Séminaire Dubreil.
Algèbre et théorie
des nombres

HAROLD DAVENPORT

Les équations diophantiennes à plusieurs variables

Séminaire Dubreil. Algèbre et théorie des nombres, tome 12, n° 2 (1958-1959), exp. n° 20, p. 1-9

<http://www.numdam.org/item?id=SD_1958-1959__12_2_A5_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire P. DUBREIL
M.-L. DUBREIL-JACOTIN et C. PISOT
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1958/59
-:-:-:-

6 avril 1959

LES ÉQUATIONS DIOPHANTIENNES À PLUSIEURS VARIABLES

par Harold DAVENPORT

La question que je considérerai dans cette conférence est très simple, mais assez générale. Soit $f(x_1, \ldots, x_n)$ un polynôme homogène à n variables, de degré d, à coefficients entiers. Sous quelles conditions de caractère général (conditions portant surtout sur n) peut-on affirmer que l'équation

$$f(x_1, \ldots, x_n) = 0 \tag{1}$$

possède une solution en nombres entiers, non tous nuls ? Une solution en nombres rationnels, non tous nuls, revient au même parce que f est homogène.

Le cas $d = 2$ est classique. Une forme quadratique se laisse transformer en forme diagonale au moyen d'une transformation linéaire à coefficients rationnels. Il suffit ainsi de traiter une équation de la forme

$$a_1 x_1^2 + \ldots + a_n x_n^2 = 0 \quad . \tag{2}$$

Evidemment, une condition nécessaire, c'est que les coefficients $a_1, \ldots, a_n$ ne soient ni tous positifs ni tous négatifs ; autrement dit, que la forme f soit indéfinie. En 1785, LEGENDRE a trouvé les conditions nécessaires et suffisantes pour que l'équation ait une solution quand $n = 3$. Ces conditions (sauf celle mentionnée) sont des conditions qui exigent que certaines congruences soient possibles. En 1884, MEYER a trouvé les conditions nécessaires et suffisantes quand $n = 4$, et il a démontré en outre que pour $n \geq 5$ toute équation est résoluble pourvu qu'elle satisfasse à la condition touchant les signes des coefficients. Ce dernier résultat se laisse formuler comme suit : <u>toute forme quadratique indéfinie à 5 ou plus de variables représente zéro</u>.

En 1923, HASSE a exprimé ces résultats classiques dans une forme plus lumineuse. Pour qu'une équation diophantienne quelconque soit résoluble, il faut évidemment qu'elle soit résoluble à la fois dans le corps réel et dans chaque corps p-adique.

HASSE démontra que, pour les équations quadratiques homogènes, ces conditions nécessaires sont en même temps suffisantes. Si $n \geq 5$, la condition de résolubilité dans les corps p-adiques est toujours remplie ; si $n = 3$ ou 4, elle est toujours remplie, sauf peut-être pour les nombres premiers p qui divisent 2 dét f, et il reste ainsi un nombre fini de conditions congruentielles. HASSE démontra aussi qu'un théorème analogue est valable pour les équations quadratiques homogènes dans les corps algébriques.

C'est seulement pendant le demi-siècle passé qu'on a obtenu des résultats vraiment généraux sur les équations diophantiennes (de n'importe quelle espèce) de degré supérieur au deuxième. Pendant ce temps sont apparus les travaux de L. J. MORDELL, de André WEIL, et de C. L. SIEGEL, travaux qui sont tout à fait remarquables tant pour leur généralité que pour leur profondeur. Cependant, ces recherches portent sur les équations à deux ou trois variables indépendantes, et elles ont, par conséquent, peu de rapport avec le problème que je voudrais traiter ici.

Au cours des années 1920 à 1930, HARDY et LITTLEWOOD ont développé leur méthode célèbre pour la solution du problème de Waring et d'autres problèmes de caractère additif. Cette méthode est à l'origine des travaux dont je vais parler tout à l'heure, et il faut donc que j'en esquisse les lignes principales.

Le problème de Waring, c'est le problème de représenter tout entier N suffisamment grand comme une somme de puissances d-ièmes d'entiers positifs :

$$N = x_1^d + \ldots + x_n^d , \quad x_i \geq 0 \qquad . \tag{3}$$

Le résultat final du travail de HARDY et LITTLEWOOD, c'est que, si $n \geq n_0(d)$, il existe une formule asymptotique pour le nombre $r(N)$ de représentations, valable quand N augmente indéfiniment.

