Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 34 (1988)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: LE PROBLÈME DE GAUSS SUR LE NOMBRE DE CLASSES

Autor: Oesterlé, J.

Kapitel: §1. Représentation des entiers par les formes quadratiques

DOI: https://doi.org/10.5169/seals-56588

le plus grand d correspondant est respectivement 163, 427, 907, 1555, 2683, 3763, 5923, 6307, 10627, 13843.

Cela semble suggérer que tous les discriminants fondamentaux $-d$ pour lesquels $h(-d) \leqslant 10$ figurent dans la table de Buell. Peut-on le prouver? C'est à ce type de question qu'est consacrée la fin de l'exposé. On s'intéresse à ce problème car les discriminants pour lesquels $h(-d)$ est petit possèdent comme nous le verrons des propriétés arithmétiques remarquables. Nous allons commencer par décrire les deux outils essentiels pour l'étude de $h(-d)$, à savoir les nombres de représentations des entiers par les formes quadratiques et les fonctions zêta associées.

Les formes quadratiques de discriminant -3 *et* -4 *ont des automorphismes distincts de* $\pm I$ *dans* $SL_2(\mathbf{Z})$. *Pour éviter les complications techniques qui en résultent, nous supposerons dans la suite* $d \neq 3$ *et* $d \neq 4$ *(donc* $d \geqslant 7$*).*

§ 1. Représentation des entiers par les formes quadratiques

Soit q une forme quadratique de discriminant $-d$ (distinct de -3 et -4). Le *nombre de représentations primitives* d'un entier $n \geqslant 1$ par q, comptées au signe près, est

$$(12) \quad r_n(q) = \frac{1}{2}\,\mathrm{Card}\,\{(u, v) \in \mathbf{Z}^2 \mid q(u, v) = n \quad \text{et} \quad \mathrm{pgcd}\,(u, v) = 1\}\,.$$

Ce nombre ne dépend que de la classe C de la forme quadratique q, et on le note aussi $r_n(C)$. Soit $ax^2 + bxy + cy^2$ la forme réduite appartenant à C. On a $3a^2 \leqslant 4ac - b^2 < 4c^2$ (l'inégalité est stricte car $d \neq 4$), d'où $a \leqslant \sqrt{d/3}$ et $c > \sqrt{d}/2$. On a $r_a(C) \neq 0$, et si $n \geqslant 1$ est un entier $< c$ tel que $r_n(C) \neq 0$, on a nécessairement $n = a$ et $r_n(C) = 1$ (I. § 2, formule (6)). On en déduit

$$(13) \qquad \sum_{n \leqslant \sqrt{d}/2} r_n(C) \leqslant 1 \leqslant \sum_{n \leqslant \sqrt{d/3}} r_n(C)\,.$$

Introduisons le *nombre total des représentations primitives*, comptées au signe près, de l'entier n par les différentes classes de formes quadratiques de discriminant $-d$:

$$(14) \qquad r_n(-d) = \sum_{C \in Cl(-d)} r_n(C)\,.$$

On déduit de (13) un *encadrement du nombre de classes*

$$\sum_{n \leqslant \sqrt{d}/2} r_n(-d) \leqslant h(-d) \leqslant \sum_{n \leqslant \sqrt{d/3}} r_n(-d), \tag{15}$$

ce qui montre que l'étude de $h(-d)$ est liée à celle des nombres $r_n(-d)$.

Il n'existe à ma connaissance aucune formule simple permettant pour une classe C donnée de calculer $r_n(C)$. Par contre, Gauss a obtenu le résultat remarquable suivant [1]:

THÉORÈME. *Pour tout entier* $n \geqslant 1, r_n(-d)$ *est le nombre de* b (mod. $2n$) *tels que* $b^2 \equiv -d$ (mod. $4n$).

La démonstration de Gauss est très élégante: Soit (q_i) un système de représentants des classes de formes quadratiques de discriminant $-d$. Si b est un entier tel que b^2 s'écrive $-d + 4nc$, la forme quadratique $nx^2 + bxy + cy^2$ a pour discriminant $-d$ et s'écrit $q_i(ux+wy, vx+ty)$ pour un unique indice i et une certaine matrice $\begin{pmatrix} u & w \\ v & t \end{pmatrix} \in SL_2(\mathbf{Z})$. On a $q_i(u, v) = n$, et (u, v) est déterminé au signe près par b (mod. $2n$) car I et $-I$ sont les seuls automorphismes de q_i dans $SL_2(\mathbf{Z})$. Inversement, chaque représentation primitive de n par l'une des formes q_i s'obtient par ce procédé à partir d'un unique b (mod. $2n$) tel que $b^2 \equiv -d$ (mod. $4n$).

