I. La classification de Gauss des formes quadratiques

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **34 (1988)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

L'exposé est divisé en deux parties:

Les résultats exposés dans la première partie sont dus pour l'essentiel à Gauss [1]). On y montre pour commencer qu'il n'y a qu'un nombre *fini* de classes de formes quadratiques de discriminant $\Delta < 0$ donné (§ 1). On donne un algorithme simple permettant d'obtenir un *système de représentants* de ces classes, et de calculer le *nombre* $\tilde{h}(\Delta)$ *de telles classes* (§ 2 et § 3). Une des découvertes fondamentales de Gauss est l'existence d'une structure de *groupe abélien* naturelle sur l'ensemble $Cl(\Delta)$ des classes de formes quadratiques *primitives* de discriminant Δ (*primitives* signifie *telles que* $\mathrm{pgcd}(a, b, c) = 1$): cette structure de groupe est décrite au § 4; le lien avec l'arithmétique des *corps quadratiques imaginaires* est exposé aux § 4 et § 5.

En dressant une table des nombres de classes, Gauss constate expérimentalement que ces nombres semblent tendre vers $+\infty$ lorsque le discriminant tend vers $-\infty$ (en satisfaisant à (2)). Il faudra attendre plus de cent ans, avec les travaux de Heilbronn en 1934, pour voir cette assertion démontrée. Se pose alors la question de dresser, pour les petites valeurs de h entier $\geqslant 1$, la liste complète des $\Delta < 0$ tels que $\tilde{h}(\Delta) = h$. C'est essentiellement l'histoire (sans démonstrations) des progrès récents obtenus sur cette question qui fait l'objet de la seconde partie de l'exposé. Nous expliquerons le rôle joué par les courbes elliptiques dans ces progrès.

I. La classification de Gauss des formes quadratiques

§ 1. Finitude du nombre de classes [2])

Théorème. *Soit* d *un entier* $\geqslant 1$. *Il n'y a qu'un nombre fini de classes de formes quadratiques de discriminant* $-d$.

Ce théorème résulte des deux lemmes suivants:

Lemme 1. *Toute classe contient une forme quadratique* $ax^2 + bxy + cy^2$ *telle que* $|b| \leqslant a \leqslant c$.

---

[1]) C.-F. Gauss, *Disquisitiones Arithmeticae*, 1801 (Werke, t. I), Section cinquième. (Traduction française par A.-C.-M. Poullet-Delisle, parue en 1807.) Dans cet ouvrage, Gauss suppose les formes $ax^2 + bxy + cy^2$ paires, c'est-à-dire telles que b soit pair. Le cas général s'y ramène facilement, en remplaçant $ax^2 + bxy + cy^2$ par $2ax^2 + 2bxy + 2cy^2$ lorsque b est impair.

[2]) C.-F. Gauss, *Disquisitiones Arithmeticae*, n° 174.

LEMME 2. *Il n'y a qu'un nombre fini de triplets de nombres entiers* (a, b, c) *tels que* $b^2 - 4ac = -d$ *et* $|b| \leqslant a \leqslant c$.

Démontrons le lemme 1. Soit $ax^2 + bxy + cy^2$ une forme quadratique appartenant à la classe C considérée. Par hypothèse cette forme est positive, de sorte que $a > 0$ et $c > 0$. Les changements de variables $(x, y) \mapsto (x - \varepsilon y, y)$ et $(x, y) \mapsto (x, y - \varepsilon x)$, où ε est le signe de b, ont pour effet de remplacer (a, b, c) par $(a, b - 2\varepsilon a, a + c - |b|)$ et par $(a + c - |b|, b - 2\varepsilon c, c)$. Si donc $|b| > a$ ou $|b| > c$, on peut remplacer $ax^2 + bxy + cy^2$ par une forme équivalente pour laquelle la quantité $a + c$ est strictement plus petite. Après un nombre fini de substitutions de ce type, on trouve une forme $ax^2 + bxy + cy^2$ dans C pour laquelle $|b| \leqslant a$ et $|b| \leqslant c$. Cette forme, ou la forme $cx^2 - bxy + ay^2$ qui s'en déduit par le changement de variables $(x, y) \mapsto (y, -x)$, remplit les conditions du lemme 1.