Le point de départ du travail se trouve dans une expression de $r(N)$ à l'aide de la somme exponentielle :

$$S(\alpha) = \sum_{0 < x < N^{1/k}} e^{2\pi i \alpha x^d} , \tag{4}$$

où α est réel. Cette expression est

$$r(N) = \int_0^1 (S(\alpha))^n \, e^{-2\pi i \alpha N} d\alpha , \tag{5}$$

et elle découle directement du fait que

$$\int_0^1 e^{2\pi i \alpha m} \, d\alpha = \begin{cases} 1 & \text{si } m = 0 , \\ 0 & \text{si } m \text{ est un entier } \neq 0 . \end{cases}$$

L'intégrale (5) se divise en deux parties. Pour chaque nombre rationnel $\frac{a}{q}$, où q est inférieur à une certaine fonction de N, il y a un intervalle de valeurs de α voisines de $\frac{a}{q}$, dans lequel on peut remplacer $S(\alpha)$ par une approximation. Dans cette approximation entre la somme arithmétique

$$S_{a,q} = \sum_{x=1}^{q} e^{2\pi i \frac{a}{q} x^d} , \tag{6}$$

et, à part cette somme, il y entre seulement une fonction élémentaire de $\alpha - \frac{a}{q}$. Ces intervalles s'appellent les "major arcs", et le reste de l'intervalle $0 < \alpha < 1$ forme les "minor arcs". Dans ce dernier cas, il faut employer une borne supérieure pour $|S(\alpha)|$. Une telle borne est fournie par l'inégalité de Weyl, qu'il a établie, en principe, dans son mémoire célèbre de 1916 sur "Gleichverteilung". La contribution des minor arcs à l'intégrale (5) est inférieure à la contribution des major arcs pourvu que n soit plus grand qu'une certaine fonction de d.

Les détails du travail sont compliqués, et peuvent être développés de plusieurs façons. La formule asymptotique pour $r(N)$ qui en résulte est de la forme

$$r(N) \sim C(d , n) \, N^{\frac{n}{d}-1} \prod_p \chi_p(d , n) . \tag{7}$$

On peut considérer le facteur $C(d , n) \, N^{\frac{n}{d}-1}$ comme mesure de la densité des solutions de (3), y inclues les conditions de grandeur, dans le corps réel, et on peut considérer le facteur $\chi_p(d , n)$ comme mesure de la densité des solutions de (3) dans le corps p-adique. Il existe donc une liaison entre cette formule asymptotique et le théorème de Hasse sur les équations quadratiques homogènes. Mais, bien entendu, la formule asymptotique est plus profonde, et n'est valable que si n est suffisamment grand par rapport à d.

On peut appliquer la méthode de Hardy et Littlewood à l'étude des équations de la forme

$$a_1 x_1^d + \ldots + a_n x_n^d = 0 , \tag{8}$$

et aucune grande difficulté nouvelle ne se présente. Une telle équation représente un type spécial (type diagonal) de l'équation générale (1). Il faut noter une différence évidente avec le problème de Waring : la variable N est absente de la

formulation du problème, et il faut introduire, au lieu de N, un paramètre comme mesure de la grandeur des variables $x_1, \dots, x_n$. Cela se fait le plus simplement comme suit. Nous prenons une solution réelle $\xi_1, \dots, \xi_n$ de l'équation (8), dont aucune des variables n'est nulle, et nous étudions le nombre de solutions en entiers $x_1, \dots, x_n$ qui satisfont aux inégalités

$$(9) \qquad \frac{1}{2} P < \frac{x_j}{\xi_j} < 2P \qquad (j = 1, \dots, n) \quad ,$$

quand $P \to \infty$. Comme mesure de grandeur, P prend la place de $N^{\frac{1}{d}}$. On obtient une formule asymptotique pour le nombre de solutions qui a la même structure que celle qu'on trouve pour le problème de Waring. Cette formule est valable, et montre que le nombre de solutions tend vers l'infini avec P, pourvu que $n \geq n_1(d)$. Au cours de la démonstration, il faut montrer que l'équation est résoluble dans chaque corps p-adique, mais cela ne présente pas de grande difficulté.

La méthode de Hardy et Littlewood nous donne par conséquent une certaine classe d'équations du type (1), dont nous pouvons affirmer la résolubilité, pourvu que $n \geq n_1(d)$ et pourvu, bien entendu, que l'équation soit possible dans le corps réel. La dernière condition existe seulement si d est pair, et dans ce cas elle revient à la condition évidente sur les signes des coefficients.

Si $d > 2$, l'équation générale (1) ne se laisse pas transformer linéairement en une équation du type spécial (type diagonal) dont nous venons de parler. Cela est évident, parce que l'équation générale contient plus que $\frac{n^d}{d!}$ coefficients arbitraires, tandis que la transformation linéaire ne contient que n^2 coefficients. Ainsi, la propriété de résolubilité des équations diagonales ne s'étend pas de manière directe aux équations générales.

