Université de Montréal

Sur la répartition des unités dans les corps quadratiques réels

par

Marc-André Lacasse

Département de mathématiques et de statistique
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)
en mathématiques

Orientation Mathématiques pures

décembre 2011

Université de Montréal

Faculté des études supérieures

Ce mémoire intitulé

Sur la répartition des unités dans les corps quadratiques réels

présenté par

Marc-André Lacasse

a été évalué par un jury composé des personnes suivantes :

Matilde Lalín

(président-rapporteur)

Andrew Granville

(directeur de recherche)

Shabnam Akhtari

(membre du jury)

Mémoire accepté le:

22 décembre 2011

RÉSUMÉ

Ce mémoire s'emploie à étudier les corps quadratiques réels ainsi qu'un élément particulier de tels corps quadratiques réels : l'unité fondamentale. Pour ce faire, le mémoire commence par présenter le plus clairement possible les connaissances sur différents sujets qui sont essentiels à la compréhension des calculs et des résultats de ma recherche.

On introduit d'abord les corps quadratiques ainsi que l'anneau de ses entiers algébriques, et on décrit ce que sont ses unités. On parle ensuite des fractions continues puisqu'elles se retrouvent dans un algorithme de calcul de l'unité fondamentale. On traite ensuite des formes binaires quadratiques et de la formule du nombre de classes de Dirichlet, laquelle fait intervenir l'unité fondamentale en fonction d'autres variables.

Une fois cette tâche accomplie, on présente nos calculs et résultats. Notre recherche est à propos de la répartition des unités fondamentales des corps quadratiques réels, de la répartition des unités des corps quadratiques réels ainsi que des moments du logarithme de l'unité fondamentale. (Le logarithme de l'unité fondamentale est appelé le régulateur.)

Mots-clés : Corps quadratiques réels, Unité fondamentale, Régulateur, Nombre de classes, Fractions continues, Équation de Pell, Répartition des unités quadratiques, Fonctions-L de Dirichlet, Formule du nombre de classes de Dirichlet.

SUMMARY

This memoir aims to study real quadratic fields and a particular element of such real quadratic fields : the fundamental unit. To achieve this, the memoir begins by presenting as clearly as possible the state of knowledge on different subjects that are essential to understand the computations and results of my research.

We first introduce quadratic fields and their rings of algebraic integers, and we describe their units. We then talk about continued fractions because they are present in an algorithm to compute the fundamental unit. Afterwards, we proceed with binary quadratic forms and Dirichlet's class number formula, which involves the fundamental unit as a function of other variables.

Once the above tasks are done, we present our calculations and results. Our research concerns the distribution of fundamental units in real quadratic fields, the distribution of units in real quadratic fields and the moments of the logarithm of the fundamental unit. (The logarithm of the fundamental unit is called the regulator.)

Keywords : Real quadratic fields, Fundamental unit, Regulator, Class number, Continued fractions, Pell's equation, Distribution of quadratic units, Dirichlet L-function, Dirichlet's class number formula.

TABLE DES MATIÈRES

LISTE DES FIGURES

REMERCIEMENTS

Tout d'abord, je remercie profondément et chaleureusement Andrew Granville, mon directeur, pour son support et sa grande patience tout au long de ma maîtrise. J'ai apprécié avoir le privilège d'étudier sous sa direction.

Je remercie également Herman te Riele d'avoir partagé avec moi le programme qu'il a développé aux fins de vérification des heuristiques de Cohen-Lenstra.

Je remercie enfin mes proches pour leur soutien.

J'ai été boursier du CRSNG pendant ma maîtrise et je suis reconnaissant de leur support.

INTRODUCTION

Les corps quadratiques s'insèrent dans le concept plus général de corps de nombres algébriques. Les corps de nombres algébriques doivent leur existence aux tentatives de solutionner le Dernier Théorème de Fermat. Le 1$^{\text{er}}$ mars 1847, Gabriel Lamé annonça à l'Académie de Paris avoir solutionné le Dernier Théorème de Fermat. Sa solution s'appuyait sur la factorisation unique de certains entiers algébriques (les entiers cyclotomiques). Mais Ernst Kummer avait déjà montré trois ans auparavant que cette factorisation unique échouait parfois.

Un corps quadratique, bref, est une extension des nombres rationnels et correspond à l'ensemble

$$\left\{a + b\sqrt{d} \;\middle|\; a, b \in \mathbb{Q},\ \ d \in \mathbb{Z}\backslash\{0, 1\},\ \ d \text{ libre de carré}\right\} \;=\; \mathbb{Q}(\sqrt{d})$$

Le corps quadratique est dit réel si $d > 1$ et imaginaire si $d < 0$. Ce mémoire traite des corps quadratiques réels. Un corps quadratique réel possède un élément appelé l'unité fondamentale. (Dans un corps quadratique réel, une unité est un entier algébrique dont la multiplication par son conjugué donne ± 1. Et l'unité fondamentale est la plus petite unité qui soit supérieure à 1.) La grosseur de l'unité fondamentale en fonction de d (donc en fonction du corps quadratique) varie beaucoup. On essaie dans ce mémoire de comprendre un peu plus sa répartition.

Une formule faisant intervenir l'unité fondamentale est la formule du nombre de classes de Dirichlet. C'est une relation essentiellement entre l'unité fondamentale ε_d , le nombre de classes $h_i(d)$, d lui-même et une certaine fonction-L. La

formule s'écrit comme suit :

$$2 \cdot \log(\varepsilon_d) \cdot h_i(d) \quad = \quad \sqrt{D} \ \cdot \ L(1, \chi)$$

$L(1, \chi)$ est mieux connu, mais on connaît moins la variation de $\log(\varepsilon_d)$ et de $h_i(d)$ en fonction de d.

Dans ce mémoire, les calculs portent principalement sur la répartition des unités fondamentales des corps quadratiques réels (où $d > 0$), sur la répartition des unités des corps quadratiques réels et sur les moments du logarithme des unités fondamentales.
Par répartition des unités fondamentales des corps quadratiques réels, on entend le nombre de corps quadratiques réels $\mathbb{Q}(\sqrt{d})$, pour d borné inférieurement et supérieurement, dont l'unité fondamentale est égale à N, pour tout N.
Par répartition des unités des corps quadratiques réels, on entend le nombre de corps quadratiques réels $\mathbb{Q}(\sqrt{d})$, pour d borné inférieurement et supérieurement, dont au moins une unité est égale à N, pour différents $N \in \mathbb{N}$.
Un des objectifs est de vérifier si les résultats des calculs peuvent concorder avec une hypothèse de Granville sur la répartition des unités quadratiques.

Tout au long du mémoire, une attention particulière fut portée à ce que les sujets soient présentés simplement et avec moults détails pour que la lecture du mémoire soit aisée pour un lecteur n'ayant aucune connaissance préalable dans ce domaine.

Chapitre 1

NOMBRES ALGÉBRIQUES

Historiquement, la théorie des nombres algébriques n'est pas étrangère au désir de résoudre des équations diophantiennes, c'est-à-dire la résolution d'équations par des valeurs entières ou rationnelles. La théorie des nombres algébriques s'est également développée conjointement avec le désir et les tentatives de solutionner le dernier théorème de Fermat - qui stipule que l'équation $x^n + y^n = z^n$ n'a aucune solution en entiers x, y, z strictement positifs pour tout $n \geq 3$.

Les nombres algébriques sont les racines de certains polynômes. Les polynômes dont il sera question seront des polynômes à coefficients rationnels ou entiers. La famille des polynômes à une variable et à coefficients rationnels est notée $\mathbb{Q}[x]$, où $\mathbb{Q}$ est le corps des nombres rationnels. De la même façon, $\mathbb{Z}[x]$ représente l'ensemble des polynômes à une variable et à coefficients dans $\mathbb{Z}$, l'ensembles des entiers rationnels. Généralement, $F[x]$ dénote l'ensemble des polynômes à une variable et à coefficients dans un ensemble F quelconque.

Dans un polynôme $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n$, $a_0 \neq 0$, "n" est appelé le degré du polynôme. Si $a_0 = 1$, on dit que le polynôme est monique (ou unitaire). Par ailleurs, pour le polynôme $f(x) = a_0x^0$, où $a_0 = 0$, le degré du polynôme est 0.

Définition 1.0.1. *Un polynôme $f(x)$ non nul est IRRÉDUCTIBLE, ou PREMIER, par rapport à $\mathbb{Q}$ s'il n'existe pas de factorisation $f(x) = g(x) \cdot h(x)$ avec*

$g(x), h(x) \in \mathbb{Q}[x]$ et avec $g(x)$ et $h(x)$ étant en outre de degré plus grand ou égal à 1.

Maintenant que nous avons introduit certaines notions sur les polynômes, nous sommes prêts à définir les nombres algébriques.

Définition 1.0.2. *Un nombre complexe ξ est appelé un NOMBRE ALGÉBRIQUE s'il satisfait une équation polynomiale $f(x) = 0$, où $f(x) \in \mathbb{Z}[x]$, c'est-à-dire où $f(x)$ est un polynôme à coefficients dans $\mathbb{Z}$, et où $f(x)$ n'est pas identiquement nul.*

Remarque 1.0.1. *On peut étendre la notion de nombre algébrique à d'autres corps que les nombres complexes.*

Théorème 1.0.1. *Un nombre algébrique ξ satisfait un unique polynôme monique et irréductible $g(x)$ tel que $g(x) = 0$, où $g(x) \in \mathbb{Q}[x]$.*
De plus, tout polynôme $f(x) \in \mathbb{Q}[x]$ ayant ξ pour racine est divisible par $g(x)$.

Démonstration. De toutes les équations polynomiales dans $\mathbb{Q}[x]$ satisfaites par ξ, on en choisit une de degré minimal, disons $G(x) = 0$. Si le coefficient du terme dominant de $G(x)$ est c, on définit $g(x) = c^{-1} \cdot G(x)$. Ainsi $g(\xi) = 0$ et $g(x)$ est monique.
Le polynôme $g(x)$ est également irréductible. S'il ne l'était pas, on aurait $g(x) = h_1(x) \cdot h_2(x)$. On aurait alors que soit $h_1(\xi) = 0$ ou $h_2(\xi) = 0$ ou les deux, ce qui contredirait le fait que $G(x)$ et $g(x)$ sont des polynômes de degré minimal ayant ξ pour racine.
Maintenant soit $f(x) \in \mathbb{Q}[x]$ ayant ξ pour racine. Par la division euclidienne pour les polynômes, il existe $q(x), r(x) \in \mathbb{Q}[x]$ tels que $f(x) = g(x) \cdot q(x) + r(x)$, où degré($r$)<degré($g$). Alors $r(x)$ se doit d'être identiquement nul, sinon on aurait $r(\xi) = 0$ puisque $f(\xi) = 0 = g(\xi)$, ce qui contredirait le fait que $g(x)$ est de degré minimal parmi les polynômes $\in \mathbb{Q}[x]$ ayant ξ pour racine. Ainsi $g(x)|f(x)$.
Enfin, on prouve l'unicité de $g(x)$. Supposons que $g_1(x) \in \mathbb{Q}[x]$ soit un autre

polynôme monique et irréductible tel que $g_1(\xi) = 0$. On vient de démontrer que $g(x)|g_1(x)$, c'est-à-dire $g_1(x) = g(x) \cdot q(x)$. Mais $g_1(x)$ est irréductible implique que $q(x)$ soit une constante ; en fait $q(x) = 1$ puisque $g_1(x)$ et $g(x)$ sont moniques. Donc $g_1(x) = g(x)$. □

Définition 1.0.3. *Le POLYNÔME MINIMAL d'un nombre algébrique ξ est le polynôme $g(x)$ décrit au théorème précédent.*
Le DEGRÉ d'un nombre algébrique est le degré de son polynôme minimal.

Définition 1.0.4. *Un nombre algébrique ξ est un ENTIER ALGÉBRIQUE s'il est racine d'un polynôme monique $f(x) = x^n + b_1 x^{n-1} + ... + b_n$ à coefficients dans $\mathbb{Z}$, c'est-à-dire d'un polynôme monique $f(x) \in \mathbb{Z}[x]$.*

Remarque 1.0.2. *L'ensemble de tous les nombres algébriques forme un corps.*
L'ensemble de tous les entiers algébriques forme un anneau.

Pour vérifier cela, on n'a qu'à vérifier les propriétés des corps et des anneaux. Certaines sont tout à fait directes (puisque nous sommes dans les nombres complexes).

Définition 1.0.5. *Soit F l'ensemble de tous les nombres algébriques (F est un corps). On appelle un CORPS DE NOMBRES ALGÉBRIQUES n'importe quel sous-corps $E \subset F$ tel que E soit une extension finie de $\mathbb{Q}$.*

Théorème 1.0.2. *Soient $\mathbb{Q}$ le corps des nombres rationnels et α un nombre algébrique de degré n. Soit $\mathbb{Q}(\alpha) = \{f(\alpha) \mid f(x) \in \mathbb{Q}[x]\} = \{f(\alpha) \mid f(x)$ est un polynôme à coefficients dans $\mathbb{Q}\}$. Alors $\mathbb{Q}(\alpha)$ est un corps.*
Remarque 1.0.3. *On appelle $\mathbb{Q}(\alpha)$ le corps de nombres algébriques engendré par α.*
Le degré $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ de $\mathbb{Q}(\alpha)$ par rapport à $\mathbb{Q}$ est égal au degré de α.

DÉMONSTRATION. $f(\alpha) \in \mathbb{C}$ donc $\mathbb{Q}(\alpha) \subseteq \mathbb{C}$. $\mathbb{Q}(\alpha)$ est donc associatif et commutatif pour l'addition et la multiplication. Il respecte aussi la distributivité. 0 et 1 sont ses éléments neutres pour l'addition et la multiplication.
Inverse additif : $-f(\alpha) \in \mathbb{Q}(\alpha)$.
Fermeture : $f(\alpha) + g(\alpha) \in \mathbb{Q}(\alpha)$ et $f(\alpha) \cdot g(\alpha) \in \mathbb{Q}(\alpha)$
Inverse multiplicatif : Soit $f(\alpha) \in \mathbb{Q}(\alpha), f(\alpha) \neq 0$. Et soit $g(x)$ le polynôme minimal de α. $g(x)$ est irréductible et $f(x)$ est tel que $f(\alpha) \neq 0$. Donc $f(x)$ et $g(x)$ sont relativement premiers et alors il existe $r(x), s(x) \in \mathbb{Q}[x]$ tels que $f(x) \cdot r(x) + g(x) \cdot s(x) = 1$. En remplaçant x par α, ça donne $f(\alpha) \cdot r(\alpha) = 1$. Et $r(\alpha)$ est l'inverse multiplicatif de $f(\alpha)$. □

Théorème 1.0.3. *Soit α un nombre algébrique de degré n. Alors tout nombre $f(\alpha) \in \mathbb{Q}(\alpha)$ peut s'écrire uniquement sous la forme $a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$, où $a_0, ..., a_{n-1} \in \mathbb{Q}$.*

DÉMONSTRATION. Soit $g(x)$ le polynôme minimal de α.
Par la division euclidienne, il existe $q(x), r(x) \in \mathbb{Q}[x]$ tels que $f(x) = g(x) \cdot q(x) + r(x)$, où $deg(r) < deg(g) = n$.
En remplaçant x par α, on obtient $f(\alpha) = r(\alpha)$, où $deg(r) \leq n - 1$.

Pour l'unicité maintenant. Soit $f(\alpha) \in \mathbb{Q}(\alpha)$ un nombre. Supposons qu'on puisse écrire ce nombre de deux façons différentes sous la forme $a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$. Appelons $r(\alpha)$ et $r_1(\alpha)$ ces deux façons. Ce sont deux façons distinctes, alors $r(x) \neq r_1(x)$ (par $\neq$ ici on veut dire n'est pas identiquement égal à). Donc $r(x) - r_1(x) \neq 0$ est un polynôme de degré $\leq n - 1$ avec $r(\alpha) - r_1(\alpha) = 0$, ce qui donne un polynôme non nul de degré $< n$ ayant α pour racine, ce qui contredit le fait que $g(x)$ est le polynôme minimal de α. □

Définition 1.0.6. - *Un entier algébrique α est DIVISIBLE par un entier algébrique β s'il existe un entier algébrique γ tel que $\alpha = \beta \cdot \gamma$. On dit aussi dans ce cas que β est un DIVISEUR de α. On peut noter $\beta|\alpha$.*

- Un entier algébrique ε est une UNITÉ (donc inversible) s'il existe un entier algébrique β tel que $\varepsilon \cdot \beta = 1$.
- Deux entiers algébriques α et β sont ASSOCIÉS s'il existe une unité ε telle que $\alpha = \varepsilon \cdot \beta$.

Remarque 1.0.4. *- Si ε_1 est une unité, alors son inverse l'est aussi. En effet, il existe un entier algébrique ε_2 tel que $\varepsilon_1 \cdot \varepsilon_2 = 1$. Pour ε_2, il existe donc l'entier algébrique ε_1 tel que $\varepsilon_1 \cdot \varepsilon_2 = 1$.*
De plus, le produit de deux unités ε_1 et ε_3 est une unité. En effet, il existe un entier algébrique ε_4 tel que $\varepsilon_3 \cdot \varepsilon_4 = 1$. Donc $\varepsilon_1 \cdot \varepsilon_3$ est tel qu'il existe un entier algébrique $\varepsilon_2 \cdot \varepsilon_4$ avec $(\varepsilon_1 \cdot \varepsilon_3) \cdot (\varepsilon_2 \cdot \varepsilon_4) = 1$. C'est-à-dire que $\varepsilon_1 \cdot \varepsilon_3$ est une unité.
- Ce que nous venons d'écrire ci-haut dans la remarque nous permet d'affirmer que les unités d'un corps de nombre algébrique forment un groupe multiplicatif.
- Si α et β sont associés, alors β et α le sont aussi. En effet, soit ε une unité telle que $\alpha = \varepsilon \cdot \beta$. Nous avons que ε est une unité alors il existe γ un entier algébrique tel que $\varepsilon \cdot \gamma = 1$. Ainsi $\gamma \cdot \alpha = \gamma \cdot \varepsilon \cdot \beta = \beta$ d'où $\beta = \gamma \cdot \alpha$, où γ est une unité.

Définition 1.0.7. *Soit R l'anneau des entiers algébriques dans un corps de nombres algébriques K.*

- *Un entier algébrique a est IRRÉDUCTIBLE si chaque diviseur de a dans R est son associé ou une unité.*
- *R est un DOMAINE DE FACTORISATION UNIQUE si tout élément de R peut être exprimé de façon unique comme un produit d'éléments irréductibles.*

Références spécifiques à ce chapitre :

Alan Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, 1984.
Ivan Niven, Herbert S. Zuckerman et Hugh L. Montgomery, *An introduction to the theory of numbers, Fifth edition*, Jon Wiley & Sons, 1991.

Chapitre 2

CORPS QUADRATIQUES

Nous travaillerons principalement par la suite avec un type particulier de corps de nombres algébriques. Il s'agit de $\mathbb{Q}(\alpha)$, lorsque α est un nombre algébrique de degré deux.

Définition 2.0.8. *Soit α un nombre algébrique de degré deux. $\mathbb{Q}(\alpha)$ est appelé un CORPS QUADRATIQUE.*

Nous avons démontré que $\mathbb{Q}(\alpha) = \{f(\alpha)|f(x) \in \mathbb{Q}[x]\}$ est un corps. Nous avons aussi démontré que si $f(\alpha) \in \mathbb{Q}(\alpha)$, alors $f(\alpha)$ peut s'écrire uniquement sous la forme $a_0 + a_1\alpha$, où $a_0, a_1 \in \mathbb{Q}$. Ainsi $\{f(\alpha)|f(x) \in \mathbb{Q}[x]\} \subseteq \{u + v\alpha|u, v \in \mathbb{Q}\}$. De plus, $u + vx \in \mathbb{Q}[x]$. Donc $\{u + v\alpha|u, v \in \mathbb{Q}\} \subseteq \{f(\alpha)|f(x) \in \mathbb{Q}[x]\}$. Ainsi $\mathbb{Q}(\alpha) = \{u + v\alpha|u, v \in \mathbb{Q}\}$.

α est un nombre algébrique de degré deux. Soit $g(x) = b_0 + b_1x + b_2x^2$ le polynôme minimal de α, où $b_0, b_1, b_2 \in \mathbb{Q}$. $g(\alpha) = 0$.
Ainsi $b_0 + b_1\alpha + b_2\alpha^2 = 0 \Rightarrow \alpha = \frac{-b_1 \pm \sqrt{b_1^2 - 4b_2b_0}}{2b_2} = \frac{a+b\sqrt{d}}{c}$ où $a, b, c, d \in \mathbb{Z}$ et où $c \neq 0$ car sinon α ne serait pas de degré deux. (En multipliant $b_0, b_1, b_2 \in \mathbb{Q}$ par le ppcm de leur dénominateur, ils deviennent des entiers. Considérons-les comme des entiers.)

Ici on écrit $b_1^2 - 4b_2b_0 = b'^2 \cdot d$ où $d \in \mathbb{Z}$ est libre de carré. Ainsi $b = \pm b'$, $a = -b_1, c = 2b_2$.
De plus, $d \neq 1$ car sinon on aurait $\alpha = \frac{a+b}{c} \in \mathbb{Q}$ et α serait de degré au plus 1.

De même, $d \neq 0$ et $b \neq 0$ car sinon on aurait $\alpha = \frac{a}{c} \in \mathbb{Q}$ et α serait de degré au plus 1.

Tentons de voir si on pourrait exprimer le corps quadratique $\mathbb{Q}(\alpha) = \{u + v\alpha \mid u, v \in \mathbb{Q}\}$ plutôt en fonction de $\sqrt{d}$. On sait que α peut s'écrire $\alpha = \frac{a+b\sqrt{d}}{c}$.

Alors $u + v\alpha = u + v\left(\frac{a+b\sqrt{d}}{c}\right) = u + \frac{va}{c} + \frac{vb\sqrt{d}}{c} = u' + v'\sqrt{d}$ avec $u', v' \in \mathbb{Q}$.
Ainsi $\{u + v\alpha \mid u, v \in \mathbb{Q}\} \subseteq \{u' + v'\sqrt{d} \mid u', v' \in \mathbb{Q}\}$.

Aussi $u' + v'\sqrt{d} = u' + v'(\frac{c\alpha - a}{b}) = (u' - \frac{av'}{b}) + \frac{v'c}{b}\alpha = u + v\alpha$ avec $u, v \in \mathbb{Q}$ car $b \neq 0$.
Ainsi $\{u' + v'\sqrt{d} \mid u', v' \in \mathbb{Q}\} \subseteq \{u + v\alpha \mid u, v \in \mathbb{Q}\}$.

Bref, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$. Tout corps quadratique peut donc s'écrire sous la forme $\mathbb{Q}(\sqrt{d})$, où

$$d \in \mathbb{Z} \text{ est libre de carré}, d \neq 0 \text{ et } d \neq 1. \tag{2.0.1}$$

Réciproquement, soit un tel d. Alors $\sqrt{d}$ est un nombre algébrique de degré deux. D'où $\mathbb{Q}(\sqrt{d})$ est un corps quadratique.

Mentionnons que si d_1 et d_2 respectent la condition (2.0.1) avec $d_1 \neq d_2$, alors $\mathbb{Q}(\sqrt{d_1}) \neq \mathbb{Q}(\sqrt{d_2})$. En effet, $\sqrt{d_1} \in \mathbb{Q}(\sqrt{d_1})$. Supposons que $\sqrt{d_1} \in \mathbb{Q}(\sqrt{d_2})$, alors $\sqrt{d_1} = u + v\sqrt{d_2} \Longrightarrow d_1 = (u + v\sqrt{d_2})^2 \Longrightarrow d_1 = u^2 + 2uv\sqrt{d_2} + v^2 d_2 \Longrightarrow 2uv\sqrt{d_2} = d_1 - u^2 - v^2 d_2 \in \mathbb{Q}$.
Si $u = 0$, alors $\sqrt{d_1} = v\sqrt{d_2} \Longrightarrow d_1 = v^2 d_2$ or d_1 libre de carré $\Longrightarrow v^2 = 1 \Longrightarrow d_1 = d_2$, une contradiction.
Si $v = 0$, alors $\sqrt{d_1} = u \Longrightarrow d_1 = u^2$ or d_1 libre de carré $\Longrightarrow d_1 = u^2 = 1$, une contradiction car $d_1 \neq 1$.
Donc $\sqrt{d_2} = \frac{d_1 - u^2 - v^2 d_2}{2uv}$ et $\frac{d_1 - u^2 - v^2 d_2}{2uv} \in \mathbb{Q}$, une contradiction.
Ainsi $\sqrt{d_1} \notin \mathbb{Q}(\sqrt{d_2})$ et donc on a bien que $\mathbb{Q}(\sqrt{d_1}) \neq \mathbb{Q}(\sqrt{d_2})$.

Définition 2.0.9. *Le CONJUGUÉ* $\overline{x}$ *d'un élément* $x = u + v\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ *est* $\overline{x} = u - v\sqrt{d}$.
La NORME $N(x)$ *d'un élément* $x = u + v\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ *est le produit de* x *par son conjugué. C'est-à-dire* $N(x) = x\overline{x} = (u + v\sqrt{d})(u - v\sqrt{d}) = u^2 - dv^2$.

Remarque 2.0.5. - *Soient* $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$. *Disons* $\alpha = u_1 + v_1\sqrt{d}, \beta = u_2 + v_2\sqrt{d}$. *Alors* $\overline{\alpha\beta} = \overline{(u_1 + v_1\sqrt{d})(u_2 + v_2\sqrt{d})} = \overline{u_1u_2 + u_1v_2\sqrt{d} + u_2v_1\sqrt{d} + dv_1v_2} = u_1u_2 + dv_1v_2 - (u_1v_2 + u_2v_1)\sqrt{d} = (u_1 - v_1\sqrt{d})(u_2 - v_2\sqrt{d}) = \overline{\alpha}\overline{\beta}$.
- *On a aussi* $N(\alpha\beta) = \alpha\beta \cdot \overline{\alpha\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$.
- *Et* $N(\alpha) = 0 \Longleftrightarrow \alpha = 0$. *En effet,* $N(\alpha) = 0 \Leftrightarrow \alpha\overline{\alpha} = 0 \Leftrightarrow (\alpha = 0$ *ou* $\overline{\alpha} = 0)$. *Or* $\overline{\alpha} = 0 \Leftrightarrow \alpha = 0$.

Références spécifiques à ce chapitre :

Alan Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, 1984.

Ivan Niven, Herbert S. Zuckerman et Hugh L. Montgomery, *An introduction to the theory of numbers, Fifth edition*, Jon Wiley & Sons, 1991.

Chapitre 3

ENTIERS ALGÉBRIQUES DES CORPS QUADRATIQUES

On se souvient qu'un nombre algébrique α est un entier algébrique s'il est racine d'un polynôme monique $f(x) \in \mathbb{Z}[x]$. On peut donc se demander quels sont les entiers algébriques dans un corps quadratique $\mathbb{Q}(\sqrt{d})$.

Théorème 3.0.4. *Soit θ l'ensemble des entiers algébriques de $\mathbb{Q}(\sqrt{d})$.*
Alors

$$\theta = \begin{cases} \{u + v\sqrt{d} | u, v \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{d}] & \text{si } d \equiv 2 \text{ ou } 3 \text{ mod } 4 \\ \{\frac{u'+v'\sqrt{d}}{2} | u', v' \in \mathbb{Z} \text{ et } u' \equiv v' \text{ mod } 2\} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{si } d \equiv 1 \text{ mod } 4 \end{cases} \tag{3.0.2}$$

Démonstration. Soit α un entier algébrique de $\mathbb{Q}(\sqrt{d})$.
Si α est de degré 1, soit $g(x) = x + b_0$ son polynôme minimal $\Rightarrow \alpha \in \mathbb{Z}$ et on peut écrire $\alpha = u + 0\sqrt{d}$ si $d \equiv 2$ ou 3 mod 4 ou $\alpha = \frac{u'+0\sqrt{d}}{2}$ avec $u' \equiv 0$ mod 2 si $d \equiv 1$ mod 4.
Sinon α est de degré 2 et soit $g(x) = x^2 + b_1 x + b_0$ le polynôme minimal de α, où $b_0, b_1 \in \mathbb{Z}$. Alors $\alpha = \frac{-b_1 \pm \sqrt{b_1^2 - 4b_0}}{2}$.
Donc on peut écrire $\alpha = \frac{u+v\sqrt{d}}{2}$, où $u, v \in \mathbb{Z}$.
$b_0 = \alpha\overline{\alpha} = \left(\frac{u+v\sqrt{d}}{2}\right)\left(\frac{u-v\sqrt{d}}{2}\right) = \frac{u^2-dv^2}{4}$ et $b_0 \in \mathbb{Z} \Rightarrow u^2 \equiv dv^2 \bmod 4$
$\Rightarrow u \equiv u^2 \equiv dv^2 \equiv dv \mod 2$

Si $d \equiv 1 \bmod 4$, alors $u \equiv v \bmod 2$.
Si $d \equiv 2 \bmod 4$, alors $u \equiv dv \equiv 0 \bmod 2$. Et donc $0 \equiv u^2 \equiv dv^2 \equiv 2v^2 \bmod 4 \Rightarrow v \equiv 0 \bmod 2$
Si $d \equiv 3 \bmod 4$, alors $u \equiv dv \equiv v \mod 2$. Si $u \equiv v \equiv 1 \mod 2$, alors $1 \equiv u^2 \equiv dv^2 \equiv 3 \cdot 1 \equiv 3 \mod 4$, une contradiction. Donc u et v sont pairs.

Bref, on a donc montré jusqu'ici que

$$\theta \subseteq \begin{cases} \{u + v\sqrt{d} \mid u, v \in \mathbb{Z}\} & \text{si } d \equiv 2 \text{ ou } 3 \bmod 4 \\ \left\{ \frac{u'+v'\sqrt{d}}{2} \;\middle|\; u', v' \in \mathbb{Z} \text{ et } u' \equiv v' \bmod 2 \right\} & \text{si } d \equiv 1 \bmod 4 \end{cases} \tag{3.0.3}$$

Réciproquement,

Si $d \equiv 2$ ou $3 \bmod 4$: Soit $\alpha = u + v\sqrt{d}$ avec $u, v \in \mathbb{Z}$. Alors $(\alpha - u)^2 = dv^2 = \alpha^2 - 2u\alpha + u^2$.
Donc α est racine de $x^2 - 2ux + u^2 - dv^2$, un polynôme monique à coefficients dans $\mathbb{Z}$. Ainsi α est un entier algébrique de $\mathbb{Q}(\sqrt{d})$.

Si $d \equiv 1 \bmod 4$: Soit $\alpha = \frac{u'+v'\sqrt{d}}{2}$ avec $u', v' \in \mathbb{Z}$ et $u' \equiv v' \bmod 2$.
Alors $(2\alpha - u')^2 = dv'^2 = 4\alpha^2 - 4\alpha u' + u'^2 \Longrightarrow$
$4(\alpha^2 - u'\alpha) + u'^2 - dv'^2 = 0$.
Donc α est racine de $x^2 - u'x + \frac{u'^2 - dv'^2}{4}$, un polynôme monique qui est à coefficients dans $\mathbb{Z}$ puisque $u' \equiv v' \bmod 2$ et donc $u'^2 - dv'^2 \equiv 0 \bmod 4$, c'est-à-dire $u'^2 - dv'^2$ est un multiple de 4, d'où $\frac{u'^2 - dv'^2}{4} \in \mathbb{Z}$.
Ainsi α est un entier algébrique de $\mathbb{Q}(\sqrt{d})$.

□

Rappelons que selon la définition (1.0.6), un entier algébrique ε de $\mathbb{Q}(\sqrt{d})$ est une unité s'il existe un entier algébrique β de $\mathbb{Q}(\sqrt{d})$ tel que $\varepsilon\beta = 1$.

Théorème 3.0.5. *Soit α un entier algébrique de $\mathbb{Q}(\sqrt{d})$. Alors $N(\alpha) \in \mathbb{Z}$. De plus, $N(\alpha) = \pm 1 \Longleftrightarrow \alpha$ est une unité.*

Démonstration. Soit $\alpha = u + v\sqrt{d}$. Nous avons vu dans la preuve du théorème précédent que si $g(x) = x^2 + b_1 x + b_0$ est le polynôme minimal de α, alors $b_1 = -2u = -(\alpha + \overline{\alpha})$ et $4b_0 = 4u^2 - 4dv^2 \Rightarrow b_0 = u^2 - dv^2 = N(\alpha)$. On peut écrire $g(x) = x^2 - (\alpha + \overline{\alpha})x + N(\alpha)$. Or $b_0 \in \mathbb{Z}$ alors $N(\alpha) \in \mathbb{Z}$.
Si α n'est pas de degré 2 mais est plutôt de degré 1, alors $\alpha \in \mathbb{Z}$ et $N(\alpha) = \alpha\overline{\alpha} = \alpha\alpha = \alpha^2 \in \mathbb{Z}$.

De plus, $N(\alpha) = \pm 1 \Rightarrow \alpha\overline{\alpha} = \pm 1 \Rightarrow \alpha(\pm\overline{\alpha}) = 1$.
Or, $\overline{\alpha}$ est aussi un entier algébrique puisque solution de $x^2 - (\alpha + \overline{\alpha})x + N(\alpha)$ et $-\overline{\alpha}$ est aussi un entier algébrique puisque solution de $x^2 + (\alpha + \overline{\alpha})x + N(\alpha)$. Bref, α est une unité.

Réciproquement, si α est une unité, alors il existe un entier algébrique β tel que $\alpha\beta = 1$. Donc $N(\alpha\beta) = N(1) \Rightarrow N(\alpha)N(\beta) = 1 \Rightarrow N(\alpha) = \pm 1$ puisque $N(\alpha), N(\beta) \in \mathbb{Z}$. □

Selon le fait que d soit positif ou négatif, le corps quadratique $\mathbb{Q}(\sqrt{d})$ sera appelé réel ou imaginaire.

Définition 3.0.10. *Le corps quadratique $\mathbb{Q}(\sqrt{d})$ est dit RÉEL si $d > 1$ et il est dit IMAGINAIRE si $d < 0$.*

Références spécifiques à ce chapitre :

Alan Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, 1984.
Ivan Niven, Herbert S. Zuckerman et Hugh L. Montgomery, *An introduction to the theory of numbers, Fifth edition*, Jon Wiley & Sons, 1991.

Chapitre 4

LES UNITÉS DANS LES CORPS QUADRATIQUES IMAGINAIRES

Soit $\mathbb{Q}(\sqrt{d})$ un corps quadratique imaginaire ($d < 0$). Soit $\alpha = u + v\sqrt{d}$ un entier algébrique de $\mathbb{Q}(\sqrt{d})$. Alors α est une unité de ce corps quadratique imaginaire $\Longleftrightarrow \pm 1 = N(\alpha) = \alpha\overline{\alpha} = (u+v\sqrt{d})(u-v\sqrt{d}) = u^2 - dv^2 = u^2 + (-d)v^2 > 0$

Si $d \equiv 2$ ou $3 \bmod 4$, $d \neq -1$, les unités $\alpha = u + v\sqrt{d}$ sont solution de $u^2 + (-d)v^2 = 1$, avec $u, v \in \mathbb{Z}$.
Or, $d < -1 \Rightarrow -d > 1 \Rightarrow 1 = u^2 + (-d)v^2 \geq (-d)v^2 > v^2 \Rightarrow v = 0 \Rightarrow u = \pm 1$
D'où les seules et uniques unités de $\mathbb{Q}(\sqrt{d})$ pour $d \equiv 2$ ou $3 \bmod 4$, $d \neq -1$, sont ± 1.

Si $d = -1$, les unités $\alpha = u + v\sqrt{d}$ sont solution de $u^2 + 1 \cdot v^2 = 1$, avec $u, v \in \mathbb{Z}$. Or, $1 = u^2 + v^2 \geq u^2 \Rightarrow |u| \leq 1$. De même, $|v| \leq 1$.
Donc, parmi ces possibilités, on a $u^2 + v^2 = 1$ seulement pour $u = \pm 1, v = 0$ ou pour $u = 0, v = \pm 1$.
D'où les seules et uniques unités de $\mathbb{Q}(\sqrt{-1})$ sont ± 1 et $\pm\sqrt{-1}$.

Si $d \equiv 1 \bmod 4$, $d \neq -3$, les unités $\alpha = \frac{u+v\sqrt{d}}{2}$ sont solution de
$1 = \frac{(u+v\sqrt{d})}{2}\frac{(u-v\sqrt{d})}{2} = \frac{u^2+(-d)v^2}{4} \Leftrightarrow u^2 + (-d)v^2 = 4$ où $u, v \in \mathbb{Z}$, $u \equiv v \bmod 2$
Or, $d \leq -7 \Rightarrow -d \geq 7 \Rightarrow 4 = u^2 + (-d)v^2 \geq (-d)v^2 \geq 7v^2 \Rightarrow v = 0 \Rightarrow u = \pm 2 \Rightarrow \alpha = \frac{u+v\sqrt{d}}{2} = \pm 1$

D'où les seules et uniques unités de $\mathbb{Q}(\sqrt{d})$ pour $d \equiv 1 \bmod 4$, $d \neq -3$, sont ± 1.

Si $d = -3$, les unités $\alpha = \frac{u+v\sqrt{d}}{2}$ sont solution de $1 = \alpha\overline{\alpha} = \frac{u^2+3v^2}{4} \Leftrightarrow u^2 + 3v^2 = 4$ où $u, v \in \mathbb{Z},\ u \equiv v \bmod 2$
Or, $4 = u^2 + 3v^2 \geq 3v^2 \Rightarrow |v| \leq 1$. Si $v = \pm 1$, alors $u = \pm 1$. Et si $v = 0$, alors $u = \pm 2$.
D'où les seules et uniques unités de $\mathbb{Q}(\sqrt{-3})$ sont ± 1 et $\frac{\pm 1 \pm \sqrt{-3}}{2}$.

Nous avons donc prouvé ce qui suit :

Théorème 4.0.6. *Soit $\mathbb{Q}(\sqrt{d})$ un corps quadratique imaginaire.*
Si $d \neq -1$ et $d \neq -3$, alors $\{\xi \in \mathbb{Q}(\sqrt{d}) \mid \xi \text{ est une unité }\} = \{\pm 1\}$
Par ailleurs, $\{\xi \in \mathbb{Q}(\sqrt{-1}) \mid \xi \text{ est une unité }\} = \{\pm 1, \pm\sqrt{-1}\}$
$\{\xi \in \mathbb{Q}(\sqrt{-3}) \mid \xi \text{ est une unité }\} = \left\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\right\}$

Ceci étant dit, à partir de maintenant, nous travaillerons avec les corps quadratiques réels.

Références spécifiques à ce chapitre :

Alan Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, 1984.

Chapitre 5

LES UNITÉS DANS LES CORPS QUADRATIQUES RÉELS

Soit $\mathbb{Q}(\sqrt{d})$ un corps quadratique réel. Soit $\alpha = u + v\sqrt{d}$ un entier algébrique de $\mathbb{Q}(\sqrt{d})$. Alors α est une unité de ce corps quadratique réel $\iff \pm 1 = N(\alpha) = \alpha\overline{\alpha} = (u + v\sqrt{d})(u - v\sqrt{d}) = u^2 - dv^2$.

Nous voulons montrer qu'il y a une infinité d'unités dans $\mathbb{Q}(\sqrt{d})$ un corps quadratique réel. Nous montrerons également sous quelle forme on peut écrire ces unités. Pour ce faire, nous aurons besoin du lemme suivant :

Lemme 5.0.1 (Théorème de Dirichlet)**.** *Soit $\xi \in \mathbb{R}\backslash\mathbb{Q}$ un nombre irrationnel. Pour tout $n \in \mathbb{N}$, il existe $p, q \in \mathbb{Z}$ tels que $0 < q \leq n$ et tels que $\left|\xi - \frac{p}{q}\right| < \frac{1}{qn}$.*

Démonstration. Notons par $\{x\} = x - \lfloor x \rfloor$ la partie fractionnaire du nombre réel x.

Considérons les $n + 1$ nombres : $0, \{\xi\}, \{2\xi\}, ..., \{n\xi\}$, qui sont compris entre 0 et 1 et qui sont donc distribués à l'intérieur des n intervalles $[\frac{s}{n}, \frac{s+1}{n}[$ pour $s = 0, 1, 2, ..., n - 1$.

Par le principe des tiroirs, comme il y a $n + 1$ nombres dans n intervalles, il doit forcément y avoir deux de ces nombres dans un même intervalle. Soient $\{q_1\xi\}$ et $\{q_2\xi\}$ ces deux nombres tels que $|\{q_1\xi\} - \{q_2\xi\}| < \frac{1}{n}$. Supposons, sans perdre de généralité, que $q_2 > q_1$ et posons $q = q_2 - q_1$. Alors $0 < q \leq n$ et $\min\{|q\xi - m| \ : \ m \in \mathbb{Z}\} < \frac{1}{n}$. Il existe donc $p \in \mathbb{Z}$ tel que $|q\xi - p| < \frac{1}{n}$. □

Théorème 5.0.7. *Soit $\mathbb{Q}(\sqrt{d})$ un corps quadratique réel. Alors ce corps contient une infinité d'unités.*

Démonstration. Supposons que η soit une unité $\neq \pm 1$. (Nous montrerons par la suite qu'une telle unité existe.) Donc $N(\eta) = \pm 1$. Alors $N(\eta^m) = [N(\eta)]^m = (\pm 1)^m = \pm 1 \Longrightarrow \eta^m$ est une unité $\forall m \in \mathbb{Z}$.
Nous voulons aussi montrer que pour différents m, les unités sont distinctes.
Soient $m_1 \neq m_2 \in \mathbb{Z}$. η^{m_1} et η^{m_2} sont des unités. Comme $m_1 - m_2 \neq 0 \Longrightarrow \eta^{m_1 - m_2} \neq 1$ (car nous sommes dans les nombres réels) $\Longrightarrow \eta^{m_1} \neq \eta^{m_2}$.
Bref, nous venons de montrer que si η est une unité $\neq \pm 1$, alors η^m sont des unités distinctes $\forall m \in \mathbb{Z}$, ce qui donne une infinité d'unités.

Il reste à montrer qu'il existe une unité $\eta \neq \pm 1$.
Selon le théorème de Dirichlet précédemment prouvé, $\sqrt{d}$ étant irrationnel, on obtient que pour tout $n \in \mathbb{N}$, il existe $p, q \in \mathbb{Z}$ tels que $0 < q \leq n$ et tels que $|p - q\sqrt{d}| < \frac{1}{n}$. Soit $\alpha = p - q\sqrt{d}$. Considérons son conjugué $\overline{\alpha} = p + q\sqrt{d} = \alpha + 2q\sqrt{d}$. Il est tel que $|\overline{\alpha}| \leq |\alpha| + |2q\sqrt{d}| = |\alpha| + 2q\sqrt{d} < \frac{1}{n} + 2n\sqrt{d} \leq 1 + 2n\sqrt{d} \leq n\sqrt{d} + 2n\sqrt{d} = 3n\sqrt{d}$. Ainsi, $|N(\alpha)| = |\alpha\overline{\alpha}| < \frac{1}{n} 3n\sqrt{d} = 3\sqrt{d}$.
Comme $\sqrt{d} \in \mathbb{R}\backslash\mathbb{Q}$, alors $\alpha = p - q\sqrt{d} \in \mathbb{R}\backslash\mathbb{Q}$ et en particulier $\alpha = p - q\sqrt{d} \neq 0$.
On peut donc choisir n_1 tel que $\frac{1}{n_1} < |\alpha|$ et cela donne par le théorème de Dirichlet $|\alpha_1| := |p_1 - q_1\sqrt{d}| < \frac{1}{n_1}$ avec $|N(\alpha_1)| < 3\sqrt{d}$.
On obtient par ce processus une infinité de α_i distincts tels que $|N(\alpha_i)| < 3\sqrt{d}$.
En effet, supposons au contraire que $|\alpha| > |\alpha_1| > ... > |\alpha_k|$ sont les seuls α_i tels que $|N(\alpha_i)| < 3\sqrt{d}$. Puisque $\alpha_k \neq 0$ (car $\alpha_k \in \mathbb{R}\backslash\mathbb{Q}$), alors on peut choisir n_{k+1} tel que $\frac{1}{n_{k+1}} < |\alpha_k|$. Par le théorème de Dirichlet, il existe $p_{k+1}, q_{k+1} \in \mathbb{Z}$ tels que $|\alpha_{k+1}| := |p_{k+1} - q_{k+1}\sqrt{d}| < \frac{1}{n_{k+1}}$. Donc $N(\alpha_{k+1}) = |\alpha_{k+1}\overline{\alpha_{k+1}}| < \frac{1}{n_{k+1}} 3n_{k+1}\sqrt{d} = 3\sqrt{d}$. On a donc effectivement une infinité de α_i distincts tels que $|N(\alpha_i)| < 3\sqrt{d}$.
Mais $N(\alpha_i) = p_i^2 - dq_i^2 \in \mathbb{Z}$ et $N(\alpha_i)$ est borné indépendamment de n, d'où $N(\alpha_i)$ doit prendre une même valeur, disons N, pour une infinité de α_i. Parmi cette infinité de α_i, on peut en prendre deux distincts, disons $\beta_1 = p_a - q_a\sqrt{d}$

et $\beta_2 = p_b - q_b\sqrt{d}$, tels que $p_a \equiv p_b \bmod N$ et $q_a \equiv q_b \bmod N$ (si ce n'était pas possible, il n'y aurait pas une infinité de α_i).
Posons $\eta = \frac{\beta_1}{\beta_2}$. Ça implique que $N(\eta) = \frac{N(\beta_1)}{N(\beta_2)} = \frac{N}{N} = 1$.
Et $\eta = \frac{(p_a - q_a\sqrt{d})}{(p_b - q_b\sqrt{d})}\frac{(p_b + q_b\sqrt{d})}{(p_b + q_b\sqrt{d})} = \frac{(p_a p_b - dq_a q_b) + (p_a q_b - p_b q_a)\sqrt{d}}{N}$ qui sera un entier algébrique si $\frac{p_a p_b - dq_a q_b}{N} \in \mathbb{Z}$ et si $\frac{p_a q_b - p_b q_a}{N} \in \mathbb{Z}$.
Or, $p_a p_b - dq_a q_b \equiv p_a p_a - dq_a q_a \equiv N \equiv 0 \mod N$ et $p_a q_b - p_b q_a \equiv p_a q_a - p_a q_a \equiv 0 \mod N$.
Alors on a bien que $\frac{p_a p_b - dq_a q_b}{N} \in \mathbb{Z}$ et $\frac{p_a q_b - p_b q_a}{N} \in \mathbb{Z}$. D'où η est un entier algébrique de norme 1, c'est-à-dire que η est une unité.

Enfin, $\eta \neq 1$ puisque $\beta_1 \neq \beta_2$ ($\beta_1 = \beta_2$ est une contradiction de la construction).
Et $\eta \neq -1 \Leftrightarrow \beta_1 \neq -\beta_2 \Leftrightarrow p_a - q_a\sqrt{d} \neq -p_b + q_b\sqrt{d} \Leftrightarrow p_a + p_b \neq (q_a + q_b)\sqrt{d}$
ce qui est vrai puisque $p_a + p_b \in \mathbb{Z}$ et $(q_a + q_b)\sqrt{d} \in \mathbb{R}\backslash\mathbb{Q}$
car $0 < q_a + q_b \in \mathbb{Z}$ et $\sqrt{d} \in \mathbb{R}\backslash\mathbb{Q}$.

$\therefore$ Bref, il existe une unité $\eta \neq \pm 1$ et η^m sont toutes des unités distinctes $\forall m \in \mathbb{Z}$. □

On peut maintenant se demander si on peut exprimer simplement toute unité d'un corps quadratique réel. On a vu dans le théorème précédent que si η est une unité, alors η^m est une unité $\forall m \in \mathbb{Z}$. Réciproquement, on peut se demander s'il existe un certain ε tel que toute unité d'un corps quadratique réel puisse s'écrire sous la forme ε^m.

Soit $E = \{\xi \in \mathbb{Q}(\sqrt{d}) \mid \xi \text{ est une unité}, \xi > 1\}$.
E est non vide. En effet, soit η l'unité $\neq \pm 1$ du théorème précédent.
Si $\eta > 1$, alors E est non vide. Si $0 < \eta < 1$, alors $\frac{1}{\eta} \in E$ et E est non vide.
Si $-1 < \eta < 0$, alors $\frac{-1}{\eta} \in E$. Et si $\eta < -1$, alors $-\eta \in E$.
Tout élément $\xi \in E$ est de la forme $\xi = u + v\sqrt{d}$, avec soit $u, v \in \mathbb{Z}$ ou soit $2u, 2v, u + v \in \mathbb{Z}$.
De plus, $\xi = u + v\sqrt{d} > \overline{\xi} = u - v\sqrt{d}$ car sinon on aurait $N(\xi) = \xi\overline{\xi} \geq \xi\xi > 1$, une contradiction.

Donc $\xi - \overline{\xi} = 2v\sqrt{d} > 0 \Rightarrow v > 0$.
Aussi, $u > 0$ car sinon si $u \leq 0$, on aurait $\overline{\xi} = u - v\sqrt{d} \leq -u - v\sqrt{d} = -\xi < -1$, ce qui impliquerait que $N(\xi) = \xi\overline{\xi} < -\xi < -1$, une contradiction car $N(\xi) = \pm 1$.
Ainsi, tout élément $\xi = u + v\sqrt{d} \in E$ avec $u, v > 0$. Ceci implique qu'il n'y a qu'un nombre fini de $\xi \in E$ avec $\xi \leq \eta'$, η' étant égal à $\pm\eta$ ou $\pm\frac{1}{\eta}$, afin d'avoir $\eta' > 1$.
Alors E possède un plus petit élément (l'infimum de E est élément de E). Appelons ε ce plus petit élément dans E.

Maintenant, si $\varepsilon' \in \mathbb{Q}(\sqrt{d})$ est une unité telle que $\varepsilon' > 0$. Alors il existe un unique $m \in \mathbb{Z}$ tel que $\varepsilon^m \leq \varepsilon' < \varepsilon^{m+1}$, ce qui implique que $1 \leq \frac{\varepsilon'}{\varepsilon^m} < \varepsilon$. Or, ε est la plus petite unité > 1, alors puisque $\frac{\varepsilon'}{\varepsilon^m}$ est une unité (ε^m est une unité, $\frac{1}{\varepsilon^m}$ aussi et donc $\frac{\varepsilon'}{\varepsilon^m}$ également), la minimalité de ε nous donne $\varepsilon' = \varepsilon^m$.

Définition 5.0.11. *Soit* $\varepsilon_d = \inf\{\xi \in \mathbb{Q}(\sqrt{d}) \mid \xi \text{ est une unité, } \xi > 1\}$.
- ε_d *est appelé l'UNITÉ FONDAMENTALE du corps quadratique réel* $\mathbb{Q}(\sqrt{d})$.
- $\log(\varepsilon_d)$ *est appelé le RÉGULATEUR du corps quadratique réel* $\mathbb{Q}(\sqrt{d})$.

Nous venons de démontrer :
Théorème 5.0.8. *Soient* $\mathbb{Q}(\sqrt{d})$ *un corps quadratique réel et* ε_d *son unité fondamentale.*
Alors $\{\xi \in \mathbb{Q}(\sqrt{d}) \mid \xi \text{ est une unité}\} = \{\pm(\varepsilon_d)^m \mid m \in \mathbb{Z}\}$.

Ce dernier théorème pour les corps quadratiques réels est un cas particulier du théorème de Dirichlet sur les unités dans les corps de nombres algébriques. Ledit théorème de Dirichlet stipule ce qui suit :
Supposons qu'un corps K soit engendré par un nombre algébrique α de degré n et qu'exactement s des conjugués $\alpha_1, ..., \alpha_n$ de α soient réels. Ainsi $n = s + 2t$, où t est le nombre de paires de conjugués complexes.
Alors il existe $r = s + t - 1$ unités fondamentales $\varepsilon_1, ..., \varepsilon_r$ dans K telles que toute unité de K puisse être exprimée de façon unique sous la forme $\rho\varepsilon_1^{m_1}\varepsilon_2^{m_2}...\varepsilon_r^{m_r}$, où

$m_1, ..., m_r \in \mathbb{Z}$ et où ρ est une racine de l'unité dans K.

On peut se demander s'il existe un algorithme permettant de calculer l'unité fondamentale ε_d peu importe le corps quadratique réel $\mathbb{Q}(\sqrt{d})$. C'est possible. Avant de définir cet algorithme, nous devons introduire les fractions continues.

Références spécifiques à ce chapitre :

Alan Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, 1984.

Chapitre 6

FRACTIONS CONTINUES

L'étude des fractions continues remonte entre autres à l'époque de Fermat et atteint son apogée vers la fin du XVIII^e siècle sous l'impulsion de Lagrange et Legendre. Les fractions continues servent notamment à approximer des nombres irrationnels par des nombres rationnels.

6.1. Les fractions continues finies

Définition 6.1.1. – *Une FRACTION CONTINUE FINIE est une expression de la forme* $a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$, *où* $a_i \in \mathbb{R} \quad \forall\ 0 \leq i \leq n$ *et* $a_i \geq 0 \quad \forall\ 1 \leq i \leq n$.

On note $[a_0, a_1, ..., a_n]$ *une telle fraction continue finie.*

– *La fraction continue* $[a_0, a_1, ..., a_n]$ *est dite SIMPLE si* $a_i \in \mathbb{Z}\ \forall\ i$.

– *Soit* $[a_0, ..., a_n]$ *une fraction continue finie. La fraction continue* $C_k = [a_0, ..., a_k],\ 0 \leq k \leq n$, *est appelée sa* k^e*-RÉDUITE.*

Bien évidemment, une fraction continue simple finie où $a_n \neq 0$ est un nombre rationnel. On pourrait le montrer par induction en utilisant l'identité $[a_i, a_{i+1}, ..., a_n] = a_i + \frac{1}{[a_{i+1}, ..., a_n]}$.

Réciproquement, soit $\frac{a}{b} \in \mathbb{Q}$ avec $\text{pgcd}(a,b) = 1$ et $b > 0$.
L'algorithme de division d'Euclide implique que

$$\begin{aligned}
a &= a_0 b + b_1 && \text{avec } 0 < b_1 < b \\
b &= a_1 b_1 + b_2 && \text{avec } 0 < b_2 < b_1 \\
b_1 &= a_2 b_2 + b_3 && \text{avec } 0 < b_3 < b_2 \\
&\vdots \\
b_{n-2} &= a_{n-1} b_{n-1} + b_n && \text{avec } 0 < b_n < b_{n-1} \\
b_{n-1} &= a_n b_n
\end{aligned}$$

Nous avons $a_0 \in \mathbb{Z}$, $b_1, ..., b_n \in \mathbb{N}$, $a_1, ..., a_n \in \mathbb{N}$ et $a_n \geq 2$.
Par des substitutions successives, on obtient

$$\frac{a}{b} = a_0 + \frac{b_1}{b} = a_0 + \frac{1}{b/b_1} = a_0 + \frac{1}{a_1 + \dfrac{b_2}{b_1}} = ... = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

Ainsi, un nombre peut être représenté par une fraction continue simple finie où $a_n \neq 0$ si et seulement si c'est un nombre rationnel.
Cette représentation est unique si on choisit les a_i tels que donnés par l'algorithme d'Euclide. C'est ce que nous considérerons dorénavant.

Soit $C_n = [a_0, ..., a_n]$ une fraction continue finie. On peut calculer ses réduites.
$C_0 = [a_0] = a_0$
$C_1 = [a_0, a_1] = a_0 + \dfrac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$
$C_2 = [a_0, a_1, a_2] = a_0 + \cfrac{1}{a_1 + \dfrac{1}{a_2}} = a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1} = \frac{(a_0 a_1 + 1) a_2 + a_0}{a_1 a_2 + 1}$
$C_3 = a_0 + \frac{a_2 a_3 + 1}{a_1 a_2 a_3 + a_1 + a_3} = \frac{a_0 a_1 a_2 a_3 + a_0 a_1 + a_0 a_3 + a_2 a_3 + 1}{a_1 a_2 a_3 + a_1 + a_3} = \frac{(a_0 a_1 a_2 + a_0 + a_2) a_3 + a_0 a_1 + 1}{(a_1 a_2 + 1) a_3 + a_1}$
$= \frac{[(a_0 a_1 + 1) a_2 + a_0] a_3 + a_0 a_1 + 1}{(a_1 a_2 + 1) a_3 + a_1}$

On remarque qu'il semble y avoir une relation de récurrence entre les réduites. Introduisons donc les suites $\{p_n\}$ et $\{q_n\}$ définies par :

$$p_0 = a_0 \qquad p_1 = a_0a_1 + 1 \qquad p_n = a_np_{n-1} + p_{n-2} \qquad \text{où } n \geq 2 \qquad (6.1.1)$$

$$q_0 = 1 \qquad q_1 = a_1 \qquad q_n = a_nq_{n-1} + q_{n-2} \qquad \text{où } n \geq 2 \qquad (6.1.2)$$

On a ainsi $1 = q_0 \leq q_1 < q_2 < q_3 < ...$ et $\{q_n\}$ est une suite strictement croissante à partir de $n = 1$ puisque $q_n = a_nq_{n-1} + q_{n-2} > a_nq_{n-1} \geq q_{n-1}$.
On constate aussi que $C_0 = \frac{p_0}{q_0}$, $C_1 = \frac{p_1}{q_1}$, $C_2 = \frac{p_2}{q_2}$, $C_3 = \frac{p_3}{q_3}$ et on va montrer que ce résultat est vrai pour toute réduite.

Pour prouver ce résultat, introduisons d'abord une autre suite :

$$p'_0 = a_1 \qquad p'_1 = a_1a_2 + 1 \qquad p'_n = a_{n+1}p'_{n-1} + p'_{n-2} \qquad \text{où } n \geq 2$$

$$q'_0 = 1 \qquad q'_1 = a_2 \qquad q'_n = a_{n+1}q'_{n-1} + q'_{n-2} \qquad \text{où } n \geq 2$$

Lemme 6.1.1. $p'_i = q_{i+1} \quad \forall i \geq 0$

Démonstration. C'est vrai pour $i = 0, 1$. Supposons que ce soit vrai jusqu'à k. Alors $p'_{k+1} = a_{k+2}p'_k + p'_{k-1} = a_{k+2}q_{k+1} + q_k = q_{k+2}$. La preuve par induction est complétée. □

Lemme 6.1.2. $a_0q_{k+1} + q'_k = p_{k+1} \quad \forall k \geq 0$

Démonstration. $a_0q_1 + q'_0 = a_0a_1 + 1 = p_1$
$a_0q_2 + q'_1 = a_0(a_1a_2 + 1) + a_2 = a_2(a_0a_1 + 1) + a_0 = p_2$
Ainsi l'énoncé est vrai pour $k = 0, 1$. Supposons que ce soit vrai jusqu'à i.

Alors $$\begin{aligned} a_0q_{i+2} + q'_{i+1} &= a_0(a_{i+2}q_{i+1} + q_i) + a_{i+2}q'_i + q'_{i-1} \\ &= a_{i+2}(a_0q_{i+1} + q'_i) + a_0q_i + q'_{i-1} = a_{i+2}p_{i+1} + p_i = p_{i+2}. \end{aligned}$$

Donc l'énoncé est aussi vrai pour $i + 1$ et l'induction est complétée. □

Pour ce qui suit, définissons $C'_k = [a_1, ..., a_{k+1}]$.
On constate que $C'_0 = [a_1] = a_1 = \frac{p'_0}{q'_0}$ $C'_1 = [a_1, a_2] = a_1 + \frac{1}{a_2} = \frac{p'_1}{q'_1}$
Et en fait, si $C_k = [a_0, ..., a_k] = \frac{p_k}{q_k}$, alors $C'_k = [a_1, ..., a_{k+1}] = \frac{p'_k}{q'_k}$ puisque les suites p'_k et q'_k sont les suites p_k et q_k dans lesquelles on a remplacé chaque a_i par a_{i+1}.

