G. Ricci (Ed.)

CIME Summer Schools

Teoria dei numeri

5

Varenna, Italy 1955

Springer

FONDAZIONE CIME ROBERTO CONTI

G. Ricci (Ed.)

Teoria dei numeri

Lectures given at the
Centro Internazionale Matematico Estivo (C.I.M.E.),
held in Varenna (Como), Italy,
August 16-25, 1955

C.I.M.E. Foundation
c/o Dipartimento di Matematica “U. Dini”
Viale Morgagni n. 67/a
50134 Firenze
Italy
cime@math.unifi.it

ISBN 978-3-642-10891-4 e-ISBN: 978-3-642-10892-1
DOI:10.1007/978-3-642-10892-1
Springer Heidelberg Dordrecht London New York

Reprint of the 1st ed. C.I.M.E., Florence, 1955
With kind permission of C.I.M.E.

Printed on acid-free paper

Springer.com

CENTRO INTERNATIONALE MATEMATICO ESTIVO
(C.I.M.E)

2° Ciclo - Varenna, Villa Monastero – 16-25 Agosto, 1955

TEORIA DEI NUMERI

H. D A V E N P O R T

PROBLEMES D'EMPILEMENT ET DE DECOUVREMENT

ROMA-Istituto Matematico dell'Università,1955-ROMA

H.Davenport

PROBLEMES D'EMPILEMENT ET DE DECOUVREMENT

Le sujet que je me propose de traiter dans ces conférences offre beaucoup de problèmes simples et intéressants, qui pour la plupart attendent toujours une solution. Jusqu'à présent on n'a pas trouvé beaucoup de méthodes applicables à ces problèmes, et à mon avis, un riche terrain attend encore la découverte d'idées nouvelles.

1. Définitions .

Les concepts d'empilement le plus compact et de recouvrement les moins compact sont très généraux, et nos définitions seront donc d'une portée plus large que nous n'est nécessaire plus tard.

Le sujet se rapporte à l'espace numérique réel à n dimensions et nous nous servirons de la notation suivante. Nous désignerons un point quelconque de l'espace par

$$\underline{x} = (x_1,\ldots,x_n)$$

et nous définissons

$$\lambda \underline{x} = (\lambda x_1,\ldots,\lambda x_n) \qquad (\lambda \text{ un nombre réel}),$$
$$\underline{x} + \underline{y} = (x_1+y_1,\ldots,x_n+y_n).$$

Pour chaque ensemble E de points, nous noterons λE l'ensemble de tous les points $\lambda \underline{x}$, où $\underline{x}$ est un point quelconque de E. Ici λ désigne un nombre réel, soit positif, soit négatif. Pour chaque point $\underline{p}$ de l'espace, notons $E+\underline{p}$ l'ensemble de tous les points $\underline{x} + \underline{p}$, où $\underline{x}$ est un point quelconque de E.

Soit S un ensemble borné de points, mesurable au sens de

Lebesgue et à mesure $m(S) > 0$.
Soit C le cube

$$|x_1| < \frac{1}{2}, \ldots, |x_n| < \frac{1}{2} .$$

Soient $p_1, \ldots, p_k$ des points tels que les ensembles

$$S + p_1, \ldots, S + p_k$$

soient tous disjoints et soient tous contenus dans le cube λC, où λ est un grand nombre positif,

Nous disons que ces ensembles sont <u>empilés</u> dans le cube λC. La mesure totale des ensembles est $k\, m(S)$, et la mesure (c'est-à-dire le volume) de λC est λ^n. La densité de l'empilement est ainsi $k\, m(S)/\lambda^n$. Si k_0 désigne la plus grande valeur possible de k, nous définissons la densité de l'empilement le plus compact de S dans λC comme suit:

$$(1) \qquad \delta(S; \lambda C) = \frac{k_0\, m(S)}{\lambda^n}$$

On a $0 < \delta(S; \lambda C) \leq 1$.