Démontrons le lemme 2. Si (a, b, c) sont comme dans l'énoncé de ce lemme, on a

$$d = 4ac - b^2 \geqslant 4a^2 - a^2 = 3a^2 , \tag{3}$$

de sorte que a ne peut prendre qu'un nombre fini de valeurs; il en est alors de même de b et de c, puisque $|b| \leqslant a$ et $c = (b^2 + d)/4a$.

§ 2. FORMES QUADRATIQUES RÉDUITES [1])

Dans ce paragraphe, nous montrons comment la *théorie de la réduction* de Gauss permet de sélectionner un représentant dans chaque classe C de formes quadratiques de discriminant $-d$.

Nous savons déjà que C contient une forme quadratique $ax^2 + bxy + cy^2$ telle que $|b| \leqslant a \leqslant c$ (lemme 1 du § 1). Peut-il y avoir plusieurs formes de ce type dans C? En fait, la seule autre possible est $ax^2 - bxy + cy^2$, lorsqu'elle est dans C. Ceci vient du fait que $|b|$ est déterminé par a et c (on a $b^2 - 4ac = -d$), et que a, c sont caractérisés par le fait que pour toute forme quadratique $q \in C$, on a

$$a = \inf(q(\mathbf{u})) \qquad (\mathbf{u} \neq 0 \text{ dans } \mathbf{Z}^2) ; \tag{4}$$

$$ac = \inf(q(\mathbf{u})q(\mathbf{v})) \qquad (\mathbf{u}, \mathbf{v} \text{ non colinéaires dans } \mathbf{Z}^2) . \tag{5}$$

Il nous suffit en effet de vérifier (4) et (5) pour une seule forme quadratique $q \in C$, par exemple la forme $ax^2 + bxy + cy^2$ elle-même. Mais

[1]) C.-F. GAUSS, *Disquisitiones Arithmeticae*, n° 171 et 172.

pour celle-ci, on a $q(1, 0) = a$, $q(0, 1) = c$ et $q(x, y) \geqslant ax^2 - |b||xy| + cy^2 \geqslant (2a-|b|)|xy| + (c-a)y^2$, d'où

$$\begin{array}{lll} & q(x, 0) \geqslant a\,, & \text{si} \quad x \neq 0 \\ (6) & q(0, y) \geqslant c\,, & \text{si} \quad y \neq 0 \\ & q(x, y) \geqslant (2a-|b|) + (c-a) = a + c - |b| \geqslant c & \text{si} \quad xy \neq 0\,, \end{array}$$

et donc les égalités (4) et (5).

Voyons maintenant dans quels cas la forme $ax^2 - bxy + cy^2$ appartient à la classe C:

LEMME. *Pour que la forme* $q(x, y) = ax^2 + bxy + cy^2$ *(avec* $|b| \leqslant a \leqslant c$*) soit équivalente à la forme* $q'(x, y) = ax^2 - bxy + cy^2$, *il faut et il suffit que l'on ait* $a = |b|$, $a = c$ *ou* $b = 0$.

On a $q(x, y) = q'(x \pm y, y)$ si $a = \pm b$, $q(x, y) = q'(y, -x)$ si $a = c$, $q(x, y) = q'(x, y)$ si $b = 0$. Supposons $0 < |b| < a < c$. S'il existe $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbf{Z})$ tel que $q'(x, y) = q(\alpha x + \beta y, \gamma x + \delta y)$, on a $q(\alpha, \gamma) = a$ et $q(\beta, \delta) = c$, d'où $\gamma = 0$ puis $\beta = 0$ en appliquant (6), et finalement $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \pm I$, ce qui est absurde.

L'étude qui précède nous conduit à adopter la définition suivante: une forme quadratique $ax^2 + bxy + cy^2$ est dite *réduite* si l'on a

$$\begin{array}{l} |b| \leqslant a \leqslant c \\ b \geqslant 0 \quad \text{si} \quad a \text{ est égal à } |b| \text{ ou à } c\,. \end{array}$$

Nous avons alors prouvé le théorème suivant:

THÉORÈME. *Chaque classe de formes quadratiques de discriminant* $-d$ *contient une unique forme réduite.*

La démonstration du lemme 1 du § 1 fournit en fait un algorithme permettant d'obtenir la forme quadratique réduite équivalente à une forme donnée.

Exemple. Appliqué à la forme quadratique $9x^2 + 43xy + 53y^2$ (représentée par (9, 43, 53) pour abréger), cet algorithme s'écrit

$$(9, 43, 53) \sim (9, 25, 19) \sim (9, 7, 3) \sim (5, 1, 3) \sim (3, -1, 5)$$

et $3x^2 - xy + 5y^2$ est la forme réduite cherchée.

