[13] H. Iwaniec, I. van de Lune and H. te Riele, *The limits of Buchstab's iteration sieve*, Report 2W 129/79, Mathematish Centrum, Amsterdam 1979.
[14] S. Salerno, *A note on Selberg sieve*, Acta Arith. 45 (1986), 279–288.
[15] A. Selberg, *Sieve methods*, Proc. Sympos. Pure Math. 20 (1971), 311–351.

ISTITUTO DI FISICA, MATEMATICA ED INFORMATICA
UNIVERSITÀ DI SALERNO
84081 Fisciano (SA)
Italy

Received on 28.9.1989
and in revised form on 30.7.1990 (1973)

ACTA ARITHMETICA
LIX.1 (1991)

Recouvrement optimal du cercle par les multiples d'un intervalle

par

M. DELEGLISE (Villeurbanne)

Introduction. Une partie A de N est une *base asymptotique d'ordre h* si tout entier assez grand est une somme d'au plus h éléments de A et si h est le plus petit entier tel que cette propriété soit vérifiée.

Erdős et Graham [E-G] ont défini la notion d'ordre exact de la manière suivante: Une partie A de N est une *base asymptotique d'ordre exact h* si tout entier assez grand est une somme d'exactement h éléments de A, et si h est le plus petit entier vérifiant cette propriété.

Il existe des bases asymptotiques d'ordre h qui n'admettent pas d'ordre exact, par exemple l'ensemble des entiers impairs. Erdős et Graham donnent une condition nécessaire et suffisante très simple pour qu'une base asymptotique possède un ordre exact et étudient le problème de l'évaluation de l'ordre exact maximal d'une base d'ordre h. Plus précisément, ils définissent la fonction $g(h)$ qui est le maximum des ordres exacts des parties A qui sont des bases d'ordre h et qui admettent un ordre exact.

On sait actuellement que

$$h^2/3-2h \leqslant g(h) \leqslant h^2/2+3h/2 \quad \text{pour tout } h \geqslant 2. \tag{0.1}$$

La majoration est due à Nash [N] (cf. [G, Bx] pour une preuve simplifiée). La minoration est due à G. Grekos (voir [G, th] ou [G, Bx]). Celui-ci définit la fonction $L(h)$ égale à la longueur du plus petit intervalle fermé I de $T = R/Z$ tel que $I, 2I, \ldots, hI$ recouvrent T (l'intervalle kI étant défini par récurrence par l'égalité $kI = I+(k-1)I$, ou encore $kI = (k\alpha, k\beta)$ si $I = (\alpha, \beta)$), et il démontre que:

$$g(h) \geqslant 1/L(h) \quad \text{et} \quad L(h) \leqslant 3/h^2+18/h^3,$$

ce qui donne la minoration de (0.1).

Dans cet article nous démontrons les deux théorèmes suivants:

THÉORÈME A. *Soit* $I = [\alpha, \alpha+L]$ *un intervalle fermé de longueur minimum tel que* $I, 2I, \ldots, hI$ *recouvrent* T; *alors, si* $h \geqslant 3$:

$$L = \begin{cases} 3/(h(h+2)) & \text{si } h \equiv 0 \text{ ou } 1 \pmod 3, \\ 3/(h(h+2)-2) & \text{si } h \equiv 2 \pmod 3. \end{cases}$$

De plus on obtient toutes les solutions (à la symétrie près $x \to -x$) en prenant:

Si $h = 2$

$$I = [1/3, 2/3].$$

Si $h = 3$

$$\alpha = 2/5 \quad et \quad \alpha = 1/5$$

et si $h > 3$:

Si $h \equiv 0 \pmod 3$

$$\alpha = hL.$$

Si $h \equiv 1 \pmod 3$

$$\alpha = (h+1)L.$$

Si $h \equiv 2 \pmod 6$

$$\alpha = (h-1)L \quad ou \quad \alpha = (h+2)L.$$

Si $h \equiv 5 \pmod 6$

$$\alpha = (h-1)L \quad ou \quad \alpha = (h+2)L \quad ou \quad \alpha = (h^2+5h-2)L/6.$$

THÉORÈME B. *Soit* $I = [\alpha, \alpha+L]$ *un intervalle fermé de* T *de longueur maximum tel que* $I, 2I, \ldots, hI$ $(h \geqslant 3)$ *soient d'intérieurs disjoints. I est déterminé par (modulo la symétrie* $x \to -x$*):*

Si $h = 6$

$$L = 1/30 \quad et \quad \alpha = 8/30.$$

Si $h \neq 6$:

Si $h = 2k+1$

$$L = 4/(3h^2+1) \quad et \quad \alpha = (3k+1)L.$$

Si $h = 4k$

$$L = 4/(3h^2+4) \quad et \quad \alpha = (6k^2+3k)L.$$

Si $h = 4k+2$

$$L = 4/(3h^2+16) \quad et \quad \begin{array}{lll} si & k = 2k' & \alpha = (12k'^2+9k'+2)L, \\ si & k = 2k'+1 & \alpha = (12k'^2+15k'+5)L. \end{array}$$

Du théorème A il résulte que $L(h)$ est équivalent à $3/h^2$ quand h tend vers l'infini comme le conjecturait J. M. Deshouillers. Cela montre aussi que l'on ne peut pas améliorer par cette méthode le terme principal dans la minoration de $g(h)$, si ce terme était susceptible d'amélioration.

Notons que récemment Jia [J] a obtenu par un procédé différent la même minoration asymptotique de $g(h)$, $g(h) \geqslant h^2/3(1+o(h))$.

Il serait peut être intéressant de déterminer la longueur $L(n, h)$ du plus court intervalle I de $\boldsymbol{Z}/n\boldsymbol{Z}$ tel que $I, 2I, \ldots, hI$ recouvrent $\boldsymbol{Z}/n\boldsymbol{Z}$ (avec $kI = I+I+\ \ldots\ +I$). Les résultats précédents permettent de déterminer $L(n, h)$ à une unité près:

$$L(n, h) = [nL(h)] + \varepsilon(n, h)$$

avec $\varepsilon(n, h) = 0$ si $nL(n, h)$ est entier, $\varepsilon(n, h) = 1$ ou 2 si $nL(n, h)$ n'est pas entier; nous ne connaissons pas, pour le moment, de formule donnant exactement $\varepsilon(n, h)$.

