Table des matières

Chapitre 1

Philippe Michel. Sommes de carrés

Si f et g sont deux fonctions sur $\mathbb{R}$ à valeurs réelles alors le symbole $f(x) \ll_A g(x)$ signifie que $|f(x)|$ est inférieur à une constante, qui ne dépend que de A, multiplié par $g(x)$ au moins pour $|x|$ assez grand.

1.1 Sommes de quatre carrés

1.1.1 Le théorème des quatre carrés de J.L. Lagrange

Un entier naturel n est somme de quatre carrés d'entiers s'il existe un quadruplet (a, b, c, d) d'entiers relatifs vérifiant

$$n = a^2 + b^2 + c^2 + d^2. \tag{1.1}$$

Par exemple, 39 est somme de quatre carrés d'entiers puisque $39 = 2^2 + (-5)^2 + 1^2 + 3^2$.

Un quadruplet (a, b, c, d) vérifiant (1.1) est une représentation de n en somme de quatre carrés d'entiers. Soit q_4 la forme quadratique définie positive sur $\mathbb{Q}^4$, un $\mathbb{Q}$-espace vectoriel de dimension finie égale à quatre, définie par

$$\forall (a, b, c, d) \in \mathbb{Q}^4, \quad q_4(a, b, c, d) = a^2 + b^2 + c^2 + d^2.$$

Un quadruplet (a, b, c, d) vérifiant (1.1) est une représentation entière de n par la forme quadratique q_4.

Notons $R_4(n)$ l'ensemble de ces représentations entières c'est-à-dire

$$R_4(n) = \big\{(a, b, c, d) \in \mathbb{Z}^4, q_4(a, b, c, d) = n\big\}$$

et

$$r_4(n) = \mathrm{card}(R_4(n))$$

le cardinal de cet ensemble fini. J.L. Lagrange a prouvé le résultat suivant au 18ième siècle.

Théorème 1.1.1 (Théorème de J.L. Lagrange (1770) : énoncé 1)**.** *Tout entier naturel est somme de quatre carrés d'entiers. En d'autres termes,*

$$\forall n \in \mathbb{N}, \quad R_4(n) \neq \varnothing$$

ou bien, de façon équivalente,

$$\forall n \in \mathbb{N}, \quad r_4(n) \geqslant 1.$$

Une preuve classique et élégante de ce résultat attribuée à B.A. Venkov ([22], [23]) repose sur l'usage de l'algèbre des quaternions de Hamilton [(1)] $B(\mathbb{Q})$. Nous avons déja fait la connaissance d'une $\mathbb{Q}$-algèbre commutative de dimension finie égale à quatre depuis le début de l'exposé à savoir $(\mathbb{Q}^4, +, \times, .)$. L'algèbre des quaternions de Hamilton $(B(\mathbb{Q}), +, \times, .)$ est une $\mathbb{Q}$-algèbre non-commutative de dimension finie égale à quatre construite de la façon suivante. C'est le $\mathbb{Q}$-espace vectoriel de dimension finie égale à quatre engendré par $(1, i, j, k)$ muni des règles de multiplication

$$i^2 = j^2 = k^2 = -1, \quad i \times j = -j \times i = k.$$

Bien entendu, 0 est le neutre du $\mathbb{Q}$-espace vectoriel $(B(\mathbb{Q}), +, .)$ et 1 est l'élément unité de l'anneau $(B(\mathbb{Q}), +, \times)$.

Les symboles . et $\times$ désignant la multiplication externe et la multiplication sont généralement omis. Ainsi, $(3/2 + 4i - 5j)(j + k)$ signifie $(3/2.1 + 4.i - 5.j) \times (j + k)$. Donnons un exemple de calcul dans cette algèbre.

$$\begin{aligned}(j+k)(2i-1) &= 2ji - j + 2ki - k \\ &= -2k - j + 2j - k \\ &= j - 3k\end{aligned}$$

alors que

$$\begin{aligned}(2i-1)(j+k) &= 2ij + 2ik - j - k \\ &= 2k - 2j - j - k \\ &= -3j + k\end{aligned}$$

ce qui prouve la non-commutativité de cette algèbre.

Le centre noté $Z(B(\mathbb{Q}))$ de cette algèbre, c'est-à-dire les éléments de cette algèbre qui commutent avec tous les autres, est exactement

$$Z(B(\mathbb{Q})) = \{z_1 \in B(\mathbb{Q}), \forall z_2 \in B(\mathbb{Q}), z_1 z_2 = z_2 z_1\} = \mathbb{Q} + \mathbb{Q}i.$$

Cette algèbre est munie de l'involution

$$\begin{array}{rccc} \text{conj} : & B(\mathbb{Q}) & \to & B(\mathbb{Q}) \\ & z = a + bi + cj + dk & \mapsto & \text{conj}(z) = \overline{z} = a - bi - cj - dk. \end{array}$$

Il est facile de vérifier que $\text{conj}^{-1} = \text{conj}$ et que $\overline{z_1 z_2} = \overline{z_2 z_1}$ pour tous éléments z_1 et z_2 de cette algèbre.

Le groupe multiplicatif des éléments inversibles de l'anneau $(B(\mathbb{Q}), +, \times)$ noté $B(\mathbb{Q})^\times$ est exactement l'ensemble des éléments non-nuls de $B(\mathbb{Q})$: on dit que l'anneau $(B(\mathbb{Q}), +, \times)$ est un corps.

