

Sur les propriétés additives des nombres

L. G. Schnirelmann

Nous appelons suite de nombres naturels $n_1, n_2, \dots, n_k, \dots$ une suite de densité supérieure à a ($a > 0$) si la limite inférieure du rapport k/n_k est supérieure à a .

Premier lemme fondamental

Quelle que soit la suite $n_1, n_2, \dots$ de densité supérieure à $a > 0$, on peut décomposer tout nombre x en une somme de $2[1/a]$ termes de cette suite, à un terme près ne dépassant pas une constante fixée A (ne dépendant pas du nombre x à décomposer, mais seulement de la suite $n_1, n_2, \dots$).

Désignons par $N(x)$ le nombre de termes de la suite $n_1, n_2, \dots$ ne dépassant pas x .

Si $N(x) > x/2$, alors le nombre x se décompose évidemment en une somme de deux termes de la suite. En effet, considérons la suite $x - n_1, x - n_2, \dots, x - n_k, \dots$; le nombre de termes de cette suite ne dépassant pas x est le même que pour la précédente, c'est-à-dire supérieur à $x/2$. Il existe donc un terme n_i de la première suite qui est égal à un certain terme $x - n_j$ de la seconde suite. On en déduit : $x = n_i + n_j$.

Supposons que $N(x) < x/2$. Si la densité de la suite est supérieure à $a > 0$, alors il existe un nombre p possédant la propriété suivante : quel que soit $m > p$, on a la relation $N(m) > (a - \varepsilon)m$ (ε étant un nombre positif arbitrairement petit).

Supposons que $x > p$.

Considérons la somme $R(x)$ de toutes les différences $n_{i+1} - n_i$ qui sont supérieures à p , avec $n_i < n_{i+1} < x$.

Deux cas sont possibles :

- 1) $R(x) < x/2$,
- 2) $R(x) > x/2$.

Dans le premier cas, le nombre de tous les entiers différant des termes de la suite $n_1, n_2, \dots, n_k, \dots$ d'au plus $(p+1)/2$ est supérieur à $x/2$. On peut donc décomposer x en une somme de deux termes de la suite $n_1, n_2, \dots$ et d'un terme ne dépassant pas $p+1$.

Dans le second cas, on intercale entre deux termes consécutifs n_i et n_{i+1} de notre suite tels que $n_{i+1} - n_i > p$, la série de nombres suivante : $n_i + n_1, n_i + n_2, \dots, n_i + n_j$ (jusqu'au plus grand $n_i + n_j$ ne dépassant pas n_{i+1}). En vertu des propriétés du nombre p , on obtient $j \geq (a - \varepsilon)(n_{i+1} - n_i)$. Le nombre total de termes ainsi introduits dépasse $(a - \varepsilon) \sum (n_{i+1} - n_i) = (a - \varepsilon) R(x) \geq \frac{1}{2}(a - \varepsilon)x$.

Désignons les termes de la nouvelle suite par $m_1, m_2, \dots, m_k, \dots$. Cette suite contient plus de $(a - \varepsilon)x + 2ax$ termes ne dépassant pas x . Si ce nombre est supérieur à $2x$, alors x peut être décomposé en une somme de deux termes de la nouvelle suite, c'est-à-dire en quatre termes de la suite initiale. Dans le cas contraire, on répète le raisonnement précédent pour la nouvelle suite $m_1, m_2, \dots$.

Formons de nouveau la somme $R_1(x)$ de toutes les différences $m_{i+1} - m_i$ ne dépassant pas p ; deux cas sont encore possibles : $R_1(x) < x/2$ et $R_1(x) > x/2$. Dans le premier cas, on peut décomposer x en une somme de deux termes de la suite $m_1, m_2, \dots$, c'est-à-dire en quatre termes de la suite initiale; dans le second cas, ou bien le nombre x se décompose en une somme de huit termes de la suite initiale, ou bien on peut répéter le processus précédent.

En poursuivant ce raisonnement, on démontre que, ou bien le nombre x se décompose en une somme de 2^k termes de la suite initiale et d'un terme ne dépassant pas $p + 1$, ou bien on peut construire une suite constituée de sommes $(k + 1)$ -uples de termes de la suite initiale et telle que le nombre de termes de cette nouvelle suite ne dépassant pas x soit supérieur à

$$(a - \varepsilon)x + \frac{k}{2}(a - \varepsilon)x = \frac{k + 2}{2}(a - \varepsilon)x.$$

Lorsque $\frac{k+2}{2}(a - \varepsilon)$ dépasse $1/2$, c'est-à-dire $k \geq [1/(a - \varepsilon)] - 1$, notre processus s'arrête, car dans la dernière suite le nombre de ses termes ne dépassant pas x est supérieur à $x/2$. Ainsi x se décompose en une somme d'au plus $2[1/(a - \varepsilon)]$ termes de la suite initiale et d'un terme ne dépassant pas $p + 1$. Cela démontre le lemme avec $A = p + 1$ (car pour $\varepsilon > 0$ suffisamment petit, $[1/(a - \varepsilon)] = [1/a]$).