Considérons, en premier lieu, le cas $d = 3$. On a cru, pendant longtemps, qu'il existait une constante absolue n_0 telle que l'équation cubique générale soit toujours résoluble si $n \geq n_0$. Cette conjecture a été démontrée en 1957 par D. J. LEWIS [4], B. J. BIRCH [1] et moi-même [3], tous trois indépendamment l'un de l'autre. Chaque démonstration utilise, directement ou indirectement, la méthode de Hardy et Littlewood.

Les démonstrations de LEWIS et de BIRCH se basent sur le travail de Richard BRAUER en 1945 [2]. BRAUER démontra le théorème suivant. Soit K un corps avec la propriété suivante : pour tout entier positif r il existe $n_0(r)$ tel que toute

équation

$$(10) \qquad a_1 x_1^r + \ldots + a_n x_n^r = 0 \quad ,$$

à coefficients dans K , possède une solution non banale dans K , pourvu que $n \geq n_0(r)$. Alors, un résultat analogue est valable pour les équations homogènes générales, sous la condition $n \geq n_1(r)$, où $n_1(r)$ est naturellement beaucoup plus grand que $n_0(r)$. Et, de plus, un résultat analogue est valable pour les systèmes d'équations homogènes simultanées, sous la condition $n \geq n_1(r_1 , \ldots , r_m)$, où $r_1, \ldots , r_m$ désignent les degrés des équations. La démonstration s'obtient par récurrence sur le degré maximum, et quoiqu'elle soit élémentaire, elle est très subtile.

Le théorème de Brauer ne s'applique pas si K est le corps rationnel, car dans ce corps l'équation (10) n'est pas nécessairement résoluble si r est pair. L'oeuvre de LEWIS se base sur le fait que le théorème de Brauer s'applique au corps des nombres complexes rationnels (corps de Gauss). La résolubilité des équations (10) dans ce corps a été démontrée, comme pour le corps rationnel, par la méthode de Hardy et Littlewood [6], et il n'y a aucune condition analogue à la condition sur les signes des coefficients. Il en résulte, pourvu que $n \geq n_0$, qu'il existe des nombres rationnels complexes $z_1 , \ldots , z_n$, non tous nuls, qui satisfont à

$$f(z_1 , \ldots , z_n) = 0 \quad ,$$

f désignant maintenant une forme cubique générale à coefficients entiers. Si $z_1 , \ldots , z_n$ sont, en effet, rationnels, il n'y a rien à démontrer. Sinon, les conjugués complexes $\bar{z}_1 , \ldots , \bar{z}_n$ satisfont à la même équation. Or, la ligne droite passant par les points $(z_1 , \ldots , z_n)$ et $(\bar{z}_1 , \ldots , \bar{z}_n)$ dans l'espace à n dimensions rencontre le cône cubique $f(x_1 , \ldots , x_n) = 0$ dans un troisième point. Ce point est rationnel et nous donne la solution cherchée.

Le travail de BIRCH se base aussi sur la méthode de Brauer, mais avec une variante importante. BIRCH démontre que la méthode de Brauer fonctionne toujours, si on se borne dans l'hypothèse et dans la conclusion, aux équations de degré impair. Le théorème qui résulte est est ainsi valable dans le corps rationnel, et implique que tout système d'équations simultanées de degrés impairs :

$$f_{d_1}(x_1 , \ldots , x_n) = 0 , \ldots , f_{d_m}(x_1 , \ldots , x_n) = 0$$

possède une solution rationnelle (ou entière) non nulle, pourvu que

$n \geqslant n_2(d_1 , \ldots , d_m)$.

Je vais donner une illustration des recherches de BIRCH en démontrant la résolubilité de l'équation cubique générale. Cette démonstration est d'une simplicité remarquable ; elle exige seulement la résolution d'équations linéaires, en plus, bien entendu, de la résolubilité d'une équation diagonale

$$a_1 x_1^3 + \ldots + a_k x_k^3 = 0 \quad ,$$

démontrée par la méthode de Hardy et Littlewood. Pour cette dernière équation, on peut prendre $k = 8$.