Théorème 6.1.1. *Toute réduite C_k de la fraction continue finie $[a_0, a_1, ..., a_n]$ satisfait $C_k = \frac{p_k}{q_k}$, où $0 \leq k \leq n$.*

Démonstration. On va le montrer par induction. Nous avons déjà vérifié que c'est vrai pour $k = 0, 1, 2, 3$.
Supposons que $C_k = \frac{p_k}{q_k}$ soit vrai pour un certain $k < n$ et montrons que ce sera aussi vrai pour $k + 1$.

$$C_{k+1} = [a_0, ..., a_k, a_{k+1}] = a_0 + \frac{1}{[a_1, ..., a_{k+1}]} = a_0 + \frac{1}{C'_k} = a_0 + \frac{1}{p'_k/q'_k} = a_0 + \frac{q'_k}{p'_k}$$
$$= a_0 + \frac{q'_k}{q_{k+1}} = \frac{a_0 q_{k+1} + q'_k}{q_{k+1}} = \frac{p_{k+1}}{q_{k+1}}$$

□

Les nombres p_k et q_k sont ainsi appelés respectivement numérateur et dénominateur de la k^e réduite C_K.

6.2. Les propriétés de p_k et q_k

Théorème 6.2.1. *Pour $k \geq 1$, on a que* $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$

Démonstration. On procède par induction.
Pour $k = 1$: $p_1 q_0 - p_0 q_1 = (a_0 a_1 + 1)1 - a_0(a_1) = 1 = (-1)^{1-1}$
Supposons que ce soit vrai pour k et montrons que ça implique que c'est alors

aussi vrai pour $k+1$.

$$p_{k+1}q_k - p_kq_{k+1} = (a_{k+1}p_k + p_{k-1})q_k - p_k(a_{k+1}q_k + q_{k-1})$$
$$= a_{k+1}p_kq_k - a_{k+1}p_kq_k + p_{k-1}q_k - p_kq_{k-1} = -\left((-1)^{k-1}\right) = (-1)^k$$

□

De ce théorème, on peut déduire le corollaire suivant.

Corollaire 6.2.1. *Si la fraction continue est simple, alors*
$pgcd(p_k, p_{k+1}) = pgcd(q_k, q_{k+1}) = pgcd(p_k, q_k) = 1 \quad \forall k \geq 0$

Démonstration. D'après le théorème précédent, $p_{k+1}q_k - p_kq_{k+1} = (-1)^k$.
Donc $p_{k+1}(-1)^k q_k + p_k(-1)^{k+1}q_{k+1} = 1$.
Cette identité nous donne les trois résultats. □

Le théorème précédent nous permet aussi d'obtenir un résultat important sur les réduites. Ce résultat suivra le lemme suivant.

Lemme 6.2.1.

$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_kq_{k-1}} \qquad \textit{pour} \quad 1 \leq k \leq n \quad \textit{et}$$
$$C_k - C_{k-2} = \frac{(-1)^k(q_k - q_{k-2})}{q_kq_{k-1}q_{k-2}} \qquad \textit{pour} \quad 2 \leq k \leq n$$

Démonstration.

$$C_k - C_{k-1} = \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{p_kq_{k-1} - p_{k-1}q_k}{q_kq_{k-1}} = \frac{(-1)^{k-1}}{q_kq_{k-1}}$$
$$C_k - C_{k-2} = C_k - C_{k-1} + C_{k-1} - C_{k-2} = \frac{(-1)^{k-1}}{q_kq_{k-1}} + \frac{(-1)^{k-2}}{q_{k-1}q_{k-2}}$$
$$= \frac{(-1)^{k-1}q_{k-2} + (-1)^{k-2}q_k}{q_kq_{k-1}q_{k-2}} = \frac{(-1)^{k-2}(q_k - q_{k-2})}{q_kq_{k-1}q_{k-2}}$$

□

Théorème 6.2.2. $C_0 < C_2 < C_4 < ... < C_5 < C_3 < C_1$

DÉMONSTRATION. Puisque $q_k - q_{k-2} > 0$ et $q_k > 0$, le signe de $C_k - C_{k-2}$ est le même que celui de $(-1)^k$.
Ainsi, pour k pair, on a $\quad C_k - C_{k-2} > 0 \;\Rightarrow\; C_k > C_{k-2}$.
Et pour k impair, on a $\quad C_k - C_{k-2} < 0 \;\Rightarrow\; C_k < C_{k-2}$.
Nous avons donc établi que $\quad C_0 < C_2 < C_4 < ... \quad$ et $\quad C_1 > C_3 > C_5 > ...$
Nous savons par ailleurs que $\quad C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}} \quad$ et donc que $C_k - C_{k-1}$ est du même signe que $(-1)^{k-1}$.
Si k est pair, disons $k = 2m$, alors $\quad C_k - C_{k-1} < 0 \;\Rightarrow\; C_{2m} < C_{2m-1}$
Ainsi on déduit que $\quad C_{2a} < C_{2(a+b+1)} < C_{2(a+b)+1} < C_{2b+1} \quad$ et donc
$C_{2a} < C_{2b+1} \quad$ pour tout a et b, ce qui prouve le résultat. □

Remarque 6.2.1. *Il est intéressant de remarquer que les réduites (qu'on appelle aussi convergents) peuvent être calculées par multiplication matricielle. En effet, on peut montrer facilement par induction que pour $k \geq 1$,*

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} ... \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} .$$

6.3. Les fractions continues infinies

Théorème 6.3.1. *Soit $\{a_i\}_{i\geq 0}$ une suite infinie avec $a_0 \in \mathbb{Z}$ et $a_i \in \mathbb{N}\ \forall i \geq 1$. Soit $C_k = [a_0, ..., a_k]$. Alors la suite $\{C_k\}$ converge vers un nombre réel.*

DÉMONSTRATION. On peut considérer les C_k comme étant les réduites d'une fraction continue simple finie.
Par le théorème précédent, $\{C_{2k}\}$ est une suite strictement croissante bornée supérieurement par C_1, donc elle converge, disons vers α. De même, $\{C_{2k+1}\}$ est une suite strictement décroissante bornée inférieurement par C_0, donc elle

converge, disons vers β. Nous montrerons que $\alpha = \beta$.

Nous avons que $q_0, q_1 \geq 1$. Nous voulons montrer que $q_k \geq k$. On le fait par induction, puisqu'alors $q_{k+1} = a_{k+1}q_k + q_{k-1} \geq q_k + q_{k-1} \geq k + (k-1) = 2k - 1 \geq k + 1 \quad \forall k \geq 2$. En effet, $a_i \geq 1 \; \forall i \geq 1$.

Ainsi par le lemme (6.2.1), $C_{2j+1} - C_{2j} = \frac{1}{q_{2j+1}q_{2j}} \leq \frac{1}{(2j+1)(2j)} \xrightarrow{j\to\infty} 0$

Donc $\beta = \lim_{j\to\infty} C_{2j+1} = \lim_{j\to\infty}(C_{2j+1} - C_{2j}) + \lim_{j\to\infty} C_{2j} = 0 + \alpha = \alpha$

$\therefore \lim_{k\to\infty} C_k = \alpha$. □

Définition 6.3.1. *Soit $\{a_i\}_{i\geq 0}$ une suite avec $a_0 \in \mathbb{Z}$ et $a_i \in \mathbb{N} \; \forall i \geq 1$. L'expression $[a_0, a_1, ...]$ est appelée FRACTION CONTINUE SIMPLE INFINIE et est définie comme étant le nombre $\lim_{k\to\infty} C_k$.*

Théorème 6.3.2. *Soit $\alpha = [a_0, a_1, ...]$ une fraction continue simple infinie. Alors $\alpha \in \mathbb{R}\backslash\mathbb{Q}$.*

Démonstration. Nous avons que $C_0 < C_2 < ... < \alpha < ... < C_3 < C_1$. Pour tout k, le nombre α est compris entre C_k et C_{k+1}, d'où $0 < |\alpha - C_k| < |C_{k+1} - C_k| = \frac{1}{q_{k+1}q_k}$. En multipliant par q_k, on obtient $0 < |q_k\alpha - p_k| < \frac{1}{q_{k+1}}$. Supposons que $\alpha \in \mathbb{Q}$. $\alpha = \frac{a}{b}$ avec $b > 0$. Alors l'inégalité devient $0 < |q_k\frac{a}{b} - p_k| < \frac{1}{q_{k+1}} \Rightarrow 0 < |aq_k - bp_k| < \frac{b}{q_{k+1}}$. Comme $\{q_k\}$ est une suite qui croît à l'infini, on peut choisir k suffisamment grand pour que $q_{k+1} > b$. (Entre autres $q_{b+1} \geq b + 1 > b$.) On en déduit que le nombre $|aq_k - bp_k| \in \mathbb{Z}$ est compris strictement entre 0 et 1, ce qui n'est pas possible.

Il est impossible que $\alpha \in \mathbb{R}$ soit $\in \mathbb{Q}$. $\therefore \alpha \in \mathbb{R}\backslash\mathbb{Q}$. □

Lemme 6.3.1. *Soit $\alpha = [a_0, a_1, ...]$ une fraction continue simple infinie. Alors $a_0 = \lfloor\alpha\rfloor$.*

De plus, soit $\alpha_1 = [a_1, a_2, ...]$. Alors $\alpha = a_0 + \frac{1}{\alpha_1}$.

DÉMONSTRATION. Nous avons vu que $C_0 < \alpha < C_1$. Comme $C_0 = [a_0] = a_0$ et $C_1 = [a_0, a_1] = a_0 + \frac{1}{a_1}$, où $a_1 \geq 1$, on obtient que $a_0 < \alpha < a_0 + \frac{1}{a_1} \leq a_0 + 1 \Rightarrow a_0 < \alpha < a_0 + 1$, c'est-à-dire $a_0 = \lfloor \alpha \rfloor$.

$$\text{De plus, } \alpha_1 = \lim_{n\to\infty} [a_1, a_2, ..., a_n] = \lim_{n\to\infty} \frac{1}{\frac{1}{[a_1,a_2,...,a_n]} + a_0 - a_0}$$

$$= \lim_{n\to\infty} \frac{1}{[a_0, a_1, ..., a_n] - a_0} = \frac{1}{\lim_{n\to\infty} [a_0, ..., a_n] - a_0} = \frac{1}{\alpha - a_0} \ . \quad \square$$

Théorème 6.3.3. *Deux fractions continues simples infinies distinctes convergent vers des valeurs différentes.*

DÉMONSTRATION. Supposons le contraire. Soient $[a_0, a_1, ...]$ qui converge vers α et $[b_0, b_1, ...]$ qui converge aussi vers α. Le lemme précédent nous indique que $a_0 = \lfloor \alpha \rfloor = b_0$ et que $a_0 + \frac{1}{[a_1,...]} = \alpha = b_0 + \frac{1}{[b_1,...]}$. Bref $[a_1, ...] = [b_1, ...]$.
Si $[a_i, ...] = \alpha_i = [b_i, ...]$, alors $a_i = \lfloor \alpha_i \rfloor = b_i$ et $a_i + \frac{1}{[a_{i+1},a_{i+2},...]} = \alpha_i = b_i + \frac{1}{[b_{i+1},b_{i+2},...]}$. Bref, $[a_{i+1}, ...] = [b_{i+1}, ...]$. Alors par induction $a_i = b_i \ \forall i \geq 0$.
Or, $[a_0, a_1, ...]$ et $[b_0, b_1, ...]$ devraient être deux fractions continues distinctes, une contradiction. $\square$

Nous avons vu que α est une fraction continue simple finie si et seulement si $\alpha \in \mathbb{Q}$. Nous avons aussi montré que si α est une fraction continue simple infinie, alors $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. Nous allons donc maintenant montrer que si $\alpha \in \mathbb{R}\backslash\mathbb{Q}$, alors α peut s'exprimer comme une fraction continue infinie qui converge vers α.

Soit $\alpha = \alpha_0 \in \mathbb{R}\backslash\mathbb{Q}$.
Définissons la suite $\{a_i\}_{i\geq 0}$ par la relation de récurrence suivante :

$$a_k = \lfloor \alpha_k \rfloor \quad , \quad \alpha_{k+1} = \frac{1}{\alpha_k - a_k} \qquad \forall k \geq 0$$

Par induction, on montre que $\alpha_k \in \mathbb{R}\backslash\mathbb{Q}\ \forall k \geq 0$, car si $\alpha_k \in \mathbb{R}\backslash\mathbb{Q}$, alors $\alpha_{k+1} = \frac{1}{\alpha_k - a_k} \in \mathbb{R}\backslash\mathbb{Q}$. (Si α_{k+1} était $\in \mathbb{Q}$, alors on aurait $\alpha_k \in \mathbb{Q}$, une contradiction.)

Donc $0 < \alpha_k - a_k < 1 \Rightarrow \alpha_{k+1} = \frac{1}{\alpha_k - a_k} > 1 \Rightarrow a_{k+1} = \lfloor \alpha_{k+1} \rfloor \geq 1\ \forall k \geq 0$ ce qui veut dire que $[a_0, a_1, ...]$ est bien une fraction continue simple.

De plus, $\alpha = \alpha_0 = \lfloor \alpha_0 \rfloor + \alpha_0 - \lfloor \alpha_0 \rfloor = a_0 + \frac{1}{\alpha_1} = [a_0, \alpha_1]$. Supposons que $\alpha = [a_0, ..., a_{i-1}, \alpha_i]$. Alors $\alpha = [a_0, ..., a_{i-1}, \lfloor \alpha_i \rfloor + \alpha_i - \lfloor \alpha_i \rfloor] = \left[a_0, ..., a_{i-1}, a_i + \frac{1}{\alpha_{i+1}}\right]$ $= [a_0, ..., a_{i-1}, a_i, \alpha_{i+1}]$. Ainsi par induction $\alpha = [a_0, ..., a_k, \alpha_{k+1}]\ \forall k \geq 0$.

Donc $\alpha = [a_0, ..., a_k, \alpha_{k+1}] = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}}$

ce qui implique que $|\alpha - C_k| = \left| \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}} - \frac{p_k}{q_k} \right| = \left| \frac{\alpha_{k+1} p_k q_k + p_{k-1} q_k - p_k \alpha_{k+1} q_k - p_k q_{k-1}}{(\alpha_{k+1} q_k + q_{k-1}) q_k} \right|$ $= \frac{|p_{k-1} q_k - p_k q_{k-1}|}{q_k \cdot |\alpha_{k+1} q_k + q_{k-1}|} = \frac{1}{q_k (\alpha_{k+1} q_k + q_{k-1})} < \frac{1}{q_k (q_k + q_{k+1})} < \frac{1}{q_k^2} < \frac{1}{k^2}$ tel que démontré dans le théorème (6.3.1). Et $\frac{1}{k^2} \xrightarrow{k \to \infty} 0$.

$\therefore \alpha = \lim_{k \to \infty} [a_0, ..., a_k] = [a_0, a_1, ...]$

Nous venons de démontrer le théorème suivant :

Théorème 6.3.4. *Soit $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. Alors α a une représentation unique comme fraction continue simple infinie.*

Théorème 6.3.5. *Soit $n \in \mathbb{N}$ et soit $C_n = \frac{p_n}{q_n}$ la n-ième réduite de $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. Soient $a, b \in \mathbb{Z}$ tels que $1 \leq b < q_{n+1}$. Alors $|q_n \alpha - p_n| \leq |b\alpha - a|$.*

Démonstration. Soit le système d'équations suivant : $\begin{cases} p_n x + p_{n+1} y = a \\ q_n x + q_{n+1} y = b \end{cases}$

Étant donné que le déterminant des coefficients est $p_n q_{n+1} - q_n p_{n+1} = -(p_{n+1} q_n - p_n q_{n+1}) = (-1)^{n+1} \neq 0$, le système d'équations possède une solution unique. Cette unique solution est $\in \mathbb{Z}$ puisqu'en effet on trouve facilement que la solution est :

$\begin{cases} x = (-1)^n (b p_{n+1} - a q_{n+1}) \\ y = (-1)^n (a q_n - b p_n) \end{cases}$

Remarquons que $x \neq 0$, car sinon $q_{n+1} y = b \Rightarrow q_{n+1} \mid b$ ce qui contredit le

fait que $b < q_{n+1}$ par hypothèse.
Par ailleurs, si $y = 0$, alors $a = p_n x$ et $b = q_n x \Rightarrow |q_n\alpha - p_n| \leq |x| \cdot |q_n\alpha - p_n| = |b\alpha - a|$ car x est un entier non nul et le résultat est démontré.

Maintenant, il nous reste à vérifier le cas où $x, y \neq 0$.
Dans ce cas, on verra que x et y sont de signes opposés.
$y < 0 \Rightarrow q_n x = b - q_{n+1}y > 0 \Rightarrow x > 0$ puisque $q_i \geq 1\ \forall i$
$y > 0$ (et $y \in \mathbb{N}$ donc $y \geq 1$) implique, étant donné $b < q_{n+1}$, que $b < q_{n+1}y \ \Rightarrow$ $xq_n = b - q_{n+1}y < 0 \ \Rightarrow \ x < 0$
De plus, α est entre deux réduites consécutives, c'est-à-dire soit $\frac{p_n}{q_n} < \alpha < \frac{p_{n+1}}{q_{n+1}}$ ou $\frac{p_{n+1}}{q_{n+1}} < \alpha < \frac{p_n}{q_n}$. D'où $\alpha q_n - p_n$ et $\alpha q_{n+1} - p_{n+1}$ sont de signes opposés.
Ainsi, $x(q_n\alpha - p_n)$ et $y(q_{n+1}\alpha - p_{n+1})$ sont du même signe. Donc la valeur absolue de leur somme est égale à la somme de leur valeur absolue. On obtient alors

$$\begin{aligned}
|b\alpha - a| &= |(q_n x + q_{n+1}y)\alpha - (p_n x + p_{n+1}y)| = |x(q_n\alpha - p_n) + y(q_{n+1}\alpha - p_{n+1})| \\
&= |x(q_n\alpha - p_n)| + |y(q_{n+1}\alpha - p_{n+1})| \\
&= |x| \cdot |q_n\alpha - p_n| + |y| \cdot |q_{n+1}\alpha - p_{n+1}| \geq |x| \cdot |q_n\alpha - p_n| \\
&\geq 1 \cdot |q_n\alpha - p_n| \qquad \text{ce qui termine la preuve}
\end{aligned}$$

□

Soit $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. Ses réduites constituent de bonnes approximations rationnelles, c'est-à-dire :

Corollaire 6.3.1. *Soit $n \in \mathbb{N}$ et soit $C_n = \frac{p_n}{q_n}$ la n-ième réduite de $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. Soient $a, b \in \mathbb{Z}$ tels que $1 \leq b \leq q_n$. Alors $\left|\alpha - \frac{p_n}{q_n}\right| \leq \left|\alpha - \frac{a}{b}\right|$*

Démonstration. Supposons le contraire, $\left|\alpha - \frac{p_n}{q_n}\right| > \left|\alpha - \frac{a}{b}\right|$. Alors $|q_n\alpha - p_n| = q_n \cdot \left|\alpha - \frac{p_n}{q_n}\right| > q_n \cdot \left|\alpha - \frac{a}{b}\right| \geq b \cdot \left|\alpha - \frac{a}{b}\right| = |b\alpha - a|$ une contradiction avec le théorème précédent. □

Théorème 6.3.6. *Soit $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ et soit $\frac{a}{b} \in \mathbb{Q}$ avec a et b relativement premiers, $a \in \mathbb{Z}, b \in \mathbb{N}$, tels que $\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$. Alors $\frac{a}{b}$ est une réduite de la fraction continue de α.*

DÉMONSTRATION. Supposons le contraire, c'est-à-dire $\frac{a}{b} \neq \frac{p_n}{q_n}$ $\forall n$. Soit $k = \max\{n \mid q_n \leq b\}$. Un tel k existe puisque $q_0 = 1 \leq b$ et q_n est une suite strictement croissante qui tend vers l'infini. Ainsi $q_k \leq b < q_{k+1}$.
Par le théorème précédent, on a : $|q_k\alpha - p_k| \leq |b\alpha - a| = b\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b}$ par hypothèse. $\Rightarrow \left|\alpha - \frac{p_k}{q_k}\right| = \frac{|q_k\alpha - p_k|}{q_k} < \frac{1}{2bq_k}$
Et puisque $\frac{a}{b} \neq \frac{p_k}{q_k} \Rightarrow aq_k - bp_k \neq 0 \Rightarrow |aq_k - bp_k| \geq 1$, on obtient aussi $\frac{1}{bq_k} \leq \frac{|aq_k - bp_k|}{bq_k} = \left|\frac{a}{b} - \frac{p_k}{q_k}\right| = \left|\frac{a}{b} - \alpha + \alpha - \frac{p_k}{q_k}\right| \leq \left|\alpha - \frac{a}{b}\right| + \left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{2b^2} + \frac{1}{2bq_k} \Rightarrow \frac{1}{2bq_k} < \frac{1}{2b^2} \Rightarrow b < q_k$
Ceci est une contradiction, car $b \geq q_k$. □

Corollaire 6.3.2. *Soit $d \in \mathbb{N}$, d n'étant pas un carré parfait. Soient $x, y \in \mathbb{N}$ avec $pgcd(x, y) = 1$. Si $|x^2 - dy^2| < \sqrt{d}$, alors $\frac{x}{y}$ est une réduite de la fraction continue de $\sqrt{d}$.*

DÉMONSTRATION. Tout d'abord, $x^2 - dy^2 \neq 0$, puisque d n'est pas un carré parfait.

Cas 1)

Si $0 < x^2 - dy^2 < \sqrt{d} \Rightarrow (x + y\sqrt{d})(x - y\sqrt{d}) > 0$
et $x, y \in \mathbb{N} \Rightarrow x + y\sqrt{d} > 0 \Rightarrow x - y\sqrt{d} > 0 \Rightarrow x > y\sqrt{d}$

$$\Rightarrow \left|\sqrt{d} - \frac{x}{y}\right| = \frac{|y\sqrt{d} - x|}{y} = \frac{x - y\sqrt{d}}{y} = \frac{(x - y\sqrt{d})(x + y\sqrt{d})}{y(x + y\sqrt{d})} = \frac{x^2 - dy^2}{y(x + y\sqrt{d})}$$
$$< \frac{x^2 - dy^2}{y(y\sqrt{d} + y\sqrt{d})} = \frac{x^2 - dy^2}{2y^2\sqrt{d}} < \frac{1}{2y^2}\,.$$

Le théorème précédent nous indique que $\frac{x}{y}$ est une réduite de la fraction continue de $\sqrt{d}$.

Cas 2)

Si $\quad -\sqrt{d} < x^2 - dy^2 < 0 \quad \Rightarrow \quad 0 < dy^2 - x^2 < \sqrt{d} \quad \Rightarrow \quad 0 < y^2 - \frac{x^2}{d} < \frac{1}{\sqrt{d}}$

$\Rightarrow \quad \left(y - \frac{x}{\sqrt{d}}\right)\left(y + \frac{x}{\sqrt{d}}\right) > 0$

et $\; x, y \in \mathbb{N} \quad \Rightarrow \quad y + \frac{x}{\sqrt{d}} > 0 \quad \Rightarrow \quad y - \frac{x}{\sqrt{d}} > 0 \quad \Rightarrow \quad y > \frac{x}{\sqrt{d}}$

$\Rightarrow \quad \left|\frac{1}{\sqrt{d}} - \frac{y}{x}\right| = \left|\frac{\frac{x}{\sqrt{d}} - y}{x}\right| = \frac{(y - \frac{x}{\sqrt{d}})}{x}\frac{(y + \frac{x}{\sqrt{d}})}{(y + \frac{x}{\sqrt{d}})} = \frac{y^2 - \frac{x^2}{d}}{x(y + \frac{x}{\sqrt{d}})} < \frac{y^2 - \frac{x^2}{d}}{x(\frac{x}{\sqrt{d}} + \frac{x}{\sqrt{d}})} =$

$\frac{y^2 - \frac{x^2}{d}}{2x^2\frac{1}{\sqrt{d}}} < \frac{1}{2x^2}$

Le théorème précédent nous indique que $\frac{y}{x}$ est une réduite de la fraction continue de $\frac{1}{\sqrt{d}}$.

Maintenant, soit $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. Alors $\alpha = [a_0, a_1, ...] \Leftrightarrow \frac{1}{\alpha} = 0 + \frac{1}{[a_0, a_1, ...]} = [0, a_0, a_1, ...]$. C'est-à-dire que la $k+1^e$ réduite de la fraction continue de $\frac{1}{\alpha}$ est l'inverse de la k^e réduite de la fraction continue de α, et ce $\forall k \geq 0$.

Bref, on obtient que $\frac{x}{y}$ est une réduite de la fraction continue de $\sqrt{d}$. □

Lemme 6.3.2. *Soit $\alpha \in \mathbb{R}\backslash\mathbb{Q}$, α étant un nombre algébrique de degré deux (c'est-à-dire quadratique).*

Alors il existe $P_0, Q_0, d \in \mathbb{Z}$ tels que $\alpha = \frac{P_0 + \sqrt{d}}{Q_0}$ avec $Q_0 | (d - P_0^2)$.

Par ailleurs, définissons $\alpha_k = \frac{P_k + \sqrt{d}}{Q_k}$, $\quad a_k = \lfloor \alpha_k \rfloor$, $\quad P_{k+1} = a_k Q_k - P_k$, $Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k}$, $\quad$ où $k = 0, 1, 2, ...$

Alors $[a_0, a_1, a_2, ...]$ est la fraction continue simple de α.

Démonstration. α étant un irrationnel quadratique, il existe $a, b \in \mathbb{Z}$ et $e, f \in \mathbb{N}$, e étant libre de carré, tels que $\alpha = \frac{a + b\sqrt{e}}{f} = \frac{af + \sqrt{eb^2f^2}}{f^2}$. Posons $P_0 = af, d = eb^2f^2$ et $Q_0 = f^2$. On a bien que $Q_0 | (d - P_0^2)$.

Ensuite, α_k, a_k, P_{k+1} et Q_{k+1} sont définis récursivement. C'est bien défini à condition que $Q_k \neq 0 \; \forall k$. Vérifions. $Q_0 = f^2 \neq 0$. Et $Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k}$ où d n'est pas un carré parfait donc $d - P_{k+1}^2 \neq 0$. Donc $Q_k \neq 0 \; \forall k$.

On a que $\alpha_0 = \frac{P_0 + \sqrt{d}}{Q_0} = \alpha$, alors par le théorème (6.3.4), si on parvient à montrer que $\alpha_{k+1} = \frac{1}{\alpha_k - a_k} \; \forall k$, on aura par le fait même que $\alpha = [a_0, a_1, a_2, ...]$.

$$\alpha_k - a_k = \frac{P_k + \sqrt{d}}{Q_k} - a_k = \frac{P_k + \sqrt{d} - a_k Q_k}{Q_k} = \frac{\sqrt{d} - (a_k Q_k - P_k)}{Q_k}$$
$$= \frac{(\sqrt{d} - P_{k+1})(\sqrt{d} + P_{k+1})}{Q_k(\sqrt{d} + P_{k+1})} = \frac{d - P_{k+1}^2}{Q_k(\sqrt{d} + P_{k+1})} = \frac{Q_{k+1}}{\sqrt{d} + P_{k+1}} = \frac{1}{\alpha_{k+1}}$$

□

Définition 6.3.2. *Une fraction continue simple* $[a_0, a_1, a_2, ...]$ *est dite PÉRIODIQUE de période* t *s'il existe* $t \in \mathbb{N}, N \in \mathbb{Z}, N \geq 0$ *tels que* $a_n = a_{n+t}\ \forall n \geq N$. *On dénote une telle fraction continue ainsi* $[a_0, ..., a_{N-1}, \overline{a_N, ..., a_{N+t-1}}]$.

Théorème 6.3.7. α *est un irrationnel quadratique (*$\alpha \in \mathbb{R}\backslash\mathbb{Q}$ *et* α *étant un nombre algébrique de degré deux)* $\Longleftrightarrow$ α *peut être représenté par une fraction continue simple périodique.*

Démonstration.

$\Longleftarrow$)

Soit $\alpha = [a_0, a_1, ..., a_{N-1}, \overline{a_N, ..., a_{N+t-1}}]$. Alors $\alpha_N = [\overline{a_N, ..., a_{N+t-1}}]$ et
$\alpha = \frac{\alpha_N p_{N-1} + p_{N-2}}{\alpha_N q_{N-1} + q_{N-2}}$ si $N \geq 2$, où $\frac{p_n}{q_n} (n = 0, 1, ...)$ sont les réduites de α.
Puisque $\alpha_N = [a_N, ..., a_{N+t-1}, \overline{a_{N+t}, ..., a_{N+2t-1}}] = [a_N, ..., a_{N+t-1}, \overline{a_N, ..., a_{N+t-1}}]$,
on a $\alpha_N = \frac{\alpha_N r_{N+t-1} + r_{N+t-2}}{\alpha_N s_{N+t-1} + s_{N+t-2}}$ si $t \geq 2$, où $\frac{r_n}{s_n}$ $(n = 0, 1, ...)$ sont les réduites de α_N.
Cette dernière équation implique $s_{N+t-1}\alpha_N^2 + (s_{N+t-2} - r_{N+t-1})\alpha_N - r_{N+t-2} = 0$
Or, α_N est irrationnel puisque son développement en fraction continue simple est infini et il est aussi quadratique puisque solution à la dernière équation. Disons $\alpha_N = a + \sqrt{b}$ avec $a, b \in \mathbb{Q}$.
α est lui aussi irrationnel puisque son développement en fraction continue simple est infini et $\alpha = \frac{(a+\sqrt{b})p_{N-1} + p_{N-2}}{(a+\sqrt{b})q_{N-1} + q_{N-2}} = \frac{(ap_{N-1} + p_{N-2} + p_{N-1}\sqrt{b})(aq_{N-1} + q_{n-2} - q_{N-1}\sqrt{b})}{(aq_{N-1} + q_{N-2} + q_{N-1}\sqrt{b})(aq_{N-1} + q_{n-2} - q_{N-1}\sqrt{b})}$
$= A + B\sqrt{b}$ où $A, B \in \mathbb{Q}$ d'où α est un irrationnel quadratique.
La preuve est donc faite $\forall N \geq 2$ et $\forall t \geq 2$. Il reste à prouver lorque $N = 0$ ou 1 et lorque $t = 1$.
Soit $\alpha = [a_0, \overline{a_1}]$ alors $\alpha = [a_0, a_1, \overline{a_2, a_3}]$ et la preuve demeure valide.

Soit $\alpha = [\overline{a_0}]$ alors $\alpha = [a_0, a_1, \overline{a_2, a_3}]$ et la preuve demeure valide.

$\Longrightarrow$)

Soit $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ un irrationnel quadratique. Par le lemme précédent, il existe $P_0, Q_0, d \in \mathbb{Z}$ tels que $\alpha = \frac{P_0+\sqrt{d}}{Q_0}$ avec $Q_0 \mid (d - P_0^2)$. Posons $\alpha_k = \frac{P_k+\sqrt{d}}{Q_k}$, $a_k = \lfloor \alpha_k \rfloor$, $P_{k+1} = a_k Q_k - P_k$, $Q_{k+1} = \frac{d-P_{k+1}^2}{Q_k}$, $k = 0, 1, 2, ...$

Alors toujours selon le lemme précédent, $\alpha = [a_0, a_1, a_2, ...]$ et $\alpha = \frac{\alpha_k p_{k-1}+p_{k-2}}{\alpha_k q_{k-1}+q_{k-2}}$ où $\frac{p_k}{q_k}$ sont les réduites de α.

Dénotons par α' le conjugué de α et par α'_k le conjugué de α_k. Alors $\alpha' = \frac{P_0-\sqrt{d}}{Q_0}$ et $\alpha'_k = \frac{P_k-\sqrt{d}}{Q_k}$. Aussi

$$\alpha' = \left(\frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}\right)' = \frac{(\alpha_k p_{k-1} + p_{k-2})'}{(\alpha_k q_{k-1} + q_{k-2})'} = \frac{\left(\left(\frac{P_k+\sqrt{d}}{Q_k}\right) p_{k-1} + p_{k-2}\right)'}{\left(\left(\frac{P_k+\sqrt{d}}{Q_k}\right) q_{k-1} + q_{k-2}\right)'}$$

$$= \frac{\left(\frac{P_k-\sqrt{d}}{Q_k}\right) p_{k-1} + p_{k-2}}{\left(\frac{P_k-\sqrt{d}}{Q_k}\right) q_{k-1} + q_{k-2}} = \frac{\alpha'_k p_{k-1} + p_{k-2}}{\alpha'_k q_{k-1} + q_{k-2}}$$

$\Rightarrow \alpha'\alpha'_k q_{k-1} + \alpha' q_{k-2} = \alpha'_k p_{k-1} + p_{k-2} \quad \Rightarrow \quad \alpha'\alpha'_k q_{k-1} - \alpha'_k p_{k-1} = p_{k-2} - \alpha' q_{k-2}$

$\Rightarrow \alpha'_k = \frac{p_{k-2}-\alpha' q_{k-2}}{\alpha' q_{k-1}-p_{k-1}} = \frac{q_{k-2}(C_{k-2}-\alpha')}{q_{k-1}(\alpha'-C_{k-1})} = \frac{-q_{k-2}}{q_{k-1}} \left(\frac{\alpha'-C_{k-2}}{\alpha'-C_{k-1}}\right)$

Or, $\lim_{k\to\infty} C_{k-1} = \alpha$ et $\lim_{k\to\infty} C_{k-2} = \alpha$. D'où $\lim_{k\to\infty} \frac{\alpha'-C_{k-2}}{\alpha'-C_{k-1}} = \frac{\alpha'-\alpha}{\alpha'-\alpha} = 1$

Ceci indique que pour k suffisamment grand, disons pour $k \geq K$, on a $\alpha'_k < 0$ et comme $\alpha_k > 0$, alors $\alpha_k - \alpha'_k = \frac{P_k+\sqrt{d}}{Q_k} - \frac{P_k-\sqrt{d}}{Q_k} = \frac{2\sqrt{d}}{Q_k} > 0 \quad \Rightarrow \quad Q_k > 0$

On veut aussi montrer que $P_k, Q_k \in \mathbb{Z}\ \forall k \geq 0$. Procédons par induction. Nous savons que $P_0, Q_0, \in \mathbb{Z}$ avec $Q_0 \mid (d - P_0^2)$. Supposons que $P_k, Q_k \in \mathbb{Z}$ avec $Q_k \mid (d - P_k^2)$. Alors $P_{k+1} = a_k Q_k - P_k \in \mathbb{Z}$. $Q_{k+1} = \frac{d-P_{k+1}^2}{Q_k} = \frac{d-(a_k Q_k - P_k)^2}{Q_k} = \frac{d-(a_k^2 Q_k^2 - 2a_k Q_k P_k + P_k^2)}{Q_k} \in \mathbb{Z}$ puisque $Q_k \mid (d - P_k^2)$. Et $Q_k Q_{k+1} = d - P_{k+1}^2$ où $P_{k+1}, d, Q_k, Q_{k+1} \in \mathbb{Z} \quad \Rightarrow \quad Q_{k+1} \mid (d - P_{k+1}^2)$. Ainsi, par induction, $P_k, Q_k \in \mathbb{Z}\ \forall k \geq 0$.

Donc $Q_k > 0\ \forall k \geq K$ veut dire $Q_k \geq 1\ \forall k \geq K$. Alors on a que $\forall k \geq K, \quad 1 \leq Q_k \leq Q_k Q_{k+1} = d - P_{k+1}^2 \leq d$ et $P_{k+1}^2 \leq d - Q_k < d \Rightarrow -\sqrt{d} < P_{k+1} < \sqrt{d}$.

Bref, P_k et Q_k ne peuvent prendre qu'un nombre fini de valeurs. Il existe donc des entiers $0 \leq i < j$ tels que $P_i = P_j, Q_i = Q_j$. $\Rightarrow \alpha_i = \frac{P_i+\sqrt{d}}{Q_i} = \frac{P_j+\sqrt{d}}{Q_j} = \alpha_j \quad \Rightarrow a_i = a_j \quad \Rightarrow P_{i+1} = a_i Q_i - P_i = a_j Q_j - P_j = P_{j+1}$ et de même

$Q_{i+1} = Q_{j+1} \quad \Rightarrow \alpha_{i+1} = \alpha_{j+1} \quad \Rightarrow a_k = a_{k+(j-i)}\ \forall k \geq i$ puisque les α_k (et donc aussi les a_k) sont définis récursivement.

$\therefore \alpha = [a_0, a_1, ..., a_{i-1}, \overline{a_i, ..., a_{j-1}}]$ □

Définition 6.3.3. *Une fraction continue simple $[a_0, a_1, a_2, ...]$ est dite PURE-MENT PÉRIODIQUE de période t s'il existe $t \in \mathbb{N}$ tel que $a_n = a_{n+t}\ \forall n \geq 0$.*

Proposition 6.3.1. *Soit α une fraction continue simple périodique, où α' est le conjugué de α.*
Elle est purement périodique $\iff$ $\alpha > 1$ et $-1 < \alpha' < 0$.

Démonstration.
$\Longrightarrow$)
α est purement périodique donc $\alpha > a_0 = a_t \geq 1$ où t est la période et $\alpha = \alpha_0 = \alpha_t$. D'où $\alpha = \frac{\alpha_t p_{t-1} + p_{t-2}}{\alpha_t q_{t-1} + q_{t-2}} = \frac{\alpha p_{t-1} + p_{t-2}}{\alpha q_{t-1} + q_{t-2}}$ où $\frac{p_n}{q_n}, n \geq 0$, sont les réduites de α et donc $\alpha^2 q_{t-1} + \alpha q_{t-2} = \alpha p_{t-1} + p_{t-2}$
α satisfait l'équation suivante : $q_{t-1}x^2 + (q_{t-2} - p_{t-1})x - p_{t-2} = 0$
et on vient de montrer que $\alpha > 1$. L'autre racine de cette équation est α' le conjugué de α. On cherche à montrer que $-1 < \alpha' < 0$.
Soit $f(x) = q_{t-1}x^2 + (q_{t-2} - p_{t-1})x - p_{t-2}$. On a $f(0) = -p_{t-2} < 0, \quad f(\alpha) = 0,$ $f(-1) = q_{t-1} - q_{t-2} + p_{t-1} - p_{t-2} > 0$ puisque $\{q_i\}$ est une suite strictement croissante, de même que $\{p_i\}$ car $p_0 = a_0 \geq 1$.
Ainsi la racine α' se retrouve entre -1 et 0. $\therefore\ \alpha > 1$ et $-1 < \alpha' < 0$

$\Longleftarrow$)
Soit α une fraction continue simple périodique de période t avec $\alpha > 1$ et $-1 < \alpha' < 0$.
Rappelons que $\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$. Donc $\alpha'_{k+1} = \left(\frac{1}{\alpha_k - a_k}\right)' = \frac{1}{(\alpha_k - a_k)'} = \frac{1}{\alpha'_k - a_k}$
$-1 < \alpha'_0 < 0 \ \Rightarrow \ \alpha'_1 = \frac{1}{\alpha'_0 - a_0} < 0$ puisque $a_0 = \lfloor \alpha_0 \rfloor \geq 1$
et $\alpha'_0 - a_0 \leq \alpha'_0 - 1 < -1 \ \Rightarrow \ 1 > \frac{-1}{\alpha'_0 - a_0} \ \Rightarrow \ -1 < \frac{1}{\alpha'_0 - a_0}$
Bref, si $-1 < \alpha'_0 < 0$, alors $-1 < \alpha'_1 < 0$.

Supposons que $-1 < \alpha'_k < 0$. Alors $\alpha'_{k+1} = \frac{1}{\alpha'_k - a_k} < 0$ puisque $a_k \geq 1\ \forall k \in \mathbb{N}$.
Et $\alpha'_k - a_k \leq \alpha'_k - 1 < -1 \Rightarrow 1 > \frac{-1}{\alpha'_k - a_k} \Rightarrow -1 < \frac{1}{\alpha'_k - a_k} = \alpha'_{k+1}$
Bref, on vient de montrer par induction que $-1 < \alpha'_k < 0\ \forall k \geq 0$
Il s'ensuit que $\alpha'_k - a_k = \frac{1}{\alpha'_{k+1}} \Rightarrow \alpha'_k - \frac{1}{\alpha'_{k+1}} = a_k \in \mathbb{N} \Rightarrow a_k = \frac{-1}{\alpha'_{k+1}} + \alpha'_k < \frac{-1}{\alpha'_{k+1}} = a_k - \alpha'_k < a_k + 1$ C'est-à-dire $a_k = \left\lfloor \frac{-1}{\alpha'_{k+1}} \right\rfloor\ \forall k \geq 0$
Supposons que α ne soit pas purement périodique. Alors $\alpha = [a_0, ..., a_{N-1}, \overline{a_N, ..., a_{N+t-1}}]$. On a $\alpha_N = \alpha_{N+t} \Rightarrow \alpha'_N = \alpha'_{N+t} \Rightarrow \frac{1}{\alpha'_N} = \frac{1}{\alpha'_{N+t}} \Rightarrow a_{N-1} = a_{N+t-1}$, une contradiction avec la supposition que ça commencerait seulement à être périodique à partir de a_N.

$\therefore \alpha$ est purement périodique. □

Corollaire 6.3.3. *Soit* $\alpha = \frac{1}{\sqrt{d} - \lfloor \sqrt{d} \rfloor}$ *, où* $d \in \mathbb{N}$*, d n'étant pas un carré parfait. Alors* α *est purement périodique.*

Démonstration. α est un irrationnel quadratique, donc il peut être représenté par une fraction continue simple périodique. Et $0 < \sqrt{d} - \lfloor \sqrt{d} \rfloor < 1$ $(\sqrt{d} \neq \lfloor \sqrt{d} \rfloor$ puisque d n'est pas un carré parfait$) \Rightarrow \alpha = \frac{1}{\sqrt{d} - \lfloor \sqrt{d} \rfloor} > 1$
Par ailleurs, $\alpha' = \frac{-1}{\sqrt{d} + \lfloor \sqrt{d} \rfloor} < 0$ et $-1 < \alpha' = \frac{-1}{\sqrt{d} + \lfloor \sqrt{d} \rfloor}$ car $\sqrt{d} + \lfloor \sqrt{d} \rfloor > 1$. □

Corollaire 6.3.4. *Soit* $\alpha = \sqrt{d}$*, où* $d \in \mathbb{N}$*, d n'étant pas un carré parfait. Alors* α *est presque purement périodique, c'est-à-dire que* $\alpha = [a_0, \overline{a_1, ..., a_t}]$.

Démonstration. $\alpha = [a_0, a_1, a_2, ...] = a_0 + \frac{1}{[a_1, a_2, ...]} \Rightarrow [a_1, a_2, ...] = \frac{1}{\alpha - a_0} = \frac{1}{\sqrt{d} - \lfloor \sqrt{d} \rfloor}$ qui est purement périodique (corollaire précédent), disons de période t.

$\therefore\ \alpha = [a_0, \overline{a_1, ..., a_t}]$. □

Références spécifiques à ce chapitre :

Alan Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, 1984.

Jean-Marie De Koninck et Armel Mercier, *Introduction à la théorie des nombres*, Modulo, 1994.

Ivan Niven, Herbert S. Zuckerman et Hugh L. Montgomery, *An introduction to the theory of numbers, Fifth edition*, Jon Wiley & Sons, 1991.

Chapitre 7

CALCUL DE L'UNITÉ FONDAMENTALE

Nous nous demandions à la toute fin du chapitre 5 s'il existait un algorithme permettant de calculer l'unité fondamentale ε_d d'un corps quadratique $\mathbb{Q}(\sqrt{d})$. Nous sommes prêts à tenter de l'établir.

Une unité d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ peut s'écrire

$$\begin{cases} u + v\sqrt{d}\ (u, v \in \mathbb{Z}) & \text{si } d \equiv 2 \text{ ou } 3 \mod 4 \\ \frac{u'+v'\sqrt{d}}{2}\ (u', v' \in \mathbb{Z}, u' \equiv v' \bmod 2) & \text{si } d \equiv 1 \mod 4 \end{cases} \tag{7.0.1}$$

à la condition d'avoir ± 1 pour norme.

Si $d \equiv 2$ ou $3 \mod 4$: $x + y\sqrt{d}$ est une unité $\Leftrightarrow\ x^2 - dy^2 = \pm 1$ avec $x, y \in \mathbb{Z}$

Si $d \equiv 1 \mod 4$: $x + y\sqrt{d}$ est une unité $\Longleftrightarrow$

$$x^2 - dy^2 = \pm 1 \quad \text{avec } x = \tfrac{u'}{2}, y = \tfrac{v'}{2}, u', v' \in \mathbb{Z}, u' \equiv v' \bmod 2$$

$$\Longleftrightarrow \quad \begin{cases} u_1^2 - dv_1^2 = \pm 1 & \text{avec } u_1, v_1 \in \mathbb{Z} \qquad (\text{cas } u' \equiv v' \equiv 0 \mod 2 \\ u'^2 - dv'^2 = \pm 4 & \text{avec } u', v' \in \mathbb{Z}, u' \equiv v' \equiv 1 \mod 2 \end{cases}$$

Bref, dans un cas comme dans l'autre ($d \equiv 1$, 2 ou 3 mod 4), $\quad x^2 - dy^2 = \pm 1$ où $x, y \in \mathbb{Z}\ \Rightarrow\ x + y\sqrt{d}$ est une unité.

Pour $d \equiv 2$ ou 3 mod 4, ce sont les seules unités possibles.

Pour $d \equiv 1$ mod 4, il est possible qu'il y ait d'autres unités : $\quad x^2 - dy^2 = \pm 4$ avec $x, y \in \mathbb{Z},\ x \equiv y \bmod 2 \quad \Rightarrow \quad \frac{x+y\sqrt{d}}{2}$ est une unité.

Nous devons donc solutionner cette équation $x^2 - dy^2 = \pm 1$ en entiers. Cela nous permettra de trouver l'unité fondamentale lorsque $d \equiv 2$ ou $3 \bmod 4$. Lorsque $d \equiv 1 \bmod 4$, ça ne donnera pas nécessairement l'unité fondamentale (quoique oui parfois), mais ça donnera à tout le moins un candidat possible qui permettra ensuite de trouver très rapidement l'unité fondamentale.

7.1. Équation de Pell

L'équation $x^2 - dy^2 = 1$ est dite de Pell. Il est intéressant de mentionner que c'est Euler qui a baptisé ainsi cette équation, même si Pell n'y aurait apparamment pas contribué autrement que par la traduction d'un livre traitant du sujet. Fermat a travaillé sur l'équation de Pell en remettant aussi à l'ordre du jour les équations diophantiennes, c'est-à-dire la recherche de solutions entières ou rationnelles à des équations algébriques.

Nous avons vu dans le théorème (5.0.7) qu'une telle solution à l'équation de Pell existe. Nous recherchons sa solution fondamentale, c'est-à-dire la plus petite solution entière pour laquelle $x, y > 0$.

Soit une solution entière quelconque de l'équation de Pell avec $x > 0$ et $y > 0$. Alors le corollaire (6.3.2) nous indique que $\frac{x}{y}$ est une réduite de la fraction continue de $\sqrt{d}$. En effet, on a bien que pgcd(x,y) $= 1$ car sinon il serait impossible que $x^2 - dy^2 = 1$. Et par ailleurs $x^2 - dy^2 = 1 < \sqrt{d}$ pour tout $d > 1$.

Nous venons de démontrer :

Lemme 7.1.1. *Soit $x^2 - dy^2 = 1$ avec $x, y \in \mathbb{N}$ où d n'est pas un carré parfait. Alors $\frac{x}{y}$ est une réduite de $\sqrt{d}$.*

Nous avons établi au corollaire (6.3.4) que la fraction continue de $\sqrt{d}$ est de la forme $[a_0, \overline{a_1, ..., a_t}]$ où t est la période de la fraction continue.
Soient $\frac{p_n}{q_n}$ les réduites de $\sqrt{d}$. $\frac{x}{y}$ est une réduite donc $x = p_n, y = q_n$ pour un

certain n .

Lemme 7.1.2. *Soit $x = p_n, y = q_n$ une solution de $x^2 - dy^2 = 1$. Alors n doit être impair.*

DÉMONSTRATION. Nous avons $\sqrt{d} = \frac{p_n\alpha_{n+1}+p_{n-1}}{q_n\alpha_{n+1}+q_{n-1}}$ et $p_nq_{n-1}-p_{n-1}q_n = (-1)^{n-1}$.
D'où $y\sqrt{d}-x = q_n\sqrt{d}-p_n = q_n\frac{(p_n\alpha_{n+1}+p_{n-1})}{(q_n\alpha_{n+1}+q_{n-1})} - p_n\frac{(q_n\alpha_{n+1}+q_{n-1})}{(q_n\alpha_{n+1}+q_{n-1})} = \frac{q_np_{n-1}-p_nq_{n-1}}{q_n\alpha_{n+1}+q_{n-1}} = \frac{(-1)^n}{q_n\alpha_{n+1}+q_{n-1}}$

Et n pair $\Rightarrow\ y\sqrt{d}-x > 0\ \Rightarrow\ x - y\sqrt{d} < 0\ \Rightarrow\ (x-y\sqrt{d})(x+y\sqrt{d}) < 0$

$\Rightarrow\ x^2 - dy^2 \neq 1$ une contradiction.

$\therefore$ Il faut que n soit impair. □

Lemme 7.1.3. *Soit $x = p_n, y = q_n$ une solution de $x^2 - dy^2 = 1$. Alors n doit être de la forme $l \cdot t - 1$ avec $l = \begin{cases} 1, 2, 3, ... & \text{si } t \text{ est pair} \\ 2, 4, 6, ... & \text{si } t \text{ est impair} \end{cases}$*

C'est-à-dire que n doit être de la forme suivante : $n \equiv \begin{cases} -1 \mod t & \text{si } 2 \mid t \\ -1 \mod 2t & \text{si } 2 \nmid t \end{cases}$

DÉMONSTRATION. Nous avons $\sqrt{d} = \frac{p_n\alpha_{n+1}+p_{n-1}}{q_n\alpha_{n+1}+q_{n-1}}$
$\Rightarrow\ q_n\sqrt{d}\alpha_{n+1} + q_{n-1}\sqrt{d} = p_n\alpha_{n+1} + p_{n-1}$
$\Rightarrow\ (p_n - q_n\sqrt{d})\alpha_{n+1} = -p_{n-1} + q_{n-1}\sqrt{d}$
$\Rightarrow\ (p_n - q_n\sqrt{d})\alpha_{n+1}(p_n + q_n\sqrt{d}) = (-p_{n-1} + q_{n-1}\sqrt{d})(p_n + q_n\sqrt{d})$
$\Rightarrow\ (p_n^2 - dq_n^2)\alpha_{n+1} = \underbrace{-p_np_{n-1} + dq_nq_{n-1}}_{c\text{ , un entier}} + \sqrt{d}(p_nq_{n-1} - q_np_{n-1}) = (-1)^{n-1}\sqrt{d} + c$

Mais on veut que $p_n^2 - dq_n^2 = 1$ et pour ce faire, n doit être impair.
Avec ces conditions, $1 \cdot \alpha_{n+1} = 1 \cdot \sqrt{d} + c$
Par sa fraction continue, $\sqrt{d} = a_0 + \frac{1}{\alpha_1}$ où α_1 est purement périodique (donc > 0).
$\alpha_{n+1} = \sqrt{d}+c = a_0+\frac{1}{\alpha_1}+c$ et $\alpha_{n+1} = a_{n+1}+\frac{1}{\alpha_{n+2}}$ où $\alpha_1 > 1$ et $\alpha_{n+2} > 1$

C'est-à-dire que $0 < \alpha_{n+1} - (a_0 + c) < 1$ et $0 < \alpha_{n+1} - a_{n+1} < 1$, d'où $a_0 + c = \lfloor \alpha_{n+1} \rfloor = a_{n+1}$ et donc $\alpha_1 = \alpha_{n+2}$.

Bref, $n+1$ est un multiple de la période $t \quad \Rightarrow \quad n+1 = l \cdot t \quad \Rightarrow \quad n = l \cdot t - 1$

si t est pair, alors $l = 1, 2, 3, ...$ sont possibles et n sera impair.

si t est impair, alors $l = 2, 4, 6, ...$ doit être pair pour que n soit impair. $\square$

On a montré que les seules solutions entières positives possibles à $x^2 - dy^2 = 1$ pourraient être $x = p_n$ et $y = q_n$ où $\frac{p_n}{q_n}$ est un convergent de $\sqrt{d}$ avec $n = l \cdot t - 1$ tel que décrit ci-haut.

Toutes ces solutions possibles s'avèrent en fait des solutions qui satisfont $x^2 - dy^2 = 1$. Elles constituent donc l'ensemble des solutions positives. En effet :

Lemme 7.1.4. *Soit* $x = p_n, y = q_n$ *où* $\frac{p_n}{q_n}$ *est une réduite de* $\sqrt{d} = [a_0, \overline{a_1, ..., a_t}]$, *d n'étant pas un carré parfait, et où* $n = l \cdot t - 1$

avec $l = \begin{cases} 1, 2, 3, ... & \text{si } t \text{ est pair} \\ 2, 4, 6, ... & \text{si } t \text{ est impair} \end{cases}$. *Alors* $p_n^2 - dq_n^2 = 1$.

DÉMONSTRATION. $n+1$ est un multiple de la période t et en particulier $\alpha_1 = \alpha_{n+2}$

Par ailleurs, $\sqrt{d} = \frac{p_{n+1}\alpha_{n+2} + p_n}{q_{n+1}\alpha_{n+2} + q_n} = \frac{p_{n+1}\alpha_1 + p_n}{q_{n+1}\alpha_1 + q_n}$ et $\sqrt{d} = a_0 + \frac{1}{\alpha_1} \Rightarrow \alpha_1 = \frac{1}{\sqrt{d} - a_0}$

$\Longrightarrow \sqrt{d} = \frac{\frac{p_{n+1}}{\sqrt{d}-a_0} + p_n}{\frac{q_{n+1}}{\sqrt{d}-a_0} + q_n} = \frac{p_{n+1} + p_n\sqrt{d} - p_n a_0}{q_{n+1} + q_n\sqrt{d} - q_n a_0}$

$\Rightarrow \sqrt{d}\, q_{n+1} + dq_n - \sqrt{d}\, q_n a_0 = p_{n+1} + p_n\sqrt{d} - p_n a_0$

$\Rightarrow \sqrt{d} \underbrace{(q_{n+1} - q_n a_0 - p_n)}_{\in \mathbb{Z}} = \underbrace{p_{n+1} - p_n a_0 - dq_n}_{\in \mathbb{Z}}$

$\Rightarrow q_{n+1} - q_n a_0 - p_n = 0 \quad$ et $\quad p_{n+1} - p_n a_0 - dq_n = 0 \quad$ puisque $\sqrt{d} \in \mathbb{R} \backslash \mathbb{Q}$

$\Rightarrow a_0 = \frac{q_{n+1} - p_n}{q_n} = \frac{p_{n+1} - dq_n}{p_n} \quad \Rightarrow \quad p_n q_{n+1} - p_n^2 = p_{n+1} q_n - dq_n^2$

$\Rightarrow p_n^2 - dq_n^2 = p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1} = 1 \quad$ puisque n est impair. $\square$

7.2. L'ÉQUATION $x^2 - dy^2 = -1$

Une unité d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ peut aussi être de norme -1.
Soit une solution entière quelconque (x, y) de l'équation $x^2 - dy^2 = -1$, avec $x > 0$ et $y > 0$.
Alors le corollaire (6.3.2) nous indique que $\frac{x}{y}$ est une réduite de la fraction continue de $\sqrt{d}$. En effet, on a bien que pgcd$(x,y) = 1$ car sinon il serait impossible que $x^2 - dy^2 = -1$. Et par ailleurs $|x^2 - dy^2| = |-1| = 1 < \sqrt{d}$ pour tout $d > 1$.

Nous venons de démontrer :

Lemme 7.2.1. *Soit $x^2 - dy^2 = -1$, avec $x, y \in \mathbb{N}$ et où d n'est pas un carré parfait. Alors $\frac{x}{y}$ est une réduite de $\sqrt{d}$.*

Lemme 7.2.2. *Soit $x = p_n, y = q_n$ une solution de $x^2 - dy^2 = -1$. Alors n doit être pair.*

DÉMONSTRATION. Nous avons $\sqrt{d} = \frac{p_n\alpha_{n+1}+p_{n-1}}{q_n\alpha_{n+1}+q_{n-1}}$ et $p_nq_{n-1} - p_{n-1}q_n = (-1)^{n-1}$
D'où $y\sqrt{d} - x = q_n\sqrt{d} - p_n = q_n\frac{(p_n\alpha_{n+1}+p_{n-1})}{q_n\alpha_{n+1}+q_{n-1}} - p_n\frac{(q_n\alpha_{n+1}+q_{n-1})}{q_n\alpha_{n+1}+q_{n-1}} = \frac{(-1)^n}{q_n\alpha_{n+1}+q_{n-1}}$

Et n impair $\Rightarrow$ $y\sqrt{d} - x < 0$ $\Rightarrow$ $x - y\sqrt{d} > 0$ $\Rightarrow$ $(x - y\sqrt{d})(x + y\sqrt{d}) > 0$
$\Rightarrow$ $x^2 - dy^2 \neq -1$ une contradiction.

$\therefore$ Il faut que n soit pair. □

Lemme 7.2.3. *Soit $x = p_n, y = q_n$ une solution de $x^2 - dy^2 = -1$. Alors t est impair et n doit être de la forme $l \cdot t - 1$ avec $l = 1, 3, 5, ...$*

DÉMONSTRATION. Nous avons $\sqrt{d} = \frac{p_n\alpha_{n+1}+p_{n-1}}{q_n\alpha_{n+1}+q_{n-1}}$
$\Rightarrow$ $(p_n - q_n\sqrt{d})\alpha_{n+1} = -p_{n-1} + q_{n-1}\sqrt{d}$
$\Rightarrow$ $(p_n - q_n\sqrt{d})\alpha_{n+1}(p_n + q_n\sqrt{d}) = (-p_{n-1} + q_{n-1}\sqrt{d})(p_n + q_n\sqrt{d})$
$\Rightarrow$ $(p_n^2 - dq_n^2)\alpha_{n+1} = \underbrace{-p_np_{n-1} + dq_nq_{n-1}}_{c, \text{ un entier}} + \sqrt{d}(p_nq_{n-1} - q_np_{n-1}) = (-1)^{n-1}\sqrt{d} + c$

Mais on veut que $p_n^2 - dq_n^2 = -1$ et pour ce faire, n doit être pair.
Avec ces conditions, $-\alpha_{n+1} = -\sqrt{d} + c \quad \Rightarrow \ \alpha_{n+1} = \sqrt{d} - c$
Par sa fraction continue, $\sqrt{d} = a_0 + \frac{1}{\alpha_1}$ où α_1 est purement périodique (donc > 0).
$\alpha_{n+1} = \sqrt{d} - c = a_0 + \frac{1}{\alpha_1} - c$ et $\alpha_{n+1} = a_{n+1} + \frac{1}{\alpha_{n+2}}$ où $\alpha_1 > 1$ et $\alpha_{n+2} > 1$
C'est-à-dire que $0 < \alpha_{n+1} - a_0 + c < 1$ et $0 < \alpha_{n+1} - a_{n+1} < 1$,
d'où $a_0 - c = \lfloor \alpha_{n+1} \rfloor = a_{n+1}$ et donc $\alpha_1 = \alpha_{n+2}$.
Bref, $n+1$ est un multiple de la période $t \quad \Rightarrow \ n+1 = l \cdot t \quad \Rightarrow \ n = l \cdot t - 1$
Et n étant pair, $l \cdot t$ est impair $\quad \Rightarrow$ t est impair et l est impair ($l = 1, 3, 5, ...$). $\square$

On a montré que les seules solutions entières positives possibles à $x^2 - dy^2 = -1$ pourraient être $x = p_n$ et $y = q_n$ où $\frac{p_n}{q_n}$ est un convergent de $\sqrt{d}$ avec $n = l \cdot t - 1$, $l = 1, 3, 5, ...$ Toutes ces solutions possibles s'avèrent en fait des solutions qui satisfont $x^2 - dy^2 = -1$. Elles constituent donc l'ensemble des solutions positives. En effet :

Lemme 7.2.4. *Soit $x = p_n, y = q_n$ où $\frac{p_n}{q_n}$ est une réduite de $\sqrt{d} = [a_0, \overline{a_1, ..., a_t}]$, d n'étant pas un carré parfait, mais étant tel que t soit impair, et où $n = l \cdot t - 1$ avec $l = 1, 3, 5, ...$ Alors $p_n^2 - dq_n^2 = -1$.*

DÉMONSTRATION. $n+1$ est un multiple de la période t et en particulier $\alpha_1 = \alpha_{n+2}$
Par ailleurs, $\sqrt{d} = \frac{p_{n+1}\alpha_{n+2} + p_n}{q_{n+1}\alpha_{n+2} + q_n} = \frac{p_{n+1}\alpha_1 + p_n}{q_{n+1}\alpha_1 + q_n}$ et $\sqrt{d} = a_0 + \frac{1}{\alpha_1} \ \Rightarrow \ \alpha_1 = \frac{1}{\sqrt{d} - a_0}$
$\Longrightarrow \ \sqrt{d} = \frac{\frac{p_{n+1}}{\sqrt{d}-a_0} + p_n}{\frac{q_{n+1}}{\sqrt{d}-a_0} + q_n} = \frac{p_{n+1} + p_n\sqrt{d} - p_n a_0}{q_{n+1} + q_n\sqrt{d} - q_n a_0}$
$\Rightarrow \ \sqrt{d}\underbrace{(q_{n+1} - q_n a_0 - p_n)}_{\in \mathbb{Z}} = \underbrace{p_{n+1} - p_n a_0 - dq_n}_{\in \mathbb{Z}}$
$\Rightarrow \ q_{n+1} - q_n a_0 - p_n = 0 \quad$ et $\quad p_{n+1} - p_n a_0 - dq_n = 0 \qquad$ puisque $\sqrt{d} \in \mathbb{R} \backslash \mathbb{Q}$
$\Rightarrow \ a_0 = \frac{q_{n+1} - p_n}{q_n} = \frac{p_{n+1} - dq_n}{p_n} \qquad \Rightarrow \quad p_n q_{n+1} - p_n^2 = p_{n+1} q_n - dq_n^2$
$\Rightarrow \ p_n^2 - dq_n^2 = p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1} = -1 \qquad$ puisque n est pair car l et t sont impairs. $\square$

Nous avons prouvé :

Théorème 7.2.1. *Soit* $\mathbb{Q}(\sqrt{d})$ *un corps quadratique avec* $d \equiv 1, 2$ *ou* $3 \bmod 4$*, où* d *n'est pas un carré parfait. Alors* $\sqrt{d} = [a_0, \overline{a_1, ..., a_t}]$.
De plus, soit $\frac{p_n}{q_n}$ *les réduites de* $\sqrt{d}$.
Si t *est pair, alors* $\{(x,y) \in \mathbb{N}^2 \mid x^2 - dy^2 = 1\}$
$$= \{(p_n, q_n) \mid n = l \cdot t - 1 \text{ avec } l = 1, 2, 3, ...\}$$
Si t *est pair, alors* $\{(x,y) \in \mathbb{N}^2 \mid x^2 - dy^2 = -1\} = \emptyset$
Si t *est impair, alors* $\{(x,y) \in \mathbb{N}^2 \mid x^2 - dy^2 = 1\}$
$$= \{(p_n, q_n) \mid n = l \cdot t - 1 \text{ avec } l = 2, 4, 6, ...\}$$
Si t *est impair, alors* $\{(x,y) \in \mathbb{N}^2 \mid x^2 - dy^2 = -1\}$
$$= \{(p_n, q_n) \mid n = l \cdot t - 1 \text{ avec } l = 1, 3, 5, ...\}$$
En particulier, pour $d \equiv 2$ *ou* $3 \bmod 4$*, l'unité fondamentale* $\varepsilon_d = p_{t-1} + q_{t-1}\sqrt{d}$.