Cette algèbre est également munie de deux applications intéressantes : la trace réduite et la norme réduite. La trace réduite est l'application $\mathbb{Q}$-linéaire définie par

$$\begin{array}{rccc} \text{tr} : & B(\mathbb{Q}) & \to & \mathbb{Q} \\ & z = a + bi + cj + dk & \mapsto & \text{tr}(z) = z + \overline{z} = 2a \end{array}$$

(1). Nous renvoyons le lecteur vers [19, Section 5.7] pour non seulement davantage d'informations concernant les quaternions mais aussi les démonstrations de certaines de leurs propriétés nécessaires dans ce texte.

alors que la norme réduite est la forme quadratique définie positive définie par

$$\begin{array}{rccc} \mathrm{Nr}: & B(\mathbb{Q}) & \to & \mathbb{Q} \\ & z = a + bi + cj + dk & \mapsto & \mathrm{Nr}(z) = z\overline{z} = a^2 + b^2 + c^2 + d^2. \end{array}$$

Les espaces euclidiens $(\mathbb{Q}^4, q_4)$ et $(B(\mathbb{Q}), \mathrm{Nr})$ sont isométriques. En effet, l'application

$$\begin{array}{ccc} (\mathbb{Q}^4, q_4) & \to & (B(\mathbb{Q}), \mathrm{Nr}) \\ (a, b, c, d) & \mapsto & z = a + bi + cj + dk \end{array}$$

est une isométrie. Ceci permet de donner un énoncé équivalent du théorème de Lagrange.

Théorème 1.1.2 (Théorème de J.L. Lagrange (1770) : énoncé 2)**.** *Pour tout entier naturel n, il existe z dans $B(\mathbb{Z})$ tel que $Nr(z) = n$.*

La fin de cette section contient une esquisse de preuve de cet énoncé du théorème de Lagrange. Soit n un entier naturel. Nous pouvons supposer que $n \geqslant 1$ car $0 = \mathrm{Nr}(0)$. La multiplicativité de la norme réduite implique que nous pouvons supposer que n est un nombre premier p. Le cas $p = 2$ est facile car $2 = \mathrm{Nr}(1 + i)$. Nous pouvons donc supposer que p est un nombre premier impair.

Introduisons le sous-ensemble

$$B(\mathbb{Z}) = \left\{ z = a + bi + cj + dk, (a, b, c, d) \in \mathbb{Z}^4 \right\}$$

de l'algèbre des quaternions de Hamilton. $B(\mathbb{Z})$ est à la fois un anneau (non commutatif) et un $\mathbb{Z}$-module libre de rang 4 : on dit que c'est un ordre de $B(\mathbb{Q})$.

Un autre ordre important de $B(\mathbb{Q})$ est l'ordre des quaternions de Hurwitz défini par

$$\mathcal{O}_B = B(\mathbb{Z}) + \mathbb{Z}\frac{1 + i + j + k}{2}$$

qui contient strictement $B(\mathbb{Z})$ et dont l'ensemble des éléments inversibles est

$$\mathcal{O}_B^\times = \left\{ \pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}$$

c'est-à-dire exactement l'ensemble des éléments de $\mathcal{O}_B$ de norme réduite égale à 1.

Une propriété cruciale de cet ordre est sa principalité [(2)] ce qui signifie que si $I \subset B(\mathbb{Q})$ est un $\mathcal{O}_B$-module à gauche de type fini (c'est-à-dire un $\mathbb{Z}$-module satisfaisant $\mathcal{O}_B I \subset I$) alors il existe q dans $B(\mathbb{Q})^\times$ tel que $I = \mathcal{O}_B q$ (confer [19, Lemme 3 Page 98]).

Choisissons des entiers relatifs a, b et c tels que p divise à la fois $a^2 + b^2 + c^2$ et $a - 1$. Un tel choix est possible selon [19, Remarque Page 100]. Posons

$$w = ai + bj + ck \in \mathcal{O}_B, \quad I = \mathcal{O}_B w + \mathcal{O}_B p.$$

I est un $\mathcal{O}_B$ module à gauche de $B(\mathbb{Q})$ contenant strictement $\mathcal{O}_B p$ (car w n'appartient pas à $\mathcal{O}_B p$) et strictement inclus dans $\mathcal{O}_B$ (car tous les éléments de I ont leur norme réduite divisible par p). La principalité de $\mathcal{O}_B$ assure l'existence de z dans $\mathcal{O}_B$ (nécessairement pas inversible) tel que $I = \mathcal{O}_B z$.

(2). En fait, $\mathcal{O}_B$ est Euclidien par rapport à la norme réduite.

Etant donné que p appartient à I, il existe z' (nécessairement pas inversible) dans $\mathcal{O}_B$ tel que $p = zz'$. En particulier,

$$p^2 = \mathrm{Nr}(p) = \mathrm{Nr}(z)\mathrm{Nr}(z')$$

d'où

$$\mathrm{Nr}(z) = p$$

car à la fois z et z' ne sont pas de norme 1.

La preuve est essentiellement terminée, hormis le fait que z appartient à $\mathcal{O}_B$ et pas forcément à $B(\mathbb{Z})$. Un calcul direct assure qu'il est possible de multiplier z par une unité de $\mathcal{O}_B$ (donc de norme 1) afin de le ramener dans $B(\mathbb{Z})$.

1.1.2 Formule de Jacobi

Nous avons vu dans la section précédente que tout entier naturel admet une représentation entière par la forme quadratique q_4. Il est alors naturel de se demander quel est le nombre de représentations entières d'un entier naturel par q_4. La réponse à cette question est donnée par la formule de Jacobi.

Théorème 1.1.3 (Formule de Jacobi (1828))**.** *Si n est un entier naturel non-nul alors*

$$r_4(n) = 8\sum_{\substack{d|n\\ 4\nmid n}} d = 8(1+2\delta_{2|n}) \prod_{\substack{p \text{ premier}\\ p^\alpha || n\\ p\neq 2}} \frac{p^{\alpha+1}-1}{p-1}.$$

Nous renvoyons le lecteur vers [8, Chapitre 11] pour une démonstration de cette formule.