On dit qu'une forme (c'est-à-dire un polynôme homogène) $f(x_1 , \ldots , x_n)$ <u>représente</u> une autre forme $g(y_1 , \ldots , y_\ell)$, où $\ell \leqslant n$, s'il existe ℓ formes linéaires indépendantes :

$$(11) \qquad y_i = b_{i1} x_1 + \ldots + b_{in} x_n \qquad (i = 1 , \ldots , \ell) \quad ,$$

qui transforment f en g . Nous supposons les coefficients b_{ij} rationnels. Notre but sera de démontrer que toute forme cubique f représente une forme cubique g du type

$$(12) \qquad g(y_1 , \ldots , y_\ell) = c_1 y_1^3 + g'(y_2 , \ldots , y_\ell) \quad ,$$

où ℓ est une fonction de n seulement, qu'on peut rendre grande en prenant n suffisamment grand. Cette démonstration faite, le résultat voulu en résulte ; car si l'on répète le raisonnement sur g' , et qu'on le répète encore 7 fois en tout, on trouve que f représente une forme du type

$$g^* = a_1 z_1^3 + \ldots + a_8 z_8^3 \quad .$$

Une solution non banale de l'équation $g^* = 0$ donne une solution non banale de l'équation $f = 0$.

Écrivons la forme cubique donnée sous la forme :

$$f = \sum_i \sum_j \sum_k c_{ijk} x_i x_j x_k \quad .$$

Soit $\mathfrak{p} = (p_1 , \ldots , p_n)$ le point dans l'espace des variables x qui se transformera en le point $(1 , 0 , \ldots , 0)$ des variables y . Quelles sont les conditions sous lesquelles la nouvelle forme g est du type (12) ? On peut les formuler comme suit : il doit exister un espace linéaire à $\ell - 1$ dimensions

dans l'espace des variables $\mathfrak{x}$, qui ne contient pas $\mathfrak{p}$, tel que

(1) $\sum\sum\sum c_{ijk}\, p_i\, p_j\, x_k = 0$ pour tout point $\mathfrak{x}$ de l'espace,

(2) $\sum\sum\sum c_{ijk}\, p_i\, x_j\, x'_k = 0$ pour tout couple de points $\mathfrak{x}$, $\mathfrak{x}'$ de l'espace.

Car, si l'on transforme l'espace à $\ell - 1$ dimensions dans l'espace $y_1 = 0$ des variables $\mathfrak{y}$, la condition (1) exprime le fait que les termes $y_1^2 y_2$, ... , $y_1^2 y_\ell$ dans g ont des coefficients nuls, et la condition (2) exprime le fait que les termes $y_1 y_2^2$, $y_1 y_2 y_3$, ... dans g ont des coefficients nuls.

Nous choisissons un point $\mathfrak{p}$ de la forme

$$\mathfrak{p} = (0 , \dots , 0 , p_{\ell+1} , \dots , p_n) \quad ,$$

de telle façon que

$$\sum_i c_{ijk}\, p_i = 0 \quad \text{pour} \quad j = 1 , \dots , \ell \quad \text{et} \quad k = 1 , \dots , \ell \quad .$$

Il y a ici $\frac{1}{2}\ell(\ell+1)$ conditions linéaires, et le choix de $\mathfrak{p}$ est possible pourvu que

$$n - \ell > \tfrac{1}{2}\ell(\ell+1) \quad .$$

Les conditions (2) sont maintenant remplies pour tout point $\mathfrak{x}$ dans l'espace à ℓ dimensions défini par

$$x_{\ell+1} = \dots = x_n = 0 \quad .$$

La condition (1) définit un sous-espace à $\ell - 1$ dimensions de cet espace à ℓ dimensions. Les conditions (1) et (2) sont toutes les deux remplies, et notre but est atteint.

Je voudrais maintenant esquisser ma propre démonstration de la résolubilité des équations cubiques. Cette démonstration n'est pas aussi générale que celle de Birch, mais elle donne la condition $n \geqslant 32$, tandis que la méthode de Birch exige que n soit très grand. Il est probable que la condition véritable soit $n \geqslant 10$; il existe des contre-exemples avec $n = 9$ [5].

Dans cette démonstration, j'ai essayé d'appliquer directement la méthode de Hardy et Littlewood. Dans ce but, il faut étudier la somme exponentielle

$$S(\alpha) = \sum_{x_1} \dots \sum_{x_n} e^{2\pi i \alpha f(x_1,\dots,x_n)} \quad ,$$

où la sommation s'étend sur les points entiers $(x_1, \ldots, x_n)$ d'un grand pavé (c'est-à-dire produit cartésien d'intervalles). Le pavé est choisi comme auparavant ; il est défini au moyen d'une solution réelle $\xi_1, \ldots, \xi_n$ de l'équation $f = 0$, et d'un nombre P qui augmente indéfiniment. L'étude des sommes exponentielles multiples présente des difficultés sérieuses, à moins que la somme ne puisse s'exprimer comme produit de sommes à une variable.