Et pour $d \equiv 1 \bmod 4$, $p_{t-1}+q_{t-1}\sqrt{d}$ est une unité. C'est un bon candidat pour l'unité fondamentale, mais il se peut que l'unité fondamentale soit plutôt comprise entre 1 et $p_{t-1} + q_{t-1}\sqrt{d}$ et soit $\frac{u'}{2} + \frac{v'}{2}\sqrt{d}$ où $u'^2 - dv'^2 = \pm 4$, $u', v' \in \mathbb{N}$, $u' \equiv v' \equiv 1 \bmod 2$.

7.3. L'ÉQUATION $u'^2 - dv'^2 = \pm 4$

Considérons justement l'équation $u'^2 - dv'^2 = \pm 4$ avec $u', v' \in \mathbb{N}$ et $u' \equiv v' \equiv 1 \bmod 2$.
Notons qu'on a $\pm 4 = u'^2 - dv'^2 \equiv 1 - d \cdot 1 \equiv 1 - d \bmod 8 \Rightarrow d \equiv 5 \bmod 8$. Alors le corollaire (6.3.2) nous indique que $\frac{u'}{v'}$ est une réduite de la fraction continue de $\sqrt{d}$. En effet, on a bien que pgcd(u',v') = 1 car sinon il serait impossible que $u'^2 - dv'^2 = \pm 4$ puisque u' et v' sont impairs. Et par ailleurs $|u'^2 - dv'^2| = |\pm 4| = 4 < \sqrt{d}$ pour tout $d > 16$.

(Donc la démarche ne sera pas valide a priori pour les corps quadratiques avec $d = 5$ et $d = 13$. Dans ces cas, on calcule au besoin la solution fondamentale de cette équation sans l'aide des fractions continues et on compare avec $p_{t-1} + q_{t-1}\sqrt{d}$.)

Nous venons de démontrer :

Lemme 7.3.1. *Soit* $u'^2 - dv'^2 = \pm 4$ *, avec* $u', v' \in \mathbb{N}$ *et où* $d \equiv 1 \bmod 4$ *,* $d \neq 5, 13$ *, n'est pas un carré parfait. Alors* $\frac{u'}{v'}$ *est une réduite de* $\sqrt{d}$*.*

De plus, tout comme dans le lemme (7.1.2), on trouve aussi dans le cas de $u'^2 - dv'^2 = 4$ que n doit être impair dans la réduite $\frac{u'}{v'} = \frac{p_n}{q_n}$.

De même, tout comme dans le lemme (7.2.2), on trouve aussi dans le cas de $u'^2 - dv'^2 = -4$ que n doit être pair dans la réduite $\frac{u'}{v'} = \frac{p_n}{q_n}$.

7.4. Mise en commun. Expression de l'unité fondamentale pour $d \equiv 2, 3 \bmod 4$ ou pour $d \equiv 1 \bmod 8$

Bref, résumons ce qui précède :

Théorème 7.4.1. *Soit* $\mathbb{Q}(\sqrt{d})$ *un corps quadratique avec* $d \equiv 2$ *ou* $3 \bmod 4$ *ou avec* $d \equiv 1 \bmod 8$ *, où* $d \neq 2$ *n'est pas un carré parfait. Alors* $\sqrt{d} = [a_0, \overline{a_1, ..., a_t}]$*. De plus, soient* $\frac{p_n}{q_n}$ *les réduites de* $\sqrt{d}$*. Alors l'unité fondamentale est* $\varepsilon_d = p_{t-1} + q_{t-1}\sqrt{d}$ *.*

Théorème 7.4.2. *Soit* $\mathbb{Q}(\sqrt{d})$ *un corps quadratique avec* $d \equiv 5 \bmod 8$*, où* $d \neq 5, 13$ *n'est pas un carré parfait. Alors* $\sqrt{d} = [a_0, \overline{a_1, ..., a_t}]$*.*
De plus, soient $\frac{p_n}{q_n}$ *les réduites de* $\sqrt{d}$*.*

$$\text{Soit } i = \begin{cases} \min \left\{ n \in \{0, 1, 2, ..., t-2\} \;\middle|\; p_n^2 - dq_n^2 = \pm 4 \right\} \\ \qquad\qquad si \quad \left\{ n \in \{0, 1, 2, ..., t-2\} \;\middle|\; p_n^2 - dq_n^2 = \pm 4 \right\} \neq \emptyset \\ t - 1 \qquad\qquad sinon \end{cases}$$

$$\text{Alors l'unité fondamentale } \varepsilon_d = \begin{cases} \frac{p_i + q_i\sqrt{d}}{2} \qquad quand \quad i < t-1 \\ p_i + q_i\sqrt{d} \quad sinon\ quand \quad i = t-1 \end{cases}$$

Nous possédons ainsi un algorithme, utilisant l'expression en fraction continue de $\sqrt{d}$, pour calculer l'unité fondamentale des corps quadratiques $\mathbb{Q}(\sqrt{d})$. Ladite unité fondamentale est exprimée en fonction des réduites de la fraction continue de $\mathbb{Q}(\sqrt{d})$. Établissons dans ce qui suit le lien entre les unités, qui sont des réduites, et l'unité fondamentale.

Nous avons vu au théorème (5.0.8) que si $\mathbb{Q}(\sqrt{d})$ est un corps quadratique réel et ε_d son unité fondamentale, alors $\{\xi \in \mathbb{Q}(\sqrt{d}) \mid \xi \text{ est une unité}\} = \{\pm(\varepsilon_d)^m \mid m \in \mathbb{Z}\}$.
Et $\{+(\varepsilon_d)^m \mid m \in \mathbb{N}\} = \{\xi \in \mathbb{Q}(\sqrt{d}) \mid \xi \text{ est une unité et } \xi > 1\}$
$= \{x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d}) \mid x + y\sqrt{d} \text{ est une unité et } x + y\sqrt{d} > 1\}$
$= \{x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d}) \mid x^2 - dy^2 = \pm 1 \text{ avec } x, y \in \mathbb{N}\}$ pour $d \equiv 1, 2, 3, 6$ ou $7 \bmod 8$.

Pour $d \equiv 5 \bmod 8$, il peut y avoir d'autres unités > 1 que celles-ci, c'est-à-dire $\frac{x+y\sqrt{d}}{2}$ lorsque $x^2 - dy^2 = \pm 4$ où $x, y \in \mathbb{N}$ et $x \equiv y \equiv 1 \bmod 2$.
(Lorsque $x \equiv y \equiv 0 \bmod 2$, les unités ont déjà été prises en compte dans la solution de $x^2 - dy^2 = \pm 1$ avec $x, y \in \mathbb{N}$.)

Bref, étant donné ε_d qui est connu, que pouvons-nous dire sur les autres unités ?
Commençons par ce corollaire au théorème (7.2.1).

Corollaire 7.4.1. *Soit $\mathbb{Q}(\sqrt{d})$ un corps quadratique avec $d \equiv 1, 2$ ou $3 \bmod 4$, où d n'est pas un carré parfait. De plus, soient $\frac{p_n}{q_n}$ les réduites de $\sqrt{d}$.*
Alors $\{(x, y) \in \mathbb{N}^2 \mid x^2 - dy^2 = \pm 1\} = \{(p_n, q_n) \mid n = l \cdot t - 1 \text{ où } l \in \mathbb{N}\}$.

Démonstration. C'est vrai lorsque t est pair et lorsque t est impair, où t représente la période de l'expansion en fraction continue de $\sqrt{d}$. Donc c'est vrai pour tout t. □

Théorème 7.4.3. *Soit* $\mathbb{Q}(\sqrt{d})$ *un corps quadratique avec* $d \equiv 2$ *ou* $3 \bmod 4$ *ou avec* $d \equiv 1 \bmod 8$*, où* d *n'est pas un carré parfait. De plus, soient* $\frac{p_n}{q_n}$ *les réduites de* $\sqrt{d} = [a_0, \overline{a_1, ..., a_t}]$.

Alors $\{(\varepsilon_d)^m \mid m \in \mathbb{N}\} = \{p_{l\cdot t-1} + q_{l\cdot t-1}\sqrt{d} \mid l \in \mathbb{N}\}$,

c'est-à-dire $(\varepsilon_d)^l = (p_{t-1} + q_{t-1}\sqrt{d})^l = p_{l\cdot t-1} + q_{l\cdot t-1}\sqrt{d}$.

Démonstration. $\{(\varepsilon_d)^m \mid m \in \mathbb{N}\}$

$= \{x + y\sqrt{d} \mid (x, y) \in \mathbb{N}^2 \text{ et } x^2 - dy^2 = \pm 1\}$ établi ci-haut

$= \{p_n + q_n\sqrt{d} \mid n = l \cdot t - 1 \text{ et } l \in \mathbb{N}\}$ par le corollaire précédent

Ce qui prouve la première affirmation. Pour ce qui est de la seconde affirmation maintenant, remarquons d'abord que les suites $\{|p_n|\}$ et $\{q_n\}$ sont strictement croissantes. (et pour nous $p_n = |p_n|$ car on tente d'approximer $\sqrt{d}$ d'où $a_0 = \lfloor\sqrt{d}\rfloor > 0$ et $a_i \geq 1 \; \forall i \geq 1$)

Alors $p_{l\cdot t-1} + q_{l\cdot t-1}\sqrt{d}$ croît strictement lorsque l croît strictement.

Aussi $\varepsilon_d > 1$ donc $\{(\varepsilon_d)^m \mid m \in \mathbb{N}\}$ croît strictement lorsque m croît strictement.

Bref, on a bien que $(\varepsilon_d)^1 = p_{t-1} + q_{t-1}\sqrt{d} = p_{1\cdot t-1} + q_{1\cdot t-1}\sqrt{d}$

Et comme $\{(\varepsilon_d)^m \mid m \in \mathbb{N}\} = \{p_{l\cdot t-1} + q_{l\cdot t-1}\sqrt{d} \mid l \in \mathbb{N}\}$ pour deux suites strictement croissantes avec égalité lorsque $l = 1 = m$, il y a aussi égalité lorsque $l = k = m \quad \forall k \in \mathbb{N}$ puisque sinon un des termes de la suite serait présent seulement d'un des deux côtés, une contradiction.

Ainsi, on a bien que $(p_{t-1} + q_{t-1}\sqrt{d})^l = (\varepsilon_d)^l = p_{l\cdot t-1} + q_{l\cdot t-1}\sqrt{d}$. □

Ce théorème reste-t-il vrai pour $d \equiv 5 \bmod 8$? Parfois oui et parfois non.

Lorsque $d \equiv 5 \bmod 8$ et lorsque l'équation $p_n^2 - dq_n^2 = \pm 4$ n'a pas de solution pour $n \in \{0, 1, 2, ..., t-2\}$, alors $\varepsilon_d = p_{t-1} + q_{t-1}\sqrt{d}$ et

$\{x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d}) \mid x + y\sqrt{d} \text{ est une unité et } x + y\sqrt{d} > 1\}$

$= \{x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d}) \mid x^2 - dy^2 = \pm 1 \text{ avec } x, y \in \mathbb{N}\}$

$= \{p_n + q_n\sqrt{d} \mid n = l \cdot t - 1 \text{ et } l \in \mathbb{N}\}$.

Bref, dans ce cas, le théorème reste vrai (pour $d > 16$ bien sûr, pour se conformer

au théorème (7.4.2)).

Que se passe-t-il alors lorsque $d \equiv 5 \bmod 8$ et lorsque l'équation $p_n^2 - dq_n^2 = \pm 4$ a une solution pour un certain $n \in \{0, 1, 2, ..., t-2\}$?
Dans ce cas, soit $i = \min\left\{n \in \{0, 1, 2, ..., t-2\} \mid p_n^2 - dq_n^2 = \pm 4\right\}$. Alors $\varepsilon_d = \frac{p_i + q_i\sqrt{d}}{2} < p_{t-1} + q_{t-1}\sqrt{d}$.
Or, $p_{t-1} + q_{t-1}\sqrt{d}$ est tout de même une unité et est donc une puissance de ε_d . Quelle est cette puissance ? Est-ce toujours la même puissance ou varie-t-elle en fonction de certains paramètres ? Expérimentalement, cette puissance est toujours 3 pour $17 < d < 262144 = 2^{18}$. Nous avons arrêté nos calculs à cette valeur de d. Nous n'avons pas testé plus loin, pour de plus grands d.
Dans ces calculs que nous avons fait pour $17 < d < 2^{18}$, nous avons aussi remarqué un lien qui unit $(\varepsilon_d)^2 = \left(\frac{p_i + q_i\sqrt{d}}{2}\right)^2$ à $p_{t-1} + q_{t-1}\sqrt{d}$. C'est ce qui suit : $(\varepsilon_d)^2 = \left(\frac{p_i + q_i\sqrt{d}}{2}\right)^2 = \frac{p_{t-i-2} + q_{t-i-2}\sqrt{d}}{2}$.
Ainsi,

Théorème 7.4.4. *Soit $\mathbb{Q}(\sqrt{d})$ un corps quadratique avec $d \equiv 5 \bmod 8$, $d > 16$, où d n'est pas un carré parfait. De plus, soient $\frac{p_n}{q_n}$ les réduites de $\sqrt{d} = [a_0, \overline{a_1, ..., a_t}]$.*
Alors $p_{l \cdot t-1} + q_{l \cdot t-1}\sqrt{d} = (p_{t-1} + q_{t-1}\sqrt{d})^l$
$$= \begin{cases} (\varepsilon_d)^l & \text{si } \left\{n \in \{0, 1, 2, ..., t-2\} \mid p_n^2 - dq_n^2 = \pm 4\right\} = \emptyset \\ ((\varepsilon_d)^r)^l = \left(\left(\frac{p_i + q_i\sqrt{d}}{2}\right)^r\right)^l & \text{sinon} \end{cases}$$
où $i = \min\left\{n \in \{0, 1, ..., t-2\} \mid p_n^2 - dq_n^2 = \pm 4\right\}$.

Théorème 7.4.5. *$r = 3$ dans le théorème précédent ,*
c'est-à-dire $(\varepsilon_d)^3 = \left(\frac{p_i + q_i\sqrt{d}}{2}\right)^3 = p_{t-1} + q_{t-1}\sqrt{d}$
lorsque $\left\{n \in \{0, 1, 2, ..., t-2\} \mid p_n^2 - dq_n^2 = \pm 4\right\} \neq \emptyset$.

Démonstration. Soit $\varepsilon_d = \frac{p_i + q_i\sqrt{d}}{2}$. Alors $(\varepsilon_d)^2 = \frac{p_i^2 + dq_i^2 + 2p_iq_i\sqrt{d}}{4}$.
Puisque $d \equiv 1 \bmod 4$ ($d \equiv 5 \bmod 8$ en fait) et que p_i et q_i sont tels que $p_i^2 - dq_i^2 = \pm 4$, alors p_i et q_i sont impairs. (Sinon, c'est qu'ils sont tous les

deux pairs, mais ceci contredit la minimalité de $p_{t-1}+q_{t-1}\sqrt{d}$ comme solution de $x^2-dy^2=\pm 1$.)

$\Rightarrow\ p_i^2+dq_i^2 \ \equiv\ 1+1\cdot 1 \ \equiv\ 2 \bmod 4$ et $p_i\cdot q_i \equiv 1 \bmod 2 \ \Rightarrow\ 2p_i\cdot q_i \equiv 2 \bmod 4$

Bref, $(\varepsilon_d)^2 = \dfrac{\frac{p_i^2+dq_i^2}{2}+p_iq_i\sqrt{d}}{2}$ est de la forme $\dfrac{a+b\sqrt{d}}{2}$ avec a et b impairs.

Aussi, $(\varepsilon_d)^3 = \dfrac{p_i^3+3dp_iq_i^2+(3p_i^2q_i+dq_i^3)\sqrt{d}}{8} = \dfrac{p_i(p_i^2+3dq_i^2)+q_i(3p_i^2+dq_i^2)\sqrt{d}}{8}$

où $p_i^2+3dq_i^2 \equiv 1+3\cdot 5\cdot 1 \equiv 0 \bmod 8$ et où $3p_i^2+dq_i^2 \equiv 3\cdot 1+5\cdot 1 \equiv 0 \bmod 8$

Bref, $(\varepsilon_d)^3$ est de la forme $a+b\sqrt{d}$.

Mais en fait, soit la solution $\varepsilon_d = \frac{p_i+q_i\sqrt{d}}{2}$ du théorème (7.4.4), alors $(\varepsilon_d)^3$ est une unité de la forme $a+b\sqrt{d}$, solution de $a^2-db^2=\pm 1$. Donc si $r>3$ dans le théorème (7.4.4), alors $(\varepsilon_d)^3$ est une unité solution de $a^2-db^2=\pm 1$, mais $(\varepsilon_d)^3<(\varepsilon_d)^r$ contredit la minimalité de $(\varepsilon_d)^r$ comme solution de $x^2-dy^2=\pm 1$.

Bref, $r=2$ ou $r=3$.

Mais $r=2$ est impossible car $(\varepsilon_d)^2$ n'est pas de la forme $a+b\sqrt{d}$ avec $a,b\in\mathbb{Z}$.

$\therefore\quad r=3$ □

Conjecture 7.4.1. *Lorsque* $\left\{n\in\{0,1,2,...,t-2\}\ \middle|\ p_n^2-dq_n^2=\pm 4\right\} \neq \emptyset$ *dans le théorème (7.4.4), alors* $(\varepsilon_d)^2 = \left(\dfrac{p_i+q_i\sqrt{d}}{2}\right)^2 = \dfrac{p_{t-i-2}+q_{t-i-2}\sqrt{d}}{2}$, *c'est-à-dire que si* ε_d *correspond à la* $i^{\text{ième}}$ *réduite , alors* $(\varepsilon_d)^2$ *correspondra à la* $(t-i-2)^{\text{ième}}$ *réduite.*

Conséquemment, si on trouve une solution à $x^2-dy^2=\pm 4$ plus petite que la solution à $x^2-dy^2=\pm 1$, c'est soit ε_d ou $(\varepsilon_d)^2$.

Lorsque $d\equiv 5 \bmod 8$, l'unité fondamentale est donc soit $p_{t-1}+q_{t-1}\sqrt{d}$ ou soit $\frac{p_i+q_i\sqrt{d}}{2} = (p_{t-1}+q_{t-1}\sqrt{d})^{1/3}$.

Pour ces $d\equiv 5 \bmod 8$, on peut aussi plutôt exprimer l'unité fondamentale en fonction des réduites de $\frac{1+\sqrt{d}}{2}$. Voyons comment.

7.5. Lorsque l'unité fondamentale peut être calculée en fonction de $\frac{1+\sqrt{d}}{2}$

Voici un corollaire au théorème (6.3.6) .

Corollaire 7.5.1. *Soit* $d \in \mathbb{N}$, d *n'étant pas un carré parfait. Soient* $x, y \in \mathbb{N}$ *avec* $pgcd(x, y) = 1$. *Si* $|(2x - y)^2 - dy^2| < 2\sqrt{d}$, *alors* $\frac{x}{y}$ *est une réduite de la fraction continue de* $\frac{1+\sqrt{d}}{2}$.

Démonstration. Tout d'abord, $(2x - y)^2 - dy^2 \neq 0$, puisque d n'est pas un carré parfait.

Cas 1)

Si $0 < (2x - y)^2 - dy^2 < 2\sqrt{d} \Rightarrow (2x - y + y\sqrt{d})(2x - y - y\sqrt{d}) > 0$

et $x, y \in \mathbb{N} \Rightarrow 2x+y(\sqrt{d}-1) > 0 \Rightarrow 2x-y-y\sqrt{d} > 0 \Rightarrow 2x-y > y\sqrt{d}$

$$\Rightarrow \left|\frac{1+\sqrt{d}}{2} - \frac{x}{y}\right| = \frac{|2x - y - y\sqrt{d}|}{2y} = \frac{2x - y - y\sqrt{d}}{2y}$$

$$= \frac{(2x - y - y\sqrt{d})(2x - y + y\sqrt{d})}{2y(2x - y + y\sqrt{d})} = \frac{(2x - y)^2 - dy^2}{2y(2x - y + y\sqrt{d})}$$

$$< \frac{2\sqrt{d}}{2y(2x - y + y\sqrt{d})} < \frac{2\sqrt{d}}{2y(2y\sqrt{d})} < \frac{1}{2y^2} .$$

Le théorème (6.3.6) nous indique que $\frac{x}{y}$ est une réduite de la fraction continue de $\frac{1+\sqrt{d}}{2}$.

Cas 2)

Si $-2\sqrt{d} < (2x - y)^2 - dy^2 < 0 \Leftrightarrow 0 < dy^2 - (2x - y)^2 < 2\sqrt{d}$

$\Rightarrow 0 < y^2 - \frac{(2x-y)^2}{d} < \frac{2}{\sqrt{d}} \Rightarrow \left(y - \frac{(2x-y)}{\sqrt{d}}\right)\left(y + \frac{(2x-y)}{\sqrt{d}}\right) > 0$

et $x, y \in \mathbb{N} \Rightarrow \frac{2x+y(\sqrt{d}-1)}{\sqrt{d}} > 0 \Rightarrow y - \frac{(2x-y)}{\sqrt{d}} > 0 \Rightarrow y\sqrt{d}+y-2x > 0$

$$\Rightarrow \quad \left|\frac{2}{1+\sqrt{d}} - \frac{y}{x}\right| = \left|\frac{2x-y-y\sqrt{d}}{x(1+\sqrt{d})}\right| = \frac{-2x+y+y\sqrt{d}}{x(1+\sqrt{d})}$$

$$= \frac{(y\sqrt{d}-2x+y)(y\sqrt{d}+2x-y)}{x(1+\sqrt{d})(y\sqrt{d}+2x-y)}$$

$$= \frac{dy^2-(2x-y)^2}{x(1+\sqrt{d})(y\sqrt{d}+2x-y)} < \frac{2\sqrt{d}}{x(1+\sqrt{d})(y\sqrt{d}+2x-y)}$$

$$= \frac{2\sqrt{d}}{x(2x-y+2x\sqrt{d}+dy)}$$

$$= \frac{2\sqrt{d}}{x(4x\sqrt{d}-2x\sqrt{d}+2x+y(d-1))}$$

$$= \frac{2\sqrt{d}}{x(4x\sqrt{d}-2x(\sqrt{d}-1)+y(\sqrt{d}-1)(\sqrt{d}+1))}$$

$$= \frac{2\sqrt{d}}{x(4x\sqrt{d}+(\sqrt{d}-1)(-2x+y+y\sqrt{d}))} < \frac{2\sqrt{d}}{x(4x\sqrt{d})}$$

$$= \frac{1}{2x^2} \qquad \text{vrai, car} \quad -2x+y+y\sqrt{d}>0 \quad \text{et} \quad \sqrt{d}-1>0$$

Le théorème (6.3.6) nous indique que $\frac{y}{x}$ est une réduite de la fraction continue de $\frac{2}{1+\sqrt{d}}$.
Ainsi, tel que montré dans le corollaire (6.3.2), $\frac{x}{y}$ est une réduite de la fraction continue de $\frac{1+\sqrt{d}}{2}$. □

De façon équivalente à l'équation (7.0.1), une unité d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ où $d \equiv 1 \bmod 4$ peut s'écrire $\frac{(2x-y)+y\sqrt{d}}{2}$ où $x, y \in \mathbb{Z}$ à condition d'avoir ± 1 pour norme.
L'unité fondamentale aura $2x-y>0$ et $y>0 \quad \Rightarrow \quad x>0$.
Les unités sont telles que $\frac{(2x-y)^2-dy^2}{4} = \pm 1 \quad \Leftrightarrow \quad (2x-y)^2-dy^2 = \pm 4$.
Ainsi dans ce cas on obtient $\text{pgcd}(x,y) \leq 2$.
Dans l'éventualité où y soit pair, alors les unités sont solutions de l'équation de Pell $a^2-db^2 = \pm 1$, équation que nous avons déjà traitée. Nous nous intéresserons donc plutôt à trouver l'unité fondamentale des corps quadratiques $\mathbb{Q}(\sqrt{d})$ où $d \equiv 1 \bmod 4$ pour lesquels y est impair $\Rightarrow$ $\text{pgcd}(x,y) = 1$.

Lemme 7.5.1. *Soit* $(2x-y)^2 - dy^2 = \pm 4$ *avec* $x, y \in \mathbb{N}$, *où* $pgcd(x,y) \neq 2$ *et où* $d > 4$ *n'est pas un carré parfait. Alors* $\frac{x}{y}$ *est une réduite de la fraction continue de* $\frac{1+\sqrt{d}}{2}$.

Démonstration. On a que $|(2x-y)^2 - dy^2| = 4 \quad < \quad 2\sqrt{d} \quad \forall\, d > 4$.
Ceci implique, par le corollaire (7.5.1), que $\frac{x}{y}$ est une réduite de $\frac{1+\sqrt{d}}{2}$. □

Ainsi, pour l'unité fondamentale $\frac{2x-y+y\sqrt{d}}{2}$ $(x, y \in \mathbb{N}$ et $\text{pgcd}(x,y) = 1)$, on a que $\frac{x}{y}$ est une réduite de $\frac{1+\sqrt{d}}{2}$. Maintenant, après un petit lemme, on pourra essayer de vérifier si on peut établir de quelle réduite précisément il s'agit.

Lemme 7.5.2. *Soit* $\alpha = \dfrac{1}{\frac{1+\sqrt{d}}{2} - \left\lfloor \frac{1+\sqrt{d}}{2} \right\rfloor}$, *où* $d \in \mathbb{N}$, d *n'étant pas un carré parfait. Alors* α *est purement périodique.*

Démonstration. $0 < \frac{1+\sqrt{d}}{2} - \left\lfloor \frac{1+\sqrt{d}}{2} \right\rfloor < 1 \quad \Rightarrow \quad \alpha > 1$

$$\alpha = \frac{1}{\left(\frac{1}{2} - \left\lfloor \frac{1+\sqrt{d}}{2} \right\rfloor + \frac{\sqrt{d}}{2}\right)} \cdot \frac{\left(\frac{1}{2} - \left\lfloor \frac{1+\sqrt{d}}{2} \right\rfloor - \frac{\sqrt{d}}{2}\right)}{\left(\frac{1}{2} - \left\lfloor \frac{1+\sqrt{d}}{2} \right\rfloor - \frac{\sqrt{d}}{2}\right)} \qquad \Rightarrow$$

$$\text{conjugué}(\alpha) = \frac{\left(\frac{1}{2} - \left\lfloor \frac{1+\sqrt{d}}{2} \right\rfloor + \frac{\sqrt{d}}{2}\right)}{\left(\frac{1}{2} - \left\lfloor \frac{1+\sqrt{d}}{2} \right\rfloor + \frac{\sqrt{d}}{2}\right)\left(\frac{1}{2} - \left\lfloor \frac{1+\sqrt{d}}{2} \right\rfloor - \frac{\sqrt{d}}{2}\right)} = \frac{1}{\frac{1}{2} - \left\lfloor \frac{1+\sqrt{d}}{2} \right\rfloor - \frac{\sqrt{d}}{2}} < 0$$

et $\text{conjugué}(\alpha) > -1 \quad \Leftrightarrow \quad 1 < \frac{-1}{2} + \frac{\sqrt{d}}{2} + \left\lfloor \frac{1+\sqrt{d}}{2} \right\rfloor$ vrai $\forall d \geq 2$

$\therefore$ Par la proposition (6.3.1), α est purement périodique. □

Ainsi, si $d \in \mathbb{N}$ n'est pas un carré parfait, on peut écrire $\frac{1+\sqrt{d}}{2} = [a_0, \overline{a_1, ..., a_s}]$.

Soient $\frac{x}{y} = \frac{p_n}{q_n}$ les réduites de $\frac{1+\sqrt{d}}{2}$. Ainsi $x = p_n$, $y = q_n$ pour un certain n.

7.5.1. L'équation $(2x-y)^2 - dy^2 = 4$

Lemme 7.5.3. *Soit* $x = p_n$, $y = q_n$ *une solution de* $(2x-y)^2 - dy^2 = 4$. *Alors* n *doit être impair.*

Démonstration.

Nous avons $\frac{1+\sqrt{d}}{2} = \frac{p_n\alpha_{n+1}+p_{n-1}}{q_n\alpha_{n+1}+q_{n-1}}$ et $p_nq_{n-1} - p_{n-1}q_n = (-1)^{n-1}$.

D'où $y\frac{(1+\sqrt{d})}{2} - x = q_n\frac{(p_n\alpha_{n+1}+p_{n-1})}{(q_n\alpha_{n+1}+q_{n-1})} - p_n\frac{(q_n\alpha_{n+1}+q_{n-1})}{(q_n\alpha_{n+1}+q_{n-1})} = \frac{q_np_{n-1}-p_nq_{n-1}}{q_n\alpha_{n+1}+q_{n-1}} = \frac{(-1)^n}{q_n\alpha_{n+1}+q_{n-1}}$

Et n pair $\Rightarrow$ $y\frac{(1+\sqrt{d})}{2} - x > 0$ $\Rightarrow$ $\frac{(2x-y-y\sqrt{d})}{2}\frac{(2x-y+y\sqrt{d})}{2} < 0$

$\Rightarrow$ $(2x-y)^2 - dy^2 \neq 4$ une contradiction.

$\therefore$ Il faut que n soit impair. □

Lemme 7.5.4. *Soit* $x = p_n$, $y = q_n$ *une solution de* $(2x-y)^2 - dy^2 = 4$. *Alors* n *doit être de la forme* $l \cdot s - 1$, *où* s *est la période de la fraction continue de* $\frac{1+\sqrt{d}}{2}$, *avec* $l = \begin{cases} 1,2,3,... & \text{si } s \text{ est pair} \\ 2,4,6,... & \text{si } s \text{ est impair} \end{cases}$

Démonstration. Nous avons $\frac{1+\sqrt{d}}{2} = \frac{\alpha_{n+1}p_n+p_{n-1}}{\alpha_{n+1}q_n+q_{n-1}}$

$\Rightarrow \quad \alpha_{n+1}\cdot\left(-q_n\frac{(1+\sqrt{d})}{2} + p_n\right) = -p_{n-1} + q_{n-1}\frac{(1+\sqrt{d})}{2}$

$\Rightarrow \alpha_{n+1}\cdot\frac{(2p_n-q_n-q_n\sqrt{d})}{2}\cdot\frac{(2p_n-q_n+q_n\sqrt{d})}{2} = \left(-p_{n-1} + q_{n-1}\frac{(1+\sqrt{d})}{2}\right)\cdot\left(p_n + q_n\frac{(1+\sqrt{d})}{2} - q_n\right)$

$\Rightarrow \quad \alpha_{n+1}\cdot\frac{((2p_n-q_n)^2-dq_n^2)}{4} = \frac{(1+\sqrt{d})}{2}\cdot(p_nq_{n-1} - p_{n-1}q_n) - p_np_{n-1} + p_{n-1}q_n$

$$+q_nq_{n-1}\cdot\left(\frac{1+\sqrt{d}}{2}\right)^2 - q_nq_{n-1}\cdot\left(\frac{1+\sqrt{d}}{2}\right)$$

$$= \frac{(1+\sqrt{d})}{2}\cdot(-1)^{n-1} - p_np_{n-1} + p_{n-1}q_n + q_nq_{n-1}\cdot\left(\frac{1+\sqrt{d}}{2}\right)\left(\frac{-1+\sqrt{d}}{2}\right)$$

$$= \frac{(1+\sqrt{d})}{2}\underbrace{-p_np_{n-1} + p_{n-1}q_n + q_nq_{n-1}\cdot\frac{(d-1)}{4}}_{c\ ,\ \text{un entier, car } d\equiv 1 \bmod 4}$$

$\Rightarrow \quad a_{n+1} + \frac{1}{\alpha_{n+2}} = \alpha_{n+1} = c + \frac{(1+\sqrt{d})}{2} = c + a_0 + \frac{1}{\alpha_1}$ où $\alpha_1 > 1$ et $\alpha_{n+2} > 1$

C'est-à-dire que $0 < \alpha_{n+1} - (a_0 + c) < 1$ et $0 < \alpha_{n+1} - a_{n+1} < 1$,

d'où $a_0 + c = \lfloor \alpha_{n+1} \rfloor = a_{n+1}$ et donc $\alpha_1 = \alpha_{n+2}$.

Bref, $n+1$ est un multiple de la période s $\Rightarrow$ $n+1 = l\cdot s$ $\Rightarrow$ $n = l\cdot s - 1$

Si s est pair, alors $l = 1,2,3,...$ sont possibles et n sera impair.

Si s est impair, alors $l = 2,4,6,...$ doit être pair pour que n soit impair. □

On a montré que les seules solutions entières positives possibles à $(2x-y)^2-dy^2=4$, lorsque $\text{pgcd}(x,y)\neq 2$, pourraient être $x=p_n$ et $y=q_n$ où $\frac{p_n}{q_n}$ est une réduite de $\frac{1+\sqrt{d}}{2}$ avec $n=l\cdot s-1$ tel que décrit ci-haut.
Toutes ces solutions possibles s'avèrent en fait des solutions qui satisfont $(2x-y)^2-dy^2=4$. Elles constituent donc l'ensemble des solutions positives. En effet :

Lemme 7.5.5. *Soit* $x=p_n, y=q_n$ *où* $\frac{p_n}{q_n}$ *est une réduite de* $\frac{1+\sqrt{d}}{2}=[a_0,\overline{a_1,...,a_s}]$, d *n'étant pas un carré parfait, et où* $n=l\cdot s-1$ *avec* $l=\begin{cases}1,2,3,... & \text{si } s \text{ est pair}\\ 2,4,6,... & \text{si } s \text{ est impair}\end{cases}$. *Alors* $(2p_n-q_n)^2-dq_n^2=4$.

Démonstration.

$n+1$ est un multiple de la période s et en particulier $\alpha_1=\alpha_{n+2}$.

Par ailleurs, $\frac{1+\sqrt{d}}{2} = \frac{\alpha_{n+2}p_{n+1}+p_n}{\alpha_{n+2}q_{n+1}+q_n} = \frac{\alpha_1 p_{n+1}+p_n}{\alpha_1 q_{n+1}+q_n}$

et $\frac{1+\sqrt{d}}{2} = a_0+\frac{1}{\alpha_1} \quad\Rightarrow\quad \alpha_1=\frac{2}{1+\sqrt{d}-2a_0}$

$\Rightarrow \quad \frac{1+\sqrt{d}}{2} = \frac{\frac{2p_{n+1}}{1+\sqrt{d}-2a_0}+p_n}{\frac{2q_{n+1}}{1+\sqrt{d}-2a_0}+q_n} = \frac{2p_{n+1}+p_n+p_n\sqrt{d}-2a_0p_n}{2q_{n+1}+q_n+q_n\sqrt{d}-2a_0q_n}$

$\Rightarrow \quad 2q_{n+1}+q_n+q_n\sqrt{d}-2a_0q_n+2q_{n+1}\sqrt{d}+q_n\sqrt{d}+dq_n-2a_0q_n\sqrt{d}$

$= 4p_{n+1}+2p_n+2p_n\sqrt{d}-4a_0p_n$

$\Rightarrow \quad \sqrt{d}\cdot(\underbrace{q_n+2q_{n+1}+q_n-2a_0q_n-2p_n}_{\in\mathbb{Z}}) = \underbrace{4p_{n+1}+2p_n-4a_0p_n-dq_n+2a_0q_n-2q_{n+1}-q_n}_{\in\mathbb{Z}}$

$\Rightarrow \quad 4p_{n+1}-2q_{n+1}+2p_n-q_n-2a_0(2p_n-q_n)-dq_n = 0$

et $\quad 2q_n-2p_n+2q_{n+1}-2a_0q_n = 0 \qquad$ puisque $\quad \sqrt{d}\in\mathbb{R}\backslash\mathbb{Q}$

$\Rightarrow \quad \frac{q_n-p_n+q_{n+1}}{q_n} = a_0 = \frac{4p_{n+1}-2q_{n+1}+2p_n-q_n-dq_n}{4p_n-2q_n}$

$\Rightarrow \quad 4p_nq_n-2q_n^2-4p_n^2+2p_nq_n+4p_nq_{n+1}-2q_nq_{n+1}$

$= 4p_{n+1}q_n-2q_nq_{n+1}+2p_nq_n-q_n^2-dq_n^2$

$\Rightarrow \quad 4(p_nq_{n+1}-p_{n+1}q_n) = 4p_n^2-4p_nq_n+q_n^2-dq_n^2$

$\Rightarrow \quad (2p_n-q_n)^2-dq_n^2 = -4\cdot(-1)^n = 4 \qquad$ puisque n est impair. $\square$

7.5.2. L'équation $(2x-y)^2 - dy^2 = -4$

Lemme 7.5.6. *Soit* $x = p_n$, $y = q_n$ *une solution de* $(2x-y)^2 - dy^2 = -4$. *Alors* n *doit être pair.*

Démonstration.

Nous avons $\frac{1+\sqrt{d}}{2} = \frac{p_n\alpha_{n+1}+p_{n-1}}{q_n\alpha_{n+1}+q_{n-1}}$ et $p_nq_{n-1} - p_{n-1}q_n = (-1)^{n-1}$.

D'où $y\frac{(1+\sqrt{d})}{2} - x = q_n\frac{(p_n\alpha_{n+1}+p_{n-1})}{(q_n\alpha_{n+1}+q_{n-1})} - p_n\frac{(q_n\alpha_{n+1}+q_{n-1})}{(q_n\alpha_{n+1}+q_{n-1})} = \frac{q_np_{n-1}-p_nq_{n-1}}{q_n\alpha_{n+1}+q_{n-1}} = \frac{(-1)^n}{q_n\alpha_{n+1}+q_{n-1}}$

Et n impair $\Rightarrow$ $y\frac{(1+\sqrt{d})}{2} - x < 0$ $\Rightarrow$ $\frac{(2x-y-y\sqrt{d})}{2}\frac{(2x-y+y\sqrt{d})}{2} > 0$

$\Rightarrow$ $(2x-y)^2 - dy^2 \neq -4$ une contradiction.

$\therefore$ Il faut que n soit pair. □

Lemme 7.5.7. *Soit* $x = p_n$, $y = q_n$ *une solution de* $(2x-y)^2 - dy^2 = -4$. *Soit* s *la période de la fraction continue de* $\frac{1+\sqrt{d}}{2}$. *Alors* s *est impair et* n *doit être de la forme* $l \cdot s - 1$, *avec* $l = 1, 3, 5, ...$

Démonstration. Nous avons $\frac{1+\sqrt{d}}{2} = \frac{\alpha_{n+1}p_n+p_{n-1}}{\alpha_{n+1}q_n+q_{n-1}}$

$\Rightarrow \quad \alpha_{n+1}\cdot\left(-q_n\frac{(1+\sqrt{d})}{2} + p_n\right) = -p_{n-1} + q_{n-1}\frac{(1+\sqrt{d})}{2}$

$\Rightarrow \alpha_{n+1}\cdot\frac{(2p_n-q_n-q_n\sqrt{d})}{2}\cdot\frac{(2p_n-q_n+q_n\sqrt{d})}{2} = \left(-p_{n-1} + q_{n-1}\frac{(1+\sqrt{d})}{2}\right)\cdot\left(p_n + q_n\frac{(1+\sqrt{d})}{2} - q_n\right)$

$$\begin{aligned}\Rightarrow \quad \alpha_{n+1}\cdot\tfrac{((2p_n-q_n)^2-dq_n^2)}{4} &= \tfrac{(1+\sqrt{d})}{2}\cdot(p_nq_{n-1} - p_{n-1}q_n) - p_np_{n-1} + p_{n-1}q_n \\ &\quad + q_nq_{n-1}\cdot\left(\tfrac{1+\sqrt{d}}{2}\right)^2 - q_nq_{n-1}\cdot\left(\tfrac{1+\sqrt{d}}{2}\right) \\ &= \tfrac{(1+\sqrt{d})}{2}\cdot(-1)^{n-1} - p_np_{n-1} + p_{n-1}q_n + q_nq_{n-1}\cdot\left(\tfrac{1+\sqrt{d}}{2}\right)\left(\tfrac{-1+\sqrt{d}}{2}\right) \\ &= -\tfrac{(1+\sqrt{d})}{2}\underbrace{-p_np_{n-1} + p_{n-1}q_n + q_nq_{n-1}\cdot\frac{(d-1)}{4}}_{-c\ ,\ \text{un entier, car}\ \ d\equiv 1 \bmod 4}\end{aligned}$$

$\Rightarrow \quad a_{n+1} + \frac{1}{\alpha_{n+2}} = \alpha_{n+1} = c + \frac{(1+\sqrt{d})}{2} = c + a_0 + \frac{1}{\alpha_1}$ où $\alpha_1 > 1$ et $\alpha_{n+2} > 1$

C'est-à-dire que $0 < \alpha_{n+1} - (a_0 + c) < 1$ et $0 < \alpha_{n+1} - a_{n+1} < 1$,

d'où $a_0 + c = \lfloor\alpha_{n+1}\rfloor = a_{n+1}$ et donc $\alpha_1 = \alpha_{n+2}$.

Bref, $n+1$ est un multiple de la période s $\Rightarrow$ $n+1 = l\cdot s$ $\Rightarrow$ $n = l\cdot s - 1$

Si s est pair, alors il n'y a aucune solution possible puisque n est pair.

Si s est impair, alors $l = 1, 3, 5, ...$ doit être impair pour que n soit pair. □

On a montré que les seules solutions entières positives possibles à $(2x-y)^2 - dy^2 = -4$, lorsque $\text{pgcd}(x,y) \neq 2$, pourraient être $x = p_n$ et $y = q_n$ où $\frac{p_n}{q_n}$ est une réduite de $\frac{1+\sqrt{d}}{2}$ avec $n = l \cdot s - 1$ tel que décrit ci-haut.
Toutes ces solutions possibles s'avèrent en fait des solutions qui satisfont $(2x - y)^2 - dy^2 = -4$. Elles constituent donc l'ensemble des solutions positives. En effet :

Lemme 7.5.8. *Soit* $x = p_n, y = q_n$ *où* $\frac{p_n}{q_n}$ *est une réduite de* $\frac{1+\sqrt{d}}{2} = [a_0, \overline{a_1, ..., a_s}]$, d *n'étant pas un carré parfait, mais étant tel que* s *soit impair, et où* $n = l \cdot s - 1$ *avec* $l = 1, 3, 5, ...$. *Alors* $(2p_n - q_n)^2 - dq_n^2 = -4$.

Démonstration.

$n+1$ est un multiple de la période s et en particulier $\alpha_1 = \alpha_{n+2}$.

Par ailleurs, $\dfrac{1+\sqrt{d}}{2} = \dfrac{\alpha_{n+2}p_{n+1} + p_n}{\alpha_{n+2}q_{n+1} + q_n} = \dfrac{\alpha_1 p_{n+1} + p_n}{\alpha_1 q_{n+1} + q_n}$

et $\dfrac{1+\sqrt{d}}{2} = a_0 + \dfrac{1}{\alpha_1} \quad \Rightarrow \quad \alpha_1 = \dfrac{2}{1+\sqrt{d}-2a_0}$

$\Rightarrow \quad \dfrac{1+\sqrt{d}}{2} = \dfrac{\frac{2p_{n+1}}{1+\sqrt{d}-2a_0} + p_n}{\frac{2q_{n+1}}{1+\sqrt{d}-2a_0} + q_n} = \dfrac{2p_{n+1} + p_n + p_n\sqrt{d} - 2a_0p_n}{2q_{n+1} + q_n + q_n\sqrt{d} - 2a_0q_n}$

$\Rightarrow \quad 2q_{n+1} + q_n + q_n\sqrt{d} - 2a_0q_n + 2q_{n+1}\sqrt{d} + q_n\sqrt{d} + dq_n - 2a_0q_n\sqrt{d}$

$= 4p_{n+1} + 2p_n + 2p_n\sqrt{d} - 4a_0p_n$

$\Rightarrow \quad \sqrt{d} \cdot (\underbrace{q_n + 2q_{n+1} + q_n - 2a_0q_n - 2p_n}_{\in \mathbb{Z}}) = \underbrace{4p_{n+1} + 2p_n - 4a_0p_n - dq_n + 2a_0q_n - 2q_{n+1} - q_n}_{\in \mathbb{Z}}$

$\Rightarrow \quad 4p_{n+1} - 2q_{n+1} + 2p_n - q_n - 2a_0(2p_n - q_n) - dq_n = 0$

et $\quad 2q_n - 2p_n + 2q_{n+1} - 2a_0q_n = 0 \qquad$ puisque $\quad \sqrt{d} \in \mathbb{R}\backslash\mathbb{Q}$

$\Rightarrow \quad \dfrac{q_n - p_n + q_{n+1}}{q_n} = a_0 = \dfrac{4p_{n+1} - 2q_{n+1} + 2p_n - q_n - dq_n}{4p_n - 2q_n}$

$\Rightarrow \quad 4p_nq_n - 2q_n^2 - 4p_n^2 + 2p_nq_n + 4p_nq_{n+1} - 2q_nq_{n+1}$

$= 4p_{n+1}q_n - 2q_nq_{n+1} + 2p_nq_n - q_n^2 - dq_n^2$

$\Rightarrow \quad 4(p_nq_{n+1} - p_{n+1}q_n) = 4p_n^2 - 4p_nq_n + q_n^2 - dq_n^2$

$\Rightarrow \quad (2p_n - q_n)^2 - dq_n^2 = -4 \cdot (-1)^n = -4 \qquad$ puisque n est pair. $\square$

7.5.3. Expression de l'unité fondamentale pour $d \equiv 5 \bmod 8$

Bref, on avait comme résultat dans la section (7.4) que l'unité fondamentale d'un corps quadratique $\mathbb{Q}(\sqrt{d})$, $d \equiv 5 \bmod 8$, était soit $p_{t-1} + q_{t-1}\sqrt{d}$ ou soit $(p_{t-1} + q_{t-1}\sqrt{d})^{1/3}$ où $\frac{p_{t-1}}{q_{t-1}}$ est la $(t-1)^{\text{ième}}$ réduite de $\sqrt{d}$.

À la lumière des résultats précédents de la section (7.5), nous donnerons une expression unique pour l'unité fondamentale, lorsque $d \equiv 5 \bmod 8$, plutôt que d'avoir comme dans la section (7.4) une expression avec deux résultats possibles.

Lemme 7.5.9. *Soit* $d \equiv 5 \bmod 8$. *Soient* $x, y \in \mathbb{Z}$ *tels que* $(2x-y)^2 - dy^2 = \pm 4$. *Alors* $pgcd(x, y) \neq 2$.

Démonstration. Supposons le contraire, c'est-à-dire supposons que $\gcd(x, y) = 2$. Alors x est pair.

Cas 1) Si $y \equiv 2 \bmod 4$

$\Rightarrow \; 4 \equiv (2x-y)^2 - dy^2 \equiv 4 \cdot 1 - 5 \cdot 4 \equiv 0 \bmod 8$, une contradiction.

Cas 2) Si $y \equiv 0 \bmod 4$

$\Rightarrow \; 4 \equiv (2x-y)^2 - dy^2 \equiv 16 - 5 \cdot 16 \equiv 0 \bmod 8$, une contradiction.

$\therefore \; \gcd(x, y) \neq 2$ □

Théorème 7.5.1. *Soit* $\mathbb{Q}(\sqrt{d})$ *un corps quadratique avec* $d \equiv 5 \bmod 8$, *où* $d > 4$ *n'est pas un carré parfait. De plus, soient* $\frac{p_n}{q_n}$ *les réduites de* $\frac{1+\sqrt{d}}{2} = [a_0, \overline{a_1, ..., a_s}]$. *Alors l'unité fondamentale* $\varepsilon_d = \dfrac{2p_{s-1} - q_{s-1} + q_{s-1}\sqrt{d}}{2}$.

Démonstration. Par les lemmes (7.5.5) et (7.5.8), $\dfrac{2p_{s-1} - q_{s-1} + q_{s-1}\sqrt{d}}{2}$ est tel que $\dfrac{(2p_{s-1} - q_{s-1} + q_{s-1}\sqrt{d})}{2} \cdot \dfrac{(2p_{s-1} - q_{s-1} - q_{s-1}\sqrt{d})}{2} = \pm 1$ et est donc une unité.

Pourrait-il y avoir une unité plus petite que celle-ci ?

Soit une unité > 1. Elle peut s'écrire $\frac{2x-y+y\sqrt{d}}{2}$, $x, y \in \mathbb{N}$, où $(2x-y)^2 - dy^2 =$

± 4 .

Or, $\text{pgcd}(x, y) \leq 2$. Mais par le lemme précédent, on obtient $\text{pgcd}(x, y) = 1$. Et par les lemmes (7.5.1), (7.5.4) et (7.5.7), $\frac{x}{y}$ est une réduite $\frac{p_n}{q_n}$ de $\frac{1+\sqrt{d}}{2}$ où $n = l \cdot s - 1$ $(l \in \mathbb{N})$. Ainsi, parmi les unités > 1, la plus petite sera donnée par la $(s-1)^{\text{ième}}$ réduite.

$\therefore \quad \varepsilon_d = \dfrac{2p_{s-1} - q_{s-1} + q_{s-1}\sqrt{d}}{2}$. $\square$

Références spécifiques à ce chapitre :

Alan Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, 1984.

L.K. Hua, *On the least solution of Pell's equation*, Bulletin of the American Mathematical Society, Volume 48, 1942, pages 731-735.

Ivan Niven, Herbert S. Zuckerman et Hugh L. Montgomery, *An introduction to the theory of numbers, Fifth edition*, Jon Wiley & Sons, 1991.

Chapitre 8

FORMES BINAIRES QUADRATIQUES ET NOMBRE DE CLASSES

Nous introduirons dans ce chapitre les formes binaires quadratiques et le nombre de classes. La théorie des formes binaires quadratiques est intimement liée avec l'étude des corps quadratiques, abordée dans les chapitres précédents.

La théorie des formes quadratiques s'est développée sur des résultats isolés depuis les Babyloniens entre 1900 et 1600 avant J.-C., Brahmagupta au VII^e siècle de notre ère ainsi que Fermat et Euler un millénaire plus tard. Lagrange et surtout Gauss ont édifié et solidifié cette théorie. Une grande portion du livre *Disquisitiones Arithmeticae* de Gauss est consacrée à l'étude des formes quadratiques. L'égalité $x^2 - dy^2 = (x+y\sqrt{d})(x-y\sqrt{d}) = N(x+y\sqrt{d})$ est un exemple qui indique les liens entre l'étude des formes binaires quadratiques et la théorie des corps quadratiques. En fait, les racines d'une forme binaire quadratique de discriminant D sont des éléments de $\mathbb{Q}(\sqrt{d})$; la forme se factorise dans le corps quadratique.

Le nombre de classes est une quantité reliée aux formes binaires quadratiques. Gauss l'a étudié et en plus d'émettre certaines conjectures le concernant et de formuler son problème du nombre de classes.

Au XIX^e siècle, des mathématiciens crurent avoir démontré le Dernier Théorème de Fermat mais leur preuve reposait sur la croyance qu'il y avait une factorisation unique en premiers pour les entiers cyclotomiques et plus généralement pour les nombres complexes. Toutefois, un nombre de classes égal à 1 implique la

factorisation unique en premiers dans un anneau d'entiers quadratiques. Kummer développa toutefois une autre théorie pour faire avancer la résolution du Dernier Théorème de Fermat.

Le premier à conjecturer une formule pour le nombre de classes fut Jacobi en 1832. Dirichlet prouva ensuite une telle formule. Ces travaux de Dirichlet sur le nombre de classes furent importants dans sa preuve de l'infinité de nombres premiers dans les progressions arithmétiques.

Abordons maintenant plus en détail ces notions.

8.1. Formes binaires quadratiques

Définition 8.1.1. - *Un polynôme à plusieurs variables est appelé une FORME, ou est dit HOMOGÈNE, si tous ses monômes sont du même degré.*
- *Une forme de degré 2 est dite QUADRATIQUE.*
- *Une forme à 2 variables est dite BINAIRE.*
- *Bref, une forme binaire quadratique s'écrit sous la forme suivante :* $f(x,y) = ax^2 + bxy + cy^2$

Nous travaillerons avec les formes binaires quadratiques à coefficients entiers.

Définition 8.1.2. *Le DISCRIMINANT* D *d'une forme binaire quadratique* $f(x,y) = ax^2 + bxy + cy^2$ *est la quantité* $D = b^2 - 4ac$.
Il est dit FONDAMENTAL lorsque $D \in \mathbb{Z}$ *est un entier libre de carré impair qui est* $\equiv 1 \bmod 4$ *ou qui est* $\equiv 8$ *ou* $12 \bmod 16$.

On remarque que $D \equiv 0 \bmod 4$ si b est pair et $D \equiv 1 \bmod 4$ si b est impair. Réciproquement, il existe au moins une forme binaire quadratique à coefficients entiers et de discriminant D pour tout $D \equiv 0$ ou $1 \bmod 4$. En effet, les formes $x^2 - \frac{D}{4}y^2$ pour $D \equiv 0 \bmod 4$ et $x^2 + xy + \frac{1-D}{4}y^2$ pour $D \equiv 1 \bmod 4$ sont appelées les formes principales de discriminant D .

Puisque $f(x,y) = ax^2 + bxy + cy^2$, on a que

$$\begin{aligned} 4a \cdot f(x,y) &= 4a^2x^2 + 4abxy + 4acy^2 = 4a^2x^2 + 4abxy + b^2y^2 + (4ac - b^2)y^2 \\ &= (2ax + by)^2 - Dy^2 \end{aligned}$$

Alors si $D < 0$, les valeurs prises par $f(x,y)$ seront toutes > 0 ou seront toutes < 0 (sauf en $x = 0 = y$). La forme $f(x,y)$ est alors respectivement appelée DÉFINIE POSITIVE (si $a > 0$) ou DÉFINIE NÉGATIVE (si $a < 0$).
Si $D = 0$, les valeurs prises par $f(x,y)$ seront toutes ≥ 0 ou seront toutes ≤ 0. La forme $f(x,y)$ est alors respectivement appelée SEMIDÉFINIE POSITIVE ou SEMIDÉFINIE NÉGATIVE.
Et si $D > 0$, $f(x,y)$ prendra des valeurs positivies et négatives et sera appelée INDÉFINIE.

Justement, parlant des valeurs prises par $f(x,y)$, on dit que la forme binaire quadratique $f(x,y)$ REPRÉSENTE un entier n s'il existe des entiers x_0, y_0 tels que $f(x_0, y_0) = n$. Une telle représentation est dite PROPRE si $\text{pgcd}(x_0, y_0) = 1$ et est dite IMPROPRE sinon.

Soit $f(x_0, y_0) = n$ une représentation impropre avec $\text{pgcd}(x_0, y_0) = g$. Alors $g^2 | n$, $\text{pgcd}(\frac{x_0}{g}, \frac{y_0}{g}) = 1$ et $f(\frac{x_0}{g}, \frac{y_0}{g}) = \frac{n}{g^2}$. Donc les représentations de n par la forme $f(x,y)$ peuvent être trouvées à l'aide des représentations propres de $\frac{n}{g^2}$ pour tout entier g tel que $g^2 | n$.

Il arrive que deux formes représentent exactement les mêmes nombres. Par exemple, si $f(x,y) = x^2 + y^2$ et $g(x,y) = x^2 + 2xy + 2y^2$, alors un petit changement de variables nous donne $g(x,y) = f(x+y, y)$ ou encore $f(x,y) = g(x-y, y)$. Ce changement de variable veut dire que les formes f et g représentent ici exactement le même ensemble d'entiers.

On cherche donc à établir des critères qui nous permettent de déterminer lorsque deux formes sont équivalentes.

Définition 8.1.3. *Soit (x, y) un point. Lorsque $x, y \in \mathbb{Z}$, le point (x, y) est appelé un POINT DE RÉSEAU.*

Déterminons maintenant quels changements de variables linéaires transforment l'ensemble des points de réseau en lui-même de façon bijective.

Théorème 8.1.1. *Soit $M = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix}$ une matrice 2x2 à entrées réelles. Posons*

$$\begin{bmatrix} u \\ v \end{bmatrix} = M \cdot \begin{bmatrix} x \\ y \end{bmatrix} \tag{8.1.1}$$

Alors les deux énoncés suivants sont équivalents :

i) la transformation linéaire (8.1.1) définit une permutation de points de réseau (un ensemble de points de réseau est envoyé sur lui-même de façon bijective)

ii) la matrice M est à coefficients entiers et dét$(M) = \pm 1$.

Remarque 8.1.1. *C'est analogue au théorème d'algèbre linéaire qui affirme que (8.1.1) définit une permutation de $\mathbb{R}^2$ si et seulement si dét$(M) \neq 0$.*

Démonstration du théorème.

(ii) $\Rightarrow$ (i) :

Si M est à coefficients entiers et que (x, y) est un point de réseau (c'est-à-dire $x, y \in \mathbb{Z}$), alors (u, v) est aussi un point de réseau. Puisque dét$(M) = \pm 1 \neq 0$, la matrice inverse M^{-1} existe et en fait $M^{-1} = \begin{bmatrix} \frac{m_{22}}{\Delta} & \frac{-m_{12}}{\Delta} \\ \frac{-m_{21}}{\Delta} & \frac{m_{11}}{\Delta} \end{bmatrix}$, où $\Delta :=$dét$(M) = \pm 1$. Bref M^{-1} sera aussi à coefficients entiers. On a ainsi l'application inverse $\begin{bmatrix} x \\ y \end{bmatrix} = M^{-1} \cdot \begin{bmatrix} u \\ v \end{bmatrix}$ qui indique que lorsque (u, v) est un point de réseau, alors (x, y) sera aussi un point de réseau.