Deux remarques s'imposent. Quelle est l'origine de 8 dans cette formule ? Il est facile de vérifier que

$$B(\mathbb{Z})^{(1)} = \{z \in B(\mathbb{Z}), \mathrm{Nr}(z) = 1\} = \{\pm 1, \pm i, \pm j, \pm k\}$$

est un groupe multiplicatif abélien de cardinal 8. Quelle est l'origine de ce produit Eulerien ? L'ensemble

$$B(\mathbb{Z})^{(n)} = \{z \in B(\mathbb{Z}), \mathrm{Nr}(z) = n\}$$

admet une action du groupe $B(\mathbb{Z})^{(1)}$ par multiplication à gauche. Il se trouve que l'ensemble quotient est un ensemble fini de cardinal

$$\mathrm{card}\left(B(\mathbb{Z})^{(1)} \setminus B(\mathbb{Z})^{(n)}\right) = (1+2\delta_{2|n}) \prod_{\substack{p \text{ premier}\\ p^\alpha || n\\ p\neq 2}} \frac{p^{\alpha+1}-1}{p-1}.$$

1.1.3 Equirépartition selon A.V. Malyshev et H.D. Kloosterman

La formule de Jacobi assure que

$$\frac{1}{\sqrt{n}} R_4(n) = \left\{ \left(\frac{a}{\sqrt{n}}, \frac{b}{\sqrt{n}}, \frac{c}{\sqrt{n}}, \frac{d}{\sqrt{n}}, \right), (a,b,c,d) \in \mathbb{Z}^4, q_4(a,b,c,d) = n \right\}$$

est un sous-ensemble de la sphère unité $\mathbb{S}^3$ de $\mathbb{R}^4$ constitué d'au moins n éléments. Il est alors naturel d'étudier la distribution de cet ensemble sur $\mathbb{S}^3$. La réponse à cette question a été donnée indépendamment par A.V. Malyshev ([13]) et H.D. Kloosterman ([11]).

Théorème 1.1.4 (A.V. Malyshev, H.D. Kloostermann). $\left(\frac{1}{\sqrt{n}}R_4(n)\right)_{n\geqslant 0}$ *s'équirépartit sur* $\mathbb{S}^3$ *par rapport à la mesure de Lebesque normalisée sur* $\mathbb{S}^3$ *notée* $\lambda_{\mathbb{S}^3}$ *lorsque* n *tend vers l'infini parmi les entiers naturels. En d'autres termes, si* $f:\mathbb{S}^3\to\mathbb{C}$ *est une fonction continue alors*

$$\frac{1}{r_4(n)}\sum_{\mathbf{x}\in R_4(n)} f\left(\frac{\mathbf{x}}{\sqrt{n}}\right)\to_{n\to+\infty}\int_{\mathbf{x}\in\mathbb{S}^3} f(\mathbf{x})\mathrm{d}\lambda_{\mathbb{S}^3}(\mathbf{x}).$$

Comment visualiser cette équirépartition dans un espace ambiant de dimension quatre ? La fibration de Hopf permet de résoudre ce problème. Soit $B^0(\mathbb{Q})$ le $\mathbb{Q}$-espace vectoriel de dimension 3 constitué des quaternions de trace nulle c'est-à-dire

$$B^0(\mathbb{Q})=\{z\in B(\mathbb{Q}),\mathrm{Tr}(z)=0\}.$$

L'espace quadratique $(B^0(\mathbb{Q}),\mathrm{Nr})$ est isométrique à l'espace quadratique $(\mathbb{Q}^3,q_3)$ où q_3 est la forme quadratique définie positive sur $\mathbb{Q}$ définie par

$$\forall(a,b,c)\in\mathbb{Q}^3,\quad q_3(a,b,c)=a^2+b^2+c^2.$$

Le groupe multiplicatif $B(\mathbb{Q})^\times$ agit sur $B^0(\mathbb{Q})$ par conjugaison. En d'autres termes,

$$\forall g\in B(\mathbb{Q})^\times,\forall z\in B^0(\mathbb{Q}),\quad g.z=gzg^{-1}.$$

Ainsi, tout élément g de $B(\mathbb{Q})^\times$ induit une bijection notée ρ_g de $B^0(\mathbb{Q})$ dans lui-même par la formule $\rho_g(z)=g.z$ pour tout z dans $B^0(\mathbb{Q})$. Ces bijections ρ_g sont des transformations spéciales orthogonales de l'espace quadratique $(B^0(\mathbb{Q}),\mathrm{Nr})$ c'est-à-dire des éléments du groupe $(SO(B^0(\mathbb{Q}),\mathrm{Nr}))$, lui-même isomorphe à $S0_3(\mathbb{Q})$.

Nous en déduisons la suite exacte

$$1\to\mathbb{Q}^\times\to B(\mathbb{Q})^\times\to\left(SO(B^0(\mathbb{Q})),\mathrm{Nr}\right)\simeq SO_3(\mathbb{Q})\to 1.$$

De façon analogue,

$$1\to\{\pm 1\}\to B(\mathbb{R})^{(1)}\to\left(SO(B^0(\mathbb{R})^{(1)}),\mathrm{Nr}\right)\simeq SO_3(\mathbb{R})\to 1$$

où

$$\begin{array}{rcl} B(\mathbb{R})^{(1)} & = & \{z=a+bi+cj+dk,\mathrm{Nr}(z)=1\}\simeq\mathbb{S}^3\subset\mathbb{R}^4,\\ B^0(\mathbb{R})^{(1)} & = & \{z=a+bi+cj+dk,\mathrm{Nr}(z)=1,\mathrm{tr}(z)=0\}.\end{array}$$

Le théorème de Witt ([21, Théorème 3 Page 58]) assure que $SO_3(\mathbb{R})$ agit transitivement sur $\mathbb{S}^2$. Soit x_0 dans $\mathbb{S}^2$. Nous disposons d'une application

$$\begin{array}{rcl} SO_3(\mathbb{R}) & \to & \mathbb{S}^2\\ A & \mapsto & Ax_0\end{array}$$

dont la suite exacte suivante découle

$$B(\mathbb{R})^{(1)}\simeq\mathbb{S}^3\to\left(SO(B(\mathbb{R})^{(1)}),\mathrm{Nr}\right)\simeq SO_3(\mathbb{R})\to\mathbb{S}^2\to 1$$

où toutes les flèches sont surjectives. Cette suite exacte est appelée fibration de Hopf.

Une fibre au-dessus d'un point est isomorphe à un $\mathbb{S}^1$ pour la raison suivante. Soient z et z' dans $B(\mathbb{R})^{(1)}$. On a $\rho_z(w)=\rho_{z'}(w)$ si et seulement si $w(z^{-1}z')=(z^{-1}z')w$ si et seulement si $z^{-1}z'=a+bw$ avec $a^2+b^2=1$.