Second lemme

Considérons la suite $n_1, n_2, \dots, n_k, \dots$, où $n_j < Cj\varphi(j)$ ($\varphi(j)$ étant une fonction croissante de j , telle que $\varphi(j) = o(\sqrt{j})$).

Désignons par $A(u, x)$ le nombre de solutions de l'équation $n_j - n_i = u$, où $n_i < n_j < x$, et par $T(x, s)$ la somme $\sum_{u=1}^s A^2(u, x)$.

Si pour tout $x > 0$ on a $T(x, s) < k_s x^2$, alors tout nombre x se décompose en une somme d'un nombre borné I de termes de la suite $n_1, n_2, \dots$ et d'un terme ne dépassant pas A . I et A ne dépendent pas du nombre à décomposer x , mais seulement de la suite $n_1, n_2, \dots$.

Démonstration

Formons un tableau à double entrée

$$\begin{array}{cccc}
 n_1, & n_2, & \dots, & n_k \\
 2n_1, & n_1 + n_2, & \dots, & n_1 + n_k \\
 n_2 + n_1, & 2n_2, & \dots, & n_2 + n_k \\
 \vdots & \vdots & \ddots & \vdots \\
 n_l + n_1, & n_l + n_2, & \dots, & n_l + n_k
 \end{array}$$

et estimons le nombre de termes distincts de ce tableau ne dépassant pas x .

Soit $n_k < x < n_{k+1}$. La première ligne du tableau contient plus de $\frac{x}{C\varphi(x)}$ termes, la seconde — plus de $\frac{x-n_1}{C\varphi(x-n_1)} - A(n_1, x)$ nouveaux termes, la troisième — plus de $\frac{x-n_2}{C\varphi(x-n_2)} - A(n_2, x) - A(n_2 - n_1, x)$ termes n'appartenant pas aux deux premières lignes, et ainsi de suite.

Le tableau entier contient $M(x)$ termes distincts, où

$$\begin{aligned}
 M(x) &\geq \frac{x}{C\varphi(x)} + \frac{x-n_1}{C\varphi(x-n_1)} - A(n_1, x) + \\
 &+ \frac{x-n_2}{C\varphi(x-n_2)} - A(n_2, x) - A(n_2 - n_1, x) + \dots + \\
 &+ \frac{x-n_l}{C\varphi(x-n_l)} - A(n_l, x) - A(n_l - n_1, x) - \dots - A(n_l - n_{l-1}, x) = \\
 &= \frac{1}{C} \sum_{j=1}^l \frac{x-n_j}{\varphi(x-n_j)} - \sum_{u=1}^{n_l} A(u, x) A(u, n_l),
 \end{aligned}$$

car chaque $A(u, x)$ apparaît autant de fois qu'il y a de façons de représenter le nombre u comme une différence $n_{j'} - n_j$, où $n_j < n_{j'} < n_l$, c'est-à-dire $A(u, n_l)$ fois.

D'après l'inégalité de Schwarz, on a

$$\begin{aligned}
 M(x) &\geq \frac{1}{C} \sum_{j=1}^l \frac{x-n_j}{\varphi(x-n_j)} - \sqrt{\sum_{u=1}^{n_l} A^2(u, x) \sum_{u=1}^{n_l} A^2(u, n_l)} = \\
 &= \frac{1}{C} \sum_{j=1}^l \frac{x-n_j}{\varphi(x-n_j)} - \sqrt{T(x, n_l) T(n_l, n_l)}.
 \end{aligned}$$

Choisissons $l = a\varphi(x)$ (a est un nombre réel supérieur à 0). On a $n_l < Ca\varphi(x)\varphi[a\varphi(x)]$. Comme $\varphi(x) = o(\sqrt{x})$, on a $n_l < x$ et $\varphi(n_l) > (1-\eta)\varphi(x)$ (où η est arbitrairement petit, x suffisamment grand).

