Comptage d'objets arithmétiques

Tianyi Bai Max Dupré La Tour Léonard Pille-Schneider

5 juillet 2016

Table des matières

I Préliminaires **4**

1 Théorie algébrique des nombres **4**
1.1 Anneau des entiers d'un corps de nombres 4
1.2 Normes, traces, conjugués 5
1.3 Discriminant d'un corps de nombres 8
1.4 Factorisation dans $\mathcal{O}_K$ 10
1.5 Groupe des classes d'idéaux 13

2 Classes d'idéaux et formes quadratiques **14**
2.1 Généralités sur les formes 14
2.2 Liens avec les classes d'idéaux 18

3 Formule analytique du nombre de classes de Dirichlet **20**
3.1 Caractères de Dirichlet 21
3.2 Le symbole de Jacobi-Kronecker 24
3.3 Formule du nombre de classes 24
3.4 Fonction ζ d'un corps quadratique imaginaire 25
3.5 Factorisation de ζ_K 27

II Corps quadratiques et leurs groupes de classes **27**

4 Théorème de Siegel sur les fonctions L **28**

5 Théorème de Siegel pour les formes quadratiques **33**
5.1 Preuve analytique 33
5.2 Preuve géométrique 36

III Corps cubiques **46**

6 Théorème de Davenport-Heilbronn **46**
6.1 Correspondance de Delone-Faddeev 47
6.2 Estimations globales 49
6.3 Correspondance de Davenport-Heilbronn 55
6.4 Comportement local, densité en p 57
6.5 Passage à la limite 59

Introduction

Un *corps de nombres* K est une extension de degré fini de $\mathbf{Q}$. On peut lui associer un invariant très intéressant, son *discriminant* D_K, qui est un nombre entier. A n et X, Y fixés, il n'existe à isomorphisme près qu'un nombre fini $N(n, X, Y)$ de corps de nombres K de degré n et de discriminant $Y \leq D_K \leq X$. On peut alors chercher à obtenir des formules pour $N(n, X, Y)$, ou moins des formules asymptotiques pour $X, Y \longrightarrow \pm\infty$.
L'objet de cet exposé est l'étude des comportements asymptotiques de $N(n, 0, X)$ et $N(n, -X, 0)$ pour $X \longrightarrow +\infty$, ainsi que d'autres quantités arithmétiques significatives, dans les cas $n = 2$ (corps *quadratiques*) et $n = 3$ (corps *cubiques*).

En fait, nous allons voir assez rapidement qu'il est facile d'exprimer les quantités $N(2, 0, X)$ et $N(2, -X, 0)$; on dispose en effet d'une paramétrisation très simple des corps quadratiques par leurs discriminants. Nous allons alors leur associer leurs *groupes de classes d'idéaux*, qui sont des groupes finis définis dans la section 1, et estimer asymptotiquement la somme des cardinaux de ces groupes sur un ensemble de corps quadratiques de discriminant borné, et cela suivant deux méthodes ; une purement analytique, utilisant l'analyse complexe et les séries L de Dirichlet, et une plus géométrique, due à Siegel. Ceci fait l'objet des sections 3 et 4. Dans le second cas, la méthode s'appuiera sur une correspondance mise en évidence par Gauss entre ces objets arithmétiques et certaines classes de formes quadratiques entières, qui sera explicitée dans la section 2.

Pour $n = 3$, il est déjà difficile d'obtenir une description explicite des classes d'isomorphisme de corps cubiques. On va cependant disposer, à nouveau, d'une correspondance entre corps cubiques et certaines formes cubiques binaires, qui sera présentée au début de la section 5, et qui va nous permettre, à partir techniques de comptage de points entiers dans des domaines fondamentaux et d'arguments de densité locales de discriminants, de donner des équivalents asymptotiques des quantités $N(3, 0, X)$ et $N(3, -X, 0)$.

Première partie
Préliminaires

1 Théorie algébrique des nombres

1.1 Anneau des entiers d'un corps de nombres

Soit $\mathbf{Z}$ l'anneau des entiers relatifs, et $\mathbf{Q}$ le corps des nombres rationnels. On voit que l'on peut construire $\mathbf{Q}$ comme le corps des fractions de $\mathbf{Z}$; cependant, en théorie algébrique des nombres, on va être amené à considérer des *corps de nombres*, plus gros que $\mathbf{Q}$; on aimerait alors, de la même manière que pour $\mathbf{Z}$ et $\mathbf{Q}$, leur associer un *anneau d'entiers*, dont ils seront le corps de fractions. Cela nous conduit aux définitions suivantes :

Définition 1. *On appelle* corps de nombres *un sous-corps $K \subset \mathbf{C}$ (qui contient donc $\mathbf{Q}$ et est de caractéristique 0), qui est aussi un espace vectoriel de dimension finie sur $\mathbf{Q}$. On note $[K : \mathbf{Q}]$ cette dimension, appelée* degré *de K sur $\mathbf{Q}$. Il s'agit en particulier d'une extension* algébrique *de $\mathbf{Q}$, ce qui veut dire que chaque élément de K est* algébrique *sur $\mathbf{Q}$, c'est-à-dire est racine d'un polynôme à coefficients rationnels, puisque $(1, x, ..., x^{[K:\mathbf{Q}]})$ est liée sur $\mathbf{Q}$.*
On appelle anneau des entiers *de K, et on note $\mathcal{O}_K$ l'ensemble des $x \in K$* entiers *sur K, c'est-à-dire qui sont racines d'un polynôme* **unitaire** *à coefficients dans $\mathbf{Z}$.*
Il s'agit d'un sous-anneau de K, contenant $\mathbf{Z}$, de corps des fractions K.

Si $n = [K : \mathbf{Q}]$, pour $x \in K$, la famille $(1, x, ..., x^n)$ est $\mathbf{Q}$-liée, et donc on peut trouver un polynôme annulateur de x de degré plus petit que n. De plus, l'ensemble des polynômes annulateurs de x est un idéal de $\mathbf{Q}[X]$ et est donc principal, on appellera *polynôme minimal* de x sur $\mathbf{Q}[X]$ le polynôme unitaire engendrant cet idéal. Si $x \in \mathcal{O}_K$, ce polynôme est dans $\mathbf{Z}[X]$.
De plus, on remarque que l'anneau des entiers de $\mathbf{Q}$ est $\mathbf{Z}$: en effet, si $x = \frac{p}{q}$, avec p premier à q, est entier sur $\mathbf{Q}$, on a :

$$\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + ... + a_0 = 0, \text{ avec des } a_i \text{ entiers.}$$

Il s'ensuit, en multipliant par q^n, que $q|p^n$, et comme p est premier à q, par application répétée du lemme d'Euclide, on a $q|p$ donc $q = 1$ et $x \in \mathbf{Z}$.

Exemple :

Soit K un corps *quadratique*, i.e. un corps de dimension 2 sur $\mathbf{Q}$ (un corps *cubique* correspondant au cas $[K : \mathbf{Q}] = 3$), et soit $x \in K - \mathbf{Q}$.

Alors $(1, x)$ est libre, donc forme une base de K. Or comme $x \notin \mathbf{Q}$, le polynôme minimal de x est de degré exactement 2, et $x = \frac{-b+\sqrt{\Delta}}{2}$, avec $b, \Delta \in \mathbf{Q}$; en translatant puis dilatant on trouve une base $(1, \sqrt{\Delta})$ de K, $\Delta \in \mathbf{Q}$, et en chassant le dénominateur et les facteurs carrés du dénominateur, on a montré le fait suivant :

Proposition 1. *(Corps de nombres quadratiques)*
Les corps quadratiques sur $\mathbf{Q}$ *sont exactement les* $\mathbf{Q}(\sqrt{d})$*, où* d *parcourt l'ensemble des entiers relatifs sans facteurs carrés. On remarque que* $K \subset \mathbf{R}$ *si et seulement si* d *est positif.*

On va au passage calculer les entiers de $\mathbf{Q}(\sqrt{d})$:

Proposition 2. *(Entiers des corps quadratiques)*
Soit d *un entier relatif sans facteurs carrés.*
(1) Si $d \equiv 2, 3[4]$ *alors l'anneau des entiers de* $\mathbf{Q}(\sqrt{d})$ *est* $\mathbf{Z}[\sqrt{d}]$.
(2) Si $d \equiv 1[4]$ *alors l'anneau des entiers de* $\mathbf{Q}(\sqrt{d})$ *est* $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$.

Démonstration. On va librement utiliser le fait que l'anneau des entiers d'un corps de nombres est en effet un anneau.
Remarquons que si $x = a + b\sqrt{d} \in \mathcal{O}_K$, $a, b \in \mathbf{Q}$, alors $\bar{x} = a - b\sqrt{d}$ aussi, ils ont d'ailleurs le même polynôme minimal ; cela se vérifie par un calcul direct. Mais alors $x + \bar{x}$ et $x\bar{x}$ sont dans $\mathcal{O}_K$, et aussi dans $\mathbf{Q}$: comme l'anneau des entiers de $\mathbf{Q}$ est $\mathbf{Z}$; ces quantités sont entières : on doit alors avoir $2a \in \mathbf{Z}$ et $a^2 - db^2 \in \mathbf{Z}$.
Notons que cette condition est suffisante, puisqu'alors $(X - x)(X - \bar{x}) = X^2 - 2aX + (a^2 - db^2) \in \mathbf{Z}[X]$ annule x.
On voit alors que $d(2b)^2 \in \mathbf{Z}$, d étant sans facteurs carrés, si $2b$ avait un facteur premier au dénominateur, d ne pourrait pas ramener $(2b)^2$ dans $\mathbf{Z}$: il s'ensuit que $2b \in \mathbf{Z}$.
On écrit alors $2a = u$, $2b = v$: on a alors $u^2 - dv^2 \in 4\mathbf{Z}$; donc si u est impair, on doit avoir $dv^2 \equiv 1[4]$, et un carré ne peut être que 0 ou 1 modulo 4 : la seule possibilité est alors $d \equiv 1[4]$ et v impair. De plus, si u est pair, comme 4 ne divise pas d, on a nécessairement v pair aussi : autrement dit u et v sont dans la même classe modulo 2, et ne peuvent être impairs que si $d \equiv 1[4]$. Ceci prouve la proposition. □

1.2 Normes, traces, conjugués

La preuve précédente nous a amené à considérer les quantités entières $a^2 - db^2$ et $2a$, pour un élément $x = a + \sqrt{db}$ d'un corps quadratique. La structure de $\mathbf{Q}$-espace vectoriel dont on dispose sur K permet de généraliser ces quantités à tous les corps de nombres.

Définition 2. *Soit K un corps de nombres. Pour $x \in K$, on note $m_x : y \longmapsto xy$ le $\mathbf{Q}$-endomorphisme de K de multiplication par x. On définit alors la* trace *de x sur $\mathbf{Q}$ comme celle de l'endomorphisme m_x ; et sa norme comme le déterminant de m_x ; on notera :*

$$Tr_{K/\mathbf{Q}}(x) := Tr(m_x) \ ; \ N_{K/\mathbf{Q}}(x) = \det(m_x).$$

Dans le cas des corps quadratiques, on avait aussi associé à $x =$ son *conjugué* $\bar{x} = a - \sqrt{d}b$; de telle sorte que $Tr(x) = x + \bar{x}$ et $N(x) = x\bar{x}$. Cette notion de conjugué peut aussi être généralisée. Le théorème suivant, permettant de décrire assez simplement les corps de nombres, est donné sans démonstration :

Théorème 1. *(Théorème de l'élément primitif) Soit K un corps de nombres. Il existe $x \in K$, dit* primitif, *tel que $K = \mathbf{Q}(x)$. Le résultat s'étend de plus aux corps finis : si $\mathbf{F}_q$ est une extension finie de $\mathbf{F}_p = (\mathbf{Z}/p\mathbf{Z})$, il existe $x \in \mathbf{F}_q$ tel que $\mathbf{F}_q = \mathbf{F}_p(x)$.*

Soit alors x un élément primitif pour l'extension K. On cherche les $\mathbf{Q}$-morphismes de K à valeurs dans $\mathbf{C}$, c'est-à-dire les morphismes de corps de K laissant $\mathbf{Q}$ invariant. Si $P \in \mathbf{Q}[X]$ est le polynôme minimal de x sur K (nécessairement de degré $[K : \mathbf{Q}]$), en appliquant un tel morphisme σ à l'équation $P(x) = 0$, on obtient $P(\sigma(x)) = 0$. On voit que l'on a autant de $\mathbf{Q}$-morphismes de K que le polynôme minimal de x a de racines distinctes dans $\mathbf{C}$. Or, supposons que P ait une racine double : alors P' et P auraient une racine commune, et, le pgcd ne dépendant pas du corps dans lequel on le calcule, le pgcd de P et P' serait non trivial. Or P est irréductible par définition ; donc cela entraînerait $P|P'$, ce qui n'est possible que si P est constant ; ce qui n'est pas le cas. En remarquant qu'un morphisme de corps est toujours injectif, on a prouvé le résultat suivant :

Proposition 3. *Soit K un corps de nombres, avec $K = \mathbf{Q}(x)$, et n son degré. Alors il existe exactement n $\mathbf{Q}$-isomorphismes $\sigma_1, ..., \sigma_n$ de corps de K dans un sous-corps de $\mathbf{C}$, envoyant x sur les racines complexes distinctes de son polynôme minimal. Pour $y \in K$, les $\sigma_i(y)$ sont ses* conjugués, *et les images de ces morphismes sont les* corps conjugués *de K.*

On va alors généraliser les formules quadratiques $N(x) = x\bar{x}$ et $Tr(x) = x + \bar{x}$:

Proposition 4. *Soit $x \in K$. On a :*

$$N(x) = \prod_{i=1}^{n} \sigma_i(x) \ ; et \ Tr(x) = \sum_{i=1}^{n} \sigma_i(x).$$

Démonstration. On commence par supposer x primitif. Dans ce cas, la famille $(1, ..., x^{n-1})$ forme une base de K. Si $P(X) = X^n + a_{n-1}X^{n-1} + ... + a_0$

est le polynôme minimal de x sur $\mathbf{Q}$, on calcule la matrice de l'endomorphisme m_x dans la base $(1, ..., x^{n-1})$:

$$M_x = \begin{pmatrix} 0 & 0 & \cdots & -a_0 \\ 1 & 0 & \ddots & -a_1 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

Il s'agit de la matrice compagnon de P, on sait que sa trace est $-a_{n-1}$ et son déterminant est $(-1)^n a_0$: ce sont respectivement la somme et le produit des racines de P, qui sont les conjugués de x : ceci prouve la proposition pour x primitif.
Si x n'est pas primitif, on note $r = [K : \mathbf{Q}(x)]$. On peut facilement se convaincre, à l'aide de bases adaptées, que :

$$[K : \mathbf{Q}] = [K : \mathbf{Q}(x)][\mathbf{Q}(x) : \mathbf{Q}].$$

On va montrer que le polynôme caractéristique de m_x est $P(X)^r$, où P est toujours le polynôme minimal de x. En effet, si $(y_1, ..., y_r)$ est une base de K sur $\mathbf{Q}(x)$, on vérifie facilement que $(x^i y_j)_{i,j}$ est une $\mathbf{Q}$-base de K ; si on ordonne cette base dans l'ordre lexicographique on voit que :

$$M_x = \begin{pmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & M \end{pmatrix};$$

où M est la matrice de m_x restreint à $\mathbf{Q}(x)$; ce qui termine la preuve. □

On en tire aussi une caractérisation des éléments entiers de K :

Proposition 5. *Soit $x \in K$, de polynôme minimal P. Alors $x \in \mathcal{O}_K$ si et seulement si $P \in \mathbf{Z}[X]$.*

Démonstration. On prouve l'implication directe, l'autre étant vraie par définition. Par ce qui précède, les coefficients de P sont des fonctions symétriques élémentaires en les $\sigma_i(x)$, les conjugués de x. En appliquant σ_i à l'équation $P(x) = 0$, on voit que les conjugués de x sont racines d'un polynôme unitaire à coefficients entiers : ils sont entiers ; ainsi comme l'ensemble des éléments de $\mathbf{C}$ entiers sur $\mathbf{Z}$ est un anneau, il s'ensuit que les coefficients de P sont rationnels, racines d'un polynôme unitaire à coefficients entiers, donc entiers sur $\mathbf{Q}$: on a vu que dans ce cas ils sont nécessairement entiers. □

1.3 Discriminant d'un corps de nombres

On donne tout d'abord la définition générale du discriminant d'un polynôme, qui étend la définition habituelle pour les polynômes de degré 2 :

Définition 3. *Soit $P \in \mathbf{C}_n[X]$, de coefficient dominant a, et de racines $x_1, ..., x_n$. Son* discriminant *est la quantité :*

$$D = a^n \prod_{i<j} (x_i - x_j)^2$$

C'est un polynôme homogène de degré $2n-2$ en les coefficients de P.

Dans le cas $n = 2$, il s'agit juste de $\Delta = b^2 - 4ac$. Pour $P(x) = ax^3 + bx^2 + cx + d$, on a $D = b^2c^2 - 4ac^3 - 4b3d - 27a^2d^2 + 18abcd$.

Définition 4. *(Discriminant d'une base) Soit $(x_1, ..., x_n)$ une base de K corps de nombres. On définit le* discriminant *de K relativement à cette base comme la quantité :*

$$D(x_1, ..., x_n) = \det((Tr(x_i x_j)_{i,j})).$$

Il s'agit en fait du discriminant de la forme quadratique $(x, y) \longmapsto Tr(xy)$, on sait que cette quantité est définie à un carré rationnel près, elle dépend donc du choix de la base. On peut la calculer en utilisant les conjugués des x_i :

Proposition 6. *Soit K corps de nombres, et $\sigma_1, ..., \sigma_n$ les n isomorphismes distincts de K dans ses corps conjugués. Si $(x_1, ..., x_n)$ est une base de K, on a $D(x_1, ..., x_n) = [\det(\sigma_i(x_j))]^2 \neq 0$*

Démonstration. La première égalité résulte d'un calcul direct :

$$D(x_1, ..., x_n) = \det(Tr(x_i x_j)) = \det(\sum_{k \leq n} \sigma_k(x_i x_j))$$

$$= \det(\sum_{k \leq n} \sigma_k(x_i)\sigma_k(x_j)) = \det(\sigma_k(x_i)) \det(\sigma_k(x_j)) = [\det(\sigma_i(x_j))]^2.$$

Reste à prouver que cette quantité est non nulle ; si elle l'était on aurait un vecteur $(u_1, ..., u_n) \in \mathbf{C}^n$ tel que $\sum_{i=1}^n u_i \sigma_i(x_j) = 0 \; \forall \; j$.
Par linéarité on en tire $\sum_{i=1}^n u_i \sigma_i = 0$; ce qui est contradictoire par indépendance linéaire des caractères. □

Dans le cas où $K = \mathbf{Q}(x)$, on peut alors calculer le discriminant de K relativement à la base $(1, x, ..., x^{n-1})$: en effet, $\sigma_i(x^j) = (\sigma_i(x)^j)$ et donc $D(1, ..., x^{n-1}) = (\det((x_i)^j))^2$ où les x_i sont les conjugués de x. On reconnaît alors un déterminant de Vandermonde, et ainsi on obtient l'égalité $D(1, ..., x^{n-1}) = \prod_{i<j}(x_i - x_j)^2 = Disc(P)$, où P désigne le polynôme

minimal de x. Ceci justifie le choix du terme *discriminant*.

Le fait que le discriminant soit non nul montre que la forme quadratique $(x,y) \longmapsto Tr(x,y)$ est non dégénérée : si $Tr(xy) = 0$ pour tout $x \in K$ alors $y = 0$. Ainsi l'application de K dans son dual (vus comme $\mathbf{Q}$-espaces vectoriels) $y \longmapsto Tr(.,y)$ est injective et donc surjective pour des raisons de dimensions : ceci garantit l'existence de bases duales : si $(x_1, ..., x_n)$ est une base de K, il existe une base $(y_1, ..., y_n)$ telle que $Tr(x_i y_j) = \delta_{i,j}$ pour tous i,j. Cette remarque va nous être utile. Avant de pouvoir définir le discriminant absolu d'un corps de nombres, on prouve :

Théorème 2. *Soit K un corps de nombres, et n son degré. Alors $\mathcal{O}_K$ est un $\mathbf{Z}$-module libre de rang n, c'est-à-dire qu'il existe $y_1, ..., y_n \in \mathcal{O}_K$ $\mathbf{Z}$-indépendants tels que $\mathcal{O}_K = \mathbf{Z}y_1 \oplus ... \oplus \mathbf{Z}y_n$.*

Démonstration. Soit $(x_1, ..., x_n)$ une base de K sur $\mathbf{Q}$. Chaque x_i est algébrique sur $\mathbf{Q}$, on en tire n équations polynomiales à coefficients rationnels $a_{n,i}x_i^n + ... + a_{0,i} = 0$, où l'on peut toujours supposer $a_{n,i} \neq 0$.
En multipliant par $a_{n,i}^{n-1}$, on voit que $a_{n,i}x_i = x_i'$ est entier sur K ; de plus les $(x_i')_{i \leq n}$ forment une base de K, constituées d'éléments entiers.
On prend alors $(y_1, ..., y_n)$ une base duale des x_i' ; soit alors $z \in \mathcal{O}_K$. On peut décomposer z suivant les y_j : $z = \sum_{j=1}^n b_j y_j$, où les b_j sont rationnels. Or pour un i quelconque $x_i' z \in \mathcal{O}_K$; donc $Tr(x'iz) = \sum_{j=1}^n b_j Tr(x_i' y_j) = b_j \in \mathbf{Z}$. Ainsi $\mathcal{O}_K$ est contenu dans le $\mathbf{Z}$-module $\mathbf{Z}y_1 \oplus ... \oplus \mathbf{Z}y_n$. C'est donc un sous-groupe d'un groupe abélien libre de type fini : c'est donc aussi un groupe abélien libre, de rang n puisqu'il contient une base de K. □

Définition 5. *(Discriminant absolu) Soit alors $(y_1, ..., y_n)$ une $\mathbf{Z}$-base de $\mathcal{O}_K$: on définit le* discriminant absolu *(que l'on appelera juste discriminant lorsqu'il n'y aura pas de confusion possible) la quantité :*

$$D = Disc(K) = Disc(x_1, ..., x_n).$$

A nouveau, il n'est défini qu'à un carré près, plus précisément au carré du déterminant d'une matrice de changement de $\mathbf{Z}$-base près. Or une telle matrice est inversible à coefficients entiers, et de fait son déterminant est ± 1, et son carré vaut 1 : ceci prouve que le déterminant ne dépend pas du choix de la base.
En pratique, si $K = \mathbf{Q}(x)$, de degré n, tout élément de $\mathcal{O}_K$ s'écrit $d^{-1} \sum n_i x^i$, avec $n_i \in \mathbf{Z}$ et $d = Disc(1, ..., x^{n-1})$ (noter que $Disc(K) = [\mathcal{O}_K : \mathbf{Z}[x]]^2 d$).
On énonce sans démonstration le résultat suivant :

Théorème 3. *(Hermite) Pour tous entiers D et n fixés, il n'existe qu'un nombre fini de corps de nombres de degré n et de discriminant absolu D.*

Discriminant des corps quadratiques

En guise d'exemple, on calcule le discriminant du corps quadratique $\mathbf{Q}(\sqrt{d})$:
Si $d \equiv 2, 3\ [4]$, $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}\sqrt{d}$, la matrice $(Tr(x_i x_j))$ s'écrit tout simplement :

$$\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix}.$$

Le discriminant de K est alors $4d$.
Si $d \equiv 1\ [4]$, $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}(\frac{1+\sqrt{d}}{2})$, et la matrice de la forme quadratique s'écrit :

$$\begin{pmatrix} 2 & 1 \\ 1 & (d+1)/2 \end{pmatrix}.$$

Le discriminant de K est alors d.
On peut donc aussi paramétrer les corps quadratiques par leurs discriminants : si D est un *discriminant fondamental*, i.e. un entier congru à 0 ou 1 modulo 4, et sans facteur carré autre que 4, alors il est le discriminant d'un unique corps quadratique ; réciproquement le discriminant d'un corps quadratique est toujours de cette forme.