Ainsi, ρ dans $R_4(n)$ induit un $\overline{\rho}$ dans $SO_3(\mathbb{R})$. L'énoncé suivant est un corollaire du théorème précédent.

Corollaire 1.1.1. *Soit x_0 dans $\mathbb{S}^2$. L'ensemble*

$$\{\overline{\rho}.x_0, \rho \in R_4(n)\}$$

s'équirépartit sur $\mathbb{S}^2$ par rapport à la mesure de Lebesgue normalisée sur $\mathbb{S}^2$ lorsque n tend vers l'infini parmi les entiers naturels.

L'équirépartition précédente a lieu dans un espace ambient de dimension réelle deux.

La fin de cette section contient une esquisse de preuve du théorème d'équirépartition de A.V. Malyshev et de H.D. Kloostermann, fidèle à la présentation donnée dans [8, Chapitre 11].

Selon [5], l'espace topologique des fonctions continues sur $\mathbb{S}^3$ est engendré par les polynômes harmoniques homogènes c'est-à-dire par les polynômes homogènes P sur $\mathbb{R}^4$

$$\exists s \in \mathbb{R}, \forall \lambda \in \mathbb{R}, \forall \mathbf{x} \in \mathbb{R}^4, \quad P(\lambda \mathbf{x}) = \lambda^s P(\mathbf{x})$$

annulés par le Laplacien Euclidien de $\mathbb{R}^4$

$$\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2} + \frac{\partial^2}{\partial t^2}\right)(P) = 0.$$

Il suffit donc de prouver le théorème d'équirépartition pour f un tel polynôme homogène P. Si P est un polynôme homogène de degré 0 donc constant de valeur c alors

$$\frac{1}{r_4(n)} \sum_{\mathbf{x} \in R_4(n)} P\left(\frac{\mathbf{x}}{\sqrt{n}}\right) = c = \int_{\mathbf{x} \in \mathbb{S}^3} P(\mathbf{x}) \mathrm{d}\lambda_{\mathbb{S}^3}(\mathbf{x}).$$

Nous pouvons donc supposer que P est de degré $s \geqslant 1$. Il s'agit alors de prouver que

$$\frac{1}{r_4(n)} \sum_{\mathbf{x} \in R_4(n)} P\left(\frac{\mathbf{x}}{\sqrt{n}}\right) \to_{n \to +\infty} \int_{\mathbf{x} \in \mathbb{S}^3} P(\mathbf{x}) \mathrm{d}\lambda_{\mathbb{S}^3}(\mathbf{x}) = \langle P, \mathbf{1} \rangle = 0$$

car P est orthogonal pour le produit scalaire standard à $\mathbf{1}$, le polynôme homogène de degré 0 de valeur constante égale à 1. Soit $\varepsilon > 0$ arbitrairement petit. Nous avons

$$\begin{aligned} \frac{1}{r_4(n)} \sum_{\mathbf{x} \in R_4(n)} P\left(\frac{\mathbf{x}}{\sqrt{n}}\right) &= \frac{1}{r_4(n) n^{s/2}} \sum_{\mathbf{x} \in R_4(n)} P(\mathbf{x}) \\ &\ll_\varepsilon \frac{1}{n^{1+s/2-\varepsilon}} \sum_{\mathbf{x} \in R_4(n)} P(\mathbf{x}). \end{aligned}$$

Il s'agit donc de prouver qu'il existe une constante $\delta > 0$ telle que

$$\sum_{\mathbf{x} \in R_4(n)} P(\mathbf{x}) \ll n^{1+s/2-\delta}.$$

C'est ici qu'interviennent les formes modulaires. Soient

$$\mathbb{H} = \{z = x + iy \in \mathbb{C}, y > 0\}$$

le demi-plan supérieur et

$$\Gamma_0(4) = \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}), ad - bc = 1, 4 \mid c\right\}$$

le groupe de congruence de niveau 4. Ce groupe agit sur $\mathbb{H}$ par homographies selon la formule

$$\forall z \in \mathbb{H}, \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4), \quad \gamma.z = \frac{az+b}{cz+d}.$$

Définissons une fonction sur $\mathbb{H}$ par

$$\theta_P(z) = \sum_{n \geqslant 0} \left(\sum_{\mathbf{x} \in R_4(n)} P(\mathbf{x}) \right) \exp(2i\pi n z).$$

Les coefficients de Fourier de cette fonction sont précisément les quantités à estimer afin de terminer la preuve.

Proposition 1.1.1. *La fonction θ_P est une forme modulaire de poids $s+2$ et de niveau 4.*

Cela signifie que θ_P satisfait les symmétries données par

$$\forall z \in \mathbb{H}, \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4), \quad \theta_P(\gamma.z) = (cz+d)^{s+2}\theta_P(z).$$

Le lecteur trouvera une preuve de cette proposition dans [8, Théorème 10.8].

Il est facile de démontrer que

$$\sum_{\mathbf{x} \in R_4(n)} P(\mathbf{x}) \ll n^{(s+2)/2}.$$

Il est fascinant d'observer que cette borne, dite borne triviale, est presque suffisante pour terminer la preuve. Toute amélioration même microscopique de celle-ci implique le résultat d'équidistribution. La première amélioration est dûe à H.D. Kloosterman ([11]), qui a prouvé que

$$\sum_{\mathbf{x} \in R_4(n)} P(\mathbf{x}) \ll n^{(s+2)/2-1/6}.$$

Ce résultat est une conséquence d'estimations non-triviales de certaines sommes exponentielles : les sommes de Kloosterman.