En insérant ces expressions dans l'inégalité précédente, on obtient, en vertu de la condition du

lemme,

$$\begin{aligned}
M(x) &\geq \frac{(1-\eta)ax}{C} - \sqrt{\frac{kx^3}{\varphi^4(n_l)} \frac{kn_l^2}{\varphi^4(n_l)}} = \frac{(1-\eta)ax}{C} - \frac{kx}{\varphi^2(x)\varphi^2(n_l)} \\
&= \frac{(1-\eta)ax}{C} - kx \frac{\{Ca\varphi(x)\varphi[a\varphi(x)]\}^2}{\varphi^2(x)\varphi^2(Ca\varphi(x)\varphi[a\varphi(x)])} \geq \\
&\geq \frac{(1-\eta)ax}{C} - a^2C^2kx \frac{\{\varphi[a\varphi(x)]\}^2}{\{\varphi[a\varphi(x)]\}^2} = \frac{(1-\eta)ax}{C} - a^2C^2kx
\end{aligned}$$

(car pour x suffisamment grand, $\varphi\{a\varphi(x)\varphi[a\varphi(x)]\} > \varphi[a\varphi(x)]$).

En choisissant $a = \frac{1}{2C^2k}$, on obtient $M(x) > \frac{x}{4C^2k}$, c'est-à-dire que pour x suffisamment grand, le tableau contient plus de $\frac{x}{4C^2k}$ termes ne dépassant pas x . En rangeant les termes du tableau par ordre croissant, on obtient une suite dont la densité est au moins $\frac{1}{4C^2k}$. Le second lemme est donc une conséquence du premier.

Troisième lemme

Pour la suite des nombres premiers $p_1, p_2, \dots, p_k, \dots$, on a les relations : $\varphi(x) = \ln x$, $C = 1 + \varepsilon$ et

$$A(u, x) < \frac{x}{\ln^2 x} S(u),$$

où

$$S(u) = \sum_{\substack{p_i | u \\ p_i \text{ impair}}} \left(1 - \frac{2}{p_i}\right)^{-1},$$

le produit étant étendu à tous les diviseurs premiers impairs distincts p_i de u (ε est arbitrairement petit).

La démonstration de ce lemme est tout à fait analogue à celle de la formule

$$Z(x) < \frac{x}{\ln^2 x},$$

donnée par Viggo Brun, où $Z(x)$ est le nombre de nombres premiers jumeaux ne dépassant pas x .

Quatrième lemme

Posons $S(u)$ comme dans le lemme 3. On a

$$\sum_{u=1}^x S^2(u) < kx,$$

où k est une constante.

Démonstration

Considérons le produit

$$P(u) = \prod_{p_i|u} \left(1 + \frac{1}{p_i}\right)$$

étendu à tous les diviseurs premiers impairs distincts p_i de u . On a

$$\begin{aligned} S(u) &= \prod_{p_i|u} \left(1 - \frac{2}{p_i}\right)^{-1} = \prod_{p_i|u} \frac{p_i}{p_i - 2} \\ &= \prod_{p_i|u} \left(1 + \frac{2}{p_i - 2}\right) < \prod_{p_i|u} \left(1 + \frac{4}{p_i}\right) < 2^{\omega(u)}, \end{aligned}$$

où $\omega(u)$ est le nombre de diviseurs premiers distincts de u . Par conséquent, $S(u) < 2^{\omega(u)}$.

De plus,

$$S(u) = \prod_{p_i|u} \left(1 + \frac{2}{p_i} + \frac{4}{p_i^2} + \dots\right) = \sum_{d|u, (d,2)=1} \frac{g(d)}{d},$$

où $g(d)$ est une fonction multiplicative bornée.

On a alors

$$\sum_{u=1}^x S^2(u) \leq \sum_{u=1}^x \left(\sum_{d|u} \frac{g(d)}{d} \right)^2 = \sum_{d_1, d_2} \frac{g(d_1)g(d_2)}{d_1 d_2} \left[\frac{x}{\text{ppcm}(d_1, d_2)} \right].$$

En majorant $[x/\text{ppcm}]$ par x/ppcm et en utilisant la convergence des séries de Dirichlet associées, on obtient

$$\sum_{u=1}^x S^2(u) \leq kx,$$

où k est une constante. Ceci démontre le lemme.

Application à la suite $[n \ln n]$

Considérons la suite $p_1 = 1 \ln 1 = 0$, $p_2 = 2 \ln 2$, ..., $p_k = k \ln k$, ... et extrayons-en une série de termes $q_1 = k_1 \ln k_1$ de l'ordre de $\ln^3 x$, c'est-à-dire $k_1 = \left\lfloor \frac{\ln^3 x}{3 \ln \ln x} \right\rfloor$, et de même $q_2 = k_2 \ln k_2 \sim 2 \ln^3 x$, $q_3 = k_3 \ln k_3 \sim 3 \ln^3 x$, ... et ainsi de suite, jusqu'à $q_{a \ln x} = k_{a \ln x} \ln k_{a \ln x} \sim a \ln^4 x$.