Corps cubiques

Dans le cas cubique, la situation est plus compliquée : tout d'abord, le discriminant ne détermine plus les corps, i.e. il existe des corps cubiques de même discriminant non isomorphes. On sait cependant calculer $\mathcal{O}_K$ dans des cas simples, par exemple le cas "cubique pur", i.e. $K = \mathbf{Q}(\sqrt[3]{m})$ où m est entier sans facteur cubique : en supposant que m est de plus sans facteur carré, si $x = \sqrt[3]{(m)}$, une base de $\mathcal{O}_K$ est donnée par $(1, x, x^2)$ si $m \neq \pm 1[9]$, ou $(1, x, \frac{x^2 \pm x + 1}{3})$ lorsque $m \equiv \pm 1[9]$; le lecteur intéressé pourra trouver plus de détails dans [?].

1.4 Factorisation dans $\mathcal{O}_K$

Le théorème fondamental de l'arithmétique nous dit que tout entier $n \in \mathbf{Z}$ peut s'écrire, de façon unique à l'ordre des facteurs près, sous la forme $n = \pm p_1^{\alpha_1} ... p_r^{\alpha_r}$, où $p_1, ..., p_r$ sont des nombres premiers, et les α_i des exposants positifs. On dit que $\mathbf{Z}$ est *factoriel*. On s'est progressivement rendu compte, au XIXème siècle, qu'en général les anneaux d'entiers de corps de nombres ne sont pas factoriels ; le problème n'étant dans ce cas précis pas l'existence de la décomposition en éléments premiers mais *l'unicité*, comme le montre l'exemple suivant :
Dans $\mathbf{Z}[i\sqrt{5}]$, qui est l'anneau des entiers de $\mathbf{Q}[i\sqrt{5}]$, on a $6 = 2.3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. On va montrer que 2, 3, $(1 + i\sqrt{5})$ et $(1 - i\sqrt{5})$ sont premiers dans cet anneau : en effet, un élément de $\mathbf{Z}[i\sqrt{5}]$ a le carré de son

module entier, et par multiplicativité de cette quantité, on voit par exemple qu'un diviseur de $1 + i\sqrt{5}$ doit avoir un module au carré divisant 6, et on se convainc facilement en regardant les petites valeurs prises par la forme quadratique $x^2 + 5y^2$ qu'au signe près, les seuls diviseurs de $(1 + i\sqrt{5})$ sont 1 et lui-même. Le même genre de raisonnement vaut pour les autres.
L'idée de Dedekind est alors de rajouter dans ces anneaux des "nombres idéaux", qui permettraient de poursuivre la décomposition : dans l'exemple ci-dessus, on aimerait avoir 4 nombres en plus γ_i, $1 \leq i \leq 4$, tels que $2 = \gamma_1\gamma_2$, $3 = \gamma_3\gamma_4$, $1 + i\sqrt{5} = \gamma_1\gamma_3$ et $1 - i\sqrt{5} = \gamma_2\gamma_4$. En fait, l'idée centrale est d'identifier un élément $x \in \mathcal{O}_K$ avec l'idéal principal (x) qu'il engendre ; et de chercher, au lieu d'une décomposition en facteurs premiers, une décomposition en idéaux premiers d'un idéal donné. On rappelle ici les définitions générales :

Définition 6. *Soit A un anneau intègre :*
On dit qu'un idéal $I \subset A$ est premier *si son complémentaire est stable par multiplication, i.e. $\{xy \in I \iff x \text{ ou } y \in I\}$. Cela revient à demander à ce que l'anneau quotient A/I soit intègre.*
On dit qu'un idéal $I \subset A$ est maximal *si les seuls idéaux qui le contiennent sont A et lui-même. Cela revient à demander à ce que l'anneau quotient A/I soit un corps.*

Par exemple, dans $\mathbf{Z}$, et plus généralement dans tout anneau principal, les idéaux premiers coïncident avec les idéaux maximaux, et sont ceux engendrés par les éléments irréductibles.

Définition 7. *Si A est un anneau intègre, $I, J \subset A$, on définit le produit et la somme de I et J par :*

$$I + J = \{x + y \ ; \ x \in I, y \in J\}$$

$$IJ = \left\{ \sum_{i \leq k} x_i y_i \ ; \ x_i \in I, y_i \in J \right\}$$

On vérifie immédiatement que ce sont des idéaux de A.

Proposition 7. *Soit $A = \mathcal{O}_K$ l'anneau des entiers d'un corps de nombres K. Pour tout $x \in A$ non nul, on a $|N(x)| = |A/Ax|$.*

Démonstration. Soit $(v_1, ..., v_n)$ une $\mathbf{Z}$-base de A. L'idéal Ax en est un sous-module de même rang ; par le théorème de la base adaptée il existe des entiers c_1,..., c_n tels que $(c_1v_1, ..., c_nv_n)$ forme une $\mathbf{Z}$-base de Ax. Le quotient A/Ax est alors isomorphe, en tant que groupe additif, au produit $\mathbf{Z}/c_1\mathbf{Z} \times ... \times \mathbf{Z}/c_n\mathbf{Z}$; et son cardinal est donc $c_1...c_n$.
Soit $u : A \longrightarrow Ax$ l'application $\mathbf{Z}$-linéaire envoyant v_i sur c_iv_i ; il est clair

que son déterminant est $c_1...c_n$.
Or il est clair que $(xv_1, ..., xv_n)$ forme aussi une base de Ax : soit alors v l'automorphisme de Ax envoyant $c_i v_i$ sur xv_i : on alors $v \circ u = m_x$, donc $\det(u)\det(v) = N(x)$. Or v est un automorphisme de $\mathbf{Z}$-module, son déterminant est $\mathbf{Z}$-inversible et vaut donc ± 1, ce qui donne le résultat. □

On définit alors la *norme* d'un idéal :

Définition 8. *Si $I \subset A$ est un idéal non nul de A anneau des entiers d'un corps de nombres, on définit sa norme comme le cardinal de l'anneau-quotient A/I.*

Notons que tout idéal non nul est contenu dans l'idéal principal engendré par n'importe lequel de ses éléments non nuls, et donc que $N(I) \leq N(x)$ pour tout $x \in I$: ceci montre la finitude de la norme. De plus, la multiplicativité de la norme est conservée : on a toujours $N(IJ) = N(I)N(J)$.

L'exemple de $\mathbf{Z}[i\sqrt{5}]$ a montré la factorialité ne passait pas aux extensions entières ; on introduit alors la notion plus faible, d'anneau de Dedekind, et admettre le théorème fondamental suivant :

Théorème-définition 1. *(Dedekind) Soit A un anneau intègre. On dira que A est* de Dedekind *si tout idéal $I \subset A$ admet une décomposition, unique à l'ordre des facteurs près, de la forme :*

$$I = P_1^{e_1}...P_r^{e_r}$$

où les P_i sont des idéaux premiers de A, et les e_i sont des exposants positifs. L'anneau des entiers d'un corps de nombres est de Dedekind.

On peut par ailleurs remarquer que les idéaux "divisant" I, c'est-à-dire les contenant, sont ceux dont les valuations e_i sont toutes inférieures à celles de I. Par conséquent, dans un anneau de Dedekind, tout idéal premier est maximal. On admet aussi le théorème suivant, décrivant la décomposition des nombres premiers en idéaux premiers dans $\mathcal{O}_K$:

Théorème 4. *Tout idéal premier de $\mathcal{O}_K$ contient exactement un nombre premier p. Pour un tel p, les idéaux premiers le contenant sont exactement les idéaux apparaissant dans la décomposition :*

$$p\mathcal{O}_K = P_1^{e_1}...P_r^{e_r}$$

.
Le corps résiduel $\mathcal{O}_K/(P_i)$ est un $\mathbf{F}_p$-espace vectoriel de dimension finie f_i, appelée degré résiduel *de P_i. Le nombre e_i est appelé* indice de ramification *de p au-dessus de P_i.*
On a alors, pour tout premier p, la formule $\sum_{i=1}^{r} e_i f_i = n$.

On dira que p se ramifie *dans $\mathcal{O}_K$ si au moins un des indices de ramification e_i est strictement plus grand que* 1.
En fait, les nombres premiers se ramifiant dans $\mathcal{O}_K$ sont précisément les diviseurs du discriminant de K ; et il en y en a toujours au moins un.

Décomposition des nombres premiers dans les corps quadratiques

Etant donné la formule $\sum_{i=1}^{r} e_i f_i = 2$ on a trois types de décompositions possibles : $e = 2$ et $f = 1$ (cas ramifié) ; $e = 1$ et $f = 2$ (cas inerte) ; et $e_1 = f_1 = e_2 = f_2$ (cas décomposé). On décrit ici le cas $d \equiv 2, 3[4]$, i.e. $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}] \cong \mathbf{Z}[X]/(X^2 - d)$.
Le cas ramifié correspond au cas où $p|D$; le quotient $\mathcal{O}_K/(p)$ est une $\mathbf{F}_p$-algèbre non réduite, c'est-à-dire contenant des éléments nilpotents.
Le cas inerte correspond au cas où l'idéal (p) reste premier dans $\mathcal{O}_K$; or $\mathcal{O}_K/(p) \cong \mathbf{F}_p[X]/(X^2 - d)$; et donc le polynôme $X^2 - d$ est irréductible dans $\mathbf{F}_p$: cela signifie exactement que d n'est pas un carré modulo p. Le quotient $\mathcal{O}_K/(p)$ est isomorphe à $\mathbf{F}_{p^2}$.
Enfin, dans le cas décomposé, le quotient $\mathcal{O}_K/(p)$ est isomorphe à $\mathcal{O}_K/(P_1) \times \mathcal{O}_K/(P_2)$ par le lemme chinois ; et donc au produit de deux corps : $X^2 - d$ est scindé modulo p par l'argument précédent. Ainsi d est un carré modulo p et $\mathcal{O}_K/(p) \cong \mathbf{F}_p^2$.

On dispose alors d'une structure multiplicative sur l'ensemble des idéaux de $\mathcal{O}_K$; on va le munir d'une structure de groupe et en identifier un quotient fini intéressant, qui va nous permettre de mesurer le défaut de principalité de $\mathcal{O}_K$

1.5 Groupe des classes d'idéaux

On a vu comment munir l'ensemble des idéaux non nuls de $\mathcal{O}_K$ d'un produit, dont on vérifie facilement qu'il est associatif, et que $\mathcal{O}_K$ est un élément neutre pour cette multiplication. Pour transformer ce monoïde en groupe, on va avoir besoin d'ajouter des inverses aux idéaux :

Définition 9. *(Idéal fractionnaire) On dira qu'un sous $\mathbf{Z}$-module I de K est un* idéal fractionnaire *s'il existe $d \in \mathcal{O}_K$ tel que $I \subset d^{-1}\mathcal{O}_K$.*
Cela revient à dire que les éléments de I ont un dénominateur commun d. On remarque les idéaux habituels sont des idéaux fractionnaires (prendre $d = 1$) ; on les appellera idéaux entiers. *On généralise la construction à tout anneau de Dedekind A, de corps des fractions K.*
On étend alors la somme et le produit des idéaux aux idéaux fractionnaires, exactement de la même manière.

On admet le théorème suivant, dont la preuve utilise une propriété importante des anneaux de Dedekind, appelée *noethérianité* :

Théorème 5. *Soit A un anneau de Dedekind, et K son corps des fractions. Tout idéal fractionnaire de A se décompose, d'une manière unique à l'ordre des facteurs près :*

$$I = P_1^{v_1}....P_n^{v_n}$$

où les P_i sont des idéaux premiers de A, et les v_i des entiers relatifs.
En particulier, l'ensemble des idéaux fractionnaires de A forme un groupe abélien, noté $I(A)$.

On constate que les idéaux fractionnaires principaux, c'est-à-dire les idéaux fractionnaires $x\mathcal{O}_K$, $x \in K$, forment un sous-groupe $\Pi(A)$ de $I(A)$, le produit et l'inverse étant donnés par le produit et l'inverse des générateurs.

Définition 10. *Le* groupe des classes d'idéaux *de A anneau de Dedekind est le groupe quotient $Cl(A) = I(A)/\Pi(A)$. Il est trivial si et seulement si A est principal. Dans le cas où A est l'anneau des entiers d'un corps de nombres, c'est en fait un groupe* fini.

La finitude du groupe de classes d'idéaux sera démontrée dans le cas des corps quadratiques dans la section suivante ; bien qu'il s'agisse d'un fait général à tous les corps de nombres.

2 Classes d'idéaux et formes quadratiques

2.1 Généralités sur les formes

Définition 11. *On appelle forme quadratique binaire entière une fonction de la forme $q : \mathbf{Z}^2 \to \mathbf{Z}$ vérifiant $q(x, y) = ax^2 + bxy + cy^2, \forall x, y \in \mathbf{Z}$ avec $(a, b, c) \in \mathbf{Z}^3$.*

L'objectif principal est de prouver le théorème 6, qui établit un lien très étroit entre formes quadratiques binaires à équivalence près et classes d'idéaux.

Lorsqu'il n'y a pas de confusion possible, on appellera "forme" une "forme quadratique binaire entière". Une forme étant entièrement déterminée par le triplet $(a, b, c) \in \mathbf{Z}^3$, on utilisera la notation (a, b, c) pour la désigner. Une forme (a, b, c) est dite *primitive* si a, b et c sont premiers entre eux dans leur ensemble, c'est-à-dire si (a, b, c) n'est pas de la forme nq, où q est une forme et $n \geq 2$.

Définition 12. *Soit $q = (a, b, c)$ une forme, son* discriminant *est l'entier $Disc(q) = b^2 - 4ac$.*

On munit maintenant l'ensemble des formes d'une relation d'équivalence. On rappelle que $SL_2(\mathbf{Z})$ est l'ensemble des matrices de $\mathcal{M}_2(\mathbf{Z}) \cap SL_2(\mathbf{R})$, dont l'inverse est également dans $\mathcal{M}_2(\mathbf{Z})$. On définit une action de $SL_2(\mathbf{Z})$

sur l'ensemble des formes par changement de coordonnées : Si q est une forme et $M \in SL_2(\mathbf{Z})$ on note $q \cdot M$ la forme $q(M \begin{pmatrix} x \\ y \end{pmatrix})$. Soient q une forme et $M, N \in SL_2(\mathbf{Z})$, on a clairement $q \cdot MN = (q \cdot N) \cdot M$ et $q \cdot I_2 = q$, il s'agit donc bien d'une action de groupe. On considère la relation d'équivalence suivante : $q \sim q'$ si q et q' appartiennent à la même orbite sous l'action de $SL_2(\mathbf{Z})$. Autrement dit $q \sim q'$ si il existe une $\mathbf{Z}$-base directe u, v de $\mathbf{Z}^2$ telle que $q'(x, y) = q(xu + yv)$.

Proposition 8. *Deux formes équivalentes sont primitives en même temps et ont le même discriminant.*

Démonstration. Soient q, q' deux formes telles que $q \sim q'$, il existe $M \in SL_2(\mathbf{Z})$ telle que $q' = q \cdot M$. Supposons q non primitive, il existe $m \geq 2$ et p une forme telle que $q = mp$. On a $q' = (mp) \cdot M = m(q \cdot M)$ donc q' n'est pas primitive.
Pour montrer l'invariance du discriminant on définit si $q = (a, b, c)$:
$Mat(q) = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$. On a $det(Mat(q)) = -Disc(q)$. De plus pour tout $x, y \in \mathbf{Z}$, on a $2q(x, y) = {}^t \begin{pmatrix} x \\ y \end{pmatrix} Mat(q) \begin{pmatrix} x \\ y \end{pmatrix}$.
On a donc $Mat(q \cdot M) = {}^t MMat(q)M$, et $Disc(q \cdot M) = det(M)^2 Disc(q)$, et $Disc(q) = Disc(q')$. □

Proposition 9. *Soit $D \in \mathbf{Z}$. Il n'existe qu'un nombre fini de classes d'équivalence de formes de discriminant D.*

Pour le démontrer, on va étudier séparément le cas où D est un carré et le cas où il ne l'est pas.

Lemme 1. *(Réduction de Lagrange) Toute forme de discriminant D non carré est équivalente à une forme (a, b, c) avec $-|a| < b \leq |a| \leq |c|$.*

Démonstration. On va démontrer ce lemme de manière algorithmique, étant donné une forme (a, b, c) ne vérifiant pas toutes les inégalités de $|b| \leq |a| \leq |c|$, on va trouver une forme (a', b', c') équivalente à (a, b, c) telle que $|a'| + |b'| < |a| + |b|$, on pourra alors conclure.
Si $|c| < |a|$, on pose $(a', b', c') = (a, b, c) \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = (c, -b, a)$.
Si $|c| \geq |a|$, $|b| > |a|$, on a $a \neq 0$ car D n'est pas un carré. On a donc soit $|b + a| < |b|$, soit $|b - a| < |b|$.
Si $|b+a| < |b|$, on pose $(a', b', c') = (a, b, c) \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = (a, b+2a, c+a+b)$.
Si $|b-a| < |b|$, on pose $(a', b', c') = (a, b, c) \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = (a, b-2a, c+a-b)$.
Le fait que dans chaque cas on ait $|a'| + |b'| < |a| + |b|$ nous assure la

terminaison de l'algorithme. Dans chaque classe, il existe donc une forme (a, b, c) telle que $|b| \leq |a| \leq |c|$.
Il reste à éliminer le cas $|c| \geq |a|$, $b = -|a|$, dans ce cas si $a = b$ on pose $(a', b', c') = (a, b-2a, c+a-b)$ c'est-à-dire $(a', b', c') = (a, -a, c)$. Si $a = -b$, on pose $(a', b', c') = (a, b+2a, c+a+b)$ c'est-à-dire $(a', b', c') = (a, a, c)$. Cela revient à changer le signe de b et on obtient dans chaque classe un représentant vérifiant les inégalités souhaitées. □

Lemme 2. *Toute forme de discriminant $D = k^2, k > 0$ carré est équivalente à une forme $(0, \pm k, c)$, avec $0 \leq c < k$.*

Démonstration. Montrons dans un premier temps le lemme sans la condition sur c. Soit (a, b, c) une forme de discriminant D. Si $a = 0$, on a directement le résultat souhaité. Si $c = 0$, on se ramène au premier cas en posant $(a', b', c') = (c, -b, a)$. On peut donc maintenant supposer $a \neq 0$ et $c \neq 0$ c'est Ã dire $|b| \neq k$. Dans ce cas, on a $q(b-k, 2a) = a(b-k)^2 + 2ab(k-b) + 4a^2c = a(k^2 - (b^2 - 4ac)) = 0$. Comme $b - k \neq 0$ et $2a \neq 0$, on obtient en divisant $b - k$ et $2a$ par leur *pgcd*, $(\alpha, \beta) \in (Z)^2$ avec $q(\alpha, \beta) = 0$ et $pgcd(\alpha, \beta) = 1$. Comme α et β sont premiers entre eux, on peut compléter (α, β) dans le but d'obtenir une $\mathbf{Z}$ -base directe de $\mathbf{Z}$. Soit $M = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in SL_2(\mathbf{Z})$, soit $(a', b', c') = (a, b, c) \cdot M$, on a $q(M \begin{pmatrix} 1 \\ 0 \end{pmatrix}) = q(\alpha, \beta) = 0$. On a donc $a' = 0$ et $b = \pm k$ ce qui est le résultat souhaité. Dans chaque classe, il existe donc un représentant de la forme $(0, \pm k, c)$. Il s'agit maintenant de montrer que l'on peut prendre $0 \leq c < k$. Pour cela, on itère des transformations de la forme $(a', b', c') = (a, b+2a, c+a+b)$ (ou $(a', b', c') = (a, b-2a, c+a-b)$ selon les signes de b et c)pour se ramener au reste de c modulo $|b|$. □

Démonstration. (de la proposition) Si D est un carré, le second lemme nous assure qu'il y a au plus $2k$ classes. Supposons D non carré ; d'après le premier lemme, il existe dans chaque classe une forme (a, b, c) telle que $-|a| < b \leq |a| \leq |c|$, on a alors $4|a|^2 \leq 4ac \leq |b|^2 + |D| \leq |a|^2 + |D|$. On a donc $1 \leq |a| \leq \sqrt{\frac{|D|}{3}}$. Il n'existe donc qu'un nombre fini de triplets vérifiant ces conditions, et donc qu'un nombre fini de classes. □

Définition 13. *On désigne par Cl(D) (resp. P(D)) l'ensemble des classes d'équivalence de formes(resp. de formes primitives) de discriminant D. Dans le cas où $D < 0$, on ne considère que les formes positives, c'est $\tilde{A}$ dire les formes (a, b, c) avec $a > 0$. On note de plus $h_D = \#P(D)$.*

Dans le cas, où $D < 0$ on va voir qu'il y a presque unicité de la forme réduite au sens de Lagrange. Cela nous permettra plus tard d'estimer le nombre de classe de discriminant $D < 0$, en comptant le nombre de triplets vérifiant les inégalités satisfaites par la forme réduite.

Proposition 10. *(Réduction de Gauss) Une forme (a, b, c) positive de discriminant < 0 est équivalente à une unique forme telle que $-a < b \leq a \leq c$, et telle que $b \geq 0$ si $a = c$. On appelle "forme réduite" une telle forme.*

Comme $(a, b, a) \sim (a, -b, a)$, le lemme 1 nous assure que quitte à changer le signe de b dans le cas $a = c$, toute forme positive de discriminant < 0 est équivalente à une forme réduite. Il ne reste plus qu'à montrer l'unicité.

Lemme 3. *Soit $q = (a, b, c)$ une forme réduite. On dit qu'un vecteur (x, y) de $\mathbf{Z}^2$ est primitif si $pgcd(x, y) = 1$. L'entier a est le plus petit entier tel qu'il existe $(x, y) \in \mathbf{Z}^2$ primitif, avec $q(x, y) = a$. De plus :*
Si $a < c$, $a = q(u)$ pour exactement 2 vecteurs $u \in \mathbf{Z}^2$. Dans ce cas, c est la seconde plus petite valeur telle qu'il existe $(x, y) \in \mathbf{Z}^2$ primitif avec $q(x, y) = c$.
De plus, $c = q(v)$ pour exactement 2 vecteurs primitifs $v \in \mathbf{Z}^2$ si $b \neq a$, et 4 si $b = a$.
Si $a = c$, $a = q(u)$ pour exactement 4 vecteurs primitifs $u \in \mathbf{Z}^2$ si $b \neq a$, et 6 si $b = a$.

Démonstration. Soit $(x, y) \in \mathbf{Z}^2$ un vecteur primitif, si $y = 0$, on a $x = \pm 1$ et $q(\pm 1, 0) = a$. Pour montrer la minimalité de a, on va exploiter la relation : $4aq(x, y) = (2ax + by)^2 - Dy^2$. Si $y \geq 2$, on a $aq(x, y) \geq -D$, or $D \geq 3ac$ car $|b| \leq a \leq c$. On a donc $q(x, y) \geq 3c > c$ dès que $|y| \geq 2$. On considère donc pour finir le cas $y = 1$ (le cas $y = -1$ s'en déduit immédiatement).
Comme $-a < b \leq a$, on a $|2ax + b| \leq |b|$ pour tout $x \in \mathbf{Z}$, avec égalité si et seulement si $x = 0$, ou si $b = a$ et $x = -1$. Ainsi, pour tout $x \in \mathbf{Z}$, $q(x, 1) \geq \frac{b^2 - D}{4a} = c$ avec égalité si, et seulement si, $x = 0$, ou $b = a$ et $x = -1$. Cela nous permet terminer la démonstration du lemme. □

Démonstration. (de l'unicité) Soient $q = (a, b, c)$, $q' = (a', b', c')$ deux formes réduites telles que $q' = q \cdot M$ avec $M \in SL_2(\mathbf{Z})$. Si il existe $(x, y) \in \mathbf{Z}^2$ primitif, $M \begin{pmatrix} x \\ y \end{pmatrix}$ l'est également. L'ensemble des valeurs que prend une forme sur les vecteurs primitifs est donc invariant par équivalence, de plus le nombre de solutions primitives de l'équation $n = q(x)$ où n est un entier fixé, est également invariant par équivalence. On en déduit que $a = a'$, en utilisant la minimalité de a établie au lemme précédent. De même $c = c'$ car si $a = q(x)$ a 2 solutions primitives, $c = c'$ est d'après le lemme précédent la seconde plus petite valeur primitive de$q$ et q', et si $a = q(x)$ a 4 ou 6 solutions, on a $c = a = a' = c'$.