Le nombre de points entiers dans le grand pavé, qui satisfont à $f = 0$, s'exprime par

$$\int_0^1 S(\alpha)\, d\alpha \quad .$$

On décompose l'intervalle d'intégration en deux parties : les major arcs et les minor arcs. Les major arcs fournissent la contribution principale (au moins, on l'espère), contribution qui est de l'ordre de grandeur P^{n-3}. Ce sont les minor arcs qui présentent la vraie difficulté. On cherche naturellement un analogue de l'inégalité de Weyl. On découvre que, si la somme est d'un ordre de grandeur qui approche P^n (disons : $> P^{n-3}$), la forme cubique f possède nécessairement des propriétés tout à fait remarquables, mais une démonstration du fait que ces propriétés sont en contradiction m'échappe jusqu'ici. Cependant, j'ai pu démontrer que si la somme est grande, pour un nombre α qui appartient aux minor arcs, la forme cubique f représente une forme du type

$$c_1 y_1^3 + g'(y_2, \ldots, y_\ell) \quad .$$

On arrive ainsi à une situation pareille à celle qui se présente dans le travail de BIRCH, sauf que, dans le raisonnement actuel, ℓ est presque aussi grand que n. Si $|S(\alpha)| > P^{n-3}$, on trouve que $\ell = n - 7$.

Comme dans la propre méthode de Hardy et Littlewood, on obtient une formule asymptotique pour le nombre de solutions quand $P \to \infty$, et cette formule est une généralisation de celle pour une forme cubique diagonale. Cependant, elle dépend maintenant de l'hypothèse que la forme f ne représente aucune forme g, comme indiqué ci-dessus.

Si la forme f représente une forme du type g, il faut étudier cette forme à ℓ variables de nouveau. Le problème prend maintenant un caractère en partie additif. Il faut répéter ces études en tout 7 fois, jusqu'à ce que la forme qui reste soit enfin diagonale.

De cette façon on arrive à une formule asymptotique pour le nombre de solutions,

valable sous la condition qu'il n'y ait point de solutions - conclusion à première vue paradoxale, qui souligne le fait que la démonstration s'achève par la "reductio ad absurdum".

Les équations de degré pair (> 2) présentent de grandes difficultés. Il est certain qu'il ne suffit pas que n soit grand et que l'équation soit résoluble dans le corps réel. Par exemple, l'équation

$$(x_1^2 + \ldots + x_r^2)^2 + (x_{r+1}^2 + \ldots + x_s^2)^2 - 3(x_{s+1}^2 + \ldots + x_n^2)^2 = 0$$

ne possède pas de solution non banale. On pourrait peut-être attribuer cette non-résolubilité au fait que l'équation ne possède pas de solution non singulière dans le corps p-adique quand $p = 3$. Mais SWINNERTON-DYER a donné un exemple plus compliqué, auquel cette objection ne s'applique pas. C'est l'équation

$$3(x_1^2 + \ldots + x_r^2)^3 + 4(x_{r+1}^2 + \ldots + x_s^2)^3 - 5(x_{s+1}^2 + \ldots + x_n^2)^3 = 0 \quad .$$

SELMER [7] a démontré que l'équation $3X^3 + 4Y^3 - 5Z^3 = 0$ est impossible dans le corps rationnel.

Il semble que les conditions de résolubilité pour les équations de degré pair doivent tenir compte de la possibilité d'exprimer f comme polynôme de degré n_1 en d'autres polynômes de degré n_2, où $n = n_1 n_2$. Mais on attend toujours la formulation définitive de telles conditions.

BIBLIOGRAPHIE

[1] BIRCH (B. J.). - Homogeneous forms of odd degree in a large number of variables, Mathematika, t. 4, 1957, p. 102-105.

[2] BRAUER (Richard). - A note on systems of homogeneous algebraic equations, Bull. Amer. math. Soc., t. 51, 1945, p. 749-755.

[3] DAVENPORT (Harold). - Cubic forms in 32 variables, Phil. Trans. royal Soc., Series A, t. 251, 1959, p. 193-232.

[4] LEWIS (D. J.). - Cubic forms over algebraic number fields, Mathematika, t. 4, 1957, p. 97-101.

[5] MORDELL (L. J.). - A remark on indeterminate equations in several variables, J. London math. Soc., t. 12, 1937, p. 127-129.

[6] PECK (L. G.). - Diophantine equations in algebraic number fields, Amer. J. of Math., t. 71, 1949, p. 387-402.

[7] SELMER (J. S.). - The Diophantine equation $ax^3 + by^3 + cz^3 = 0$, Acta Math., t. 85, 1951, p.203-362.