1.2 Sommes de trois carrés

1.2.1 Le théorème des trois carrés de C.F. Gauß et de A.-M. Legendre

Un entier naturel d est somme de trois carrés d'entiers s'il existe un triplet (a,b,c) d'entiers relatifs vérifiant

$$d = a^2 + b^2 + c^2. \tag{1.2}$$

Par exemple, 30 est somme de trois carrés d'entiers puisque $30 = 2^2 + (-5)^2 + 1^2$. Un triplet (a,b,c) vérifiant (1.2) est une représentation de d en somme de trois carrés d'entiers. Soit q_3 la forme quadratique définie positive sur $\mathbb{Q}^3$, un $\mathbb{Q}$-espace vectoriel de dimension finie égale à trois, définie par

$$\forall (a,b,c) \in \mathbb{Q}^3, \quad q_3(a,b,c) = a^2 + b^2 + c^2.$$

Un triplet (a,b,c) vérifiant (1.2) est une représentation entière de d par la forme quadratique q_3. Notons $R_3(d)$ l'ensemble de ces représentations entières c'est-à-dire

$$R_3(d) = \big\{(a,b,c) \in \mathbb{Z}^3, q_3(a,b,c) = d\big\}$$

et

$$r_3(d) = \mathrm{card}(R_3(d))$$

le cardinal de cet ensemble fini. A.-M. Lengendre et C.F. Gauß ont prouvé le résultat suivant en 1801.

Théorème 1.2.1 (Théorème des trois carrés (1801) : énoncé 1)**.** *Un entier naturel non-nul d est somme de trois carrés d'entiers si et seulement si d n'est pas du type $4^k(8\ell+7)$ où k et ℓ sont des entiers naturels.*

Il existe donc des obstructions locales empêchant à un entier naturel non-nul quelconque d'être une somme de trois carrés d'entiers. Par exemple, 7 ne peut pas être une somme de trois carrés d'entiers car il est possible de vérifier «à la main» que sa projection dans l'anneau commutatif unitaire $(\mathbb{Z}/8\mathbb{Z},+,\times)$ n'est pas une somme de trois carrés.

La preuve initiale de A.-M. Legendre de 1798 nécessitait le théorème de la progression arithmétique de Dirichlet [(3)], un résultat prouvé une cinquantaine d'années plus-tard.

Les espaces euclidiens $(\mathbb{Q}^3, q_3)$ et $(B^0(\mathbb{Q}), \mathrm{Nr})$ sont isométriques. En effet, l'application

$$\begin{array}{ccc} (\mathbb{Q}^3, q_3) & \to & (B^0(\mathbb{Q}), \mathrm{Nr}) \\ (a,b,c) & \mapsto & z = ai + bj + ck \end{array}$$

est une isométrie. Ceci permet de donner un énoncé équivalent du théorème des trois carrés.

Théorème 1.2.2 (Théorème des trois carrés (1801) : énoncé 2)**.** *Pour tout entier natuel non-nul d, il existe z dans $B^0(\mathbb{Z})$ tel que $Nr(z) = d$ si et seulement si d n'est pas du type $4^k(8\ell+7)$ où k et ℓ sont des entiers naturels.*

La fin de cette section contient une esquisse de preuve de cet énoncé du théorème des trois carrés. Soit d un entier naturel non-nul qui n'est pas du type $4^k(8\ell+7)$ où k et ℓ sont des entiers naturels.

Le principe de Hasse-Minkowski (un principe local-global nécessitant le théorème de la progression arithmétique de Dirichlet et détaillé dans [21, Théorème 8 Page 73]) implique qu'il existe z dans $B^0(\mathbb{Q})$ tel que $\mathrm{Nr}(z) = d$. Or, $\mathrm{Nr}(z) = z\overline{z} = -z^2$ car z est de trace nulle ce qui implique que $z^2 = -d$.

En particulier,

$$\mathbb{Z}[z] = \{Q(z), Q \in \mathbb{Z}[X]\}$$

est un anneau commutatif de type fini inclus dans $\mathcal{O}_B$.

Un corollaire de la principalité de l'ordre $\mathcal{O}_B$ est que si R est un sous-anneau de type fini de $B(\mathbb{Q})$ alors R est conjugué à un sous-anneau de $\mathcal{O}_B$. En d'autres termes, il existe q dans $B(\mathbb{Q})^\times$ vérifiant $q^{-1}Rq \subset \mathcal{O}_B$. En effet, $\mathcal{O}_B R$ est un $\mathcal{O}_B$-module de type fini à gauche donc il existe q dans $B(\mathbb{Q})^\times$ satisfaisant $\mathcal{O}_B R = \mathcal{O}_B q$ donc

$$qRq^{-1} \subset \mathcal{O}_B qRq^{-1} = \mathcal{O}_B RRq^{-1} = \mathcal{O}_B RRq^{-1} = \mathcal{O}_B qq^{-1} = \mathcal{O}_B.$$

(3). Ce résultat est détaillé dans [21, Chapitre VI].

Les deux remarques précédentes assurent qu'il existe q dans $B(\mathbb{Q})^\times$ tel que

$$q\mathbb{Z}[z]q^{-1} \subset \mathcal{O}_B.$$

En particulier,

$$qzq^{-1} \in \mathcal{O}_B \cap B^0(\mathbb{Q}) = B^0(\mathbb{Z})$$

avec $\mathrm{Nr}(qzq^{-1}) = d$, ce qui achève l'esquisse de preuve.

1.2.2 Formes quadratiques (C.F. Gauß) et nombre de classes (P.G.L. Dirichlet)

L'objectif de cette section est de donner une formule pour $r_3(d)$. Supposons pour simplifier que d soit un entier sans facteurs carrés satisfaisant $d \equiv 3 \pmod 4$. Par exemple, le fait que d soit sans facteurs carrés implique que si (a, b, c) est une représentation de d par q_3 alors a, b et c sont premiers entre eux [(4)].

L'ensemble des formes quadratiques binaires entières de discriminant -d donnée par

$$\mathcal{Q}(-d) = \left\{q_{a,b,c}(X, Y) = aX^2 + bXY + cY^2, (a, b, c) \in \mathbb{Z}^3, b^2 - 4ac = -d\right\}$$

admet une action de $SL_2(\mathbb{Z})$ définie par

$$\left(q_{a,b,c}.\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\right)(X, Y) = q_{a,b,c}(\alpha X + \gamma Y, \beta X + \delta Y).$$

C.F. Gauss a prouvé que l'ensemble quotient $SL_2(\mathbb{Z}) \setminus \mathcal{Q}(d)$ est non seulement fini mais admet également une structure de groupe abélien [(5)]. Il s'identifie au groupe des classes d'idéaux $Cl(-d)$ du corps quadratiques imaginaire pur $\mathbb{Q}(\sqrt{-d}) = K_{-d}$ dont l'anneau des entiers est $\mathbb{Z}[(1 + \sqrt{-d})/2] = \mathcal{O}_{-d}$. $Cl(-d)$ est le quotient de l'ensemble des idéaux fractionnaires de $\mathcal{O}_{-d}$ par l'ensemble de ses idéaux principaux. Son cardinal s'appelle le nombre de classes et est noté $h(-d)$.