Il reste à montrer que $b = b'$: si $c = a$, on a $b, b' > 0$ donc $b = b'$. On suppose donc maintenant $a < c$, le lemme précédent montre que $b = a$ si et seulement si $b' = a'$. On suppose donc maintenant $b, b' \neq a$. D'après le lemme précédent, les équations $c = q(x)$ et $a = q(c)$ ont chacune exactement deux

solutions primitives : $(\pm 1, 0)$ pour la première et $(0, \pm 1)$ pour la seconde. Comme M envoie les solutions de $c = q(x)$ et $a = q(x)$ sur celles de $c = q'(x)$ et $a = q'(x)$, on en déduit que $M = \pm I_2$. Dans tous les cas, on a $b = b'$. □

2.2 Liens avec les classes d'idéaux

Soit D un entier tel que $D \equiv 0, 1 \pmod 4$. On considère le sous-anneau $A_D = \mathbf{Z}(\alpha)$, avec $\alpha = \frac{1}{2}\sqrt{D}$ si $D \equiv 0 \pmod 4$, $\alpha = \frac{1+\sqrt{D}}{2}$ si $D \equiv 1 \pmod 4$, et où $\sqrt{D}$ désigne la racine carrée de D dont la partie imaginaire est positive si $D < 0$. Dans les deux cas, on a $Disc(A_D) = D$. On munit l'ensemble des idéaux fractionnaires de A_D de la relation d'équivalence suivante : soient I, I' deux idéaux fractionnaires de A_D, on a $I \sim I'$ s'il existe $z \in \mathbf{Q}(\sqrt{D})$ tel que $N(z) > 0$, et tel $I' = zI$. Cette relation d'équivalence est la même que celle précédemment introduite dans le cas $D < 0$, mais est plus fine dans le cas $D > 0$. Le but de cette partie est de construire une bijection entre les classes idéaux fractionnaires de A_D et $Cl(D)$.

Soit σ l'automorphisme non trivial de $\mathbf{Q}(\sqrt{D})$(dans le cas où $D < 0$, il s'agit de la conjugaison complexe). Soit I un idéal fractionnaire de A_D. Si $D > 0$, on dit qu'une $\mathbf{Q}$-base (u, v) de I est directe, si le déterminant $\begin{vmatrix} u & v \\ \sigma(u) & \sigma(v) \end{vmatrix}$ est positif. Si $D < 0$, on dit qu'une $\mathbf{Q}$-base (u, v) de $\mathbf{Q}(\sqrt{D})$ est directe, si le déterminant $\begin{vmatrix} u & v \\ \sigma(u) & \sigma(v) \end{vmatrix}$ a une partie imaginaire positive. Soit (u, v) une $\mathbf{Z}$-base directe de I. On a $\begin{vmatrix} u & v \\ \sigma(u) & \sigma(v) \end{vmatrix} = \sqrt{D}N(I)$. On considère l'application $q_{u,v} : \mathbf{Z}^2 \to \mathbf{Q}$ définie par $q_{u,v}(x, y) = \frac{N(xu+yv)}{N(I)}$.

Proposition 11. *$q_{u,v}$ est une forme quadratique binaire entière de discriminant D ; de plus, si $D < 0$, $q_{u,v}$ est positive.*

Démonstration. Pour tout $(x, y) \in \mathbf{Z}^2$, on a $xu + yv \in I$. Or pour tout $k \in I$, $N(I)$ divise $N((k)) = \pm N(k)$, donc $q_{u,v}$ ne prend que des valeurs entières. On a $q_{u,v} = ax^2 + bxy + cy^2$, avec $a = \frac{u\sigma(u)}{N(I)} = \frac{N(u)}{N(I)}$, $b = \frac{u\sigma(v)+v\sigma(u)}{N(I)}$, et $c = \frac{v\sigma(v)}{N(I)} = \frac{N(v)}{N(I)}$. $q_{u,v}$ est donc une forme quadratique binaire entière, et si $D < 0$, on a clairement $a > 0$. De plus,

$$Disc(q_{u,v}) = \frac{(u\sigma(v) + v\sigma(u))^2 - 4u^2v^2\sigma(u)^2\sigma(v)^2}{N(I)^2} = \frac{1}{N(I)^2}\begin{vmatrix} u & v \\ \sigma(u) & \sigma(v) \end{vmatrix}^2,$$

et $\begin{vmatrix} u & v \\ \sigma(u) & \sigma(v) \end{vmatrix} = \sqrt{D}N(I)$, donc $Disc(q_{u,v}) = D$. □

Proposition 12. *La classe de la forme $q_{u,v}$ ne dépend pas du choix de la base (u, v).*

Démonstration. Soit (u', v') une autre base directe de I. Comme (u, v) et (u', v') sont directes, il existe $M = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in SL_2(\mathbf{Z})$ tel que :
$\begin{pmatrix} u' & v' \\ \sigma(u') & \sigma(v') \end{pmatrix} = \begin{pmatrix} u & v \\ \sigma(u) & \sigma(v) \end{pmatrix} M$, on a alors, $q_{u',v'} = q_{u,v} * M$. *Ainsi* $q_{u',v'}$ et $q_{u,v}$ appartiennent à la même classe. On peut à présent noter q_I la classe des $q_{u,v}$ où (u, v) est une base directe de I. □

Proposition 13. *La classe q_I ne dépend pas de la classe de I dans $Cl(A_D)$.*

Démonstration. Soit I un idéal fractionnaire de A_D, et soit $z \in \mathbf{Q}(\sqrt{D})$ tel que $N(z) > 0$.
Soit (u, v) une base directe de I, on a $\begin{vmatrix} zu & zv \\ \sigma(z)\sigma(u) & \sigma(z)\sigma(v) \end{vmatrix} = N(z)\sqrt{D}N(I) = \sqrt{D}N((z))N(I) = \sqrt{D}N(zI)$, car la norme est multiplicative pour les idéaux. (zu, zv) est donc une base directe de zI.
Ainsi, $q_{zu,zv}$ est un représentant de q_{zI}, on a $q_{zu,zv}(x, y) = \frac{N(zux+zvy)}{N(zI)} = \frac{N(ux+vy)}{N(I)} = q_{u,v}(x, y)$, qui est un représentant de q_I. On en déduit que $q_I = q_{zI}$. □

Théorème 6. *(Dedekind) L'application qui, à la classe de I dans A_D associe la classe q_I, est bijective.*

Démonstration. Commençons par montrer la surjectivité. Soit $Q = (a, b, c)$ une forme quadratique binaire entière, on va montrer que $I = a\mathbf{Z} + \frac{b-\sqrt{D}}{2}\mathbf{Z}$ est un idéal de A_D. Il s'agit de vérifier que $a\alpha \in I$, et $\alpha\frac{b-\sqrt{D}}{2} \in I$. On a $\frac{b-\sqrt{D}}{2} - \alpha \in \mathbf{Z}$, donc $a\alpha \in I$. D'autre part, $a(\frac{b-\sqrt{D}}{2a})^2 - b\frac{b-\sqrt{D}}{2a} + c = 0$, donc $(\frac{b-\sqrt{D}}{2})^2 \in I$ et $\alpha\frac{b-\sqrt{D}}{2} \in I$.
On pose $u = a$ et $v = \frac{b-\sqrt{D}}{2}$. Soit $z \in A_D$ tel que $N(z)$ soit du signe de a. Si a est positif (ce qui est toujours le cas lorsque $D < 0$), on peut par exemple prendre $z = 1$, sinon on peut prendre $z = \sqrt{D}$. Dans ce cas, (zu, zv) est une base directe de zI, car $\begin{vmatrix} zu & zv \\ \sigma(zu) & \sigma(zv) \end{vmatrix} = N(z)\begin{vmatrix} a & \frac{b-\sqrt{D}}{2} \\ a & \frac{b+\sqrt{D}}{2} \end{vmatrix} = a\sqrt{D}N(z)$, et $N(z)$ est du signe de a, donc $aN(z)$ est positif. On a de plus, $aN(z) = n(zI)$. On en déduit que
$q_{zu,zv} = \frac{N(z)}{N(zI)}N(ax + \frac{b-\sqrt{D}}{2}y) = \frac{1}{a}(a^2x^2 + abxy + y^2\frac{b^2-D}{4}) = Q(x, y)$.
Montrons maintenant l'injectivité. Soient I, J deux idéaux fractionnaires de A_D tels que $q_I = q_J$. Soient (u_1, v_1) et (u_2, v_2) leur base respective. Quitte à changer de base, on peut supposer $q_{u_1,v_1} = q_{u_2,v_2}$. On va montrer qu'il existe $z \in A_D$ tel que $I = zJ$, et tel que $N(z) > 0$. Les racines de $q_{u_1,v_1}(1, y)$ sont $-\frac{u_1}{v_1}$ et $-\frac{\sigma(u_1)}{\sigma(v_1)}$. On a donc $\frac{u_1}{v_1} = \frac{u_2}{v_2}$ ou $\frac{u_1}{v_1} = \frac{\sigma(u_2)}{\sigma(v_2)}$.
Dans le premier cas, on pose $z = \frac{u_1}{u_2} = \frac{v_1}{v_2}$, on a alors $u_1 = zu_2$ et $v_1 = zv_2$

et donc $I = zJ$. De plus $\begin{vmatrix} u_1 & v_1 \\ \sigma(u_1) & \sigma(v_1) \end{vmatrix} = N(z) \begin{vmatrix} u_2 & v_2 \\ \sigma(u_2) & \sigma(v_2) \end{vmatrix}$, les bases (u_1, v_1), (u_2, v_2) étant directes, on en déduit $N(z) > 0$.
Dans le second cas, on pose $z = \frac{u_1}{\sigma(u_2)} = \frac{v_1}{\sigma(v_2)}$, on a $\begin{vmatrix} u_1 & v_1 \\ \sigma(u_1) & \sigma(v_1) \end{vmatrix} = N(z) \begin{vmatrix} \sigma(u_2) & \sigma(v_2) \\ u_2 & v_2 \end{vmatrix}$. Comme les bases sont directes, on en déduit $N(z) < 0$. On a également $\frac{1}{N(J)}(u_2x+v_2y)(\sigma(u_2)x+\sigma(v_2)y) = q_{u_2,v_2}(x,y) = q_{u_1,v_1}(x,y)$, donc $\frac{1}{N(J)}(u_2x+v_2y)(\sigma(u_2)x+\sigma(v_2)y) = \frac{z\sigma(z)}{N(I)}(u_2x+v_2y)(\sigma(u_2)x+\sigma(v_2)y)$. On en déduit $N(I) = N(J)N(z)$, ce qui contredit $N(z) < 0$. Le deuxième cas est donc impossible. □

Corollaire 1. *Le nombre de classe d'idéaux d'un corps quadratique est fini. De plus, la preuve précédente nous donne un système de représentants de l'ensemble des classes d'idéaux : les idéaux de la forme* $(za, z\frac{b-\sqrt{D}}{2})$*, où* $z = 1$*,si* $a > 0$ *et* $z = \sqrt{D}$ *si* $a < 0$.

Proposition 14. *La classe d'idéal de* I *est inversible si et seulement si la classe d'idéal de* q_I *est primitive.*

Démonstration. Soit $q_I = ax^2 + bxy + cy^2$, I est de la forme $za\mathbf{Z} + z\frac{b-\sqrt{D}}{2}\mathbf{Z}$, où $z = 1$, si $a > 0$ et $z = \sqrt{D}$ si $a < 0$. L'idéal $J = I\sigma(I)$ est le groupe abélien engendré par $z^2a^2, az^2\frac{b-\sqrt{D}}{2}, az^2\frac{b+\sqrt{D}}{2}$, et $z^2\frac{b-\sqrt{D}}{2}\frac{b+\sqrt{D}}{2} = z^2ac$. On a $J = az^2(pgcd(a,b,c)\mathbf{Z} + \frac{b+\sqrt{D}}{2}\mathbf{Z})$ car $\frac{b-\sqrt{D}}{2} + \frac{b+\sqrt{D}}{2} = b$. Si q_I est primitive, on a $J = (az^2)$, et $N(az^2) > 0$. La classe de J est donc inversible.
Réciproquement, on considère l'idéal $K = J\sigma(J)$. On montre de la même manière qu'on a $K = a^2z^4pgcd(a,b,c)(pgcd(a,b,c)\mathbf{Z} + \frac{b+\sqrt{D}}{2}\mathbf{Z}) = az^2pgcd(a,b,c)J$. Si I est inversible, $\sigma(I)$ et J le sont aussi. On a donc $\sigma(J) = J = (az^2pgcd(a,b,c))$, comme $J = az^2(pgcd(a,b,c)\mathbf{Z} + \frac{b+\sqrt{D}}{2}\mathbf{Z})$, on a donc $pgcd(a,b,c) = 1$ et q_I est primitive. □

Corollaire 2. *On dit que l'entier* $D \equiv 0, 1 \mod 4$ *est un discriminant fondamental si toutes les formes de discriminant* D *sont primitives.* D *est fondamental si et seulement si tout idéal non nul de* A_D *est inversible. Dans ce cas* A_D *est l'anneau des entiers de* $\mathbf{Q}(\sqrt{D})$*.*

3 Formule analytique du nombre de classes de Dirichlet

L'objet de cette section est de prouver l'inégalité de Polya-Vinogradov sur les caractères de Dirichlet (théorème 7), et la formule analytique du nombres de classes de Dirichlet (théorème 8), qui relie de manière explicite les quantités arithmétiques d'un corps quadratique à une valeur remarquable d'une certaine fonction de la variable complexe.

3.1 Caractères de Dirichlet

Définition 14. *On appelle* caractère de Dirichlet *modulo D tout morphisme de groupes χ de $(\mathbf{Z}/D\mathbf{Z})^\times$ dans $\mathbf{S}^1 = \{z \in \mathbf{C}\ ;\ |z| = 1\}$.*

On remarque qu'étant donné un entier D, et d un diviseur de D, on a une projection naturelle :

$$(\mathbf{Z}/D\mathbf{Z})^\times \xrightarrow{\pi} (\mathbf{Z}/d\mathbf{Z})^\times$$

et donc qu'un caractère χ_d modulo d induit un caractère $\chi_d \circ \pi$ modulo D. On dira alors qu'un caractère modulo D est primitif s'il n'est induit par aucun caractère modulo d pour $d|D$; D est alors appelé le *conducteur* de χ.

Le symbole de Legendre

Définition 15. *Pour $D \in \mathbf{N}^*$, on définit le symbole de Legendre associé à D par :*

$$\left(\frac{n}{D}\right) = \begin{cases} 0 & \text{si } D|n \\ 1 & \text{si } n \text{ est un carré non nul modulo } D \\ -1 & \text{sinon} \end{cases}$$

Il est clair que le symbole $\left(\frac{n}{D}\right)$ ne dépend que de la classe de n modulo D ; de plus on vérifie sans difficulté que ce symbole est multiplicatif en n : le symbole de Legendre définit ainsi un caractère de Dirichlet modulo D. Notons que comme le morphisme $x \longmapsto x^2$ de $(\mathbf{Z}/D\mathbf{Z})^\times$ a pour noyau $\{\pm 1\}$, son image est d'indice 2, et donc exactement la moitié des résidus non nuls modulo D sont des carrés dans $(\mathbf{Z}/D\mathbf{Z})^\times$.
Remarquons que la valeur du symbole de Legendre $\left(\frac{d}{p}\right)$ nous donne la décomposition de (p) dans l'anneau des entiers de $\mathbf{Q}(\sqrt{(}d))$: $\left(\frac{d}{p}\right) = 0$ correspond au cas ramifié, $\left(\frac{d}{p}\right) = 1$ correspond au cas décomposé et le cas $\left(\frac{d}{p}\right) = -1$ correspond au cas inerte. Il est en fait plus pratique de lire cette information sur un caractère modulo d, multiplicatif en la classe de p modulo d ; c'est rendu possible par le résultat suivant, que l'on admettra :

Proposition 15. *(Loi de réciprocité quadratique)*
Soient p, q deux nombres premiers impairs. On a :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

On a de plus $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Revenons à l'étude générale des caractères :

Lemme 4. *Pour un caractère non trivial de conducteur fixé, les sommes partielles $S_n = \sum_{k\leq n} \chi_D(k)$ sont bornées.*

Démonstration. En effet, si $r \in \mathbf{N}$ est un entier arbitraire et v premier à D, on a :

$$\sum_{k=r}^{r+D-1} \chi_D(k) = \sum_{k=r}^{r+D-1} \chi_D(vk) = \chi_D(v) \sum_{k=r}^{r+D-1} \chi_D(k)$$

car la multiplication par v est une bijection de $(\mathbf{Z}/D\mathbf{Z})^*$.
Le caractère χ_D étant non trivial, on peut trouver un v tel que $\chi_D(v) \neq 1$ et donc $\sum_{k=r}^{r+D-1} \chi_q(k) = 0$, et ainsi pour tout $n \in \mathbf{N}$, $|S_n| \leq |(\mathbf{Z}/D\mathbf{Z})^*| \leq \varphi(D) \leq |D|$. □

On va en fait affiner ce résultat en donnant une borne plus fine sur la dépendance en D de la taille de ces sommes partielles :

Théorème 7. *(Inégalité de Polya-Vinogradov)*
Soit χ un caractère de Dirichlet primitif modulo D. On a, $\forall n \in \mathbf{N}$,

$$\left| \sum_{k\leq n} \chi(k) \right| \leq \sqrt{D} \ln(D) \ .$$

Démonstration. On définit la somme de Gauss associée à χ :

$$G(n,\chi) = \sum_{k=0}^{D-1} \chi(k) e^{2\pi i k n/D}$$

On réécrit χ comme somme de sa série de Fourier :

$$\chi(k) = \sum_{n=0}^{D-1} \hat{\chi}(n) e^{2\pi i k n/D}$$

où $\hat{\chi}(k) = \frac{1}{D} \sum_{k=0}^{D-1} e^{-2\pi i k n/D} = \frac{1}{D} G(-k,\chi)$; la vérification de la formule d'inversion de Fourier utilisée ici est immédiate. Si n est premier à D, $k \longmapsto kn$ est une bijection de $(\mathbf{Z}/D\mathbf{Z})^\times$, par un changement de variable $u = kn$:

$$G(n,\chi) = \sum_{k=0}^{D-1} \chi(k) e^{2\pi i k n/D} = \overline{\chi(n)} \sum_{k=0}^{D-1} (\chi(u) e^{2\pi u/D} = \overline{\chi(n)} G(1,\chi)$$

On affirme que le résultat reste vrai même si n n'est pas premier à D : on note $\lambda = pgcd(n,D)$, de telle sorte que $n = \lambda p$ et $D = \lambda q$, $p \wedge q = 1$. Alors :

$$G(n,\chi) = \sum_{k=0}^{D-1} \chi(k) e^{2\pi i k p/q} = \sum_{u=0}^{\lambda-1} \sum_{k=0}^{q-1} \chi(uq+k) e^{2\pi i u} e^{2\pi i k p/q}$$

Par le même argument que précédemment, en calculant la première somme géométrique :

$$G(n,\chi) = \sum_{u=0}^{\lambda-1} \chi(uq) \sum_{k=0}^{q-1} \chi(k) e^{2\pi i k p/q} = \overline{\chi(p)} \frac{1}{1-\chi(1)e^{2\pi i p/q}} \sum_{u=0}^{\lambda-1} \chi(uq)$$

La dernière somme est nécessairement nulle car sinon le caractère de $(\mathbf{Z}/\lambda\mathbf{Z})$ associé serait trivial et alors χ proviendrait en fait d'un caractère modulo q, ce qui est faux par hypothèse : on a bien $G(n,\chi) = 0 = \overline{\chi(n)} G(1,\chi)$.
Revenant à la formule d'inversion de Fourier, on a :

$$\chi(n) = \sum_{k=0}^{D-1} \frac{1}{D} \overline{\chi(-k)} G(1,\chi) e^{2\pi i k n/D} = \frac{G(1,\chi)}{D} \sum_{k=0}^{D-1} \chi(k) e^{2\pi i k n/D} \; puis$$

$$\sum_{n=1}^{N} \chi(n) = \frac{G(1,\chi}{D} \sum_{n=1}^{N} \sum_{k=0}^{D-1} \chi(k) e^{2\pi i k n/D} = \frac{G(1,\chi}{D} \sum_{k=0}^{D-1} \chi(k) \sum_{n=1}^{N} e^{2\pi i k n/D}$$

Soit alors $f(k) = \sum_{n=1}^{N} e^{2\pi i k n/D}$, de telle sorte que $\sum_{n=1}^{N} \chi(n) = \frac{G(1,\chi)}{D} \sum_{k=1}^{D-1} \chi(k) f(k)$.
On a alors :

$$\left| \sum_{n=1}^{N} \chi(n) \right| \leq \frac{|G(1,\chi)|}{D} \sum_{k=1}^{D-1} |f(k)|$$

Remarquant que $f(D-k) = \overline{f(k)}$ et donc que $|f(k)| = |f(D-k)|$, on a :

$$\sum_{k=1}^{D-1} |f(k)| \leq 2 \sum_{k \leq D/2} |f(k)|$$

Notant $r = e^{2\pi i k/D}$, on a :

$$|f(k)| = \left| \frac{1-r^{N+1}}{1-r} \right| \leq \frac{2}{|1-r|} \leq \frac{1}{\sin(\frac{\pi k}{D})} \leq \frac{D}{2k}$$

où l'on minore le sinus par la corde reliant 0 à $\frac{\pi}{2}$. Alors :

$$\left| \sum_{n=1}^{N} \chi(n) \right| \leq 2 \frac{|G(1,\chi)|}{D} \sum_{k \leq \frac{D}{2}} \frac{D}{2k} \leq |G(1,\chi)| \sum_{k \leq \frac{D}{2}} \frac{1}{k} \leq |G(1,\chi)| \ln(D)$$

où la dernière inégalité est vraie pour D suffisamment grand. Or on sait depuis Gauss que $|G(1,\chi)| = \sqrt{D}$: le résultat annoncé en découle. □

En fait, Landau a prouvé une majoration analogue pour les caractères non primitifs ; ainsi dans la suite on utilisera ce résultat sans se préoccuper de la primitivité des caractères.

