ACTA ARITHMETICA
LXIX.4 (1995)

Points entiers au voisinage d'une courbe plane de classe C^n

par

M. N. Huxley (Cardiff) et P. Sargos (Nancy)

1. Introduction et énoncé du résultat. Soient $a \in \mathbb{R}$, N un entier ≥ 2, $f : [a, a+N] \to \mathbb{R}$ une fonction de classe C^n ($n \geq 2$) et $\delta \in \mathbb{R}$ ($0 \leq \delta \leq 1/4$). On pose :

$$\Gamma_\delta = \{(x,y) \in \mathbb{R}^2 \mid a \leq x \leq a+N,\ |y - f(x)| \leq \delta\} \tag{1.1}$$

et

$$\nu(\Gamma_\delta) = \#(\Gamma_\delta \cap \mathbb{Z}^2).$$

Le problème annoncé dans le titre consiste à majorer $\nu(\Gamma_\delta)$. On fait l'hypothèse :

$$|f^{(n)}(x)| \asymp \lambda, \quad \text{pour } a \leq x \leq a+N, \tag{1.2}$$

où λ est un réel positif "petit". On cherche des majorations de la forme

$$\nu(\Gamma_\delta) \ll N\lambda^{\alpha_n} + N\delta^{\beta_n} + \text{ termes secondaires}, \tag{1.3}$$

où les termes secondaires ne peuvent dominer que dans la situation marginale où λ est trop petit.

Les majorations de $\nu(\Gamma_\delta)$ obtenues par des méthodes de sommes d'exponentielles fournissent la valeur optimale $\beta_n = 1$ mais avec une valeur de α_n trop faible. Par exemple, le résultat classique de van der Corput (cf. [3], Théorème 2.8), qui s'applique sous la seule hypothèse (1.2), donne la valeur $\alpha_n = 1/(2^n - 1)$, avec en outre des termes secondaires élevés.

En se ramenant par un procédé de nature combinatoire au cas facile où $n = 1$, le premier auteur [4] a obtenu une amélioration de α_n, substantielle pour n grand, au détriment de β_n. Le résultat est

$$\nu(\Gamma_\delta) \ll N\lambda^{2/(n(n+1))} + N\delta^{2/(n(n-1)+2)} + \delta\lambda^{-1}(\log N)^n + N^{1-1/n} + 1, \tag{1.4}$$

sous la seule hypothèse (1.2).

Par une méthode géométrique simple, nous améliorons (1.4) en remplaçant $\beta_n = 2/(n(n-1)+2)$ par $\beta_n = 2/(n(n-1))$, mais surtout en obtenant les termes secondaires optimaux. Notre résultat s'énonce ainsi.

Théorème 1. *Sous la seule hypothèse* (1.2), *on a*

$$\nu(\Gamma_\delta) \ll N\lambda^{2/(n(n+1))} + N\delta^{2/(n(n-1))} + (\delta\lambda^{-1})^{1/n} + 1 \tag{1.5}$$

(*le symbole* $\ll$ *sous-entend une constante qui ne dépend que de* n *et des constantes sous-entendues dans* (1.2)).

Dans le cas $n = 2$, ce résultat a été obtenu dans [1] par une méthode similaire. Le passage du cas $n = 2$ au cas $n \geq 3$ fait apparaître des difficultés dues au fait que les "arcs majeurs" ne sont plus des segments. Par ailleurs, le Lemme 3.4 de [1], sur l'espacement des arcs majeurs, est remplacé par le Lemme 7 qui semble plus adapté et qui permet, dans le cas $n = 2$, d'obtenir une importante simplification dans la démonstration de [1].

Concernant les améliorations ultérieures, signalons un article de Filaseta et Trifonov [2] dans lequel l'exposant β_n est meilleur que le nôtre dès que la dérivée $(n-1)$-ième est suffisamment petite, et que certaines contraintes sont satisfaites.

Cependant, à cause de la simplicité de nos hypothèses, et surtout à cause des termes secondaires, l'intérêt de notre résultat subsiste.