On démontre facilement que la limite

$$(2) \qquad \lim_{\lambda \to \infty} \delta(S; \lambda C) = \delta^*(S)$$

existe, et nous appelons $\delta^*(S)$ <u>la densité de l'empilement le plus compact pour S, ou le coefficient d'empilement de S.</u>
Constatons d'abord deux propriétés simples de $\delta(S; \lambda C)$, considéré comme fonction de λ. Primo, le nombre k_0 ne peut pas diminuer à mesure que λ augmente, et si $\lambda_1 < \lambda_2$ il s'ensuit que

$$\delta(S; \lambda_2 C) \geq \left(\frac{\lambda_1}{\lambda_2}\right)^n \delta(S; \lambda_1 C)$$

Secundo, on a

$$\delta(S; m\lambda C) \geqslant \delta(S; \lambda C)$$

pour tout entier positif m. Car on peut regarder le cube $m\lambda C$ comme une somme de m^n cubes, dont chacun est congru à λC; et si on répète dans chacun de ces cubes l'empilement le plus compact pour le cube λC, on obtient pour $m\lambda C$ un empilement possible à la meme densité qu'auparavant. Ces deux propriétés montrent que $\delta(S; \lambda C)$ est une fonction presque monotone de λ, et l'existence de la limite s'ensuit facilement. On a, bien entendu,

$$0 < \delta^*(S) \leqslant 1 \tag{3}$$

Remarquons que nous aurions obtenu la même valeur pour $\delta^*(S)$ si nous avions supposé le cube C fermé au lieu d'ouvert.

La définition de $\delta^*(S)$ que nous venons de donner est un peu spéciale, en tant qu'elle emploie un système particulier de coordonnées et une espèce particuliere de corps (c'est-à-dire un cube). Ces limitations se laissent facilement lever. Premièrement, il est évident qu'une translation du système de coordonnées n'a aucun effet.

Deuxièmement, on peut remplacer le cube C par tout ensemble J qui est quarrable, c'est-à-dire, mesurable au sens de Jordan. Dans ce cas-là, nous définissons $\delta(S; \lambda J)$ de la même façon que $\delta(S; \lambda C)$ mais nous remplaçons λ^n par $\lambda^n m(J)$. Il est facile de démontrer que

$$\lim_{\lambda \to \infty} \delta(S; \lambda J) = \delta^*(S) \tag{4}$$

Car, puisque J est mesurable au sens de Jordan, il est contenu

dans la réunion d'un ensemble fini de cubes non-empiétants $C_1,\dots,C_r$, et contient lui-même un ensemble fini de cubes non-empiétamts $C_1',\dots,C_S'$, tels que et

$$m(C_1) + .. + m(C_r) - m(J)$$

et

$$m(J) - m(C_1') - \dots - m(C_S')$$

puissent se faire arbitrairement petits. Avec une notation évidente, nous avons

$$k_0(\lambda J) \geqslant k_0(\lambda C_1') + \dots + k_0(\lambda C_S'),$$

et

$$k_0(\lambda J) \leqslant k_0(\lambda C_1) + \dots + k_0(\lambda C_r) + O(\lambda^{n-1})$$

où le terme $O(\lambda^{n-1})$ est introduit afin de tenir compte du nombre des corps $S + p_i$ qui sont contenus dans λJ mais non entièrement contenus dans un de $\lambda C_1,\dots,\lambda C_r$. En faisant tendre λ vers ∞ nous obtenons

$$\liminf_{\lambda\to\infty} \delta(S;\lambda J) \geqslant \frac{m(C_1') + \dots + m(C_S')}{m(J)}\,\delta^*(S)$$

$$\limsup_{\lambda\to\infty} \delta(S;\lambda J) \leqslant \frac{m(C_1) + \dots + m(C_r)}{m(J)}\,\delta^*(S)$$

ce qui donne (4).