3.2 Le symbole de Jacobi-Kronecker

Théorème-définition 2. *Soit D un* discriminant fondamental*, i.e. un entier $D \equiv 0, 1[4]$, qui soit le discriminant d'un certain corps quadratique. Il existe un unique caractère de Dirichlet modulo D à valeurs réelles :*

$$\chi_D : (\mathbf{Z}/D\mathbf{Z})^\times \longmapsto \{\pm 1\},$$

que l'on étend à $\mathbf{Z}$ par D-périodicité, tel que :

$$\chi_D(p) = 0 \Leftrightarrow p|D \Leftrightarrow p \text{ se ramifie dans } \mathcal{O}_K$$

$$\chi_D(p) = 1 \Leftrightarrow D \text{ est un carré modulo } 4p \Leftrightarrow p \text{ est décomposé dans } \mathcal{O}_K$$

$$\chi_D(p) = -1 \Leftrightarrow D \text{ n'est pas un carré modulo } 4p \Leftrightarrow p \text{ est inerte dans } \mathcal{O}_K$$

De plus, χ_D est impair : $\chi_D(-1) = (-1)$.
On appelle ce caractère le symbole de Jacobi-Kronecker*.*

Démonstration. L'unicité est claire ; pour l'existence la preuve s'appuie essentiellement sur ce qu'on a déjà vu sur la décomposition des nombres premiers dans les corps quadratiques et sur la loi de réciprocité quadratique. Nous donnerons seulement l'idée dans le cas $D = -l \leq 0$, $l \equiv 3[4]$.
Dans ce cas, montrons que $\chi_{-l}(\cdot) = \left(\frac{\cdot}{l}\right)$: en effet, pour les nombres premiers impairs, cela revient tout simplement à demander $\left(\frac{p}{l}\right) = \left(\frac{-l}{p}\right)$, ce qui découle facilement de la loi de réciprocité quadratique en décomposant l en produit de nombres premiers. Le cas $p = 2$ est laissé au lecteur. □

3.3 Formule du nombre de classes

Définition 16. *(Série L de Dirichlet) Soit (a_n) une suite de nombres complexes. On définit la série L associée à cette suite par :*

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},\ s \in \mathbf{C}$$

On peut définir une abscisse de convergence pour cette série, i.e. il existe un réel σ tel que la série converge absolument pour $\Re(s) > \sigma$ et diverge pour $\Re(s) < \sigma$; cette notion n'est pas sans rappeler le rayon de convergence des séries entières.
On peut aisément vérifier, par une transformation d'Abel, que si $\sum_{n \leq N} a_n = O(N^r)$ alors la série converge absolument sur le demi-plan $\Re(s) > r$. Ainsi, si $a_n = \chi_D(n)$, on a vu que les sommes partielles sont bornées, si bien que la série L associée au caractère χ_D, définie par $L(s, \chi_D) = \sum_{n=1}^{\infty} \frac{\chi_D(n)}{n^s}$ converge sur le demi-plan $\Re(s) > 0$, et y définit une fonction holomorphe.
On va prouver le résultat suivant dans le cas imaginaire :

Théorème 8. *(Dirichlet) Si K est un corps quadratique imaginaire de discriminant D, on a :*

$$\frac{2\pi h_D}{w_K\sqrt{|D|}} = L(1,\chi_D)$$

où w_K désigne l'ordre du groupe des unités du corps quadratique K associé à D.
Si K est quadratique réel, on a cette fois :

$$\frac{h_D \ln \varepsilon_D}{\sqrt{D}} = L(1,\chi_D)$$

où ε_D est ce qu'on appelle une unité fondamentale, i.e. est un générateur du groupe des unités de K. En d'autres termes, $\varepsilon_D = \frac{t+u\sqrt{D}}{2}$, où u et t sont les plus petites solutions entières de l'équation de Pell-Fermat $t^2 - Du^2 = 4$.

3.4 Fonction ζ d'un corps quadratique imaginaire

On définit la série L associée à un corps quadratique imaginaire K :

Définition 17.

$$\zeta_K(s) = \sum_I \frac{1}{N(I)^s}$$

où I parcourt les idéaux non nuls de $\mathcal{O}_K$. Pour $n \in \mathbf{N}$, le nombre d'idéaux de norme n est fini, égal par définition à a_n : on réécrit donc cette série sous la forme :

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

(Remarquer que si $K = \mathbf{Q}$ on récupère la fonction ζ de Riemann usuelle)

En s'inspirant de la factorisation de ζ en produit eulérien, on obtient un résultat analogue pour ζ_K :

Proposition 16.

$$\zeta_K(s) = \prod_P \frac{1}{1 - N(P)^{-s}} \ ,$$

le produit portant sur les idéaux premiers P de $\mathcal{O}_K$, et étant absolument convergent pour $\Re(s) > 1$.

La preuve est essentiellement la même que pour ζ, en remarquant que, $\mathcal{O}_K$ étant de Dedekind, $a_{mn} = a_m a_n$ si m et n sont premiers entre eux.
De plus, ζ_K admet un prolongement méromorphe avec un unique pôle simple, dont on sait exprimer le résidu à partir de quantités arithmétiques associées au corps de base :

Théorème 9. *Pour K quadratique imaginaire, ζ_K admet un prolongement méromorphe au demi-plan $\Re(s) > \frac{1}{2}$, avec pour unique pôle (simple) $s = 1$, de résidu :*

$$Res_{s=1}\, \zeta_K = \frac{2\pi h_D}{w_K \sqrt{|D|}}$$

où D est le discriminant de K.

Démonstration. L'idée de la preuve consiste à dénombrer les idéaux par classes, et à se ramener aux cas d'idéaux principaux pour les dénombrer comme des points entiers d'une partie du plan. On va alors aboutir à l'estimation suivante, ramenant l'étude de ζ_K à celle de ζ :

$$\zeta_K(s) = \frac{2\pi h_D}{w_K \sqrt{|D|}} \zeta(s) + \sum_{n=1}^{\infty} \frac{b_n}{n^s} \ ,$$

avec $\sum_{k \leq n} b_k = O(n^{\frac{1}{2}})$: le théorème en découle (on rappelle que ζ se prolonge en une fonction méromorphe sur $\mathbf{C}$ admettant un unique pôle simple en 1 de résidu 1).
Pour une classe C d'idéaux de $\mathcal{O}_K$, on note $a_{n,C}$ le nombre d'idéaux de C de norme n ; il est alors clair que $a_n = \sum_{C \in Cl(\mathcal{O}_K)} a_{n,C}$; on affirme le fait suivant, qui entraîne le théorème en sommant sur les $C \in Cl(\mathcal{O}_K)$:

$$\text{Pour } C \in Cl(\mathcal{O}_K), \ \sum_{k=1}^{n} a_{k,C} = \frac{2\pi n}{w_K \sqrt{|D|}} + O(n^{\frac{1}{2}}).$$

On se ramène alors au cas où les idéaux à compter sont principaux : si $I \in C$, $J \in C^{-1}$ (i. e. IJ est principal) , alors l'application $I \longmapsto IJ$ est une bijection entre les idéaux de C de norme n et les idéaux principaux inclus dans J de norme $nN(J)$. On fixe donc $J \in C^{-1}$; et on dénombre les idéaux principaux de norme $\leq nN(J)$. Un tel idéal a w_K générateurs, et comme $N((z)) = N(z)$ cela revient au même que de compter les éléments de $\mathcal{O}_K$ (vu comme réseau de $\mathbf{C}$) de module $\leq \sqrt{nN(J)}$.
On note Λ le réseau de $\mathbf{C}$ associé à l'idéal J. Si Π est un pavé fondamental pour Λ, et $r > 0$, on trouve $\delta > 0$ tel que $\Pi \subset \mathcal{D}(\delta)$ où $\mathcal{D}(\delta)$ est le disque ouvert centré en 0 de rayon δ. On note $f(r)$ le nombre de points de Λ contenus dans $\mathcal{D}(r)$, et $n(r)$ le nombre de translatés $v + \Pi$, pour $v \in \Lambda$, contenus dans $\mathcal{D}(r)$; clairement :

$$n(r) \leq f(r) \leq n(r + \delta)$$

On voit que si $v + \Pi$ rencontre $\mathcal{D}(r)$, alors $v + \Pi$ est contenu dans $\mathcal{D}(r + \delta)$: cela entraîne :

$$covol(\Lambda) n(r) \leq \pi r^2 \leq covol(\Lambda) n(r + \delta)$$

Ces encadrements donnent $\pi r^2 \leq covol(\Lambda) f(r) \leq \pi(r + \delta)^2$ soit $f(r) = \frac{\pi r^2}{covol(\Lambda)} + \mathcal{O}(r)$, et donc, en se rappelant que $covol(\Lambda) = \frac{1}{2} N(J) \sqrt{|D|}$ on a bien $\sum_{k \leq n} a_{k,C} = \frac{2\pi n}{w_K \sqrt{|D|}} + O(n^{\frac{1}{2}})$. □

3.5 Factorisation de ζ_K

On va maintenant factoriser la fonction ζ_K du corps quadratique imaginaire. Cela est rendu possible par le fait qu'on l'on puisse lire directement sur un caractère de Dirichlet comment, pour p premier, l'idéal $p\mathcal{O}_K$ se décompose en idéaux premiers dans $\mathcal{O}_K$; on en déduit le théorème suivant :

Théorème 10. *(Factorisation de ζ_K)*
Pour $\Re(s) > \frac{1}{2}$, on a $\zeta_K(s) = \zeta(s)L(s, \chi_D)$ où, pour $\Re(s) > 0$,

$$L(s, \chi_D) = \sum_{n=1}^{\infty} \frac{\chi_D(n)}{n^s}.$$

Démonstration. Pour commencer, la convergence de la série L dans le demi-plan $\Re(s) > 0$ est justifiée par le fait que pour un caractère non trivial, la somme partielle $S_n = \sum_{k \leq n} \chi_D(k)$ est bornée indépendamment de n, comme vu plus haut. De plus, on a le développement en produit eulérien $L(s, \chi_D) = \prod_{p \in \mathbf{P}} \frac{1}{1-\chi_D(p)p^{-s}}$ pour $\Re(s) > 1$, qui s'obtient de manière analogue à celui de ζ.
Par le théorème du prolongement analytique, il suffit alors de montrer le théorème dans le demi-plan $\Re(s) > 1$; on réarrange alors le produit eulérien de ζ_K selon les p ramifiés, inertes puis décomposés :

$$\zeta_K(s) = \prod_{p|D} \frac{1}{1-p^{-s}} \prod_{\chi_D(p)=1} \frac{1}{(1-p^{-s})^2} \prod_{\chi_D(p)=-1} \frac{1}{1-p^{-2s}}$$

Comme $1 - p^{-2s} = (1 - p^{-s})(1 + p^{-s})$, en gardant d'un côté pour chaque p un terme $1-p^{-s}$, et en remplaçant les signes que l'on a pour les p ne divisant pas D on voit que l'on récupère bien le produit des produits eulériens de ζ et $L(\chi_D)$. □

Démonstration. (de la formule de Dirichlet) En prenant les résidus en 1 des deux cotés de l'égalité donnée par la factorisation de ζ_K, on en tire la formule du nombre de classes pour un corps quadratique imaginaire, ce qui achève la preuve du théorème. □

Deuxième partie

Corps quadratiques et leurs groupes de classes

Dans cette partie, nous allons nous concentrer sur le cas quadratique, et donner un équivalent asymptotique de la somme des cardinaux des groupes de classes des corps quadratiques.

4 Théorème de Siegel sur les fonctions L

Soit χ_D un caractère de Dirichlet (donc réel) primitif modulo D ; on va prouver, par une méthode due à Goldfeld :

Théorème 11. *(Siegel)*
Pour tout $\epsilon > 0$, il existe C_ϵ indépendante de D telle que $L(1, \chi_D) > \frac{C_\epsilon}{D^\epsilon}$.

Corollaire 3. *Pour tout $\epsilon > 0$, il existe C_ϵ tel que, pour tout $D \leq 0$:*

$$h_D \geq C_\epsilon |D|^{1/2-\epsilon};$$

en particulier h_D tend vers $+\infty$ quand D tend vers $-\infty$.

Démonstration. Ce résultat découle immédiatement de l'estimation de Siegel puisque $h_D = \frac{w_K \sqrt{(|D|)} L(1,\chi_D)}{2\pi}$ par la formule du nombres de classes, il suffit alors de noter que $w_K = 2$ dès que $D \leq -5$ pour conclure. □

Il est cependant important de remarquer que cela ne s'applique dans le cas $D \leq 0$. En effet, on ne sait pas bien estimer l'ordre de croissance du terme $\ln \epsilon_D$ apparaissant dans le cas réel, et de fait, même s'il a été conjecturé, dès Gauss, que h_D tend vers $+\infty$ quand D tend vers $+\infty$; ce résultat reste encore à démontrer.

Pour établir la première partie du théorème, on définit, pour $\Re(s) > 0$ et $D_1, D_2 \leq 0$

$$f(s) = \zeta(s) L(s, \chi_1) L(s, \chi_2) L(s, \chi_1 \chi_2);$$

où χ_i est le symbole de Jacobi-Kronecker associé à D_i ; et le résidu de f en $s = 1$: $\lambda := L(1, \chi_1) L(1, \chi_2) L(1, \chi_1 \chi_2)$.
On fixe un $\epsilon > 0$; et on affirme le fait suivant : il existe un caractère de Dirichlet primitif modulo D_1 et $\beta \in]1 - \epsilon; 1[$ tels qu'on aie $f(\beta) \leq 0$, et ce pour tout D_2 et χ_2.
En effet, si aucune fonction $L(s, \chi)$ ne s'annule sur le segment réel $[1 - \epsilon; 1]$; il suffit d'avoir $\zeta(\beta) < 0$, et un tel β existe étant donné qu'on a, grâce au développement de Laurent en 1 de ζ ; $\lim_{x \to 1^-} \zeta(x) = -\infty$
Dans le cas où une certaine fonction $L(s, \chi)$ s'annule en $\beta \in]1 - \epsilon; 1[$, alors il nous suffit de prendre les D_1 et χ_1 associés, et le fait sera vrai quelque soient D_2 et χ_2.
On fixe alors un tel β, et pour $x \in \mathbf{R}$, on définit :

$$I(x) = \int_{2+i\mathbf{R}} f(s + \beta) \frac{x^s ds}{s(s+1)(s+2)(s+3)(s+4)}$$

On va d'abord établir deux résultats :

Proposition 17. *$I(x)$ est minorée en module indépendamment de x assez grand, à D_1 et D_2 fixés.*

Démonstration. Soient $t < -4$ et $R > 0$; si $u \in \mathbf{R}, u > 1$, on prend comme contour d'intégration le rectangle $R_{t,R}$ orienté dans le sens direct $[t - iR; 2 - iR; 2 + iR; t + iR]$:
Dans ce cas, le théorème des résidus appliqué sur $R_{t,R}$ donne, pour tous $R > 0, t < -4$:

$$\frac{1}{2i\pi}\int_{R_{t,R}} \frac{u^s ds}{s(s+1)(s+2)(s+3)(s+4)} = \frac{1}{24} - \frac{1}{3u} + \frac{1}{4u^2} - \frac{1}{6u^3} + \frac{1}{24u^4}$$

On évalue les contributions horizontales, par exemple celle sur le segment du bas : pour $s \in [t-iR; t+iR]$ on a $|s(s+1)(s+2)(s+2)(s+3)(s+4)| \geq R^5$ et, si $\sigma = \Re(s)$, $|u^s| = |u|^\sigma \leq u^2$ et donc $\left|\int_{t+iR}^{2+iR} \frac{u^s ds}{s(s+1)(s+2)(s+3)(s+4)}\right| \leq \frac{(2-t)u^2}{R^5}$, et ainsi, en appliquant le même genre de majoration à la contribution horizontale du haut et en faisant tendre R vers $+\infty$, il en résulte :

$$\frac{1}{2i\pi}\int_{2+i\mathbf{R}} \frac{u^s ds}{s(s+1)(s+2)(s+3)(s+4)}$$

$$= \frac{1}{2i\pi}\int_{t+i\mathbf{R}} \frac{u^s ds}{s(s+1)(s+2)(s+3)(s+4)} + \frac{1}{24} - \frac{1}{3u} + \frac{1}{4u^2} - \frac{1}{6u^3} + \frac{1}{24u^4}$$

De plus, pour $s \in t + i\mathbf{R}$, $|s(s+1)(s+2)(s+3)(s+4)| \geq C\,|t|^5$ avec C une constante universelle ; et $|u^s| \leq u^2$:
ainsi cette intégrale s'annule pour t tendant vers $-\infty$, d'où l'égalité :

$$\frac{1}{2i\pi}\int_{2+i\mathbf{R}} \frac{u^s ds}{s(s+1)(s+2)(s+3)(s+4)} = \frac{1}{24} - \frac{1}{3u} + \frac{1}{4u^2} - \frac{1}{6u^3} + \frac{1}{24u^4}$$

valable pour $u > 1$. Si $u < 1$, on effectue le même genre de calcul, en déplaçant cette fois l'axe d'intégration vers la droite : à nouveau l'intégrale s'annule quand l'axe part à l'infini, et donc en l'absence de pôles dans la partie de droite du plan, on obtient :

$$\int_{2+i\mathbf{R}} \frac{u^s ds}{s(s+1)(s+2)(s+3)(s+4)} = 0$$

.
On écrit alors $f(s+\beta) = \sum_{n\geq 1} \frac{a_n}{n^{s+\beta}}$; en prenant le logarithme dans la définition de f (possible sur le domaine simplement connexe $\Re(s) > 1$ puisque ni ζ ni les séries L ne s'y annulent, en vertu de leur expression comme produit eulérien sur ce domaine), il vient :

$$\ln(f(s)) = \ln(\zeta(s)) + \ln(L(s, \chi_1)) + \ln(L(s, \chi_2)) + \ln(L(s, \chi_1\chi_2))$$

Or pour $\Re(s) > 1, \ln(L(s,\chi)) = \ln(\prod_{p\in\mathcal{P}} \frac{1}{1-\chi(p)p^{-s}}) = \sum_{p\in\mathcal{P}} \sum_{n\in\mathbf{N}} \frac{\chi(p^n)}{np^{ns}}$; ceci étant valable pour n'importe quel caractère χ il vient :

$$\ln(f(s)) = \sum_{p\in\mathcal{P}} \sum_{n\in\mathbf{N}} \frac{(1+\chi_1(p^n))(1+\chi_2(p^n))}{np^{ns}}$$

Or, χ_1 et χ_2 étant à valeurs réelles, en prenant l'exponentielle de l'écriture ci-dessus, si $c_n = \frac{(1+\chi_1(p^n))(1+\chi_2(p^n))}{n}$,

$$f(s) = \prod_{p\in\mathcal{P},n\in\mathbf{N}} \exp(\frac{c_n}{p^{ns}}) = \prod_{p\in\mathcal{P},n\in\mathbf{N}} \sum_{k\in\mathbf{N}} \frac{c_n^k}{k!p^{nks}}$$

(les diverses interversions sont possibles car tout converge absolument sur $\Re(s) > 1$).
On voit que l'on récupère les a_n comme sommes de produits de puissances de c_n (éventuellement pondérés pas des $k!$) ; ainsi, les c_n étant positifs, on en conclut que les a_n sont tous positifs.
Par les calculs d'intégrale précédents, la somme $\sum_{n\geq 1} \int_{2+i\mathbf{R}} \frac{a_n x^s ds}{n^{s+\beta}s(s+1)(s+2)(s+3)(s+4)}$ est en fait finie ; on a alors :

$$\frac{1}{2i\pi}\int_{2+i\mathbf{R}} f(s+\beta)\frac{x^s ds}{s(s+1)(s+2)(s+3)(s+4)} = \sum_{n=1}^{[x]} a_n[\frac{1}{24} - \frac{n}{3x} + \frac{n^2}{4x^2} - \frac{n^3}{6x^3} + \frac{n^4}{24x^4}],$$

d'où $|I(x)| \geq \sum_{n=1}^{[x]} \frac{a_n}{25}$ pour x assez grand ; or f a un pôle en 1 donc $\sum_n a_n$ diverge. Ainsi pour x assez grand (borne dépendant de D_1 et D_2) on peut minorer $|I_x|$ par la constante que l'on veut. □

Lemme 5. *Au voisinage de la droite $\Re(s) = 1$ on a l'estimation :*

$$\forall s = \sigma + it \ |L(s,\chi_D)| \leq K\frac{|D|\,|s|}{\sigma}.$$

Sur la droite $\Re(s) = 0$, on a :

$$(1)\ \forall \delta > 0\ , \exists C_\delta > 0 \text{ telle que, } \forall\ t \in \boldsymbol{R}\ : |\zeta(it)| \leq C_\delta\,|t|^{\delta+\frac{1}{2}}$$

$$(2)\ |L(it,\chi_D)| = |D|^{3/2}O(\frac{|t|^{3/2}}{(1+\sinh(|t|))^{3/2}}),$$

où la dernière estimation est uniforme en D.

Démonstration. On a l'écriture suivante de l'équation fonctionnelle de ζ :

$$\zeta(s) = 2^s\ \pi^{s-1}\ \sin(\frac{\pi s}{2})\ \Gamma(1-s)\ \zeta(1-s)$$

On a, pour $t \in \mathbf{R}$, $|\Gamma(1-it)| = \sqrt{\frac{t\sinh(\pi|t|)}{\pi}}$, et donc :

$$|\zeta(it)| = \sqrt{\frac{t}{\pi\sinh(\pi t)}}\sinh(\frac{\pi t}{2})\,|\zeta(1+it)|\,;$$

et ainsi l'estimation voulue découle du fait bien connu que $|\zeta(1+it)| \leq C_\delta\,|t|^\delta$ pour une constante C_δ, pour tout $\delta > 0$.

Pour établir la première estimation sur L, on va sommer par parties la série L associée à χ ; on note à nouveau $S_n = \sum_{k\leq n}\chi_D(k)$. On a établi plus haut l'estimation grossière $|S_n| \leq \varphi(D) \leq |D|$. Or :

$$\sum_{n=1}^{N}\frac{\chi_D(n)}{n^s} = \sum_{n=1}^{N}\frac{S_n - S_{n-1}}{n^s} = \frac{S_N}{(N+1)^s} + \sum_{n=1}^{N} S_n(\frac{1}{n^s} - \frac{1}{(n+1)^s}).$$

$$\text{Donc}\left|\sum_{n=1}^{N}\frac{\chi_D(n)}{n^s}\right| \leq |D|\sum_{n=1}^{N}\frac{|s|}{n^{\sigma+1}};$$

et comme $\zeta(\sigma) \sim \dfrac{1}{\sigma-1}$, la limite $N \to \infty$ donne la borne souhaitée.

On veut maintenant estimer $L(s,\chi)$ au voisinage de $\Re(s) = 0$; pour cela on utilise l'équation fonctionnelle associée à la fonction L ; si $\Lambda(s,\chi) = (\frac{\pi}{|D|})^{\frac{-s}{2}}\,\Gamma(\frac{s}{2})\,L(s,\chi)$, alors on admet que $L(s,\chi)$ vérifie l'équation fonctionnelle suivante, avec $|\epsilon| = 1$, formé à partir de la somme de Gauss associée à χ :

$$\Lambda(s,\chi) = \epsilon\,\Lambda(1-s,\overline{\chi})$$

Cela donne alors, en isolant L et en prenant le module :

$$|L(it,\chi)| = \sqrt{\frac{D}{\pi}}\frac{\left|\Gamma(1-\frac{it}{2})\right|}{\left|\Gamma(\frac{1+it}{2})\right|}\,|L(1-it,\chi)|$$

Et des estimations analogues à celles pour ζ sur $\Re(s) = 0$ montrent que $\frac{\left|\Gamma(1-\frac{it}{2})\right|}{\left|\Gamma(\frac{1+it}{2})\right|} = O(\frac{|t|^{1/2}}{\sinh(|t|)^{3/2}})$pour t tendant vers $+\infty$, ce qui donne la dernière estimation voulue. □

Proposition 18.

$$\frac{1}{2i\pi}\int_{2+i\boldsymbol{R}} f(s+\beta)\frac{x^s ds}{s(s+1)(s+2)(s+3)(s+4)} = \frac{\lambda\,x^{1-\beta}}{(1-\beta)(2-\beta)(3-\beta)(4-\beta)(5-\beta)}$$

$+\frac{f(\beta)}{24} + O(\frac{(D_1D_2)^3x^{-\beta}}{1-\beta})$
lorsque D_1, D_2 tendent vers $-\infty$, et x tend vers $+\infty$.