Formons le tableau

$$\begin{array}{cccc} p_1, & p_2, & \dots, & p_t \\ p_1 + q_1, & p_2 + q_1, & \dots, & p_t + q_1 \\ p_1 + q_2, & p_2 + q_2, & \dots, & p_t + q_2 \\ \vdots & & & \\ p_1 + q_{a \ln x}, & p_2 + q_{a \ln x}, & \dots, & p_t + q_{a \ln x} \end{array}$$

où $p_t \leq x < p_{t+1}$. Le nombre de termes distincts de ce tableau est au moins

$$\frac{x}{\ln x} + \left[\frac{x}{\ln x} - A(q_1, x) \right] + \left[\frac{x}{\ln x} - A(q_2, x) - A(q_2 - q_1, x) \right] + \dots + \left[\frac{x}{\ln x} - A(q_j, x) - \dots - A(q_j - q_{j-1}, x) \right] + \dots$$

Dans ce cas, toutes les différences $q_i - q_j$ sont comprises entre $\ln^3 x$ et $\ln^4 x$. Donc tous les $A(q_i - q_j, x) < 3,2 \frac{x}{\ln^2 x}$, et le nombre de termes distincts du tableau est au moins

$$a \frac{x}{\ln x} \ln x - 3,2a \frac{x}{\ln x} \sum_{n=1}^{a \ln x} n = ax - 3,2 \frac{a^2 \ln^2 x}{2 \ln^2 x} x = x(a - 1,6a^2).$$

Critère général pour une base additive

Soit donnée une suite $n_1, n_2, \dots$ de nombres naturels, et soit $N(x)$ le nombre de ses termes ne dépassant pas x . Considérons les sommes de u termes de cette suite. Soit A_j le nombre de représentations du nombre j comme somme de u termes de la suite, et soit

$$D(x) = \sum_{j=1}^x A_j^2.$$

Si pour un certain u fixé on a

$$D(x) < C \frac{N(x/u)^{2u}}{x^{2u}},$$

alors la suite formée par les sommes de u termes a une densité positive $\geq 1/C$.

En effet, on a

$$\sum_{j=1}^x A_j \geq \left(N\left(\frac{x}{u}\right) \right)^u.$$

D'après l'inégalité de Schwarz,

$$\left(\sum_{j=1}^x A_j \right)^2 \leq \mu(x) \sum_{j=1}^x A_j^2,$$

où $\mu(x)$ est le nombre de A_j non nuls pour $j \leq x$. Par conséquent,

$$\mu(x) \geq \frac{(N(x/u))^{2u}}{D(x)} \geq \frac{x}{C}.$$

Ainsi, la suite des sommes de u termes a une densité $\geq 1/C$. La première lemme fondamental implique alors que la suite initiale est une base additive.

Remarque

La condition $D(x) < C \frac{N(x/u)^{2u}}{x}$ peut être remplacée par

$$\frac{1}{x} \sum_{a=0}^{x-1} \left| f_x \left(\frac{a}{x} \right) \right|^{2u} < C \frac{N^{2u}(x/u)}{x},$$

où

$$f_x(t) = \sum_{n_i \leq x} e^{2\pi i n_i t}.$$

En effet, on a

$$\frac{1}{x} \sum_{a=0}^{x-1} \left| f_x \left(\frac{a}{x} \right) \right|^{2u} = \sum_{j=1}^{un_k} A_j^2 + 2 \sum_{j,k} A_j A_k \frac{1}{x} \sum_{a=0}^{x-1} \cos 2\pi \frac{a}{x} (j-k).$$

Or

$$\frac{1}{x} \sum_{a=0}^{x-1} \cos 2\pi \frac{a}{x} (j-k) = \begin{cases} 1, & \text{si } x \mid (j-k), \\ 0, & \text{sinon.} \end{cases}$$

Donc

$$\frac{1}{x} \sum_{a=0}^{x-1} \left| f_x \left(\frac{a}{x} \right) \right|^{2u} \geq \sum_{j=1}^x A_j^2 = D(x).$$

Lemme de van der Corput

Soit $g(v)$ une fonction de la variable réelle v . Si $\theta \leq g(v+1) - g(v) \leq \pi$ et $g(v+1) - 2g(v) + g(v-1) > 0$, alors

$$\left| \sum_{v=1}^n e^{ig(v)} \right| < \frac{1}{\alpha} + C,$$

où C est une constante absolue.