Le calcul de $L(h)$ a d'abord été fait par G. Grekos ([G, Bx]) pour $h \leqslant 7$; nous avons calculé $L(h)$ sur ordinateur pour $h \leqslant 35$, en remarquant que ce nombre est une fraction de termes bornés. Les résultats nous ont permis de conjecturer le théorème A.

Notre démonstration utilise le théorème des trois distances et la notion de réduite de Farey. Dans les paragraphes 1 et 2 nous rappelons les propriétés élémentaires des suites circulaires et leurs relations avec les réduites de Farey.

Pour le théorème des trois distances, on pourra consulter [L], [Sl], [Su], [So], ou [K-N].

La théorie des réduites de Farey est très classique (cf. par exemple [H-W]); on énonce ici les résultats sous une forme adaptée à la suite de l'exposé. Pour une autre application du théorème des trois distances voir [B-N]. Je remercie G. Grekos et J. L. Nicolas pour les stimulantes conversations que nous avons eues ensemble, et l'aide qu'ils m'ont apportée pour améliorer la rédaction de cet article.

1. Rappels sur le théorème des trois distances. Dans tout cet article C est un cercle orienté de périmètre 1, identifie à $T = \boldsymbol{R}/\boldsymbol{Z}$. La notation $[a\,..\,b]$ représente l'intervalle formé des entiers i, $a \leqslant i \leqslant b$.

1.0. DÉFINITION. Une *suite circulaire* est une suite finie $M_0, M_1, \ldots, M_{h-1}$ de h points de C, tous distincts, tels que les arcs M_iM_{i+1} aient tous la même mesure α. On dira que α est *l'incrément* de la suite (M_i).

1.1. DÉFINITION. Nous dirons qu'un point M_j est le *successeur géométrique* d'un point M_i si l'arc M_iM_j ne contient pas d'autre point M_k $(0 \leqslant k \leqslant h-1)$. Cette relation sera notée $i \to j$ et on dira encore que j est le successeur de i. Dans la suite on notera $j(i)$ le successeur de i.

1.2. DÉFINITION. *Paramètres* d'une suite circulaire. Ce sont les deux indices s et q caractérisés par $s \to 0 \to q$.

Remarque. On considèrera aussi des suites circulaires indicées par un intervalle de la forme $[r+1\,..\,r+t]$; les paramètres s et q seront alors évidemment définis par

$$r+1+s \ \to\ r+1 \ \to\ r+1+q.$$

1.3. PROPOSITION. *Les deux paramètres* s *et* q *d'une suite circulaire de cardinal* h *vérifient* $s+q \geqslant h$.

Démonstration. Si on avait $s+q < h$ le point M_{s+q} figurerait parmi les M_i. Mais M_0 étant situé entre M_s et M_q, M_{s+q} est entre M_s et M_q car on passe de M_s à M_{s+q} par la même rotation que de M_0 à M_q.

1.4. PROPOSITION. *Soit M_i une suite circulaire, $0 \leqslant i \leqslant h-1$. Si M_i et M_j sont deux points géométriquement consécutifs et si i et j sont tous les deux strictement inférieurs à $h-1$ alors M_{i+1} et M_{j+1} sont géométriquement consécutifs sauf si $i+1=s$, et dans ce cas le seul point appartenant à l'intervalle M_{i+1}, M_{j+1} est M_0. Autrement dit, si i est distinct de $s-1$, et $j(i)$ distinct de $h-1$, $j(i+1)=j(i)+1$.*

Démonstration. La relation "C est entre A et B" étant préservée par rotation, s'il existe un point M_k qui sépare M_{i+1} et M_{j+1} avec $k>0$, alors M_{k-1} sépare M_i et M_j. Le seul point susceptible de séparer M_{i+1} et M_{j+1} est donc M_0, et dans ce cas, par définition de s, $i+1=s$.

1.5. LE THÉORÈME DES TROIS DISTANCES. *Soit une suite circulaire de cardinal h et de paramètres s et q. L'application successeur j: $[0..h-1] \to [0..h-1]$ est caractérisée par:*

$$\begin{aligned} \text{si } i+q \leqslant h-1 \quad & \text{alors} \quad j(i)=i+q, \\ \text{si } i \geqslant s \quad & \text{alors} \quad j(i)=i-s, \\ \text{si } h-q \leqslant i < s \quad & \text{alors} \quad j(i)=i+q-s. \end{aligned}$$

Démonstration. Découpons l'intervalle $[0..h-1]$ en trois sous-intervalles:

$$[0..h-1-q], \quad [h-q..s-1], \quad [s..h-1].$$

Ceci est possible d'après 1.3, l'intervalle du milieu étant vide lorsque $s=h-q$. Sur chacun de ces intervalles on raisonne par récurrence en utilisant 1.4.

1) *Premier cas*: $i \leqslant h-1-q$. Il suffit de montrer que $j(0)=q$, ce qui est la définition de q.

2) *Deuxième cas*: $s \leqslant i \leqslant h-1$. Il suffit de montrer que $j(s)=0$ et c'est la définition de s.

3) *Troisième cas*: $h-q \leqslant i < s$. Ici il suffit de vérifier que $j(h-q)=h+q-s$.

Par les deux cas précédents le successeur de $h-q-1$ est $h-1$ et le successeur de $h-1$ est $h-1-s$. On a donc

$$h-q-1 \to h-1 \to h-1-s. \tag{1.5.1}$$

Il faut montrer que M_{h-q} et M_{h-s} sont consécutifs; si un point $M_k, k>0$, les séparait, le point M_{k-1} séparerait M_{h-q-1} et M_{h-s-1} et, par (1.5.1), on aurait $k-1=h-1$, d'où $k=h$, ce qui est impossible. Le seul point qui pourrait séparer M_{h-q} et M_{h-s} est donc M_0, mais cela aussi est impossible car cela entraînerait $h-q=s$.