Démonstration. Par la même méthode que précédemment, en décomposant f en série $\sum_n \frac{a_n}{n^s}$ qui est en fait finie, on voit qu'on peut décaler l'axe d'intégration à $\Re(s) = -\beta$, on obtient donc :

$$\frac{1}{2i\pi}\int_{2+i\mathbf{R}} f(s+\beta)\frac{x^s ds}{s(s+1)(s+2)(s+3)(s+4)} = \frac{\lambda\, x^{1-\beta}}{(1-\beta)(2-\beta)(3-\beta)(4-\beta)(5-\beta)}$$

$$+\frac{f(\beta)}{24} + \frac{1}{2i\pi}\int_{-\beta+i\mathbf{R}} f(s+\beta)\frac{x^s ds}{s(s+1)(s+2)(s+3)(s+4)}$$

Il nous reste alors à estimer l'intégrale sur $-\beta + \mathbf{R}$; par le lemme précédent, les bornes obtenues en $D\,|t|$ pour L sur $\Re(s) = 1$, combinées à l'estimée pour ζ (en prenant par exemple $\delta = \frac{1}{2}$), donnent pour f :

$$|f(it)| \leq C\,|D_1 D_2|^3\,\frac{|t|^{5/2}}{1+\sinh(|t|)^{9/2}}$$

En majorant $|x^s| \leq x^{-\beta}$ et en minorant $s(s+1)(s+2)(s+3)(s+4) \geq (1-\beta)\,|t|^4$, avec $t = \Im(s)$ et où le $1-\beta$ provient du deuxième terme du produit, on obtient, en formant la constante C à partir de l'intégrale indépendante de x, D_1, D_2, restante :

$$\left|\frac{1}{2i\pi}\int_{-\beta+i\mathbf{R}} f(s+\beta)\frac{x^s ds}{s(s+1)(s+2)(s+3)(s+4)}\right| \leq C(D_1D_2)^3\frac{x^{-\beta}}{1-\beta}$$

Cela termine la preuve de la proposition. □

Il nous reste à en déduire le théorème de Siegel : on voit que si l'on prend x suffisamment grand par rapport à D_1D_2, la quantité dans le $\mathcal{O}$ est aussi petite que l'on veut. Rappelons que $f(\beta) \leq 0$: ainsi, par la proposition 8, la quantité $\lambda x^{1-\beta}$ est minorée dès que $x \geq (D_1D_2)^{\frac{3}{\beta}}$; d'où pour x suffisamment grand :

$$\lambda \geq K(1-\beta)\frac{|D_1D_2|}{x}$$

On rappelle alors que D_1 est fixé ; pour contrôler le $L(1, \chi_1\chi_2)$ on utilise l'inégalité de Polya-Vinogradov :

$$L(1, \chi_1\chi_2) \leq C\sqrt{D_1D_2}\ln(D_1D_2),$$

et donc on a l'inégalité $L(1,\chi_2) \geq \frac{C'}{x}\frac{\sqrt{|D_2|}}{\ln|D_2|}$; en prenant x suffisamment grand on obtient bien $L(1,\chi_2) \geq \frac{C_\epsilon}{|D_2|^\epsilon}$, ce qui conclut la preuve.
Remarquons que même si l'on dispose ainsi d'une borne inférieure sur les quantités h_D et $h_D \ln \epsilon_D$, on ne sait toujours pas en donner un équivalent simple.
Cependant, on est capable de déterminer des équivalents des sommes $\sum_{D\leq N} h_D$ et $\sum_{D\leq N} h_D \ln \epsilon_D$; c'est l'objet de la section suivante.

5 Théorème de Siegel pour les formes quadratiques

Dans cette section on prouve le théorème de Siegel suivant, où h_D désigne toujours le nombre de classes de formes quadratiques entières primitives de discriminant D, avec $\epsilon_D = (t + u\sqrt{D})/2$, où t, u est la plus petite solution entière de $t^2 - Du^2 = 4$.

Théorème 12. *(Siegel)*

$$(1) \qquad \sum_{-N \leq D \leq 0, -D \text{ non carré}, D \equiv 0,1[4]} h_D = \frac{\pi}{18} N^{3/2} + O(N \ln N)$$

$$(2) \qquad \sum_{0 < D \leq N, D \text{ non carré}, D \equiv 0,1[4]} h_D \ln \epsilon_D = \frac{\pi^2}{18\zeta(3)} N^{3/2} + O(N \log N).$$

Noter que les discriminants non fondamentaux sont aussi pris en compte dans la somme, c'est-à-dire les discriminants ayant d'éventuels facteurs carrés ; et ainsi cette forme du théorème ne nous donne *a priori* pas d'information sur la somme des cardinaux des groupes de classes de corps quadratiques. Nous en obtiendrons cependant une estimation, qui ne sera démontrée que dans la dernière section :

Théorème 13. *Soit $h(K)$ l'ordre du groupe de classes d'idéaux du corps quadratique K, et soit $\mathcal{K}_X$ l'ensemble des corps quadratiques de discriminant $-X \leq D \leq 0$. On note $\Lambda = \prod_{p \in \mathbf{P}} (1 - p^{-2} - p^{-3} + p^{-4})$. Alors, pour $X \longrightarrow +\infty$:*

$$\sum_{K \in \mathcal{K}_X} h(K) = \frac{\Lambda \pi}{18} X^{3/2} + o(X^{3/2}).$$

On va en fait fournir deux démonstrations du théorème de Siegel, une première reposant essentiellement sur la formule analytique du nombre de classes de Dirichlet ; et une seconde plus géométrique, reposant sur des méthodes de comptage de points entiers dans certains domaines du plan, moins directe mais s'adaptant ensuite au cas cubique.

5.1 Preuve analytique

On va utiliser la formule analytique du nombre de classes et l'inégalité de Polya-Vinogradov, prouvées dans les préliminaires. Pour commencer, on définit

$$f_D = \frac{h_D}{\sqrt{D}} \log \epsilon_D,$$

$$\sigma_t = \sum_{n=1}^{N} (\frac{t}{n}) n^{-1},$$

$$P_r(n) = \sum_t (\frac{t}{n}).$$

Pour alléger les notations, on précise que dans cette section les sommes en t sont prises pour $t \equiv r[4]$, avec $r = 0$ ou 1, et les sommes en D pour $0 < D \leq N, D \equiv r[4], D \neq u^2$.

. D'abord, on évalue la somme des f_D, et on estime l'erreur commise par rapport à la somme des σ_t :

Proposition 19.

$$\sum_D f_D = \sum_t \sigma_t + O(\sqrt{N}\log N) = \sum_1^N \frac{1}{n} P_r(n) + O(\sqrt{N}\log N).$$

Démonstration. Par la formule du nombre de classes,

$$|f_D - \sigma_D| = \sum_{n=N+1}^{\infty} \frac{\chi_D(n)}{n},$$

où χ_D est le symbole de Jacobi-Kronecker, qui est non trivial.
On effectue une transformation d'Abel pour estimer cette somme :

$$\sum_{n=N+1}^{\infty} \frac{\chi_D(n)}{n} = \sum_{n=N+1}^{\infty} S_n(\frac{1}{n} - \frac{1}{n+1}) - \frac{S_N}{N+1},$$

où $S_n = \sum_{k=1}^n \chi_D(k)$.
Donc par l'inégalité de Polya-Vinogradov, on a une estimation de S_n

$$|f_D - \sigma_D| = O(\frac{1}{\sqrt{N}}\log N).$$

On voit aussi que $\sum_{t=u^2} \frac{(\frac{t}{n})}{n} = O(\log N)$, puisque tous les termes valent $\frac{1}{n}$, donc

$$\sum_D f_D - \sum_t \sigma_t = O(\sqrt{N}\log N),$$

puisque cette différence est dominée par $O(N)$ termes en $|f_D - \sigma_D|$ et $O(\sqrt{N})$ termes valant 1, correspondant aux indices de sommation qui sont des carrés. La deuxième égalité résulte juste d'une interversion dans l'ordre de sommation. □

Reste alors à estimer $P_r(n)$:

Proposition 20. *(1) $P_r(n) = O(\sqrt{n}\log n)$ quand n n'est pas un carré,*
(2) Quand $n = u^2$ est un carré avec u impair, $P_r(n) = \frac{\varphi(u)}{4u} N + uO(1)$, où φ est l'indicatrice d'Euler.
(3) Quand $n = u^2$ est un carré avec u pair, $P_r(n) = \frac{r\varphi(u)}{2u} N + uO(1)$,

Démonstration. (1) On discute selon la valeur de r et celle de n :
Quand $r = 0$, et n pair, $P_r(n) = 0$ puisque pour tout t, $\gcd(t, n) \neq 1$, donc le symbole de Jacobi est trivial.
Quand $r = 0$, et n impair, $(\frac{t}{n}) = (\frac{4}{n})(\frac{t/4}{n})$. Donc $P_r(n)$ est $(\frac{4}{n})$ fois la somme d'un caractère non trivial, qui est donc en $O(\sqrt{n}\log n)$ par l'inégalité de Polya-Vinogradov.
Quand $r = 1$, on écrit n comme $l \cdot s$, où l est impair, et s est une puissance de 2. Donc $(\frac{t}{n}) = (\frac{t}{l})(\frac{t}{s})$, mais $(\frac{t}{s})$ est une puissance de $(\frac{t}{2}) = 1$, donc on peut supposer que n est impair.
Soit $\chi_1(k) = (\frac{k}{n})(\frac{k}{2})$ et $\chi_2(k) = (\frac{-1}{k})\chi_1(k)$, donc $\chi_1(k), \chi_2(k)$ sont non nuls si et seulement si k est impair, de plus ils sont égaux si $k \equiv 1[4]$, et sont opposés si $k \equiv 3[4]$. Alors $P_r(n) = \frac{1}{2}\sum_{n=1}^{N}(\chi_1(k) + \chi_2(k))$. Comme χ_1 et χ_2 sont des caractères non triviaux, par l'inégalité de Polya leurs sommes sont d'ordre $O(\sqrt{n}\log n)$.
(2) $(\frac{t}{u^2}) = (\frac{t}{u})^2$, donc vaut 1 si $\gcd(t, u) = 1$, 0 sinon. Alors $P_r(n)$ est juste une somme de 1, prise sur les nombres premiers à u. Pour chaque u, il y a exactement $\varphi(u)$ termes, et on s'intéresse à ceux de la forme $4k+1$. Comme u est impair, on a donc $P_r(n) = \phi(u)/4 \cdot N/u + O(u)$.
(3) S'obtient de la même manière que (2). □

Maintenant, on peut estimer la somme des $P_r(n)/n$; on découpe en un terme correspondant aux indices carrés, et un second terme ; la proposition précédente permet d'estimer le second terme :

$$\left|\sum_{n\leq N, n\neq u^2} \frac{P_r(n)}{n}\right| \leq C\sum_{n\leq N}\frac{\ln(n)}{\sqrt{n}} \leq C\ln(N)\sqrt{N}, \text{ donc :}$$

$$\sum_{n\leq N}\frac{1}{n}P_r(n) = \sum_{u^2\leq N}\frac{1}{u^2}P_r(u^2) + O(\sqrt{N}\ln N) = \frac{N(r+3)\zeta(2)}{14\zeta(3)} + O(\sqrt{N}\ln N),$$

où la deuxième égalité résulte du lemme suivant :

Lemme 6. $\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}\cdot\zeta(s) = \zeta(s-1)$, *pour* $\Re(s) > 2$.

Démonstration. Par la formule d'inversion de Möbius, on a $\varphi(n) = \sum d|n\frac{\mu(d)}{d}n$, donc :

$$\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s} = \sum_{n=1}^{\infty}\sum_{d|n}\frac{\mu(d)}{d}\frac{1}{n^{s-1}} = \sum_{d=1}^{\infty}\frac{\mu(d)}{d}\sum_{n\in d\mathbf{N}}\frac{1}{n^{s-1}}$$

$$= \sum_{d=1}^{\infty}\frac{\mu(d)}{d^s}\sum_{n=1}^{\infty}\frac{1}{n^{s-1}} = \frac{\zeta(s-1)}{\zeta(s)},$$

où les diverses interversions sont justifiées par l'absolue convergence dans le demi-plan $\Re(s) > 2$. □

Donc on conclut que

$$T_N = \sum_D f_D = \frac{\pi^2 N(r+3)}{84\zeta(3)} + O(\sqrt{N}\log N).$$

Par transformation d'Abel, on a

$$\begin{aligned}\sum_D \sqrt{D} f_D &= \sum_D T_D(\sqrt{D} - \sqrt{D+1}) + T_N\sqrt{N+1} \\ &= \sum_D T_D \frac{1}{\sqrt{D}+\sqrt{D+1}} + T_N\sqrt{N+1} \\ &= \frac{\pi^2 N^{2/3}(r+3)}{126\zeta(3)} + O(\sqrt{N}\log N)\end{aligned}$$

Finalement, la première partie du théorème de Siegel s'obtient en prenant $r = 0$ et en remplaçant N par $4N$. Pour la deuxième partie on somme les résultats obtenus pour $r = 0$ et $r = 1$.
De plus, on a même obtenu un résultat un peu plus précis :

$$\sum_{0<k\leq N,\text{k non carré}} h_{4k} \ln \epsilon_{4k} = \frac{4\pi^2}{21\zeta(3)} N^{3/2} + O(N\log N).$$

On remarque que pour $D < 0$ la preuve est exactement la même, hormis le fait qu'on n'a plus de $\ln(\epsilon_D)$ dans la formule du nombre de classes, f_D est défini par $f_D = \frac{h_D}{\sqrt{D}}$.
Cependant, pour la preuve géométrique, on aura cette fois une différence notable entre les cas réel et imaginaire ; la preuve pour $D < 0$ repose en fait sur un argument assez simple, et on va ensuite utiliser une astuce géométrique pour se ramener à ce cas pour $D > 0$.

5.2 Preuve géométrique

On va montrer le théorème de Siegel en utilisant cette fois une méthode géométrique, avec cependant un moins bon terme d'erreur :

$$(1) \qquad \sum_{-N\leq D\leq 0,\text{-D non carré},D\equiv 0,1[4]} h_D = \frac{\pi}{18} N^{3/2} + o(N^{\frac{3}{2}});$$

$$(2) \qquad \sum_{0<D\leq N,\text{D non carré},D\equiv 0,1[4]} h_D \ln \epsilon_D = \frac{\pi^2}{18\zeta(3)} N^{3/2} + o(N^{\frac{3}{2}}).$$

La stratégie mise en oeuvre est la suivante : on souhaite compter des classes de formes quadratiques ; dans le cas imaginaire l'unicité de la forme réduite

nous donne un représentant canonique pour chaque classe ; on est alors ramené à compter des formes réduites de discriminant borné, que l'on identifie à des triplets $(a, b, c) \in \mathbf{Z}^3$, vérifiant certaines inégalités. On va alors estimer leur nombre par le volume du domaine associé de $\mathbf{R}^3$ à l'aide de sommes de Riemann, avec une complication technique due au défaut de compacité du domaine. Dans le cas réel, la non-unicité de la forme réduite va nous obliger à nous ramener au cas imaginaire.

Cas imaginaire

Soit $Q(x, y) = ax^2 + bxy + cy^2$ une forme binaire telle que $a \neq 0$ et $D = b^2 - 4ac < 0$. Soient $D = b^2 - 4ac$, soit $\tau = \xi + i\eta$ la racine de $ax^2 + bx + c$ dont la partie imaginaire est positive.
On dit que Q est réduite si |b|<a<c. Soit $F = \{\xi + i\eta | -\frac{1}{2} \leqslant \xi \leqslant \frac{1}{2}$ et $\xi^2 + \eta^2 \geqslant 1\}$.

Proposition 21. *Q est réduite si et seulement si $\tau \in F$.*

Démonstration. On a $b/a = -2\xi$, $c/a = \xi^2+\eta^2$. La condition $|b| < a$ est donc équivalente à $\frac{-1}{2} \leqslant \xi \leqslant \frac{1}{2}$, de même $a < c$ est équivalente à $\xi^2+\eta^2 \geqslant 1\}$. □

Proposition 22. *Soit $J = \iiint_{|b|<a<c, 0<4ac-b^2<1} dadbdc$, on a $J = \frac{\pi}{18}$.*

Démonstration. On effectue le changement de variable $(a, b, c) \to (D, \xi, \eta)$.
On a $D = -(2a\eta)^2$, donc $dD = -8a\eta d(a\eta)$ et $\frac{d(D,\xi,\eta)}{d(a,b,c)} = -\frac{a}{8\eta}\frac{d(b/a,c/a)}{d(\xi,\eta)}$.
Or $b/a = -2\xi$ et $c/a = \xi^2 + \eta^2$, donc $\frac{d(b/a,c/a)}{d(\xi,\eta)} = \begin{vmatrix} -2 & 0 \\ 2\xi & 2\eta \end{vmatrix} = -4\eta$, et $\frac{d(D,\xi,\eta)}{d(a,b,c)} = \frac{a}{2\eta} = \frac{\sqrt{-D}}{4\eta^2}$.
On a $J = \iiint_{D\in[-1,0],(\xi,\eta)\in F} \frac{\sqrt{-D}}{4\eta^2} dDd\eta d\xi$, donc :

$$J = \frac{1}{4}\int_{-1}^{0} \sqrt{-D}dD \iint_F \frac{d\xi d\eta}{\eta^2} = \frac{1}{6}\int_{-1/2}^{1/2} d\xi \int_{\sqrt{1-\xi^2}}^{\infty} 1/x^2 = \frac{1}{6}\int_{-1/2}^{1/2} \frac{d\xi}{\sqrt{1-\xi^2}} = \frac{\pi}{18}.$$

□

Soit $\theta > 0$, on définit $J_\theta := \iiint_{|b|\leq a\leq c, 0\leq 4ac-b^2\leq 1, a\geq\theta} dadbdc$.

L'ensemble $\{|b| \leq a \leq c, 0 \leq 4ac - b^2 \leq 1, a \geq \theta\}$ est compact car a et b sont bornés et $|c| \leq \frac{1}{4\theta}$ donc c l'est aussi. On a $\lim_{\theta\to 0} J_\theta = J$. On va maintenant donner une formule discrète pour J_θ.

Proposition 23. *Soit S_1 l'ensemble des formes Q à coefficients entiers réduites telles que $a \geq \theta N$ et $-D \leq N^2$, on a : $J_\theta = \lim_{N\to+\infty} \frac{1}{N^3} \sum_{Q\in S_1} 1$.*

Démonstration. Si $A_\theta = \Big\{(a,b,c) \in \mathbf{N}^3, |b| \leq a \leq c, 4\frac{a}{N}\frac{c}{N} - \frac{b^2}{N^2} \leq 1, a \geq \theta\Big\}$, on a :

$$\frac{\#(S_1)}{N^3} = \sum_{(a,b,c)\in A_\theta} \frac{1}{N^3}.$$

On reconnait ici une somme de Riemann, comme $\{|b| \leq a \leq c, 0 \leq 4ac - b^2 \leq 1, a \geq \theta\}$ est compact on obtient le résultat souhaité. □

Proposition 24. *Soit S l'ensemble des formes Q à coefficients entiers réduites telles que $a \geq \theta N$ et $-D \leq N^2$, on a : $J = \lim_{N\to+\infty} \frac{1}{N^3} \sum_{Q\in S} 1$.*

Lemme 7. *Soit S_0 l'ensemble des formes Q à coefficients entiers réduites telles que $a < \theta N$ et $D \leq N^2$ On a $\#(S_0) = \theta O(N^3)$*

Démonstration. On a $4ac - b^2 \leq N^2$, donc $4ac \leq N^2 + b^2$ et $c \leq \frac{N^2(1+\theta^2)}{a}$. On en déduit une majoration du cardinal de S_0 : on a $\#(S_0) \leq \sum_{a<\theta N} \sum_{|b|\leq a} \frac{N^2(1+\theta^2)}{a}$. Donc $\#(S_0) \leq \theta N \times 2N^2(1+\theta^2) = \theta O(N^3)$. □

Démonstration. (de la proposition) On a $S_0 \cap S_1 = \emptyset$ et $S = S_0 \cup S_1$. Donc $\#(S - S_1) = \#(S_0)$, et $\frac{1}{N^3}\#(S - S_1) = \theta O(1)$.
$\limsup_{N\to+\infty} |J_\theta - \frac{1}{N^3}\#(S)| = \theta O(1)$ En faisant tendre θ vers 0, on obtient $\lim_{N\to\infty} \frac{1}{N^3}\#(S) = J$. □

Proposition 25. *Soit H_{-D} le nombre de classes d'équivalence de formes quadratiques binaires. On considère ici toutes les classes, même celles qui ne sont pas primitives.*
On a $\sum_{D\leq N^2} H(-D) \sim \#(S) \sim \frac{\pi}{18} N^3$.

Démonstration. On sait qu'une forme de discriminant < 0 est proprement équivalente à une unique forme réduite, c'est-à-dire une forme (a,b,c) telle que :
$-a < b \leq a \leq c$, et telle que $b > 0$ si $a = c$.
En comptant le nombre de triplets de discriminant $0 < -D \leq N^2$ vérifiant ces conditions, on obtient donc le nombre de classes de discriminant $0 < -D \leq N^2$. Soit S' l'ensemble de ces triplets. Il reste à vérifier, qu'on a $\#(S) \sim \#(S')$, c'est à dire que $\#(S - S') = o(N^3)$. L'ensemble des triplets $(a, -a, c)$tels que $a \leq c$ et $4ac - a^2 \leq N^2$; et l'ensemble des triplets (c, b, c) tels que $b < 0 < c$ et $4c^2 - b^2 \leq N^2$ recouvrent $(S - S')$. On a dans le premier cas $O(N)$ choix pour a et c, donc son cardinal est un $O(N^2)$. Dans le second cas, on a également $O(N)$ choix pour c et $|b| \leq c$ donc son cardinal est également $O(N^2)$. On a donc

$$\sum_{D\leq N^2} H(-D) = \#(S') \sim \#(S).$$

□

Proposition 26. $\sum_{D\leq N} h_{-D} = \frac{\pi}{18\zeta(3)} N^{\frac{3}{2}} + o(N^{\frac{3}{2}})$.

Démonstration. On note $\mathcal{D}_D$ l'ensemble des diviseurs d de D tels que $\frac{D}{d}$ est un carré.
On a pour tout $D > 0$, $H_{-D} = \sum_{d\in\mathcal{D}_D} h_{-d}$. Soit $D = ap^2$, avec a sans facteurs carrés, On définit les fonctions $f(n) = h_{-n^2a}$ et $g(n) = H_{-n^2a}$. On a $g(n) = \sum_{d|n} f(d)$, donc en appliquant la formule d'inversion de Mobius :$f(n) = \sum_{d|n} \mu(d)g(n/d)$. On a donc $h_{-D} = \sum_{d|p} \mu(d)H_{-D/d^2}$.
On en déduit que $\sum_{D\leq N^2} h_{-D} = \sum_{D\leq N^2} \sum_{d|p} \mu(d)H_{-D/d^2}$. En inversant les sommes, on obtient :

$$\sum_{D\leq N^2} h_{-D} = \sum_{d\leq N^2} \mu(d) \sum_{D\leq N^2, D/d^2\in\mathbf{N}} H_{-D/d^2} = \sum_{d\leq N^2} \mu(d) \sum_{n\leq N^2/d^2} H_{-n}.$$

On va maintenant estimer cette somme en utilisant l'équivalent de $\sum_{n\leq N^2} H_{-n}$ que l'on a trouvé. Soit T un entier que l'on fixera plus tard, on a

$$\sum_{d\leq N^2} \mu(d) \sum_{n\leq N^2/d^2} H_{-n} = \sum_{d\leq T} \mu(d) \sum_{n\leq N^2/d^2} H_{-n} + \sum_{T<d\leq N^2} \mu(d) \sum_{n\leq N^2/d^2} H_{-n}.$$

On a pour le premier terme :

$$\sum_{d\leq T} \mu(d) \sum_{n\leq N^2/d^2} H_{-n} = \sum_{d\leq T} \mu(d) \frac{\pi}{18} (N/d)^3 + \epsilon(N/d)(N/d)^3,$$

où $x \to \epsilon(x)$ tend vers 0 lorsque x tend vers $+\infty$.
On majore le second terme par $\sum_{T<d\leq N^2} C(N/d)^3$ où C est une constante suffisamment grande. On a donc

$$|\frac{\pi}{18} \sum_{d\leq T} \frac{\mu(d)}{d^3} - \sum_{k\leq N^2} h_{-D}| \leq \sum_{d\leq T} \epsilon(N/d)(N/d)^3 + \sum_{T<d\leq N^2} C(N/d)^3.$$

Or on a $\sum_{d\leq T} \epsilon(N/d)(N/d)^3 \leq \zeta(3) max(\epsilon(N/d), d \leq T)N^3$, et par comparaison série intégrale, on a :

$$\sum_{T<d\leq N^2} C(N/d)^3 \leq CN^3(\frac{1}{T^2} - \frac{1}{N^2}).$$

En choisissant $T = \sqrt{N}$, on a :

$$\zeta(3)\ max(\epsilon(N/d), d \leq T)N^3 = o(N^3) \text{ et } CN^3(\frac{1}{T^2} - \frac{1}{N^2}) = CN^3(\frac{1-N}{N^2}) = o(N^3).$$

On a donc $\sum_{D\leq N^2} h_{-D} \sim \frac{\pi}{18} N^3 \sum_{d\leq N^2} \frac{\mu(d)}{d^3}$. On obtient ainsi le résultat souhaité : $\sum_{D\leq N} h_{-D} = \frac{\pi}{18\zeta(3)} N^{\frac{3}{2}} + o(N^{\frac{3}{2}})$. □

Cas réel

Soit $Q(x,y) = ax^2 + bxy + cy^2$ une forme bilinéaire telle que $a \neq 0$ et $D = b^2 - 4ac > 0$. Soient p_1, p_2 les racines de $Q(x,1)$ telles que $a(p_1 - p_2) > 0$.
Pour tout $\lambda > 0$, on définit :
$P_\lambda := |a|(\lambda^{-1}(x-p_1)^2 + \lambda(y-p_2)^2) = \alpha_\lambda x^2 + 2\beta_\lambda xy + \gamma_\lambda y^2$.
Le déterminant de P_λ étant négatif, on pose $\tau_\lambda = \xi_\lambda + i\eta_\lambda$ la racine de $P(x,1)$ telle que $\eta_\lambda > 0$.
On dit que Q est réduite s'il existe $\lambda > 0$ tel que P_λ soit réduite, c'est à dire tel que $2|\beta_\lambda| \leqslant \alpha_\lambda \leqslant \gamma_\lambda$.