La relation (4) montre en particulier que $\delta^*(S)$ est un <u>invariant affine</u> de S, c'est-à-dire que $\delta^*(S_1) = \delta^*(S_2)$ si S_1 se transforme en S_2 au moyen d'une trasformation linéaire de l'espace à déterminant non-nul. Car, dans une telle trasformation, la mesure de J et la mesure de D se multipliant tous les deux par

le même nombre, à savoir le déterminant de la transformation.

Nous passons maintenant à la définition d'un autre nombre: la densité du recouvrement le moins compact pour S, ou <u>le coefficient de recouvrement de S</u>, que nous désignerons par $\vartheta^*(S)$. S nnte toujours un ensemble de points borné et mesurable, mais nous allons supposer maintenant que S ait au moins un point intérieur, afin d'assurer que la densité soit toujours finie. Soient $\underline{a}_1,\dots,\underline{a}_l$ des points tels que la réunion des ensembles

$$S + \underline{a}_1 ,\dots, S + \underline{a}_l$$

contienne tout le cube λC. Nous disons que ces ensembles <u>recouvrent</u> λC. Soit l_0 la moindre valeur possible de l. Nous définissons la densité du recouvrement le moins compact de λC par S comme suit:

$$\vartheta(S;\lambda C) = \frac{l_0\, m(S)}{\lambda^n} \tag{5}$$

On démontre dans difficulté que

$$\lim_{\lambda\to\infty} \vartheta(S;\lambda C) = \vartheta^*(S)$$

existe. L'analogue de (4) tient, d'où il suit que $\vartheta^*(S)$ est aussi un invariant affine de S.

On a

$$\vartheta^*(S) \geqslant 1 \tag{6}$$

Les définitions de $\delta^*(S)$ et de $\vartheta^*(S)$ peuvent se formuler autrement. Désignons par $\underline{p}_1,\underline{p}_2,\dots$ un ensemble infini de points, tel que les ensembles $S + \underline{p}_1$, $S + \underline{p}_2,\dots$ soient tous disjoints. Prenons la densité supérieure de la réunion de ces ensembles, et notons $\delta^*(S)$ la borne supérieure de cette densité supérieure, prise pour tout ensemble $\underline{p}_1,\underline{p}_2,\dots$ permis. On démontre aisément que

cette définition équivaut à la définition donnée plus tard. Et de même pour $\vartheta^*(S)$.

2. Empilements et recouvrements réguliers.

On appelle réseau l'ensemble de points qu'on obtient de l'ensemble de tous les points à coordonnées entières au moyen d'une transformation linéaire de l'espace. Ainsi les points $\underline{x}$ du réseau s'obtiennent de n formes linéaires

$$x_1 = \alpha_{11} u_1 + \cdots + \alpha_{1n} u_n$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$x_n = \alpha_{n1} u_1 + \cdots + \alpha_{nn} u_n ,$$

en donnant aux variables, $u_1, \ldots u_n$ toutes les valeurs entières. Les coefficients α_{ij} sont des nombres réels arbitraires, à condition que dét α_{ij} soit non égal à 0. [On peut aussi définir un réseau comme un groupe additif de points qui n'à aucun point d'accumulation et qui n'est contenu dans aucune espace linéaire à n-1 dimensions] .

Dans le langage des matrices, les points $\underline{x}$ d'un réseau s'obtiennent de

$$\underline{x} = A \underline{u} ,$$

où A désigne une matrice réelle non-singulière et où $\underline{u}$ est le point (vecteur) général à coordonnées entières. Une substitution $\underline{u} = M \underline{v}$, où M est une matrice unimodulaire (c.-à-d. matrice d'éléments entiers à déterminant ± 1), transforme l'ensemble de tous les points entiers $\underline{u}$ en l'ensemble de tous les points entiers $\underline{v}$. Il s'ensuit que le réseau reste le même si on remplace la matrice A par la matrice AM.