Notations. Soient u et v deux réels positifs. La notation : $u \ll v$ signifie: $u \leq Av$, où A est une constante qui ne dépend que de n et des constantes introduites antérieurement. Comme d'habitude, $u \asymp v$ signifie qu'on a à la fois : $u \ll v$ et $v \ll u$.

La lettre M désigne systématiquement un élément de $\mathbb{Z}^2$ (point entier ou point à coordonnées entières), d'abscisse m et d'ordonnée l : $M = (m, l)$, $M_i = (m_i, l_i), \ldots$

Si E est une partie du plan, $\nu(E)$ est le nombre de points entiers de $E : \nu(E) = \#(E \cap \mathbb{Z}^2)$. Si $\mathcal{P}$ est une famille de parties du plan, on pose

$$\nu(\mathcal{P}) = \nu\Big(\bigcup_{E\in\mathcal{P}} E\Big).$$

Dans tout ce qui suit, on suppose $n \geq 2$.

2. Espacement des points isolés. Nous présentons deux lemmes de base. Le premier a été introduit dans le problème par Swinnerton-Dyer [5] et généralise, d'une certaine façon, la formule des accroissements finis. Le deuxième, qui est une conséquence du premier, montre que si $n + 1$ points entiers de Γ_δ sont "en position générale", alors ils sont bien espacés. Cela permet déjà de montrer que le nombre de points sur la courbe (cas $\delta = 0$) vérifie

$$\nu(\Gamma_0) \ll N\lambda^{2/(n(n+1))} + 1. \tag{2.1}$$

LEMME 1. *Soit $g : [a, b] \to \mathbb{R}$ une fonction C^k. Etant donnés $a \le x_0 < x_1 < \ldots < x_k \le b$, on désigne par $Q(x)$ l'unique polynôme de degré $\le k$ vérifiant $Q(x_i) = g(x_i)$ pour $i = 0, 1, \ldots, k$. Alors il existe $\xi \in \,]x_0, x_k[$ tel que $Q^{(k)}(\xi) = g^{(k)}(\xi)$.*

La démonstration consiste en une application répétée du Théorème de Rolle (cf. [5]). Rappelons que la formule d'interpolation de Lagrange qui donne $Q(x)$ s'écrit :

$$Q(x) = \sum_{j=0}^{k} \left(\prod_{i \ne j} \frac{x - x_i}{x_j - x_i} \right) g(x_j),$$

où la notation abrégée $\prod_{i \ne j}$ signifie $\prod_{0 \le i \le k,\, i \ne j}$.

Pour le lemme suivant, nous n'aurons pas besoin de l'hypothèse (1.2), mais seulement de la propriété :

$$|f^{(n)}(x)| \le \mu \quad \text{pour } a \le x \le a + N. \tag{2.2}$$

LEMME 2. *Soient $M_0, M_1, \ldots, M_n$ $n + 1$ points entiers de Γ_δ, vérifiant $a \le m_0 < m_1 < \ldots < m_n \le a + N$, et qui ne sont pas tous sur une même courbe polynômiale de degré $< n$. Alors, sous l'hypothèse* (2.2), *on a*

$$m_n - m_0 \ge \min\big(\mu^{-2/(n(n+1))}, \tfrac{1}{6}\delta^{-2/(n(n-1))}\big). \tag{2.3}$$

Par courbe polynômiale de degré $< n$, on entend une courbe $y = P(x)$ où P est un polynôme de degré $< n$, éventuellement nul.

Démonstration. Posons $f(m_i) = l_i + \delta_i$, $|\delta_i| \le \delta$, $i = 0, \ldots, n$. Par le Lemme 1, on peut écrire

$$\frac{1}{n!} f^{(n)}(\xi) = \sum_{j=0}^{n} \frac{l_j + \delta_j}{\prod_{i \ne j}(m_j - m_i)}.$$

De même, si $P(x) = \sum_{j=0}^{n} b_j x^j$ est le polynôme d'interpolation des M_i $(0 \le i \le n)$, alors on a

$$b_n = \sum_{j=0}^{n} \frac{l_j}{\prod_{i \ne j}(m_j - m_i)} = \frac{u}{v},$$

avec $u \in \mathbb{Z}$ et $v = \prod_{0 \le i < j \le n}(m_j - m_i)$. Par hypothèse, $b_n \ne 0$, donc $|u| \ge 1$, d'où

$$\frac{1}{v} \le \frac{1}{n!} |f^{(n)}(\xi)| + \sum_{j=0}^{n} \left| \frac{\delta_j}{\prod_{i \ne j}(m_j - m_i)} \right|$$

et donc

$$1 \le \frac{1}{n!} \mu (m_n - m_0)^{n(n+1)/2} + (n+1)\delta (m_n - m_0)^{n(n-1)/2},$$

et (2.3) en découle.