L'application est injective. Supposons en effet que $M \cdot \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \begin{bmatrix} u \\ v \end{bmatrix}$ et que

$M \cdot \begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} u \\ v \end{bmatrix}$ avec $\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \neq \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$. Alors $\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = M^{-1} \cdot \begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$, une contradiction.

L'application est surjective. En effet, soit (u, v) un point de réseau. Alors $M^{-1} \cdot \begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$ et donc il existe un point de réseau (x, y) tel que $\begin{bmatrix} u \\ v \end{bmatrix} = M \cdot \begin{bmatrix} x \\ y \end{bmatrix}$. L'application est ainsi bijective. (Et on peut montrer de façon tout à fait similaire que l'application inverse est également bijective.)

(i) $\Rightarrow$ (ii) :

Supposons maintenant que la transformation linéaire (8.1.1) définisse une permutation de points de réseau. Considérons le point de réseau $(x, y) = (1, 0)$. L'équation (8.1.1) donne $u = m_{11}$ et $v = m_{21}$, où (u, v) est un point de réseau. Ce qui donne $m_{11}, m_{21} \in \mathbb{Z}$. En considérant le point de réseau $(x, y) = (0, 1)$, l'équation (8.1.1) donne $u = m_{12}$ et $v = m_{22}$, où (u, v) est un point de réseau. Ce qui donne $m_{12}, m_{22} \in \mathbb{Z}$. Bref, on a montré que la matrice M sera à coefficients entiers.

Il reste à montrer que dét$(M) = \pm 1$. Prenons le point de réseau $(u, v) = (1, 0)$. Puisque (i) implique que (8.1.1) est surjective, alors il existe un point de réseau (x_1, y_1) tel que $\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}$. De même, pour $(u, v) = (0, 1)$, il existe un point de réseau (x_2, y_2) tel que $\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} \cdot \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$.

On peut exprimer ces deux équations précédentes sous la seule équation matricielle suivante : $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} \cdot \begin{bmatrix} x_1 & x_2 \\ y_1 & y_2 \end{bmatrix}$. Un peu d'algèbre linéaire nous donne $1 = \text{dét}\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = \text{dét}(M) \cdot \text{dét}\left(\begin{bmatrix} x_1 & x_2 \\ y_1 & y_2 \end{bmatrix}\right)$. Et puisque $m_{11}, m_{12}, m_{21}, m_{22}, x_1, y_1, x_2, y_2 \in \mathbb{Z}$, alors $1 = \text{dét}(M) \cdot \text{dét}\left(\begin{bmatrix} x_1 & x_2 \\ y_1 & y_2 \end{bmatrix}\right)$,

où $\det(M) \in \mathbb{Z}$ et où $\det\left(\begin{bmatrix} x_1 & x_2 \\ y_1 & y_2 \end{bmatrix}\right) \in \mathbb{Z}$. Bref, $\det(M) \mid 1$.

$\therefore \det(M) = \pm 1$ □

On restreint maintenant notre attention sur les matrices où $\det(M) = \pm 1$.

Soient M et N deux matrices 2x2 à coefficients entiers et de déterminant 1. Alors $M \cdot N$ est une matrice 2x2 à coefficients entiers et $\det(M \cdot N) = \det(M) \cdot \det(N) = 1 \cdot 1 = 1$, d'où la propriété de fermeture. L'associativité est généralement vraie chez les matrices de même que l'existence de la matrice identité $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ qui est à coefficients entiers et de déterminant 1. La matrice inverse M^{-1} existe quant à elle et $\det(M^{-1}) = 1$, puisque $M^{-1} = \begin{bmatrix} \frac{m_{22}}{\det(M)} & \frac{-m_{12}}{\det(M)} \\ \frac{-m_{21}}{\det(M)} & \frac{m_{11}}{\det(M)} \end{bmatrix}$. Ainsi l'ensemble des matrices 2x2 à entrées entières et de déterminant 1 forme un groupe.

Définition 8.1.4. *Le groupe des matrices 2x2 à coordonnées entières et de déterminant 1 est noté $SL(2,\mathbb{Z})$ et est appelé le GROUPE SPÉCIAL LINAIRE DE DEGRÉ 2 SUR $\mathbb{Z}$.*

Nous sommes maintenant prêts à définir lorsque deux formes binaires quadratiques seront dites équivalentes et nous montrerons un peu plus loin que cela implique que deux formes équivalentes représentent le même ensemble d'entiers.

8.2. Équivalence entre formes binaires quadratiques

Définition 8.2.1. *Les formes binaires quadratiques $f(x,y) = ax^2 + bxy + cy^2$ et $g(x,y) = Ax^2 + Bxy + Cy^2$ sont dites ÉQUIVALENTES, et on écrit $f \sim g$, s'il existe une matrice $M = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} \in SL(2,\mathbb{Z})$ (c'est-à-dire à coordonnées entières et de déterminant 1) telle que $g(x,y) = f(m_{11}x + m_{12}y, m_{21}x + m_{22}y)$. On dit alors que M amène f sur g.*

On doit maintenant démontrer que la notion d'équivalence qu'on vient de définir est une relation d'équivalence, c'est-à-dire que c'est une relation réflexive, symétrique et transitive.

Mais avant cela, introduisons une notation matricielle à cette dernière définition. Ça permettra de raccourcir grandement les prochaines preuves en évitant les longs développements de variables.

Nous voulons une notation matricielle qui permettra d'exprimer l'égalité

$$Ax^2 + Bxy + Cy^2 = g(x,y) = f(m_{11}x + m_{12}y, m_{21}x + m_{22}y)$$
$$= a(m_{11}x + m_{12}y)^2 + b(m_{11}x + m_{12}y)(m_{21}x + m_{22}y) + c(m_{21}x + m_{22}y)^2$$
$$= (am_{11}^2 + bm_{11}m_{21} + cm_{21}^2)x^2 + (2am_{11}m_{12} + bm_{11}m_{22} + bm_{12}m_{21} + 2cm_{21}m_{22})xy$$
$$+ (am_{12}^2 + bm_{12}m_{22} + cm_{22}^2)y^2$$

c'est-à-dire qui permettra d'exprimer que

$$\begin{cases} A = am_{11}^2 + bm_{11}m_{21} + cm_{21}^2 \\ B = 2am_{11}m_{12} + bm_{11}m_{22} + bm_{12}m_{21} + 2cm_{21}m_{22} \\ C = am_{12}^2 + bm_{12}m_{22} + cm_{22}^2 \end{cases} \tag{8.2.1}$$

Posons $\quad F = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}, \quad G = \begin{bmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{bmatrix}$ et $\quad X = \begin{bmatrix} x \\ y \end{bmatrix}$

Alors $\quad M^tFM = \begin{bmatrix} m_{11} & m_{21} \\ m_{12} & m_{22} \end{bmatrix} \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix}$

$$= \begin{bmatrix} m_{11} & m_{21} \\ m_{12} & m_{22} \end{bmatrix} \begin{bmatrix} am_{11} + \frac{b}{2}m_{21} & am_{12} + \frac{b}{2}m_{22} \\ \frac{b}{2}m_{11} + cm_{21} & \frac{b}{2}m_{12} + cm_{22} \end{bmatrix}$$

$$= \begin{bmatrix} am_{11}^2 + bm_{11}m_{21} + cm_{21}^2 & \frac{2am_{11}m_{12} + bm_{11}m_{22} + bm_{12}m_{21} + 2cm_{21}m_{22}}{2} \\ \frac{2am_{11}m_{12} + bm_{11}m_{22} + bm_{12}m_{21} + 2cm_{21}m_{22}}{2} & am_{12}^2 + bm_{12}m_{22} + cm_{22}^2 \end{bmatrix}$$

$$= \begin{bmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{bmatrix} \quad = \quad G \qquad \text{par (8.2.1)}$$

Par ailleurs, on remarque aussi que $X^tFX = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$

$= \begin{bmatrix} ax + \frac{by}{2} & \frac{bx}{2} + cy \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax^2 + bxy + cy^2 \end{bmatrix} = \begin{bmatrix} f(x,y) \end{bmatrix}$

De même, $X^tGX = \begin{bmatrix} g(x,y) \end{bmatrix}$

Ainsi, on peut dire que deux formes binaires quadratiques f et g sont équivalentes si et seulement s'il existe une matrice $M \in \mathrm{SL}(2,\mathbb{Z})$ telle que $M^tFM = G$.

Maintenant que la notation matricielle est établie, il sera plus aisé de prouver le théorème suivant :

Théorème 8.2.1. *Soient f, g et h des formes binaires quadratiques. Alors*
1) $f \sim f$
2) Si $f \sim g$, alors $g \sim f$
3) Si $f \sim g$ et $g \sim h$, alors $f \sim h$

Démonstration. 1) La matrice identité $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ et elle est telle que $I^tFI = F$, d'où $f \sim f$.

2) Si $f \sim g$, alors il existe une matrice $M \in \mathrm{SL}(2,\mathbb{Z})$ telle que $M^tFM = G$. Pour montrer que $g \sim f$, on devra montrer qu'il existe une matrice $N \in \mathrm{SL}(2,\mathbb{Z})$ telle que $N^tGN = F$. Prenons pour ce faire la matrice inverse de M. On a $M^{-1} = \begin{bmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z})$. De plus, $(M^{-1})^tM^tFMM^{-1} = (M^{-1})^tGM^{-1} \Rightarrow (M^{-1})^tGM^{-1} = I^tFI = F$. Ainsi $g \sim f$.

3) Si $f \sim g$, alors il existe une matrice $M \in \mathrm{SL}(2,\mathbb{Z})$ telle que $M^tFM = G$. Et si $g \sim h$, alors il existe une matrice $N \in \mathrm{SL}(2,\mathbb{Z})$ telle que $N^tGN = H$.

$\Rightarrow\ H = N^t(M^tFM)N = (MN)^tF(MN)$ où la matrice $(M \cdot N) \in \mathrm{SL}(2,\mathbb{Z})$ puisque $\mathrm{SL}(2,\mathbb{Z})$ est un groupe. $\therefore f \sim h$. □

Nous prouvons maintenant que deux formes équivalentes représentent les mêmes entiers.

Théorème 8.2.2. *Soient f et g deux formes binaires quadratiques équivalentes, et soit $n \in \mathbb{Z}$. Alors les représentations de n par f sont en bijection avec les représentations de n par g. Les représentations propres de n par f sont aussi en bijection avec les représentations propres de n par g. Enfin, les discriminants respectifs de f et g seront égaux.*

Démonstration. Tout d'abord, $f \sim g \ \Rightarrow$ il existe une matrice $M \in \mathrm{SL}(2,\mathbb{Z})$ telle que $g(x,y) = f(m_{11}x + m_{12}y, m_{21}x + m_{22}y)$.
Soit $n \in \mathbb{Z}$ et soit $g(x_1,y_1)$ une représentation de n par g. Alors $n = g(x_1,y_1) = f(m_{11}x_1 + m_{12}y_1, m_{21}x_1 + m_{22}y_1) = f(u_1,v_1)$ pour un seul et unique point de réseau (u_1,v_1), selon le théorème (8.1.1).
De même, on prouve la réciproque en utilisant la matrice $M^{-1} \in \mathrm{SL}(2,\mathbb{Z})$. Ce qui prouve la première affirmation du théorème.

Pour prouver la seconde affirmation, il reste à montrer qu'une représentation propre de n par f correspond à une représentation propre de n par g, et vice versa. Ainsi soit $g(x,y)$ une représentation et soit $f(u,v)$ la représentation correspondante. Si $r = \mathrm{pgcd}(x,y)$ et $s = \mathrm{pgcd}(u,v)$, alors $g(\frac{x}{r},\frac{y}{r})$ sera une représentation propre. Comme $\frac{1}{r} \cdot \begin{bmatrix} x \\ y \end{bmatrix}$ est un point de réseau, alors $M \cdot \left(\frac{1}{r} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \right) = \frac{1}{r} \cdot \left(M \cdot \begin{bmatrix} x \\ y \end{bmatrix} \right) = \frac{1}{r} \cdot \begin{bmatrix} u \\ v \end{bmatrix}$ est aussi un point de réseau par le théorème (8.1.1), c'est-à-dire que $r|u$ et $r|v$, d'où $r|s$. Réciproquement, on prouve que $s|r$ et donc $r = s$. D'où $f(\frac{u}{r},\frac{v}{r})$ est aussi une représentation propre

puisque $\text{pgcd}(\frac{u}{r}, \frac{v}{r}) = \text{pgcd}(\frac{u}{s}, \frac{v}{s}) = 1$.

Pour démontrer la troisième affirmation, soit $d = b^2 - 4ac$ et $D = B^2 - 4AC$ les discriminants respectifs de f et g. Alors $-\frac{D}{4} = \text{dét}(G) = \text{dét}(M^t F M)$
$= \text{dét}(M^t) \cdot \text{dét}(F) \cdot \text{dét}(M) = 1 \cdot \text{dét}(F) \cdot 1 = -\frac{d}{4}$
$\therefore d = D$. □

On a montré précédemment que la relation $\sim$ était une relation d'équivalence. On peut donc partitionner l'ensemble des formes binaires quadratiques en classes d'équivalence.

Définition 8.2.2. *Soit $D \in \mathbb{Z}$, où D n'est pas un carré parfait. Le nombre de classes d'équivalence parmi les formes binaires quadratiques de discriminant D est appelé le NOMBRE DE CLASSES de D, et est noté $h(D)$. (Lorsque le contexte l'exigera, nous l'appellerons le nombre de classes de formes de D, pour ne pas le confondre avec un autre nombre de classes que l'on définira subséquemment.)*

À prime abord, il n'est toutefois pas aisé de déterminer si deux formes sont équivalentes, car on doit statuer sur l'existence ou non d'une matrice M. Il est donc encore moins aisé de déterminer le nombre de classes de D, puisque parmi toutes les formes binaires quadratiques possibles de discriminant D, on doit les classer en classes d'équivalence avant de compter le nombre de classes. Ça prend donc un autre outil pour nous aider à déterminer le nombre de classes. On utilisera donc les formes réduites, puisqu'à partir de n'importe quelle forme binaire quadratique, on peut trouver une forme réduite qui lui est équivalente.

8.3. Réduction d'une forme binaire quadratique

Nous étudierons dans un premier temps la réduction pour les formes binaires quadratiques de discriminant $D < 0$ et dans un deuxième temps pour les formes binaires quadratiques de discriminant $D > 0$.

8.3.1. Réduction des formes binaires quadratiques de discriminant $D < 0$

Définition 8.3.1. *Soit* $f(x,y) = ax^2+bxy+cy^2$ *une forme binaire quadratique de discriminant* $D < 0$, *où* $D \in \mathbb{Z}$ *n'est pas un carré parfait. On dit que* f *est RÉDUITE si* $-|a| < b \leq |a| < |c|$ *ou si* $0 \leq b \leq |a| = |c|$.

Il existe un algorithme qui permet d'obtenir une forme réduite à partir d'une quelconque forme binaire quadratique de discriminant n'étant pas un carré parfait, en demeurant dans la même classe d'équivalence. Cet algorithme est composé de deux transformations qui sont répétées jusqu'à l'obtention d'une forme réduite. Avant de décrire ces deux transformations, mentionnons que le discriminant $D = b^2 - 4ac$ de la forme f , n'étant pas un carré parfait, indique qu'on aura $a \neq 0$ et $c \neq 0$.

La première transformation est appliquée lorsque $|a| > |c|$ ou lorsqu'on a $|a| = |c|$ et $-|a| \leq b < 0$. On utilise dans ce cas la matrice $M = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ et on a alors $f(x,y) \sim g(x,y) = f(y,-x) = ay^2 + by(-x) + c(-x)^2 = cx^2 - bxy + ay^2$.
On a donc interchangé a et c tout en prenant $-b$ au lieu de b . Si on avait $|a| = |c|$ avec $-|a| \leq b < 0$, on a maintenant $0 < b \leq |a| = |c|$, ce qui donne ici une forme réduite. Et si on avait $|a| > |c|$, on a maintenant $|a| < |c|$; il reste ici à vérifier la valeur de b pour vérifier si la forme est réduite ou non.

La seconde transformation est appliquée lorsque b n'est pas compris dans l'intervalle $]-|a|, |a|\,]$, c'est-à-dire lorsque $b \leq -|a|$ ou lorsque $b > |a|$. On utilise alors la matrice $M = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ et on obtient $f(x,y) \sim g(x,y) = f(x+my, y) = a(x+my)^2+b(x+my)y+cy^2 = ax^2+(2am+b)xy+(am^2+bm+c)y^2$.
On doit choisir m comme étant l'unique entier tel que $-|a| < b+2am \leq |a|$. La forme ainsi obtenue n'est toutefois pas nécessairement réduite puisqu'il se peut

que $|am^2 + bm + c| \leq |a|$.
Si $|am^2 + bm + c| = |a|$ et $-|a| < b + 2am < 0$, alors la forme deviendra réduite après une application de la première transformation. Et sinon, si $|am^2 + bm + c| < |a|$, alors on recommence la séquence des deux transformations, au besoin.

On doit alors forcément aboutir à une forme réduite en un nombre fini d'étapes, puisque quand on répète ces deux transformations, soit on obtient une forme réduite ou soit le coefficient de x^2 est strictement décroissant (à chaque application de la première transformation).

Théorème 8.3.1. *Soit $D \in \mathbb{Z}$, $D < 0$ n'étant pas un carré parfait. Toutes les classes d'équivalence parmi les formes binaires quadratiques de discriminant D contiennent au moins une forme réduite.*

Démonstration. Toute classe d'équivalence contient au moins une forme et toute forme peut être réduite tout en préservant l'équivalence, comme on vient de le démontrer. □

Il est démontré dans le théorème précédent que toute classe d'équivalence parmi les formes binaires quadratiques de discriminant $D < 0$ contient au moins une forme réduite. Nous nous emploierons maintenant à montrer que c'est en fait exactement une forme réduite, c'est-à-dire qu'il y a une et une seule forme réduite dans chaque classe d'équivalence pour $D < 0$. Bref, nous avons démontré l'existence et nous montrerons l'unicité.

Lemme 8.3.1. *Soit $f(x, y) = ax^2+bxy+cy^2$ une forme réduite définie positive. Si pour certains $x, y \in \mathbb{Z}$ nous avons $pgcd(x, y) = 1$ et $f(x, y) \leq c$, alors $f(x, y) = a$ ou c et le point (x, y) est un des six suivants : $\pm(1, 0)$, $\pm(0, 1)$,*

$\pm(1,-1)$. *De plus, le nombre de représentations propres de* a *par* f *est* $\begin{cases} 2 & si\ a < c \\ 4 & si\ 0 \le b < a = c \\ 6 & si\ a = b = c \end{cases}$.

DÉMONSTRATION. Supposons que $\text{pgcd}(x,y) = 1$.

Si $y = 0$, alors $x = \pm 1$ (pour avoir $\text{pgcd}(x,y) = 1$) et on remarque que $f(\pm 1, 0) = a$, d'où une partie du premier résultat.

Si $y = \pm 1$ et $|x| \ge 2$, alors

$|2ax + by| \ \ge\ |2ax| - |by|$ par l'inégalité du triangle

$\ge\ 2a \cdot 2 - |b| \ \ge\ 4a - |a| \ =\ 3a$ puisque f réduite $\Rightarrow\ |b| \le |a|$

et f définie positive $\Rightarrow\ a > 0$

D'où $4af(x,y) \ =\ (2ax+by)^2 - Dy^2 \ \ge\ 9a^2 - Dy^2 \ =\ 9a^2 - D$

$= 9a^2 - (b^2 - 4ac) \ >\ a^2 + 4ac - b^2$ (puisque $a \ne 0$)

$\ge\ 4ac$ (puisque $|b| \le |a| \ \Rightarrow\ b^2 \le a^2$)

$\Rightarrow f(x,y) > c$

Si $|y| \ge 2$, alors

$4af(x,y) \ =\ (2ax+by)^2 - Dy^2 \ \ge\ -Dy^2 \ \ge\ -4D \ =\ -4(b^2 - 4ac)$

$>\ 8ac - 4b^2$ (en effet $ac > 0$ puisque $0 > D = b^2 - 4ac$)

$\ge\ 4a^2 + 4ac - 4b^2$ (car f réduite $\Rightarrow\ |a| \le |c|$)

$\ge\ 4ac$ (car f réduite $\Rightarrow\ |b| \le |a|$)

$\Rightarrow\ f(x,y) > c$

Il reste les possibilités suivantes pour (x,y) : $\pm(1,0), \pm(0,1), \pm(1,-1), \pm(1,1)$.

Or $f(1,1) \ =\ a+b+c \ >\ c$

puisque f réduite définie positive $\Rightarrow$ ($a+b > 0$ ou ($b \ge 0$ et $a > 0$)) .

Quant à $\pm(1,-1)$, on a

$f(\pm 1, \mp 1) \ =\ a - b + c \ \le\ c \ \Leftrightarrow\ a \le b$ or f réduite et on a ici $a \ge b$

$f(\pm 1, \mp 1) = a - b + c \leq c \quad \Leftrightarrow \quad a = b$ et dans ce cas $f(\pm 1, \mp 1) = c$
Aussi $f(0, \pm 1) = c$.

Pour la seconde affirmation du lemme, on constate que si $a < c$, alors $f(\pm 1, 0)$ sont les deux seules représentations propres de a par f .
Si $0 \leq b < a = c$, alors on aura aussi $f(0, \pm 1) = c = a$.
Et si $a = b = c$, on rajoutera $f(\pm 1, \mp 1) = c = a$. □

Théorème 8.3.2. *Soient* $f(x, y) = ax^2 + bxy + cy^2$ *et* $g(x, y) = Ax^2 + Bxy + Cy^2$ *deux formes binaires quadratiques réduites et définies positives.*
Si $f \sim g$, *alors* $f = g$.

Démonstration. Supposons que $f \sim g$.
Par le lemme précédent, a est le plus petit nombre positif représenté proprement par f et c'est A dans le cas de g . Par le théorème (8.2.2), a est aussi représenté proprement par g , d'où $a \geq A$, et A est également représenté proprement par f , d'où $A \geq a$. Bref, $a = A$.

1^o Considérons le cas $a < c$
Par le lemme précédent, il y a exactement deux représentations propres de a par f et par le théorème (8.2.2), il y a aussi deux représentations propres de a par g , ce qui nous indique que $a = A < C$ par le lemme précédent. Toujours par le lemme précédent, puisqu'on a $a < c$ et $A < C$, c est le plus petit entier strictement supérieur à a qui est représenté proprement par f et C est le plus petit entier strictement supérieur à A qui est représenté proprement par g . Par le théorème (8.2.2), c est aussi représenté proprement par g , d'où $c \geq C$, et C est aussi représenté proprement par f , d'où $C \geq c$. Bref, $c = C$.

Pour montrer que $b = B$, on considère les matrices $M \in \mathrm{SL}(2, \mathbb{Z})$ pouvant amener f sur g .
Puisque $\det(M) = m_{11}m_{22} - m_{21}m_{12} = 1$, alors $\mathrm{pgcd}(m_{11}, m_{21}) = 1$. Ainsi

l'équation (8.2.1) indique que $f(m_{11}, m_{21}) = A = a$ est une représentation propre de a, d'où en fait les deux seules représentations propres de a sont $(m_{11}, m_{21}) = (\pm 1, 0)$.

De façon similaire, $\text{pgcd}(m_{22}, m_{12}) = 1$ et l'équation (8.2.1) indique que $f(m_{12}, m_{22}) = C = c$ est une représentation propre de c, d'où $(m_{12}, m_{22}) = (0, \pm 1)$ ou $\pm(1, -1)$.

Ainsi, puisque $\text{dét}(M) = 1$, les candidats possibles pour M sont $\pm I$ et $\pm \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$. Or, si $M = \pm \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$, alors l'équation (8.2.1) donne $B = -2a + b$. Mais f et g étant toutes deux réduites et définies positives, on a $-a < b \leq a$ et $-a = -A < B \leq A = a \Rightarrow -a < -2a + b \leq a \Rightarrow a < b$ $\rightarrow\leftarrow$ une contradiction.

Alors $M = \pm I$ et l'équation (8.2.1) donne $B = b$.

$\therefore f = g$

2^o Considérons le cas $a = c$

Par le lemme précédent, il y a 4 ou 6 représentations propres de a par f. Par le théorème (8.2.2), il y a aussi quatre ou six représentations propres de a par g, ce qui nous indique que $c = a = A = C$ par le lemme précédent.

Le théorème (8.2.2) nous indique également que les discriminants de f et g sont égaux, d'où : $b^2 - 4ac = B^2 - 4AC = B^2 - 4ac \Rightarrow b^2 = B^2$ et puisque par la définition (8.3.1) on a $0 \leq b \leq a$ et $0 \leq B \leq A$, alors $b = B$.

$\therefore f = g$ □

Ainsi on obtient ce qui suit :

Théorème 8.3.3. - *Si $D < 0$, toutes les classes d'équivalence parmi les formes binaires quadratiques de discriminant D contiennent en fait exactement une forme réduite. La forme réduite est unique dans chaque classe d'équivalence.*

- Ainsi, pour $D < 0$, le nombre de formes réduites distinctes de discriminant D est égal à $h(D)$, le nombre de classes d'équivalence de formes de discriminant D.

Théorème 8.3.4. *Soit* $f(x,y) = ax^2+bxy+cy^2$ *une forme binaire quadratique réduite de discriminant* $D < 0$ *, où* D *n'est pas un carré parfait. Si* f *est définie positive, alors* $0 < a \leq \sqrt{-\frac{D}{3}}$ *. Le nombre de formes réduites de discriminant* D *est fini. Ainsi* $h(D)$ *est fini pour* $D < 0$ *.*

Démonstration. Si f est définie positive, alors $a > 0$ et $D < 0$.
$\Rightarrow$ $c > 0$ puisque $D = b^2 - 4ac$.
$\Rightarrow$ $D = b^2 - 4ac \leq a^2 - 4ac = a^2 - 4 \cdot |a| \cdot |c| \leq a^2 - 4 \cdot |a| \cdot |a| = -3a^2$
$\Rightarrow$ $a^2 \leq -\frac{D}{3}$ $\Rightarrow$ $a \leq \sqrt{-\frac{D}{3}}$ puisque $a > 0$

Ainsi, pour $D < 0$ fixé, a est borné et f étant réduite, b est bornée par a . Pour D fixé, a et b ne peuvent donc prendre qu'un nombre fini de valeurs. Et puisque $D = b^2 - 4ac$, il existe au plus une valeur entière de c qui corresponde à un triplet (D, a, b) .

$\therefore$ Le nombre de formes réduites de discriminant $D < 0$ est fini. Et $h(D)$ étant égal à ce nombre, il est fini lui aussi. □

8.3.2. Réduction des formes binaires quadratiques de discriminant $D > 0$

Dans le cas des formes binaires quadratiques indéfinies, les différents ouvrages ne donnent pas tous la même définition. Celui de Niven & Zuckerman donne la même définition pour $D > 0$ que pour $D < 0$, ce qui simplifie peut-être la réduction, mais ça a le désavantage de pouvoir avoir plus qu'une formes réduites qui seraient équivalentes. Par exemple, **[Jo]** mentionne $f(x,y) = x^2 - 23y^2$ et $g(x,y) = 2x^2 + 2xy - 11y^2$ qui sont toutes deux réduites selon la définition de Niven, car $-|1| < 0 \leq |1| < |-23|$ pour f et $-|2| < 2 \leq |2| < |-11|$ pour g , mais qui sont aussi équivalentes puisque la transformation $M = \begin{bmatrix} 2 & 9 \\ 1 & 5 \end{bmatrix}$

amène g sur f. En effet,

$$M^tGM = \begin{bmatrix} 2 & 1 \\ 9 & 5 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ 1 & -11 \end{bmatrix} \cdot \begin{bmatrix} 2 & 9 \\ 1 & 5 \end{bmatrix} = \begin{bmatrix} 5 & -9 \\ 23 & -46 \end{bmatrix} \cdot \begin{bmatrix} 2 & 9 \\ 1 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -23 \end{bmatrix} = F$$

Buchmann ([**Bu**]) et Buell ([**Bue**]) présentent quant à eux des définitions équivalentes qui diffèrent de celle de Niven. Cette définition a l'avantage de pouvoir imposer des conditions pour n'avoir qu'une seule forme réduite (en fait un seul cycle de formes réduites) par classe d'équivalence. C'est une telle définition que nous utiliserons.

Définition 8.3.2. *Soit* $f(x,y) = ax^2+bxy+cy^2$ *une forme binaire quadratique de discriminant* $D > 0$, *où* $D \in \mathbb{Z}$ *n'est pas un carré parfait. On dit que* f *est RÉDUITE si* $\begin{cases} 0 < b < \sqrt{D} \\ \sqrt{D} - b < 2 \cdot |a| < \sqrt{D} + b \end{cases}$.

Proposition 8.3.1. *Soit* $f(x,y) = ax^2 + bxy + cy^2$ *une forme binaire quadratique réduite de discriminant* $D > 0$, *où* $D \in \mathbb{Z}$.
Alors $\sqrt{D} - b < 2 \cdot |c| < \sqrt{D} + b$.

Démonstration.

$$D = b^2 - 4ac \quad \Rightarrow \quad 0 = 0 \cdot 0 < (\sqrt{D} - b)(\sqrt{D} + b) = -4ac = (2|a|)\,(2|c|)$$

$$2|c| = \frac{(\sqrt{D} - b)}{2|a|}\,(\sqrt{D} + b) < \sqrt{D} + b \qquad \text{car } f \text{ réduite}$$

$$2|c| = (\sqrt{D} - b)\,\frac{(\sqrt{D} + b)}{2|a|} > \sqrt{D} - b \qquad \text{car } f \text{ réduite}$$

□

Théorème 8.3.5. *Le nombre de formes binaires quadratiques réduites, pour un discriminant* $D > 0$ *donné, est fini.*

DÉMONSTRATION. Puisque f est réduite ($\Rightarrow \quad 0 < b < \sqrt{D}$) et que D est fixé, alors b ne peut prendre qu'un nombre fini de valeurs. Ensuite, les inégalités $\sqrt{D} - b < 2 \cdot |a| < \sqrt{D} + b$ et $\sqrt{D} - b < 2 \cdot |c| < \sqrt{D} + b$ entraînent que a et c aussi ne peuvent prendre qu'un nombre fini de valeurs, d'où le résultat. □

Nous donnerons maintenant un algorithme de réduction pour les formes indéfinies. Ainsi, ça prouvera que toutes les classes d'équivalence parmi les formes binaires quadratiques de discriminant $D > 0$ (D pas un carré parfait) contiennent au moins une forme réduite.

Théorème 8.3.6. *Soit $f(x, y) = ax^2 + bxy + cy^2$ une forme binaire quadratique indéfinie, de discriminant $D > 0$, D n'étant pas un carré parfait. Alors on peut trouver une forme réduite $g(x, y)$, équivalente à $f(x, y)$, qui soit de même discriminant que f .*

DÉMONSTRATION. Nous donnerons un algorithme de réduction pour f , si f n'est pas déjà réduite.
Puisque $D = b^2 - 4ac$ n'est pas un carré parfait, alors $a \neq 0$ et $c \neq 0$.
Il est évident que $\sqrt{D} - 2|c| < \sqrt{D}$ et on peut trouver un unique $\delta \in \mathbb{Z}$ tel que $\sqrt{D} - 2|c| < -b + 2c\delta < \sqrt{D}$.
La forme $f(x, y) = ax^2 + bxy + cy^2$ est équivalente à la forme $cx^2 + (-b + 2c\delta)xy + (a - b\delta + c\delta^2)y^2$ par la matrice $M = \begin{bmatrix} 0 & -1 \\ 1 & \delta \end{bmatrix}$.
Puisque a et c sont $\neq 0$, alors c le coefficient de x^2 dans la nouvelle forme est non nul, de même que $a - b\delta + c\delta^2$ le coefficient de y^2 . En effet, $a - b\delta + c\delta^2 = 0 \quad \Leftrightarrow \quad \delta = \dfrac{b \pm \sqrt{b^2 - 4ac}}{2c} = \dfrac{b \pm \sqrt{D}}{2c}$. Or, δ a été choisi comme étant $\in \mathbb{Z}$ mais $\dfrac{b \pm \sqrt{D}}{2c} \notin \mathbb{Z}$ puisque D n'est pas un carré parfait. Bref $a - b\delta + c\delta^2 \neq 0$.
Si $|a - b\delta + c\delta^2| < |c|$, on répète le processus de trouver une nouvelle forme

équivalente à l'aide de la matrice $M_i = \begin{bmatrix} 0 & -1 \\ 1 & \delta_i \end{bmatrix}$. Le processus comporte un nombre fini d'étapes, car le coefficient de x^2 en valeur absolue rapetisse tout le temps à chaque itération du processus. À la fin, on se retrouve avec une forme $g(x,y) = Ax^2 + Bxy + Cy^2$, équivalente à f, telle que $|A| \leq |C|$ et telle que $\sqrt{D} - 2|A| < B < \sqrt{D}$ puisque chacun des δ ou δ_i a été choisi de façon à ce que $\sqrt{D} - 2|c| < -b + 2c\delta < \sqrt{D}$.

$\Rightarrow \quad 0 < \sqrt{D} - B < 2|A| \qquad \text{et} \qquad 2|C| = \dfrac{|4AC|}{2|A|} = \dfrac{|D - B^2|}{2|A|}$

$$= |\sqrt{D} + B| \cdot \frac{|\sqrt{D} - B|}{2|A|} = |\sqrt{D} + B| \cdot \frac{(\sqrt{D} - B)}{2|A|} < |\sqrt{D} + B|$$

$\Rightarrow \quad |\sqrt{D} + B| > 2|C| \geq 2|A| > \sqrt{D} - B$

$\Rightarrow \quad |\sqrt{D} + B| > \sqrt{D} - B > 0 \qquad$ si $B = 0 \Rightarrow \sqrt{D} > \sqrt{D} \quad \rightarrow\leftarrow$ impossible

si $B < 0 \Rightarrow \sqrt{D} - B = \sqrt{D} + |B| \geq |\sqrt{D} + B| \quad \rightarrow\leftarrow$ impossible

Ainsi $B > 0$. Et $2|A| < |\sqrt{D} + B| = \sqrt{D} + B$

$\therefore \quad 0 < B < \sqrt{D}$ et $\sqrt{D} - B < 2|A| < \sqrt{D} + B$, c'est-à-dire $g(x,y)$ est réduite. □

Théorème 8.3.7. *Soit $D \in \mathbb{N}$, D n'étant pas un carré parfait. Alors $h(D)$ est fini.*

Démonstration. Il y a au moins une forme réduite dans chaque classe d'équivalence. Ainsi $h(D)$ est majoré par le nombre de formes binaires quadratiques réduites de discriminant D, lequel est fini. □

Nous avons mentionné au début de la présente sous-section que l'avantage de la définition de forme réduite que nous utilisons est de n'avoir qu'un seul cycle de formes réduites par classe d'équivalence, ce qui est bien puisque le nombre de cycles de formes réduites sera égal au nombre de classes. Élaborons quelque peu sur ce sujet.

Définition 8.3.3. *On définit deux formes réduites* $ax^2+bxy+a'y^2$ *et* $a'x^2+b'xy+a''y^2$ *comme étant ADJACENTES si* $b+b' \equiv 0 \bmod 2a'$.

Notation : Une forme binaire quadratique $ax^2+bxy+cy^2$ peut être notée (a,b,c) par soucis de concision lorsque le contexte ne peut pas engendrer d'ambiguïté.

Lemme 8.3.2. *Soit* (a,b,c) *une forme binaire quadratique réduite et* (c,e,f) *une autre forme binaire quadratique réduite de même discriminant* D *qui lui est adjacente. Cette forme* (c,e,f) *est unique, c'est-à-dire que les valeurs* e *et* f *sont uniques.*

Démonstration. La forme (c,e,f) étant réduite (voir définition 8.3.2), nous aurons $0<e<\sqrt{D}$, choisissons e de façon à ce qu'il soit minimal. Supposons que (c,e_1,f_1) soit elle aussi adjacente à (a,b,c) . Par le choix de e , nous aurons $e_1>e$. Nous avons $e+b \equiv e_1+b \equiv 0 \bmod 2c \Rightarrow e=-b+2cn$ et $e_1 \geq e+2|c|$.
Or, (c,e,f) réduite $\Rightarrow \sqrt{D}-e<2\cdot|c| \Rightarrow \sqrt{D}-e_1 \leq \sqrt{D}-(e+2|c|)<0$ et si (c,e_1,f_1) était réduite, on aurait $\sqrt{D}-e_1>0 \quad \rightarrow\leftarrow$ une contradiction. Il ne peut pas y avoir de forme (c,e_1,f_1) adjacente à (a,b,c) et différente de (c,e,f) , puisqu'une fois e choisi de façon unique, la relation $D=e^2-4cf$ implique un unique choix pour f . □

Proposition 8.3.2. *L'ensemble des formes binaires quadratiques réduites, pour un discriminant* $D>0$ *donné, peut être partitionné en cycles de formes adjacentes.*

Démonstration. L'ensemble des formes binaires quadratiques réduites, pour un discriminant $D>0$ donné, est fini, tel que prouvé au théorème (8.3.5). Ça implique que la liste des formes adjacentes successives (a,b,a'), (a',b',a''),

(a'', b'', a'''), ... est finie et doit donc aboutir à une certaine forme $(a^{(n-1)}, b^{(n-1)}, a)$ avant de retourner à la forme originale (a, b, a'). Si on ne revient pas à la forme initiale, la finitude de l'ensemble serait contredite.
Ceci donne un premier cycle de formes adjacentes.
Si ce cycle représente la totalité des formes binaires quadratiques réduites de discriminant $D > 0$, alors le processus est terminé. Sinon on choisit une forme qui n'a pas encore été utilisée dans un cycle et on trouve son cycle. On répète ce processus jusqu'à ce que l'ensemble des formes binaires quadratiques réduites de discriminant $D > 0$ soit partitionné en cycles de formes adjacentes. □

Proposition 8.3.3. *Soient deux formes binaires quadratiques réduites. Si elles sont dans le même cycle, alors elles sont équivalentes.*

Démonstration. Soient les deux formes adjacentes $f = (a, b, a')$ et $g = (a', b', a'')$. Elles sont équivalentes puisque la transformation $M = \begin{bmatrix} 0 & -1 \\ 1 & \frac{b+b'}{2a'} \end{bmatrix}$ amène f sur g. En effet,

$$\begin{aligned} M^tFM &= \begin{bmatrix} 0 & 1 \\ -1 & \frac{b+b'}{2a'} \end{bmatrix} \cdot \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & a' \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & \frac{b+b'}{2a'} \end{bmatrix} = \begin{bmatrix} \frac{b}{2} & a' \\ -a + \frac{b(b+b')}{4a'} & \frac{b'}{2} \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & \frac{b+b'}{2a'} \end{bmatrix} \\ &= \begin{bmatrix} a' & \frac{-b}{2} + \frac{b+b'}{2} \\ \frac{b'}{2} & a - \frac{-b(b+b')}{4a'} + \frac{b'(b+b')}{4a'} \end{bmatrix} = \begin{bmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & a + \frac{b'^2-b^2}{4a'} \end{bmatrix} = \begin{bmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & \frac{4aa'-b^2+b'^2}{4a'} \end{bmatrix} \\ &= \begin{bmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & \frac{-D+b'^2}{4a'} \end{bmatrix} = \begin{bmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & a'' \end{bmatrix} = G \end{aligned}$$

Puisque toutes formes adjacentes sont équivalentes, alors par transitivité de la relation d'équivalence, toutes les formes d'un même cycles sont équivalentes. □

La réciproque de la proposition précédente est plus longue et compliquée. Elle peut être trouvée dans [**Bue**]. La proposition et sa réciproque forment ensemble le théorème suivant :

Théorème 8.3.8. *Soient deux formes binaires quadratiques réduites. Elles sont dans le même cycle si et seulement si elles sont équivalentes.*

Corollaire 8.3.1. *Soit* $D \in \mathbb{N}$, D *n'étant pas un carré parfait. Le nombre de cycles de formes réduites est égal au nombre de classes.*

Fin de la sous-section 8.3.2

Remarque 8.3.1.

- Pour $D < 0$ *, on sait maintenant qu'il n'y a que neuf discriminants pour lesquels* $h(d) = 1$ *. Ce sont* $D \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$.

- Pour $D > 0$ *, Gauss a conjecturé qu'il y aurait une infinité de* $D \in \mathbb{N}$, D *étant un discriminant fondamental, pour lesquels* $h(D) = 1$.

Remarque 8.3.2. *Comme nous le mentionnions dans l'introduction de ce chapitre, un nombre de classes égal à* 1 *implique la factorisation unique en premiers dans un anneau d'entiers quadratiques* θ *. En fait, le nombre de classes est égal à* 1 *si et seulement si* θ *est un domaine d'idéaux principaux (PID). Et tout domaine d'idéaux principaux (PID) est un domaine de factorisation unique (UFD). Le nombre de classes indique à quel point les idéaux de* θ *sont près d'être principaux. La conjecture de Gauss tout juste citée est donc équivalente au fait de dire qu'il y aurait une infinité de corps quadratiques réels ayant la factorisation unique.*

Remarque 8.3.3. *Gauss a prouvé que si* D *n'est pas un carré parfait, alors il existe des formules de composition reliant les différentes classes d'équivalence de formes binaires quadratiques primitives (voir définition 8.5.3) de discriminant* D *. Ces formules de composition entraînent lesdites classes d'équivalence à former un groupe abélien. Il fut découvert par la suite que cela correspondait à la structure de classes d'idéaux dans un corps quadratique de discriminant* D *. Si on avait*

permis des matrices de déterminant -1 *dans la définition (8.1.4) , la structure de groupe n'aurait pas tenu.*

8.4. Le nombre de classes d'idéaux

Nous quittons brièvement dans cette section les formes binaires quadratiques et nous revenons sur le sujet des corps quadratiques, afin de définir un autre nombre de classes, dit le nombre de classes d'idéaux.

Soient $\mathbb{Q}(\sqrt{d})$ un corps quadratique et θ l'ensemble des entiers algébriques de $\mathbb{Q}(\sqrt{d})$, θ étant un sous-anneau de $\mathbb{Q}(\sqrt{d})$. Un idéal I de θ est un sous-groupe additif de θ tel que $\forall\, \alpha \in I$ et $\forall\, \xi \in \theta$, on a $\alpha\, \xi \in I$. L'ensemble $(\beta) := \{\xi \cdot \beta \mid \xi \in \theta\}$ est l'idéal engendré par $\beta \in \theta$.

Définition 8.4.1. *On dit que deux idéaux* I *et* J *de* θ *sont STRICTEMENT ÉQUIVALENTS s'il existe* $\alpha, \beta \in \theta$ *tels que* $(\alpha) \cdot I = (\beta) \cdot J$ *avec* $N(\alpha \cdot \beta) > 0$. *On dira alors que* I *et* J *sont dans la même CLASSE D'ÉQUIVALENCE ÉTROITE D'IDÉAUX et on définit* H_i^+ *comme étant le groupe abélien fini modulo cette relation d'équivalence.* H_i^+ *sera appelé le GROUPE DE CLASSES ÉTROIT D'IDÉAUX et sa cardinalité, notée* $h_i^+(d)$ *, sera appelée le NOMBRE DE CLASSES ÉTROIT D'IDÉAUX.*

Définition 8.4.2. *On dit que deux idéaux* I *et* J *de* θ *sont ÉQUIVALENTS s'il existe* $\alpha, \beta \in \theta$ *tels que* $(\alpha) \cdot I = (\beta) \cdot J$.
On dira alors que I *et* J *sont dans la même CLASSE D'ÉQUIVALENCE LARGE D'IDÉAUX et on définit* H_i *comme étant le groupe abélien fini modulo cette relation d'équivalence.* H_i *sera appelé le GROUPE DE CLASSES D'IDÉAUX (ou parfois le groupe de classes large d'idéaux) et sa cardinalité, notée* $h_i(d)$ *, sera appelée le NOMBRE DE CLASSES D'IDÉAUX (ou parfois le nombre de classes large d'idéaux).*

Remarque 8.4.1. - *Soit* $\mathbb{Q}(\sqrt{d})$ *un corps quadratique de discriminant* D *. Le nombre de classes de formes de* D *est égal au nombre de classes étroit d'idéaux de* d *, c'est-à-dire que* $h(D) = h_i^+(d)$ *.*
- Par ailleurs, il existe une relation entre $h_i^+(d)$ *et* $h_i(d)$ *. On a que*

$$h(D) = h_i^+(d) = \begin{cases} h_i(d) & \text{si } d < 0 \text{ ou si } (d > 0 \text{ et } N(\varepsilon_d) = -1) \\ 2 \cdot h_i(d) & \text{si } d > 0 \text{ et } N(\varepsilon_d) = 1 \end{cases}$$

8.5. Formule du nombre de classes de Dirichlet

Bien qu'on ait vu que le nombre de classes de formes ne peut pas être calculé aisément par sa définition, on a exposé une façon de le majorer en utilisant les formes réduites. Il serait toutefois utile d'avoir d'autres façons de le calculer ou d'avoir d'autres relations faisant intervenir le nombre de classes. La formule du nombre de classes de Dirichlet met en relation le nombre de classes d'idéaux avec les fonctions-L. Cette formule, dans sa forme la plus simple, a tout d'abord été conjecturée par Jacobi en 1832 et a été prouvée par Dirichlet en 1839.

La formule fut trouvée par Dirichlet au moment où il travaillait sur le problème des nombres premiers dans les progressions arithmétiques. Rappelons qu'on croyait, bien avant l'époque de Dirichlet, que toute progression arithmétique $\{a, a+q, a+2q, ...\}$, où a et q sont relativement premiers, comportait une infinité de nombres premiers. La première preuve fut de Dirichlet mais n'était valide que lorsque q était lui-même premier. Pour le cas général où $\text{pgcd}(a, q) = 1$ pour tout a et $q \in \mathbb{N}$, Dirichlet eut besoin de prouver sa formule du nombre de classes.

Le point de départ de Dirichlet, pour montrer l'infinité de nombres premiers dans les progressions arithmétiques, était la preuve d'Euler de l'infinité des nombres premiers. Cette preuve de 1748 impliquait que $\prod \left(1 - \frac{1}{p}\right)^{-1} =$

$\sum \frac{1}{n} \to \infty$, d'où l'infinité des nombres premiers. Toutefois, cette preuve ne marchait pas directement pour les nombres premiers dans une progression arithmétique puisqu'il n'y a pas de représentation naturelle en série pour le produit $\prod_{p \equiv a \bmod q} \left(1 - \frac{1}{p}\right)^{-1}$. Dirichlet voulait remédier à cette difficulté en introduisant des fonctions arithmétiques appelées caractères de Dirichlet.

Définition 8.5.1. *Soit* $\chi : \mathbb{Z}/q\mathbb{Z} \to \{z \in \mathbb{C} \mid |z| = 1\}$ *(c'est-à-dire vers l'ensemble des racines de l'unité) tel que*

1) $\chi(n+q) = \chi(n)$ $\quad \forall\, n \in \mathbb{Z}$

2) $\chi(m \cdot n) = \chi(m) \cdot \chi(n)$ $\quad \forall\, m, n \in \mathbb{Z}$

3) $\chi(n) = 0$ *si et seulement si* $pgcd(n, q) > 1$.

Alors χ *est appelé un CARACTÈRE DE DIRICHLET.*

Il y a $\phi(q)$ tels caractères modulo q, et ils satisfont la relation d'orthogonalité suivante :

$$\frac{1}{\phi(q)} \cdot \sum_{\chi \bmod q} \overline{\chi}(a) \cdot \chi(n) \quad = \quad \begin{cases} 1 & \text{si } n \equiv a \bmod q \\ 0 & \text{sinon} \end{cases} .$$

Avec l'aide desdits caractères, Dirichlet définit ensuite les fonctions-L comme suit :

$$L(x, \chi) = \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \qquad \text{pour } \mathrm{Re}(s) > 1.$$

Il pouvait ainsi produire quelque chose d'analogue au produit d'Euler en faisant tendre s vers 1 et en ayant une fonction qui pourrait prendre la valeur 1 lorsque $p \equiv a \bmod q$ et 0 sinon.

Similairement à la preuve d'Euler, on peut obtenir que $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$, $\chi(n)$ étant une fonction multiplicative.

Avant de pouvoir présenter la formule du nombre de classes de Dirichlet, nous devons aborder certaines notions et précisions sur les caractères de Dirichlet.

Définition 8.5.2. *Soit* $\chi_0(n) = \begin{cases} 1 & \text{lorsque } pgcd(n,q) = 1 \\ 0 & \text{lorsque } pgcd(n,q) > 1 \end{cases}$.
Alors χ_0 *est appelé le CARACTÈRE PRINCIPAL modulo* q.

Définition 8.5.3. *Soit* $\chi \neq \chi_0$ *un caractère modulo* q *différent du caractère principal. Il est possible que pour les valeurs de* n *telles que* $pgcd(n,q) = 1$, *la période de* χ *soit plus petite que* q. *Dans ce cas, on dit que* χ *est NON PRIMITIF. Sinon* χ *est dit PRIMITIF.*
D'un point de vue algébrique, un caractère de Dirichlet est dit PRIMITIF si et seulement si son noyau se réduit à l'élément neutre.

Nous sommes maintenant en mesure de comprendre la formule du nombre de classes de Dirichlet.

Théorème 8.5.1 (FORMULE DU NOMBRE DE CLASSES DE DIRICHLET)**.**
{sans preuve}

$$h_i(d) = \begin{cases} \frac{w(D)\cdot\sqrt{|D|}}{2\pi} \cdot L(1,\chi) & \text{si } D < 0 \\ \frac{\sqrt{D}}{2\cdot\log\varepsilon_d} \cdot L(1,\chi) & \text{si } D > 0 \end{cases}$$

où χ *est un caractère primitif réel modulo* $|D|$

Par $w(D)$ nous entendons le nombre d'unités dans le corps quadratique $\mathbb{Q}(\sqrt{d})$ de discriminant D. Ici D correspond à ce qu'on appelle le discriminant du corps quadratique $\mathbb{Q}(\sqrt{d})$. Les corps de nombre algébrique ont effectivement un invariant qui s'appelle le discriminant.

Définition 8.5.4. *Soit* $d \in \mathbb{Z}$ *un entier libre de carré.*
Alors le DISCRIMINANT de $\mathbb{Q}(\sqrt{d})$ *est* $D = \begin{cases} d & \text{si } d \equiv 1 \bmod 4 \\ 4d & \text{si } d \equiv 2 \text{ ou } 3 \bmod 4 \end{cases}$.
Le discriminant D *d'un corps quadratique* $\mathbb{Q}(\sqrt{d})$ *est toujours dit FONDAMENTAL si* d *est libre de carré.*

On peut aussi dire que le discriminant D d'une forme binaire quadratique est dit fondamental lorsque $D \in \mathbb{Z}$ est un entier libre de carré impair qui est $\equiv 1 \bmod 4$ ou qui est $\equiv 8$ ou $12 \bmod 16$.

Pour revenir à $w(D)$, nous avons déjà établi au théorème (4.0.6) que

$$w(D) = \begin{cases} 4 & \text{si } d = -1, \text{ c'est-à-dire si } D = -4 \\ 6 & \text{si } d = -3, \text{ c'est-à-dire si } D = -3 \\ 2 & \text{si } d = -2 \text{ ou si } d < -4, \text{ c'est-à-dire si } D < -4 \end{cases}$$

Quant à lui, $\log(\varepsilon_d)$ représente le régulateur du corps quadratique $\mathbb{Q}(\sqrt{d})$ de discriminant D.

Il est mentionné dans la formule du nombre de classes de Dirichlet que $\chi(n)$ est un caractère primitif réel. Un caractère donne des valeurs dans $\{z \in \mathbb{C} \mid |z| = 1\}$. Un caractère réel pourra donc valoir seulement ± 1. En fait, un caractère primitif réel se doit d'être le symbole de Kronecker $\chi(n) = \left(\frac{D}{n}\right)$, qui sera un caractère primitif réel modulo $|D|$. Pour définir le symbole de Kronecker, nous devrons toutefois parler d'abord des symboles de Legendre et de Jacobi.

Définition 8.5.5. *Soient $a, m \in \mathbb{Z}$ tels que $pgcd(a, m) = 1$.*
Si la congruence $x^2 \equiv a \bmod m$ possède une solution, alors a est appelé un RÉSIDU QUADRATIQUE MODULO m.
Si la congruence $x^2 \equiv a \bmod m$ n'a pas de solution, alors a est appelé un NON-RÉSIDU QUADRATIQUE MODULO m.

Définition 8.5.6. *Soit* $p \in \mathbb{N}$ *un nombre premier impair. Le SYMBOLE DE LEGENDRE* $\left(\frac{a}{p}\right)$ *est défini comme suit :*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un résidu quadratique modulo } p \\ -1 & \text{si } a \text{ est un non-résidu quadratique modulo } p \\ 0 & \text{si } p|a \end{cases}$$

Définition 8.5.7. *Soit* $Q \in \mathbb{N}$ *un entier positif impair tel que* $Q = q_1 \cdot q_2 \cdot \ldots \cdot q_s$ *où les* q_i *sont des nombres premiers impairs pas nécessairement distincts. Alors le SYMBOLE DE JACOBI* $\left(\frac{P}{Q}\right)$ *est défini comme suit :*

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s} \left(\frac{P}{q_j}\right)$$

où les $\left(\frac{P}{q_j}\right)$ *du côté droit de l'égalité sont des symboles de Legendre.*

Remarque 8.5.1 (Remarques sur les symboles de Jacobi)**.**
- Si $pgcd(P,Q) > 1$ *, alors* $\left(\frac{P}{Q}\right) = 0$ *; si* $pgcd(P,Q) = 1$ *, alors* $\left(\frac{P}{Q}\right) = \pm 1$ *.*
- Si $\left(\frac{P}{Q}\right) = 1$ *, alors* P *n'est pas nécessairement un résidu quadratique modulo* Q*.*
- Mais si $\left(\frac{P}{Q}\right) = -1$ *, alors* P *est un non-résidu quadratique modulo* Q *.*
- En fait, P *est un résidu quadratique modulo* Q *si et seulement si* $\left(\frac{P}{Q}\right) = 1$ *pour tout* q *qui divise* Q *.*

Le symbole de Kronecker, introduit par Leopold Kronecker, est une généralisation du symbole de Jacobi à tous les entiers $n \in \mathbb{Z}$.

Définition 8.5.8. *Soit* $n \in \mathbb{Z}$ *un entier non nul ayant la factorisation suivante :* $n = u \cdot p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$ *, où* u *est une unité de* $\mathbb{Z}$ *(c'est-à-dire* $u = \pm 1$ *) et où les* p_i *sont des nombres premiers distincts.*

Soit $a \in \mathbb{Z}$ *. Alors le SYMBOLE DE KRONECKER* $\left(\frac{a}{n}\right)$ *est défini comme suit :*

$$\left(\frac{a}{n}\right) \;=\; \left(\frac{a}{u}\right) \cdot \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$$

où les $\left(\frac{a}{p_i}\right)$ *du côté droit de l'égalité sont des symboles de Legendre lorsque* p_i *est un nombre premier impair.*

Pour $p_i = 2$ *, on définit* $\left(\frac{a}{2}\right) \;=\; \begin{cases} 0 & si\ a\ est\ pair \\ 1 & si\ a \equiv \pm 1 \bmod 8 \\ -1 & si\ a \equiv \pm 3 \bmod 8 \end{cases}$.

Lorsque $u = 1$ *, on a* $\left(\frac{a}{1}\right) = 1$ *puisque le symbole de Kronecker est une extension du symbole de Jacobi (et que par convention, un produit vide est égal à* 1*).*

Lorsque $u = -1$ *, on définit* $\left(\frac{a}{-1}\right) \;=\; \begin{cases} -1 & si\ a < 0 \\ 1 & si\ a \geq 0 \end{cases}$.

Enfin, pour que le symbole de Kronecker soit défini pour tout $n \in \mathbb{Z}$ *, on définit*

$$\left(\frac{a}{0}\right) = \begin{cases} 1 & si\ a = \pm 1 \\ 0 & sinon \end{cases}.$$

C'est ce qui complète cette définition du symbole de Kronecker.

Ainsi, nous avons précédemment énoncé la formule du nombre de classes de Dirichlet en mentionnant que χ devait être un caractère primitif réel, c'est-à-dire qu'il se doit d'être le symbole de Kronecker $\chi(n) = \left(\frac{D}{n}\right)$. Nous pouvons alors reciter la formule du nombre de classes de Dirichlet comme suit :

Théorème 8.5.2 (FORMULE DU NOMBRE DE CLASSES DE DIRICHLET)**.** *{sans preuve}*

$$h_i(d) = \begin{cases} \frac{w(D)\cdot\sqrt{|D|}}{2\pi} \cdot \sum_{n=1}^{\infty} \frac{1}{n}\left(\frac{D}{n}\right) \;=\; \frac{w(D)\cdot\sqrt{|D|}}{2\pi} \cdot \prod_{p} \left[1 - \frac{1}{p}\left(\frac{D}{p}\right)\right]^{-1} & si\ D < 0 \\ \frac{\sqrt{D}}{2\cdot\log\varepsilon_d} \cdot \sum_{n=1}^{\infty} \frac{1}{n}\left(\frac{D}{n}\right) \;=\; \frac{\sqrt{D}}{2\cdot\log\varepsilon_d} \cdot \prod_{p} \left[1 - \frac{1}{p}\left(\frac{D}{p}\right)\right]^{-1} & si\ D > 0 \end{cases}$$

où $\left(\frac{D}{n}\right)$ *est le symbole de Kronecker, qui est un caractère primitif réel modulo* $|D|$*.*

8.6. Borne supérieure pour $L(1,\chi)$; Comportement présumé et bornes du régulateur

Il est intéressant de réussir à borner $L(1,\chi)$, ce qui peut aider à établir un ordre de grandeur pour le régulateur $\log(\varepsilon_d)$ et pour le nombre de classes $h_i(d)$, grâce à la formule du nombre de classes de Dirichlet. Encore une fois, nous nous intéresserons au cas des corps quadratiques réels, c'est-à-dire au cas $D > 0$.

Nous commencerons par établir une propriété des caractères de Dirichlet, type de propriété qu'on nomme relation d'orthogonalité. Puisque $L(1,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n}$, établissons d'abord la valeur de $\sum_{n=1}^{D} \chi(n)$. Pour ce faire, soit $(\mathbb{Z}/D\mathbb{Z})^\times = \{a \in \mathbb{Z}/D\mathbb{Z} \mid \exists a^{-1} \in \mathbb{Z}/D\mathbb{Z} \text{ avec } aa^{-1} = 1\}$. En fait $(\mathbb{Z}/D\mathbb{Z})^\times$ est un groupe sous la multiplication et $(\mathbb{Z}/D\mathbb{Z})^\times = \{a \in \mathbb{Z}/D\mathbb{Z} \mid \text{pgcd}(a,D) = 1\}$.