La formule du nombre des classes de Dirichlet (démontrée dans [10, Equation (22.59)]) assure l'existence d'une constante réelle c_1 pour laquelle

$$h(-d) = c_1\sqrt{d}L\left(\chi_{-d}, 1\right) \tag{1.3}$$

où $L\left(\chi_{-d}, s\right)$ est la série de Dirichlet absolument convergente sur $\mathrm{Re}\left(s\right) > 1$ donnée par

$$L\left(\chi_{-d}, s\right) = \sum_{n\geqslant 1} \frac{\chi_{-d}(n)}{n^s}$$

et χ_{-d} est le caractère de Kronecker de K_{-d} défini à l'aide de symboles de Jacobi dans [10, Equation (3.43)].

C.L. Siegel a prouvé en 1935 que pour tout $\epsilon > 0$ arbitrairement petit, il existe une constante non calculable $c_\epsilon > 0$ telle que

$$L\left(\chi_{-d}, 1\right) \geqslant c_\epsilon d^{-\epsilon}. \tag{1.4}$$

(4). On dit que (a, b, c) est une représentation primitive de d par q_3.

(5). Voir par exemple [10, Chapitre 22] pour plus d'informations concernant le groupes des classes

D'autre part, le groupe $SO_3(\mathbb{Z})$ agit sur $R_3(d)$ par multiplication à droite. Il se trouve que $Cl(-d)$ agit transitivement sur l'ensemble quotient $SO_3(\mathbb{Z}) \setminus R_3(d)$ avec des stabilisateurs d'ordre au plus 2 ce qui entraîne qu'il existe une constante réelle c_2 telle que

$$r_3(d) = c_2 h(-d). \tag{1.5}$$

Les équations (1.3), (1.4) et (1.5) assurent que pour tout $\epsilon > 0$ arbitrairement petit, il existe une constante non calculable $c'_\epsilon > 0$ telle que

$$r_3(d) \geqslant c'_\epsilon d^{1/2-\epsilon}. \tag{1.6}$$

Cette minoration reste valide même si d admet des facteurs carrés ou n'est pas congru à 3 modulo 4.

Terminons ce paragraphe très dense par une description de l'action de $Cl(-d)$ sur $SO_3(\mathbb{Z}) \setminus R_3(d)$. Soient I un $\mathcal{O}_{-d}$-module de type fini et z dans $B^0(\mathbb{Z})$ avec $\mathrm{Nr}(z) = d$, c'est-à-dire $z^2 = -d$. En particulier, l'application

$$\begin{array}{rccc} i_z : & K_{-d} & \to & B(\mathbb{Q}) \\ & u + v\sqrt{-d} & \mapsto & u + vz \end{array}$$

est un plongement.

L'ensemble $i_z(I)\mathcal{O}_B$ étant un $\mathcal{O}_B$-module à gauche de type fini, nous savons qu'il existe q dans $B(\mathbb{Q})^\times$ tel que $i_z(I)\mathcal{O}_B = q\mathcal{O}_B$ car $\mathcal{O}_B$ est principal. Signalons que q est défini à une unité près de $\mathcal{O}_B$.

Définissons $z' = q^{-1}zq$. D'une part, il s'agit d'un quaternion de norme réduite égale à d et de trace nulle. D'autre part,

$$\begin{aligned} z' = q^{-1}zq &\in q^{-1}i_z(\sqrt{-d})q\mathcal{O}_B \\ &= q^{-1}i_z(\sqrt{-d})i_z(I)\mathcal{O}_B \\ &\subset q^{-1}i_z(I)\mathcal{O}_B \\ &= \mathcal{O}_B. \end{aligned}$$

Ainsi, $z' \in B^0(\mathbb{Q}) \cap \mathcal{O}_B = B^0(\mathbb{Z})$ et est de norme réduite égale à d donc défini un élément de $R_3(d)$.

L'action de la classe d'équivalence dans le groupe des classes $Cl(-d)$ de I notée $[I]$ sur z dans $R_3(d)$ est donnée par la formule

$$[I].z = z'.$$

Il s'agit alors de vérifier qu'il s'agit d'une action de $Cl(-d)$ sur $SO_3(\mathbb{Z}) \setminus R_3(d)$, le quotient par $SO_3(\mathbb{Z})$ reflétant le fait que q est défini à une unité près de $\mathcal{O}_B$, et que cette action est transitive avec des stabilisateurs d'ordre au plus 2. Nous ne le ferons pas lors de cet exposé et nous renvoyons le lecteur vers [4].

1.2.3 Equirépartition selon W. Duke, H. Iwaniec et Y.V. Linnik

L'équation (1.6) assure que

$$\frac{1}{\sqrt{d}} R_3(d) = \left\{ \left(\frac{a}{\sqrt{d}}, \frac{b}{\sqrt{d}}, \frac{c}{\sqrt{d}} \right), (a,b,c) \in \mathbb{Z}^3, q_3(a,b,c) = d \right\}$$

est un sous-ensemble de la sphère unité $\mathbb{S}^2$ de $\mathbb{R}^3$ constitué d'au moins $d^{1/2-\epsilon}$ éléments pour tout $\epsilon > 0$ si d est admissible, c'est-à-dire n'est pas de la forme $4^k(8\ell + 7)$ pour des entiers naturels k et ℓ. Il est alors naturel d'étudier la distribution de cet ensemble sur $\mathbb{S}^2$. La réponse à cette question a été donnée indépendamment par Y.V. Linnik ([12]) en 1968, modulo une condition de nature ergodique, et inconditionnellement par W. Duke et H. Iwaniec ([9] et [2]) en 1988.