Démonstration

On a

$$e^{ig(v)} = \frac{e^{ig(v+1)} - e^{ig(v)}}{i[g(v+1) - g(v)]} \cdot \frac{i[g(v+1) - g(v)]}{e^{i[g(v+1) - g(v)]} - 1}.$$

La fonction $\frac{z}{e^z - 1}$ est holomorphe à l'intérieur du cercle de rayon 2π . Le dernier facteur se développe en série entière convergente à l'intérieur de ce cercle :

$$e^{ig(v)} = \frac{e^{ig(v+1)} - e^{ig(v)}}{i[g(v+1) - g(v)]} + \sum_{k=1}^{\infty} a_k (e^{ig(v+1)} - e^{ig(v)}) [g(v+1) - g(v)]^{k-1} i^{k-1}.$$

D'après le second théorème de la moyenne, en raison des inégalités

$$\frac{1}{g(v+2) - g(v+1)} - \frac{1}{g(v+1) - g(v)} < 0,$$

et

$$[g(v+2) - g(v+1)]^k - [g(v+1) - g(v)]^k > 0,$$

on obtient

$$\left| \sum_{v=1}^n \frac{e^{ig(v+1)} - e^{ig(v)}}{i[g(v+1) - g(v)]} \right| < \frac{1}{\alpha},$$

et

$$\left| \sum_{v=1}^n (e^{ig(v+1)} - e^{ig(v)}) [g(v+1) - g(v)]^{k-1} i^{k-1} \right| < \pi^{k-1}.$$

D'où

$$\left| \sum_{v=1}^n e^{ig(v)} \right| < \frac{1}{\alpha} + \sum_{k=1}^{\infty} |a_k| \pi^{k-1} = \frac{1}{\alpha} + C,$$

car la série $\sum_{k=1}^{\infty} |a_k| z^k$ converge à l'intérieur du cercle de rayon 2π .

Lemme de Weyl

Soit $P(n) = \gamma n^p + \alpha_1 n^{p-1} + \dots$ un polynôme de degré p à coefficient dominant γ . Alors

$$\left| \sum_{n=1}^N e^{2\pi i P(n)} \right|^{2^{p-1}} < 4^{2^{p-1}} \left(N^{2^{p-1}} + N^{2^{p-1}-p} \sum_{1 \leq h_i \leq N} \frac{1}{\|p! \gamma h_1 \cdots h_{p-1}\|} \right),$$

où $\|\cdot\|$ désigne la distance à l'entier le plus proche.

Application à la somme exponentielle

On considère la somme

$$S = \sum_{n=1}^{x^{1/p}} e^{2\pi i \frac{a}{x} n^p}.$$

Premier cas : $a < \frac{x}{p}$

Posons $\alpha = \frac{a}{x}$. Si $\alpha(1+\varepsilon) < 1$, on décompose S en deux parties. La première est bornée par $O(x^{1/p})$, la seconde est estimée à l'aide du lemme de van der Corput, ce qui donne

$$|S| < \frac{x^{1/p}}{\alpha^{1/p}}.$$

Deuxième cas : $a > \frac{x}{p}$

On approche $\frac{a}{x}$ par une fraction $\frac{a'}{y}$ avec $|a'| < \frac{1}{2}$ et $y < 2p!x^{(p-1)/p}$. Deux estimations sont possibles selon la taille de y .

Première estimation (pour $y \leq x^{1/(2p)}$)

En décomposant la somme en blocs de longueur y et en utilisant le lemme de van der Corput, on obtient

$$|S| < \frac{x^{1/p}}{y^{1/p}}.$$

Deuxième estimation (pour tout y)

D'après le lemme de Weyl,

$$|S|^{2^{p-1}} < 4^{2^{p-1}} \left(x^{(p-1)/p} + x^{(p-1)/p} \sum_{p!h_1 \cdots h_{p-1}} \frac{1}{\|a/x\|} \right).$$

En utilisant la majoration de la somme par $x^{1/p}y^{1/p}$, on obtient

$$|S| < x^{1/p} \left(\frac{1}{y^{1/p}} + \frac{1}{y^{(p-1)/p}} \right).$$

Démonstration du théorème de Waring généralisé

Considérons la suite des puissances p -ièmes $1^p, 2^p, \dots$. Le nombre de termes ne dépassant pas x est $N(x) \sim x^{1/p}$. On vérifie que la condition du second lemme fondamental est satisfaite, ce qui prouve que cette suite est une base additive. Cela donne une nouvelle démonstration du théorème de Waring.