Proposition 8.6.1. *Soit $\chi(n)$ un caractère de Dirichlet modulo D, différent du caractère principal χ_0. Alors $\sum_{n=1}^{D} \chi(n) = 0$.*

Démonstration. Si $\chi \neq \chi_0$, alors il existe $m \in (\mathbb{Z}/D\mathbb{Z})^\times$ tel que $\chi(m) \neq 1$. De plus, notons que $\{m \mid m \in (\mathbb{Z}/D\mathbb{Z})^\times\} = \{m \cdot n \mid m,n \in (\mathbb{Z}/D\mathbb{Z})^\times\}$ car l'application $m \mapsto m \cdot n$ est injective et surjective.
Ainsi

$$\begin{aligned}
\sum_{n=1}^{D}\chi(n) &= \sum_{\substack{n=1\\ \text{pgcd}(n,D)=1}}^{D} \chi(n) + \sum_{\substack{n=1\\ \text{pgcd}(n,D)>1}}^{D} \chi(n) = \sum_{n\in(\mathbb{Z}/D\mathbb{Z})^\times} \chi(n) + \sum_{\substack{n=1\\ \text{pgcd}(n,D)>1}}^{D} 0 \\
&= \sum_{n\in(\mathbb{Z}/D\mathbb{Z})^\times} \chi(n) = \sum_{n\in(\mathbb{Z}/D\mathbb{Z})^\times} \chi(m\cdot n) = \sum_{n\in(\mathbb{Z}/D\mathbb{Z})^\times} (\chi(m)\cdot\chi(n)) \\
&= \chi(m)\cdot \sum_{n\in(\mathbb{Z}/D\mathbb{Z})^\times} \chi(n)
\end{aligned}$$

$$\Rightarrow \sum_{n\in(\mathbb{Z}/D\mathbb{Z})^\times} \chi(n) = \chi(m)\cdot \sum_{n\in(\mathbb{Z}/D\mathbb{Z})^\times} \chi(n) \quad \Rightarrow \quad (1-\chi(m))\cdot \sum_{n\in(\mathbb{Z}/D\mathbb{Z})^\times} \chi(n) = 0 .$$

Or, $\chi(m) \neq 1$ par la façon dont on a choisi m. Ainsi

$$\therefore \qquad \sum_{n=1}^{D} \chi(n) \quad = \quad \sum_{n \in (\mathbb{Z}/D\mathbb{Z})^\times} \chi(n) \quad = \quad 0 \,.$$

□

Ainsi, nous tentons maintenant de trouver une borne supérieure pour $L(1,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n}$ où, tout comme dans la formule du nombre de classes de Dirichlet, χ est un caractère primitif réel modulo D. On a donc $\chi \neq \chi_0$.

Lemme 8.6.1. *Soit χ un caractère primitif réel modulo D tel que $\chi \neq \chi_0$. Alors $L(1,\chi) < \log D + 2$.*

Démonstration.

$$L(1,\chi) \;=\; \sum_{n\geq 1} \frac{\chi(n)}{n} \;=\; \sum_{n=1}^{D} \frac{\chi(n)}{n} + \sum_{k\geq 1} \sum_{n=kD+1}^{(k+1)D} \frac{\chi(n)}{n} \,.$$

$$\text{Et} \sum_{n=kD+1}^{(k+1)D} \frac{\chi(n)}{n} = \sum_{j=1}^{D} \frac{\chi(kD+j)}{kD+j} = \sum_{j=1}^{D} \frac{\chi(j)}{kD+j} \quad \text{car } \chi(D+j)=\chi(j) \ \ \forall j \in \mathbb{Z}$$

$$= \sum_{j=1}^{D} \frac{\chi(j)}{kD} + \sum_{j=1}^{D} \chi(j) \cdot \left(\frac{1}{kD+j} - \frac{1}{kD} \right)$$

$$= \frac{1}{kD} \cdot \sum_{j=1}^{D} \chi(j) + \sum_{j=1}^{D} \chi(j) \cdot \left(\frac{1}{kD+j} - \frac{1}{kD} \right)$$

$$= 0 + \sum_{j=1}^{D} \chi(j) \cdot \left(\frac{1}{kD+j} - \frac{1}{kD} \right) \quad \text{par la propriété précédente}$$

$$= \sum_{j=1}^{D} \chi(j) \cdot \frac{(-j)}{(kD+j)(kD)} \leq \left| \sum_{j=1}^{D} \chi(j) \cdot \frac{(-j)}{(kD+j)(kD)} \right|$$

$$\leq \sum_{j=1}^{D} \frac{|\chi(j)| \cdot j}{(kD+j)(kD)} \leq \sum_{j=1}^{D} \frac{|\chi(j)| \cdot j}{(kD)^2}$$

$$= \sum_{j=1}^{D-1} \frac{|\chi(j)| \cdot j}{(kD)^2} + 0 \qquad \text{car } \chi(j)=0 \Leftrightarrow \text{pgcd}(j,D)>1$$

$$\leq \sum_{j=1}^{D-1} \frac{j}{(kD)^2} = \frac{(D-1)D}{2} \cdot \frac{1}{(kD)^2} \leq \frac{D^2}{2k^2D^2} = \frac{1}{2k^2} \, .$$

$$\text{D'où} \quad L(1,\chi) = \sum_{n=1}^{D} \frac{\chi(n)}{n} + \sum_{k\geq 1} \sum_{n=kD+1}^{(k+1)D} \frac{\chi(n)}{n} \leq \sum_{n=1}^{D} \frac{\chi(n)}{n} + \sum_{k\geq 1} \frac{1}{2k^2}$$

$$= \sum_{n=1}^{D} \frac{\chi(n)}{n} + \frac{1}{2} \cdot \zeta(2) = \sum_{n=1}^{D} \frac{\chi(n)}{n} + \frac{1}{2} \cdot \frac{\pi^2}{6}$$

$$\leq \left| \sum_{n=1}^{D} \frac{\chi(n)}{n} + \frac{\pi^2}{12} \right| \leq \sum_{n=1}^{D} \frac{|\chi(n)|}{n} + \frac{\pi^2}{12} = \sum_{n=1}^{D-1} \frac{|\chi(n)|}{n} + \frac{\pi^2}{12}$$

$$\leq \sum_{n=1}^{D-1} \frac{1}{n} + \frac{\pi^2}{12} = 1 + \sum_{n=2}^{D-1} \frac{1}{n} + \frac{\pi^2}{12} < 1 + \int_{n=1}^{D-1} \frac{dn}{n} + \frac{\pi^2}{12}$$

$$= 1 + \log(D-1) - \log 1 + \frac{\pi^2}{12} = 1 + \log(D-1) + \frac{\pi^2}{12}$$

$$< \log D + 2 \, .$$

□

Avec cette borne supérieure sur $L(1,\chi)$, nous pouvons aussi donner une borne supérieure sur le régulateur $\log(\varepsilon_d)$ grâce à la formule du nombre de classes :

$$\begin{aligned}\log(\varepsilon_d) &= \frac{\sqrt{D}\cdot L(1,\chi)}{2\cdot h_i(d)} < \frac{\sqrt{D}\cdot(\log D+2)}{2\cdot h_i(d)}\\ &\leq \frac{\sqrt{D}\cdot(\log D+2)}{2} \qquad \text{puisque } h(D)\geq 1\,.\end{aligned}$$

Il existe de meilleures bornes encore pour le régulateur $\log(\varepsilon_d)$ dans la littérature. Mais avant de citer ces bornes, il est intéressant de mentionner que dans la plupart des cas, on pense que l'unité fondamentale d'un corps quadratique réel $\mathbb{Q}(\sqrt{d})$ grossirait de façon exponentielle relativement à $\sqrt{d}$, bref on aurait souvent $\log(\varepsilon_d)\approx\sqrt{d}$. Voir **[H]** et **[C1]**. Nous en parlerons nous aussi plus en détail, en expliquant pourquoi le régulateur se comporterait ainsi, lorsque nous aborderons les heuristiques de Cohen-Lenstra.

Ce n'est toutefois pas toujours le cas que $\log(\varepsilon_d)\approx\sqrt{d}$. En particulier, si d est de la forme m^2+1, alors le développement en fraction continue de $\sqrt{d}$ est $\sqrt{d}=[m,\overline{2m}]$ et l'unité fondamentale peut être trouvée par la 0^e réduite $\frac{p_0}{q_0}=\frac{m}{1}$, d'où $\varepsilon_d = m+1\sqrt{d} = m+\sqrt{m^2+1}$ qui se comporte approximativement comme $2\sqrt{d}$, donc ε_d est dans ce cas-ci loin de grossir de façon exponentielle relativement à d.

Dans la littérature, on reconnaît les bornes suivantes pour le régulateur $\log(\varepsilon_d)$ du corps quadratique réel $\mathbb{Q}(\sqrt{d})$ de discriminant D.

Selon **[L]**, $\log(\varepsilon_d) \geq \log\left(\frac{1}{2}(\sqrt{D-4}+\sqrt{D})\right)$ et c'est la plus grande borne inférieure possible !

Selon [**Hu1**], $$\sum_{n=1}^{\infty} \frac{1}{n} \cdot \left(\frac{D}{n}\right) < \frac{1}{2}\log(D) + 1$$

$$\log(\varepsilon_d) < \sqrt{D} \cdot \left(\frac{1}{2}\log(D) + 1\right)$$

$$< \sqrt{D} \cdot \log(D)$$

sont des bornes supérieures, qui ne sont toutefois probablement pas les plus petites possibles, d'après [**L**].

Par ailleurs, selon une méthode de D.A. Burgess (voir [**Hu1**]), il est possible d'améliorer légèrement (par une constante) cette dernière inégalité. Ce résultat est le suivant :

$\forall\, \delta > 0 \quad \exists$ une constante $c(\delta)$ telle que

$$D > c(\delta) \;\Rightarrow\; \log(\varepsilon_d) < \left(\frac{1}{4} + \delta\right) \sqrt{D} \log D\ .$$

Mentionnons également que l'Hypothèse de Riemann Généralisée (HRG) permettrait d'améliorer sensiblement ces bornes. En effet, il est indiqué dans [**GrS**] que J.E. Littlewood a montré en 1928 qu'en assumant la véracité de HRG, on obtient que

$$L(1,\chi) \;\leq\; (2 + o(1))\; e^{\gamma}\; \log\log|D|$$

où γ est la constante d'Euler et vaut approximativement $0.57721...$.

Toujours en assumant la véracité de HRG et en utilisant la formule du nombre de classes de Dirichlet pour $D > 0$, on obtiendrait :

$$\log(\varepsilon_d) \;=\; \frac{\sqrt{D} \cdot L(1,\chi)}{2 \cdot h_i(d)} \;\leq\; \frac{\sqrt{D}}{2} \cdot (2 + o(1))\; e^{\gamma}\; \log\log D$$

$$=\; (1 + o(1))\; e^{\gamma}\; \sqrt{D}\; \log\log D\ .$$

Pour ce qui est de $h(D)$, Gauss a conjecturé que $\lim_{|D|\to\infty} h(D) = +\infty$.
Heilbronn a prouvé en 1934 que c'était vrai pour $D < 0$, c'est-à-dire que $\lim_{D\to-\infty} h(D) = +\infty$.
Et l'année suivante, en 1935, Siegel a prouvé davantage en montrant que $\lim_{D\to-\infty} \frac{\log h(D)}{\log |D|} = \frac{1}{2}$, ce qui fait qu'on connaît même l'ordre de grandeur de $h(D)$ en fonction de $D < 0$.
Par contre, la conjecture de Gauss pour $D > 0$ est encore un problème irrésolu. On ne sait pas si $\lim_{D\to+\infty} h(D) = +\infty$ ou non.
Siegel a toutefois aussi un résultat pour ce cas : $\lim_{D\to+\infty} \frac{\log(h_i(d)\cdot\log(\varepsilon_d))}{\log D} = \frac{1}{2}$.
Mais malheureusement, on n'en connaît pas suffisamment sur le comportement exact de $\log(\varepsilon_d)$ donc on ne peut pas savoir si la conjecture de Gauss est vraie ou fausse, c'est-à-dire si $\lim_{D\to+\infty} h(D) = +\infty$ ou non.

8.7. Heuristiques de Cohen-Lenstra sur le nombre de classes

Ainsi, nos connaissances sur le régulateur $\log(\varepsilon_d)$ d'un corps quadratique réel et sur son nombre de classes d'idéaux sont directement proportionnelles. Les heuristiques de Cohen-Lenstra sont des conjectures sur le nombre de classes d'idéaux, mais des conjectures qui reposent sur de bons indices, sur de bonnes évidences. Des calculs ont été effectués par différentes personnes, dont entre autres [**R**], pour vérifier expérimentalement jusqu'à certaines valeurs les heuristiques de Cohen-Lenstra.

Conjecture 8.7.1 (Heuristiques de Cohen-Lenstra)**.** *Soit $h_i(p)$ le nombre de classes d'idéaux du corps quadratique réel $\mathbb{Q}(\sqrt{p})$, où p est un nombre premier. Alors les heuristiques de Cohen-Lenstra suggèrent que la probabilité que $h_i(p) = k$ (où $k \in \mathbb{N}$ est un entier impair) soit donné par $\frac{C\cdot\varpi(k)}{k}$, où $C = 0.754458173...$ et où* $\varpi(k)^{-1} = \prod_{p^\alpha || k} p^\alpha \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right)\cdot ... \cdot \left(1 - \frac{1}{p^\alpha}\right)$

En particulier, ça donnerait
$$P(h_i(p)=1) \approx 0.7544581722$$
$$P(h_i(p)=3) \approx 0.125743$$
$$P(h_i(p)=5) \approx 0.037723$$
$$P(h_i(p)=7) \approx 0.017963$$
$$P(h_i(p)=9) \approx 0.015718\ .$$

Conjecture 8.7.2 (Hooley)**.** *Soit* $h_i(p)$ *le nombre de classes du corps quadratique réel* $\mathbb{Q}(\sqrt{p})$*, où* p *est un nombre premier. Alors la conjecture de Hooley suggère que* $H(x) := \sum_{\substack{p\leq x \\ p\ premier \\ p\equiv 1 \bmod 4}} h_i(p) \sim \frac{x}{8}$ *lorsque* $x \to +\infty$ *.*

Cohen a réussi à démontrer que les heuristiques de Cohen-Lenstra impliquent la véracité de la conjecture de Hooley.

Comme nous le mentionnions plus tôt, malgré le fait qu'il semblerait que la plupart des nombres de classes d'idéaux soit très petits et que 75% soient égaux à 1, la conjecture de Gauss (beaucoup plus faible) mentionnant qu'il y aurait une infinité de nombre de classes égaux à 1 reste encore un problème ouvert.

En prenant pour acquis toutefois que la plupart des nombres de classes soient très petits (en se fiant aux heuristiques de Cohen-Lenstra, qui concernent les cas où d est un nombre premier) et en utilisant le théorème de Siegel qui affirme que $\log\left(h_i(d)\cdot\log(\varepsilon_d)\right) \sim \frac{1}{2}\cdot\log D = \log(\sqrt{D})$, ce qui est équivalent à $h_i(d)\cdot\log(\varepsilon_d)\sim\sqrt{D}$, alors $h_i(d)$ étant très petit, on obtient que le régulateur $\log(\varepsilon_d)$ serait la plupart du temps proche de $\sqrt{D}$ lorsque d est un nombre premier.
Bien sûr le théorème de Siegel est valable lorsque $D \to +\infty$, donc le comportement décrit et attendu ici pourrait être plus facilement observable à mesure que

D grandit.

Toujours en se fiant aux heuristiques de Cohen-Lenstra et à leurs propres calculs, Jacobson, Lukes et Williams [**L**] émettent la conjecture qu'il y aurait une infinité de discriminants D pour lesquels $\log(\varepsilon_d) \gg \frac{\sqrt{D}}{\log(\log D)}$. En fait, ils vont même jusqu'à croire qu'il y aurait une infinité de discriminants D pour lesquels $\log(\varepsilon_d) \gg \sqrt{D} \cdot \log(\log D)$. (Rappelons aussi que la véracité de HRG impliquerait $\log(\varepsilon_d) \leq (1 + o(1))\, e^{\gamma} \sqrt{D} \log\log D$.) Toutefois, jusqu'à présent, les résultats sont beaucoup plus conservateurs. Selon le théorème de Halter-Koch (1989), on sait qu'il existe une infinité de discriminants D tels que $\log(\varepsilon_d) \gg (\log D)^4 = \log^4 D$.

Références spécifiques à ce chapitre :

Alan Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, 1984.

Johannes Buchmann, *Binary quadratic forms : an algorithmic approach*, Springer, 2007.

Duncan A. Buell, *Binary quadratic forms : classical theory and modern computations*, Springer-Verlag, 1989.

Henri Cohen, *A course in computational algebraic number theory*, Springer-Verlag, 1993.

Harold Davenport, *Multiplicative number theory, 3e édition*, Springer, 2000.

Andrew Granville et Kannan Soundararajan, *The distribution of values of $L(1, \chi_d)$*, Geometric And Functional Analysis, Volume 13, Numéro 5, 2003, pages 992-1028.

R. de Haan, M.J. Jacobson Jr. et H.C. Williams, *A fast, rigorous technique for computing the regulator of a real quadratic field*, Mathematics of computation, Volume 76, Numéro 260, Octobre 2007, pages 2139-2160.

Loo Keng Hua, *Introduction to number theory*, Springer-Verlag, 1982.

Michael J. Jacobson Jr., Richard F. Lukes et Hugh C. Williams, *An investigation of bounds for the regulator of quadratic fields*, Experimental Mathematics, Volume 4, Numéro 3, 1995.

Burton W. Jones, *The arithmetic theory of quadratic forms*, Mathematical Association of America : Wiley, 1950.

Ivan Niven, Herbert S. Zuckerman et Hugh L. Montgomery, *An introduction to the theory of numbers, Fifth edition*, Jon Wiley & Sons, 1991.

Herman te Riele et Hugh Williams, *New computations concerning the Cohen-Lenstra heuristics*, Stichting Centrum voor Wiskunde en Informatica, 2001, pages 1-20.

Chapitre 9

ÉTUDE DU RÉGULATEUR

9.1. Distribution du régulateur $\log(\varepsilon_d)$ d'un corps quadratique en fonction du discriminant D

Nous avons tout d'abord calculé dans cette section le régulateur $\log(\varepsilon_d)$ des corps quadratiques $\mathbb{Q}(\sqrt{d})$ pour $17 \leq d \leq 2^{16} = 65536$. Dans les graphiques suivants, le régulateur $\log(\varepsilon_d)$ (en ordonnée) d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ dépend du discriminant D (en abscisse) de ce même corps quadratique. Nous avons séparé les cas où $d \equiv 1 \bmod 4$ et où $d \equiv 2, 3 \bmod 4$ puisque le discriminant y diffère. Par ailleurs, les heuristiques de Cohen-Lenstra s'appliquent lorsque d est un nombre premier, donc nous avons également séparé les cas où d est premier, en plus de présenter dans un même graphique l'ensemble des $d \equiv 1 \bmod 4$, que d soit premier ou non, et dans un autre graphique l'ensemble des $d \equiv 2, 3 \bmod 4$, que d soit premier ou non. Ainsi, le fait de séparer lorsque d est premier ou pas nécessairement nous permettra de constater les différences dans la distribution des régulateurs, conformément aux heuristiques de Cohen-Lenstra.

Par ailleurs, nous avons aussi représenté dans ces graphiques la courbe $f(x) = \sqrt{D}$, où D est le discriminant, afin de pouvoir constater si nos attentes sont plausibles relativement au comportement du régulateur.

Ce premier graphique présente le régulateur $\log(\varepsilon_d)$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ en fonction de son discriminant D, lorsque d est un nombre premier $\equiv 1 \bmod 4$.

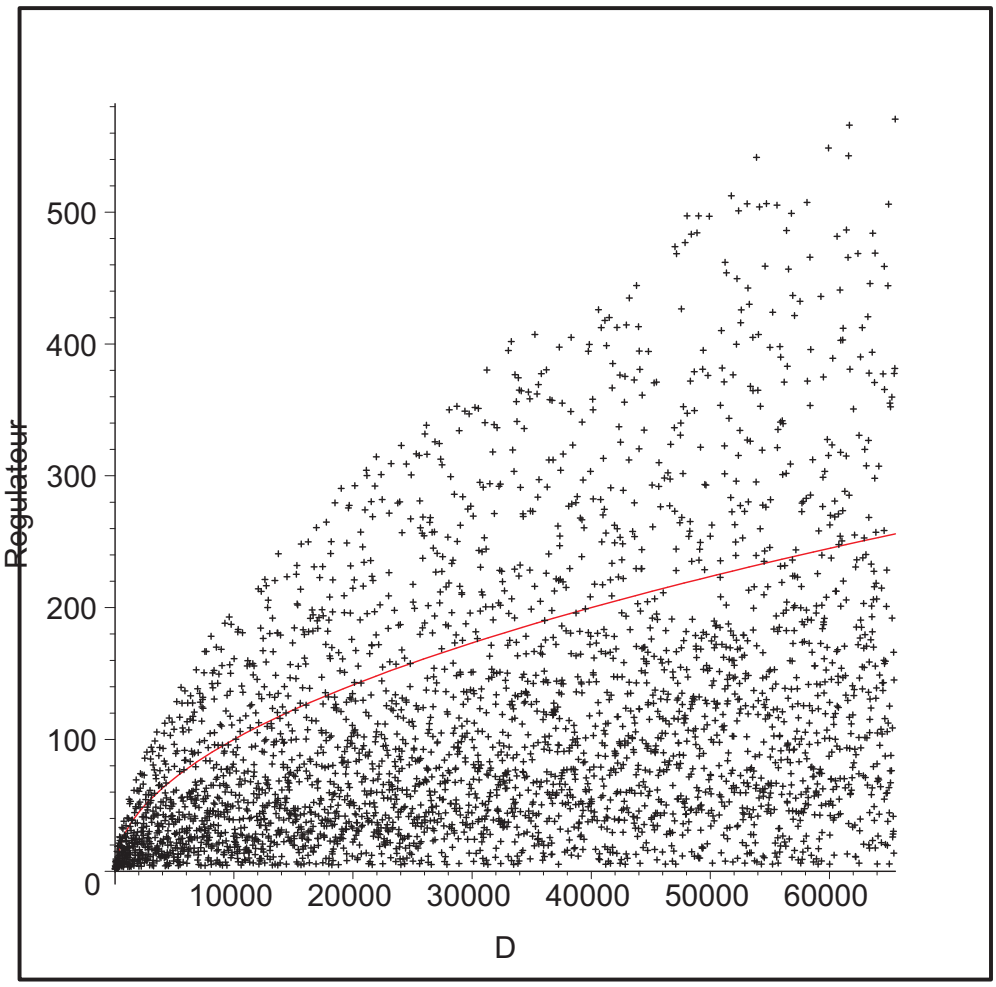

FIG. 9.1. Régulateur $\log(\varepsilon_d)$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ en fonction de son discriminant D, pour d un nombre premier $\equiv 1 \bmod 4$

Ce second graphique présente le régulateur $\log(\varepsilon_d)$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ en fonction de son discriminant D, lorsque d est un entier libre de carré $\equiv 1 \bmod 4$.

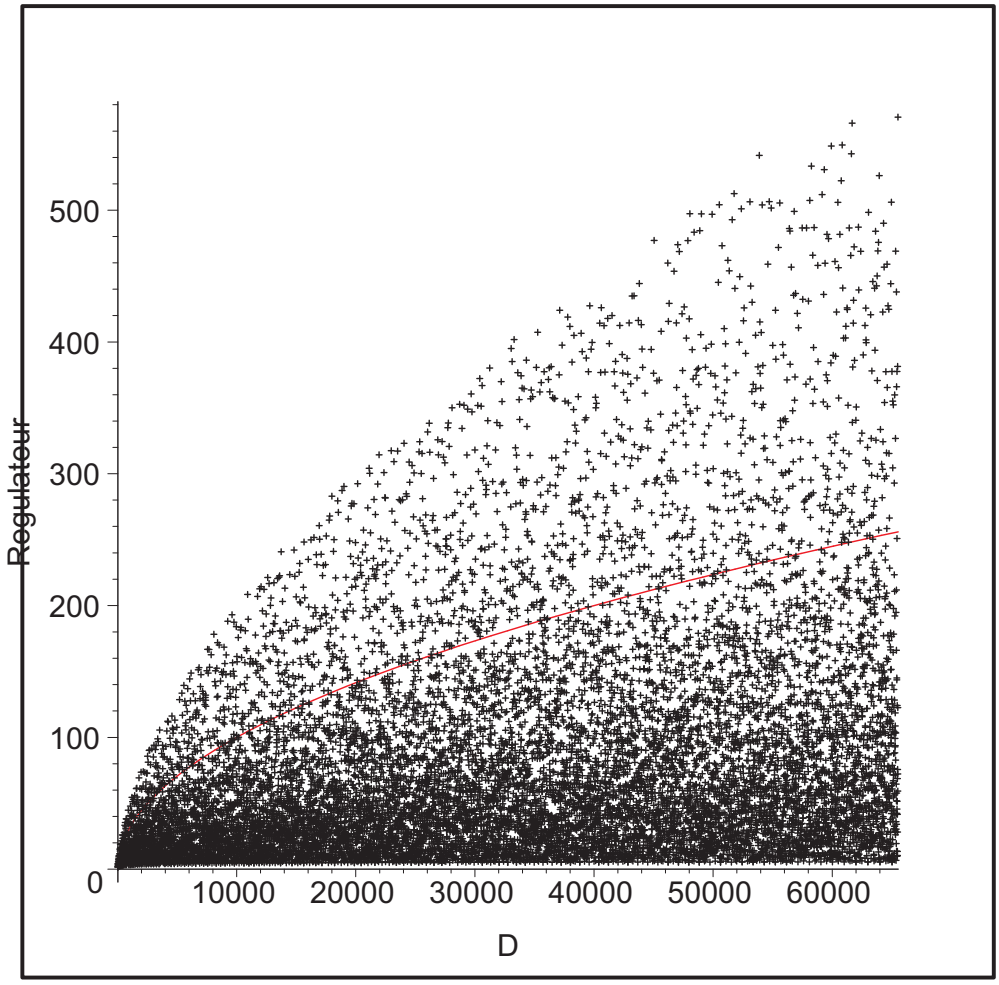

FIG. 9.2. Régulateur $\log(\varepsilon_d)$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ en fonction de son discriminant D, pour $d \equiv 1 \bmod 4$

Ce troisième graphique présente le régulateur $\log(\varepsilon_d)$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ en fonction de son discriminant D, lorsque d est un nombre premier $\equiv 2, 3 \bmod 4$.

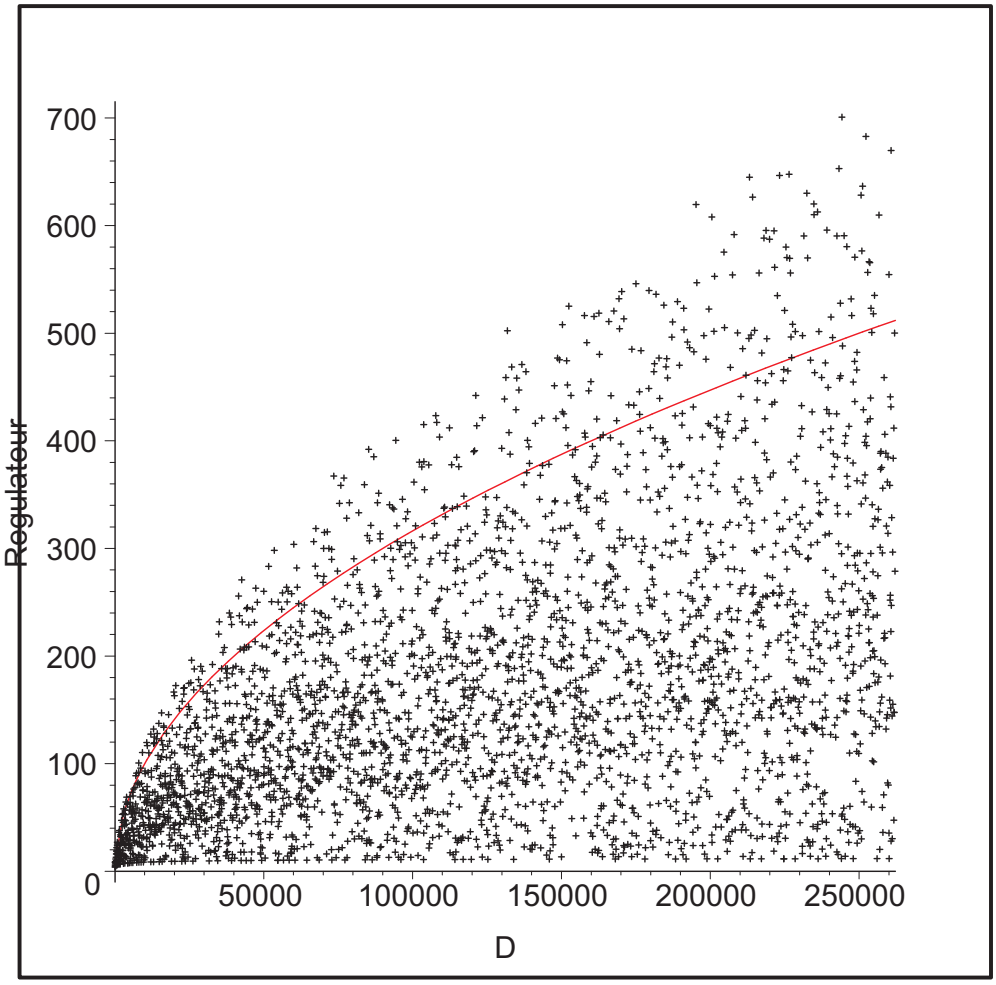

FIG. 9.3. Régulateur $\log(\varepsilon_d)$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ en fonction de son discriminant D, pour d un nombre premier $\equiv 2, 3 \bmod 4$

Ce quatrième graphique présente le régulateur $\log(\varepsilon_d)$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ en fonction de son discriminant D, lorsque d est un entier libre de carré $\equiv 2, 3 \bmod 4$.

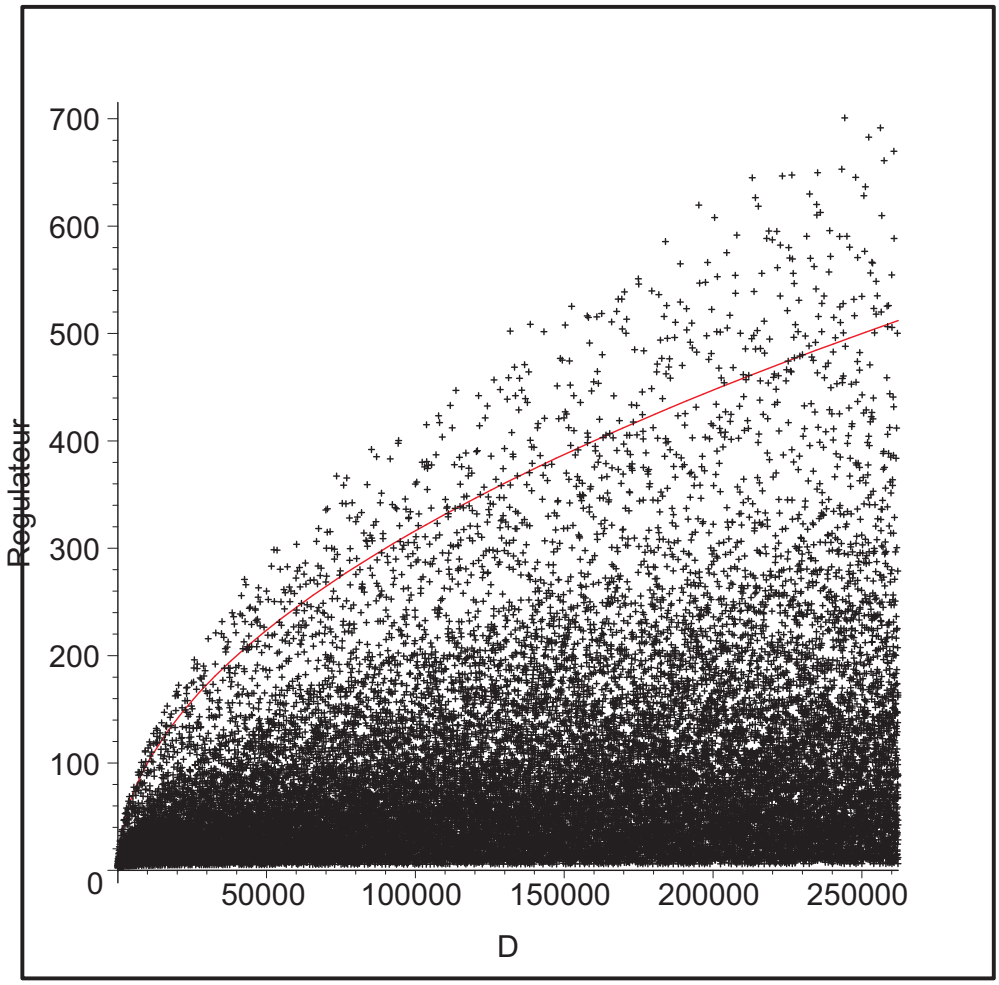

FIG. 9.4. Régulateur $\log(\varepsilon_d)$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ en fonction de son discriminant D, pour $d \equiv 2, 3 \bmod 4$

À la lumière de ces quatre graphiques, on constate effectivement que la densité des régulateurs, lorsque d n'est pas un nombre premier, est beaucoup plus élevée dans le bas du graphique, pour de petits régulateurs bien plus petits que $\sqrt{D}$. Donc, lorsque d n'est pas un nombre premier, les régulateurs ne semblent pas du tout vouloir éventuellement être de l'ordre de $\sqrt{D}$ (ce qui pourrait aussi vouloir dire que le nombre de classes $h_i(d)$ serait quant à lui plus grand que

lorsque d est premier). Alors que lorsque d est un nombre premier, ce n'est pas le cas, le comportement étant tout autre, laissant supposer que si on laisse tendre d premier vers l'infini, il est possible qu'on pourra avoir un régulateur dont l'ordre de grandeur varie majoritairement autour de $\sqrt{D}$. Et comme nous le mentionnions dans la section précédente (8.7), le théorème de Siegel est valable lorsque $D \to +\infty$, donc le comportement décrit et attendu ici pourrait être plus facilement observable à mesure que D grandit.

Aussi, si on avait tracé la courbe $\sqrt{D}\log D$ (chose que nous n'avons pas faite ici car elle est beaucoup plus haute que le nuage de points et le fait de l'inclure dans le graphique aurait comprimé grandement le nuage de points, et il aurait été plus difficile de bien voir ledit nuage), on aurait constaté que chacun des points du nuage aurait été de beaucoup inférieur à la courbe, respectant le fait que nous avons prouvé précédemment que tout régulateur est borné par $\sqrt{D}\log D$ (ou également par $\frac{1}{2}\sqrt{D}(\log D + 2)$). Tel que le mentionne **[L]**, cette borne n'est toutefois probablement pas la plus petite possible.

Par ailleurs, concernant les hypothèses de Jacobson, Lukes et Williams **[L]**, on constate effectivement un certain nombre de régulateurs supérieurs à $\sqrt{D}$ (et donc bien évidemment supérieurs à $\frac{\sqrt{D}}{\log(\log D)}$), relativement à leur conjecture qu'il y aurait une infinité de discriminants D pour lesquels $\log(\varepsilon_d) \gg \frac{\sqrt{D}}{\log(\log D)}$.

9.2. Régulateur et divisibilité du nombre de classes

Plutôt que ces derniers graphiques, il est intéressant aussi de représenter $\dfrac{\log(\varepsilon_d)\cdot 2^{\omega(d)-1}}{\sqrt{D}}$ en fonction de d, (où $\omega(d)$ est le nombre de facteurs premiers distincts de $d \in \mathbb{N}$), ratio qui équivaut grosso modo à la fonction-L $L(1,\chi)$ divisée par un facteur, facteur qui a à voir avec la divisibilité du nombre de classes.

9.2.1. Divisibilité par 2 du nombre de classes

Gauss, dans son livre *Disquisitiones Arithmeticae*, publié en 1801, développa entre autres choses une théorie des genres qui élabore sur la divisibilité par 2 du

nombre de classes des corps quadratiques. L'objectif de Gauss avec cette théorie était d'étudier la représentation d'un nombre premier par certaines formes binaires quadratiques (de discriminant fondamental) inclues dans des classes d'équivalence. Cette répartition des représentations étudiée par Gauss lui permit entre autres de prouver que l'ensemble des classes d'équivalence pouvait être partitionné de façon égale en $2^{\omega(D)-1}$, où on rappelle que $\omega(D)$ est le nombre de facteurs premiers distincts du discriminant D. Ainsi, on arrive au résultat qui nous intéresse et qui est important pour nous, c'est-à-dire que Gauss a prouvé que le nombre de classes de formes, $h(D)$, est divisible par $2^{\omega(D)-1}$. (voir [**P**])

Ainsi, soit $\quad h_2 = \dfrac{h(D)}{2^{\omega(D)-1}} \quad \in \mathbb{N}$.

Rappelons que $\quad D = \begin{cases} d & \text{si } d \equiv 1 \bmod 4 \\ 4d & \text{si } d \equiv 2 \text{ ou } 3 \bmod 4 \end{cases}$.

Alors on déduit que $\quad \omega(D) = \begin{cases} \omega(d) & \text{si } d \equiv 1 \text{ ou } 2 \bmod 4 \\ \omega(d)+1 & \text{si } d \equiv 3 \bmod 4 \end{cases}$.

<u>Pour $d \equiv 1$ ou $2 \bmod 4$:</u>

$$h_2 = \frac{h(D)}{2^{\omega(d)-1}} = \begin{cases} \dfrac{h_i(d)}{2^{\omega(d)-1}} \\ \text{ou} \\ \dfrac{2 \cdot h_i(d)}{2^{\omega(d)-1}} \end{cases} = \begin{cases} \dfrac{\sqrt{D} \cdot L(1,\chi)}{2 \cdot \log(\varepsilon_d) \cdot 2^{\omega(d)-1}} \\ \text{ou} \\ \dfrac{2 \cdot \sqrt{D} \cdot L(1,\chi)}{2 \cdot \log(\varepsilon_d) \cdot 2^{\omega(d)-1}} \end{cases}$$

$$\Rightarrow \quad \frac{\log(\varepsilon_d) \cdot 2^{\omega(d)-1}}{\sqrt{D}} = \begin{cases} \dfrac{L(1,\chi)}{2 \cdot h_2} \\ \text{ou} \\ \dfrac{L(1,\chi)}{h_2} \end{cases} \leq \frac{L(1,\chi)}{h_2} \leq L(1,\chi)$$

<u>Pour $d \equiv 3 \bmod 4$:</u>

$$h_2 \;=\; \frac{h(D)}{2^{\omega(d)}} \;=\; \begin{cases} \dfrac{h_i(d)}{2^{\omega(d)}} \\ \dfrac{2\cdot h_i(d)}{2^{\omega(d)}} \end{cases} \text{ ou } \;=\; \begin{cases} \dfrac{\sqrt{D}\cdot L(1,\chi)}{2\cdot\log(\varepsilon_d)\cdot 2^{\omega(d)}} \\ \dfrac{2\cdot\sqrt{D}\cdot L(1,\chi)}{2\cdot\log(\varepsilon_d)\cdot 2^{\omega(d)}} \end{cases} \text{ ou}$$

$$\Rightarrow \quad \frac{\log(\varepsilon_d)\cdot 2^{\omega(d)-1}}{\sqrt{D}} \;=\; \begin{cases} \dfrac{L(1,\chi)}{4\cdot h_2} \\ \dfrac{L(1,\chi)}{2\cdot h_2} \end{cases} \text{ ou } \quad \leq \;\frac{L(1,\chi)}{2\cdot h_2} \;\leq\; \frac{L(1,\chi)}{2}$$

Et puis la véracité de l'hypothèse de Riemann généralisée (HRG) impliquerait que $L(1,\chi) \;\leq\; 2e^{\gamma}\cdot\log\log D \;<\; 4\cdot\log\log D$.

Nous présentons maintenant trois graphiques où $\dfrac{\log(\varepsilon_d)\cdot 2^{\omega(d)-1}}{\sqrt{D}}$ varie en fonction de d , pour $17 \leq d \leq 2^{17} = 131072$. Les trois graphiques sont respectivement pour $d \equiv 1, 2$ et $3 \bmod 4$. Nous avons aussi tracé dans les graphiques la courbe $\log\log d$ à titre indicatif.

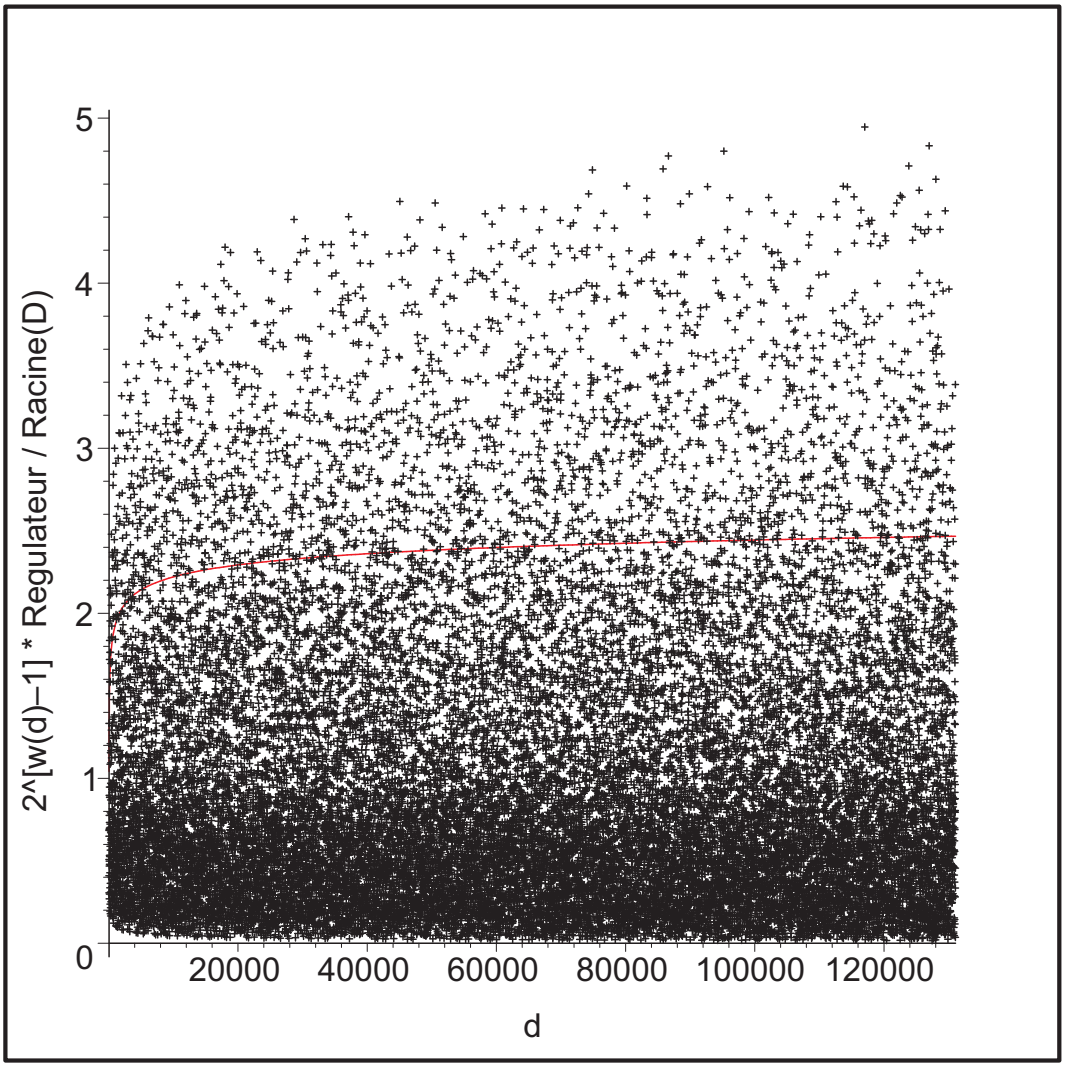

FIG. 9.5. Ratio $\dfrac{\log(\varepsilon_d)\cdot 2^{\omega(d)-1}}{\sqrt{D}}$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ en fonction de d, pour d un discriminant fondamental $\equiv 1 \bmod 4$

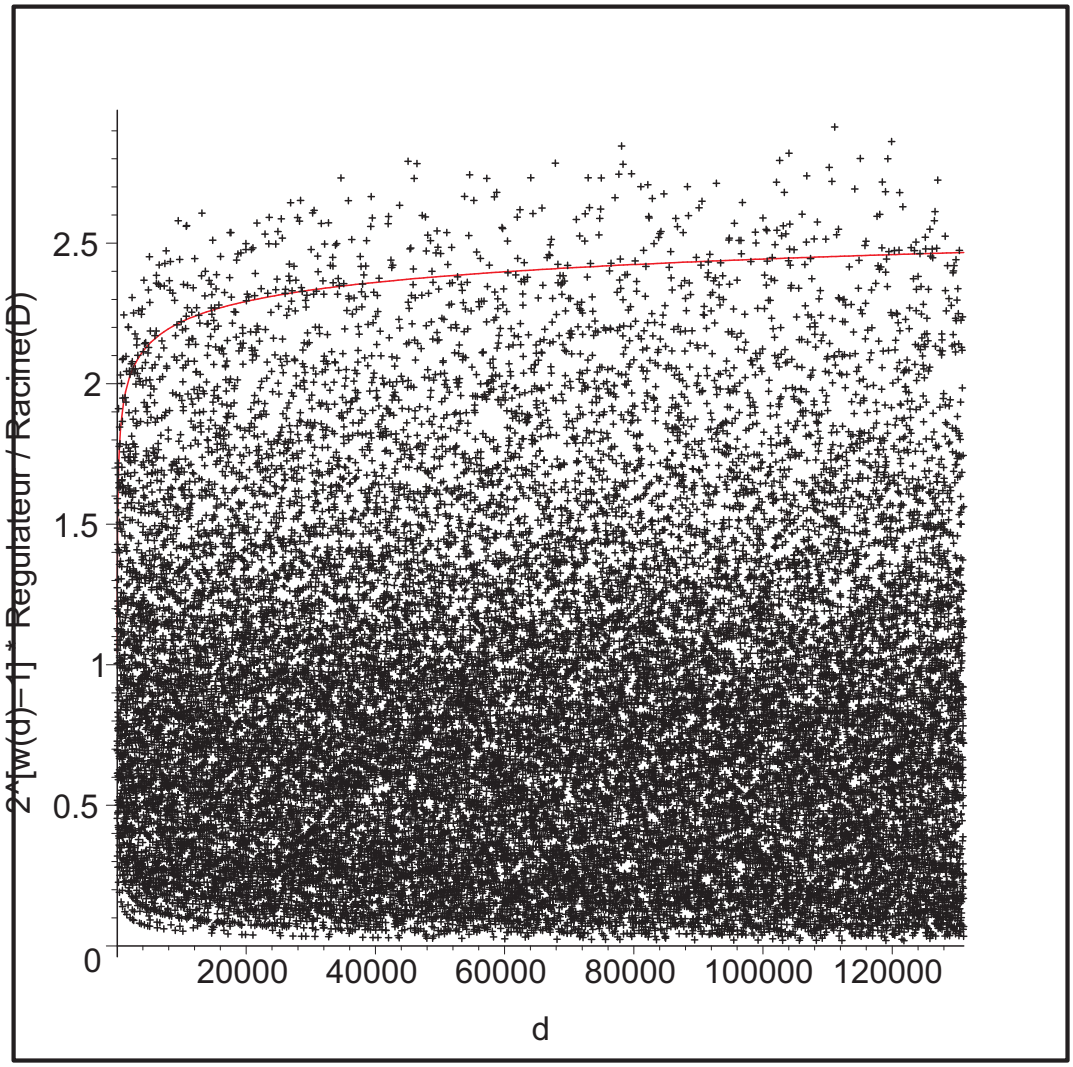

FIG. 9.6. Ratio $\dfrac{\log(\varepsilon_d)\cdot 2^{\omega(d)-1}}{\sqrt{D}}$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ en fonction de d, pour d un discriminant fondamental $\equiv 2 \bmod 4$

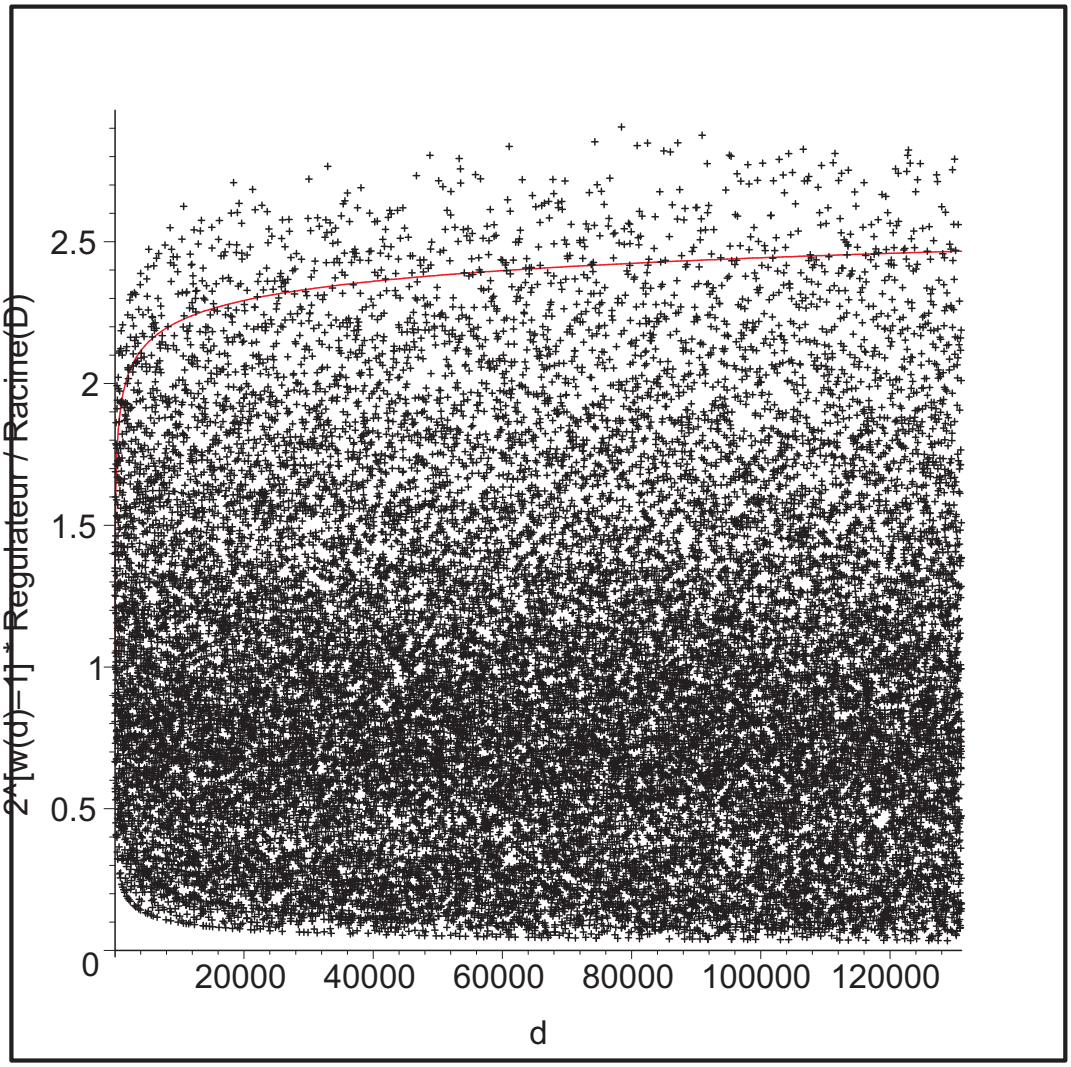

FIG. 9.7. Ratio $\dfrac{\log(\varepsilon_d)\cdot 2^{\omega(d)-1}}{\sqrt{D}}$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ en fonction de d, pour d un discriminant fondamental $\equiv 3 \bmod 4$

On constate une différence d'amplitude verticale entre le premier graphique et les deux suivants. L'ordonnée varie entre 0 et 5 lorsque $d \equiv 1 \bmod 4$ et entre 0 et 3 lorsque $d \equiv 2$ ou $3 \bmod 4$. Ça s'explique si on retourne voir les graphiques (9.2) et (9.4). Les régulateurs les plus grands peuvent être légèrement plus grands lorsque $d \equiv 2$ ou $3 \bmod 4$ que lorsque $d \equiv 1 \bmod 4$. Toutefois, comme on divise le régulateur par $\sqrt{D} = \begin{cases} \sqrt{d} & \text{si } d \equiv 1 \bmod 4 \\ \sqrt{4d} & \text{si } d \equiv 2 \text{ ou } 3 \bmod 4 \end{cases}$ pour d étant notre abscisse, le facteur 2 additionnel au dénominateur explique que les

graphiques pour 2 et $3 \bmod 4$ aient des ordonnées moindres que pour $1 \bmod 4$.

Par ailleurs, on mentionnait que sous HRG, les nuages de points devraient être inférieurs à $4 \cdot \log\log D$ pour $d \equiv 1$ ou $2 \bmod 4$ et à $2 \cdot \log\log D$ pour $d \equiv 3 \bmod 4$, ce qui est le cas. On peut juste spécifier que pour $d \equiv 2$ ou $3 \bmod 4$, la courbe $\log\log D = \log\log(4d)$ est à peine supérieure à $\log\log d$ qui est tracée (et pour $d \equiv 1 \bmod 4$, $\log\log D = \log\log d$) .

Dans les trois graphiques, il y a une forte densité de points lorsque l'ordonnée est inférieure à 1. Afin de mieux voir la distribution de ces points, nous tracerons l'inverse des trois graphiques précédents, c'est-à-dire $\dfrac{\sqrt{D}}{\log(\varepsilon_d) \cdot 2^{\omega(d)-1}}$ en fonction de d , pour $17 \leq d \leq 2^{17} = 131072$. Nous tracerons les trois graphiques respectivement encore pour $d \equiv 1, 2$ et $3 \bmod 4$. Et nous restreindrons l'axe des ordonnées à l'intervalle $[0, 5]$.

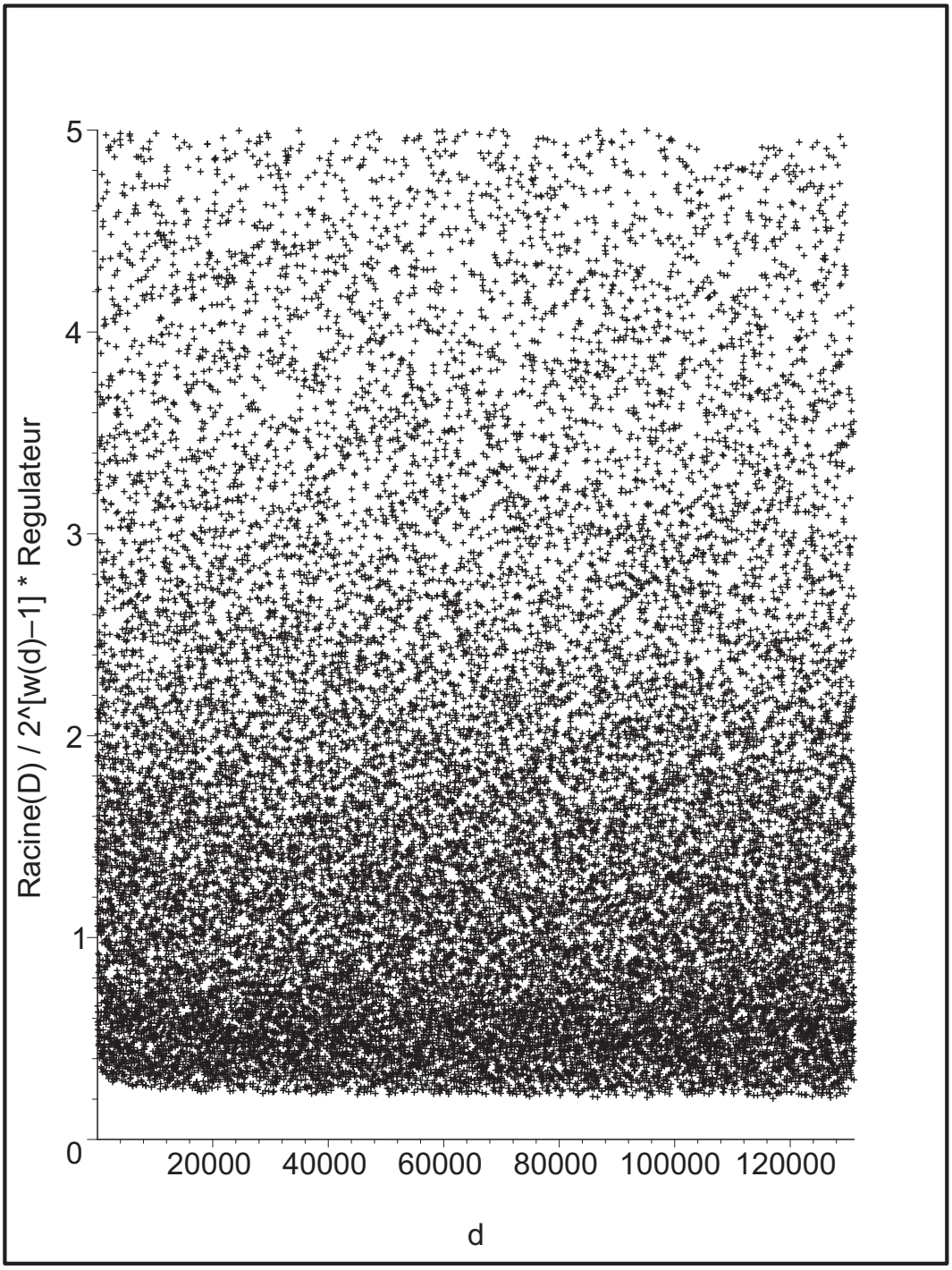

FIG. 9.8. Ratio $\dfrac{\sqrt{D}}{\log(\varepsilon_d)\cdot 2^{\omega(d)-1}}$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ en fonction de d, pour d un discriminant fondamental $\equiv 1 \bmod 4$

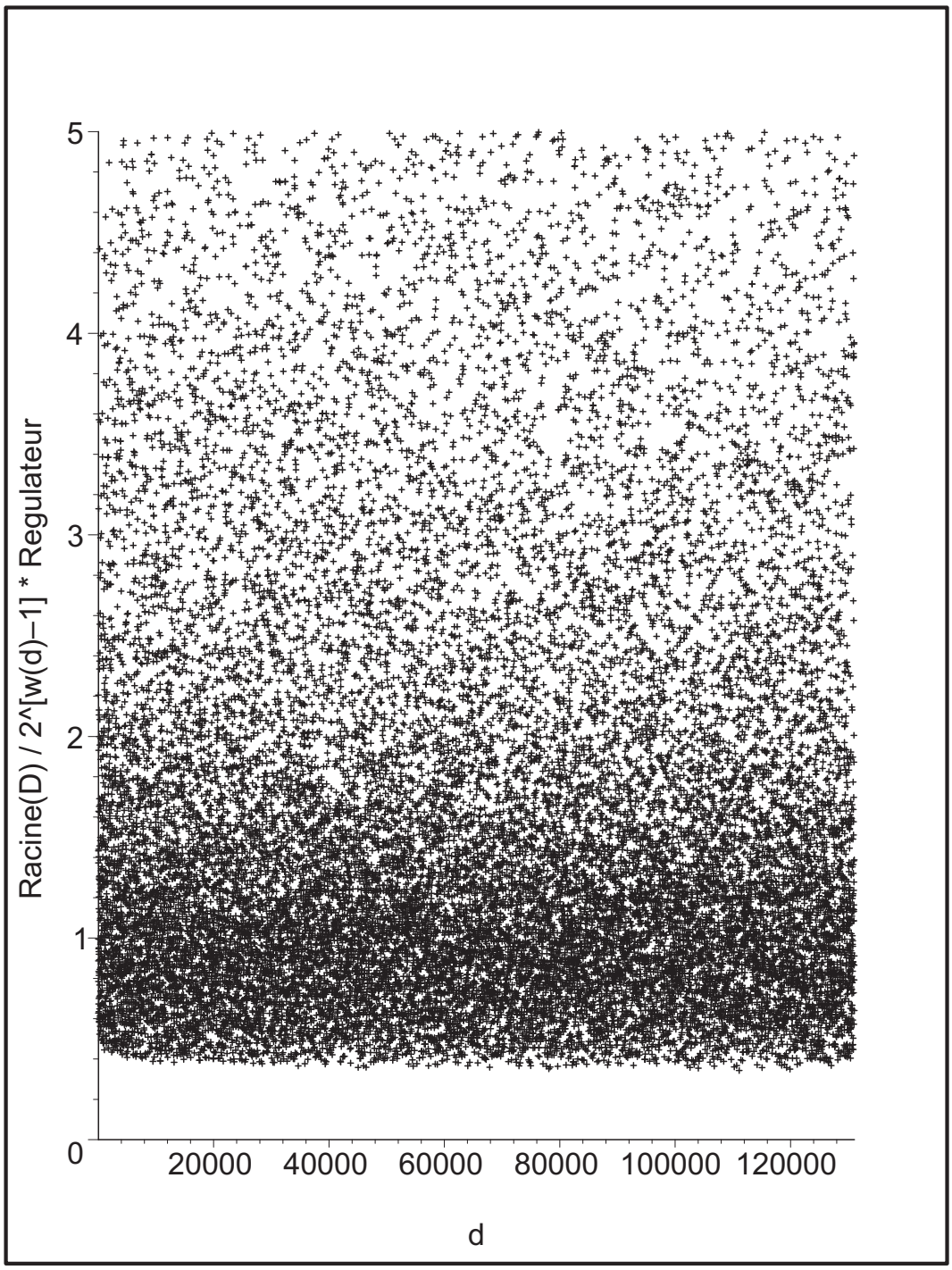

FIG. 9.9. Ratio $\dfrac{\sqrt{D}}{\log(\varepsilon_d)\cdot 2^{\omega(d)-1}}$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ en fonction de d, pour d un discriminant fondamental $\equiv 2 \bmod 4$

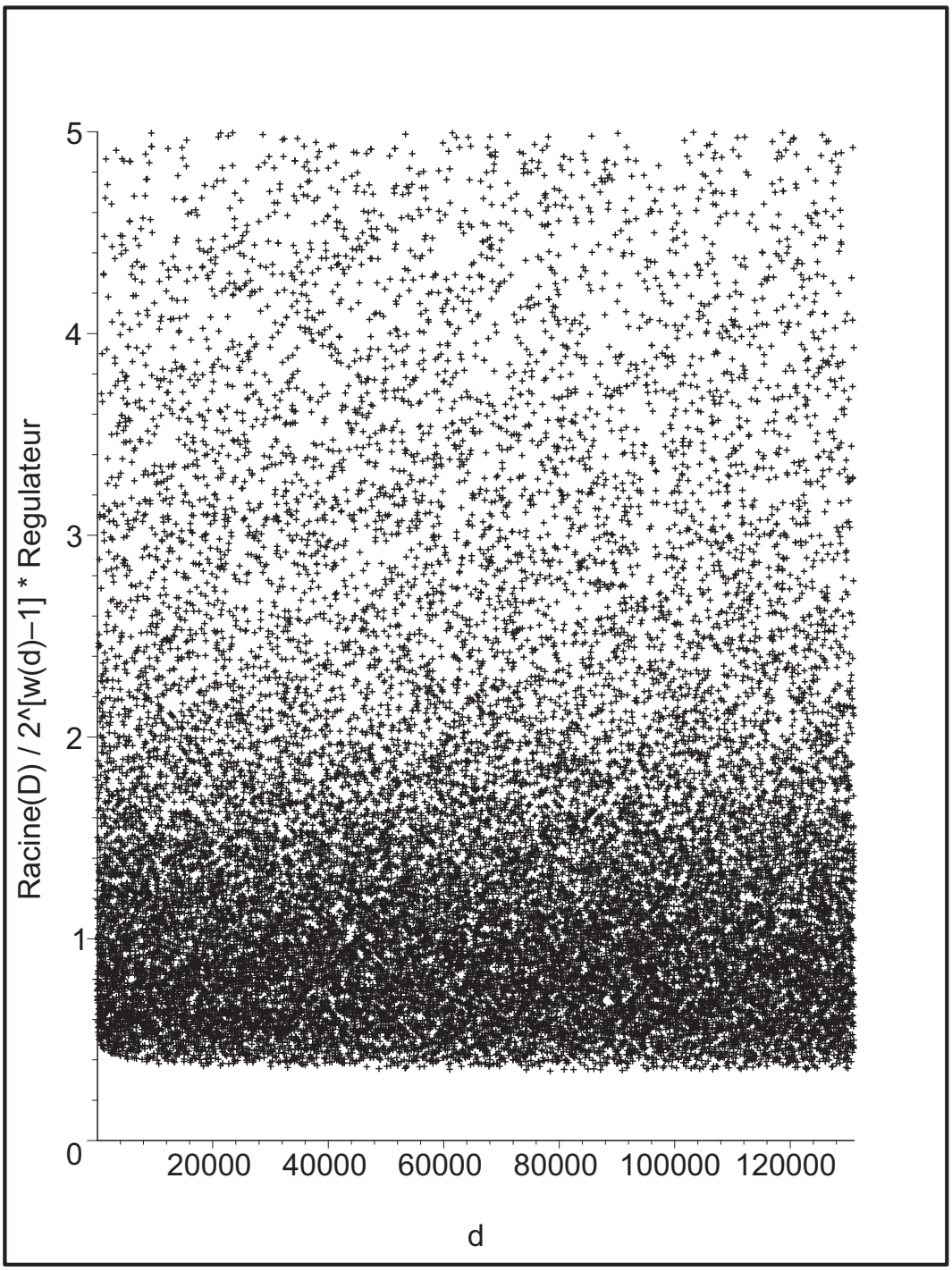

FIG. 9.10. Ratio $\dfrac{\sqrt{D}}{\log(\varepsilon_d)\cdot 2^{\omega(d)-1}}$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ en fonction de d, pour d un discriminant fondamental $\equiv 3 \bmod 4$

Dans ces graphiques, sans remarquer de tendance particulière, on constate que la densité de points est bien plus grande dans l'intervalle $[1,2]$ que dans les intervalles $[2,3]$, $[3,4]$ et $[4,5]$ (tout en tenant compte du fait que la grandeur de ces intervalles est inversement proportionnelle à la grandeur des intervalles correspondants (respectivement $[\frac{1}{2},1]$, $[\frac{1}{3},\frac{1}{2}]$, $[\frac{1}{4},\frac{1}{3}]$ et $[\frac{1}{5},\frac{1}{4}]$) des graphiques (9.5) à (9.7)), ce qui veut dire que le ratio $\dfrac{\log(\varepsilon_d)\cdot 2^{\omega(d)-1}}{\sqrt{D}}$ est à son plus dense dans l'intervalle $[\frac{1}{2},1]$ (pour $17 \leq d \leq 2^{17} = 131072$) . Sinon, ledit ratio serait semblable dans les intervalles $[\frac{1}{3},\frac{1}{2}]$, $[\frac{1}{4},\frac{1}{3}]$ et $[\frac{1}{5},\frac{1}{4}]$. Nous reparlerons de la densité de ces graphiques un peu plus loin, en l'abordant sous un autre angle.

