}(m) \neq 0$. Alors, par la relation de divisibilité (5.13), on a $|\widetilde{\psi}(m)| \geqslant D_s/e$, d'où $|\psi(m)| \geqslant D_s/e - |\beta(m)|$. Si, dans (5.22), l'inégalité $b \ll D_{st}\delta/(D_s\lambda_{n-1})$ n'est pas satisfaite, alors $b \gg D_{st}\delta/(D_s\lambda_{n-1})$, ce qui implique $|\psi(m)| \gg \beta$ d'après (5.10). On en déduit que $|\psi(m)| \gg D_s/e$, et par suite, d'après (5.10), que $b \gg 1/(e\lambda_{n-1})$. On a bien prouvé (5.22).

b) La propriété (5.22) signifie que $S_k(\underline{a})$ est formé de blocs dont le longueur est $\ll D_{st}\delta/(D_s\lambda_{n-1})$, séparés par des distances $\gg 1/(e\lambda_{n-1})$.

D'après (3.4), chaque bloc contient au plus $1 + 0(D_{st}\delta/(aD_s\lambda_{n-1})$ éléments; comme

$$\frac{D_{st}}{aD_s} = \frac{D_s}{D} \times \frac{|d_s - d_t|}{a} \leqslant \frac{D_s}{D},$$

et comme $D_s/(D\lambda_{n-1}) \gg 1$, chaque bloc possède $0(D_s\delta/(D\lambda_{n-1}))$ éléments, par (5.3). Dans chaque $S_k(\underline{a})$, le nombre de blocs est $\leqslant 1 + 0(Me\lambda_{n-1})$, puisque $S_k(\underline{a}) \subset [M, 2M]$, d'où:

$$\sharp\, S_k(\underline{a}) \ll \frac{D_s\delta}{D\lambda_{n-1}}(1 + M\lambda_{n-1}e). \tag{5.23}$$

Il ne reste plus qu'à majorer le nombre K des valeurs k prises par $\widetilde{\varphi}(m)$. Mais on a

$$\widetilde{\varphi}(m) = \varphi(m) - \eta(m) \ll \frac{D\lambda_{n-1}}{e} + \frac{D_s\delta}{e} \ll \frac{D_s\delta}{e},$$

d'après (5.3), d'où $K \ll D_s\delta/e$. On obtient le résultat cherché en écrivant:

$$R(\underline{a}) = \sum_k \big(\sharp\, S_k(\underline{a})\big) \ll M\frac{D_s^2\delta^2}{D} + \frac{D_s^2\delta^2}{eD\lambda_{n-1}}. \qquad \text{c.q.f.d.}$$

5.6. Démonstration du Théorème 3. On applique le Lemme 6 à l'ensemble S, ce qui donne:

$$R \ll H\sum_{a_1=1}^{A} \cdots \sum_{a_{n-1}=1}^{A} R(\underline{a}) + \frac{HM}{A} + M\delta^{\frac{1}{n-2}} + \Big(\frac{\delta}{\lambda_{n-1}}\Big)^{\frac{1}{n-1}} + H, \tag{5.24}$$

où H est défini en (2.11) et vérifie (2.12), où $S(\underline{a})$ vérifie (3.4) et (3.6), et où A est un paramètre libre. Pour chaque $\underline{a}$, ou bien $\underline{a}$ est dans le 3ème cas et on peut majorer $R(\underline{a})$ par (5.21), ou bien $S(\underline{a})$ est vide. Dans tous les cas, on a:

$$R(\underline{a}) \ll M\lambda_n D + M\delta\lambda_{n-1}D_s + M\frac{D_s^2\delta^2}{D}\Big(1+\frac{1}{M\lambda_{n-1}}\Big). \tag{5.25}$$

On majore D par $A^{n(n-1)/2}$, D_s par $A^{(n-1)(n-2)/2}$, et enfin D_s/D par $1/(a_1\dots a_{n-1})$; ce dernier terme, dans la sommation sur $\underline{a}$, fait apparaître un facteur $(\log M)^{n-1}$ qui est absorbé par le facteur M^ε. Il ne reste plus qu'à reporter (5.25) dans (5.24), puis à optimiser sur A pour obtenir (1.10) c.q.f.d.