Proposition 27. *Soit $H = \{\tau_\lambda \| \lambda > 0\}$. H est le demi-cercle reliant p_1 et p_2.*

Démonstration. On a $\lambda^{-1}(\tau_\lambda - p_1)^2 + \lambda(\tau_\lambda - p_2)^2 = 0$, donc
$2arg(\tau_\lambda - p_1) \equiv 2arg(\tau_\lambda - p_2)[\pi]$ et $arg(\tau_\lambda - p_1) + (\pi - arg(\tau_\lambda - p_2)) = \pi/2$.
L'angle formé par $[\tau, p_1]$ et $[\tau, p_2]$ est donc un angle droit. □

Proposition 28. *Q est réduite si et seulement si $H \cap F \neq \emptyset$.*

Démonstration. Cela se déduit immédiatement de la première proposition du cas imaginaire. □

L'ensemble $\{\lambda > 0 | P_\lambda \text{ est réduite}\}$ est donc soit vide, soit un intervalle $[\lambda_1, \lambda_2]$.
Soit $\mu(a,b,c)$ la longueur hyperbolique de l'arc $H \cap F$.

Proposition 29. *Soit $J := \iiint_{a,b,c|D<1,a>0} \mu(a,b,c) da db dc$, on a $J = \frac{\pi^2}{18}$.*

Démonstration. On a $\frac{\tau_\lambda - p_1}{\tau_\lambda - p_2} = \pm i\lambda$, car $\lambda^{-1}(\tau_\lambda - p_1)^2 + \lambda(\tau_\lambda - p_2)^2 = 0$.
La longueur hyperbolique étant invariante par homographies, on a :

$$\mu(a,b,c) = \int_{\lambda_1}^{\lambda_2} \frac{d\lambda}{\lambda} = \ln(\frac{\lambda_2}{\lambda_1}).$$

On a donc $J = \int_0^\infty (\iiint_{\tau \in F} \mu(a,b,c) da db dc) \frac{d\lambda}{\lambda}$. On fait le changement de variable $(a,b,c) \to (\alpha, \beta, \gamma)$, on a $\alpha/a = \lambda^{-1} + \lambda$, donc

$$\frac{d(\alpha,\beta,\gamma)}{d(a,b,c)} = (\lambda^{-1} + \lambda)\frac{d(\beta,\gamma)}{d(b,c)} = (\lambda^{-1} + \lambda)\frac{d(\beta/a, \gamma/a)}{d(p_1,p_2)}\frac{d(p_1,p_2)}{d(b/a, c/a)}.$$

Or $\beta/a = -\lambda^{-1}p_1 - \lambda p_2$, et $\gamma/a = \lambda p_1^2 + \lambda p_2^2$, donc

$$\frac{d(\beta/a, \gamma/a)}{d(p_1,p_2)} = \begin{vmatrix} -\lambda^{-1} & -\lambda \\ 2\lambda^{-1}p_1 & 2\lambda p_2 \end{vmatrix} = 2(p_1 - p_2).$$

De plus $b/a = -p_1 - p_2$ et $c/a = p_1 p_2$, donc $\frac{d(b/a,c/a)}{d(p_1,p_2)} = \begin{vmatrix} -1 & -1 \\ p_2 & p_1 \end{vmatrix} = p_2 - p_1$.
On a donc $\frac{d(\alpha,\beta,\gamma)}{d(a,b,c)} = -2(\lambda^{-1} + \lambda)$. Comme $D = \alpha\gamma - \beta^2$, on a

$$J = \frac{1}{2}\int_0^\infty \frac{d\lambda}{\lambda^2+1} \iiint_G d\alpha d\beta d\gamma = \frac{\pi}{4} \iiint_G d\alpha d\beta d\gamma.$$

Où G est l'ensemble $G = \{(\alpha,\beta,\gamma) | \alpha > 0, \alpha\gamma - \beta^2 \in [0,1], 2|\beta| \leq \alpha \leq \gamma\}$. On remarque que G est indépendant de λ. Pour calculer son volume, on applique le changement de variable $(\alpha,\beta,\gamma) \to (\alpha/2, \beta, \gamma/2)$. On retrouve ainsi l'intégrale utilisée dans la partie $D < 0$. On en déduit finalement $J = 4 \times \frac{\pi}{4} \times \frac{\pi}{18} = \frac{\pi^2}{18}$. □

Proposition 30. *On suppose $a > 0$, Q est réduite si et seulement si $a + c \leq \frac{|b|}{2}$.*

Démonstration. On sait que Q est réduite si et seulement si $H \cap F \neq \emptyset$, c'est à dire si et seulement si au moins un des points $\frac{\pm 1 + i\sqrt{3}}{2}$ est à l'intérieur du demi cercle H. Le centre du demi-cercle est $\frac{p_1+p_2}{2} = -\frac{b}{2a}$, son rayon est $\frac{p_1-p_2}{2} = \frac{\sqrt{D}}{2a}$.
Quand $b < 0$, Q est réduite si et seulement si $|-\frac{b}{2a} - \frac{1+i\sqrt{3}}{2}| < \frac{\sqrt{D}}{2a}$.
Quand $b > 0$, Q est réduite si et seulement si $|-\frac{b}{2a} - \frac{-1+i\sqrt{3}}{2}| < \frac{\sqrt{D}}{2a}$.
Dans le premier cas, en élevant au carré on a $b^2 + 4a^2 + 2ba \leq b^2 - 4ac$, c'est à dire $\frac{b}{2} \leq -c - a$.
Dans le second cas, on a $b^2 + 4a^2 - 2ba \leq b^2 - 4ac$, c'est à dire $-\frac{b}{2} \leq -c - a$.
Dans tous les cas Q est réduite si et seulement si $a + c \leq \frac{|b|}{2}$. □

Corollaire 4. *On a dans ce cas $a^2 \leq \frac{D}{3}, b^2 \leq \frac{4D}{3}, 4a|c| \leq D$.*

On a également montré au passage qu'à discriminant fixé le nombre de classes de formes réduites est fini.

Démonstration. On met au carré l'inégalité précédente, on a $4a^2 + 4c^2 + 8ac \leq b^2$.
Donc $3a^2 + (a+2c)^2 \leq b^2 - 4ac$, donc $3a^2 \leq D$ et on obtient la première inégalité.
On a également $b^2 \geq 16ac$ car $4a^2 + 4c^2 \geq 8ac$, donc $4b^2 - 16ac \geq 3b^2$ donc $4D \geq 3b^2$ et on a la deuxième inégalité.
L'inégalité $b^2 \geq 16ac$ nous donne également la troisième inégalité dans le cas $c > 0$, elle est évidente dans le cas $c \leq 0$. □

Proposition 31. *Soit λ tel que P_λ soit réduit, on a $a(\lambda + \lambda^{-1}) \leq 2\sqrt{\frac{D}{3}}$.*

Démonstration. Si P_λ est réduit, on a $\alpha_\lambda \leq \gamma_\lambda$ et $\alpha_\lambda \geq 2|\beta_\lambda|$, donc $D = \beta_\lambda^2 - \alpha_\lambda\gamma_\lambda \geq \alpha_\lambda^2 - \frac{1}{4}\alpha_\lambda^2 \geq \frac{3}{4}\alpha_\lambda^2$.
Comme $\alpha_\lambda > 0$, on en déduit $a(\lambda + \lambda^{-1}) = \alpha_\lambda \leq 2\sqrt{\frac{D}{3}}$. □

Soit $\theta > 0$, on définit $J_\theta := \iiint_{a,b,c|D\leq 1, a\geq\theta} \mu(a,b,c) da db dc$.
$\{D \leq 1, a \geq \theta\}$ est compact car d'après le corollaire 1, a et b sont bornés et $|c| \leq \frac{D}{4\theta}$, donc c l'est aussi. On a $\lim_{\theta\to 0} J_\theta = J$. On va maintenant donner une formule discrète pour J_θ.

Proposition 32. *Soit S_1 l'ensemble des formes Q à coefficients entiers réduites telles que $a \geq \theta N$, $D \leq N^2$. $J_\theta = \lim_{N\to+\infty} \frac{1}{N^3} \sum_{Q\in S_1} \mu(a,b,c)$*

Démonstration. La longueur $\mu(a,b,c)$ ne dépend que des racines de Q, on a donc $\mu(a,b,c) = \mu(\frac{a}{N}, \frac{b}{N}, \frac{c}{N})$. Or $\frac{1}{N^3}\sum_{Q\in S_1} \mu(\frac{a}{N}, \frac{b}{N}, \frac{c}{N})$ est une somme de Riemann, comme $\{D \leq 1, a \geq \theta\}$ est compact on obtient l'égalité souhaitée. □

Proposition 33. *Soit S l'ensemble des formes Q réduite à coefficients entiers de discriminant $D = b^2 - 4ac$ non carré, telles que $D \leq N^2$. On a $\lim_{N\to+\infty} \frac{1}{N^3}\sum_{Q\in S} \mu(a,b,c) = 2J = \frac{\pi^2}{9}$*

Lemme 8. *Soit $\epsilon > 0$, soit d la fonction qui a n associe son nombre de diviseurs positifs. On a $d(n) = o(n^\epsilon)$.*

Lemme 9. *Soit S_2 le sous ensemble de S_1 contenant les formes de discriminant carré. On a $\sum_{Q\in S_2} \mu(a,b,c) = o(N^3)$.*

Démonstration. Soit $Q \in S_1$, soit $\lambda \in [\lambda_1, \lambda_2]$, on a d'après la proposition 5 : $|\ln(\lambda)| \leq \ln(\lambda + \lambda^{-1}) \leq \ln(2) - \frac{1}{2}\ln(3) + \frac{\ln(D)}{2} - \ln(a)$.
Or $D \leq N^2$ donc $|\ln(\lambda)| \leq \ln(2) + \ln(N) - \ln(a) \leq \ln(\frac{2N}{a}) \leq \ln(\frac{2}{\theta})$.
On a donc $\mu(a,b,c) = \ln(\frac{\lambda_2}{\lambda_1}) \leq 2\ln(\frac{2}{\theta})$. $\mu(a,b,c)$ est majoré par une constante, il suffit donc maintenant de montrer que $\#(S_2) = o(N^3)$. Soit $D = h^2$, on a $4ac = b^2 - h^2$. On va distinguer les cas $b = \pm h$ et $b \neq \pm h$. Quand $b = \pm h$, on a nécessairement $c = 0$ car $a \neq 0$. On a dans ce cas $O(n)$ choix pour a car d'après le corollaire précédent, $a^2 \leq \frac{D}{3}$. On a également $O(n)$ choix pour b car $b^2 \leq \frac{4D}{3}$. Il y a donc $O(N^2)$ formes Q telles que $b = \pm h$.Quand $b \neq \pm h$, il y a $O(n^2)$ choix pour le couple (b,h). Dans ce cas a divise $b^2 - h^2$ et $b^2 - h^2 = O(N^2)$, on applique le lemme précédent avec $\epsilon < \frac{1}{2}$ et on a $o(N)$ choix pour a. Comme c est entièrement déterminé par (a,b,h), on a donc $o(N^3)$ choix de formes Q telles que $b \neq \pm h$. On a donc $\sum_{Q\in S_2} \mu(a,b,c) \leq 2\ln(\frac{2}{\theta})(o(n^3) + O(n^2)) = o(n^3)$ □

Lemme 10. *Soit S_0 l'ensemble des formes Q à coefficients entiers réduites telles que $a < \theta N$ et $D \leq N^2$.*
On a $\sum_{Q\in S_0} \mu(a,b,c) = \theta\ln(\theta^{-1})O(N^3)$.

Démonstration. On va étudier séparément le cas $|c| < 2N$ et $|c| \geq 2N$. Si $|c| < 2N$, on a $O(N)$ choix pour c, et toujours $O(N)$ pour b. On a de plus $\mu(a,b,c) \leq 2\ln(\frac{2N}{a})$. On découpe l'ensemble des valeurs possibles de a de la manière suivante : $a \in \cup_{k=0}^{+\infty}[\frac{\theta N}{2^{k+1}}, \frac{\theta N}{2^k}]$. On a :

$$\sum_{Q\in S_0,|c|<2N} \mu(a,b,c) = O(N^2)\sum_{k=0}^{+\infty}\sum_{a=\frac{\theta N}{2^{k+1}}}^{\frac{\theta N}{2^k}} 2\ln(\frac{2N}{a}).$$

Si $a \in [\frac{\theta N}{2^{k+1}}, \frac{\theta N}{2^k}]$, alors $\ln(\frac{2N}{a}) \leq \ln(\frac{2^{k+2}}{\theta})$. On a donc

$$\sum_{Q\in S_0,|c|<2N} \mu(a,b,c) = O(N^2)\sum_{k=0}^{+\infty}\frac{\theta N}{2^k}\ln(\frac{2^{k+2}}{\theta}) = O(N^3)\theta\ln(\theta^{-1}).$$

De plus :

$$\frac{d\lambda}{\lambda} = \frac{d(\frac{\tau-p_1}{\tau-p_2})}{\frac{\tau-p_1}{\tau-p_2}} = \frac{d(\tau-p_1)(\tau-p_2) - d(\tau-p_2)(\tau-p_1)}{(\tau-p_2)(\tau-p1)} = \frac{(p_1-p_2)d\tau}{(\tau-p_1)(\tau-p_2)}.$$

Or en calculant l'aire du triangle rectangle (p_1, p_2, τ) de deux façons différentes il vient $\eta(p_1-p_2) = (\tau-p_1)(\tau-p_2)$; et il est clair que $d\xi = sin(2\lambda)d\tau = \frac{2\tau-p_1-p_2}{2\eta}$ d'où

$$\frac{d\lambda}{\lambda} = \frac{(p_1-p_2)d\tau}{(\tau-p_1)(\tau-p_2)} = \frac{(p_1-p_2)d\xi}{\eta^2} = -\frac{\sqrt{D}d\xi}{2a\eta^2}.$$

On a donc :

$$\mu(a,b,c) = \int_{H\cap F}\frac{-\sqrt{(}D)d\xi}{2\alpha\eta^2} \leq \frac{N}{2a\eta_0^2}\int_{-\frac{1}{2}}^{\frac{1}{2}} d\xi = \frac{N}{2a\eta_0^2},$$

où $\eta_0 = min(\eta_\lambda; \lambda \in [\lambda_1, \lambda_2])$. Le point (η_0, ξ_0) est sur H, il vérifie donc l'equation suivante : $(\frac{p_1+p_2}{2}-\xi_0)^2+\eta_0^2 = (\frac{p_2-p_1}{2})^2$, c'est à dire $(\frac{b}{2a}+\xi_0)^2+\eta_0^2 = \frac{b^2-4ac}{2a}$. On en déduit $a(\xi_0^2+\eta_0^2)+b\xi+c = 0$.
Supposons c>0, comme $\xi_0 \in [\frac{-1}{2}, \frac{1}{2}]$, on a : $a\eta_0^2 \leq \frac{|b|}{2} - c$. D'après le corollaire précédent, on a $\frac{|b|}{2} \leq \frac{\sqrt{D}}{\sqrt{3}} < N$. Donc $a\eta_0^2 \leq N - c$ ce qui est absurde car $a > 0$ et $|c| \geq 2N$.
On a donc $|c| \leq 2N$, et $a\eta_0^2 \geq \frac{-a}{4} - \frac{|b|}{2} - c$. Or $a^2 \leq \frac{D}{3}$ et $|b| \leq 2\frac{\sqrt{D}}{\sqrt{3}}$, donc $\frac{-a}{4} - \frac{|b|}{2} \geq \frac{-N}{4\sqrt{3}} - \frac{N}{\sqrt{3}} \geq N$. On en déduit $a\eta_0^2 \geq -N - c$ et $2a\eta_0^2 \geq |c|$, car $c < 2N$. On obtient finalement $\mu(a,b,c) \leq \frac{N}{|c|}$. On a

$$\sum_{Q\in S_0,|c|\geq 2N}\mu(a,b,c) \leq \sum_{Q\in S_0,|c|\geq 2N}\frac{N}{|c|}.$$

On a toujours $O(N)$ choix pour b, donc :

$$\sum_{Q\in S_0,|c|\geq 2N} \mu(a,b,c) = O(N)\sum_{a=1}^{\theta N}\sum_{c=2N}^{\frac{N^2}{4a}} \frac{N}{c} = O(N^2)\sum_{a=1}^{\theta N} O(\ln(\frac{N}{a})),$$

donc $\sum_{Q\in S_0,|c|\geq 2N} \mu(a,b,c) = O(N^3)\theta\ln(\theta^{-1})$. □

Démonstration. (de la proposition) On a $S_0\cap S_1 = \emptyset$, $S\cap\{a>0\}\subset S_0\cup S_1$ et $(S_0\cup S_1)-(S\cap\{a>0\})\subset(S_2\cup S_0)$.
On en déduit $\frac{1}{N^3}|\sum_{S_1}\mu(a,b,c) - \sum_{S,a>0}\mu(a,b,c)| \leq \frac{1}{N^3}(\sum_{S_0}\mu(a,b,c) + \sum_{S_2}\mu(a,b,c))$.
Or on sait que si $Q\in S$, on a $-Q\in S$ et pour tout $Q\in S$, on a $a\neq 0$ et $\mu(a,b,c)=\mu(-a,-b,-c)$.
On a donc $\frac{1}{N^3}|2\sum_{S_1}\mu(a,b,c) - \sum_S \mu(a,b,c)| \leq \frac{1}{N^3}2(\sum_{S_0}\mu(a,b,c)+\sum_{S_2}\mu(a,b,c))$.
On déduit des deux lemmes précédents :

$$\limsup_{N\to+\infty} |2J_\theta - \frac{1}{N^3}\sum_S \mu(a,b,c)| = \theta\ln(\theta^{-1})O(1).$$

On fait maintenant tendre $\theta\to 0$, on a $\theta\ln(\theta^{-1})\to 0$ et $2J_\theta\to 2J$.
On obtient le résultat souhaité : $\lim_{N\to+\infty}\frac{1}{N^3}\sum_{Q\in S}\mu(a,b,c) = 2J = \frac{\pi^2}{9}$. □

Théorème 14. $\sum_{D\leq N} h_D\ln\epsilon_D \sim \frac{\pi^2}{18}N^{\frac{3}{2}}$,
la somme étant prise sur tous les $D\leq N$.

Lemme 11. *Etant donné une action d'un groupe G sur un ensemble E, on appelle domaine fondamental pour l'action de G tout sous ensemble de E contenant exactement 1 point par orbite. Soit $\mathcal{F}'$ l'ensemble $\mathcal{F}$ privé de la droite $\{Re(z)=1/2\}$ et de l'arc $\{e^{i\theta}, \frac{\pi}{3}\leq\theta<\frac{\pi}{2}\}$, $\mathcal{F}'$ est un domaine fondamental pour l'action de $SL_2(\mathbf{Z})$ sur le demi-plan.*

Démonstration. Soit $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. On remarque que pour tout $z\in\mathbf{C}, \Im(z>0$, on a $T\cdot z = z+1$ et $S\cdot z = -1/z$.
Soit $z\in\mathbf{C}, \Im(z)>0$, si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL_2(\mathbf{Z})$, on a $\Im(g\cdot z)>z$ si et seulement si $|cz+d|>1$. Ce n'est possible que pour un nombre fini de couples d'entier (c,d). On peut donc choisir un pointz_1 de l'orbite de z dont la partie imaginaire est maximale. Quitte à le translater en appliquant T, on peut supposer en plus qu'on a $-1/2\leq\Re(z_1)<1/2$. Comme $\Im(S\cdot z_1) = \frac{\Im(z_1)}{|z_1|^2}$ et $\Im(S\cdot z_1)\leq\Im(z_1)$, on en déduit $|z_1|\geq 1$. Si z_1 est sur l'arc $\{e^{i\theta}, \frac{\pi}{3}\leq\theta<\frac{\pi}{2}\}$, on applique S et on obtient un point de l'arc $\{e^{i\theta}, \frac{\pi}{2}\leq\theta<\frac{2\pi}{3}\}\subset\mathcal{F}'$. Ainsi toutes les orbites rencontrent $\mathcal{F}'$ en au moins 1 point.
Supposons qu'il existe $z,z'\in F'$ et $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL_2(\mathbf{Z})$ tels que $z' =$

$g \cdot z$. On suppose sans perte de généralité $Im(z') \geq Im(z)$, on a $|c|Im(z) \leq 1$. Comme $Im(z) > \sqrt{3}/2$, on en déduit $|c| < 2$.
Si $c = 0$, on a $ad = 1$, on a dans ce cas $\Im(z) = \Im(z')$ et comme $b \in \mathbf{Z}$, $z - z' \in \mathbf{Z}$ et $z = z'$.
Si $c = 1$, on a $|z + d| \leq 1$ donc soit $d = 0$, soit $d = 1$ et $z = j$. Si $d = 1$, on a $a - b = 1$ et $z' = a + j$, donc $z' = z$. Si $d = 0$, on a $|z| = 1$ et $z' = a - 1/z$, $-1/z$ étant le symétrique de z par rapport à l'axe imaginaire, on a donc $a = 0$ et $z = z'$.
$\mathcal{F}'$ est donc bien un domaine fondamental pour l'action de $SL_2(\mathbf{Z})$. □

Lemme 12. *Soit C l'union de l'ensemble des demi-droites verticales du plan complexe et de celui des demi-cercles de centre réel. C est stable sous l'action de $SL_2(\mathbf{Z})$.*

Il s'agit en fait des géodésiques pour la métrique hyperbolique, i.e. l'ensemble des trajectoires minimisant la longueur hyperbolique $ds = \frac{\sqrt{x^2+y^2}}{y}$.