§ 3. Une méthode élémentaire pour calculer le nombre de classes [1])

Soit d un entier $\geqslant 1$. D'après le § 2, le nombre $\tilde{h}(-d)$ de classes de formes quadratiques de discriminant $-d$ est le nombre de formes quadratiques réduites de discriminant $-d$, c'est-à-dire le nombre de triplets (a, b, c) d'entiers vérifiant

$$\text{(7)} \qquad \begin{aligned} & b^2 - 4ac = -d \\ & |b| \leqslant a \leqslant c \\ & b \geqslant 0 \quad \text{si} \quad a \text{ est égal à } |b| \text{ ou à } c\,. \end{aligned}$$

Nous savons déjà que $\tilde{h}(-d)$ est non nul si et seulement si $-d$ est congru à 0 ou à 1 modulo 4. Les conditions (7) entraînent que a, donc aussi $|b|$ est majoré par $\sqrt{d/3}$ (§ 1, formule (3)) et que $|b|$ est de même parité que d. On en déduit aussitôt la formule suivante, permettant de calculer $\tilde{h}(-d)$:

Proposition. *Supposons* $-d$ *congru à* 0 *ou à* 1 *modulo* 4. *On a:*

$$\tilde{h}(-d) = \sum_{\substack{0 \leqslant b \leqslant \sqrt{d/3} \\ b \equiv d (\mathrm{mod.}\ 2)}} \; \sum_{\substack{a \mid ((b^2+d)/4) \\ b \leqslant a \leqslant \sqrt{(b^2+d)/4}}} n(a, b)$$

avec $n(a, b) = 1$ *si l'on a* $b = 0$ *ou* $a = b$ *ou* $a = \sqrt{(b^2+d)/4}$, *et* $n(a, b) = 2$ *sinon.*

Exemple. Calculons $\tilde{h}(-347)$. On a $10 < \sqrt{347/3} < 11$, d'où le tableau suivant:

b	$(b^2+d)/4$	a	$n(a, b)$
1	$87 = 3.29$	1, 3	1, 2
3	89	—	—
5	$93 = 3.31$	—	—
7	$99 = 3^2.11$	9	2
9	107	—	—

dont on déduit $\tilde{h}(-347) = 5$. Les coefficients des cinq formes réduites se lisent sur le tableau; ce sont:

$$(1, 1, 87),\ (3, 1, 29),\ (3, -1, 29),\ (9, 7, 11) \text{ et } (9, -7, 11)\,.$$

---

[1]) C.-F. Gauss, *Disquisitiones Arithmeticae*, n° 174 et 175.

L'étude des formes quadratiques se ramène facilement à celle des formes *primitives*, c'est-à-dire celles dont les coefficients ont 1 pour plus grand commun diviseur. En effet, si $-d < 0$ est congru à 0 ou à 1 modulo 4, il existe un plus grand entier F tel que $-d$ s'écrive $-d_0F^2$ avec $-d_0$ congru à 0 ou 1 modulo 4. Pour toute classe C de formes quadratiques de discriminant $-d$, il existe un diviseur $f \geqslant 1$ de F et une classe C' de formes quadratiques primitives de discriminant $-df^{-2}$ tels que $C = fC'$.

Les nombres de classes $\tilde{h}$ et les nombres de classes primitives h sont donc reliés par l'égalité

$$\tilde{h}(-d) = \sum_{f|F} h(-df^{-2}) . \tag{8}$$

Lorsque F est égal à 1, ce qui équivaut à dire que d n'est pas divisible par le carré d'un nombre premier impair et est congru à 3 (mod. 4), à 4 (mod. 16) ou à 8 (mod. 16), on dit que $-d$ est un *discriminant fondamental*. Toute forme de discriminant $-d$ est alors primitive et on a $\tilde{h}(-d) = h(-d)$.

§ 4. Le groupe des classes [1])

Cherchant à généraliser la formule classique

$$(x^2+y^2)(x'^2+y'^2) = (xx'-yy')^2 + (xy'+yx')^2 ,$$

Gauss se demande pour quels couples (q, q') de formes quadratiques, il existe une forme quadratique q'' telle que l'on ait une identité

$$q(x, y)q'(x', y') = q''(x'', y'') ,$$

où x'' et y'' sont des combinaisons linéaires à coefficients entiers de xx', xy', yx' et yy'.