1.6. DÉFINITION. Si une suite circulaire de cardinal h, d'incrément α, de paramètres s et q vérifie $h=s+q$ on dira que c'est une *suite à deux distances.* En effet, dans ce cas l'intervalle $[h-q, s[$ est vide et le successeur de i est soit $i+q$ soit $i-s$. Ainsi la distance entre deux points géométriquement consécutifs de la suite est égale soit à la longueur de l'arc M_sM_0, soit à la longueur de l'arc M_0M_q.

1.7. PROPOSITION. *Si s et q sont les paramètres d'une suite circulaire alors s et q sont premiers entre eux.*

Démonstration. Supposons que s et q soient tous les deux divisibles par un entier $d>1$. Considérons la suite définie par $n_0=0$ et $n_{i+1}=j(n_i)$. Par le théorème des trois distances les différences $n_{i+1}-n_i$ seraient toutes divisibles par d, donc tous les n_i aussi. Cela est absurde car les valeurs des n_i sont tous les entiers $0, 1, 2, \ldots, h-1$.

1.8. PROPOSITION. *Soit une suite circulaire M_i, $0 \leqslant i \leqslant h-1$, de paramètres s et q. Si on prolonge cette suite en lui rajoutant un à un les points M_i pour $i=h, h+1, \ldots$, le premier point M_i qui tombera dans l'arc M_sM_q est le point M_{s+q}.*

Démonstration. On a déjà remarqué en 1.3 que le point M_{s+q} est situé entre M_s et M_q. Soit M_n le premier point entre M_s et M_q. Supposons que M_n tombe dans le segment M_sM_0. La suite circulaire de premier terme M_0 et de dernier terme M_n a donc pour paramètres n et q, et $s \to n \to 0 \to q$. n est donc le successeur de s et par le théorème des trois distances, $n-s$ est égal à l'un des trois nombres $q, -n, q-n$. Les deux dernières valeurs sont exclues car elles nécessitent $n=2s$ ou $2n=s+q$, ce qui est contradictoire avec $n>\max(s,q)$. On a donc $n-s=q$, soit $n=s+q$.

Une démonstration similaire marche lorsque M_n tombe dans M_0M_q.

2. Suites circulaires et réduites de Farey. Rappelons le lemme classique

2.0. LEMME. *Si a/b et c/d sont deux fractions telles que $bc-ad=1$, toute fraction appartenant à l'intervalle $[a/b, c/d]$ a un dénominateur au moins égal à $b+d$. L'unique fraction de dénominateur $b+d$ de cet intervalle est $(a+c)/(b+d)$.*

2.1. DÉFINITION. On dit qu'une fraction irréductible a/b est une *réduite de Farey* du nombre α s'il n'existe pas de fraction de dénominateur inférieur ou égal à b entre a/b et α. Si a/b est supérieur à α on dira que c'est une *réduite supérieure* de α, sinon que c'est une *réduite inférieure* de α.

Du lemme 2.0 il résulte immédiatement:

2.2. PROPOSITION ET DÉFINITION. *Soient deux fractions a/b et c/d telles que $bc-ad=1$. Alors a/b et c/d sont deux réduites de Farey de tout nombre α appartenant à l'intervalle $[a/b, c/d]$. On dira que a/b et c/d sont deux réduites de Farey **associées** de α.*

2.3. DÉFINITION. *Suite des encadrements de Farey* d'un réel α.

Soit un réel α. On définit par récurrence la suite des encadrements de Farey de α de la manière suivante:

Le premier encadrement est l'intervalle limité par les deux fractions $m/1$ et $(m+1)/1$ où m est la partie entière de α.

Soit I_n le n-ième encadrement de Farey de α: $I_n = [a_n/b_n, c_n/d_n]$; $(a_n+c_n)/(b_n+d_n)$ appartient à I_n et partage I_n en deux intervalles; I_{n+1} est celui de ces deux intervalles qui contient α.

2.4. PROPOSITION. *Tout intervalle défini par un couple de réduites de Farey associées de α figure dans la suite des encadrements de Farey de α.*

La démonstration résulte simplement des définitions et du lemme 2.0.

2.5. PROPOSITION. *Soit une suite circulaire de cardinal $h \geqslant 2$, d'incrément α, et de paramètres s et q; s est le plus grand dénominateur $\leqslant h-1$ d'une réduite de Farey supérieure de α; q est le plus grand dénominateur $\leqslant h-1$ d'une réduite de Farey inférieure de α.*

Démonstration. Montrons d'abord que q est le dénominateur d'une réduite de Farey inférieure de α et s le dénominateur d'une réduite de Farey supérieure de α.

Soit b la partie entière de $q\alpha$. Alors la mesure sur C de l'arc M_0M_q est égale à $q\alpha-b$. D'où $b/q < \alpha$; supposons qu'il existe une fraction m/n dans l'intervalle $]b/q, \alpha[$, de dénominateur $n \leqslant q$: $b/q < m/n < \alpha$. Il en résulterait

$$0 < n\alpha-m < n(\alpha-b/q) = (n/q)(q\alpha-b) < q\alpha-b$$

et ceci contredirait la définition de q car le point M_n serait dans l'intervalle M_0M_q (car $n\alpha-m$ est la mesure de l'arc M_0M_n).

De même en considérant le plus petit entier a qui dépasse $s\alpha$ on voit que la mesure de l'arc M_sM_0 est $a-s\alpha$ et qu'il n'existe pas de fraction de dénominateur $\leqslant s$ dans l'intervalle $]\alpha, a/s[$.

Il reste à montrer que les deux réduites b/q et a/s sont associées. Il suffit pour cela de montrer que les valeurs successives du couple $(b/q, a/s)$ sont les bornes des encadrements de Farey successifs de α. Cela se fait par une récurrence immédiate sur h:

Si $h = 2$ on a $s = q = 1$ et si m est la partie entière de α les deux premières réduites de Farey de α sont $m/1$ et $(m+1)/1$, toutes les deux de dénominateur 1. Et cela reste vrai pour tout h par la proposition 1.8 et la définition 2.3.