9.2.2. Divisibilité du nombre de classes par des nombres premiers impairs

Si Gauss, vers 1800, avait décrit la divisibilité par 2 du nombre de classes, la divisibilité par d'autres entiers $g \geq 3$ comporte encore son lot de mystères plus de deux siècles plus tard. Dans sa thèse, Lillian Beatrix Pierce **[P]** s'intéresse à la divisibilité par 3 du nombre de classes et elle donne des bornes pour l'exposant de 3 dans la factorisation de $h(D)$.

Honda **[Ho]** quant à lui a montré qu'il y a une infinité de corps quadratiques réels dont le nombre de classes est divisible par 3. Dans **[Ho2]**, il donne aussi un critère pour que le nombre de classes d'un corps quadratique, réel ou imaginaire, soit divisible par 3, en utilisant les courbes elliptiques.

Beaucoup plus généralement, Yamamoto **[Ya]** et Weinberger **[W]** ont montré qu'il y a une infinité de corps quadratiques réels dont le nombre de classes est divisible par g , pour tout $g \in \mathbb{N}$.

Inversement, en ce qui concerne l'indivisibilité du nombre de classes des corps quadratiques réels, Davenport et Heilbronn **[Dav2]** ont montré que le nombre de classes n'est pas divisible par 3 pour au moins $\frac{5}{6}$ des entiers d libres de carré tels

que $0 < d \leq X$. Dans le cas des corps quadratiques imaginaires, ils ont montré que le nombre de classes n'est pas divisible par 3 pour au moins la moitié des entiers d libres de carré tels que $-X \leq d < 0$.

9.3. Répartition et comportement moyen du nombre de classes des corps quadratiques réels

Nous avons étudié dans les sections précédentes le comportement du régulateur des corps quadratiques réels. Afin d'aller plus loin dans cette étude, nous ferons un détour pour présenter un parallèle avec le comportement du nombre de classes, plus sommairement abordé jusqu'ici. Le problème de trouver une formule pour calculer le nombre de classes - problème solutionné par Dirichlet - est un des problèmes qui se posa dans l'histoire du développement de la théorie du groupe de classes des formes binaires quadratiques et de la théorie similaire du groupe de classes d'idéaux des corps quadratiques. Un peu comme nous l'avons fait pour le régulateur, une question naturelle qui s'ensuit est de trouver des bornes ainsi que le comportement asymptotique du nombre de classes.

Pour borner le nombre de classes des corps quadratiques réels, référons-nous à nouveau à la formule du nombre de classes de Dirichlet, $h_i(d) = \frac{\sqrt{D} \cdot L(1,\chi)}{2 \cdot \log(\varepsilon_d)}$. Nous avons déjà borné $L(1,\chi)$ supérieurement à la section 8.6 et nous avons trouvé que $L(1,\chi) < \log D + 2$. Nous voulons donc également une borne inférieure pour le régulateur $\log(\varepsilon_d)$, où $\varepsilon_d = \frac{a+b\sqrt{d}}{2}$ et $a^2 - db^2 = \pm 4$.
Si $b = 0$, alors $a = \pm 2$ et $\varepsilon_d = \pm 1$, mais par définition on doit avoir $\varepsilon_d > 1$, donc $b \neq 0$.
Si $a = 0$, alors $\pm 4 = db^2 \Rightarrow b = 1$ ou $2 \Rightarrow d = 1$ ou $4 \Rightarrow \mathbb{Q}(\sqrt{d}) = \mathbb{Q}$. Donc $a \neq 0$.
Ainsi $\varepsilon_d \geq \frac{1+\sqrt{d}}{2}$ (car pour que ε_d soit > 1 , on doit avoir $a > 0$ et $b > 0$. On se souvient que $a < 0$ et $b < 0$ donnent $-\varepsilon_d$ et que a et b de signes opposés donneront $\frac{1}{\varepsilon_d}$ et $\frac{-1}{\varepsilon_d}$.)
Et alors $\varepsilon_d \geq \frac{1+\sqrt{d}}{2} = \frac{2+\sqrt{4d}}{4} \geq \frac{2+\sqrt{D}}{4} > \frac{\sqrt{D}}{4}$.

Nous pouvons maintenant borner $h_i(d)$ lorsque $d > 0$:

$$h_i(d) < \frac{\sqrt{D} \cdot (\log D + 2)}{2 \cdot \log(\frac{\sqrt{D}}{4})} = O\left(\frac{\sqrt{D} \cdot \log D}{2 \cdot \log(\sqrt{D})}\right) = O\left(\frac{\sqrt{D} \cdot \log D}{\log D}\right) = O(\sqrt{D}) \ .$$

Mentionnons également que comme dans le cas des bornes que nous avons trouvées pour le régulateur, l'Hypothèse de Riemann Généralisée permettrait aussi d'améliorer les bornes du nombre de classes. En effet, en assumant la véracité de HRG et en utilisant la formule du nombre de classes de Dirichlet pour $D > 0$, on obtiendrait :

$$\begin{aligned} h_i(d) &= \frac{\sqrt{D} \cdot L(1,\chi)}{2 \cdot \log(\varepsilon_d)} \leq \frac{\sqrt{D} \cdot (2 + o(1))\, e^{\gamma}\ \log\log D}{2 \cdot \log(\frac{\sqrt{D}}{4})} \\ &= \frac{(2 + o(1))\, e^{\gamma}\ \sqrt{D}\ \log\log D}{\log(\frac{D}{16})} = O\left(\frac{\sqrt{D} \cdot \log\log D}{\log D}\right) \ . \end{aligned}$$

Malgré cette borne sur le nombre de classes des corps quadratiques réels, il y a beaucoup de variance lorsqu'on observe des valeurs particulières de $h_i(d)$. Par exemple, il semblerait (et c'est une conjecture de Gauss) que $h(D)$ prendrait la valeur 1 infiniment souvent. La borne que nous venons de trouver ne nous dit donc pas grand chose sur les valeurs particulières de $h_i(d)$.

On peut donc se demander quel est le comportement de $h_i(d)$ en moyenne, sur un certain intervalle. Gauss a justement démontré, lorsque $D < 0$, que $\sum_{-x \leq D < 0} h(D) \sim \frac{4\pi x^{3/2}}{21 \cdot \zeta(3)}$ **[Dahl]**. On connaît alors le comportement moyen du nombre de classes lorsque $D < 0$. Lorsque $D > 0$, une telle formule est bien plus difficile à trouver et est en fait toujours inconnue. Pour expliquer la différence de difficulté entre les cas où D est positif et négatif, il faut mentionner que lorsque D est négatif, la variance de $h(D)$, tel qu'on peut le constater dans la formule de Dirichlet, est seulement due au comportement de $L(1,\chi)$, puisque le comportement des autres facteurs est bien connu. Et il appert que le comportement de

$L(1,\chi)$ est relativement constant en moyenne ([**Dahl**] et [**F**]), ce qui fait qu'il n'y a pas trop d'irrégularité à prendre en compte lorsqu'on désire une formule donnant le comportement moyen de $h(D)$ lorsque $D<0$.

Néanmoins, lorsqu'on tente d'étudier le comportement moyen de $h_i(d)$ avec $d>0$, on fait face à davantage de difficulté en raison du comportement très irrégulier du régulateur. On se souvient qu'on a trouvé les bornes suivantes pour le régulateur : $\frac{1+\sqrt{d}}{2} \leq \varepsilon_d < \frac{\sqrt{D}\cdot(\log D+2)}{2}$. Cet intervalle est extrêmement grand et le régulateur s'y promène de façon plutôt irrégulière. Dans la formule du nombre de classes de Dirichlet, le nombre de classes dépend du régulateur, ce qui explique la difficulté à trouver le comportement moyen du nombre de classes.

Pour tenter d'éviter cette irrégularité, Sarnak a eu l'idée d'ordonner les discriminants selon la grandeur de l'unité fondamentale. Il a montré que lorsque x tend vers l'infini, on a

$$\sum_{D:\varepsilon_d<x} h(D) = Li(x^2) + O(x^{3/2}\cdot \log^2 x)$$

[**Dahl**] . Toutefois, bien qu'intéressant, ce résultat de Sarnak ne résout pas le problème de donner le comportement moyen du nombre de classes lorsque les discriminants sont ordonnés de façon croissante. En effet, le résultat de Sarnak ordonne et considère d'abord les discriminants ayant une unité fondamentale relativement petite, alors que la contribution principale dans la somme $S(x) = \sum_{D\leq x} h(D)$ servant à calculer le comportement moyen du nombre de classes provient surtout de discriminants associés à un gros régulateur puisqu'il y en aurait un grand nombre, si l'on se fie aux conjectures (nous en avons parlé à la section 8.7).

Hooley a quand même travaillé sur cette question et ses travaux l'ont amené à proposer une conjecture quant au comportement moyen du nombre de classes. Ses idées reposent d'abord sur le contrôle d'un intervalle pour l'unité fondamentale ε_d et ensuite sur l'utilisation de l'intégration de Stieltjes dans cet intervalle. Hooley a ainsi conjecturé la formule suivante relativement au comportement moyen du

nombre de classes :

$$S(x) \;=\; \sum_{D\leq x} h(D) \quad\sim\quad \frac{25}{12\pi^2}\cdot x\cdot \log^2 x$$

[Dahl] . Ça donne donc une contrepartie conjecturale au résultat trouvé par Gauss dans le cas où $D<0$.

Par la suite, Alexander O. Dahl a tenté d'étendre cette conjecture de Hooley à tous les moments réels de $h(D)$. Il s'est intéressé à la somme $S_\lambda(x)=\sum\limits_{D\leq x} h(D)^\lambda$, où λ est un nombre réel et où D sont des discriminants tels que $D\in\{D\in\mathbb{Z} \;\mid\; 1<D<x,\ D \text{ pas un carré parfait et } D\equiv 0 \text{ ou } 1 \bmod 4\}$. Lorsque x tend vers l'infini, Dahl ([**Dahl**]) a conjecturé que

$$S_\lambda(x)\asymp\begin{cases} x\cdot(\log x)^{2^\lambda-1} & \text{si } \lambda<1\\ x\cdot\log^2 x & \text{si } \lambda=1 \quad \text{(c'est Hooley)}\\ x^{\frac{\lambda+1}{2}}\cdot\log x & \text{si } \lambda>1\end{cases} .$$

Tout comme Hooley, Dahl est arrivé à cette conjecture en tentant de limiter l'irrégularité du nombre de classes en limitant la grandeur d'un intervalle pour l'unité fondamentale. Il a d'abord considéré D avec l'unité fondamentale dans un intervalle restreint et ensuite en brisant cet intervalle en intervalles encore plus petits en utilisant l'intégration de Stieltjes.

L'objectif de Dahl d'étudier également les moments négatifs des nombres de classes émane du fait qu'il révèle que le moment -1 notamment est lié à des questions sur les formes binaires quadratiques. Il soutient en fait que le moment -1 est relié au problème de trouver la quantité de nombres premiers inférieurs à une certaine borne et pouvant être représentés par la forme binaire quadratique principale d'un discriminant donné.

9.4. Répartition et comportement moyen des régulateurs des corps quadratiques réels

De même que la conjecture de Hooley étudie le comportement du nombre de classes des corps quadratiques réels (pour obtenir la moyenne, il aurait suffi de diviser la somme $S(x) = \sum_{D \leq x} h(D)$ par la grandeur de l'intervalle, soit x) et que la conjecture de Dahl étudie le comportement des moments du nombre de classes des corps quadratiques réels, il est naturel d'étudier le comportement des régulateurs des corps quadratiques réels et de leurs moments. On se souvient en effet que notre connaissance ou notre méconnaissance des nombres de classes et des régulateurs sont intimement liées par la formule du nombre de classes de Dirichlet.

Afin d'étudier le comportement des régulateurs, nous aborderons d'abord la répartition des unités fondamentales quadratiques, nous aborderons ensuite la répartition des unités quadratiques et nous nous pencherons enfin sur les moments des régulateurs.

9.4.1. Répartition des unités fondamentales des corps quadratiques réels

En ce qui a trait à la répartition des unités fondamentales des corps quadratiques réels, on cherchait à connaître, dans un intervalle donné, la quantité de corps quadratiques réels $\mathbb{Q}(\sqrt{d})$ de discriminant fondamental $d = D \equiv 1 \bmod 4$ ayant un régulateur approximativement égal à N, pour tout N. Nous avons considéré des intervalles de la forme $[2^k, 2^{k+1}[$ pour des valeurs de k suffisamment grandes pour avoir un assez grand jeu de données, et les limitations de notre algorithme en regard de la puissance de nos ordinateurs ont imposé une valeur maximale à k pour que le temps de calcul reste raisonnable (c'est-à-dire pour que ça se compte en heures plutôt qu'en jours). De plus, nous nous sommes contentés d'approximer le régulateur $\log(\varepsilon_d)$ à l'entier inférieur ou égal, c'est-à-dire

$\lfloor \log(\varepsilon_d) \rfloor$. Ainsi, soient

$$B_k(N) \quad := \quad \# \ \Big\{ \ d \in [2^k, 2^{k+1}[\ \Big| \ d = D \text{ est un discriminant fondamental} \equiv 1 \bmod 4, \text{ où } N = \lfloor \log(\varepsilon_d) \rfloor \ \Big\}$$

et $\qquad B_k^* \ := \ \max_N B_k(N) \quad .$

Alors les six graphiques suivants représentent les couples (x, y) avec $x = \dfrac{N}{2^{k/2}}$ et $y = \dfrac{B_k(N)}{B_k^*}$, pour $k = 15, 16, ..., 20$.

On a "normalisé" les graphiques en divisant en abscisse par $2^{k/2}$ et en ordonnée par B_k^* afin de pouvoir comparer sur des bases semblables les graphiques pour différentes valeurs de k .

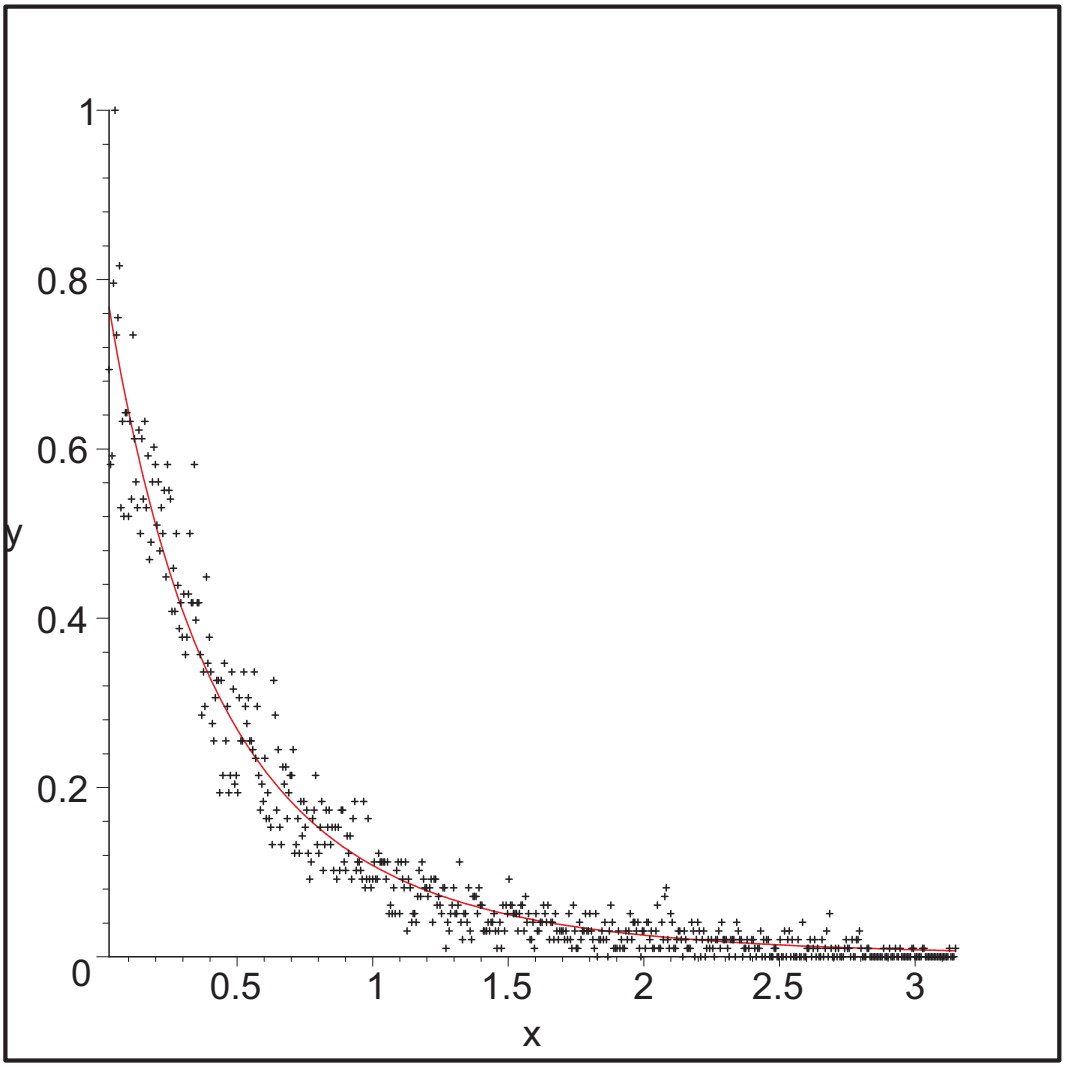

FIG. 9.11. Répartition des unités fondamentales quadratiques pour $k = 15$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{15}}}, \frac{B_{15}(N)}{B_{15}^*}\right)$

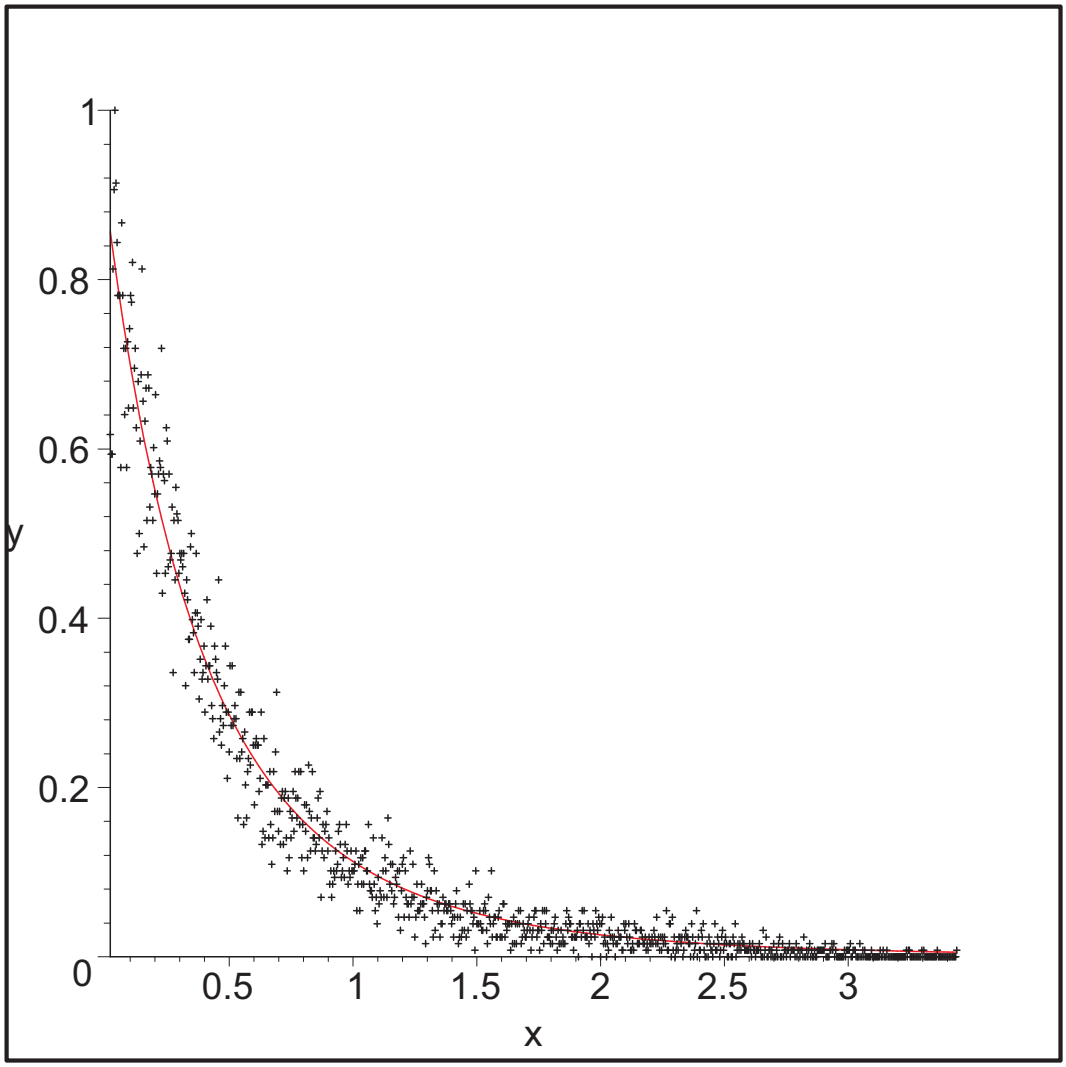

FIG. 9.12. Répartition des unités fondamentales quadratiques pour $k = 16$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{16}}}\,,\,\frac{B_{16}(N)}{B_{16}^{*}}\right)$

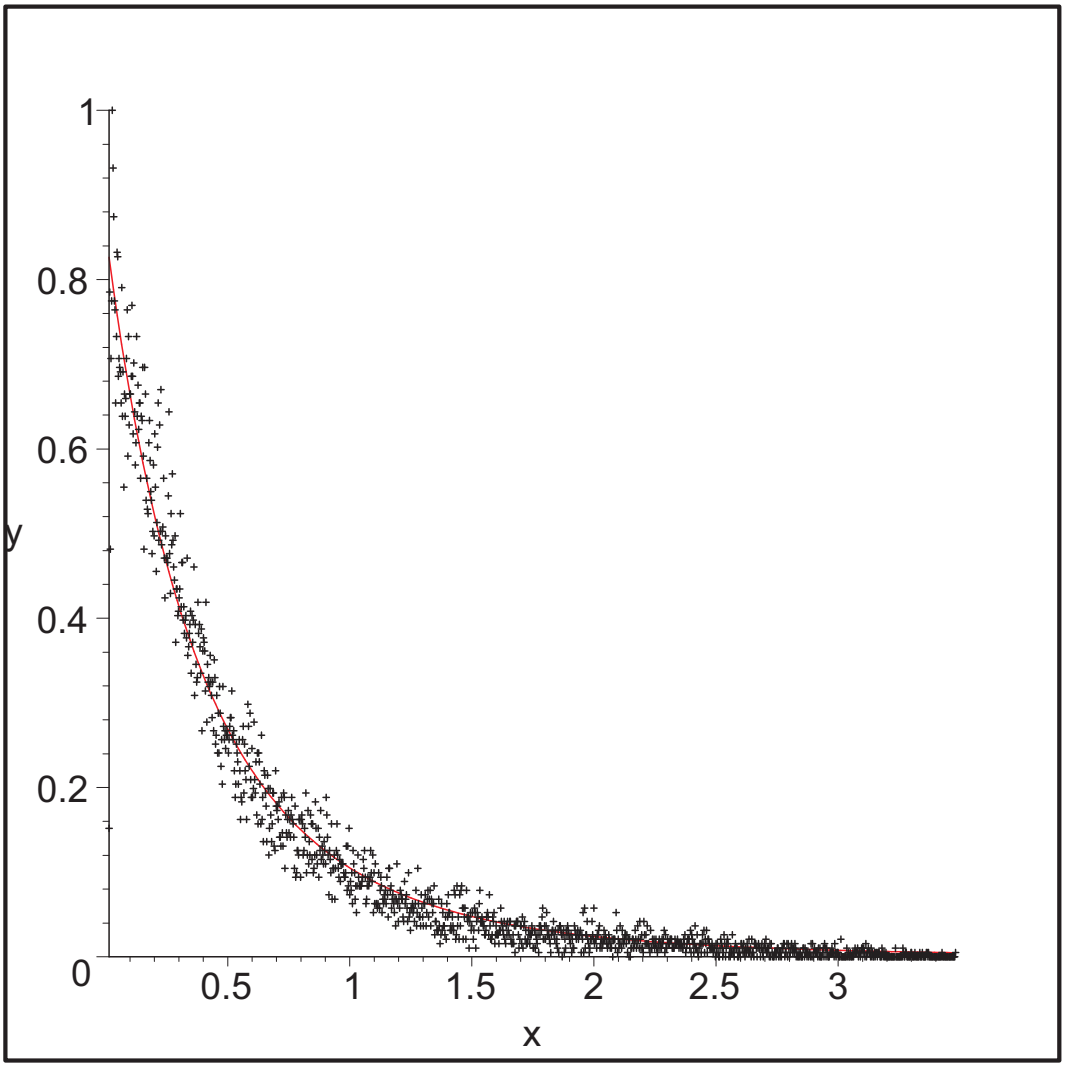

FIG. 9.13. Répartition des unités fondamentales quadratiques pour $k = 17$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{17}}}, \frac{B_{17}(N)}{B_{17}^*}\right)$

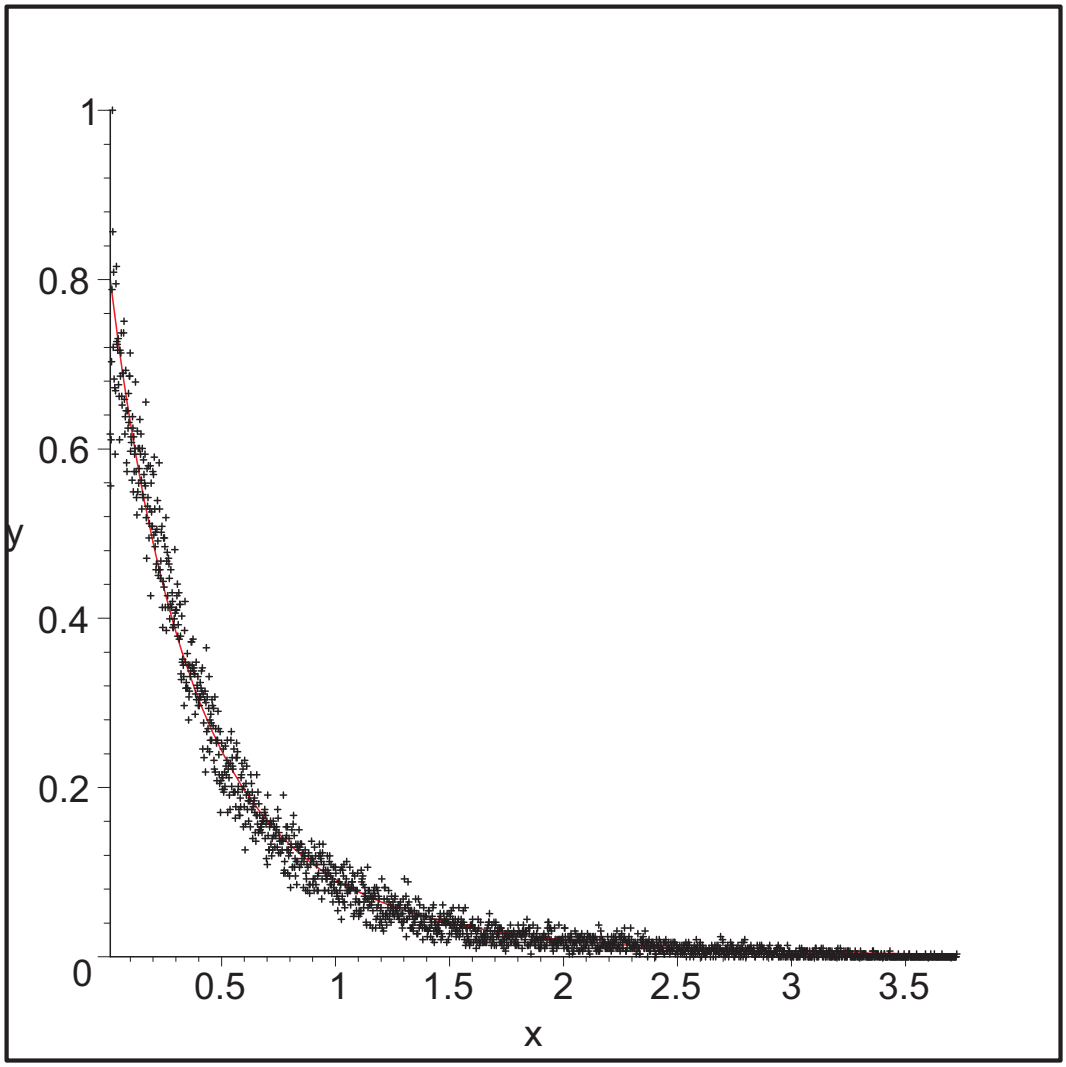

FIG. 9.14. Répartition des unités fondamentales quadratiques pour $k = 18$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{18}}}\,,\,\frac{B_{18}(N)}{B^*_{18}}\right)$

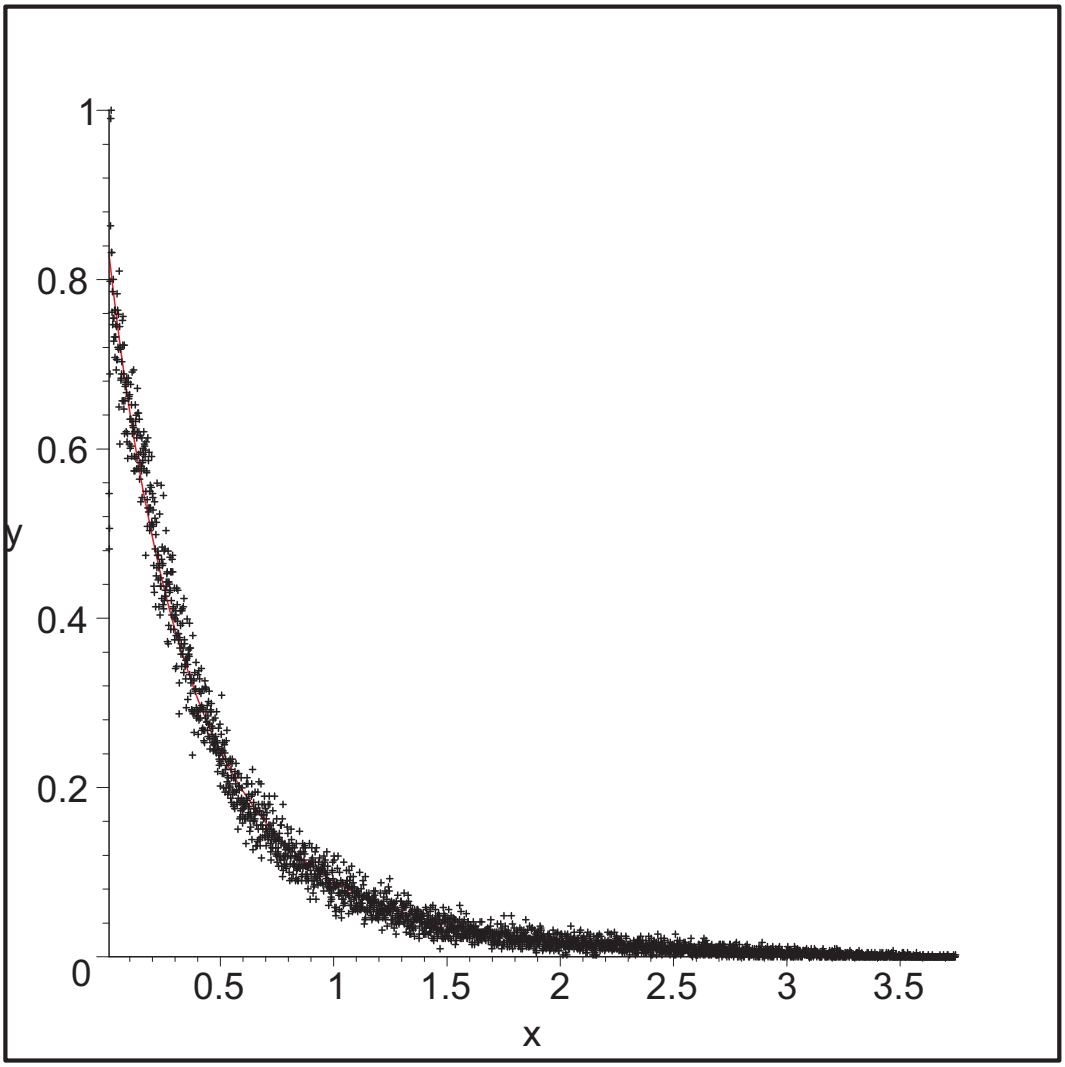

FIG. 9.15. Répartition des unités fondamentales quadratiques pour $k = 19$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{19}}}, \frac{B_{19}(N)}{B_{19}^*}\right)$

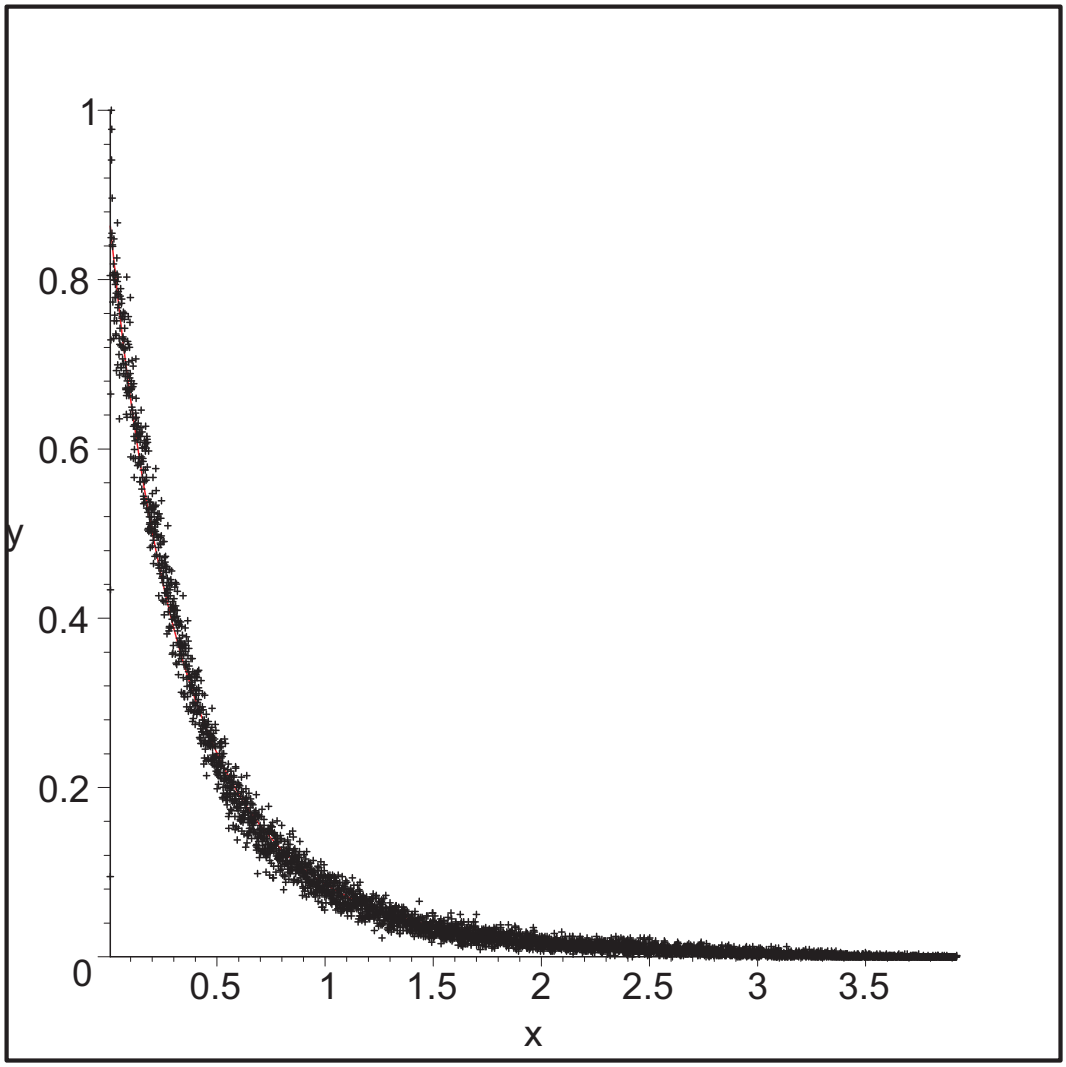

FIG. 9.16. Répartition des unités fondamentales quadratiques pour $k = 20$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{20}}} , \frac{B_{20}(N)}{B^*_{20}} \right)$

En observant ces six graphiques (9.11) à (9.16), tel qu'on peut s'y attendre suite au graphique (9.2), on constate qu'en ce qui concerne les corps quadratiques réels de discriminant $d = D \equiv 1 \bmod 4$, la plupart des régulateurs sont très petits. En fait, dans chaque graphique, on a divisé en abscisse par $\sqrt{2^k}$, ce qui fait en sorte que $\sqrt{d}$ pour $d \in [2^k, 2^{k+1}[$ va se retrouver entre 1 et $\sqrt{2}$.
En effet, $x = 1 \Rightarrow N = \sqrt{2^k}$ et $x = \sqrt{2} \Rightarrow N = \sqrt{2} \cdot \sqrt{2^k} = \sqrt{2^{k+1}}$.
Ainsi, on constate que la très grande majorité des régulateurs sont bien plus petits que $\sqrt{d}$.

On peut aussi noter qu'on avait calculé une borne supérieure (probablement pas optimale) de $\dfrac{\sqrt{D}\cdot(\log D+2)}{2}$ pour le régulateur. Dans chacun des intervalles $[2^k,2^{k+1}[$, cette borne supérieure correspond à

$$\begin{aligned}\frac{\sqrt{D}\cdot(\log_e D+2)}{2} &= \frac{\sqrt{d}\cdot(\log_e d+2)}{2} < \frac{\sqrt{2^{k+1}}\cdot\big(\log_e(2^{k+1})+2\big)}{2}\\ &= \frac{\sqrt{2^k}}{2}\cdot\big[(k+1)\cdot\sqrt{2}\cdot\log_e 2 \;+\; 2\sqrt{2}\big]\\ &< \frac{\sqrt{2^k}}{2}\cdot\big[(k+1)\cdot 1 \;+\; 2\sqrt{2}\big] \;=\; \sqrt{2^k}\cdot\left(\frac{k}{2}+\frac{1}{2}+\sqrt{2}\right)\\ &< \sqrt{2^k}\cdot\left(\frac{k}{2}+2\right).\end{aligned}$$

Bref, transposons cette borne dans les graphiques.
Si $N=\lfloor\log(\varepsilon_d)\rfloor\le\log(\varepsilon_d)<\sqrt{2^k}\cdot\left(\dfrac{k}{2}+2\right)$, alors $x=\dfrac{N}{\sqrt{2^k}}<\dfrac{k}{2}+2$, ce qui est très facilement respecté.

Par ailleurs, les précédents graphiques (9.11) à (9.16) ont la particularité de présenter entre certaines valeurs de d la densité des points sur l'ensemble des droites horizontales du graphique (9.2) . En effet, on voyait dans le graphique (9.2) le régulateur $\log(\varepsilon_d)$ en fonction de d . Mais il y avait une telle concentration de points dans le bas du graphique qu'il serait utile, pour mieux le comprendre, de savoir combien il y avait de points sur chacune des droites horizontales $y=N$ (ou en fait dans chaque bande horizontale $y\in[N,N+1[$ pour $d\in[2^k,2^{k+1}[$). C'est ce que les graphiques (9.11) à (9.16) font en nous y présentant le nombre de régulateurs dont la partie entière est égale à N .

Nous avons aussi modélisé (en minimisant les moindres carrés avec l'aide de Maple) le nuage de points des graphiques (9.11) à (9.16), qui est une fonction polynomiale inverse. Nous vous présentons les résultats de la modélisation pour chacun de ces graphiques sous la forme $y=\left(\dfrac{a}{x+b}\right)^5$, où nous avons encore que $x=\dfrac{N}{2^{k/2}}$ et $y=\dfrac{B_k(N)}{B_k^*}$. L'exposant 5 était expérimentalement celui qui donnait la meilleure modélisation. La courbe modélisée a été tracée en rouge dans les graphiques.

Pour $k = 15$, $y = \left(\dfrac{1.921}{x + 1.998}\right)^5$.

Pour $k = 16$, $y = \left(\dfrac{1.900}{x + 1.941}\right)^5$.

Pour $k = 17$, $y = \left(\dfrac{1.860}{x + 1.919}\right)^5$.

Pour $k = 18$, $y = \left(\dfrac{1.742}{x + 1.810}\right)^5$.

Pour $k = 19$, $y = \left(\dfrac{1.702}{x + 1.759}\right)^5$.

Pour $k = 20$, $y = \left(\dfrac{1.648}{x + 1.691}\right)^5$.

Nous allons en profiter, similairement, pour étudier la densité lorsque le régulateur est multiplié par $2^{\omega(d)-1}$. Les graphiques, comme on pourra le constater, seront un peu plus diffus. Plus précisément, on cherchait ici à connaître, dans un intervalle donné pour d , la quantité de corps quadratiques réels $\mathbb{Q}(\sqrt{d})$ de discriminant fondamental $d = D \equiv 1 \bmod 4$ dont le produit du régulateur par $2^{\omega(d)-1}$ est approximativement égal à N , pour tout N . Nous avons à nouveau considéré des intervalles de la forme $[2^k, 2^{k+1}[$.
Ainsi, soient

$$C_k(N) := \# \left\{ d \in [2^k, 2^{k+1}[\;\middle|\; d = D \text{ est un discriminant fondamental} \equiv 1 \bmod 4, \text{ où } N = \lfloor \log(\varepsilon_d) \cdot 2^{\omega(d)-1} \rfloor \right\}$$

et $C_k^* := \max_N C_k(N)$.

Alors les graphiques (9.17), (9.23) et (9.29) représentent les couples (x, y) avec $x = \dfrac{N}{2^{k/2}}$ et $y = \dfrac{C_k(N)}{C_k^*}$, pour $k = 18, 19, 20$.
Les graphiques (9.18), (9.24) et (9.30), quant à eux, montrent la même chose mais pour $x < 1$ afin de mieux distinguer le nuage de points au début du graphique. On a "normalisé" les graphiques en divisant en abscisse par $2^{k/2}$ et en ordonnée par C_k^* afin de pouvoir comparer sur des bases semblables les graphiques pour différentes valeurs de k .

Nous allons également présenter ces graphiques en ajoutant la restriction que $\omega(d)$ soit égal à j, pour certaines des différentes valeurs de j possibles. (Nous ne présenterons pas les graphiques où le nombre de points est trop petit pour montrer quoi que ce soit.) Ainsi, soient

$$C_k^j(N) \quad := \quad \# \left\{ d \in [2^k, 2^{k+1}[\;\middle|\; d = D \text{ est un discriminant fondamental} \right. \\ \left. \equiv 1 \bmod 4, \text{ avec } \omega(d) = j, \text{ où } N = \lfloor \log(\varepsilon_d) \cdot 2^{\omega(d)-1} \rfloor \right\}$$

et $\qquad C_k^{j\,*} \quad := \quad \max_N C_k^j(N) \quad .$

Alors les graphiques (9.19) à (9.22), (9.25) à (9.28) et (9.31) à (9.34) représentent les couples (x, y) avec $x = \dfrac{N}{2^{k/2}}$ et $y = \dfrac{C_k^j(N)}{C_k^{j\,*}}$, pour certaines des différentes valeurs de j possibles et pour $k = 18, 19, 20$.

On a ainsi à nouveau "normalisé" les graphiques en divisant en abscisse par $2^{k/2}$ et en ordonnée par $C_k^{j\,*}$ afin de pouvoir comparer sur des bases semblables les graphiques pour les différentes valeurs de j et pour différentes valeurs de k.

On remarquera peut-être que dans certains graphiques, il n'y a que certaines valeurs discrètes en ordonnée qui sont prises. C'est parce que dans ces graphiques, il n'y a qu'au plus $C_k^{j\,*}$ valeurs possibles en ordonnée.

Rappelons en passant que lorsque $d \equiv 1 \bmod 4$, on a que

$$\log(\varepsilon_d) \cdot 2^{\omega(d)-1} \quad = \quad \frac{\sqrt{D} \cdot L(1, \chi)}{\{1 \text{ ou } 2\} \cdot h_2} \quad .$$

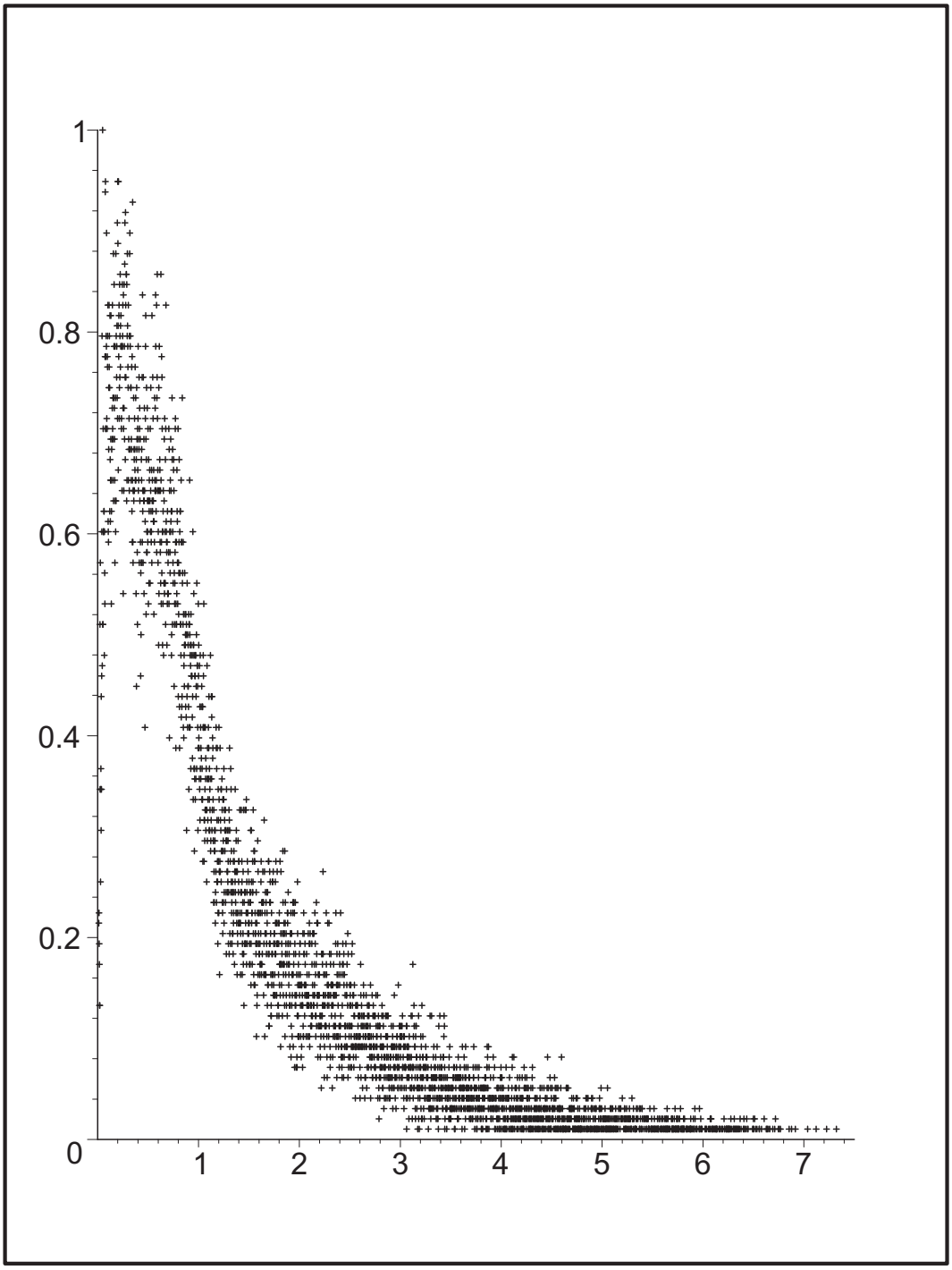

FIG. 9.17. Répartition de $\log(\varepsilon_d) \cdot 2^{\omega(d)-1}$ pour $k = 18$, c'est-à-dire ensemble des couples $\left(\dfrac{N}{\sqrt{2^{18}}} , \dfrac{C_{18}(N)}{C_{18}^*} \right)$

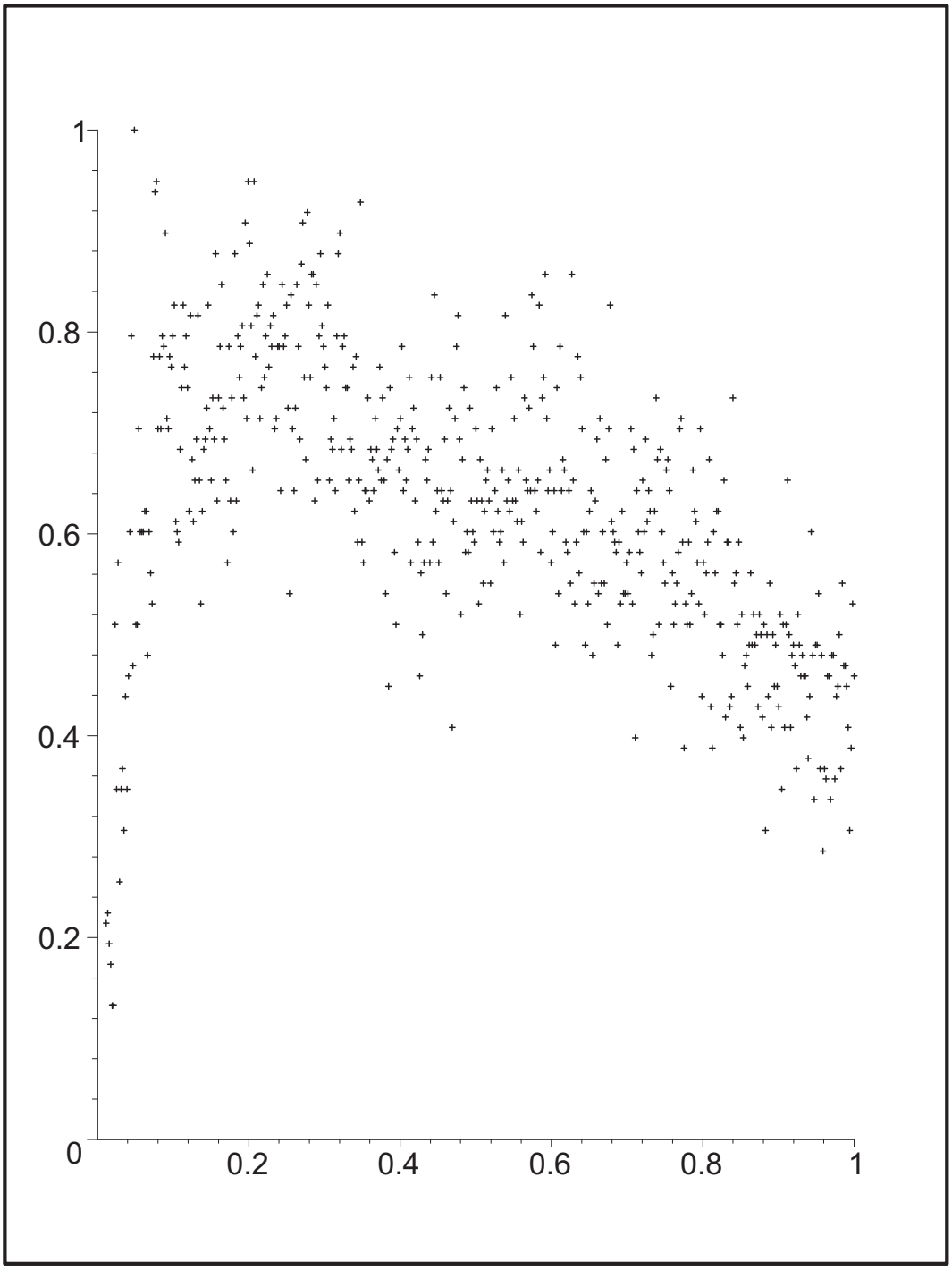

FIG. 9.18. Répartition de $\log(\varepsilon_d) \cdot 2^{\omega(d)-1}$ pour $k = 18$ et pour $x < 1$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{18}}}, \frac{C_{18}(N)}{C_{18}^*} \right)$ pour $x < 1$

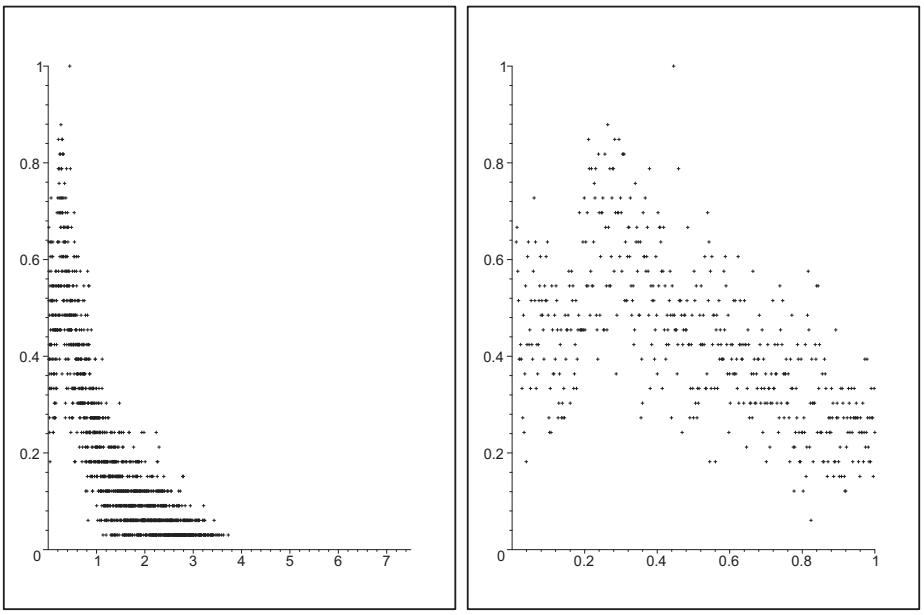

FIG. 9.19. Répartition de $\log(\varepsilon_d)\cdot 2^{\omega(d)-1}$ $\Big\{$c'est-à-dire ensemble des couples $\left(\dfrac{N}{\sqrt{2^{18}}}\,,\,\dfrac{C_{18}^{1}(N)}{C_{18}^{1\,*}}\right)\Big\}$ lorsque $\omega(d)=1$ pour $k=18$, au complet à gauche et ensuite pour $x<1$ à droite