6. Démonstration des Théorèmes 4, 5 et 6

Nous reprenons la majoration de $R(\underline{a})$ dans le 1er cas (cf. (5.1)). D'une façon approximative, on peut dire que, dans le Lemme 9, on applique à une certaine fonction ψ un argument faisant intervenir l'ordre de grandeur de ψ'; dans le Lemme 13 ci-dessous, on utilise l'ordre de grandeur de ψ'', d'où l'apparition d'un facteur $\lambda_n^{1/3}$ à la place de λ_{n-1}. Les arcs majeurs, relativement à ψ'', requièrent l'essentiel du travail. L'argument de divisibilité intervient dans le choix de ψ ; sans lui, il faudrait considérer la fonction $D_s\psi(x)/e$ au lieu de $\psi(x)$, avec un résultat moins bon.

6.1. Retour sur les arcs majeurs. Nous apportons une précision au Théorème 2 de [10]:

Lemme 11. *Soit $g : [c, c+N] \to \mathbb{R}$ une fonction de classe C^r ($c \in \mathbb{Z}$, r entier fixé $\geqslant 2$, N entier $\geqslant 4$), vérifiant:*

$$|g^{(r)}(x)| \asymp \mu, \quad \text{pour } c \leqslant x \leqslant c+N, \tag{6.1}$$

et soit δ ($0 < \delta \leqslant 1/4$). Soit S un sous-ensemble de $\widetilde{S} = \{m \in [c, c+N] \cap \mathbb{Z} \mid \|g(m)\| \leqslant \delta\}$. Soit $\mathcal{P}$ l'ensemble des arcs majeurs (relativement à S), au sens de la section 2. Soit $R = (\sharp\, S)$. Alors on a:

$$R \ll_r N\mu^{\frac{2}{r(r+1)}} + N\delta^{\frac{2}{r(r-1)}} + \max_{\mathcal{A}\in\mathcal{P}}(\sharp\,\mathcal{A}) + 1. \tag{6.2}$$

Dans le cas où $S = \widetilde{S}$, le Lemme 11 est identique au Théorème 2 de [10]; nous l'utiliserons dans le cas $r = 2$, dont la démonstration avait été omise dans [10]. C'est pourquoi nous donnons la preuve complète:

Démonstration. Soit S_0 l'ensemble des points de S qui proviennent des arcs majeurs. On pose $S_1 = S \setminus S_0$, $R_0 = (\sharp\, S_0)$, $R_1 = (\sharp\, S_1)$. Par le Lemme 1, on a:

$$R_0 \ll N\delta^{\frac{2}{r(r-1)}} + \max_{\mathcal{A}\in\mathcal{P}}(\sharp\,\mathcal{A}).$$

Soit maintenant $G = \{m_0, m_1, \ldots, m_{r^2}\}$ un groupe formé de r^2+1 points consécutifs de S_1. Comme G n'est contenu dans aucun arc majeur, on peut trouver un indice j $(r \leqslant j \leqslant r^2)$ tel que les points du plan $\big(m_0, \tilde{f}(m_0)\big), \big(m_1, \tilde{f}(m_1)\big), \ldots, \big(m_{r-1}, \tilde{f}(m_{r-1})\big), \big(m_j, \tilde{f}(m_j)\big)$ ne soient pas tous sur une courbe polynomiale $\{y = P(x)\}$, avec P de degré $< r$. On peut appliquer à ces points le Lemme 2 de [10], avec pour résultat:

$$m_{r^2} - m_0 \gg \min\Big\{\mu^{-\frac{2}{r(r+1)}}, \delta^{-\frac{2}{r(r-1)}}\Big\}.$$

De là on déduit que:

$$R_1 \ll N\Big(\mu^{\frac{2}{r(r+1)}} + \delta^{\frac{2}{r(r-1)}}\Big) + 1. \qquad \text{c.q.f.d.}$$

6.2. Arcs majeurs dans une famille de sous-intervalles. Nous poursuivons l'étude des arcs majeurs avec un Lemme qui répond à une situation très particulière:

Lemme 12. *Soit $\psi : [M, 2M] \to \mathbb{R}$ une fonction de classe C^2 telle que:*

$$|\psi''(x)| \asymp \mu, |\psi'(x)| \asymp M\mu, \quad \text{pour } M \leqslant x \leqslant 2M. \tag{6.3}$$

Soient $I_1, \ldots, I_K$ des sous-intervalles de $[M, 2M]$, de longueur au plus L, séparés entre eux par une distance $\geqslant d$. Pour chaque $k = 1, \ldots, K$, soient γ_k un réel et S_k un sous-ensemble de $\widetilde{S}_k = \{m \in I_k \mid \|\psi(m) - \gamma_k\| \leqslant \beta\}$ tel que deux points consécutifs de S_k soient distants d'au moins a ($\beta > 0$, a entier $\geqslant 1$), avec $\beta \ll \mu a M$. On pose $R_k = (\sharp\, S_k)$, et

$$R = \sum_{k=1}^{K} R_k.$$

Alors on a:

$$R \ll KL\mu^{1/3} + KL\beta + K + \sqrt{MK\beta} + \frac{M\beta^{3/2}}{d\mu^{1/2}}\mathcal{L}, \tag{6.4}$$

avec $\mathcal{L} = \log(2 + K/(M\mu))$.

Démonstration. a) On commence par appliquer le Lemme 11, avec $r = 2$, à chaque intervalle I_k : $R_k \ll L\mu^{1/3} + L\beta + (\sharp\, \mathcal{A}_k) + 1$, où $\mathcal{A}_k$ est un arc majeur relativement à S_k, de longueur $\ll L' := \sqrt{\beta/\mu}$, d'après (2.4). Soient alors I'_k le plus court intervalle contenant $\mathcal{A}_k$, et $R'_k = (\sharp\, \mathcal{A}_k)$. On a:

$$R \ll KL\mu^{1/3} + KL\beta + K + \sum_{k=1}^{K} R'_k. \tag{6.5}$$

On doit majorer

$$R' = \sum_{k=1}^{K} R'_k,$$

ce qui revient à traiter le problème initial dans lequel on a remplacé I_k par I'_k, L par L' et S_k par $\mathcal{A}_k$ (on remarque que, comme $\mathcal{A}_k \subset S_k$, deux points consécutifs de $\mathcal{A}_k$ sont distants d'au moins a). On est donc ramené à prouver (6.4) sous l'hypothèse supplémentaire:

$$L \ll \sqrt{\frac{\beta}{\mu}}. \tag{6.6}$$

b) On applique le procédé de réduction du Lemme 4, avec $r = 1$, à chaque S_k: pour chaque entier q ($a \leqslant q \leqslant Q$), on peut trouver un ensemble $S_k(q) \subset \{m \mid m \text{ et } m+q \in S_k\}$, tel que deux éléments de $S_k(q)$ soient distants d'au moins q, et tel que:

$$R_k \ll \sum_{q=a}^{Q} R_k(q) + \frac{L}{Q} + 1, \quad \text{avec } R_k(q) = \big(\sharp\, S_k(q)\big).$$

On a donc:

$$R = \sum R_k \ll \frac{KL}{Q} + K + \sum_{q=a}^{Q} \Big(\sum_{k=1}^{K} R_k(q) \Big).$$

On prend $Q \asymp \sqrt{K/M\mu}$. Si $a \geqslant Q$, la majoration $R_k \ll L/a$ conduit au résultat cherché. On suppose donc $a < Q$, et on a:

$$R \ll K + \sqrt{MK\beta} + \sum_{q=a}^{Q} \Big(\sum_{k=1}^{K} R_k(q) \Big). \tag{6.7}$$

D'autre part, on a:

$$R_k(q) \ll L/q. \tag{6.8}$$

En effet, deux points de $S_k(q)$ sont espacés d'au moins q et donc: $R_k(q) \ll L/q+1$. Si $L/q \ll 1$, alors $S_k(q) = \emptyset$, ce qui prouve (6.8).