3. Propriétés des arcs majeurs. Les points entiers de Γ_δ qui se regroupent sur une même courbe polynômiale de degré $< n$ forment des arcs majeurs, et leur contribution, plus difficile à évaluer, fait l'objet du reste de cet article. On commence par quelques propriétés générales.

Dans ce paragraphe, on remplace l'hypothèse (1.2) par la suivante :

$$0 < \lambda \le |f^{(n)}(x)| \quad \text{pour } a \le x \le a + N. \tag{3.1}$$

Soit $P(x) = \sum_{j=0}^{n-1} b_j x^j$ un polynôme à coefficients rationnels; on désigne par q le plus petit entier ≥ 1 tel que $P \in \frac{1}{q}\mathbb{Z}[X]$, et par γ la courbe

$$\{(x, y) \mid x \in \mathbb{R},\ y = P(x)\}.$$

Définition. Un *arc majeur*, d'équation $y = P(x)$, est une composante connexe $\mathcal{A}$ de $\gamma \cap \Gamma_\delta$ vérifiant $\nu(\mathcal{A}) \ge n + 1$. Le *dénominateur* de $\mathcal{A}$ est l'entier q. La *longueur* de $\mathcal{A}$ est la longueur de la projection de $\mathcal{A}$ sur l'axe des x.

Lemme 3. *Au plus n arcs majeurs ont la même équation $y = P(x)$.*

Démonstration. On prolonge, pour simplifier, f en une fonction $\widetilde{f} : \mathbb{R} \to \mathbb{R}$ de classe C^n vérifiant $\widetilde{f}^{(n)}(x) = f^{(n)}(a)$ si $x < a$ et $\widetilde{f}^{(n)}(x) = f^{(n)}(a + N)$ si $x > a + N$, de sorte que $|f^{(n)}(x)| \ge \lambda$ pour $x \in \mathbb{R}$.

Comme les comportements à l'infini de $\widetilde{f}$ et de P sont différents, $\gamma \cap \widetilde{\Gamma}_\delta$ est borné, avec

$$\widetilde{\Gamma}_\delta = \{(x, y) \mid x \in \mathbb{R},\ |\widetilde{f}(x) - y| \le \delta\},$$

si bien que chaque composante connexe $\mathcal{A}$ de $\gamma \cap \widetilde{\Gamma}_\delta$, non réduite à un point, possède deux extrémités vérifiant $P(x) = f(x) \pm \delta$. Supposons qu'il existe $n + 1$ arcs majeurs; alors il existerait $n + 1$ composantes connexes de $\gamma \cap \widetilde{\Gamma}_\delta$, non réduites à un point, et l'équation $P(x) = f(x) + \delta$ (par exemple) admettrait $n + 1$ solutions $x_0, x_1, \ldots, x_n$. Par le Lemme 1, on aurait

$$0 = \frac{P^{(n)}(\xi)}{n!} = \sum_{j=0}^{n} \frac{P(x_j)}{\prod_{i \ne j}(x_j - x_i)} = \sum_{j=0}^{n} \frac{P(x_j) - \delta}{\prod_{i \ne j}(x_j - x_i)} = \frac{f^{(n)}(\xi_1)}{n!} \ne 0,$$

avec contradiction.

Lemme 4. *La longueur d'un arc majeur est $\le 2n(\delta/\lambda)^{1/n}$.*

Démonstration. Soient $y = P(x)$ l'équation d'un arc majeur $\mathcal{A}$ et L la longueur de $\mathcal{A}$. Ecrivons $\varphi(x) = f(x) - P(x)$ et $\mathcal{A} = \{(x, y) \mid c \le x \le c + L,\ y = P(x)\}$.