Si l'on a une identité du type précédent, et si $-d$, $-d'$, $-d''$ désignent les discriminants de q, q', q'', le carré du déterminant de l'application linéaire $(x, y) \mapsto (x'', y'')$ (resp. $(x', y') \mapsto (x'', y'')$) est égal à $dq'(x', y')^2/d''$ (resp. $d'q(x, y)^2/d''$).

Gauss montre que lorsque q et q' sont des formes primitives de même discriminant $-d$, il est possible d'obtenir une identité du type ci-dessus, avec q'' forme primitive de discriminant $-d$, et

$$q'(x', y') = \det\big((x, y) \mapsto (x'', y'')\big) , \quad q(x, y) = \det\big((x', y') \mapsto (x'', y'')\big) .$$

---

[1]) C.-F. Gauss, *Disquisitiones Arithmeticae*, n° 234 à 243.

Il montre de plus que, sous ces conditions, la classe C'' de q'' ne dépend que des classes C, C' de q, q', et que la loi de composition qui à (C, C') associe C'' définit sur l'ensemble $Cl(-d)$ des classes de formes primitives de discriminant $-d$ une structure de groupe abélien.

De nos jours, on préfère introduire la loi de composition précédente en interprétant $Cl(-d)$ comme un ensemble de classes d'idéaux fractionnaires inversibles. Pour cela, introduisons l'ensemble $\mathcal{O}(-d)$ des nombres complexes de la forme $(u + iv\sqrt{d})/2$, où u et v sont des nombres entiers et $u \equiv vd \pmod 2$. C'est un sous-anneau de $\mathbf{C}$, dont le corps des fractions est $K = Q + Qi\sqrt{d}$.

Un *réseau* de K est un sous-groupe de K qui admet une base sur $\mathbf{Z}$ formée de deux éléments. On dit qu'un réseau L de K est un $\mathcal{O}(-d)$-*idéal fractionnaire inversible* si $\mathcal{O}(-d)$ est l'ensemble des $\alpha \in K$ tels que $\alpha L \subset L$. Cela équivaut à dire que L est stable par multiplication par les éléments de $\mathcal{O}(-d)$, et est un $\mathcal{O}(-d)$-module projectif (nécessairement de rang 1). On vérifie que cela équivaut aussi à l'existence d'un nombre rationnel $\lambda > 0$ tel que $L\overline{L} = \lambda\mathcal{O}(-d)$, avec $\overline{L}$ le réseau conjugué de L. Ce nombre λ est alors noté $N(L)$ et appelé *norme* de L.

Les $\mathcal{O}(-d)$-idéaux fractionnaires inversibles forment un *groupe abélien* pour la loi de composition $(L, L') \mapsto LL'$ (si $L\overline{L} = \lambda\mathcal{O}(-d)$ et $L'\overline{L'} = \lambda'\mathcal{O}(-d)$, on a $LL'(\overline{LL'}) = \lambda\lambda'\mathcal{O}(-d)$); son élément neutre est $\mathcal{O}(-d)$ et l'opposé de L est $N(L)^{-1}\overline{L}$. Les $\mathcal{O}(-d)$-idéaux fractionnaires inversibles de la forme $\lambda\mathcal{O}(-d)$ avec $\lambda \in K^\times$ sont dits *principaux* et forment un sous-groupe du groupe précédent. Le groupe quotient est *le groupe des classes de* $\mathcal{O}(-d)$-*idéaux fractionnaires inversibles.* Il s'identifie canoniquement au groupe $\mathrm{Pic}(\mathcal{O}(-d))$ des classes de $\mathcal{O}(-d)$-modules projectifs de rang 1.

Etant donné un $\mathcal{O}(-d)$-idéal fractionnaire inversible L, et une base (ω_1, ω_2) d'orientation positive de L sur $\mathbf{Z}$, la forme quadratique $q(x, y) = N(L)^{-1} \mid x\omega_1 + y\omega_2 \mid^2$ est à coefficients entiers, primitive et de discriminant $-d$: cela résulte facilement de l'égalité $L\overline{L} = N(L)\mathcal{O}(-d)$. Inversement, étant donnée une forme quadratique $ax^2 + bxy + cy^2$ primitive et de discriminant $-d$, le réseau L de K engendré par a et $(b + i\sqrt{d})/2$ est un $\mathcal{O}(-d)$-idéal fractionnaire inversible, car on a $L\overline{L} = a\mathcal{O}(-d)$. On vérifie que les constructions précédentes définissent par passage au quotient des *isomorphismes réciproques l'un de l'autre* entre le groupe des classes de $\mathcal{O}(-d)$-idéaux fractionnaires inversibles et $Cl(-d)$, muni de la structure de groupe définie par Gauss.