En décomposant $\mathbf{Z}/4n\mathbf{Z}$ en ses composantes primaires, on obtient la forme équivalente suivante de l'énoncé précédent:

COROLLAIRE. *Pour que* $r_n(-d) \neq 0$, *il faut et il suffit que* n *soit de la forme* $d'p_1^{\alpha_1} \dots p_m^{\alpha_m}$, *avec* d' *un diviseur de* d *sans facteurs carrés,* $p_1, \dots, p_m$ *des nombres premiers deux à deux distincts modulo lesquels* $-d$ *est un carré non nul, et* $\alpha_1, \dots, \alpha_m$ *des entiers* $\geqslant 1$. *On a alors* $r_n(-d) = 2^m$.

De la formule (15) et du corollaire ci-dessus, on peut retenir le principe suivant:

PRINCIPE. *Si* d *est grand et* $h(-d)$ *est petit, il y a peu de petits entiers* n *qui soient représentés par une forme quadratique de discriminant* $-d$, *et peu de petits nombres premiers modulo lesquels* $-d$ *est un carré.*

Illustrons ceci dans le cas particulier où $d = 163$. On a $h(-163) = 1$ et $x^2 + xy + 41y^2$ est la seule forme quadratique réduite de discriminant

---

[1]) C.-F. GAUSS, *Disquisitiones Arithmeticae*, n° 167, 168 et 180.

-163. D'après le début de ce paragraphe, on a $r_n(-163) = 0$ pour $2 \leqslant n \leqslant 40$. Par suite, -163 n'est un carré modulo aucun des nombres premiers $\leqslant 39$, et le corollaire au théorème ci-dessus implique que si $r_n(-163) \neq 0$ et $n < 41^2$, nécessairement n est premier. Ceci explique pourquoi la suite (découverte par Euler): 41, 43, 47, 53, 61, ..., formée par les valeurs de $x^2 + x + 41$ pour $x \geqslant 0$ ne comporte que des nombres premiers jusqu'à 1601 $(= 39^2 + 39 + 41)$.

§ 2. Fonctions zêta

Il est fructueux de réinterpréter les résultats du paragraphe précédent en introduisant des *séries de Dirichlet génératrices*: pour toute forme quadratique q de discriminant $-d$, la série de Dirichlet

$$\zeta(q, s) = \frac{1}{2} \sum_{(u, v) \in \mathbf{Z}^2 - \{(0, 0)\}} q(u, v)^{-s} \tag{16}$$

converge absolument pour $\mathrm{Re}\,(s) > 1$ et l'on a

$$\zeta(q, s) = \zeta(2s) \sum_{n=1}^{\infty} r_n(q) n^{-s} \tag{17}$$

où $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ est la fonction zêta de Riemann. Comme $\zeta(q, s)$ ne dépend que de la classe C de q, on l'écrit aussi $\zeta(C, s)$.

La fonction $\zeta(q, s)$ jouit de remarquables propriétés analytiques: la fonction

$$\Lambda(q, s) = 2 d^{s/2} (2\pi)^{-s} \Gamma(s) \zeta(q, s) \tag{18}$$

admet un *prolongement méromorphe à* $\mathbf{C}$, avec pour seuls pôles des *pôles simples en* 0 *et* 1 de résidus -1 et 1, et vérifie *l'équation fonctionnelle* $\Lambda(q, 1-s) = \Lambda(q, s)$. En effet, la fonction thêta

$$\theta(q, t) = \sum_{(n, m) \in \mathbf{Z}^2} \exp\left(-q(n, m) 2\pi t / \sqrt{d}\right) \tag{19}$$

satisfait d'après la formule sommatoire de Poisson à l'équation fonctionnelle

$$\theta(q, t^{-1}) = t\theta(q, t)\,; \tag{20}$$

on a, par échange de la somme et de l'intégrale,

$$\Lambda(q, s) = \int_0^{\infty} [\theta(q, t) - 1]\, t^{s-1} dt\,, \tag{21}$$