On pose alors $x_j = c + jL/n$ pour $0 \le j \le n$. Le Lemme 1 montre alors que

$$\frac{f^{(n)}(\xi)}{n!} = \frac{\varphi^{(n)}(\xi)}{n!} = \sum_{j=0}^{n} \frac{\varphi(x_j)}{\prod_{i \ne j}(x_j - x_i)},$$

avec $|\varphi(x_j)| \le \delta$ et $|f^{(n)}(\xi)| \ge \lambda$, si bien que

$$\frac{\lambda}{n!} \le \delta\left(\frac{n}{L}\right)^n \left(\frac{1}{n!} + \frac{1}{(n-1)!1!} + \ldots + \frac{1}{n!}\right) = \delta\left(\frac{n}{L}\right)^n \frac{2^n}{n!},$$

d'où le résultat.

Lemme 5. *Un arc majeur $\mathcal{A}$, de longueur L et de dénominateur q vérifie*

$$\nu(\mathcal{A}) \le (n-1)(Lq^{-2/(n(n-1))} + 1).$$

Démonstration. Considérons n points $M_1, \ldots, M_n \in \mathcal{A}$ avec $m_1 < m_2 < \ldots < m_n$. Si $y = P(x)$ est l'équation de $\mathcal{A}$, alors

$$P(x) = \sum_{j=1}^{n} l_j \prod_{i \ne j} \frac{x - m_i}{m_j - m_i}.$$

En particulier, q divise $\prod_{1 \le i < j \le n}(m_j - m_i) \le (m_n - m_1)^{n(n-1)/2}$, d'où $m_n - m_1 \ge q^{-2/(n(n-1))}$, d'où le lemme.

4. Espacement des arcs majeurs. Nous montrons dans ce paragraphe que les arcs majeurs dont le dénominateur n'est pas trop grand, sont bien espacés. Nous commençons par une propriété intermédiaire générale :

Lemme 6. *Soit $\varphi : [c, c+L] \to \mathbb{R}$ une fonction C^n vérifiant*

$$|\varphi(x)| \le \delta \quad \textit{et} \quad |\varphi^{(n)}(x)| \le \mu \quad \textit{pour } c \le x \le c+L. \tag{4.1}$$

Alors pour tout $x \in [c, c+L]$ et chaque $k = 1, 2, \ldots, n-1$, on a

$$|\varphi^{(k)}(x)| \le (2^n n^{n-1}\delta + \mu L^n)L^{-k}. \tag{4.2}$$

Démonstration. Etant donné k ($1 \le k \le n-1$), on écrit le polynôme d'interpolation de φ aux points $c, c+L/k, c+2L/k, \ldots, c+L$. En raisonnant comme au Lemme 4, on obtient

$$\left|\frac{\varphi^{(k)}(\xi_k)}{k!}\right| \le \frac{(2k)^k}{k!} \cdot \frac{\delta}{L^k}, \qquad \text{pour un certain } \xi_k \ (c < \xi_k < c+L).$$

On utilise la formule de la moyenne :

$$|\varphi^{(k)}(x)| \le |\varphi^{(k)}(\xi_k)| + L \sup_t |\varphi^{(k+1)}(t)|$$

pour majorer successivement $\sup|\varphi^{(n-1)}(x)|, \sup|\varphi^{(n-2)}(x)|, \ldots, \sup|\varphi'(x)|$, et on obtient (4.2).

Pour le lemme suivant, nous n'aurons besoin que de l'hypothèse (2.2).