L'*élément neutre* de $Cl(-d)$ est la classe de la forme $x^2 + (d/4)y^2$ si $d \equiv 0 \pmod 4$, celle de la forme $x^2 + xy + ((d+1)/4)y^2$ si $d \equiv 3 \pmod 4$. L'*opposé* de la classe de $ax^2 + bxy + cy^2$ est celle de $ax^2 - bxy + cy^2$. Le lemme du § 2 permet donc de dresser la liste des éléments d'ordre $\leqslant 2$ de $Cl(-d)$ (appelés *classes ambiguës* ou *ambiges*); le nombre de ces éléments est [1])

$$(9)\qquad \begin{array}{lll} 2^{t-1} & \text{si} & d \not\equiv 12 \bmod 16 \quad \text{et} \quad d \not\equiv 0 \bmod 32 \\ 2^{t-2} & \text{si} & d \equiv 12 \bmod 16 \\ 2^{t} & \text{si} & d \equiv 0 \bmod 32\,, \end{array}$$

où t est le nombre de diviseurs premiers de d.

Pour calculer le produit des classes de deux formes quadratiques $ax^2 + bxy + cy^2$ et $a'x^2 + b'xy + c'y^2$ primitives de discriminant $-d$, on pose [2])

$$\delta = \operatorname{pgcd}(a, a', (b+b')/2)\,,$$

on choisit des entiers u, v et w tels que

$$ua + va' + w(b+b')/2 = \delta\,,$$

et on pose

$$a'' = aa'/\delta^2\,,\quad b'' = [uab' + va'b + w(bb' - d)/2]/\delta\,,\quad c'' = (b''^2 + d)/4a''\,.$$

La forme quadratique $a''x^2 + b''xy + c''y^2$ est alors à coefficients entiers, primitive et de discriminant $-d$, et sa classe est le produit cherché.

En effet, aux classes des deux formes quadratiques données correspondent les classes des $\mathcal{O}(-d)$-idéaux fractionnaires: $L = \mathbf{Z}a + \mathbf{Z}(b + i\sqrt{d})/2$ et $L' = \mathbf{Z}a' + \mathbf{Z}(b' + i\sqrt{d})/2$. L'idéal fractionnaire LL' est engendré par les quatre éléments

$$aa'\,,\ (ab' + ai\sqrt{d})/2\,,\ (a'b + a'i\sqrt{d})/2\,,\ (bb' - d + i(b+b')\sqrt{d})/4$$

et l'on a $N(LL') = aa'$. On vérifie facilement que $\omega_1 = (aa')/\delta$ et $\omega_2 = \delta(b'' + i\sqrt{d})/2$ forment une base de LL' sur $\mathbf{Z}$ d'orientation positive et que l'on a $(aa')^{-1} \mid x\omega_1 + y\omega_2 \mid^2 = a''x^2 + b''xy + c''y^2$, d'où le résultat.

Exemple. Le groupe $Cl(-347)$ est cyclique d'ordre 5 (cf. § 3, exemple). Il est engendré par la classe C de la forme réduite $3x^2 + xy + 29y^2$, et

---

[1]) C.-F. GAUSS, *Disquisitiones Arithmeticae*, n° 257 à 259.

[2]) C.-F. GAUSS, *Disquisitiones Arithmeticae*, n° 242; cf. aussi le n° 243 pour des méthodes plus rapides de calcul du produit.

$2C$, $3C$, $4C$, $5C$ sont les classes des formes réduites dont les coefficients sont (9, 7, 11), (9, −7, 11), (3, −1, 29) et (1, 1, 87) respectivement.

§ 5. Lien entre $h(-d)$ et $h(-df^2)$ [1])

Soient $-d$ un *discriminant fondamental* (cf. § 3), et f un entier $\geqslant 1$. Les nombres de classes primitives $h(-df^2)$ et $h(-d)$ sont liés par une formule simple. Pour l'établir, nous allons définir un homomorphisme de groupes

$$v: Cl(-df^2) \to Cl(-d)\,.$$

C'est dans le langage des idéaux fractionnaires que cet homomorphisme se définit le plus aisément: à la classe d'un $\mathcal{O}(-df^2)$-idéal fractionnaire L, v fait correspondre la classe de $\mathcal{O}(-d)L$, qui est un $\mathcal{O}(-d)$-idéal fractionnaire.