c) On fixe q et on majore

$$R(q) = \sum_{k=1}^{K} R_k(q).$$

Pour chaque entier ℓ, on pose: $T_\ell = \{x \in [M, 2M] \mid |\psi(x+q) - \psi(x) - \ell| \leqslant 2\beta\}$. Si on pose

$$S(q) = \bigcup_{k=1}^{K} S_k(q),$$

on a

$$R(q) = \sum_\ell \Big(\sharp\big(S(q) \cap T_\ell\big)\Big).$$

Le nombre des entiers ℓ tels que $S(q) \cap T_\ell \neq \emptyset$ est $\ll q\mu M$. En effet, on a $|\psi(x+q) - \psi(x)| \asymp q\mu M$, et le résultat est vrai si $q\mu M \gg 1$. Si, au contraire, on a $q\mu M \ll 1$, alors la condition $\beta \ll aM\mu \leqslant qM\mu$ montre que $S(q) = \emptyset$, et le résultat est encore vrai. On a donc montré:

$$R(q) \ll q\mu M \max_\ell \Big(\sharp\big(S(q) \cap T_\ell\big)\Big). \tag{6.9}$$

Mais chaque T_ℓ est un intervalle de longueur $\ll \beta/q\mu$ et rencontre au plus $1 + 0(\beta/q\mu d)$ ensembles $S_k(q)$. Compte tenu de (6.8), on en déduit:

$$\sharp\big(S(q) \cap T_\ell\big) \ll \Big(1 + \frac{\beta}{q\mu d}\Big)\frac{L}{q}.$$

D'après (6.6) et (6.9) on a donc:

$$R(q) \ll \frac{M\beta^{3/2}}{qd\mu^{1/2}} + M\mu^{1/2}\beta^{1/2}.$$

Il ne reste plus qu'à sommer sur q pour obtenir (6.4). c.q.f.d.

6.3. Une variante du Lemme 9. On utilise les notations de la section 5.1.

Lemme 13. *Si $\underline{a}$ est dans le premier cas (i.e. si on suppose (5.1)) et si $S(\underline{a})$ vérifie (3.4), alors on a:*

$$\begin{aligned} R(\underline{a}) &\ll M\lambda_n D + M\delta\lambda_n^{\frac{1}{3}} D_s + M\delta^2 D_{st} \\ &\quad + M\Big(\lambda_n \delta \frac{DD_{st}}{D_s}\Big)^{1/2} + M\lambda_n^{\frac{1}{2}}\delta^{3/2} D \Big(\frac{D_{st}}{D_s}\Big)^{3/2}\mathcal{L}, \end{aligned} \tag{6.10}$$

avec $\mathcal{L} = \log(2 + \lambda_n^{-1})$ (D, D_s ont été définis à la section 5.1, D_{st} est défini à la section 5.2).

Démonstration. On reprend la fonction φ définie en (5.4). Comme $S(\underline{a})$ est contenu dans $\{x \in [M, 2M] \mid \|\varphi(x)\| \ll \eta\}$ (où η est défini en (5.7)), on se ramène à la situation du Lemme 12 en posant:

$$I_k = \{x \in [M, 2M] \mid |\varphi(x) - k| \ll \eta\}, \tag{6.11}$$

où k est un entier tel que $k \asymp K := D\lambda_{n-1}/e$ (la notation $:=$ signifie que l'égalité est une définition). Comme $|\varphi(x)| \asymp D\lambda_{n-1}/e \gg \eta$, d'après (5.1), si $D\lambda_{n-1}/e \ll 1$, alors $S(\underline{a}) = \emptyset$, et on peut toujours supposer $K \gg 1$. On a:

$$S(\underline{a}) \subset \bigcup_{k \asymp K} I_k$$

.