Lemme 7. *Soit $\mathcal{A}$ un arc majeur, d'équation $y = P(x)$, de longueur L et de dénominateur q, avec $q \le 1/(3\delta)$. Soient $M_0 \in \mathcal{A}$ et $M \in \Gamma_\delta$. On suppose* *que M n'est pas sur la courbe $y = P(x)$. Alors*

$$|m_0 - m| \gg \min\left(L(q\delta)^{-1/(n-1)}, (q\mu)^{-1/n}, \frac{1}{q\mu L^{n-1}}\right). \tag{4.3}$$

Démonstration. Posons $m = m_0 + h$ et supposons, par exemple, $h > 0$. Soit $\varphi(x) = f(x) - P(x)$ et soit $[c, c+L]$ la projection de $\mathcal{A}$ sur l'axe des x. On a

$$\varphi(m) - \varphi(m_0) = \sum_{k=1}^{n-1} \varphi^{(k)}(m_0)\frac{h^k}{k!} + \varphi^{(n)}(\xi)\frac{h^n}{n!} \tag{4.4}$$

pour un certain $\xi \in [c, c+L]$.

Mais $|\varphi(m) - \varphi(m_0)| \gg q^{-1}$. En effet, comme $M = (m, l)$ vérifie $P(m) \neq l$, on a $|P(m) - l| \geq 1/q \geq 1/(3q) + 2\delta$; par suite

$$|\varphi(m) - \varphi(m_0)| \geq |\varphi(m)| - \delta \geq |P(m) - l| - |f(m) - l| - \delta \geq 1/(3q).$$

Maintenant, on majore $|\varphi^{(k)}(m_0)|$ par le Lemme 6 et on reporte ces inégalités dans (4.4) :

$$q^{-1} \ll (\delta + \mu L^n) \sum_{k=1}^{n-1} \left(\frac{h}{L}\right)^k + \mu h^n,$$

et (4.3) en découle.

Voici maintenant la formulation particulière du Lemme 7 dont nous aurons besoin.

Lemme 8. *On suppose que $|f^{(n)}(x)| \asymp \lambda$ pour $x \in [a, a+N]$. Alors il existe une constante B qui ne dépend que de n et des constantes sous-entendues dans* (1.2) *telle que, sous la condition* : $q \leq 1/(B\delta)$, *et sous les hypothèses de Lemme* 7, *on ait* :

$$|m_0 - m| > L \tag{4.5}$$

et

$$|m_0 - m| \gg \min(L(q\delta)^{-1/(n-1)}, (q\lambda)^{-1/n}). \tag{4.6}$$

La démonstration est une conséquence immédiate de (4.3) et du Lemme 4.

5. Démonstration du Théorème. Dans tout ce paragraphe, on suppose que f vérifie (1.2). Nous allons démontrer un résultat légèrement plus précis que le Théorème 1 :

Théorème 2. *Soit $\mathcal{P}$ l'ensemble des arcs majeurs de Γ_δ. Alors on a*

$$\nu(\Gamma_\delta) \ll N\lambda^{2/(n(n+1))} + N\delta^{2/(n(n-1))} + \max_{\mathcal{A}\in\mathcal{P}} \nu(\mathcal{A}) + 1. \tag{5.1}$$

Le Théorème 2 implique le Théorème 1 puisque $\nu(\mathcal{A}) \ll (\delta\lambda^{-1})^{1/n}$, d'après le Lemme 4.

Démonstration. Soit $\mathcal{P}_0$ l'ensemble des arcs majeurs dont le dénominateur est $\le 1/(B\delta)$, B étant la constante du Lemme 8, et soit $\mathcal{R}$ l'ensemble des points entiers de Γ_δ qui ne proviennent pas de $\mathcal{P}_0$. On majore séparément $\nu(\mathcal{P}_0)$ et $\nu(\mathcal{R})$.

(a) *Majoration de* $\nu(\mathcal{R})$. On considère n^2+1 points $M_0, M_1, \ldots, M_{n^2}$ de $\mathcal{R}$ (avec $m_0 < m_1 < \ldots < m_{n^2}$). Si ces points ne sont pas tous sur une même courbe polynômiale de degré $< n$, alors le Lemme 2 montre que

$$m_{n^2} - m_0 \gg \min(\lambda^{-2/(n(n+1))}, \delta^{-2/(n(n-1))}). \tag{5.2}$$

S'ils sont sur une courbe polynômiale de degré $< n$, avec dénominateur $q > 1/(B\delta)$, alors le Lemme 5 montre que : $m_{n^2} - m_0 \gg q^{2/(n(n-1))}$, et (5.2) est encore vérifié.