Pour tout $x \in \mathcal{O}(-d)$, inversible modulo $f\mathcal{O}(-d)$, le réseau $x\mathcal{O}(-d) \cap \mathcal{O}(-df^2)$ est un $\mathcal{O}(-df^2)$-idéal fractionnaire. L'application qui à x associe la classe de cet idéal définit par passage au quotient un homomorphisme de groupes

$$u: \big(\mathcal{O}(-d)/f\mathcal{O}(-d)\big)^\times \to Cl(-df^2)\,.$$

On démontre (en utilisant le fait que « la donnée d'un réseau équivaut à celle de ses localisés ») que la suite

$$\big(\mathcal{O}(-d)/f\mathcal{O}(-d)\big)^\times \xrightarrow{u} Cl(-df^2) \xrightarrow{v} Cl(-d) \to 0$$

est exacte, et que le noyau de u est engendré par les classes des entiers relatifs inversibles modulo f et des unités de $\mathcal{O}(-d)$.

Un argument de comptage permet d'en déduire la formule

$$h(-df^2) = h(-d)w^{-1}f \prod_{\substack{p \mid f \\ p \text{ premier}}} \big(1 - p^{-1}\chi(p)\big)$$

où l'on a posé

$$w = \begin{array}{llll} 3 & \text{si} & d = 3 & \text{et} \quad f \geqslant 2 \\ 2 & \text{si} & d = 4 & \text{et} \quad f \geqslant 2 \\ 1 & \text{sinon}\,, & & \end{array}$$

et où χ désigne le caractère de Dirichlet quadratique $n \mapsto \left(\dfrac{-d}{n}\right)$ associé

[1]) C.-F. Gauss, *Disquisitiones Arithmeticae*, n° 253 à 256.

au corps $\mathbf{Q}(\sqrt{-d})$. On a en particulier si $d > 4$

$$h(-df^2) \geqslant h(-d)\varphi(f) \tag{10}$$

où φ est la fonction d'Euler.

II. Le problème du nombre de classes

Dans cette partie, nous allons étudier le comportement du nombre de classes lorsque le discriminant tend vers $-\infty$. Compte tenu des formules (8) de I. § 3 et (10) de I. § 5, il est légitime de restreindre notre étude aux discriminants fondamentaux (cf. I. § 3). Dans toute la suite, $-d$ sera un tel discriminant: on aura donc $\tilde{h}(-d) = h(-d)$.

Dans les derniers numéros de son exposé de la classification des formes quadratiques, Gauss émet quelques observations concernant les tables de nombres de classes (il avait constitué lui-même de telles tables, en particulier pour $d \leqslant 3000$); il qualifie de surprenante l'observation suivante [1]: pour chaque entier $h \geqslant 1$, il semble n'y avoir qu'un nombre *fini* de d tels que $h(-d) = h$. Ainsi, pour $h = 1$, ne trouve-t-il dans sa table que les neuf discriminants fondamentaux

$$-3, -4, -7, -8, -11, -19, -43, -67, -163$$

(et en outre les quatre discriminants non fondamentaux $-12, -16, -27, -28$).

Comme nous l'avons dit dans l'introduction, Heilbronn [2] en 1934 a démontré que, conformément à l'observation de Gauss, on a bien

$$\lim_{d \to \infty} h(-d) = +\infty . \tag{11}$$

Des tables étendues de nombres de classes ont été construites par ordinateur. Buell [3] par exemple a publié les valeurs de $h(-d)$ pour $d \leqslant 4\,000\,000$. Parmi les discriminants fondamentaux satisfaisant à cette inégalité, le nombre de ceux pour lesquels $h(-d)$ est égal à 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 est respectivement 9, 18, 16, 54, 25, 51, 31, 131, 34, 87, et

---

[1]) C.-F. Gauss, *Disquisitiones Arithmeticae*, n° 303.

[2]) H. Heilbronn, *On the class numbers in imaginary quadratic fields*, Quarterly J. of Math. (Oxford), 5 (1934), 150-160.

[3]) D. A. Buell, *Small class numbers and extreme values of L-functions of quadratic fields*, Math. of Comp. 31 (1977), 786-796.