Par (5.5) et (5.7), la longueur de chaque I_k est $\ll L := D_s\delta/(D\lambda_n)$. On définit maintenant la fonction ψ annoncée au début de la section 6:

$$\psi(x) = ef[x+d_0,\dots,\widehat{x+d_s},\dots,x+d_{n-1}] \tag{6.12}$$

(on rappelle que s est l'indice fixé au 5.1 et que e est défini en (4.12)). On a $|\psi'(x)| \asymp \mu M$ et $|\psi''(x)| \asymp \mu$, avec $\mu := e\lambda_n$. Posons $\psi_0(x) = D_s f[x+d_0,\dots,\widehat{x+d_s},\dots,x+d_{n-1}] = D_s\psi(x)/e$, et, si $m \in S(\underline{a})$, $\widetilde{\psi}_0(m) = D_s\tilde{f}[x+d_0,\dots,\widehat{x+d_s},\dots,x+d_{n-1}]$. On sait que, si $m \in S(\underline{a})$, on a, d'après (4.9):

$$\psi_0(m) = \widetilde{\psi}_0(m) + 0(D_{st}\delta).$$

En posant $S_k'(\underline{a}) = S(\underline{a}) \cap I_k$ et $R_k'(\underline{a}) = \big(\sharp\, S_k'(\underline{a})\big)$, on pourrait obtenir une majoration de $R_k'(\underline{a})$ meilleure que la majoration triviale (i.e. $R_k'(\underline{a}) \ll L/a$) en considérant les points entiers au voisinage de la courbe $\{y = \psi_0(x) \mid x \in I_k\}$. Mais on peut faire beaucoup mieux grâce au Lemme de divisibilité. En effet, si m et $m+b \in S_k'(\underline{a})$, ce dernier nous dit que $\widetilde{\psi}_0(m+b) - \widetilde{\psi}_0(m)$ est divisible par D_s/e, ce qui implique en particulier que:

$$\|\psi(m+b) - \psi(m)\| \ll \beta := eD_{st}\delta/D.$$

Alors, pour chaque k tel que $S(\underline{a}) \cap I_k \neq \emptyset$, on choisit un certain m_k dans cet ensemble, et on pose $\gamma_k = \psi(m_k)$. Il est clair qu'on a la relation:

$$S(\underline{a}) \subset \bigcup_{k \asymp K} S_k(\underline{a}), \quad \text{avec } S_k(\underline{a}) = \{m \in I_k \cap \mathbb{N} \mid \|\psi(m) - \gamma_k\| \ll \beta\}. \tag{6.13}$$

Pour se placer exactement dans les hypothèses du Lemme 12, il faut encore assurer que les I_k sont bien espacés. Il en est bien ainsi si $\eta \ll 1$, et on peut prendre $d = M/K$; on obtient alors (6.10) par simple application de (6.4).

Supposons maintenant $\eta \gg 1$. On se ramène à la situation précédente en divisant la famille des I_k en $0(\eta)$ sous-familles, formées de $0(K/\eta)$ intervalles qui sont espacés d'une distance $\gg d' := \eta M/K$. On applique (6.4) à chacune de ces sous-familles, puis on somme les $0(\eta)$ majorations obtenues, ce qui donne:

$$\begin{aligned} R(\underline{a}) &\ll M\lambda_n D + M\delta\lambda_n^{\frac{1}{3}} D_s + M\delta^2 D_{st} \\ &\quad + M(\lambda_n D\delta^2 D_{st})^{1/2} + M\lambda_n^{\frac{1}{2}}\delta^{\frac{3}{2}} D\Big(\frac{D_{st}}{D_s}\Big)^{3/2}\mathcal{L}. \end{aligned}$$

Dans le membre de droite ci-dessus, le quatrième terme est dominé par la somme du premier et du troisième, si bien que (6.10) est encore vérifié dans ce cas. c.q.f.d.

6.4. Démonstration des Théorèmes 4, 5 et 6. Pour démontrer les Théorèmes 4, 5 et 6, on reprend mot pour mot les sections 5.3, 5.4 et 5.6 respectivement, en prenant soin de remplacer la majoration du Lemme 9 par celle du Lemme 13. Il apparaît des termes supplémentaires par rapport aux résultats annoncés en (1.11), (1.14) et (1.15); mais ceux-ci disparaissent parce qu'ils sont dominés par la somme des autres. Nous allons détailler cela en démontrant, par exemple, le Théorème 4.