2.6. COROLLAIRE. *Si t est le dénominateur d'une réduite de Farey d'un nombre α, toute suite circulaire d'incrément α et de cardinal t est une suite à deux distances.*

Démonstration. Soient s et q les paramètres de la suite considérée. s et q sont les plus grands dénominateurs inférieurs à t d'une réduite de Farey de α. t est donc le premier dénominateur d'une réduite de α qui dépasse s et q. D'où $t = s+q$.

3. Recouvrement du cercle par les multiples d'un intervalle. Minoration du recouvrement. Dans ce paragraphe I est un intervalle du cercle C défini par son origine α et sa longueur L, $I = [\alpha, \beta]$ (avec $\beta = \alpha+L$); h est un entier positif et on suppose que les intervalles $I, 2I, 3I, \ldots, hI$ recouvrent le cercle C. L'objet de ce paragraphe est de déterminer une minoration de L (pour h fixé). On supposera $L \leqslant 1/h$, ce qui n'est pas restrictif.

3.0. PROPOSITION. *Si deux multiples pI et qI ont une intersection non vide de longueur d, alors $(p+1)I$ et $(q+1)I$ ont une intersection de longueur $\min(d+L, 1)$. Si pI est inclus dans qI, alors $(p-1)I$ est inclus dans $(q-1)I$ (avec $0I = \{0\}$).*

Démonstration. Il suffit de remarquer que les $k\alpha$ forment une suite circulaire d'incrément α et les $k\beta$ forment une suite circulaire d'incrément $\alpha+L$. Ainsi, en passant d'un intervalle kI au suivant, $(k+1)I$, l'extrémité avance de $\alpha+L$, tandis que l'origine n'avance que de α. Si l'extrémité de pI a une avance de d sur l'origine de qI, l'extrémité de $(p+1)I$ a une avance de $(d+L)$ sur l'origine de $(q+1)I$.

3.1. DÉFINITIONS. Soient J_1 et J_2 deux intervalles du cercle orienté C. On dit que J_2 *prolonge* J_1 si l'extrémité de J_1 appartient à l'intervalle J_2. Soient I, J, K trois intervalles de C. On dit que J est *situé exactement entre I et K* si l'extrémité de I coïncide avec l'origine de J, et si l'extrémité de J coïncide avec l'origine de K.

3.2. PROPOSITION. *Soit t le plus petit entier tel que $0 \in tI$, et soit $r = h-t$. Alors*

1) $I \subset (t+1)I$, $2I \subset (t+2)I, \ldots, rI \subset hI$.

2) *Aucun intervalle mI avec $m > r$ n'est contenu dans un autre. Autrement dit, les r premiers intervalles sont inutiles car contenus dans un autre intervalle et ce sont les seuls intervalles inutiles pour le recouvrement.*

3) *t est le dénominateur d'une réduite de Farey de α, et la suite formée des origines des intervalles utiles $(r+1)I, \ldots, hI$ est une suite circulaire à deux distances.*

Démonstration. 1) résulte de la proposition 3.0.

2) S'il existait des entiers m et k avec $m > r$ et $mI \subset kI$ on en déduirait les inclusions: $(m-1)I \subset (k-1)I, \ldots, 0 \in (k-m)I$ contredisant la définition de t car $k-m$ est strictement inférieur à $h-r = t$.

3) Enfin, dire que $0 \in tI$ c'est dire qu'il existe un entier n vérifiant

$$t\alpha \leqslant n \leqslant t(\alpha+L) \quad \text{ou encore} \quad \alpha \leqslant n/t \leqslant \alpha+L.$$

t est donc le plus petit dénominateur d'une fraction de l'intervalle $[\alpha, \alpha+L]$. C'est donc le dénominateur d'une réduite de Farey de α.

3.3. PROPOSITION. *Soit r défini comme ci-dessus et soient s et q les paramètres de la suite circulaire formée des origines des intervalles utiles*

kI ($r < k \leqslant h$). La longueur L de l'intervalle I est minorée par

$$2/(h^2+h-(r^2+r+s^2-s+q^2-q)).$$

Si $(r+1)I$ n'est pas situé exactement entre $(r+s+1)I$ et $(r+q+1)I$ la minoration est stricte.

Démonstration. De la proposition 3.2 il résulte que si l'origine de l'un des intervalles utiles a pour successeur géométrique l'origine d'un autre, ces deux intervalles ont une intersection non vide: en effet, soit $a\alpha$ et $b\alpha$ deux origines géométriquement consécutives. Si l'intersection de aI et bI était vide, il existerait un intervalle cI qui rencontre $]a\beta, b\alpha[$. $a\alpha$ et $b\alpha$ étant consécutifs, l'origine $c\alpha$ de cI précèderait $a\alpha$, et aI serait inclus dans cI, donc inutile.

Par le théorème des trois distances le successeur de $(r+i)\alpha$ est $(r+i+q)\alpha$ pour $1 \leqslant i \leqslant s$, donc l'intersection de $(r+1)I$ avec $(r+1+q)I$ n'est pas vide, et par la proposition 3.0 on a:

(3.3.1)
$$\begin{aligned}
&(r+2)I \quad \text{recouvre } (r+q+2)I \quad \text{d'une longueur } \geqslant L,\\
&(r+3)I \quad \text{recouvre } (r+q+3)I \quad \text{d'une longueur } \geqslant 2L,\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&(r+s)I \quad \text{recouvre } hI \quad \text{d'une longueur } \geqslant (s-1)L
\end{aligned}$$

(en remarquant que $L \leqslant 1/h$), de même l'intersection de $(r+1+s)I$ avec $(r+1)I$ n'est pas vide, donc:

(3.3.2)
$$\begin{aligned}
&(r+s+2)I \quad \text{recouvre } (r+2)I \quad \text{d'une longueur } \geqslant L,\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&hI \quad \text{recouvre } (r+q)I \quad \text{d'une longueur } \geqslant (q-1)L.
\end{aligned}$$

La place perdue, c'est-à-dire la longueur des intersections deux à deux des kI, est au moins égale à la somme des longueurs des intervalles inutiles augmentée de la somme des longueurs des recouvrements que l'on vient de calculer, soit:

$$L(1+2+\dots+r+1+2+\dots+(s-1)+1+2+\dots+(q-1))$$

soit

$$L(r^2+r+s^2-s+q^2-q)/2.$$

Si on écrit maintenant que la somme des longueurs des intervalles, $Lh(h+1)/2$, est égale à 1 augmenté de la place perdue on obtient l'inégalité

$$Lh(h+1)/2 \geqslant 1+L(r^2+r+s^2-s+q^2-q)/2$$

et la minoration annoncée.