Théorème 1.2.3 (W. Duke, H. Iwaniec (1988)). *$\left(\frac{1}{\sqrt{d}}R_3(n)\right)_{d \text{ admissible}}$ s'équirépartit sur $\mathbb{S}^2$ par rapport à la mesure de Lebesque normalisée sur $\mathbb{S}^2$ notée $\lambda_{\mathbb{S}^2}$ lorsque d tend vers l'infini parmi les entiers admissibles. En d'autres termes, si $f : \mathbb{S}^2 \to \mathbb{C}$ est une fonction continue alors*

$$\frac{1}{r_3(d)} \sum_{\mathbf{x} \in R_3(d)} f\left(\frac{\mathbf{x}}{\sqrt{d}}\right) \to_{\substack{d \to +\infty \\ d admissible}} \int_{\mathbf{x} \in \mathbb{S}^2} f(\mathbf{x}) \mathrm{d}\lambda_{\mathbb{S}^2}(\mathbf{x}).$$

Commençons par décrire la condition supplémentaire apparaissant dans le travail de Y.V. Linnik. Soit p un nombre premier impair fixé. Y.V. Linnik exige que d doit être sans facteurs carrés et que $-d$ doit être un carré modulo p, ce qui signifie que p est décomposé dans K_{-d}. En d'autres termes, l'idéal engendré par p dans $\mathcal{O}_{-d}$, noté $p\mathcal{O}_{-d}$, se décompose sous la forme

$$p\mathcal{O}_{-d} = \mathfrak{p}\mathfrak{p}'$$

où $\mathfrak{p}$ et $\mathfrak{p}'$ sont deux idéaux de $\mathcal{O}_{-d}$. Cette condition admet l'interprétation ergodique suivante. Le sous-groupe de $Cl(-d)$ engendré par la classe de $\mathfrak{p}$, noté $\langle[\mathfrak{p}]\rangle$, vérifie

$$\mathrm{card}\left(\langle[\mathfrak{p}]\rangle\right) \geqslant c\frac{\log(d)}{\log(p)}$$

où c est une constante. En effet, si h est un entier naturel vérifiant $[\mathfrak{p}]^h = [\mathcal{O}_{-d}]$ alors l'idéal $\mathfrak{p}^h$ est un idéal principal de $\mathcal{O}_{-d}$ engendré par $a + b\sqrt{-d}$ pour a et b des demi-entiers relatifs avec $b \neq 0$. En d'autres termes,

$$\mathfrak{p}^h = (a + b\sqrt{-d})\mathcal{O}_{-d}.$$

Un calcul de normes de ces idéaux implique que

$$p^h = a^2 + b^2 d \geqslant d/4$$

ce qui est ce que l'on cherchait. Ainsi, la condition de Linnik assure l'existence d'une dynamique exploitable sur $R_3(d)$ (hypothèse de type entropie positive).

Donnons une esquisse de la preuve de W. Duke et de H. Iwaniec, qui repose sur l'analyse harmonique et qui ressemble à la démonstration du théorème des quatre carrés de J.L. Lagrange décrite précédemment.

L'espace topologique des fonctions continues sur $\mathbb{S}^2$ est engendré par les polynômes harmoniques homogènes c'est-à-dire par les polynômes homogènes P sur $\mathbb{R}^3$ annulés par le Laplacien Euclidien de $\mathbb{R}^3$

$$\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}\right)(P) = 0$$

selon [5]. Il suffit donc de prouver le théorème d'équirépartition pour f un tel polynôme homogène P de degré $s \geqslant 1$, le cas des polynômes homogènes de degré 0 étant immédiat. Il s'agit alors de prouver que

$$\frac{1}{r_3(d)} \sum_{\mathbf{x} \in R_3(d)} P\left(\frac{\mathbf{x}}{\sqrt{d}}\right) \to_{\substack{d \to +\infty \\ d \text{ admissible}}} \int_{\mathbf{x} \in \mathbb{S}^2} P(\mathbf{x}) \mathrm{d}\lambda_{\mathbb{S}^2}(\mathbf{x}) = 0.$$

Soit $\varepsilon > 0$ arbitrairement petit. Nous avons

$$\frac{1}{r_3(d)} \sum_{\mathbf{x} \in R_3(d)} P\left(\frac{\mathbf{x}}{\sqrt{d}}\right) = \frac{1}{r_3(d) d^{s/2}} \sum_{\mathbf{x} \in R_3(d)} P(\mathbf{x}) \\ \ll_\varepsilon \frac{1}{d^{1/2+s/2-\varepsilon}} \sum_{\mathbf{x} \in R_3(d)} P(\mathbf{x}).$$

Il s'agit donc de prouver qu'il existe une constante $\delta > 0$ telle que

$$\sum_{\mathbf{x} \in R_3(d)} P(\mathbf{x}) \ll d^{1/2+s/2-\delta} = d^{(s+3/2)/2-1/4-\delta}.$$

Définissons une fonction sur $\mathbb{H}$ par

$$\theta_P(z) = \sum_{d \geqslant 1} \left(\sum_{\mathbf{x} \in R_3(d)} P(\mathbf{x}) \right) \exp(2i\pi dz).$$

dont les coefficients de Fourier sont précisément les quantités à estimer afin de terminer la preuve.

Proposition 1.2.1. *La fonction θ_P est une forme modulaire de poids $s + 3/2$ et de niveau 4.*

Cela signifie que θ_P satisfait les symmétries données par

$$\forall z \in \mathbb{H}, \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4), \quad \theta_P(\gamma.z) = \left(\left(\frac{c}{d} \right) \epsilon_d^{-1} (cz+d)^{1/2} \right)^{2s+3} \theta_P(z).$$

Ici,

$$\epsilon_d = \begin{cases} 1 & \text{if } d \equiv 1 \bmod 4, \\ i & \text{if } d \equiv 3 \bmod 4, \end{cases}$$

la racine carrée est celle qui est positive sur $\mathbb{R}_+^\times$ et le symbole de Jacobi est défini dans [10, Page 52]. Le lecteur trouvera une preuve de cette proposition dans [8, Théorème 10.8]. Une différence importante avec le cas du théorème des quatre carrés de J.L. Lagrange est que θ_P n'est pas de poids entier mais demi-entier.