On part de l'inégalité (5.18). On majore $R(\underline{a})$ par le Lemme 13, en remarquant que:

$$\frac{DD_{st}}{D_s} \leqslant aD_s \leqslant a^{\frac{n^2-3n+4}{2}}$$

et que:

$$D\Big(\frac{D_{st}}{D_s}\Big)^{3/2} = D\Big(\frac{D_s}{D}|d_s - d_t|\Big)^{3/2} \leqslant a^{3/2}\Big(\frac{D_s}{D}\Big)^{1/2} D_s$$
$$\leqslant \frac{a^{(n^2-3n+5)/2}}{(a_1 a_2 \dots a_{n-1})^{1/2}}.$$

On obtient alors:

$$R \ll M\lambda_n A^{\frac{n^2+n}{2}-1} + M\delta^2 A^{\frac{n^2-3n+5}{2}-1} + M\delta\lambda_n^{\frac{1}{3}} A^{\frac{n^2-n+2}{2}-1} + M\lambda_n^{\frac{1}{2}}\delta^{\frac{1}{2}} A^{\frac{n^2+n+4}{4}-1} + M\lambda_n^{\frac{1}{2}}\delta^{\frac{3}{2}} A^{\frac{n^2-3n+6}{2}-1}\mathcal{L} + \frac{M}{A} + 1.$$

En optimisant sur A, on en déduit:

$$R \ll M\lambda_n^{\frac{2}{n^2+n}} + M(\delta\lambda_n^{\frac{1}{3}})^{\frac{2}{n^2-n+2}} + M\delta^{\frac{4}{n^2-3n+6}} + M(\delta\lambda_n)^{\frac{2}{n^2+n+4}} + M(\delta^3\lambda_n\mathcal{L}^2)^{\frac{1}{n^2-2n+6}} + 1.$$

On vérifie que le 4ème et le 5ème terme du membre de droite ci-dessus sont dominés par la somme des trois premiers. On en déduit (1.11) et le Théorème 4 est démontré. On prouverait de même les Théorèmes 5 et 6 . c.q.f.d.

References

[1] M. Branton et O. Ramaré, *Nombre de racines d'un polynôme entier modulo q*, J. Théor. Nombres Bordeaux 10(1) (1998), 125–134.
[2] M. Branton et P. Sargos, *Points entiers au voisinage d'une courbe plane à très faible courbure.* Bull. Sci. Math. 118 (1994), 15–28.
[3] M. Filseta et O. Trifonov, *The distribution of fractional parts with applications to gap results in number theory.* Proc. London Math. Soc (3) 73 (1996), 241–278.
[4] E. Fouvry et H. Iwaniec, *Exponential sums for monomials.* J. Number Theory 33 (1989), 311–333.
[5] S.W. Graham et G. Kolesnik, *Van der Corput's method of exponential sums.* Cambridge University Press (1991).

[6] M.N. Huxley, *The integer points close to a curve.* Mathematika 36 (1989), 198–215.
[7] M.N. Huxley, *Exponential sums and lattice points.* Proc. London Math. Soc. (3) 60 (1990), 471–502.
[8] M.N. Huxley, *Exponential sums and rounding error.* J. London Math. Soc. (2) 43 (1991), 367–384.
[9] M.N. Huxley et G. Kolesnik, *Exponential sums with a large second derivative.* Number Theory (ed. M. Jutila, et T. Metsänkylä) De Gruyter, Berlin (2001), 131–144.
[10] M.N. Huxley et P. Sargos, *Points entiers au voisinage d'une courbe plane de classe C^n.* Acta Arith. 69 (1995), 359–366.
[11] P. Sargos, *Points entiers au voisinage d'une courbe, sommes trigonométriques courtes et paires d'exposants.* Proc. London Math. Soc. (3) 70 (1995), 285–312.
[12] J. Stoer et R. Bulirsch, *Introduction to numerical analysis.* Springer Verlag (1980).

Addresses: M.N. Huxley, School of Mathematics, University of Wales, College of Cardiff, 23, Senghennydd Road, Cardiff, CF24 4AG, Wales, U.K.;
P. Sargos, Institut Elie Cartan, Université Henri Poincaré, Nancy 1, B.P. 239, 54506 Vandoeuvre lès Nancy Cedex, France
E-mail: `Huxley@cardiff.ac.uk; Sargos@iecn.u-nancy.fr`
Received: 19 March 2005