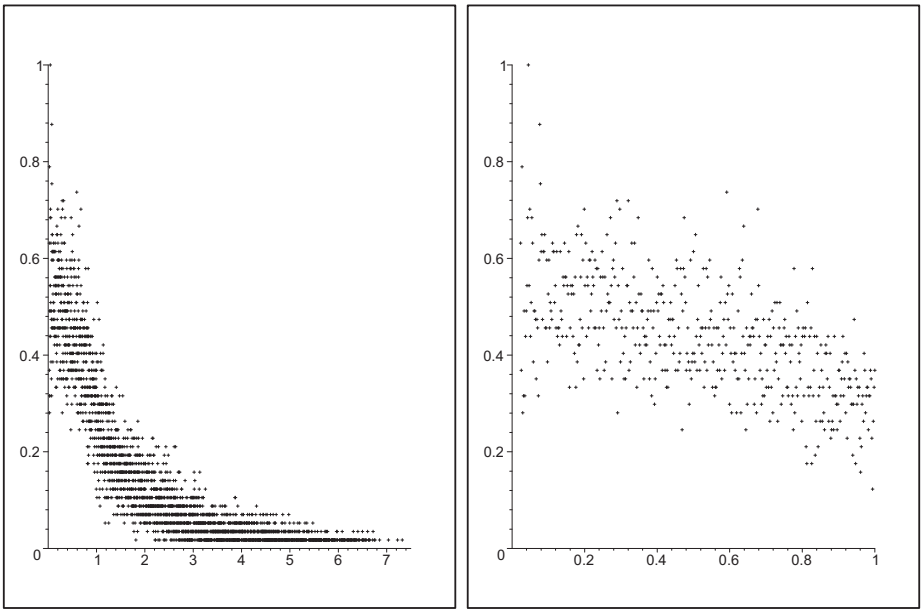

FIG. 9.20. Répartition de $\log(\varepsilon_d)\cdot 2^{\omega(d)-1}$ $\Big\{$c'est-à-dire ensemble des couples $\left(\dfrac{N}{\sqrt{2^{18}}}\,,\,\dfrac{C_{18}^{2}(N)}{C_{18}^{2\,*}}\right)\Big\}$ lorsque $\omega(d)=2$ pour $k=18$ au complet à gauche et ensuite pour $x<1$ à droite

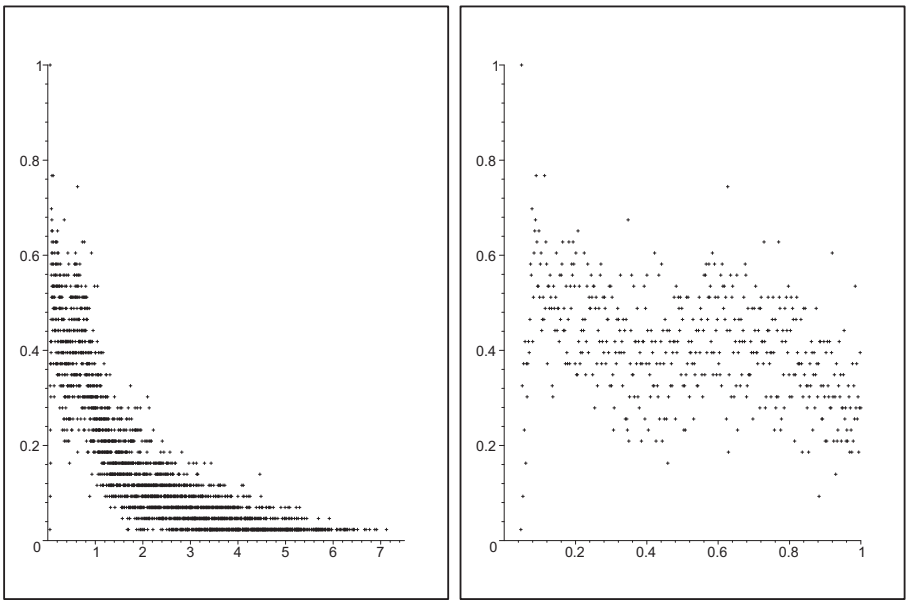

FIG. 9.21. Répartition de $\log(\varepsilon_d)\cdot 2^{\omega(d)-1}$ $\Big\{$c'est-à-dire ensemble des couples $\left(\dfrac{N}{\sqrt{2^{18}}}\,,\,\dfrac{C_{18}^{3}(N)}{C_{18}^{3\,*}}\right)\Big\}$ lorsque $\omega(d)=3$ pour $k=18$ au complet à gauche et ensuite pour $x<1$ à droite

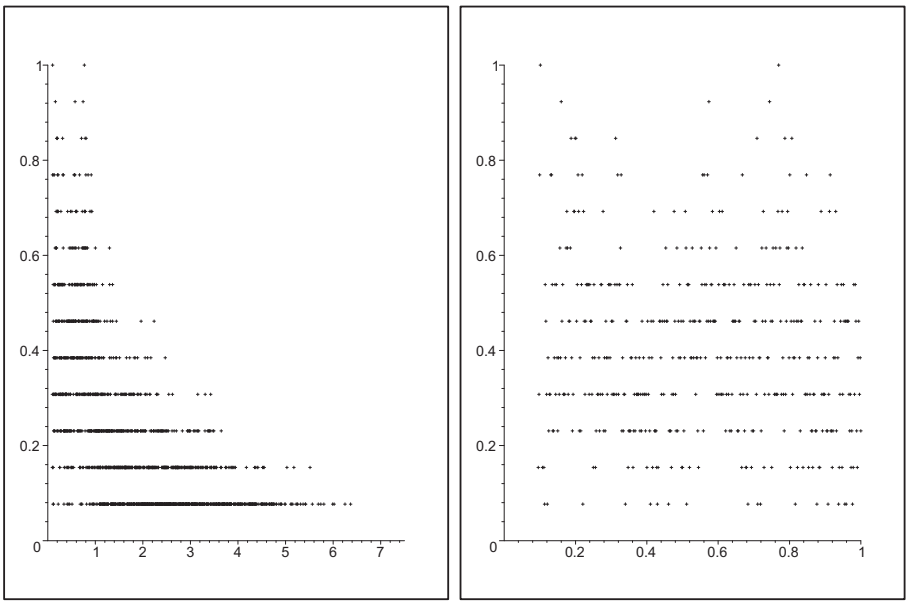

FIG. 9.22. Répartition de $\log(\varepsilon_d)\cdot 2^{\omega(d)-1}$ $\Big\{$c'est-à-dire ensemble des couples $\left(\dfrac{N}{\sqrt{2^{18}}}\,,\,\dfrac{C_{18}^{4}(N)}{C_{18}^{4\,*}}\right)\Big\}$ lorsque $\omega(d)=4$ pour $k=18$ au complet à gauche et ensuite pour $x<1$ à droite

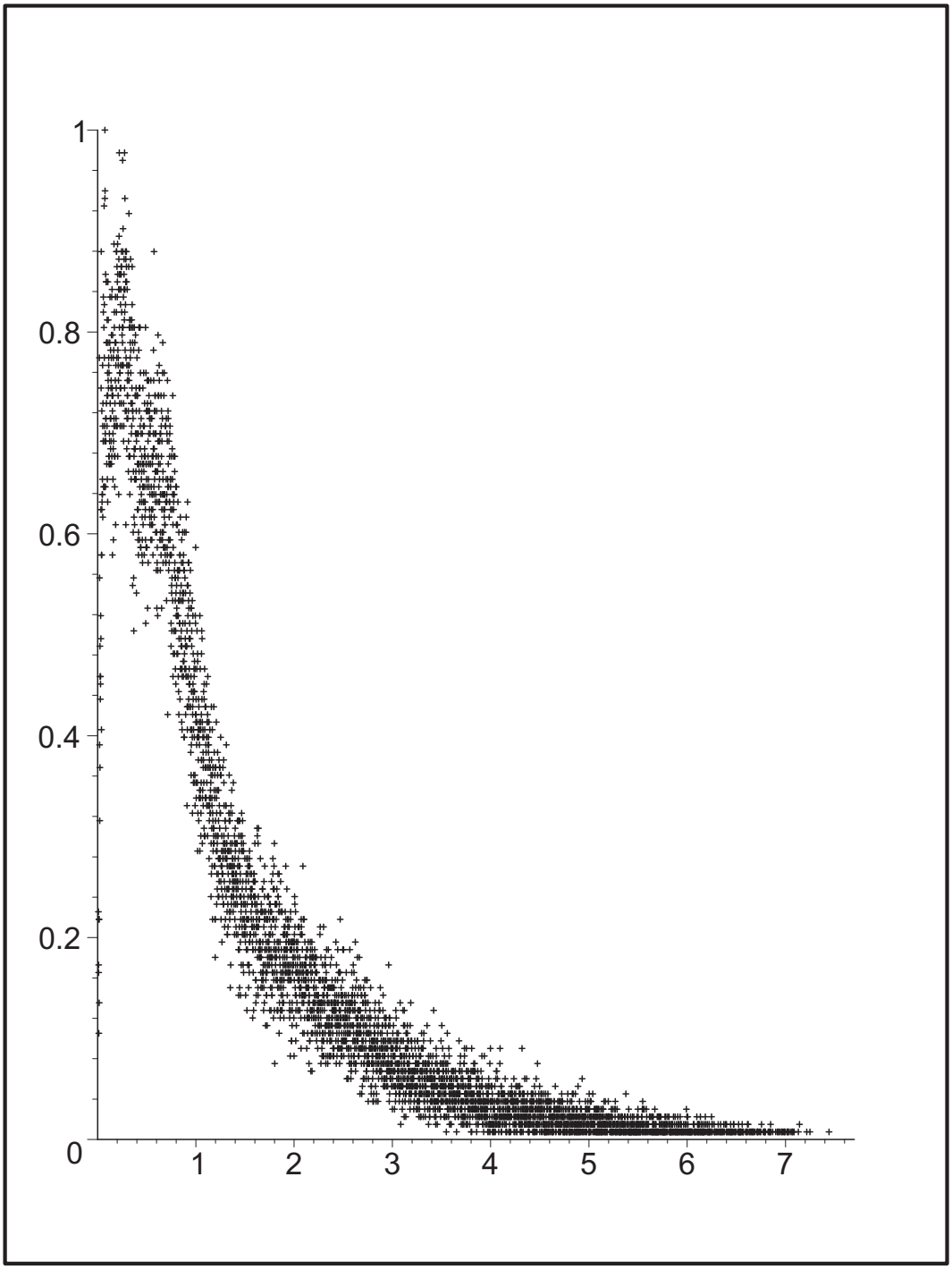

FIG. 9.23. Répartition de $\log(\varepsilon_d) \cdot 2^{\omega(d)-1}$ pour $k = 19$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{19}}}, \frac{C_{19}(N)}{C_{19}^*} \right)$

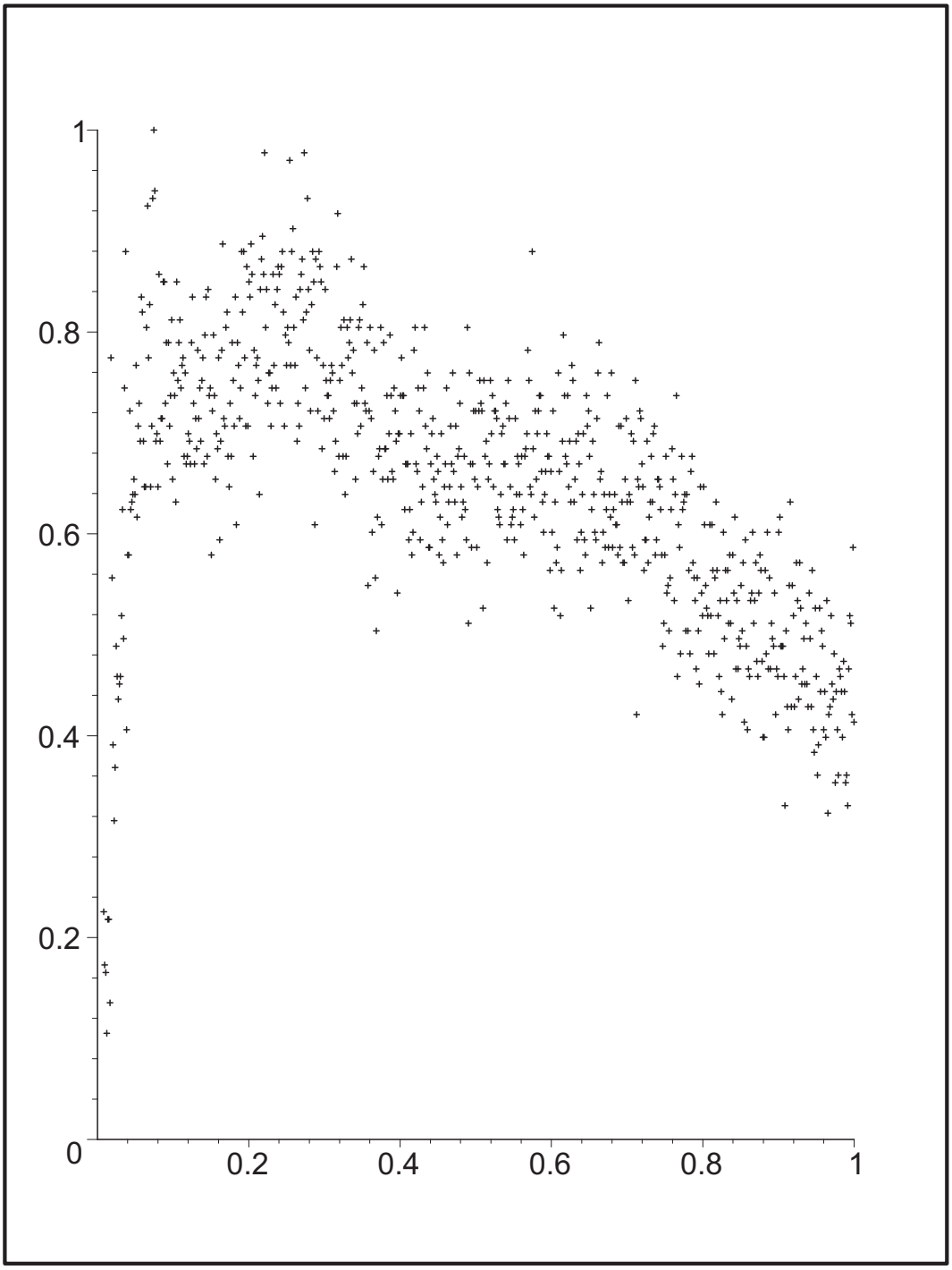

FIG. 9.24. Répartition de $\log(\varepsilon_d) \cdot 2^{\omega(d)-1}$ pour $k = 19$ et pour $x < 1$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{19}}}, \frac{C_{19}(N)}{C_{19}^*} \right)$ pour $x < 1$

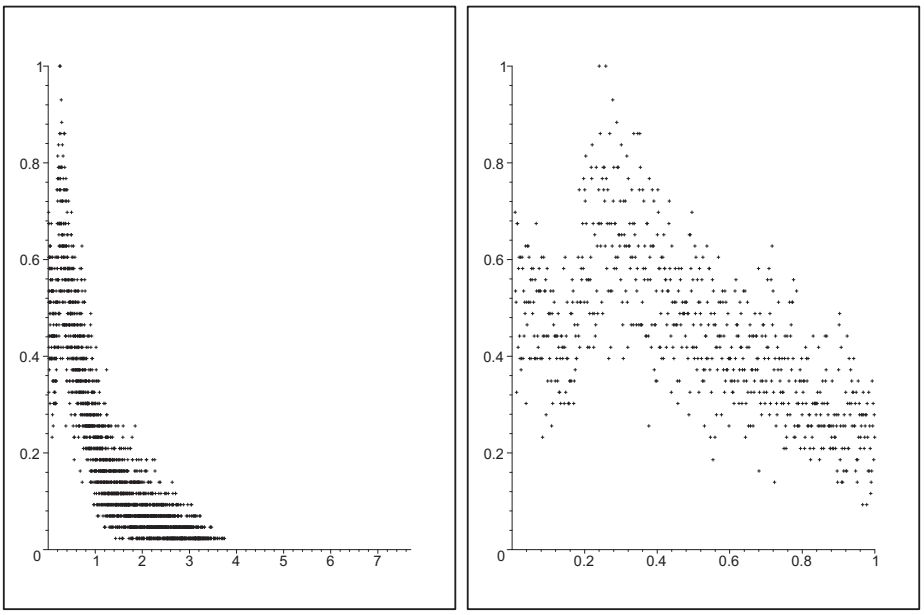

FIG. 9.25. Répartition de $\log(\varepsilon_d)\cdot 2^{\omega(d)-1}$ $\Big\{$c'est-à-dire ensemble des couples $\left(\dfrac{N}{\sqrt{2^{19}}}\,,\,\dfrac{C_{19}^{1}(N)}{C_{19}^{1\,*}}\right)\Big\}$ lorsque $\omega(d)=1$ pour $k=19$ au complet à gauche et ensuite pour $x<1$ à droite

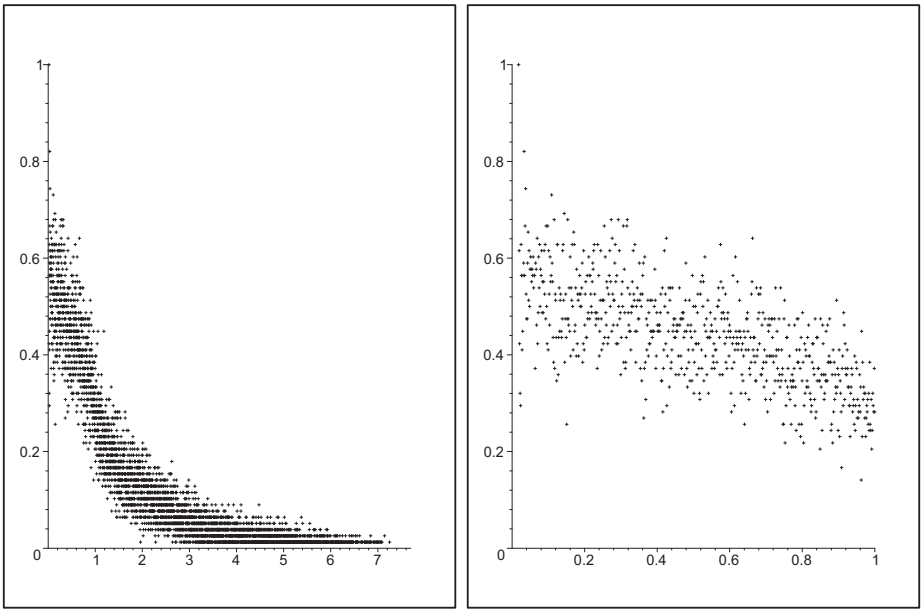

FIG. 9.26. Répartition de $\log(\varepsilon_d)\cdot 2^{\omega(d)-1}$ $\Big\{$c'est-à-dire ensemble des couples $\left(\dfrac{N}{\sqrt{2^{19}}}\,,\,\dfrac{C_{19}^{2}(N)}{C_{19}^{2\,*}}\right)\Big\}$ lorsque $\omega(d)=2$ pour $k=19$ au complet à gauche et ensuite pour $x<1$ à droite

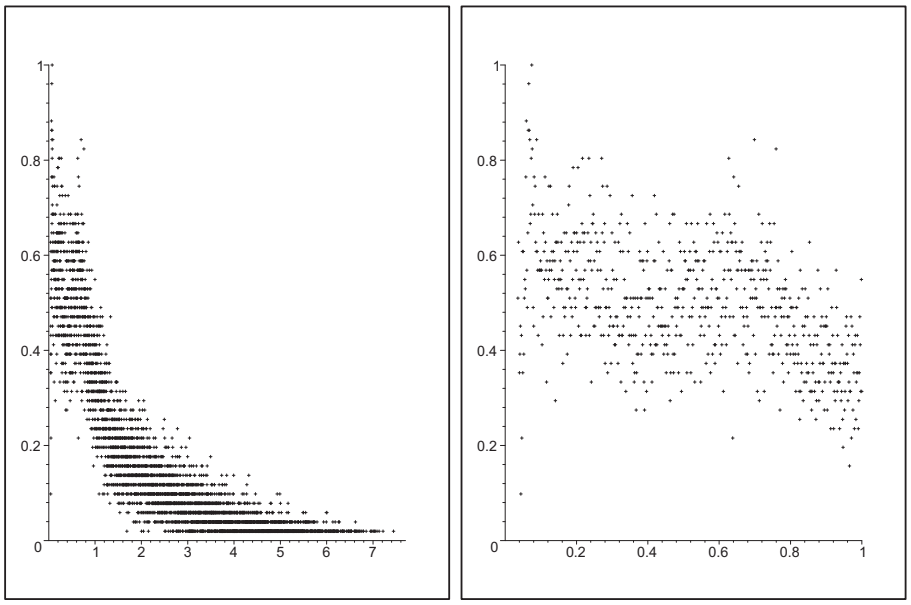

FIG. 9.27. Répartition de $\log(\varepsilon_d)\cdot 2^{\omega(d)-1}$ $\Big\{$c'est-à-dire ensemble des couples $\left(\dfrac{N}{\sqrt{2^{19}}}\,,\,\dfrac{C_{19}^{3}(N)}{C_{19}^{3\,*}}\right)\Big\}$ lorsque $\omega(d)=3$ pour $k=19$ au complet à gauche et ensuite pour $x<1$ à droite

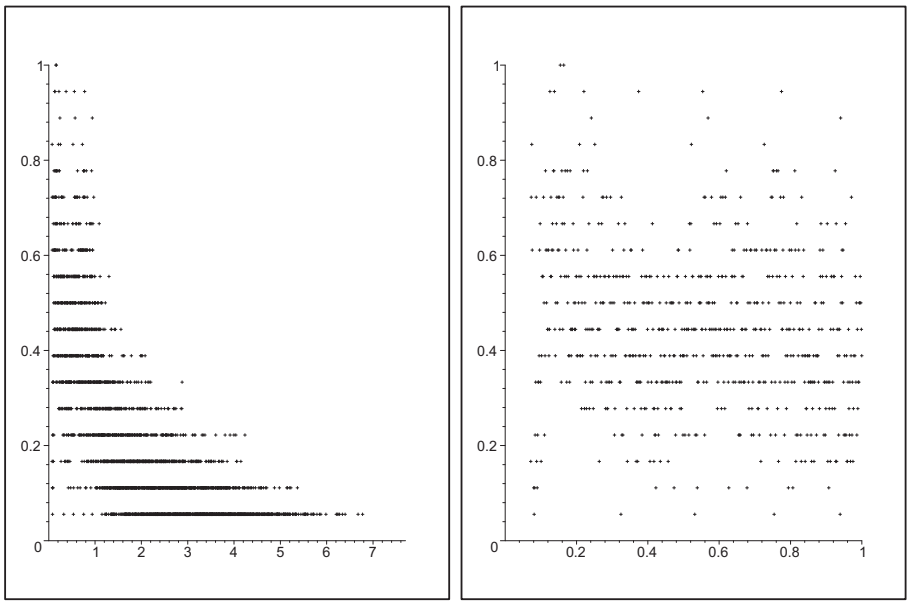

FIG. 9.28. Répartition de $\log(\varepsilon_d)\cdot 2^{\omega(d)-1}$ $\Big\{$c'est-à-dire ensemble des couples $\left(\dfrac{N}{\sqrt{2^{19}}}\,,\,\dfrac{C_{19}^{4}(N)}{C_{19}^{4\,*}}\right)\Big\}$ lorsque $\omega(d)=4$ pour $k=19$ au complet à gauche et ensuite pour $x<1$ à droite

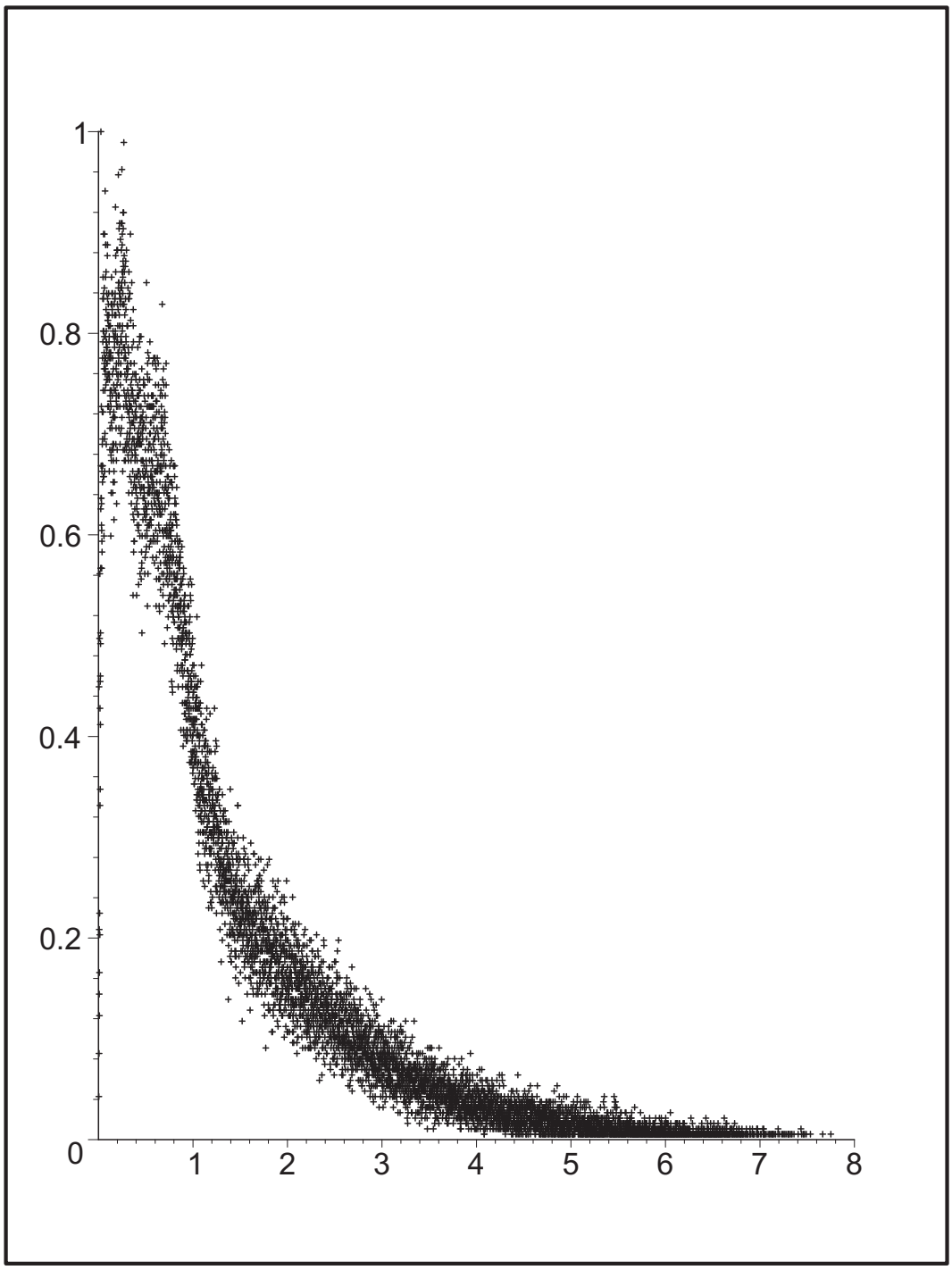

FIG. 9.29. Répartition de $\log(\varepsilon_d) \cdot 2^{\omega(d)-1}$ pour $k = 20$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{20}}}, \frac{C_{20}(N)}{C^*_{20}} \right)$

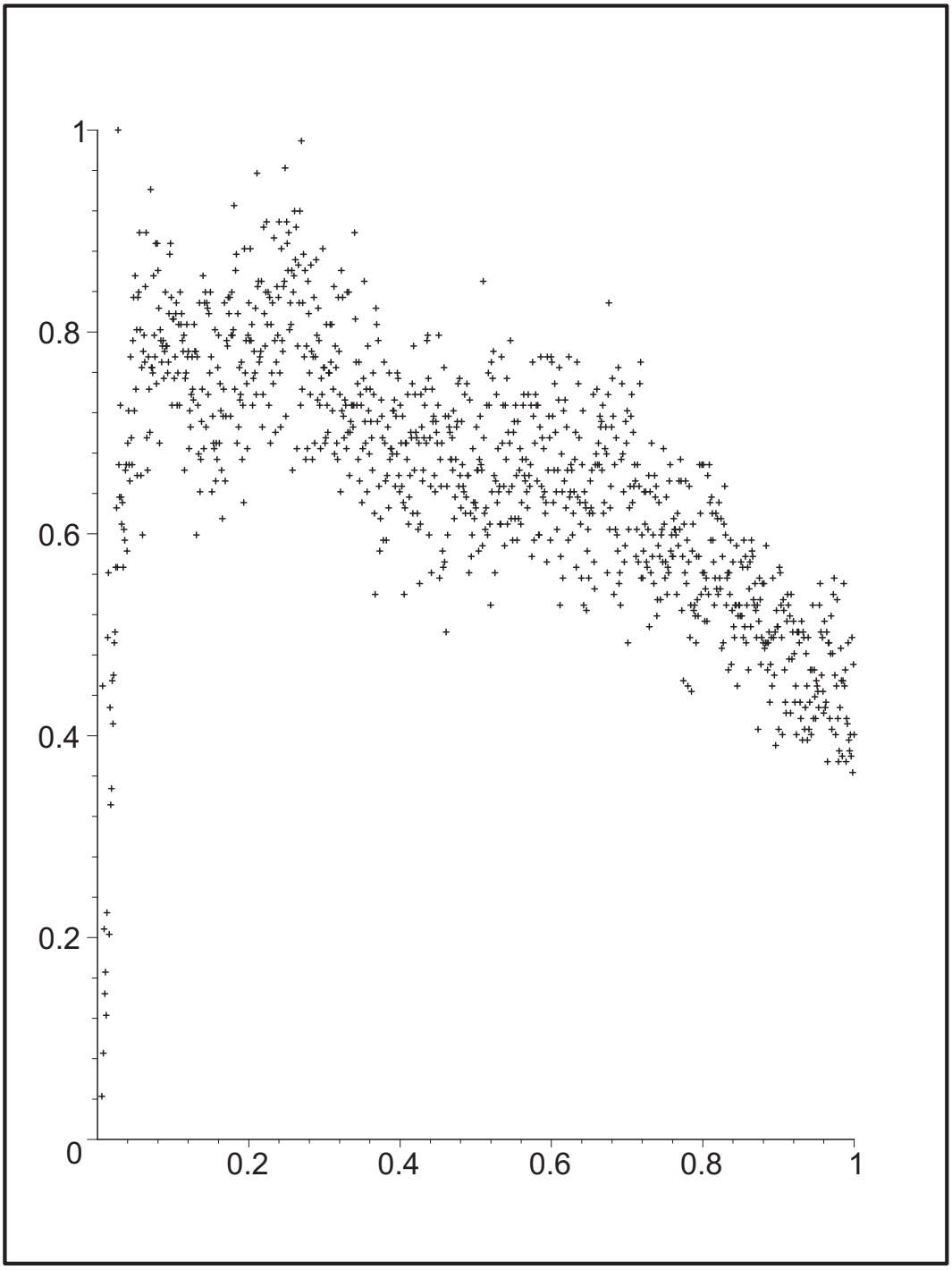

FIG. 9.30. Répartition de $\log(\varepsilon_d) \cdot 2^{\omega(d)-1}$ pour $k = 20$ et pour $x < 1$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{20}}}, \frac{C_{20}(N)}{C_{20}^*} \right)$ pour $x < 1$

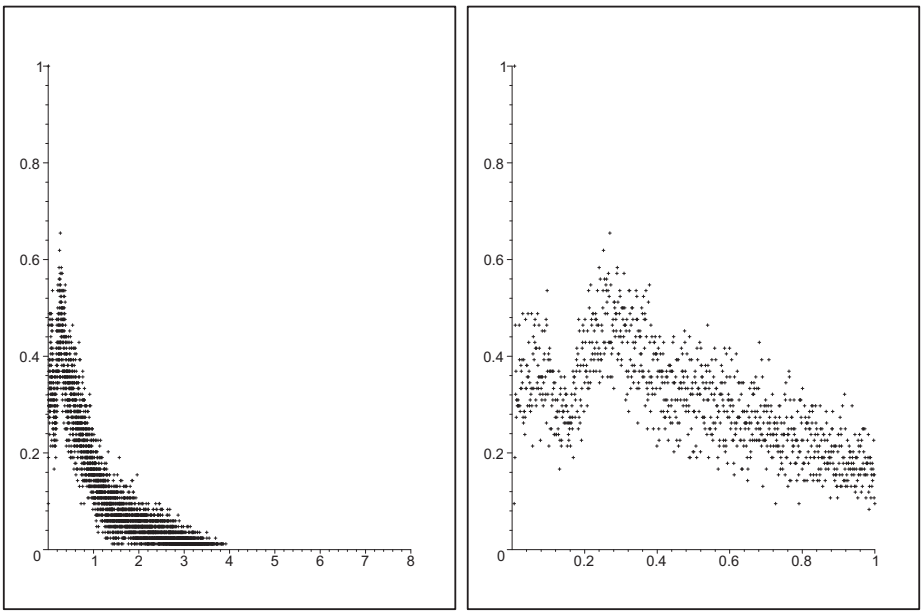

FIG. 9.31. Répartition de $\log(\varepsilon_d)\cdot 2^{\omega(d)-1}$ $\Big\{$c'est-à-dire ensemble des couples $\left(\dfrac{N}{\sqrt{2^{20}}}\,,\,\dfrac{C_{20}^{1}(N)}{C_{20}^{1\,*}}\right)\Big\}$ lorsque $\omega(d)=1$ pour $k=20$ au complet à gauche et ensuite pour $x<1$ à droite

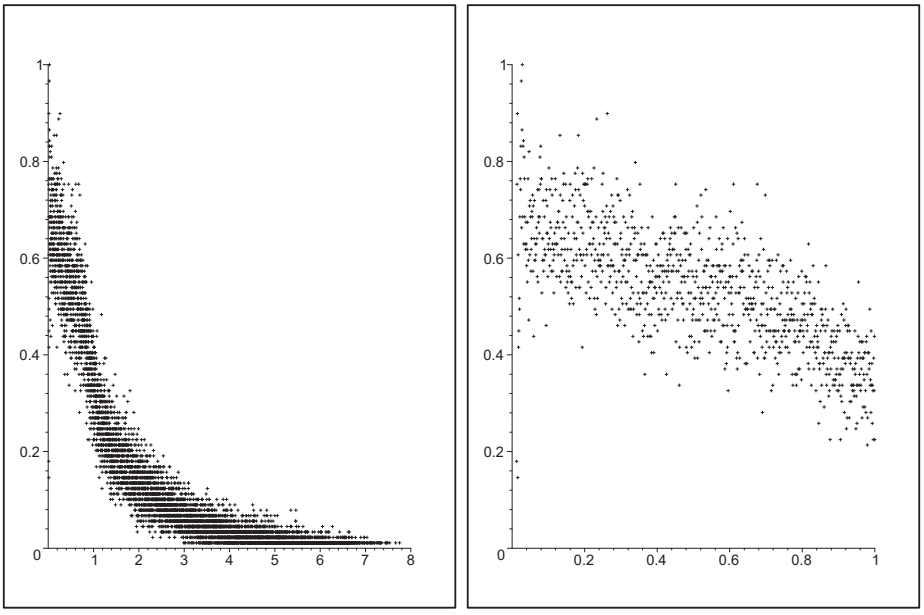

FIG. 9.32. Répartition de $\log(\varepsilon_d)\cdot 2^{\omega(d)-1}$ $\Big\{$c'est-à-dire ensemble des couples $\left(\dfrac{N}{\sqrt{2^{20}}}\,,\,\dfrac{C_{20}^{2}(N)}{C_{20}^{2\,*}}\right)\Big\}$ lorsque $\omega(d)=2$ pour $k=20$ au complet à gauche et ensuite pour $x<1$ à droite

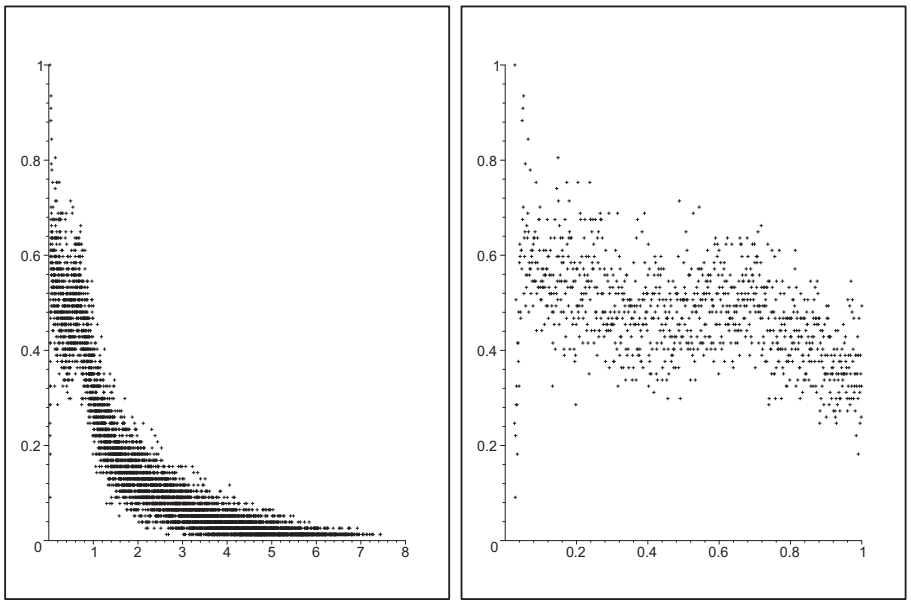

FIG. 9.33. Répartition de $\log(\varepsilon_d)\cdot 2^{\omega(d)-1}$ $\Big\{$c'est-à-dire ensemble des couples $\left(\dfrac{N}{\sqrt{2^{20}}}\,,\,\dfrac{C_{20}^{3}(N)}{C_{20}^{3\,*}}\right)\Big\}$ lorsque $\omega(d)=3$ pour $k=20$ au complet à gauche et ensuite pour $x<1$ à droite

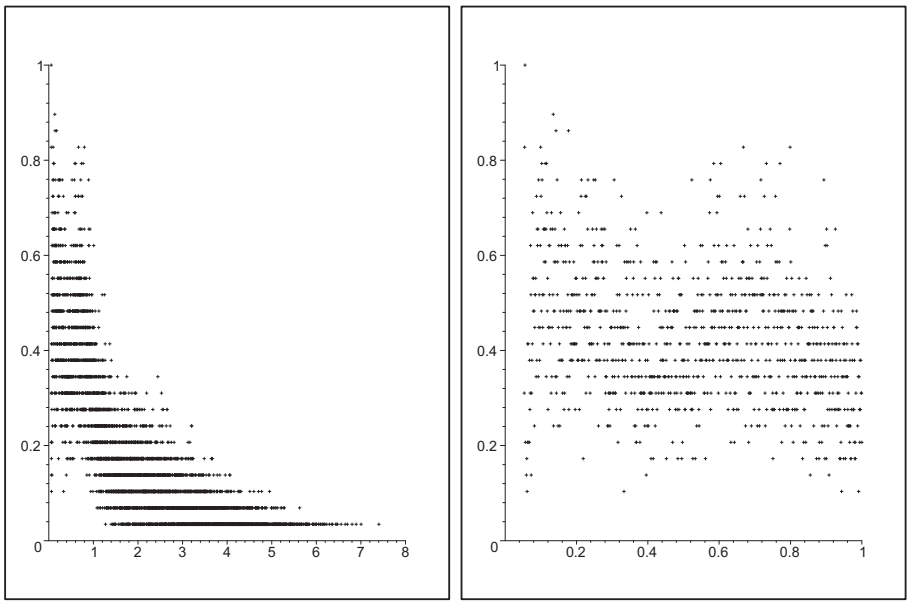

FIG. 9.34. Répartition de $\log(\varepsilon_d)\cdot 2^{\omega(d)-1}$ $\Big\{$c'est-à-dire ensemble des couples $\left(\dfrac{N}{\sqrt{2^{20}}}\,,\,\dfrac{C_{20}^{4}(N)}{C_{20}^{4\,*}}\right)\Big\}$ lorsque $\omega(d)=4$ pour $k=20$ au complet à gauche et ensuite pour $x<1$ à droite

9.4.2. Répartition des unités des corps quadratiques réels

En ce qui a trait à la répartition des unités dans les corps quadratiques réels, on cherchait à connaître, dans un intervalle donné, la quantité de corps quadratiques réels $\mathbb{Q}(\sqrt{d})$ de discriminant fondamental $d = D \equiv 1 \bmod 4$ ayant au moins une unité dont le logarithme est égal à $N \in \mathbb{N}$. Nous considérions en fait seulement les unités supérieures ou égales à l'unité fondamentale, c'est-à-dire seulement les unités incluses dans l'ensemble suivant : $\{+(\varepsilon_d)^l \mid l \in \mathbb{N}\}$. Nous avons considéré encore une fois des intervalles de la forme $[2^k, 2^{k+1}[$ pour les mêmes valeurs de k que dans notre étude de la répartition des unités fondamentales (ces valeurs de k l'ont été pour les mêmes raisons). De plus, nous nous sommes contentés d'approximer le régulateur $\log(\varepsilon_d)$ par sa partie entière, c'est-à-dire par $\lfloor \log(\varepsilon_d) \rfloor$. Ainsi, nous nous intéressions à la quantité suivante :

$$A_k(N) := \# \left\{ d \in [2^k, 2^{k+1}[\text{ tel que } d = D \equiv 1 \bmod 4 \text{ soit un discriminant fondamental et tel que } \exists\, l \in \mathbb{N} \text{ avec } N = \lfloor \log(\varepsilon_d^l) \rfloor \right\}.$$

Pour raccourcir la notation, posons

$$\mathbb{D} := \{ D \equiv 1 \bmod 4 \mid D \text{ soit un discriminant fondamental} \}.$$

Nous nous intéressions entre autres à la répartition des unités des corps quadratiques réels et à cette quantité $A_k(N)$ en raison d'une hypothèse qui est la suivante :

Hypothèse 9.4.1 (Granville). $\#\{A < d < 2A \mid \exists\, u, v \in \mathbb{N} \text{ tels que } u^2 - dv^2 = \pm 1 \text{ ou } \pm 4 \text{ et tels que } x < u + v\sqrt{d} < ex\} \approx c \cdot \sqrt{A} \cdot (\log(\frac{x}{A}))^B$ *pour* $\sqrt{A} < x < e^{\sqrt{A}}$.

En posant $x = e^N$, on peut réécrire l'hypothèse de la façon suivante :

Hypothèse 9.4.2 (Granville). $\#\{A < d < 2A \mid \exists\, l \in \mathbb{N} \text{ avec } \lfloor \log((\varepsilon_d)^l) \rfloor = N\} \approx c \cdot \sqrt{A} \cdot (N - \log A)^B$ *pour* $\log \sqrt{A} < N < \sqrt{A}$.

Ainsi $A_k(N)$ ressemble à la situation dans cette hypothèse en considérant seulement toutefois lorsque $d \equiv 1 \bmod 4$ est un discriminant fondamental.

Remarquons tout d'abord que

$$\lfloor \log((\varepsilon_d)^l) \rfloor = N \quad \Leftrightarrow \quad N \leq \log((\varepsilon_d)^l) < N+1 \quad \Leftrightarrow \quad e^N \leq (\varepsilon_d)^l < e^{N+1}$$
$$\Leftrightarrow \qquad \frac{N}{l} \leq \log(\varepsilon_d) < \frac{N}{l} + \frac{1}{l} \, .$$

Pourrait-il y avoir deux l distincts tels que $e^N \leq (\varepsilon_d)^l < e^{N+1}$?
Supposons que oui. Alors on a $e^N \leq (\varepsilon_d)^{l_1} < e^{N+1}$ et $e^N \leq (\varepsilon_d)^{l_2} < e^{N+1}$.
Ici $l_1, l_2 \in \mathbb{Z}$. Supposons sans perdre de généralité (SPDG) que $l_1 < l_2$.
Alors $e^N \leq (\varepsilon_d)^{l_1} < (\varepsilon_d)^{l_1+1} \leq (\varepsilon_d)^{l_2} < e^{N+1}$. Aussi
$e^{N+1} > (\varepsilon_d)^{l_1+1} = (\varepsilon_d)^{l_1} \cdot \varepsilon_d \geq e^N \cdot \varepsilon_d \quad \Rightarrow \quad e^N \cdot \varepsilon_d < e^N \cdot e \quad \Rightarrow \quad \varepsilon_d < e$.
Or, $e > \varepsilon_d \geq \frac{1+\sqrt{d}}{2} \quad \Rightarrow \quad \frac{1+\sqrt{d}}{2} < e \quad \Rightarrow \quad \sqrt{d} < 2e-1 \quad \Rightarrow \quad d < 20$
$\therefore$ Pour $d \geq 20$, l est unique.

Ce résultat nous permet d'affirmer que lorsque $d \geq 20$,
$$\# \{ \, d \in [A, 2A[\cap \mathbb{D} \ : \ \exists \, l \text{ avec } \lfloor \log((\varepsilon_d)^l) \rfloor = N \}$$
$$= \sum_{l=1}^{+\infty} \# \left\{ \, d \in [A, 2A[\cap \mathbb{D} \ : \ \tfrac{N}{l} \leq \log(\varepsilon_d) < \tfrac{N}{l} + \tfrac{1}{l} \, \right\} .$$

Cette somme se calcule très bien, mais il faut que le régulateur soit très précis car plus l grossit, plus la précision des décimales du régulateur doit être grande. Mais à mesure que l'intervalle $[A, 2A[$ grandit, on joue avec de plus en plus de régulateurs et il devient plus facile techniquement (à cause des ressources informatiques dont nous disposons) de tronquer le régulateur à l'unité près et de ne retenir que le nombre n_1 de régulateurs dont la partie entière est p_1 , le nombre n_2 de régulateurs dont la partie entière est p_2 , ... , plutôt que de retenir n_1 régulateurs distincts presque tous égaux, n_2 régulateurs distincts presque tous

égaux, ...
C'est pourquoi il sera plus commode de modifier légèrement la dernière somme pour tenir compte de ce que nous venons de mentionner.

Plutôt que de regarder le nombre de régulateurs entre $\frac{N}{l}$ et $\frac{N}{l}+\frac{1}{l}$, on va regarder le nombre de régulateurs entre $\frac{N}{l}$ et $\frac{N}{l}+1$, un intervalle l fois plus grand. Nous émettrons l'hypothèse que les régulateurs sont, à l'échelle locale, uniformément distribués. Dans ce cas, il doit y avoir l fois moins de régulateurs dans un intervalle qui est l fois plus petit. Nous obtenons donc, sous cette hypothèse, que

$$\sum_{l=1}^{+\infty} \#\left\{ d \in [A,2A[\cap \mathbb{D} \ : \ \tfrac{N}{l} \le \log(\varepsilon_d) < \tfrac{N}{l}+\tfrac{1}{l} \right\}$$
$$\approx \sum_{l=1}^{+\infty} \tfrac{1}{l} \cdot \#\left\{ d \in [A,2A[\cap \mathbb{D} \ : \ \tfrac{N}{l} \le \log(\varepsilon_d) < \tfrac{N}{l}+1 \right\} .$$

Et puis toujours dans l'hypothèse que les régulateurs soient localement uniformément distribués, il sera plus commode de considérer les régulateurs entre $\left\lfloor \frac{N}{l} \right\rfloor$ et $\left\lfloor \frac{N}{l} \right\rfloor + 1$ plutôt qu'entre $\frac{N}{l}$ et $\frac{N}{l}+1$, car on peut alors tout simplement tronquer les décimales du régulateur. On aura alors l'approximation suivante :

$$\sum_{l=1}^{+\infty} \tfrac{1}{l} \cdot \#\left\{ d \in [A,2A[\cap \mathbb{D} \ : \ \tfrac{N}{l} \le \log(\varepsilon_d) < \tfrac{N}{l}+1 \right\}$$
$$\approx \sum_{l=1}^{+\infty} \tfrac{1}{l} \cdot \#\left\{ d \in [A,2A[\cap \mathbb{D} \ : \ \left\lfloor \tfrac{N}{l} \right\rfloor \le \log(\varepsilon_d) < \left\lfloor \tfrac{N}{l} \right\rfloor + 1 \right\}$$
$$= \sum_{l=1}^{+\infty} \tfrac{1}{l} \cdot \#\left\{ d \in [A,2A[\cap \mathbb{D} \ : \ \lfloor \log(\varepsilon_d) \rfloor = \left\lfloor \tfrac{N}{l} \right\rfloor \right\} .$$

Ainsi, on obtient que pour $d \ge 20$

$$\#\left\{ d \in [A,2A[\cap \mathbb{D} \ : \ \exists\, l \text{ avec } \lfloor \log((\varepsilon_d)^l) \rfloor = N \right\}$$
$$\approx \sum_{l=1}^{+\infty} \tfrac{1}{l} \cdot \#\left\{ d \in [A,2A[\cap \mathbb{D} \ : \ \lfloor \log(\varepsilon_d) \rfloor = \left\lfloor \tfrac{N}{l} \right\rfloor \right\}$$

et en particulier

$$A_k(N) := \#\left\{ d \in [2^k,2^{k+1}[\cap \mathbb{D} \ : \ \exists\, l \text{ avec } \lfloor \log((\varepsilon_d)^l) \rfloor = N \right\}$$
$$\approx \sum_{l=1}^{+\infty} \tfrac{1}{l} \cdot \#\left\{ d \in [2^k,2^{k+1}[\cap \mathbb{D} \ : \ \lfloor \log(\varepsilon_d) \rfloor = \left\lfloor \tfrac{N}{l} \right\rfloor \right\}$$

$$= \quad \sum_{l=1}^{+\infty} \frac{1}{l} \cdot B_k \left(\left\lfloor \frac{N}{l} \right\rfloor \right) \ .$$

L'égalité précédente nous permettra d'établir une correspondance avec la sous-section précédente sur la répartition des unités fondamentales. Cette correspondance nous permettra en fait d'utiliser les mêmes données et de faire des calculs similaires en ayant seulement recours aux données sur les unités fondamentales pour calculer la répartition des unités.

Maintenant, essayons d'obtenir une somme finie plutôt que cette dernière somme infinie.

Si $\quad l \geq N+1 \quad$ et si $\quad \left\lfloor \frac{N}{l} \right\rfloor = \lfloor \log(\varepsilon_d) \rfloor \ , \ $ alors $\quad 0 \leq \left\lfloor \frac{N}{l} \right\rfloor \leq \left\lfloor \frac{N}{N+1} \right\rfloor = 0$

$\Rightarrow \quad \left\lfloor \frac{N}{l} \right\rfloor = 0 \quad \Rightarrow \quad \lfloor \log(\varepsilon_d) \rfloor = 0 \quad \Rightarrow \quad 0 \leq \log(\varepsilon_d) < 1$

$\Rightarrow \quad 1 \leq \varepsilon_d < e \qquad$ et puisque $\quad \varepsilon_d \geq \frac{1+\sqrt{d}}{2}$

$\Rightarrow \quad \frac{1+\sqrt{d}}{2} < e \quad \Rightarrow \quad \sqrt{d} < 2e-1 \quad \Rightarrow \quad d < 20 \ .$

Et en fait le seul corps quadratique $\mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{D}$, $d < 20$ et avec $\varepsilon_d < e$ est $\mathbb{Q}(\sqrt{5})$. Ceci correspond à $k \leq 2$ dans $d \in [2^k, 2^{k+1}[$. Ainsi, on obtient l'égalité suivante $\forall\, k \geq 3$.

$$A_k(N) \quad \approx \quad \sum_{l=1}^{+\infty} \frac{1}{l} \cdot B_k \left(\left\lfloor \frac{N}{l} \right\rfloor \right) \quad = \quad \sum_{l=1}^{N} \frac{1}{l} \cdot B_k \left(\left\lfloor \frac{N}{l} \right\rfloor \right) \qquad \forall\, k \geq 3$$

Soit maintenant $\quad A_k^* := \max_N A_k(N) \ .$

Alors les six graphiques suivants représentent les couples (x, y) avec $x = \dfrac{N}{\sqrt{2^k}}$ et $y = \dfrac{A_k(N)}{A_k^*}$, pour $k = 15, 16, ..., 20$.

On a "normalisé" ici aussi les graphiques en divisant en abscisse par $\sqrt{2^k}$ et en ordonnée par A_k^* afin de pouvoir comparer sur des bases similaires les graphiques pour différentes valeurs de k .

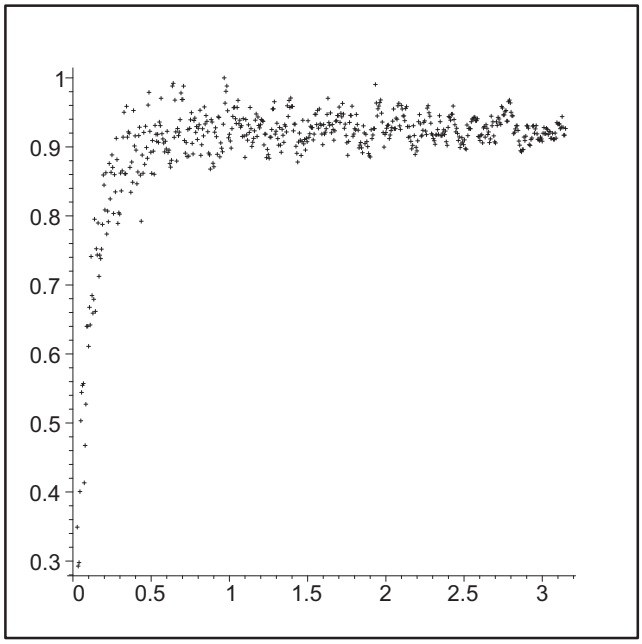

FIG. 9.35. Répartition des unités quadratiques pour $k = 15$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{15}}}\,,\,\frac{A_{15}(N)}{A^*_{15}}\right)$

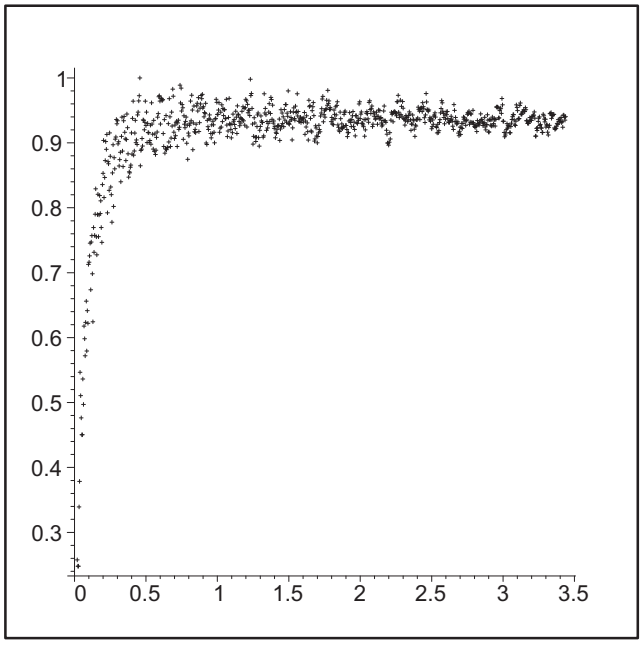

FIG. 9.36. Répartition des unités quadratiques pour $k = 16$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{16}}}\,,\,\frac{A_{16}(N)}{A^*_{16}}\right)$

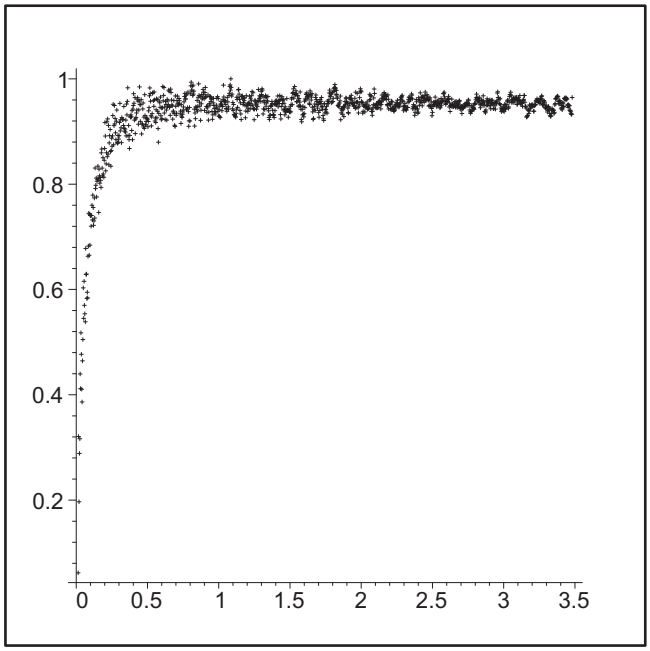

FIG. 9.37. Répartition des unités quadratiques pour $k = 17$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{17}}}, \frac{A_{17}(N)}{A^*_{17}}\right)$

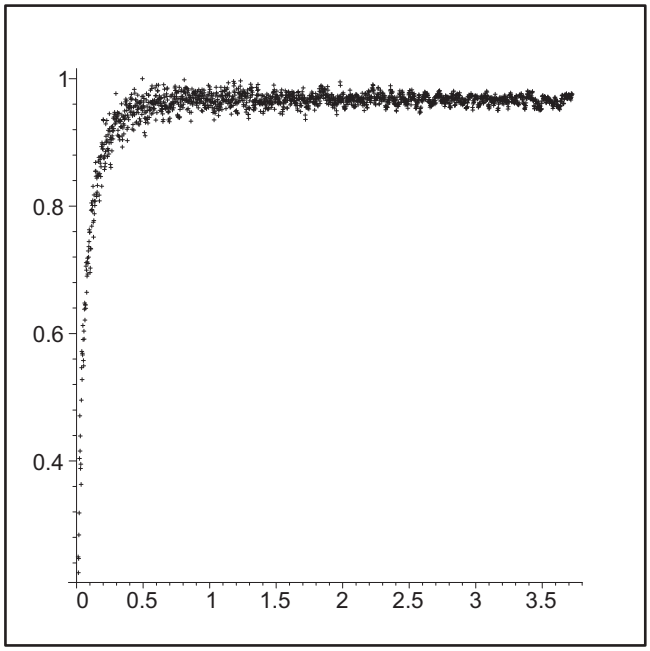

FIG. 9.38. Répartition des unités quadratiques pour $k = 18$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{18}}}, \frac{A_{18}(N)}{A^*_{18}}\right)$

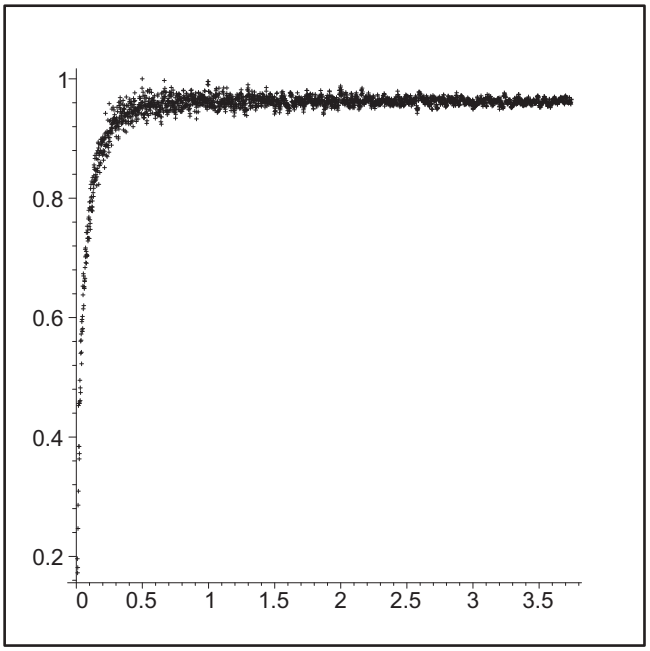

FIG. 9.39. Répartition des unités quadratiques pour $k = 19$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{19}}}\,,\,\frac{A_{19}(N)}{A^*_{19}}\right)$

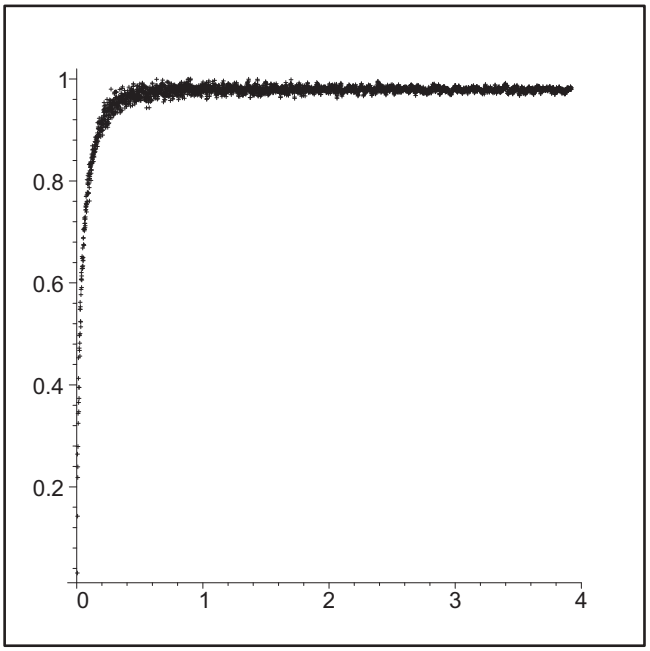

FIG. 9.40. Répartition des unités quadratiques pour $k = 20$, c'est-à-dire ensemble des couples $\left(\frac{N}{\sqrt{2^{20}}}\,,\,\frac{A_{20}(N)}{A^*_{20}}\right)$

Afin de vérifier si nos calculs respectent l'hypothèse (9.4.2), nous présentons aussi les mêmes six graphiques, mais non "normalisés" cette fois. C'est-à-dire qu'ils représentent les couples (x, y) avec $x = N$ et $y = A_k(N)$, pour $k = 15, 16, ..., 20$.