On donne le nom de déterminant d'un réseau à la valeur absolue de déterminant de A. Nous désignons le déterminant d'un réseau Λ

$d(\Lambda)$. Le déterminant d'un réseau est susceptible d'une simple interprétation géométrique: il est le réciproque de la densité du réseau. Cette densité se définit de façon naturelle comme le quotient limitant du nombre de points d'un réseau dans un grand corps divisé par le volume du corps. Or, un corps de volume V dans l'espace des points $\underline{x}$ correspond à un corps de volume $V/d(\Lambda)$ dans l'espace des points $\underline{u}$, et comme la densité des points $\underline{u}$ à coordonnées entières est égale à 1, il s'ensuit que la densité du réseau Λ dans l'espace des points $\underline{x}$ est égale à $1/d(\Lambda)$.

Soit maintenant S un ensemble donné (borné et mesurable avec $m(S) > 0$) et supposons qu'un réseau Λ ait la propriété que tous les ensembles $S + \underline{p}$, où p parcourt les points de Λ, soient disjoints. Alors Λ donne un empilement régulier pour l'ensemble S, à densité $m(S)/d(\Lambda)$. Nous définissons

$$\delta(S) = \sup_{\Lambda} \frac{m(S)}{d(\Lambda)} \tag{1}$$

et nous appelons $\delta(S)$ la densité de l'empilement régulier le plus compact pour S, ou le coefficient d'empilement régulier de S. Nous définissons de façon analogue la densité du recouvrement régulier le moins compact pour S, ou le coefficient de recouvrement régulier de S, que nous notons $\vartheta(S)$. Il est évident que

$$0 < \delta(S) \leqslant \delta^*(S) \leqslant 1 \leqslant \vartheta^*(S) \leqslant \vartheta(S), \tag{2}$$

puisque les empilements réguliers forment un sousensemble de tous les empilements, et de même quant aux recouvrements.

3. Les corps convexes.

Dorénavant, nous allons nous limiter pour la plupart au cas où l'ensemble S est un corps convexe symétrique. Un corps convexe

symétrique K est un ensemble de points, ouvert[1] et borné, tel que $\frac{1}{2}(\underline{p} - \underline{q})$ est un point de K quand $\underline{p}$ et $\underline{q}$ sont des points de K. En particulier -K = K. Il est bien connu que tout corps convexe est quarrable, c'est-à-dire possède un volume au sens classique de Jordan. Nous allons donc employer la notation V(K) au lieu de m(K).

Le problème de trouver $\delta(K)$ pour un corps convexe symétrique équivaut au problème de trouver le déterminant critique de K, voilà un des problèmes les plus importants de la géométrie des nombres. Car la condition que les corps $K + \underline{p}$ n'empiètent pas ($\underline{p}$ étant un point quelconque de Λ) équivaut à la condition que le réseau Λ n'ait pas d'autre point que l'origine O dans le corps 2K. En effet, si $K + \underline{p}_1$ et $K + \underline{p}_2$ ont un point commun $\underline{z}$, alors $\underline{z} - \underline{p}_1$ et $\underline{z} - \underline{p}_2$ se trouvent tous les deux dans K, et ainsi le point $\frac{1}{2}(\underline{p}_1 - \underline{p}_2)$ se trouve dans K. D'autre part, s'il existe un point $\underline{q}$ de Λ autre que O dans 2K, alors les corps K et $K + \underline{q}$ contiennent tous les deux le point $\frac{1}{2}\underline{q}$ et empiètent. Donc, dans la définition de $\delta(K)$ dans (1) du § 2, il nous faut choisir Λ de manière à rendre $d(\Lambda)$ minimal, toujours à condition que Λ n'ait d'autre point que O dans 2K. Le minimum de $d(\Lambda)$ sous cette condition est, par définition, le déterminant critique du corps 2K, désigné par $\Delta(2K)$. Donc

$$(1) \qquad \delta(K) = \frac{V(K)}{\Delta(2K)} = \frac{V(K)}{2^n \Delta(K)}$$

Le simple fait que $\delta(K) \leq 1$ nous donne le théorème classique de Minkowski, fondamental pour la géométrie des nombres:

$$\Delta(K) \geq 2^{-n} V(K).$$

---

1) Pour les valeurs de $\delta(K)$ etc. il n'importe rien si on inclus, dans K sa frontière ou non. Les formulations deviennent un peu plus simple si l'on inclue la frontière quand on traite les questions de recouvrement mais non quand on traite les questions d'empilement.