Si $(r+1)I$ n'est pas situé exactement entre $(r+s+1)I$ et $(r+q+1)I$, son intersection avec l'un de ces deux intervalles est de longueur strictement positive et les inégalités dans (3.3.1) ou (3.3.2) sont strictes.

3.4. Corollaire. *Si I est un intervalle tel que $I, 2I, \dots, hI$ recouvrent le cercle C, et si L est la longueur de I, alors L est supérieur à $3/(h+1)^2$.*

Démonstration. Posons

$$g(r, s, q) = r^2+r+s^2-s+q^2-q;$$

alors

$$L \geqslant 2/(h^2+h-\min\{g(r, s, q);\ r, s, q \in \mathbf{R}^+,\ r+s+q = h\}).$$

Le minimum de g est facile à calculer; il est atteint sur le triplet vérifiant $r+s+q = h$ et $2r+1 = 2s-1 = 2q-1$, soit $r = (h-2)/3$, $s = q = (h+1)/3$, et il est égal à $(h-2)(h+1)/3$. Cela donne pour L le minorant $3/(h+1)^2$.

4. Détermination des solutions optimales. Dans ce paragraphe nous allons démontrer que, réciproquement, à tout triplet (r, s, q), $r \geqslant 0$, $s, q > 0$, $r+s+q = h$, $(s, q) = 1$, on peut associer un intervalle I tel que $I, 2I, \dots, hI$ recouvrent C et de longueur égale à $2/(h^2+h-(r^2+r+s^2-s+q^2-q))$, et en déduire toutes les solutions optimales.

Pour vérifier qu'un intervalle I est solution du problème du recouvrement on utilisera le lemme suivant:

4.1. Lemme. *Soit I un intervalle du cercle orienté et $h, q, s > 0$, $r \geqslant 0$, des entiers vérifiant les trois conditions:*

1) $h = r+q+s$,
2) $(r+1+q)I$ *prolonge* $(r+1)I$,
3) $(r+1)I$ *prolonge* $(r+s+1)I$.

Alors les intervalles $(r+1)I, (r+2)I, \dots, hI$ recouvrent le cercle C.

Démonstration. Considérons l'application j de $[r+1, h]$ dans lui-même définie par

$$j(i) = \begin{cases} i+q & \text{si } i \leqslant h-q = r+s,\\ i-s & \text{si } i \geqslant r+s+1. \end{cases}$$

Les conditions 2 et 3 et la proposition 3.0 entraînent que

$$\begin{aligned}
&(i+q)I \quad \text{prolonge } iI \text{ pour } i \geqslant r+1,\\
&(i-s)I \quad \text{prolonge } iI \text{ pour } i \geqslant r+s+1.
\end{aligned}$$

On en déduit que $j(i)I$ prolonge iI pour tout i de $[r+1, h]$. Soit la suite i_k définie par $i_1 = r+1$ et $i_k = j(i_{k-1})$. Par le principe des tiroirs de Dirichlet, il existe des entiers u et v tels que

$$1 \leqslant u < v \leqslant h-r+1 \quad \text{et} \quad i_v = i_u.$$

Alors les intervalles $i_{u+1}I, i_{u+2}I, \dots, i_vI$ recouvrent C, car chacun prolonge le précédent et le premier prolonge le dernier.

4.2. LEMME. *Soient a, b, c trois entiers tels que $b-a$ et $b-c$ soient premiers entre eux, et un intervalle $I=[\alpha, \alpha+L]$ tel que bI soit situé exactement entre aI et cI. Alors il existe u et v dans $\boldsymbol{Z}$ tels que:*

$$\alpha=\frac{ua+vb}{ac-b^2} \quad et \quad L=\frac{u(b-a)-v(b-c)}{ac-b^2}. \tag{4.2.1}$$

La plus petite valeur de L est $|1/(ac-b^2)|$. Pour une valeur donnée de L il n'existe qu'une valeur de α modulo 1.

Démonstration. Le système traduisant les coïncidences de l'extrémité de aI avec l'origine de bI, et de l'extrémité de bI avec l'origine de cI s'écrit:

$$a\alpha+aL=b\alpha+v,$$
$$b\alpha+bL=c\alpha-u,$$

avec v et u dans $\boldsymbol{Z}$, soit encore

$$(b-a)\alpha-aL=-v,$$
$$(b-c)\alpha+bL=-u.$$

La résolution de ce système donne les formules annoncées. $b-a$ et $b-c$ étant premiers entre eux, il existe v et u tel que $u(b-a)-v(b-c)=1$.