Dans chacun de ces graphiques, on mettra aussi une droite et une courbe. La courbe tente d'approximer le nuage de points avec une modélisation de type $y = -\frac{a}{x} + maxA_k$, où $maxA_k := \max_{\log(\sqrt{2^k})<N<\sqrt{2^k}} A_k(N)$.

Notons que les définitions de $maxA_k$ et de A_k^* sont semblables, mais $maxA_k$ considère les valeurs de N dans un plus petit intervalle, puisqu'en fait dans les graphiques "normalisés", nous avons regardé la situation pour N inférieur approximativement à $4\sqrt{2^k}$ donc A_k^* y considère des valeurs de $A_k(N)$ pour N inférieur à environ $4\sqrt{2^k}$.

La droite représente justement $y = maxA_k$, droite vers laquelle le nuage de points tend.

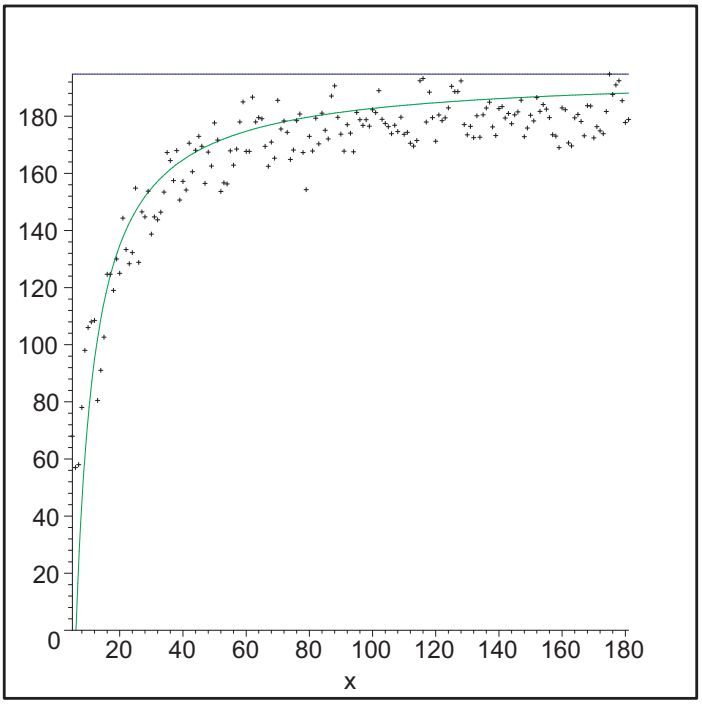

FIG. 9.41. Répartition des unités des corps quadratiques réels pour $k = 15$, c'est-à-dire ensemble des couples $(\, N\, ,\, A_{15}(N)\,)$

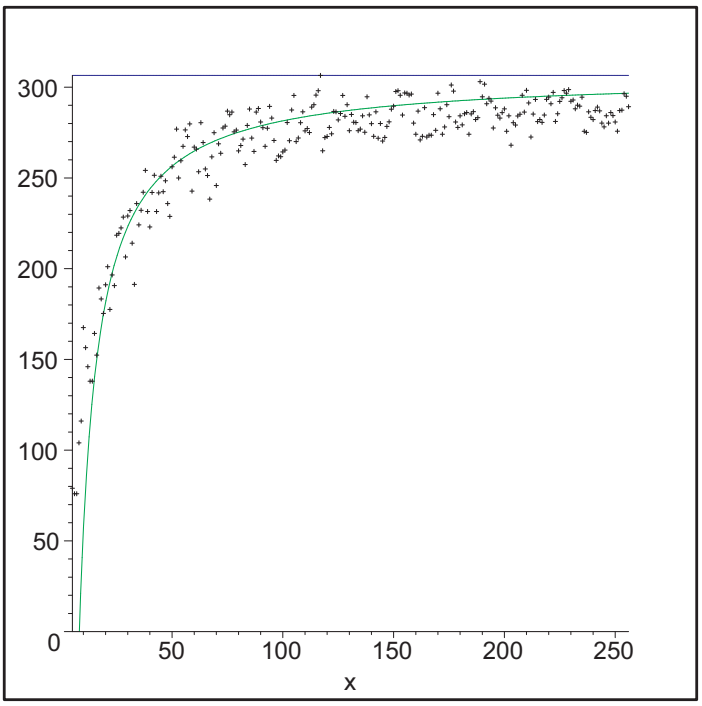

FIG. 9.42. Répartition des unités des corps quadratiques réels pour $k = 16$, c'est-à-dire ensemble des couples $(\, N\, ,\, A_{16}(N)\,)$

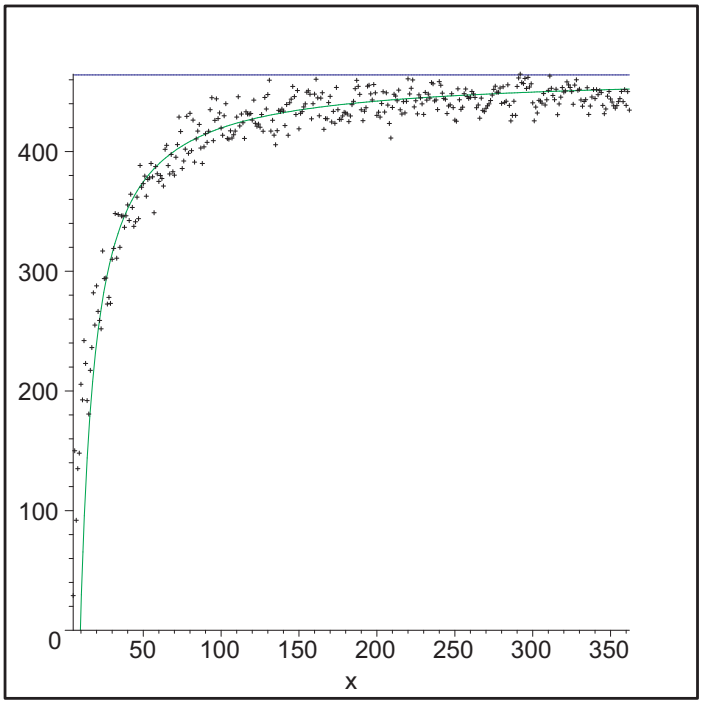

FIG. 9.43. Répartition des unités des corps quadratiques réels pour $k = 17$, c'est-à-dire ensemble des couples $(\ N\ ,\ A_{17}(N)\ )$

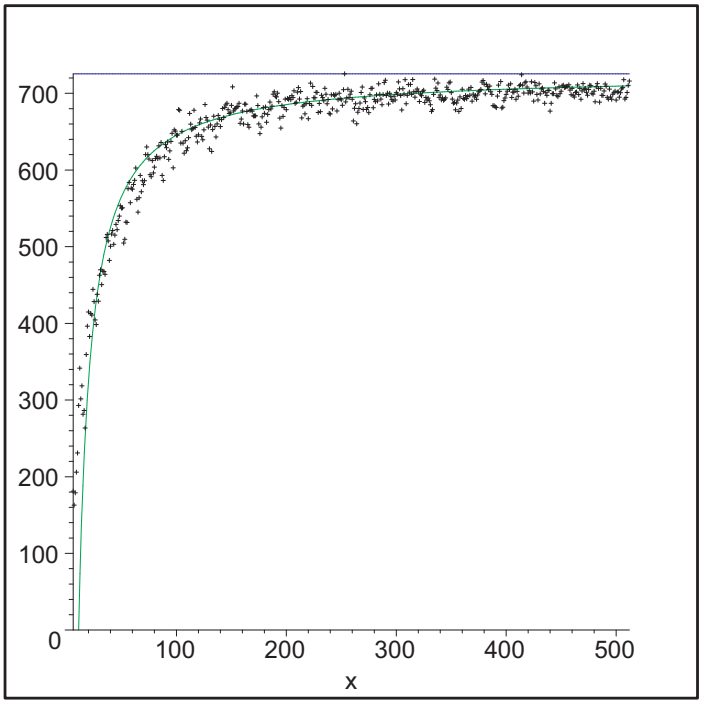

FIG. 9.44. Répartition des unités des corps quadratiques réels pour $k = 18$, c'est-à-dire ensemble des couples $(\ N\ ,\ A_{18}(N)\ )$

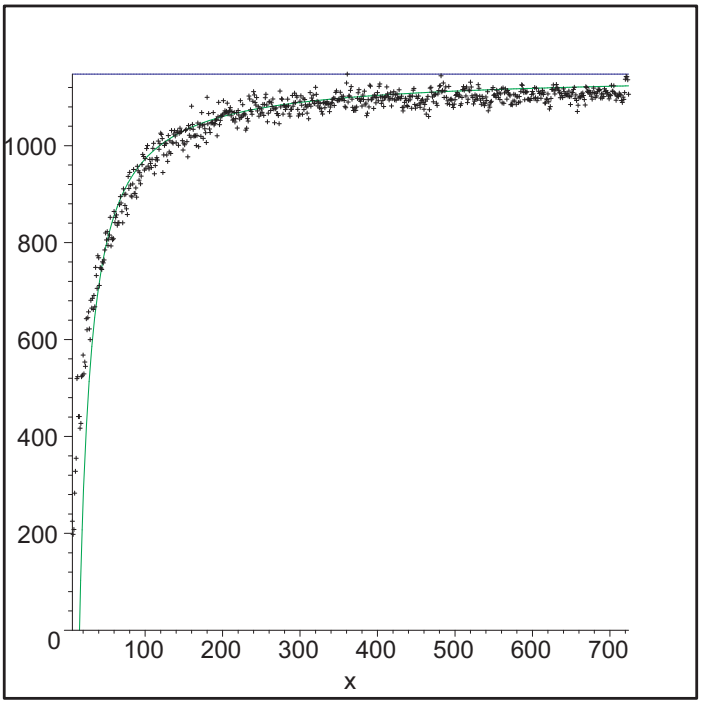

FIG. 9.45. Répartition des unités des corps quadratiques réels pour $k = 19$, c'est-à-dire ensemble des couples $(\, N\, ,\, A_{19}(N)\,)$

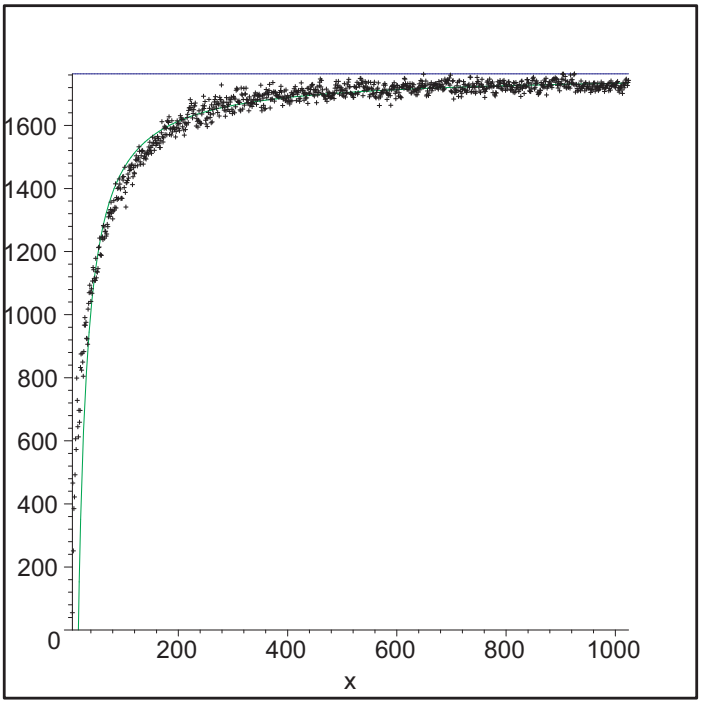

FIG. 9.46. Répartition des unités des corps quadratiques réels pour $k = 20$, c'est-à-dire ensemble des couples $(\, N\, ,\, A_{20}(N)\,)$

Dans ces graphiques, le nuage de points grimpe très rapidement avant de devenir constant.

Pour ce qui est des graphiques non "normalisés" (9.41 à 9.46), l'intervalle $\log(\sqrt{2^k}) < N < \sqrt{2^k}$ sur l'axe des abscisses correspond pratiquement à l'intervalle $0 < x < 1$ de l'axe des abscisses des graphiques (9.35 à 9.40) étant donné que $x = \dfrac{N}{\sqrt{2^k}}$.

Dans chacun de ces graphiques non "normalisés" justement (figures 9.41 à 9.46), on a approximé le nuage de points avec une modélisation de type $y = -\frac{a}{N} + maxA_k$ (courbe verte) , où N est la variable indépendante . On se souvient que d'après l'hypothèse (9.4.2), le nuage de points pourrait ressembler à $c\sqrt{A} \cdot (N - \log A)^B$. D'après la modélisation que nous avons faite, un paramètre B égal à -1 dans ceci semble être approprié. Notre modélisation n'est pas exactement sous la même forme que l'hypothèse, mais c'est semblable. On prendra $\frac{-a}{N} + maxA_k = \frac{c\sqrt{A}}{N} + maxA_k$. Cette modélisation a donné les paramètres 'a' suivants (et donc les constantes c suivantes que nous présenterons juste après) pour les différents graphiques :

k	=	15	16	17	18	19	20
a	=	1200	2500	4500	8000	17500	30000

.

Voici donc les constantes c et $maxA_k$ pour différentes valeurs de k , où c est calculée ainsi : $c := \dfrac{-a}{\sqrt{2^k}}$

k	=	15	16	17	18	19	20
c	=	-6.63	-9.77	-12.43	-15.63	-24.17	-29.30
$maxA_k$	=	195	306	465	725	1147	1763

.

9.4.3. Moments des régulateurs

Nous abordons ici enfin les moments dans notre étude du comportement des régulateurs. Tout comme Hooley et Dahl ont étudié le comportement moyen du nombre de classes et ses moments, nous calculerons nous aussi certains moments

des régulateurs des corps quadratiques réels. Nous nous intéresserons plus particulièrement à la quantité suivante, pour certaines valeurs de λ $(\lambda = 0, 1, 2, ..., 10)$.

$$S_\lambda(A) \quad := \quad \frac{1}{A^{\frac{\lambda}{2}+1}} \cdot \sum_{\substack{A \leq d < 2A \\ d \in \mathbb{D}}} \lfloor \log(\varepsilon_d) \rfloor^\lambda \quad = \quad \frac{1}{A} \cdot \sum_{\substack{A \leq d < 2A \\ d \in \mathbb{D}}} \left(\frac{\lfloor \log(\varepsilon_d) \rfloor}{\sqrt{A}} \right)^\lambda .$$

On remarque que A est la grandeur de l'intervalle $[A, 2A[$ alors le facteur $\frac{1}{A}$ a pour but d'étudier la moyenne de ce qui se retrouve à l'intérieur de la somme.

En fait, en statistique, les moments étudient différents caractères de dispersion d'une distribution. Le moment d'ordre 1 correspond à l'espérance, celui d'ordre 2 correspond à la variance, celui d'ordre 3 au coefficient d'asymétrie et le moment d'ordre 4 correspond au coefficient d'aplatissement. Ces moments sont les plus courants d'où le fait qu'ils soient connus sous un nom particulier.

Nous avons calculé $S_\lambda(A)$ pour $\lambda = 0, 1, 2, ..., 10$ et pour $A = 2^{13}, 2^{14}, ..., 2^{20}$. En fait, il est à-propos de mentionner qu'un algorithme que j'ai programmé pour calculer les régulateurs selon la théorie des fractions continues exposée dans les premiers chapitres de ce mémoire était raisonnablement rapide pour les données plus petites. Pour pouvoir faire les calculs dans les intervalles plus grands, j'ai plutôt eu la chance et le grand privilège d'utiliser un programme conçu par Herman te Riele qui est beaucoup plus complexe que mon programme mais qui est aussi plus efficace. Ce programme de te Riele était notamment fait pour calculer les régulateurs des corps quadratiques réels de discriminant $p \equiv 1 \bmod 4$, avec p un nombre premier. Mais il était d'abord et avant tout conçu afin de vérifier expérimentalement les heuristiques de Cohen-Lenstra (conjecture 8.7.1) et la conjecture de Hooley (conjecture 8.7.2) pour les nombres premiers $\equiv 1 \bmod 4$.

Grosso modo, la partie du programme de te Riele qui calcule le régulateur commence par calculer rapidement une estimation E de $h_i(d) \cdot \log(\varepsilon_d)$. On se souvient que la formule du nombre de classes de Dirichlet nous indique que $h_i(d) \cdot \log(\varepsilon_d) = \frac{\sqrt{D} \cdot L(1, \chi)}{2}$. Ainsi, l'estimation E est trouvée en estimant

$L(1,\chi)$ et en utilisant ensuite la formule du nombre de classes. Cette estimation E sert pour utiliser les idées de Shanks (section 9.5) qui permettent de parcourir beaucoup plus rapidement le développement en fraction continue. Le principe de l'algorithme de te Riele est de simplement trouver un multiple du régulateur (c'est-à-dire une unité pas nécessairement fondamentale) permettant ensuite d'obtenir le régulateur.

Bien sûr, comme le programme de te Riele fournissait les régulateurs pour les corps quadratiques de discriminant $p \equiv 1 \bmod 4$ et que nous voulions plutôt avoir les régulateurs pour les corps quadratiques de discriminant fondamental $\equiv 1 \bmod 4$, nous avons dû modifier le programme de te Riele pour qu'il nous fournisse tous les régulateurs désirés et pour qu'il effectue les calculs que nous souhaitions.

Mais revenons maintenant aux moments. Nous disions que nous avons calculé $S_\lambda(A)$ pour $\lambda = 0, 1, 2, ..., 10$ et pour $A = 2^{13}, 2^{14}, ..., 2^{20}$. Voici les résultats de ces calculs.

A $\downarrow$ $\diagdown$ $\lambda \rightarrow$	0	1	2	3
2^{13}	0.2027587891	0.1188028622	0.1284547001	0.1911993114
2^{14}	0.2023315430	0.1177363396	0.1304731332	0.2028535378
2^{15}	0.2025756836	0.1142481366	0.1257324768	0.1968931598
2^{16}	0.2027587891	0.1117205620	0.1240419266	0.1985998770
2^{17}	0.2026062012	0.1088668481	0.1211002933	0.1978153140
2^{18}	0.2026405334	0.1065749302	0.1189976961	0.1973431985
2^{19}	0.2026443481	0.1042779571	0.1161754003	0.1941173073
2^{20}	0.2026433945	0.1017062860	0.1127889157	0.1892554588

$A_{\downarrow} \diagdown \lambda_{\rightarrow}$	4	5	6	7
2^{13}	0.3369690043	0.6556622679	1.3605847340	2.9546729800
2^{14}	0.3775141127	0.7794104719	1.7190410010	3.9689637580
2^{15}	0.3730178906	0.7896789177	1.7942095220	4.2804388340
2^{16}	0.3877493418	0.8508763118	2.0134000110	5.0228912560
2^{17}	0.3978283137	0.9028849485	2.2122766460	5.7133619920
2^{18}	0.4054271527	0.9434418038	2.3761851360	6.3199748250
2^{19}	0.4040873528	0.9556686868	2.4500064480	6.6377328780
2^{20}	0.3975689476	0.9521894536	2.4792119440	6.8386063130

$A_{\downarrow} \diagdown \lambda_{\rightarrow}$	8	9	10
2^{13}	6.6387226270	15.3185239300	36.1118781800
2^{14}	9.4789033390	23.2393162200	58.1852415500
2^{15}	10.5858785600	26.9199879100	70.0103788400
2^{16}	13.0375484600	34.9160634400	95.9353484200
2^{17}	15.3351829700	42.4012217600	120.0478287000
2^{18}	17.4973831000	49.9714233900	146.3251871000
2^{19}	18.7259032100	54.5026142700	162.6509863000
2^{20}	19.6846035700	58.5688194500	178.9856016000

Ces colonnes de chiffres sont bien jolies, mais le fait de les représenter graphiquement est souvent fort utile pour bien les visualiser, pour dégager une tendance ou pour les modéliser. Nous avons donc fait des graphiques pour chaque moment, en fixant λ dans un graphique et en y faisant varier A. Nous vous présentons donc onze graphiques, pour chacun des $\lambda = 0, 1, 2, ..., 10$. Dans chacun de ces graphiques, nous modéliserons la courbe obtenue pour tenter de prédire ce vers quoi tend le moment par rapport aux intervalles étudiés.

Ce premier graphique représente $S_0(A) = S_0(2^k)$ pour $k = 13, 14, ..., 20$. Les points tendent vers la droite $y = \frac{2}{\pi^2} \approx 0.202642367$. C'est tout à fait conforme à ce que la théorie nous indique. En effet, $S_0(A) = \frac{1}{A} \cdot \sum_{\substack{A \leq d < 2A \\ d \in \mathbb{D}}} 1$. Rappelons que le corps quadratique $\mathbb{Q}(\sqrt{d})$ aura un discriminant fondamental si et seulement s'il est libre de carré impair. Il y a une proportion de $\frac{1}{p^2}$ des nombres naturels qui sont divisibles par p^2 et donc il y a une proportion de $1 - \frac{1}{p^2}$ des nombres qui ne sont pas divisibles par p^2. La proportion des nombres qui sont libres de carré impair est ainsi de $\prod_{p \geq 3} \left(1 - \frac{1}{p^2}\right)$ et la proportion des nombres qui sont des discriminants fondamentaux $\equiv 1 \bmod 4$ est de $\frac{1}{4} \cdot \prod_{p \geq 3} \left(1 - \frac{1}{p^2}\right)$. Comme l'étendue de l'intervalle $[A, 2A[$ est de A, il devrait y avoir $\frac{A}{4} \cdot \prod_{p \geq 3} \left(1 - \frac{1}{p^2}\right)$ nombres qui sont des discriminants fondamentaux $\equiv 1 \bmod 4$ entre A et $2A$. Ainsi,

$$\begin{aligned} S_0(A) &= \frac{1}{A} \cdot \sum_{\substack{A \leq d < 2A \\ d \in \mathbb{D}}} 1 = \frac{1}{A} \cdot \left(\frac{A}{4} \cdot \prod_{p \geq 3} \left(1 - \frac{1}{p^2}\right) \right) \\ &= \frac{1}{4} \cdot \frac{1 - \frac{1}{2^2}}{1 - \frac{1}{2^2}} \cdot \prod_{p \geq 3} \left(1 - \frac{1}{p^2}\right) = \frac{1}{4 \cdot \frac{3}{4}} \cdot \prod_{p \geq 2} \left(1 - \frac{1}{p^2}\right) = \frac{1}{3} \cdot \frac{1}{\zeta(2)} \\ &= \frac{1}{3} \cdot \frac{6}{\pi^2} = \frac{2}{\pi^2} \approx 0.202642367 . \end{aligned}$$

Les moments $S_0(A)$ tendent donc vers cette valeur, comme on peut le constater dans le graphique suivant.

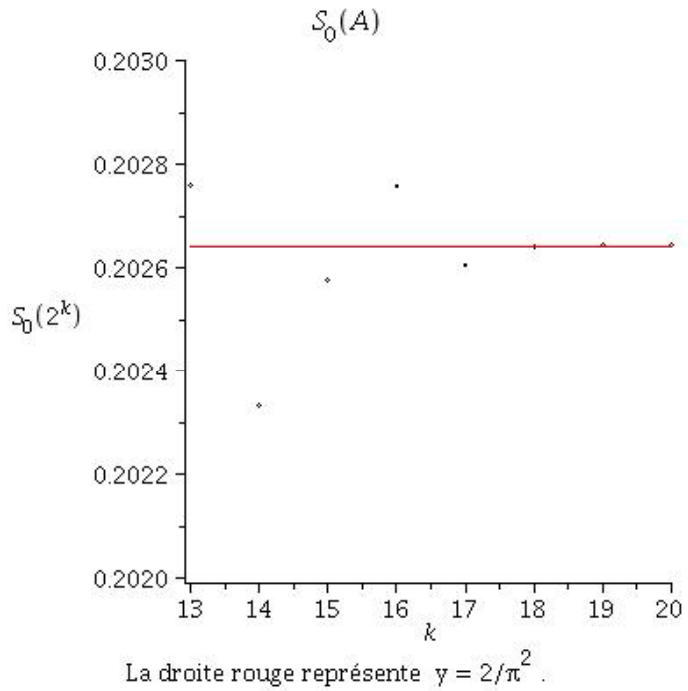

FIG. 9.47. 0^e Moments par rapport aux intervalles $[2^k, 2^{k+1}[$ pour $k = 13, 14, ..., 20$

Les dix prochains graphiques, pour $\lambda = 1, 2, ..., 10$, représentent chacun $S_\lambda(A) = S_\lambda(2^k)$, où dans chaque graphique k varie entre 13 et 20. Nous avons modélisé dans chacun de ces graphiques une courbe qui le représente bien.

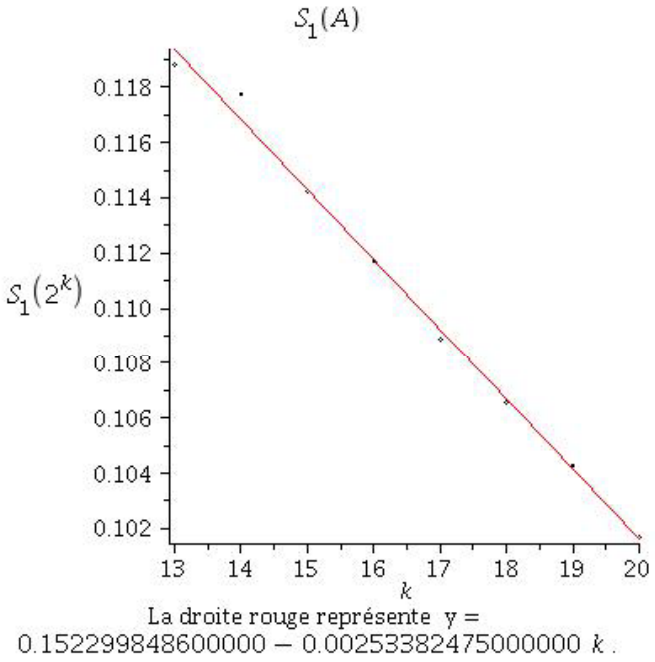

FIG. 9.48. 1^{er} Moments par rapport aux intervalles $[2^k, 2^{k+1}[$ pour $k = 13, 14, ..., 20$

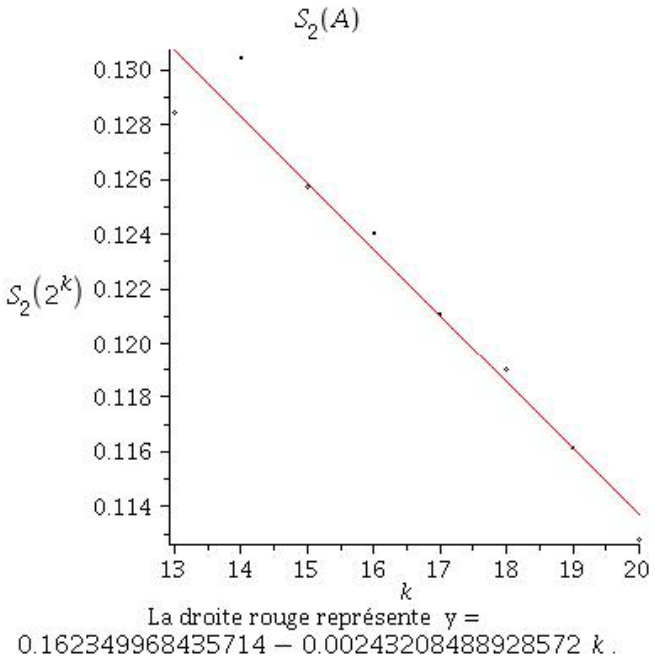

FIG. 9.49. 2^e Moments par rapport aux intervalles $[2^k, 2^{k+1}[$ pour $k = 13, 14, ..., 20$

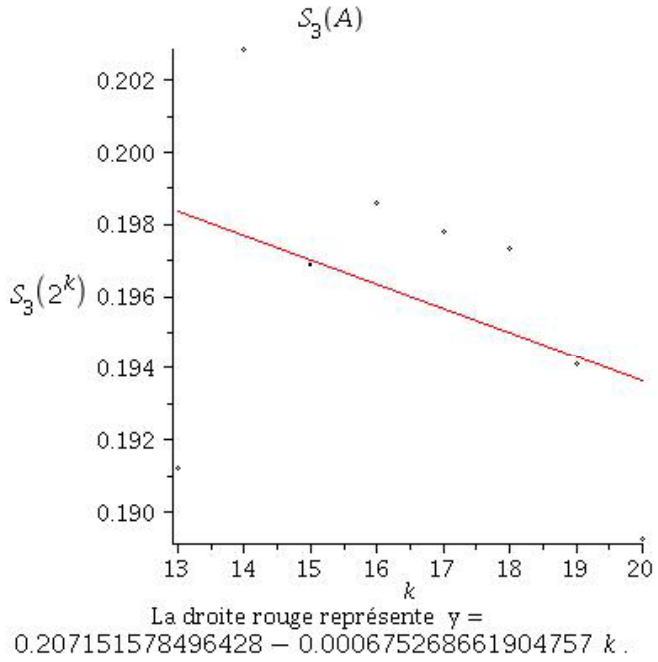

FIG. 9.50. 3^e Moments par rapport aux intervalles $[2^k, 2^{k+1}[$ pour $k = 13, 14, ..., 20$

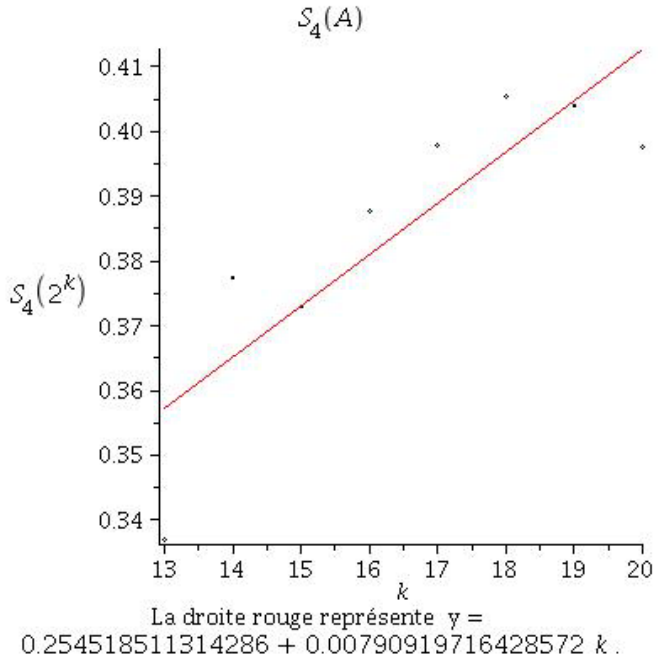

FIG. 9.51. 4^e Moments par rapport aux intervalles $[2^k, 2^{k+1}[$ pour $k = 13, 14, ..., 20$

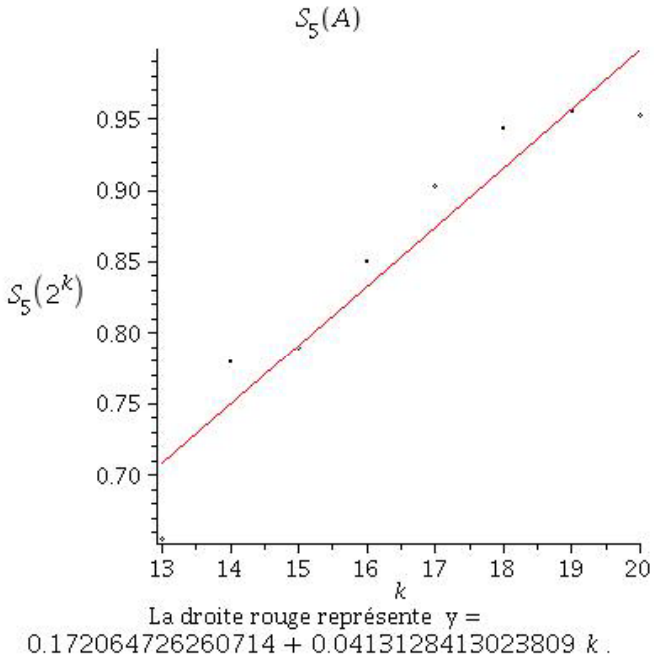

FIG. 9.52. 5^e Moments par rapport aux intervalles $[2^k, 2^{k+1}[$ pour $k = 13, 14, ..., 20$

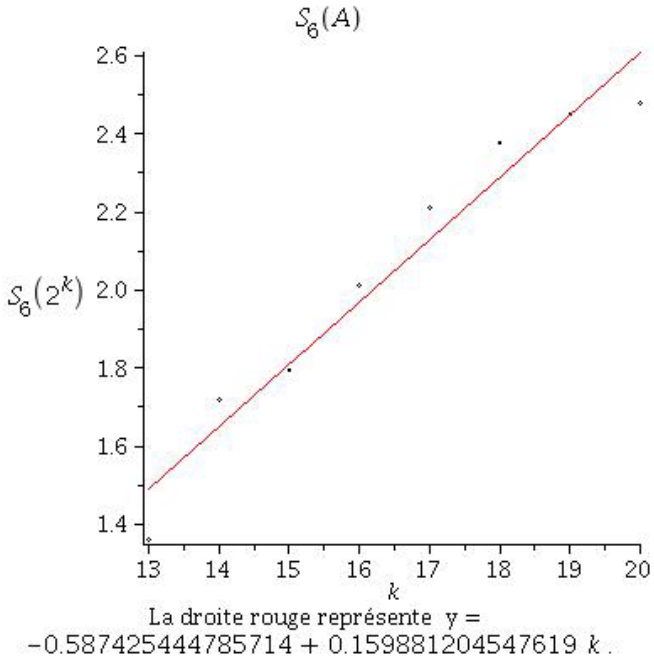

FIG. 9.53. 6^e Moments par rapport aux intervalles $[2^k, 2^{k+1}[$ pour $k = 13, 14, ..., 20$

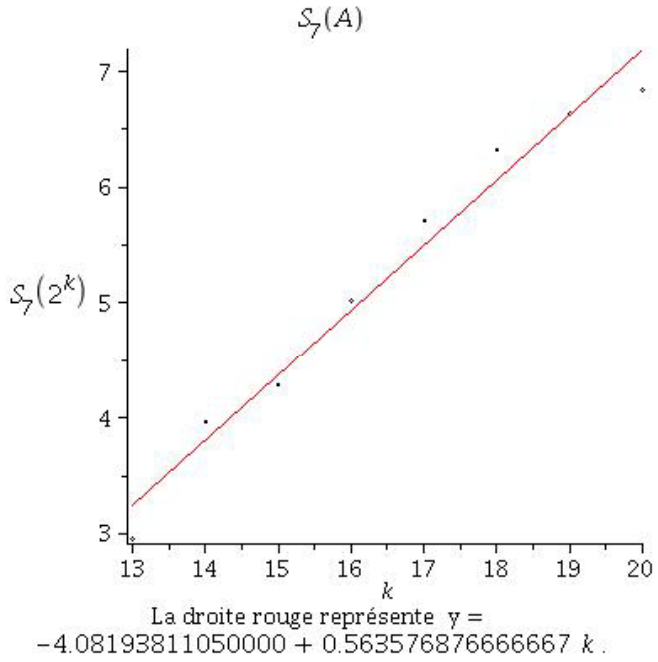

FIG. 9.54. 7^e Moments par rapport aux intervalles $[2^k, 2^{k+1}[$ pour $k = 13, 14, ..., 20$

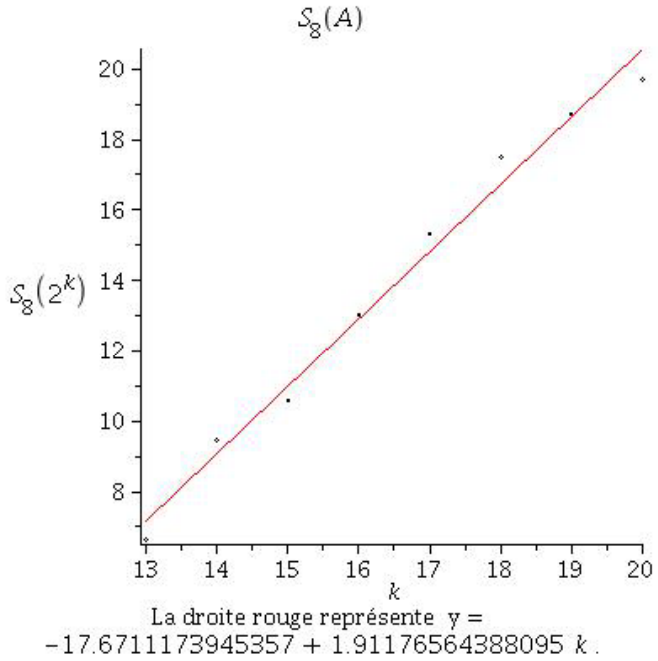

FIG. 9.55. 8^e Moments par rapport aux intervalles $[2^k, 2^{k+1}[$ pour $k = 13, 14, ..., 20$

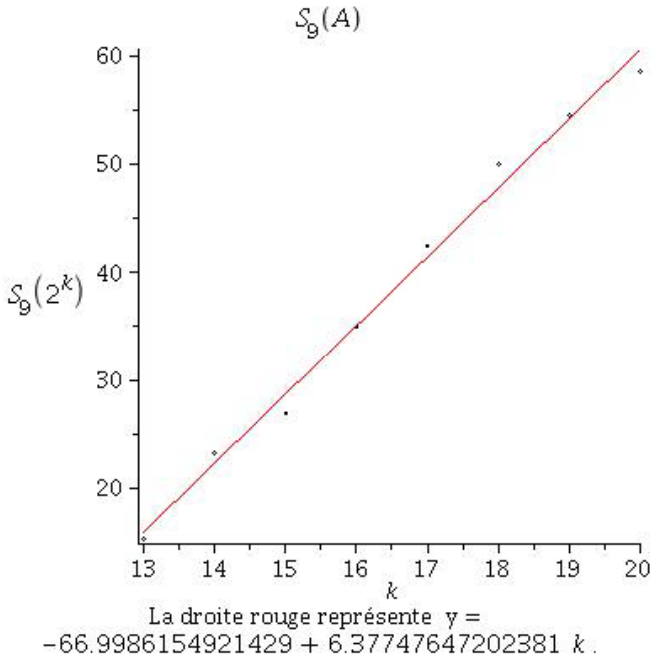

FIG. 9.56. 9^e Moments par rapport aux intervalles $[2^k, 2^{k+1}[$ pour $k = 13, 14, ..., 20$

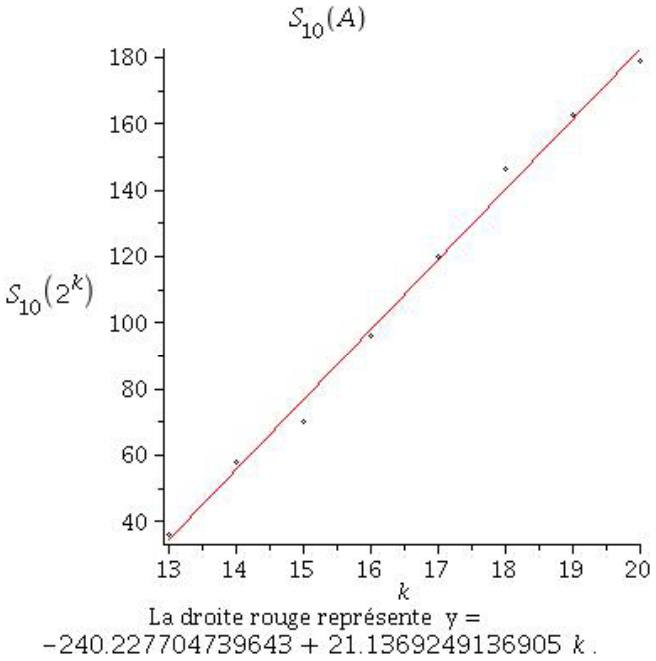

FIG. 9.57. 10^e Moments par rapport aux intervalles $[2^k, 2^{k+1}[$ pour $k = 13, 14, ..., 20$

Dans les graphiques précédents, la courbe qui modélise le mieux est souvent de la forme $f(k) = a + b \cdot k$ avec a et b qui sont ici des constantes.

On peut pousser plus loin la réflexion en essayant d'additionner les $S_\lambda\left(2^k\right)$ pour λ fixé. Comme on a alors $f(k) = S_\lambda\left(2^k\right) = a + b \cdot k$, les sommer donnera une série arithmétique.

$$\begin{aligned}
\sum_{k=k_1}^{k_2} S_\lambda\left(2^k\right) &= \sum_{k=k_1}^{k_2} (a + b \cdot k) = \sum_{k=k_1}^{k_2} a \; + \; b \cdot \sum_{k=k_1}^{k_2} k \\
&= a(k_2 - k_1 + 1) \; + \; b \cdot \sum_{i=1}^{k_2-k_1+1} (k_1 - 1 + i) \\
&= a(k_2 - k_1 + 1) \; + \; b \cdot \sum_{i=1}^{k_2-k_1+1} (k_1 - 1) \quad + \quad b \cdot \sum_{i=1}^{k_2-k_1+1} i \\
&= a(k_2 - k_1 + 1) \; + \; b \cdot (k_2 - k_1 + 1) \cdot (k_1 - 1) \\
&\qquad + \quad b \cdot \frac{(k_2 - k_1 + 1) \cdot (k_2 - k_1 + 2)}{2} \; .
\end{aligned}$$

C'est, en fonction de k_2 , un polynôme de degré 2.

9.5. Algorithmes de calcul du régulateur

Il y a essentiellement cinq méthodes pour calculer l'unité fondamentale $\varepsilon_d = \frac{u+v\sqrt{d}}{2}$ d'un corps quadratique $\mathbb{Q}(\sqrt{d})$. Ces méthodes ont des temps de calcul différents mais aussi conséquemment des niveaux de difficulté correspondants.

La première méthode, dite naïve, consiste à essayer $v = 1, 2, ...$ jusqu'à ce que $dv^2 \pm 4$ soit un carré parfait pour avoir $u^2 - dv^2 = \pm 4$. Cette méthode fonctionnera, mais est hautement inefficace. Son temps de calcul est de l'ordre de $O\left(e^{\sqrt{D}}\right)$.

La seconde méthode utilise les fractions continues et est conforme aux procédés et théorèmes que nous avons décrits. Son temps de calcul est de l'ordre de

$O\left(D^{\frac{1}{2}+\varepsilon}\right)$. Le problème qui survient toutefois avec cet algorithme est que les coefficients u et v de l'unité fondamentale sont déraisonnablement grands. Comme l'intérêt est de connaître le régulateur (ou même une estimation du régulateur) davantage que l'unité fondamentale, Henri Cohen propose dans [**C**] une formule pour calculer le régulateur sans avoir besoin de calculer d'abord l'unité fondamentale. Cette formule de Cohen n'améliore pas le nombre d'opérations effectuées par l'algorithme, mais améliore grandement son temps d'exécution, puisque les calculs peuvent être faits approximativement en utilisant une précision raisonnable, évitant d'obtenir des valeurs de u et v trop élevées.

La troisième méthode est une amélioration notable de l'algorithme sur les fractions continues (la deuxième méthode) et est due à D. Shanks. Il utilise pour ce faire une combinaison de deux idées personnelles. Sa première idée est un algorithme appelé "pas de bébé - pas de géant" qui, grâce à certaines constatations qu'il a faites, permet maintenant de parcourir le développement en fraction continue en faisant des grands sauts. Sa seconde idée concerne des remarques qu'il a faites sur l'infrastructure d'un cycle d'une fraction continue. Le temps de calcul de cette méthode de Shanks est de l'ordre de $O\left(D^{\frac{1}{4}+\varepsilon}\right)$.

L'algorithme de te Riele (basé sur les idées de Shanks) que nous avons utilisé aurait quant à lui un temps de calcul de l'ordre de $O\left(D^{\frac{1}{5}+\varepsilon}\right)$.

La quatrième méthode est une combinaison de la troisième méthode, due à Shanks, avec une méthode provenant de la théorie de la factorisation (l'utilisation de bases de facteurs) introduite par J. Buchmann. Il semblerait en pratique que le temps de calcul de cette quatrième méthode serait sous-exponentielle et serait de l'ordre de $O\left(e^{c\cdot\sqrt{\log D\cdot\log(\log D)}}\right)$, où $c > 0$ est une petite constante. La véracité de cette quatrième méthode dépendrait toutefois du fait que l'Hypothèse de Riemann Généralisée (HRG) soit vraie. Par contre, une variante plus lente ne reposant pas sur HRG aurait été trouvée et aurait un temps de calcul de l'ordre

de $O\big(D^{\frac{1}{6}+\varepsilon}\big)$.

La cinquième méthode [**F**], plus récente, donne un algorithme ayant un temps de calcul polynomial(!). Cet algorithme de Hallgren se base sur une technique pour trouver la période d'une transformée de Fourier quantique.

9.6. Applications des corps quadratiques et des formes binaires quadratiques

Les travaux de Gauss sur les formes binaires quadratiques ont engendré de fertiles développements en théorie des nombres. Mentionnons par exemple le problème du nombre de classes de Gauss pour les corps quadratiques imaginaires. Ce problème consiste à fournir pour chaque $n \in \mathbb{N}$ une liste exhaustive de corps quadratiques imaginaires ayant un nombre de classes égal à n . Pour $n = 1$, le problème a été résolu indépendamment et par des méthodes différentes par Baker et Stark, en 1966. La méthode de Baker reposait sur la théorie de la transcendance (théorie qui s'est développée notamment sur les bases du VII^e des vingt-trois problèmes d'Hilbert et grâce aux contributions de Gelfond et Schneider). La méthode de Stark, quant à elle, repose sur l'étude des fonctions modulaires elliptiques. Stark a en fait clarifié les travaux de Kurt Heegner (qui ne furent pas acceptés initialement) utilisant les formes et les équations modulaires. Par la suite, le cas $n = 2$ fut abordé en application des travaux d'Alan Baker. Pour le cas général, il fallut attendre la découverte par Dorian Goldfeld que le problème du nombre de classes soit relié aux fonctions-L des courbes elliptiques. Ceci constitue le problème du nombre de classes de Gauss pour les corps quadratiques imaginaires. En ce qui concerne les corps quadratiques réels, le même problème de fournir pour chaque $n \in \mathbb{N}$ une liste exhaustive de corps quadratiques réels ayant un nombre de classes égal à n est toujours irrésolu et est beaucoup moins connu. Comme nous l'avons déjà mentionné, dans le cas des corps quadratiques réels, il y a le régulateur qui entre en cause dans la formule du nombre de classes de Dirichlet et il est difficile à contrôler. D'où un intérêt à tenter de comprendre davantage

comment se comporte le régulateur.

Par ailleurs, les travaux de Kummer sur les facteurs d'idéaux et sur le Dernier Théorème de Fermat qu'il a prouvé pour certains exposants, dits des nombres premiers réguliers, auraient été facilités par les travaux de Dirichlet et par sa formule du nombre de classes. En effet, Kummer aurait souligné que le développement rapide de sa propre formule du nombre de classes pour les corps cyclotomiques et que ses découvertes sur les relations entre le Dernier Théorème de Fermat pour un exposant p et les nombres de Bernouilli modulo p ont été rendus possibles entre autres par les trouvailles de Dirichlet et notamment par sa formule du nombre de classes dans le cas quadratique.

Ces relations ont poussé Kummer à entâmer l'étude approfondie de certaines fonctions-L et de nombres de classes, ce qui deviendra un sujet central dans la théorie des nombres algébriques moderne et qui réapparaîtra également (sous un jour différent) au coeur de la stratégie de Wiles pour prouver la conjecture de Taniyama-Shimura. [**Dar**]

Kummer était conscient que ses travaux sur la théorie des idéaux étaient intimement liés à la théorie de Gauss sur les formes binaires quadratiques. Ainsi, bien que Kummer avait pour objectif en développant sa théorie des idéaux de tenter de résoudre le Dernier Théorème de Fermat, ce n'était pas son seul objectif. Il aurait même affirmé que ce n'était pas son objectif le plus immédiat. Il y avait parmi ses autres buts la recherche de généralisations des lois de réciprocité quadratique, cubique et biquadratique à des puissances plus élevées ainsi que l'explication de la théorie de Gauss sur la composition des formes.

Suite à Gauss, l'étude des formes binaires quadratiques s'est généralisée vers la théorie des nombres algébriques et vers l'étude des formes quadratiques en plusieurs variables. Parmi les pionniers de ces domaines se retrouvent Jacobi, Dirichlet, Eisenstein, Hermite, H.J.S. Smith, H. Minkowski et C.L. Siegel. La

théorie est toujours active de nos jours et est reliée à des théories algébriques comme par exemple la théorie des sous-groupes arithmétiques des groupes de Lie ainsi qu'à des théories analytiques telles que la théorie des fonctions modulaires. La géométrie des nombres origine elle aussi de l'étude des formes quadratiques. Plus précisément, elle provient du problème de minimiser les valeurs d'une forme quadratique dont les variables sont à valeurs entières. Minkowski participa à la création de la géométrie des nombres en essayant de résoudre des inégalités faisant intervenir des formes quadratiques. La géométrie des nombres repose essentiellement sur l'utilisation de notions géométriques, comme la connexité et les réseaux, pour résoudre des problèmes de théorie des nombres tels que la solution d'inégalités en entiers.

En ce qui concerne les développements récents dans l'étude des corps quadratiques réels, on peut lire dans [**Gr**] des liens entre le symbole de Kronecker, le discriminant fondamental et certains nombres premiers, dits inertes, des corps quadratiques réels.

On peut aussi lire dans [**Dar2**] et dans [**Dar3**] des liens qui unissent les corps quadratiques et l'équation de Pell avec l'étude des points rationnels sur les courbes elliptiques.

Toujours pour rester dans le sujet des courbes elliptiques, la conjoncture de Birch et Swinnerton-Dyer, qui prédit un lien entre la fonction-L et le rang d'une courbe elliptique, serait une extension de la formule du nombre de classes de Dirichlet reliée à des équations diophantiennes du type $X^3 + Y^3 = DZ^3$.

Par ailleurs, les corps quadratiques ont aussi des applications en cryptographie [**Bu**]. La cryptographie utilisant les corps quadratiques imaginaires est prête à être utilisée. Par contre, la cryptographie utilisant les corps quadratiques réels n'est pas encore assez efficace pour être utilisée en pratique. Pour améliorer la sécurité, certains suggèrent l'utilisation de discriminants de formes particulières, puisque dans ces cas les algorithmes actuels les plus rapides pour calculer le régulateur

sont considérablement plus lents que la moyenne. Mais il reste encore plusieurs problèmes ouverts dans ce domaine.

Références spécifiques à ce chapitre :

Johannes Buchmann, *Binary quadratic forms : an algorithmic approach*, Springer, 2007.

Henri Cohen, *A course in computational algebraic number theory*, Springer-Verlag, 1993.

Henri Cohen, *Calcul du nombre de classes d'un corps quadratique imaginaire ou réel, d'après Shanks, Williams, McCurley, A.K. Lenstra et Schnorr*, Journal de Théorie des Nombres de Bordeaux, tome 1, Numéro 1, 1989, pages 117-135.

Alexander O. Dahl, *On moments of class numbers of real quadratic fields*, Thesis, University of Toronto, 2010.

Henri Darmon, *Stark-Heegner points over real quadratic fields*, Number theory (Tiruchirapalli, 1996) Contemporary Mathematics 210, AMS, Providence, RI, 1998, pages 41-69.

Henri Darmon, Fred Diamond et Richard Taylor, *Fermat's Last Theorem*, Current Developments in Mathematics 1, 1995, International Press, pages 1-157.

Henri Darmon et Peter Green, *Elliptic curves and class fields of real quadratic fields : algorithms and evidence*, Experimental Mathematics, 11 :1, 2002, pages 37-55.

Harold Davenport et Hans Heilbronn, *On the density of discriminants of cubic fields II*, Proc. Roy. Soc. Lond. A, Volume 322, 1971, pages 405-420.

Steven Finch, *Class number theory*, http ://algo.inria.fr/csolve/clss.pdf, 2005, 23 pages.

Andrew Granville, R.A. Mollin et H.C. Williams, *An upper bound on the least inert prime in a real quadratic field*, Canadian Journal of Mathematics, Volume 52 (2), 2000, pages 369-380.

Taira Honda, *Isogenies, rational points and section points of group varieties*, Japan J. Math., Numéro 30, 1960, pages 84-101.

Taira Honda, *On real quadratic fields whose class numbers are multiples of 3*, J. Reine Angew., Numéro 233, 1968, pages 101-102.

Michael J. Jacobson Jr., Richard F. Lukes et Hugh C. Williams, *An investigation of bounds for the regulator of quadratic fields*, Experimental Mathematics, Volume 4, Numéro 3, 1995.

Lillian Beatrix Pierce, *The 3-part of class numbers of quadratic fields*, Master of science, Oxford University, Trinity 2004.

Peter Weinberger, *Real quadratic fields with class numbers divisible by n*, J. Number Theory, Volume 5, 1973, pages 237-241.

Yoshihiko Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math., Volume 7, Numéro 1, 1970, pages 57-76.

BIBLIOGRAPHIE

[B] Alan Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, 1984.

[Bu] Johannes Buchmann, *Binary quadratic forms : an algorithmic approach*, Springer, 2007.

[Bue] Duncan A. Buell, *Binary quadratic forms : classical theory and modern computations*, Springer-Verlag, 1989.

[C] Henri Cohen, *Calcul du nombre de classes d'un corps quadratique imaginaire ou réel, d'après Shanks, Williams, McCurley, A.K. Lenstra et Schnorr*, Journal de Théorie des Nombres de Bordeaux, tome 1, Numéro 1, 1989, pages 117-135.

[C1] Henri Cohen, *A course in computational algebraic number theory*, Springer-Verlag, 1993.

[C2] Henri Cohen, *Number theory Volume I : Tools and diophantine equations*, Springer, 2007.

[Dahl] Alexander O. Dahl, *On moments of class numbers of real quadratic fields*, Thesis, University of Toronto, 2010.

[Dar] Henri Darmon, Fred Diamond et Richard Taylor, *Fermat's Last Theorem*, Current Developments in Mathematics 1, 1995, International Press, pages 1-157.

[Dar2] Henri Darmon, *Stark-Heegner points over real quadratic fields*, Number theory (Tiruchirapalli, 1996) Contemporary Mathematics 210, AMS, Providence, RI, 1998, pages 41-69.

[Dar3] Henri Darmon et Peter Green , *Elliptic curves and class fields of real quadratic fields : algorithms and evidence*, Experimental Mathematics, 11 :1, 2002, pages 37-55.

[Dav1] Harold Davenport, *Multiplicative number theory, 3e édition*, Springer, 2000.

[Dav2] Harold Davenport et Hans Heilbronn, *On the density of discriminants of cubic fields II*, Proc. Roy. Soc. Lond. A, Volume 322, 1971, pages 405-420.

[D] Jean-Marie De Koninck et Armel Mercier, *Introduction à la théorie des nombres*, Modulo, 1994.

[Di] Pierre Gustave Lejeune-Dirichlet, *Lectures on number theory*, American Mathematical Society, 1999.

[E] Harold M. Edwards, *Fermat's last theorem : a genetic introduction to algebraic number theory*, Springer-Verlag, 1977.

[F] Steven Finch, *Class number theory*, http ://algo.inria.fr/csolve/clss.pdf, 2005, 23 pages.

[Go] Dorian Goldfeld, *Gauss' class number problem for imaginary quadratic fields*, Bulletin of the American Mathematical Society, Volume 13, 1985, pages 23-37.

[G] Jay R. Goldman, *The queen of mathematics : an historical motivated guide to number theory*, A.K. Peters, 1998.

[Gr] Andrew Granville, R.A. Mollin et H.C. Williams, *An upper bound on the least inert prime in a real quadratic field*, Canadian Journal of Mathematics, Volume 52 (2), 2000, pages 369-380.

[GrS] Andrew Granville et Kannan Soundararajan, *The distribution of values of $L(1, \chi_d)$*, Geometric And Functional Analysis, Volume 13, Numéro 5, 2003, pages 992-1028.

[H] R. de Haan, M.J. Jacobson Jr. et H.C. Williams, *A fast, rigorous technique for computing the regulator of a real quadratic field*, Mathematics of computation, Volume 76, Numéro 260, Octobre 2007, pages 2139-2160.

[Ho] Taira Honda, *On real quadratic fields whose class numbers are multiples of 3*, J. Reine Angew., Numéro 233, 1968, pages 101-102.

[Ho2] Taira Honda, *Isogenies, rational points and section points of group varieties*, Japan J. Math., Numéro 30, 1960, pages 84-101.

[Hu] L.K. Hua, *On the least solution of Pell's equation*, Bulletin of the American Mathematical Society, Volume 48, 1942, pages 731-735.

[Hu1] Loo Keng Hua, *Introduction to number theory*, Springer-Verlag, 1982.

[Jo] Burton W. Jones, *The arithmetic theory of quadratic forms*, Mathematical Association of America : Wiley, 1950.

[Ka] Victor J. Katz, *A history of mathematics, an introduction, 3rd edition*, Pearson, 2009.

[K] Helmut Koch, *Number theory : algebraic numbers and functions*, American Mathematical Society, 2000.

[L] Michael J. Jacobson Jr., Richard F. Lukes et Hugh C. Williams, *An investigation of bounds for the regulator of quadratic fields*, Experimental Mathematics, Volume 4, Numéro 3, 1995.

[M] Michael Metcalf, John Reid et Malcolm Cohen, *Fortran 95/2003 explained*, Oxford University Press, 2005.

[Mu] M. Ram Murty et Jody Esmonde, *Problems in algebraic number theory*, Springer, 1999.

[N] Ivan Niven, Herbert S. Zuckerman et Hugh L. Montgomery, *An introduction to the theory of numbers, Fifth edition*, Jon Wiley & Sons, 1991.

[P] Lillian Beatrix Pierce, *The 3-part of class numbers of quadratic fields*, Master of science, Oxford University, Trinity 2004.

[R] Herman te Riele et Hugh Williams, *New computations concerning the Cohen-Lenstra heuristics*, Stichting Centrum voor Wiskunde en Informatica, 2001, pages 1-20.

[S] Harold M. Stark, *An introduction to number theory*, Markham Pub. Co., 1970.

[W] Peter Weinberger, *Real quadratic fields with class numbers divisible by n*, J. Number Theory, Volume 5, 1973, pages 237-241.

[Ya] Yoshihiko Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math., Volume 7, Numéro 1, 1970, pages 57-76.

[Y] Hideo Yokoi, *Units and class numbers of real quadratic fields*, Nagoya Mathematical Journal, Volume 37, 1970, pages 61-65.