Dans les raisonnements rélatifs aux corps convexes, il est souvent utile de se servir de la norme (fonction de distance) d'un corps.

Nous définissons la norme $F(\underline{x})$ d'un corps convexe symétrique K comme suit. Si $\underline{x}$ est un point quelconque autre que 0, il existe un nombre positif et bien défini tel que $\mu \underline{x}$ se trouve sur la frontière de K, et nous posons $F(\underline{x}) = \mu^{-1}$. Pour compléter la définition nous mettons $F(0)=0$. K consiste alors des points $\underline{x}$ pour lesquels $F(x) < 1$ (ou $F(x) \leq 1$ si l'on comprend dans K sa frontière). On démontre facilement que $F(x)$ possède les propriétés suivantes:

(i) $F(0)=0$, $F(\underline{x}) > 0$ pour $\underline{x} \neq 0$;

(ii) $F(\underline{x} + \underline{y}) \leq F(\underline{x}) + F(\underline{y})$;

(iii) $F(\lambda \underline{x}) = |\lambda| F(\underline{x})$ pour tout nombre réel λ .

Réciproquement, si $F(\underline{x})$ est une fonction possédant ces trois propriétés[2], l'inégalité $F(\underline{x}) < 1$ définit un corps convexe symétrique.

Pour un corps convexe symétrique donné K, et pour un réseau donné, Λ , nous définissons le minimum M de $F(\underline{x})$ pour Λ par

$$M = \min_{p \in \Lambda, p \neq 0} F(p) \tag{2}$$

Autrement dit, M est le plus grand nombre tel que le réseau $\frac{1}{M}$ n'ait aucun point sauf 0 dans le corps K. Donc

$$\Delta(K) = \min_{\Lambda} \frac{d(\Lambda)}{M^n} . \tag{3}$$

---

(2) On peut déduire de ce trois propriétés que $F(\underline{x})$ est une fonction continue.

Suivant (1),

$$\delta(K) = \max_{\Lambda} \frac{V(K) M^n}{2^n d(\Lambda)} . \tag{4}$$

Nous définissons aussi le minimum inhomogène M_I de $F(\underline{x})$ pour Λ en posant

$$M_I = \max_{\underline{z}} \min_{\underline{p} \in \Lambda} F(\underline{p} - \underline{z}) , \tag{5}$$

où le maximum est pris pour tous les points $\underline{z}$ de l'espace. Autrement dit, M_I est le plus petit nombre avec cette propriété: pour chaque point $\underline{z}$ de l'espace il existe un point $\underline{p}$ de Λ tel que $F(\underline{p} - \underline{z}) \leqslant M_I$. Le réseau $\frac{1}{M_I} \Lambda$ fournit un recouvrement pour K. Donc

$$\vartheta(K) = \min_{\Lambda} \frac{V(K) M_I^n}{d(\Lambda)} \tag{6}$$

Ceci est simplement une autre formulation de la définition de $\vartheta(K)$, et elle reste valable si K est convexe ou non; à cet égard elle diffère de (4).

4. Deux inegalités de Rogers.

C.A.Rogers[1] établit les inégalités générales suivantes, qui relient $\vartheta(K)$ à $\delta(K)$ et $\vartheta^*(K)$ à $\delta^*(K)$.

THEOREME 1. Pour tout corps K, convexe et symétrique, on a

$$\vartheta^*(K) \leqslant 2^n \delta^*(K) \tag{1}$$

$$\vartheta(K) \leqslant 3^{n-1} \delta(K) . \tag{2}$$

Il s'ensuit que

---

1) J.London Math. Soc. 25 (1950), 327-331.