Si (v', u') et (v, u) donnent la même valeur de L il existe λ dans $\boldsymbol{Z}$ tel que

$$v'=v+\lambda(b-a) \quad et \quad u'=u+\lambda(b-c)$$

et cela donne

$$(u'a+v'b)-(ua+vb)=\lambda(ab-ac+b^2-ab)=\lambda(b^2-ac) \quad \text{d'ou } \alpha'-\alpha=-\lambda.$$

4.3. PROPOSITION. 1) *Pour tout triplet (r, s, q) vérifiant $r\geqslant 0$, $s, q>0$, $r+s+q=h$, $(s, q)=1$, il existe un unique intervalle I de longueur $L=2/(h^2+h-(r^2+r+s^2-s+q^2-q))=1/[(r+1)(s+q)+sq]$ tel que $(r+1)I$ soit situé exactement entre $(r+s+1)I$ et $(r+q+1)I$.*

2) *Si u et v, dans $\boldsymbol{Z}$, sont tels que $vq-us=1$, l'origine α de I est donnée par*

$$\alpha=[v(r+1)+u(r+s+1)]L.$$

3) *$I, 2I, \ldots, hI$ recouvrent C.*

4) *Tout intervalle I de longueur minimale tel que $I, 2I, \ldots, hI$ recouvre T est obtenu de cette manière, en prenant un triplet (r, s, q) qui minimise $2/(h^2+h-(r^2+r+s^2-s+q^2-q))$.*

Démonstration. 1) Par le lemme 4.2, avec $b=r+1$, $a=r+s+1$, $c=r+q+1$, il existe un unique intervalle I de T tel que $(r+1)I$ soit situé exactement entre $(r+s+1)I$ et $(r+q+1)I$ et dont la longueur est

$$1/(ac-b^2)=1/[(r+1)(s+q)+sq]=2/(h^2+h-(r^2+r+s^2-s+q^2-q)).$$

2) Résulte des formules (4.2.1) en prenant u et v tels que

$$u(b-a)-v(b-c)=1.$$

3) Comme $(r+1)I$ prolonge $(r+s+1)I$ et $(r+q+1)I$ prolonge $(r+1)I$, le lemme 4.1 montre que $(r+1)I, (r+2)I, \ldots, hI$ recouvrent T.

4) Il reste à montrer que toute solution optimale est obtenue par ce procédé: Soit I, de longueur minimale, tel que $I, 2I, \ldots, hI$ recouvrent T et soient (r, s, q) définis dans la proposition 3.3. Alors la longueur de I est minorée par $2/(h^2+h-(r^2+r+s^2-s+q^2-q))$ et cette minoration doit être une égalité, car la première partie de cette démonstration montre qu'il existe des solutions pour lesquelles il y a égalité; cela montre que $(r+1)I$ est situé exactement entre $(r+s+1)I$ et $(r+q+1)I$.

Démonstration du théorème A. Le problème est donc ramené à celui de la détermination du minimum de

$$g(r, s, q)=r^2+r+s^2-s+q^2-q$$

sur les triplets (r, s, q) vérifiant $r+s+q=h$, $r\geqslant 0$, $s, q>0$, $(s, q)=1$.

Cette fonction est symétrique en s et q. On ne distinguera pas deux triplets qui diffèrent par l'échange de s et q car cet échange revient à remplacer I par $-I$, c'est-à-dire remplacer une solution par une autre qui s'en déduit par symétrie autour de l'axe polaire.

On ne donnera donc que les solutions pour lesquelles $s\leqslant q$.

Premier cas: $h=3m$. Sous la seule contrainte $h=r+s+q$ et r, s, q réels on a vu en 3.3 que le minimum est atteint pour $r=(h-2)/3=m-2/3$ et $s=q=(h+1)/3$.

D'autre part pour r fixé, $g(r, s, q)$ est supérieur ou égal à $f(r)=g(r,(h-r)/2,(h-r)/2)$. Un calcul simple montre que $f(r)$ est minimum en $r=(h-2)/3$, décroissante pour r variant de 0 à $(h-2)/3$ et croissante pour r variant de $(h-2)/3$ à h.

Pour $r=m-1$ la plus petite valeur de $g(r, s, q)$ est atteinte avec $s=m$ et $q=m+1$ et cette valeur $g(m-1, m, m+1)$ est $3m^2-m$.

Pour $r=m-2$, $f(r)=3m^2-m+2$, et pour $r=m+1$, $f(r)=3m^2-m+7/2$. Le minimum est donc atteint pour $m-1\leqslant r\leqslant m$.

Pour $r=m$: Si $m=1$ on obtient encore la valeur $(3m^2-m)=2$ avec le triplet $(1, 1, 1)$. Si $m>1$, s et q doivent être différents et dans ce cas on ne peut pas obtenir moins que $g(m, m-1, m+1)=3m^2-m+2$. Donc si $h=3m$ le minimum est atteint en $(m-1, m, m+1)$.

Par les formules (4.3.2) cela donne

$$L=3/[(r+1)(s+q)+sq]=3/h(h+2) \quad et \quad \alpha=hL.$$

Si $m=1$, c'est-à-dire $h=3$, $L=1/5$ et on a une solution supplémentaire donnée par le triplet $(1, 1, 1)$ qui donne $\alpha=2/5$.

Deuxième cas: $h=3m+1$. On montre de la même façon que ci-dessus que le minimum de $g(r, s, q)$ est atteint sur l'unique triplet $(m, m+1, m+1)$ et les

formules 4.3 donent alors:

$$L = 3/(h(h+2)) \quad \text{et} \quad \alpha = (h+1)L.$$

Troisième cas: $h = 3m+2$. Cette fois, si $m \geqslant 1$, on voit que le minimum de $g(r, s, q)$ est atteint sur deux ou trois triplets selon la parité de h; ce sont:

$$r = m-1, \quad s = m+1, \quad q = m+2,$$

$$r = m+1, \quad s = m, \quad q = m+1,$$

dans tous les cas, et, en outre, si h est impair, c'est-à-dire congru à 5 modulo 6, le triplet

$$r = m, \quad s = m, \quad q = m+2.$$

Ces trois triplets réalisent le minimum de $g = 3m^2+3m+2$, qui donne

$$L(h) = 3/[h(h+2)-2].$$

La première solution donne $\alpha = (h-1)L$, la deuxième donne $\alpha = (h+2)L$ et la troisième donne $\alpha = L(h^2+5h-2)/6$.

Pour $m = 0$, c'est-à-dire $h = 2$, le minimum est atteint sur l'unique triplet $r = 0$, $s = 1$, $q = 1$, ce qui donne $L = 1/3$ et $\alpha = 1/3$.