Il est facile de démontrer que

$$\sum_{\mathbf{x} \in R_3(n)} P(\mathbf{x}) \ll d^{(s+3/2)/2-1/4+\epsilon}$$

pour tout $\epsilon > 0$. Une amélioration minuscule de cette borne implique le résultat d'équidistribution. H. Iwaniec ([9]) a prouvé que

$$\sum_{\mathbf{x} \in R_3(d)} P(\mathbf{x}) \ll d^{(s+3/2)/2-1/4-\frac{1}{22}+\epsilon}$$

pour tout $\epsilon > 0$ lorsque $s + 3/2 \geqslant 7/2$ et θ_P est une fonction holomorphe. W. Duke ([2]) a généralisé ce résultat lorsque $s + 3/2 \geqslant 1/2$ et θ_P est réelle-analytique, ce qui lui a notamment permis de conclure la preuve analytique et harmonique de ce résultat d'équidistribution.

1.3 Généralisations

Les paragraphes précédents suggèrent à juste titre que les différents résultats concernant la distribution des représentations d'un entier par une forme quadratique sont intimement liés à la théorie des formes modulaires et à la dynamique de l'action de certains tores sur des espaces homogènes. Nous renvoyons le lecteur vers [20] et [16] pour plus de détails mais nous aimerions indiquer deux champs de recherche inspirés par ce type de questions en théorie des nombres.

- Théorie des représentations automorphes :
  - fonctions L et problème de sous-convexité ([15]),
  - conjectures de B. Gross-D. Prasad ([6], [7]).
- Théorie ergodique :
  - travaux de R. Bowen et de G. Margulis sur l'équirépartition des géodésiques fermées d'une surface hyperbolique compacte ([1], [14]),
  - théorie de Ratner (classification des orbites des flots unipotents sur les espaces homogènes, [17], [18]) lorsque le nombre de variables de la forme quadratique est supérieur à quatre,
  - travaux récents de Einsiedler-Katok-Lindenstrauss sur la conjecture de Littlewood ([3]).

Bibliographie

[1] R. Bowen, *The equidistribution of closed geodesics*, Amer. J. Math.94 (1972) pp 413–423.

[2] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*, Invent. Math. 92 (1988), no. 1, pp 73–90.

[3] M. Einsiedler, A. Katok, E. Lindenstrauss, *Invariant measures and the set of exceptions to Littlewood's conjecture*, Ann. of Math. (2), 164, (2006), no 2, pp 513–560.

[4] J.S. Ellenberg, P. Michel, A. Venkatesh, *Linnik's ergodic method and the distribution of integer points on spheres*, Automorphic representations and L-functions, pp 119–185, Tata Inst. Fundam. Res. Stud. Math., 22, Tata Inst. Fund. Res., Mumbai, 2013.

[5] J. Faraut, *Analysis on Lie groups. An introduction.*, Cambridge Studies in Advanced Mathematics, 110. Cambridge University Press, Cambridge, 2008, 302 pp.

[6] B. Gross, D. Prasad, *On the decomposition of a representation of* SO_n *when restricted to* SO_{n-1}, Canad. J. Math. 44 (1992), no. 5, pp 974–1002.

[7] B. Gross, D. Prasad, *On irreducible representations of* $\mathrm{SO}_{2n+1} \times \mathrm{SO}_{2m}$, Canad. J. Math. 46 (1994), no. 5, pp 930–950.

[8] H. Iwaniec, *Topics in classical automorphic forms*, Graduate Studies in Mathematics, 17. American Mathematical Society, Providence, RI, 1997, 259 pp.

[9] H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*, Invent. Math. 87 (1987), no. 2, pp 385–401.

[10] H.Iwaniec, E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, 53, American Mathematical Society, Providence, RI, 2004, 615 pp.

[11] H.D. Kloosterman, *On the representation of numbers in the form* $ax^2 + by^2 + cz^2 + dt^2$, Acta Math. 49 (1927), no. 3-4, pp. 407–464.

[12] Y.V. Linnik, *Ergodic properties of algebraic fields*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 45, Springer-Verlag New York Inc., New York, 1968.

[13] A.V. Malyshev, *On the representations of integers by positive definite forms*, Mat. Steklov 65 (1962).

[14] G. Margulis, *Applications of ergodic theory for the investigation of manifolds of negative curvature* ,Func. Anal. Appl.3 (1969) pp 335–336.

[15] P. Michel, *Familles de fonctions L de formes automorphes et applications*, Les XXIIèmes Journées Arithmétiques (Lille, 2001), J. Théor. Nombres Bordeaux 15 (2003), no. 1, pp 275–307.

[16] P. Michel, A. Venkatesh, *Equidistribution, L-functions and ergodic theory : on some problems of Yu. Linnik*, International Congress of Mathematicians, Vol. II, pp 421–457, Eur. Math. Soc., Zürich, 2006.

[17] M. Ratner, *Strict measure rigidity for unipotent subgroups of solvable groups*, Invent. Math. 101 (1990), pp 449–482.

[18] M. Ratner, *On measure rigidity of unipotent subgroups of semisimple groups*, Acta Math. 165 (1990), pp 229–309.

[19] P. Samuel, *Théorie algébrique des nombres*, Hermann, Paris, 1967, 130pp.

[20] P. Sarnak, *Kloosterman, quadratic forms and modular forms*, Nieuw Arch. Wiskd. (5) 1 (2000), no. 4, pp 385–389.

[21] J.-P. Serre, *Cours d'arithmétique*, Deuxième édition revue et corrigée, Le Mathématicien, No. 2, Presses Universitaires de France, Paris, 1977, 188 pp.

[22] B.A. Venkov, *On the Arithmetic of Quaternions*, Bull. Acad. Sci. USSR, VI series, vol. 16, pp. 205–246, 1922.

[23] B.A. Venkov, *On the Arithmetic of Quaternions. Third letter*, Izvestiya Akademii Nauk SSSR, pp. 535–562, 1929.