Démonstration. On utilise le résultat classique suivant : $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ engendrent $SL_2(\mathbf{Z})$. Il suffit donc de vérifier la propriété pour ces deux matrices, ce qui est immédiat. □

Démonstration. (du théorème) Soit $Q = (a, b, c)$ une forme primitive de discriminant positif, on appelle G le groupe des matrices de $SL_2(\mathbf{Z})$ laissant Q invariant, ce sont les matrices de la forme $\pm M^l$, avec $M = \begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix}$ où t, u sont les plus petites solutions entières positives de $t^2 - Du^2 = 4$, et où l est entier.
L'action par homographie d'une matrice de G fixe p_1 et p_2. En effet $aup_1^2 + bup_1 + cu = 0$, donc

$$M \cdot p_1 = -M \cdot p_1 = \frac{\frac{t+bu}{2} p_1 - cu}{aup_1 + \frac{t-bu}{2}} = p_1.$$

M et $-M$ fixe p_1 et p_2, donc c'est également le cas pour toute matrice de G. On déduit du lemme précédent que H est également laissé fixe sous l'action de G. Soit $\epsilon_D := \frac{t+u\sqrt{D}}{2}$, soit $N \in SL_2(\mathbf{R})$ la matrice dont l'action par homographie est $z \to \frac{z-p_1}{z-p_2}$, on a déjà vu que cette homographie envoie H sur la demi-droite $\{\lambda i, \lambda > 0\}$. NMN^{-1} stabilise le demi-axe imaginaire et fixe 0 et $i\infty$ car M fixe p_1 et p_2. On en déduit que NMN^{-1} est de la forme $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$. En utilisant les formes explicites de N et M, on trouve :

$$\lambda = \frac{a}{\sqrt{D}}(-p_2 \frac{t - bu}{2} + p_1 p_2 au + cu + p_1 \frac{t + bu}{2})$$

$$= \frac{a}{\sqrt{D}}(\frac{-t\sqrt{D}}{2a} + 2cu - \frac{b^2u}{2a}) = \frac{-t - u\sqrt{D}}{2}.$$

On a donc $\lambda = -\epsilon_D$. Soit B un arc de H de longueur hyperbolique $2\ln\epsilon_D$, l'image de B sous l'action de N est un intervalle de la forme $[\alpha i, \beta i]$ avec $\ln(\beta) - \ln(\alpha) = 2\ln\epsilon_D$ car la longueur hyperbolique est invariante par homographie. Comme $NMN^{-1} \cdot (\lambda i) = \epsilon_D^2 \lambda i$, $N(B)$ est un domaine fondamental pour l'action de NGN^{-1} sur la demi-droite imaginaire. On en déduit que B est un domaine fondamental pour l'action de G sur H.
Soit $Q_k = (a_k, b_k, c_k)$, $1 \leq k \leq g$ l'ensemble des formes réduites équivalentes à Q. On note A_k l'arc A associé à la forme Q_k. A_k est équivalent à un arc de H. Comme B est fondamental, on peut choisir cet arc dans B. De cette manière on peut recouvrir B par des arcs équivalents aux A_k. En effet, le domaine $\mathcal{F}'$ étant fondamental pour l'action de $SL_2(\mathbf{Z})$ sur le demi plan, on en déduit que chaque élément de B appartient à l'orbite d'un unique élément de $\mathcal{F}'$. Les arcs A_k recouvrent donc B complètement, sans se chevaucher. La longueur hyperbolique étant invariante par homographie, on en déduit que

$$\sum_{1}^{g} \mu(a_k, b_k, c_k) = 2\ln\epsilon_D,$$

$$\sum_{b^2-4ac=D,(a,b,c)primitive} \mu(a_k, b_k, c_k) = 2h_D \ln\epsilon_D.$$

On pose maintenant $H_D := \sum_{k \in C_D} h_k \ln\epsilon_D$, on obtient finalement en utilisant l'équation précédente et la proposition 13,

$$\sum_{D \leq N^2} H_D \sim \frac{\pi^2}{18} N^3.$$

En appliquant exactement la même inversion que dans le cas imaginaire, on obtient finalement l'équivalence souhaitée :

$$\sum_{k \leq N} h_D \ln\epsilon_D \sim \frac{\pi^2}{18\zeta(3)} N^{\frac{3}{2}}.$$

□

Troisième partie
Corps cubiques

6 Théorème de Davenport-Heilbronn

Dans le cas des corps cubiques, on n'a plus la paramétrisation simple que l'on avait pour les corps quadratiques, simplement à partir des entiers sans

facteurs carrés. On peut alors chercher à essayer de déterminer un équivalent asymptotique du nombre de corps cubiques (à isomorphisme près) dont on borne le discriminant.
Soient alors :

$$N_0(X) = \#\left\{K \text{ corps cubique } ;\ 0 \leq Disc(K) \leq X\right\}$$

et

$$N_1(X) = \#\left\{K \text{ corps cubique } ;\ -X \leq Disc(K) \leq 0\right\}.$$

L'objectif de cette section est de prouver le résultat suivant, en suivant une approche due à Bhargava, Shankar et Tsimerman :

Théorème 15. *(Davenport-Heilbronn)*
Pour $X \to \infty$, on a :

$$N_0(X) = \frac{1}{12\zeta(3)}X + o(X) \text{ et } N_1(X) = \frac{1}{4\zeta(3)}X + o(X).$$

On va de plus, à partir du théorème de Siegel sur les formes quadratiques, donner une estimation de la taille des groupes de classes d'idéaux des formes quadratiques, suivant une méthode similaire : si $\Lambda = \prod_{p\in\mathbf{P}}(1 - p^{-2} - p^{-3} + p^{-4})$, on a, lorsque $X \longrightarrow +\infty$:

$$\sum_{K\in\mathcal{K}_X} h(K) = \frac{\Lambda\pi}{18}X^{3/2} + o(X^{3/2}).$$

La première étape de la preuve du théorème 14 consiste à exhiber des correspondances entre anneaux *cubiques*, c'est-à-dire anneaux munis d'une structure de $\mathbf{Z}$-module libre de rang 3, et certaines classes d'équivalence de formes cubiques binaires, qui nous permettra de nous ramener à estimer des tailles d'orbites de formes cubiques sous l'action de $GL_2(\mathbf{Z})$. C'est l'objet du paragraphe suivant.

6.1 Correspondance de Delone-Faddeev

Théorème 16. *(Delone-Faddeev)*
On dispose d'une bijection naturelle entre les classes d'isomorphisme d'anneaux cubiques, et les classes de formes cubiques binaires à coefficients entiers sous l'action de $GL_2(\mathbf{Z})$.

Démonstration. Soit A un anneau cubique, et $(1, \omega, \theta)$ une base de A. Si $\omega\theta = \alpha + \beta\omega + \delta\theta$, $\alpha, \beta, \delta \in \mathbf{Z}$, on remplace ω par $\omega - \delta$ et θ par $\theta - \beta$, si bien qu'on peut supposer $\omega\theta \in \mathbf{Z}$.

On définit alors les constantes de structure de l'anneau comme les entiers n, m, l, a, b, c, d tels que :

$$\left\{ \begin{array}{lcl} \omega\theta & = & n \\ \omega^2 & = & m - b\omega + a\theta \\ \theta^2 & = & l - d\omega + c\theta \end{array} \right.$$

Soit alors $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ la forme cubique associée à A ; il s'agit de la forme cubique :

$$\left\{ \begin{array}{l} A/\mathbf{Z} \longrightarrow \bigwedge^2 R/\mathbf{Z} \cong \mathbf{Z} \\ r = x\omega + y\theta \longmapsto r \wedge r^2 \end{array} \right.$$

où l'isomorphisme $\bigwedge^2 R/\mathbf{Z} \cong \mathbf{Z}$ est déterminé par le choix de la base $(1, \omega, \theta)$. Ainsi, si l'on change de base par l'action de $\gamma \in GL_2(\mathbf{Z})$ sur (ω, θ), la forme f associée devient ${}^t\gamma \cdot f$: ainsi la classe de f modulo $GL_2(\mathbf{Z})$ ne dépend que de A.
Réciproquement, soit $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ une forme binaire. On veut construire un anneau cubique A, ayant les relations de structure (modulo $GL_2(\mathbf{Z})$) données plus haut. Une fois les relations de structure imposées, la seule chose à vérifier pour s'assurer qu'on obtient un anneau est l'associativité de la multiplication ; dans ce cas précis, en utilisant la distributivité, cela revient à vérifier $(\omega\theta)\theta = \omega(\theta^2)$ et $(\omega^2)\theta = (\omega\theta)\theta$, ce qui donne les relations :

$$\left\{ \begin{array}{lcl} n & = & -ad \\ m & = & -ac \\ l & = & -bd \end{array} \right.$$

ainsi n, m, l sont entièrement déterminés ; et à isomorphisme de changement de base près, l'anneau A ainsi obtenu ne dépend pas du choix d'un représentant de f modulo $GL_2(\mathbf{Z})$. Il est clair que les deux applications $A \longmapsto f_A$ et $f \longmapsto A(f)$ sont inverses l'une de l'autre. □

La preuve permet d'ailleurs de voir que les automorphismes d'anneau de A sont en bijection naturelle avec le stabilisateur de f_A dans $GL_2(\mathbf{Z})$. Cette remarque nous servira dans la suite.
Dans un anneau cubique, on définit la trace d'un élément de la même manière que sur l'anneau des entiers d'un corps de nombres ; et on étend le discriminant de la même manière, comme discriminant de la forme bilinéaire trace.
On définit de plus le discriminant d'une forme cubique binaire comme étant le discriminant du polynôme $P(X) = f(X, 1)$. L'un des intêrets de la correspondance de Delone-Faddeev est qu'elle transporte bien les informations qui vont nous intéresser.

Proposition 34. *La correspondance de Delone-Faddeev laisse le discriminant invariant, i.e. $Disc(A(f)) = Disc(f)$ pour toute forme binaire f.*
De plus, l'anneau $A(f)$ est intègre si et seulement si la forme f est irréductible sur $\mathbf{Z}$.

Démonstration. Le premier point est un calcul direct mais fastidieux, laissé au lecteur.
Supposons que la forme f soit réductible sur $\mathbf{Z}$: comme elle est de degré 3, on obtient un facteur de degré 1, à coefficients entiers, soit une racine $f(x,1) = 0\,; x \in \mathbf{Z}$. Comme on regarde des classes d'équivalences de formes modulo $GL_2(\mathbf{Z})$, on peut alors supposer que $a = 0$. Mais en reprenant les notations de la preuve précédente, $a = 0$ entraîne $n = 0$ et donc $\omega\theta = 0$: $A(f)$ n'est pas intègre.
Réciproquement, supposons qu'il existe α, β dans A non nuls tels que $\alpha\beta = 0$. Appliquant le théorème de Cayley-Hamilton à l'endomorphisme induit par α, on obtient une équation du type $\alpha^3 + c_1\alpha^2 + c_2\alpha + c_3 = 0$; en multipliant par β il vient $c_3\beta = 0$ puis $c_3 = 0$ puisque A est un $\mathbf{Z}$-module libre, et que β est non nul par hypothèse. On a alors $\alpha(\alpha^2 + c_1\alpha + c_2) = 0$.
Si $(\alpha^2 + c_1\alpha + c_2) = 0$, on complète $(1, \alpha)$ en une base de A, et on a alors $a = 0$ dans les relations de structure obtenues ; la forme $A(f)$ est réductible.
Sinon, on note que $(\alpha^2 + c_1\alpha + c_2)^2 = c_2(\alpha^2 + c_1\alpha + c_2)$, et de même en complétant cette élément en une base on obtient $a = 0$ dans les relations de structure de l'anneau. □

6.2 Estimations globales

Définition 18. *On note $V_{\boldsymbol{R}}$ l'espace des formes cubiques, et $V_{\boldsymbol{Z}}$ des formes à coefficients entiers. $GL_2(\boldsymbol{R})$ agit naturellement sur $V_{\boldsymbol{R}}$, ce qui induit une partition en deux orbites, constituées des formes de discriminant positif $V_{\boldsymbol{R}}^{(0)}$ et des formes de discriminant négatif $V_{\boldsymbol{R}}^{(1)}$. On note $N(V_{\boldsymbol{Z}}^{(i)}; X)$ le nombre de $GL_2(\boldsymbol{Z})$-orbites constituées de formes irréductibles dans $V_{\boldsymbol{Z}}^{(i)}$, dont la valeur absolue du discriminant est bornée par X, et enfin $D_X = \{v \in V_{\mathbf{R}}\ ;\ |Disc(v)| \leq X\}$.*

L'objet de cette sous-section est de prouver le théorème suivant :

Théorème 17.

$$(1)\ N(V_{\boldsymbol{Z}}^{(0)}; X) = \frac{\pi^2}{72}X + o(X);$$

$$(2)\ N(V_{\boldsymbol{Z}}^{(1)}; X) = \frac{\pi^2}{24}X + o(X).$$

Ce sont ces équivalents qui, combinés à des arguments quantitatifs sur la densité de discriminants fondamentaux, vont nous permettre de démontrer le théorème de Davenport-Heilbronn. En fait, l'analogue quadratique

de résultat est le théorème de Siegel sur les formes quadratiques, dont on verra plus tard comment tirer des informations sur des quantités purement arithmétiques.

On a $N(V_{\mathbf{Z}}^{(i)};X) = \#\left\{V_{\mathbf{Z}}^{irr} \cap V_{\mathbf{R}}^{(i)} \cap D_X\right\}/GL_2(\mathbf{Z})$, soit $N(V_{\mathbf{Z}}^{(i)};X) = \#\left\{V_{\mathbf{Z}}^{irr} \cap D_X \cap (V_{\mathbf{R}}^{(i)}/GL_2(\mathbf{Z}))\right\}$. Dans un premier temps, nous étudions $V_{\mathbf{R}}^{(i)}/GL_2(\mathbf{Z})$.

L'action de $GL_2(\mathbf{R})$ sur $V_{\mathbf{R}}^{(i)}$ est transitive, donc pour tout $v_0 \in V_{\mathbf{R}}^{(i)}$, $V_{\mathbf{R}}^{(i)} = GL_2(\mathbf{R})v_0$, où chaque élément v apparaît $n_i = \#Stab_{GL_2(\mathbf{R})}(v)$ fois (au sens où il apparaît pour n_i éléments distincts de GL_2, si l'on indexe V par les éléments de GL_2). On calcule facilement les cardinaux des stabilisateurs en regardant l'action par permutations de $GL_2(\mathbf{R})$ sur les racines des formes : $n_0 = 6, n_1 = 2$.

On écrit donc $V_{\mathbf{R}}^{(i)}/GL_2(\mathbf{Z}) = \frac{1}{n_i}GL_2(\mathbf{R})/GL_2(\mathbf{Z})v_0$. $\frac{1}{n_i}$, pris au sens donné ci-dessus.

On utilise la décomposition d'Iwasawa, qui garantit que

$$\mathcal{F} = \left\{ \begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} k : n \in [-\frac{1}{2}, \frac{1}{2}], t \geq \sqrt[4]{3}/\sqrt{2}, \lambda > 0, k \in SO_2(\mathbf{R}) \right\}$$

est un domaine fondamental pour $GL_2(\mathbf{R})/GL_2(\mathbf{Z})$. Pour étudier $V_{\mathbf{R}}^{(i)}/GL_2(\mathbf{Z}) = \frac{1}{n_i}GL_2(\mathbf{R})/GL_2(\mathbf{Z})v_0$, il suffit d'étudier $\mathcal{F}v_0$.

Il y a cependant une subtilité, si $Stab_{GL_2(\mathbf{R})}(v) \cap GL_2(\mathbf{Z}) \neq 1$, v n'est pas compté n_i fois dans $\mathcal{F}v_0$, mais seulement k fois, avec k un diviseur de n_i. Comme $Stab_{GL_2(\mathbf{R})}(v) \cap GL_2(\mathbf{Z}) = Aut(R)$ où R est l'anneau correspondant à v, cela ne se produit que pour $Disc(v) > 0$. On montre que ce cas se produit un nombre négligeable de fois.

Lemme 13.

$$\#(V_{\boldsymbol{Z}}^{(1)} \cap D_X \cap \mathcal{F}v_0 \cap \{v : Stab \cap GL_2(\boldsymbol{Z}) \neq 1\}) = o(X).$$

Démonstration. Comme cette quantité ne dépend pas de v_0, on choisit

$$v_0 = x^3 - 3xy^2.$$

A toute forme $f = ax^3 + bx^2y + cxy^2 + dy^3$, on associe

$$H_f = (b^2 - 3ac)x^2 + (bc - 9ad)xy + (c^2 - 3bd)y^2$$

son Hessien, et on peut vérifier facilement que

$$\gamma H_f = H_{\gamma f}, \forall \gamma \in GL_2(\mathbf{R}), H_{v_0} = 9(x^2 + y^2),$$

$$\mathcal{F}H_{v_0} = \{\alpha x^2 + \beta xy + \theta y^2 : |\beta| \leq \alpha \leq \theta\}.$$

$Stab(v) \cap GL_2(\mathbf{Z}) \neq 1$ implique que $Stab(H_v) \cap GL_2(\mathbf{Z}) \neq 1$, mais le seul $H_v \in FH_{v_0}$ qui satisfaisant cette condition est $x^2 + xy + y^2$, donc $v = (a, b, c, d)$ satisfait

$$b^2 - 3ac = bc - 9ad = c^2 - 3bd.$$

Don en particulier c est entièrement déterminé par (a, b, d). Quand $a = 0$ il est facile de voir que le nombre de solutions est $o(X)$, et quand $a \neq 0$, on rappelle que

$$v = (a, b, c, d) = \begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} kv_0,$$

$Disc(v) = \lambda^4 Disc(v_0)$ implique que $\lambda = O(X^{\frac{1}{4}})$, et on calcule :

$$a = O(\lambda/t^3) = O(X^{\frac{1}{4}}), ab = O(\lambda^2/t^4) = O(X^{\frac{1}{2}}),$$

$$ad = O(\lambda^2) = O(X^{\frac{1}{2}}), abd = O(\lambda^3/t) = O(X^{\frac{3}{4}}).$$

Donc on a aussi $O(X^{\frac{3}{4}}) = o(X)$ choix possibles pour (a, b, d), et de même pour (a, b, c, d). □

On a donc montré que quelque soit $v_0 \in V^i_{\mathbf{R}}$,

$$N(V^{(i)}_{\mathbf{Z}}; X) = \frac{1}{n_i} \#(\mathcal{F}v_0 \cap V^{irr}_{\mathbf{Z}} \cap D_X) + o(X).$$

On va effectuer une seconde étape de simplification. On va prouver que les formes réductibles sont aussi en nombre négligeable. Soit $\widehat{V}_{\mathbf{Z}} = V_{\mathbf{Z}} \cap \{a \neq 0\}$, on va prouver

$$\#(\mathcal{F}v_0 \cap V^{irr}_{\mathbf{Z}} \cap D_X) = \#(\mathcal{F}v_0 \cap \widehat{V}_{\mathbf{Z}} \cap D_X) + o(X).$$

On remarque que $V^{irr}_{\mathbf{Z}} \subset \widehat{V}_{\mathbf{Z}} \subset V_{\mathbf{Z}}$; comme il y a une infinité des formes dans $D_X \cap V_{\mathbf{Z}}$ avec $a = 0$, on utilise $\widehat{V}_{\mathbf{Z}}$, plutôt que $V_{\mathbf{Z}}$.

Lemme 14. *Soit $v_0 \in V_{\boldsymbol{R}}$ avec $|det(v_0)| \geq 1$, alors*

$$\#(\mathcal{F}v_0 \cap D_X \cap (\widehat{V}_{\boldsymbol{Z}} - V^{irr}_{\boldsymbol{Z}})) = o(X).$$

Démonstration. Par le même calcul que pour le lemme précédent, on a $a = O(X^{\frac{1}{4}}), ab, ac, ad = O(X^{\frac{1}{2}}), abc, abd = O(X^{\frac{3}{4}})$. Donc quand $d = 0$, on a $O(X^{\frac{3}{4}}) = o(X)$ choix possibles pour (a, b, c, d).

Quand $d \neq 0$, on a $O(X^{\frac{3}{4}})$ choix possibles pour (a, b, d), et v réductible implique qu'il existe $rx + sy$ annulant v, donc $r, s \neq 0, r|a, s|d$. On a donc $O(X^{\epsilon})$ choix possibles pour (r, s), et la condition $v(-r, s) = 0$ détermine entièrement c. Cela nous laisse $O(X^{\frac{3}{4}+\epsilon}) = o(X)$ choix possibles. □

Ainsi, on a montré que :

$$N(V_{\mathbf{Z}}^{(i)}; X) = \frac{1}{n_i} \#(\mathcal{F}v_0 \cap \widehat{V}_{\mathbf{Z}} \cap D_X) + o(X).$$

Donc il suffit de calculer $\#\{x \in \mathcal{F}v \cap \widehat{V}_{\mathbf{Z}} : |Disc(x)| < X\}$, c'est-à-dire le nombre des points entiers dans la région $\mathcal{F}v \cap D_X$ privée du bord $\{a = 0\}$, où on note $D_X = \{x : |Disc(x)| < X\}$.

Il serait naturel d'essayer de le relier à $Vol(\mathcal{F}v \cap D_X)$; ce genre d'estimations étant en général assez bonnes pour des domaines "simples" (par exemple des convexes bornés), cependant la forme de $\mathcal{F}v \cap D_X$ peut être compliquée, ce qui nous empêchera de contrôler l'erreur commise quand on approxime le nombre de points entiers par le volume. Par exemple, $\{(x, y) : 0 < y < \frac{1}{\sqrt{x}}, x \in [0, 1]\}$ contient un nombre infini de points entiers sur l'axe y, mais son volume est fini.

On va alors remédier à ce problème en "moyennant" sur les v d'un "bon" ensemble, moyenne que l'on pourra estimer.

On admet la proposition suivante :

Proposition 35. *(Principe de Lipschitz)*
Soit $\mathcal{R}$ une partie bornée de $\mathbf{R}^n$, définie par un nombre fini d'inégalités polynomiales. Alors le nombre $N(\mathcal{R})$ des points entiers dans $\mathcal{R}$ peut s'estimer par :

$$N(\mathcal{R}) = Vol(\mathcal{R}) + O(max\{Vol(\bar{\mathcal{R}})_i, 1\}),$$

où $Vol(\bar{\mathcal{R}}_i)$ est le volume de la projection de $\mathcal{R}$ sur l'hyperplan $x_i = 0$.

Pour moyenner, on a besoin d'une mesure sur $GL_2(\mathbf{R})$, et d'une autre sur l'espace des formes binaires. Pour la première, on note $dg = t^{-2}dnd^\times tdkd^\times\lambda$, qui correspond à la décomposition d'Iwasawa $GL_2(\mathbf{R})$, normalisée de telle sorte à avoir une masse 1 sur $SO_2(\mathbf{R})$ (soit $dk = d\theta/2\pi$). Pour la seconde, on note $dv = dadbdcdd$ la mesure euclidienne sur $\mathbf{R}^4$, et $d\mu = |disc(v)|^{-1}dv$. On effectué ces choix en raison du bon comportement de ces mesures par rapport à l'action de $GL_2(\mathbf{R})$ sur les formes :

Lemme 15 (Changement de mesure)**.** *Pour tout $f \in C_0(V_{\boldsymbol{R}}^{(i)}), v_0 \in V_{\boldsymbol{R}}^{(i)}$,*

$$\int_{g \in GL_2(\boldsymbol{R})} f(g \cdot v_0)dg = \frac{1}{2\pi} \int_{v \in GL_2(\boldsymbol{R}) \cdot v_0} f(v)d\mu = \frac{n_1}{2\pi} \int_{v \in V_{\boldsymbol{R}}^{(i)}} f(v)d\mu.$$

Démonstration. La première égalité est un simple changement de variable dans l'intégrale, passant des variables (n, t, k, λ) à (a, b, c, d). La deuxième vient du fait que $GL_2(\mathbf{R}) \cdot v_0$ est un recouvrement de $V_{\mathbf{R}}^{(i)}$, où chaque point apparaît avec multiplicité n_i. □

On pose :

$$B = \{w = (a, b, c, d) \in V_{\mathbf{R}}^{(i)} : |Disc(w)| \geq 1, 3a^2 + b^2 + c^2 + 3d^2 \leq C\}$$

pour une constante C, et on pose $M = \frac{n_i}{2\pi}\int_{v\in B} d\mu$. En particulier, on remarque que $SO_2(\mathbf{R})B = B$.

Enfin on pose :

$$N = \frac{1}{2\pi M}\int_{v\in B} \#\{x \in \mathcal{F}v \cap D_X \cap \widehat{V}_{\mathbf{Z}}\}d\mu = \frac{1}{2\pi M}\sum_{x\in \widehat{V}_{\mathbf{Z}}\cap D_X}\int_{v\in B} \#\{g \in \mathcal{F} : x = gv\}d\mu.$$

Par ce qui précède,

$$\begin{aligned} N(V_{\mathbf{Z}}^{(i)}; X) &= \#\{x \in \mathcal{F}v \cap D_X \cap \widehat{V}_{\mathbf{Z}}\} + o(X) \\ &= \frac{\int_{v\in B} \#\{x \in \mathcal{F}v \cap D_X \cap \widehat{V}_{\mathbf{Z}}\}d\mu}{n_i \int_{v\in B} d\mu} + o(X) := \mathcal{N} + o(X). \end{aligned}$$

Il nous reste donc à estimer $\mathcal{N}$.