Il n'y a pas de troisième alternative, car si les points étaient tous sur une courbe polynômiale de degré $< n$, avec dénominateur $q \le 1/(B\delta)$, alors, d'après le Lemme 3, $n+1$ d'entre eux seraient sur un arc majeur $\mathcal{A} \in \mathcal{P}_0$, ce qui est impossible. Donc (5.2) est toujours vérifié, d'où

$$\nu(\mathcal{R}) \ll N\lambda^{2/(n(n+1))} + N\delta^{2/(n(n-1))} + 1. \tag{5.3}$$

(b) *Majoration de* $\nu(\mathcal{P}_0)$. Quitte à multiplier la majoration obtenue par n, on peut supposer, d'après le Lemme 3, que deux arcs majeurs de $\mathcal{P}_0$ n'ont jamais la même équation.

On désigne par σ la projection $\mathbb{R}^2 \ni (x,y) \to x \in \mathbb{R}$. D'après (4.5), les $\sigma(\mathcal{A})$ ne se chevauchent pas; on peut donc, pour chaque $\mathcal{A} \in \mathcal{P}_0$, associer le plus grand intervalle de $[a, a+N]$, noté $I(\mathcal{A})$, contenant $\sigma(\mathcal{A})$, mais ne rencontrant pas $\sigma(\mathcal{A}_1)$ pour tout $\mathcal{A}_1 \ne \mathcal{A}$. Si $|I|$ représente la longueur d'un intervalle I, on a

$$\sum_{\mathcal{A}\in\mathcal{P}_0} |I(\mathcal{A})| \le 2N. \tag{5.4}$$

Par ailleurs, si $\mathcal{A}$ est de longueur L et de dénominateur q, on a, d'après (4.6),

$$|I(\mathcal{A})| \gg \min(L(q\delta)^{-1/(n-1)}, (q\lambda)^{-1/n}),$$

sauf peut-être si $\mathcal{A}$ est à l'une des extrémités de $[a, a+N]$. D'autre part, par le Lemme 5, on a

$$\begin{aligned}\nu(\mathcal{A}) &\ll Lq^{-2/(n(n-1))} \ll |I(\mathcal{A})|\biggl(\frac{(q\delta)^{1/(n-1)}}{L} + (q\lambda)^{1/n}\biggr)Lq^{-2/(n(n-1))}\\ &\ll |I(\mathcal{A})|\delta^{2/(n(n-1))},\end{aligned}$$

la dernière inégalité prenant en compte le fait que $q \ll \delta^{-1}$ et que $L \ll (\delta/\lambda)^{1/n}$. On reporte cette inégalité dans (5.4), en prenant soin d'ajouter la contribution des arcs majeurs situés aux extrémités, ce qui donne :

$$(5.5) \qquad \nu(\mathcal{P}_0) \ll \max_{\mathcal{A}\in\mathcal{P}_0} \nu(\mathcal{A}) + N\delta^{2/(n(n-1))}.$$

Le Théorème 2 est entièrement démontré.

Bibliographie

[1] M. Branton et P. Sargos, *Points entiers au voisinage d'une courbe plane à très faible courbure*, Bull. Sci. Math. 118 (1994), 15–28.

[2] M. Filaseta and O. Trifonov, *The distribution of fractional parts with applications to gap results in Number Theory*, à paraître.

[3] S. W. Graham and G. Kolesnik, *Van der Corput's Method of Exponential Sums*, London Math. Soc. Lecture Note Ser. 126, Cambridge University Press, 1991.

[4] M. N. Huxley, *The integer points close to a curve*, Mathematika 36 (1989), 198–215.

[5] H. P. F. Swinnerton-Dyer, *The number of lattice points on a convex curve*, J. Number Theory 6 (1974), 128–135.

SCHOOL OF MATHEMATICS
UNIVERSITY OF WALES COLLEGE OF CARDIFF
23, SENGHENYDD ROAD
CARDIFF, CF2 4YH, WALES, U.K.

INSTITUT ELIE CARTAN
UNIVERSITÉ DE NANCY I
B.P. 239
54506 VANDOEUVRE CEDEX, FRANCE

Reçu le 25.11.1992
et révisé le 14.10.1994 (2344)