5. Intervalle fermé de longueur maximale tel que les h premiers multiples de I soient disjoints. Dans ce paragraphe I est un intervalle fermé de longueur l maximale tel que $I, 2I, \ldots, hI$ soient d'intérieurs disjoints. Soit $I = [\alpha, \alpha+l]$. Remarquons que α n'est pas nul.

5.1. Lemme. *L'intervalle hI est exactement contenu entre deux intervalles pI et rI avec $1 \leqslant p \leqslant h-1$ et $1 \leqslant r \leqslant h-1$.*

Démonstration. Si les extrémités des intervalles $I, 2I, \ldots, hI$ étaient toutes disjointes on pourrait par continuité augmenter la longueur de I.

Les diverses coïncidences d'une extrémité d'un qI avec une extrémité d'un rI se traduisent par un système d'équations de la forme

$$p\alpha+pl = q\alpha+n, \quad n \text{ dans } \mathbf{Z}.$$

Si ce système était de rang 1 il équivaudrait à une unique équation

$$(p-q)\alpha+pl = n \tag{5.1.0}$$

et, par continuité, on pourrait encore augmenter la longueur l, en modifiant α de sorte que (5.1.0) reste vraie sans changer les positions respectives des divers intervalles.

Ce système est donc de rang 2 et il existe au moins deux coïncidences. Par la proposition 3.0 il ne peut pas exister de coïncidence entre les extremités de deux intervalles aI et bI avec a et b strictement inférieurs à h.

Il en résulte que les deux coïncidences ne peuvent être que la coïncidence d'une extremité de hI avec l'extremité d'un autre intervalle. hI rencontre donc deux autres intervalles pI et rI, et il est nécessairement situé exactement entre ceux-ci.

5.2. Proposition. *Soient p et r les deux entiers tels que l'intervalle hI soit exactement compris entre pI et rI. Alors l, p et r vérifient:*

1) $p+r \leqslant h$,
2) *$h-p$ et $h-r$ sont premiers entre eux,*
3) $l = 1/(h^2-pr)$.

Démonstration. Considérons la suite circulaire des origines des kI, c'est-à-dire la suite $\alpha, 2\alpha, \ldots, h\alpha$. Soit s et q ses paramètres; h est le successeur de p et par le théorème des trois distances, $h = p+q$; de même r est le successeur de h et $r = h-s$. Par la proposition 1.3, $s+q$ est supérieur ou égal à h; cella s'écrit $(h-r)+(h-p) \geqslant h$ et équivaut à 1).

s et q sont premiers entre eux et cela donne 2).

Le système qui traduit les coïncidences a été résolu au paragraphe 4.2 et ses solutions sont:

$$\alpha = \frac{up+vh}{h^2-pr} \quad \text{et} \quad l = \frac{u(h-p)-v(h-r)}{h^2-pr} = \frac{B}{\Delta}. \tag{5.2.0}$$

D'autre part, en remarquant que la somme des longueurs de tous les kI est inférieure à 1 on a la majoration $lh(h+1)/2 \leqslant 1$, qui donne

$$Bh(h+1) \leqslant 2\Delta < 2h^2.$$

Cela entraîne $B = 1$ et $l = 1/(h^2-pr)$.

On en déduit immédiatement la proposition 5.3, analogue de 3.3.

5.3. Proposition. *Si l est la longueur maximale d'un intervalle I tel que $I, 2I, \ldots, hI$ soient disjoints, alors l est inférieur à $4/(3h^2)$.*

Démonstration. De $h \geqslant p+q$ il résulte $pq \leqslant h^2/4$, d'où $h^2-pq \geqslant 3h^2/4$.

La proposition suivante nous servira à construire des intervalles I tels que $I, 2I, \ldots, hI$ soient d'intérieurs disjoints.

5.4. Proposition. *Si p et r sont tels que $h \geqslant p+r$ et $(h-p)$ et $(h-r)$ premiers entre eux, il existe un intervalle I de $\mathbf{R}/\mathbf{Z}$ de longueur $l = 1/(h^2-pr)$ tel que $I, 2I, 3I, \ldots, hI$ soient d'intérieurs deux à deux disjoints.*

Démonstration. En effet, considérons les intervalles I qui sont tels que hI est compris exactement entre pI et rI. Ce sont les intervalles $I = [\alpha, \alpha+l]$ avec α et l donnés par (5.2.0) pour un u et un v arbitraires de $\mathbf{Z}$. $(h-p)$ et $(h-r)$ étant premiers entre eux, on peut choisir u et v tels que $u(h-p)-v(h-r) = 1$.

Montrons que si u et v sont choisis ainsi alors les intervalles $I, 2I, \ldots, hI$ sont d'intérieurs deux à deux disjoints. Par la proposition 3.0 il suffit pour cela de montrer que l'intervalle hI a une intersection d'intérieur vide avec tout autre kI. Comme les kI sont de longueurs strictement inférieures à celle de hI, il suffit de montrer que l'intérieur de hI ne contient pas de borne d'un kI $(1 \leqslant k \leqslant h-1)$.

Par le choix de u et v le couple de fractions $v/(h-p)$ et $u/(h-r)$ est un couple de réduites de Farey associées.

Montrons que α et $\beta = \alpha + l$ appartiennent à l'intervalle défini par ces deux fractions, c'est-à-dire que

$$\frac{v}{h-p} \leqslant \alpha = \frac{up+vh}{h^2-pr} \leqslant \frac{u}{h-r}, \qquad \frac{v}{h-p} \leqslant \beta = \frac{up+vh+1}{h^2-pr} \leqslant \frac{u}{h-r}.$$

Il faut vérifier quatre inégalités. En faisant les produits en croix, en réarrangeant les termes, et en utilisant la relation $u(h-p)-v(h-r)=1$, ces quatre égalités s'écrivent respectivement $p \geqslant 0$, $h \geqslant 0$; $h \geqslant 0$, $r \geqslant 0$.

Considérons alors la suite circulaire α, $2\alpha, \ldots, (h-1)\alpha$. Comme $(h-p)+(h-r)$ est supérieur au cardinal $(h-1)$ de cette suite, la proposition 2.5 montre que les paramètres de cette suite sont $s = h-r$ et $q = h-p$.

Par le théorème des trois distances le successeur géométrique de $p\alpha$ est l'un des trois nombres $(p+(h-p))\alpha = h\alpha$, $(p-(h-r))\alpha$, $(p+r-p)\alpha = r\alpha$. Le seul de ces nombres qui appartient à la suite considérée est le dernier $r\alpha$. Il en résulte qu'il n'existe pas de $k\alpha$ $(1 \leqslant k \leqslant h-1)$ entre $p\alpha$ et $r\alpha$, ni, *a fortiori*, dans hI.

Par le même raisonnement appliqué à la suite $\beta, 2\beta, \ldots, (h-1)\beta$ il n'existe pas de $k\beta$ entre $p\beta$ et $r\beta$ et donc pas non plus dans hI, et cela achève la démonstration.

Démonstration du théorème B. Par les propositions 5.2 et 5.4, $l = \operatorname{Max}\{1/(h^2-pr);\ p+r \leqslant h,\ ((h-p),(h-r)) = 1\}$. Pour chaque reste de h modulo 4 nous allons choisir p et r tels que pr soit maximum, avec $p+r \leqslant h$, $(h-p, h-r) = 1$; puis on cherchera u et v tels que $u(h-p)-v(h-r)=1$ et on en déduira α et L donnés par

$$L = 1/(h^2-pr) \quad \text{et} \quad \alpha = (up+vh)L.$$

Les autres choix possibles de u et v donnent la même valeur de α modulo 1 (lemme 4.2).

a) Si $h = 4k$, le produit pr est maximum pour $p = 2k-1$ et $r = 2k+1$. Il vaut alors $4k^2-1$ et on a alors $h^2-pr = 12k^2+1 = 3h^2/4+1$. On a ici $u = k$ et $v = (k+1)$, d'où $\alpha = (6k^2+3k)L$.

b) Si $h = 2k+1$, la plus grande valeur de pr est obtenue pour $p = k$ et $r = k+1$, ce qui donne $pr = k^2+k$ et $h^2-pr = 3k^2+3k+1 = (3h^2+1)/4$. Ici on a $u = v = 1$, d'où $\alpha = (h+k)L$.

c) Si $h = 4k+2$, p et r sont distincts et $h-p$, $h-r$ premiers entre eux. Il faut donc exclure les couples $(2k+1, 2k+1)$ et $(2k, 2k+2)$. Le maximum est obtenu avec le couple $(2k, 2k+1)$ ou bien le couple $(2k+3, 2k-1)$. Le premier couple donne $pr = 4k^2+2k$ et le deuxième donne $pr = 4k^2+4k-3$. La deuxième valeur est plus grande dès que $2k-3$ est positif, c'est-à-dire $k > 1$.

Pour $k = 1$, c'est-à-dire $h = 6$, on obtient $l = 1/30$ et $\alpha = 8/30$.

Pour $k > 1$ on obtient $h^2-pr = 12k^2+12k+7 = 3h^2/4+4$. Il faut trouver u et v tels que $u(h-p)-v(h-r) = 1$. On distingue deux cas selon la parité de k:

Si $k = 2k'$ on trouve $u = -k'-1$ et $v = -k'$; cela donne $\alpha = -(12k'^2+9k'+3)L$. Remplaçant l'intervalle $[a, a+L]$ par $[-a-L, a]$ on obtient la valeur $\alpha = (12k'^2+9k'+2)L$.

Si $k = 2k'+1$ on trouve $u = k'+1$ et $v = k'$, ce qui donne $\alpha = (12k'^2+15k'+5)L$.

Remarque. On peut noter que dans les deux théorèmes A et B, la "place perdue", c'est-à-dire la longueur totale des recouvrements dans le premier cas, et la longueur de la portion de T qui n'est pas recouverte dans le deuxième cas, est asymptotiquement égale à la moitié de la longueur de la réunion des kI.

References

[B-N] G. Bessi et J. L. Nicolas, *Nombres 2-hautement composés*, J. Math. Pures Appl. 56 (1977), 307–326.

[C] M. Chardin, *Lien entre deux résultats sur la répartition modulo 1 de la suite des multiples d'un nombre réel*, C. R. Acad. Sci. Paris Série I, 308 (1989), 519–520.

[E-G] P. Erdős and R. L. Graham, *On bases with an exact order*, Acta Arith. 37 (1980), 201–207.

[G, th] G. Grekos, *Quelques aspects de la théorie additive des nombres*, Thèse, Université de Bordeaux 1, 1982.

[G, Bx] –, *Sur l'ordre d'une base additive*, Séminaire de Théorie des Nombres de Bordeaux, 1987–1988, exposé n° 31, 13 p.

[H-W] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press, 1960.

[J] X. D. Jia, *Exact order of subsets of asymptotic bases in additive number theory*, J. Number Theory 28 (1988), 205–218.

[K-N] L. Kuipers and V. Niederreiter, *Uniform Distribution of Sequences*, Interscience Tracts, Wiley, New York 1974.

[L] M. Langevin, *Stimulateur cardiaque et suites de Farey*, Prepublication.

[N] J. C. Nash, *Results on bases in additive number theory*, Thèse, Rutgers University, New Jersey 1985.

[Sl] N. B. Slater, *Gaps and steps for the sequence nθ* mod 1, Proc. Cambridge Philos. Soc. 63 (1967), 1115–1223.

[St] V. T. Sós, *On the distribution* mod 1 *of the sequence nα*, Ann. Univ. Sci. Budapest. Sect. Math. 1 (1958), 127–134.

[Su] J. Surányi, *Über die Anordnung der Vielfachen einer reellen Zahl* mod 1, ibid. 107–111.

DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ LYON 1
43 Bd. du 11 novembre 1918
69622 Villeurbanne cedex, France

Reçu le 6.10.1989
et révisé le 20.7.1990

(1975)