On effectue alors un changement de variable à l'aide du lemme ci-dessus pour le calculer. On fixe $v_0 \in V_{\mathbf{R}}^{(i)}$, et on note H un sous-ensemble maximal de $GL_2(\mathbf{R})$ tel que $H\cdot v_0 = B$. On remarque que Hv_0 est donc un revêtement à n_i feuillets de B.

Par le lemme de changement de variable, on voit que :

$$\sum_{x\in \widehat{V}_{\mathbf{Z}}\cap D_X}\int_{v\in B} \#\{g \in \mathcal{F} : x = gv\}d\mu = 2\pi \sum_{x\in \widehat{V}_{\mathbf{Z}}\cap D_X}\int_{h\in H} \#\{g \in \mathcal{F} : x = ghv_0\}dh.$$

On effectue un nouveau changement de variable, de h à g :

$$\begin{aligned} &2\pi \sum_{x\in \widehat{V}_{\mathbf{Z}}\cap D_X}\int_{h\in H} \#\{g \in \mathcal{F} : x = ghv_0\}dh \\ &= 2\pi \sum_{x\in \widehat{V}_{\mathbf{Z}}\cap D_X}\int_{g\in F} \#\{h \in H : x = ghv_0\}dg \\ &= 2\pi \int_{g\in\mathcal{F}} \#\{x \in \widehat{V}_{\mathbf{Z}} \cap gHv_0 \cap D_X\}dg \\ &= 2\pi \int_{g\in\mathcal{F}} \#\{x \in \widehat{V}_{\mathbf{Z}} \cap gB \cap D_X\}dg. \end{aligned}$$

On calcule :

$$\begin{aligned} \mathcal{N} &= \frac{1}{M}\int_{g\in\mathcal{F}} \#\{x \in \widehat{V}_{\mathbf{Z}} \cap gB \cap D_X\}dg \\ &= \frac{1}{M}\int_{n,t,\lambda,k} \#\{x \in \widehat{V}_{\mathbf{Z}} \cap \begin{pmatrix}1 & \\ n & 1\end{pmatrix}\begin{pmatrix}t^{-1} & \\ & t\end{pmatrix}\begin{pmatrix}\lambda & \\ & \lambda\end{pmatrix} kB \cap D_X\}t^{-2}dnd^\times t d^\times\lambda dk, \end{aligned}$$

en réinjectant l'expression de dg. Comme que B est invariant sous l'action de $SO_2(\mathbf{R})$, on peut éliminer k, et si on note

$$B'(n,t,\lambda,X) = \begin{pmatrix}1 & \\ n & 1\end{pmatrix}\begin{pmatrix}t^{-1} & \\ & t\end{pmatrix}\begin{pmatrix}\lambda & \\ & \lambda\end{pmatrix} B \cap D_X,$$

on a :

$$\mathcal{N} = \frac{1}{M} \int_{n=-\frac{1}{2}}^{\frac{1}{2}} \int_{\lambda=(\frac{4\sqrt{3}}{\sqrt{2}})^3/C}^{\sqrt[4]{X}} \int_{t=\frac{4\sqrt{3}}{\sqrt{2}}}^{C^{\frac{1}{3}}\lambda^{\frac{1}{3}}} \#\{x \in B'(n,t,\lambda,X) \cap \widehat{V}_{\mathbf{Z}}\} t^{-2} dn d^{\times}t d^{\times}\lambda + o(X).$$

On justifie les bornes supérieures d'intégration en λ, t comme suit : quand $\lambda \geq \sqrt[4]{X}$, tout les $x \in B$ vérifient $Disc(x) > 1$, et donc B' est vide. Quand $C\lambda \geq t^3$, tous les éléments de B satisfont $a = 0$; ils sont donc réductibles, et $B'(n,t,\lambda,X) \cap \widehat{V}_{\mathbf{Z}} = \emptyset$.

Maintenant, on utilise le principe de Lipschitz pour estimer $\#\{x \in B'(n,t,\lambda,X) \cap \widehat{V}_{\mathbf{Z}}\}$. Comme B est borné, B' est borné aussi, et on voit facilement qu'il est défini par des inégalités polynomiales. Il nous reste à estimer les volumes de ses projections sur les hyperplans. Rappelons que

$$B = \{w = (a,b,c,d) \in V_{\mathbf{R}}^{(i)} : |Disc(w)| \geq 1, 3a^2 + b^2 + c^2 + 3d^2 \leq C\},$$

donc le volume d'une projection de B selon n'importe quelle direction est en $O(C^3)$.

$$B'(n,t,\lambda,X) = \begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} B \cap D_X,$$

la matrice de n ne modifie pas ces bornes sur le volume, celles de t et λ dilatent ces projections par au plus un facteur $t^3\lambda^3$; puisque la projection est tridimensionnelle. Ainsi $Vol(\bar{B}') = O(C^3 t^3 \lambda^3)$.

Finalement, le nombre de points entiers de B' s'exprime :

$$\mathcal{N}(B') = Vol(B') + O(max\{C^3 t^3 \lambda^3, 1\}).$$

Notons que ce résultat est vrai pour tout t, cependant on l'utilise seulement pour $t < C^{\frac{1}{3}}\lambda^{\frac{1}{3}}$; en effet pour les t grands la borne d'erreur obtenue est insuffisante, cependant dans ce cas $B' \cap \widehat{V}_{\mathbf{Z}} = \emptyset$, donc cette contribution disparaît automatiquement grâce aux bornes d'intégration sur t.

On a :

$$\mathcal{N} = \frac{1}{M} \int_{n=-\frac{1}{2}}^{\frac{1}{2}} \int_{\lambda=(\frac{4\sqrt{3}}{\sqrt{2}})^3/C}^{\sqrt[4]{X}} \int_{t=\frac{4\sqrt{3}}{\sqrt{2}}}^{C^{\frac{1}{3}}\lambda^{\frac{1}{3}}} (Vol(B') + O(max\{C^3 t^3 \lambda^3, 1\})) t^{-2} dn d^{\times}t d^{\times}\lambda + o(X).$$

Par le lemme de changement de variable, on a

$$\frac{1}{M} \int_{n=-\frac{1}{2}}^{\frac{1}{2}} \int_{\lambda=(\frac{4\sqrt{3}}{\sqrt{2}})^3/C}^{\sqrt[4]{X}} \int_{t=\frac{4\sqrt{3}}{\sqrt{2}}}^{\infty} Vol(B') t^{-2} dn d^{\times}t d^{\times}\lambda = \frac{1}{2\pi M_i} \int_{v \in B} Vol(\mathcal{F}v \cap D_X) d\mu,$$

et quand $t > C^{\frac{1}{3}}\lambda^{\frac{1}{3}}$, $Vol(B')$ est majoré par $C^4\lambda^4$, donc l'intégrale sur les $t > C^{\frac{1}{3}}\lambda^{\frac{1}{3}}$ est en $o(X)$. L'intégrale du terme $O(max\{C^3 t^3 \lambda^3, 1\})$ est aussi en $o(X)$.

Il s'ensuit :

$$\mathcal{N} = \frac{1}{n_i} \frac{\int_{v \in B} Vol(\mathcal{F}v \cap D_X) d\mu}{\int_{v \in B} d\mu} + o(X) = \frac{1}{n_i} Vol(\mathcal{F}v \cap D_X) + o(X).$$

Comme $Vol(SL_2(\mathbf{Z})\backslash SL_2(\mathbf{R})) = \zeta(2)/\pi$, on effectue un nouveau changement de variable avec $f(v) = |disc(v)|$,

$$Vol(\mathcal{F}v \cap D_X) = 2\pi \int_0^{\sqrt[4]{X}} \lambda^4 d^\times \lambda \cdot Vol(SL_2(\mathbf{Z})\backslash SL_2(\mathbf{R})) = \frac{\pi^2}{12} X,$$

Donc on a $N = \frac{\pi^2}{12 n_i} X + o(X)$, donc on a prouvé le théorème :

$$N(V_{\mathbf{Z}}^{(0)}; X) = \frac{\pi^2}{72} X + o(X), N(V_{\mathbf{Z}}^{(1)}; X) = \frac{\pi^2}{24} X + o(X).$$

6.3 Correspondance de Davenport-Heilbronn

On commence par distinguer les anneaux maximaux de leurs sous-anneaux ; il s'avère que cette propriété peut se déterminer efficacement à l'aide d'un principe local-global.

Définition 19. *On dit que l'anneau cubique A est maximal s'il n'est contenu dans aucun autre anneau cubique que lui-même.*
On dit de plus qu'il est maximal en p premier si on n'a jamais $A \subset A'$ pour un autre anneau cubique A', avec $[A' : A]$ divisible par p.

Le théorème de structure des groupes abéliens de type fini nous garantit qu'un sous-module de rang maximal d'un anneau cubique est forcément d'indice fini ; le principe local-global est alors vérifié, au sens où A est maximal si et seulement si il est maximal en tout premier p. L'intêret de cette notion de maximalité est le suivant :

Proposition 36. *Soit A un anneau cubique intègre ; alors il est maximal si et seulement si c'est l'anneau des entiers d'un corps cubique.*

Démonstration. On peut remarquer que le corps des fractions d'un anneau cubique intègre est toujours un corps cubique ; et de plus que cet anneau cubique est contenu dans l'anneau des entiers de son corps de fractions. Il s'ensuit qu'un anneau cubique intègre maximal est l'anneau des entiers de son corps de fractions.
Réciproquement, supposons A soit l'anneau des entiers du corps cubique K, qui est alors son corps de fractions. Si A' contient A, son corps des fractions K' contient K, mais ces deux corps sont de degré 3 sur $\mathbf{Q}$: ils sont donc égaux ; et $A' = A$ en passant à l'anneau des entiers. □

On va alors chercher à déterminer, en termes de formes cubiques, comment la maximalité en p peut être mise en défaut.

Proposition 37. *Soit A anneau cubique, non maximal en p. On peut en trouver une $\mathbf{Z}$-base $(1, \omega, \theta)$ telle que l'un des deux modules suivant soit en fait un anneau (i.e stable par produit) :*

$$\mathbf{Z} \oplus \mathbf{Z}(\omega/p) \oplus \mathbf{Z}\theta \text{ ; } \textit{ou alors } \mathbf{Z} \oplus \mathbf{Z}(\omega/p) \oplus \mathbf{Z}(\theta/p).$$

Démonstration. Soit A' anneau cubique contenant A, avec $[A' : A]$ multiple de p, et soit alors $A_1 = A' \cap (\bigoplus_{n \in \mathbf{N}} p^{-n} A)$.
On a ainsi construit un anneau contenant A, qui est aussi un $\mathbf{Z}$-module de type fini ; avec de plus $[A_1 : A] = p^k$ pour un $k \in \mathbf{N}$.
Par le théorème de la base adaptée pour les groupes abéliens de type fini, on peut trouver $i \geq j \in \mathbf{N}$, et $(1, \omega, \theta)$ tels que :

$$A_1 = \mathbf{Z} \oplus \mathbf{Z}(\omega/p^i) \oplus \mathbf{Z}(\theta/p^j).$$

Si $i = 1$, la proposition est prouvée ; sinon on va procéder par approximations successives : on peut toujours supposer que $\omega\theta \in \mathbf{Z}$; et on garde les mêmes notations que précédemment pour les relations de structure de A. On écrit les égalités garantissant que A_1 soit un anneau ; par exemple $\omega^2/p^2 i$ se décompose dans la base $(1, \omega/p^i, \theta/p^j)$, et donc la relation :

$$\frac{\omega^2}{p^2 i} = \frac{m}{p^2 i} - \frac{b\omega}{p^i p^i} - \frac{a\theta}{p^j p^{2i-j}}$$

impose alors $a \equiv 0[p^{2i-j}]$ et $b \equiv 0[p^i]$, et on obtient de la même manière les congruences $c \equiv 0[p^j]$ et $d \equiv 0[p^{2j-i}]$. Si $j = 0$, on peut remplacer (i, j) par $(i-1, j)$ sans changer la valeur de vérité des congruences listées ci-dessus ; de même si $j > 1$ en remplaçant (i, j) par $(i-1, j-1)$; cela se voit à l'aide des congruences imposées à n, m, l ; et des relations $n = -ad$; $m = -ac$ et $l = -bd$.
Ainsi on peut toujours arriver à $i = 1$ par un nombre fini d'approximations, avec dans le premier cas $j = 0$ et dans le deuxième $j = 1$, ce qui termine la preuve. □

Le premier cas correspond ainsi au cas $p^2 | a$ et $b | p$ d'après les conditions de congruence ci-dessus (les a, b sont définis modulo l'action de $GL_2(\mathbf{Z})$, on demande en fait que cette relation soit vraie pour au moins un représentant de f) ; le deuxième à un cas où a, b, c, d sont divisibles par p, ce qui revient à dire que f est divisible par p.
On a ainsi complètement décrit, en terme de formes cubiques, de quelle manière un anneau cubique peut ne pas être maximal en p.
Soit $\mathcal{U}_p$ l'ensemble des formes f ne vérifiant aucune des deux conditions ci-dessus. On a prouvé le résultat suivant :

Théorème 18. *(Davenport-Heilbronn)*
L'anneau cubique A est maximal en p si et seulement si $f_A \in \mathcal{U}_p$.
De plus, A est maximal si et seulement si $f_A \in \bigcap_p \mathcal{U}_p$.

Corollaire 5. *Le nombre de sous-anneaux cubiques de A d'indice exactement p est égal au nombre $\omega_p(f_A)$ de racines modulo p de f_A dans $\mathbf{P}^1(\mathbf{F}_p)$.*
Ce nombre est donc au plus de 3.

Démonstration. Etant donné la correspondance ci-dessus, être un sous-anneau d'indice p d'un autre anneau cubique est équivalent aux conditions $p|a$ et $p|b$ pour l'une des formes dans la classe associée à A. Cela entraîne alors l'existence d'une racine $(0, y)$ de ce représentant modulo p ; et la droite engendrée par cette racine étant entièrement constituée d'autres racines. Si on fixe une forme f de référence dans cette classe, pour tout sous-anneau d'indice p, il existe une forme dans la classe de f s'annulant sur la droite $x = 0$; modulo l'action de $PGL_2(\mathbf{F}_p)$, on en tire une racine (à homothétie près) de $f(x, y)$ dans $\mathbf{F}_p^2$. □

On va maintenant donner des estimations quantitatives sur le comportement local des formes en les premiers p.

6.4 Comportement local, densité en p

Définition 20. *Soit $S \subset V_{\mathbf{Z}}$, on peut le plonger naturellement dans $V_{\mathbf{F}_p}$ par réduction modulo p ; on note toujours ce plongement S.*
On définit la densité de S en p comme $\mu_p(S) = \frac{\#S}{\#V_{\mathbf{F}_p}}$; cette quantité est bien sûr toujours finie, et comprise entre 0 et 1.

Pour $S \subset V_{\mathbf{Z}}^i$ un sous-ensemble de formes binaires cubiques, défini par un nombre fini de relations de congruence sur les coefficients, on a le résultat suivant :

Théorème 19. *(Passage local-global)*
Soit $S \subset V_{\mathbf{Z}}^i$, défini par un nombre fini de conditions de congruence modulo des puissances de nombres premiers sur ses coefficients. On a alors :

$$\lim_{X\to\infty} \frac{N(S \cap V_{\mathbf{Z}}^i; X)}{N(V_{\mathbf{Z}}^i; X)} = \prod_p \mu_p(S),$$

où tous les termes du produit de droite sont égaux à 1 sauf un nombre fini.

Démonstration. Supposons que l'on impose $a_j \equiv r_{i,j}[p_i^{\alpha_{i,j}}]$, pour $i = 1, ..., N$, et $j = 1, ..., d$; où les a_j sont les coefficients de f.
On note $\alpha_i = \max\{\alpha_{i,j} \ ; \ j \leq d\}$, et $m = p_1^{\alpha_1}...p_N^{\alpha_N}$.
Par le lemme chinois, l'ensemble S est alors l'intersection de $V_{\mathbf{Z}}^i$ avec une réunion disjointe d'un certain nombre k de translatés $L_1, ..., L_k$ du réseau $m \cdot V_{\mathbf{Z}}$.
On est donc ramené à estimer $N(L_j \cap V_{\mathbf{Z}}^i; X)$; or par le principe de Lipschitz, en effectuant un changement d'échelle, le terme principal est $N(V_{\mathbf{Z}}^i; X/m^4)$, et les termes d'erreurs sont dilatés d'un facteur $1/m^3$ (puisque les projections

sont tridimensionnelles) qui est constant : on a ainsi $\lim_{X\to\infty} \frac{N(S\cap V^i_{\mathbf{Z}};X)}{N(V^i_{\mathbf{Z}};X)} = \frac{k}{m^4}$.
Or les vecteurs $(a,b,c,d) \in (\mathbf{Z}/m\mathbf{Z})^4$ satisfaisant la condition de congruence sont exactement ceux satisfaisant chaque condition en $p_i^{\alpha_i}$ par le théorème des restes chinois ; il s'ensuit que $\prod \mu_p(S) = \frac{k}{m^4}$, ce qui termine la preuve. □

Pour pouvoir passer d'un résultat sur les $N(V^i_{\mathbf{Z}}, X)$ à des estimations asymptotiques sur les nombres de corps cubiques de discriminant borné, on va donc avoir besoin de calculer les densités des $\mathcal{U}_p$.
De la même manière que le corps $\mathbf{C}$ pour $\mathbf{R}$, il existe un plus petit corps algébriquement clos $\overline{\mathbf{F}_p}$ contenant $\mathbf{F}_p$; on l'appelle la clôture algébrique de $\mathbf{F}_p$ (cette extension est cependant de dimension infinie puisque $\overline{\mathbf{F}_p}$ ne peut pas être un corps fini, étant algébriquement clos).
Une forme f ne vérifiant pas $f \equiv 0\ [p]$ détermine alors 3 points de $\mathbf{P}^1(\overline{\mathbf{F}_p})$; à savoir ses racines. Comme ces racines sont annulées par un polynôme de degré 3, l'extension qu'elles engendrent est au plus $\mathbf{F}_{p^3}$. De plus, comme les coefficients de f sont dans $\mathbf{F}_p$, les éventuelles racines contenues dans une extension de $\mathbf{F}_p$ sont nécessairement conjuguées. On note alors $(f,p) = (f_1^{e_1} f_2^{e_2} ...)$ où les e_i sont les degrés de multiplicité de ces racines ; et les f_i la dimension de la plus petite extension dans laquelle elles sont contenus. On admettra que pour une forme cubique f on a $\sum_{i\leq r} e_i f_i = 3$; et ainsi ce symbole peut prendre les valeurs suivantes : $(111), (\overline{12}), (3), (1^21)$, et (1^3). Ce symbole est clairement invariant sous l'action de $GL_2(\mathbf{Z})$.
Soit alors $T_p(f,p)$ l'ensemble des formes f dont le symbole est (f,p). Il est clair que la structure du module quotient $A(f)/(p)$ ne dépend que des relations de structure modulo p, et donc de la classe de la réduction modulo p de f, modulo l'action de $GL_2(\mathbf{F}_p)$.
On note de plus que si $f \notin \mathcal{U}_p$, alors $T_p(f) = (1^21)$ ou (1^3).

Lemme 16. *On a les densités :*

$$\mu(T_p(111)) = \frac{1}{6}(p-1)^2p(p+1)/p^4$$

$$\mu(T_p(12)) = \frac{1}{2}(p-1)^2p(p+1)/p^4$$

$$\mu(T_p(3)) = \frac{1}{3}(p-1)^2p(p+1)/p^4$$

$$\mu(T_p(1^21)) = (p-1)p(p+1)/p^4$$

$$\mu(T_p(1^3)) = (p-1)(p+1)/p^4.$$

On vérifie d'ailleurs que la somme de ces densités vaut bien $(p^4-1)/p^4$ (on n'a pas compté la forme nulle).

Démonstration. Le dénominateur en p^4 correspond à chaque fois au nombre total de formes. On ne prouve que quelques cas, les autres étant laissés au lecteur, la démarche étant la même.
Pour la première, choisir une telle forme revient simplement à choisir ses 3 racines distinctes dans $\mathbf{P}^1(\mathbf{F}_p)$, ce qui donne un facteur $\binom{p+1}{3}$ ($p+1$ étant le cardinal de $\mathbf{P}^1(\mathbf{F}_p)$), et à se donner son coefficient dominant, pour lequel on a $p-1$ choix possibles.
Pour la troisième, on doit se donner un point de $\mathbf{P}^1(\mathbf{F}_{p^3})$, n'étant pas dans $\mathbf{P}^1(\mathbf{F}_p)$, les autres racines étant automatiquement ses conjugués ; cela donne (comme on compte chaque triplet trois fois) $\frac{1}{3}(p-1)^2 p$, que l'on multiplie par le facteur d'échelle $p-1$.
Pour la dernière, on se donne simplement une racine dans $\mathbf{P}^1(\mathbf{F}_p)$ et un coefficient dominant. □

Il nous reste à déterminer la densité de $\mathcal{U}_p$. Soit $\mathcal{U}_p(\cdot) = \mathcal{U}_p \cap T_p(\cdot)$.

Lemme 17. *On a :*

$$\mu(\mathcal{U}_p(111)) = \frac{1}{6}(p-1)^2 p(p+1)/p^4$$

$$\mu(\mathcal{U}_p(12)) = \frac{1}{2}(p-1)^2 p(p+1)/p^4$$

$$\mu(\mathcal{U}_p(3)) = \frac{1}{3}(p-1)^2 p(p+1)/p^4$$

$$\mu(\mathcal{U}_p(1^2 1)) = (p-1)^2(p+1)/p^4$$

$$\mu(\mathcal{U}_p(1^3)) = (p-1)^2(p+1)/p^5.$$

Démonstration. On rappelle que le discriminant d'un polynôme est le produit des carrés des différences de ses racines ; ainsi il est nul si et seulement si le polynôme admet une racine double (en supposant a non divisible par p, ce qui est possible par changement de variable linéaire). Ainsi, comme dans les trois premiers cas on n'a que des racines distinctes, le discriminant de f est systématiquement premier à p ; et si $A(f)$ était d'indice p dans A' on aurait $Disc(A') = Disc(A)/p$, donc dans les 3 premiers cas A est maximal et $T_p = \mathcal{U}_p$.
Si $f \in T_p(1^2 1)$ ou $T_p(1^3)$, on peut toujours envoyer, par une transformation linéaire, l'unique racine de f dans $\mathbf{P}^1(\mathbf{F}_p)$ sur le point $(1,0)$; cette racine étant au moins double on est ramené au cas $a \equiv b \equiv 0[p]$. Reste à assurer $a \equiv 0[p^2]$: ceci est réalisé une fois sur p dans ces conditions ; et avec le facteur d'échelle on a donc multiplié la densité de T_p par un facteur $(p-1)/p$. □

En sommant sur les différents T_p, on a calculé la densité de $\mathcal{U}_p$:

Proposition 38.

$$\mu(\mathcal{U}_p) = (p^3-1)(p^2-1)/p^5.$$

6.5 Passage à la limite

Cas cubique

On utilise maintenant les calculs de densité précédents pour passer à la limite, et relier nos estimations sur les formes binaires aux quantités arithmétiques qui nous intéressent. Soit $\mathcal{Z}_p = V_{\mathbf{Z}} - \mathcal{U}_p$ l'ensembles des formes non maximales en p ; on a l'estimation suivante :

Lemme 18. *On a $N(\mathcal{Z}_p, X) = \mathcal{O}(X/p^3)$, uniformément en p.*

Démonstration. En effet, on a vu que le nombre de sous-ordres d'indice p d'un ordre donné était toujours fini (à isomorphisme près) ; et on a un nombre fini d'ordres non maximaux en p de discriminant D ; ils sont donnés par des sous-ordres des ordres de discriminant inférieur à X/p^d ; dont le nombre est en CX. Le lemme s'ensuit. □

Soit alors $\mathcal{U} = \bigcap_p \mathcal{U}_p$. On a montré plus haut :

$$\lim_{X\to\infty} \frac{N(\bigcap_{p\leq Y} \mathcal{U}_p \cap V_{\mathbf{Z}}^i; X)}{N(V_{\mathbf{Z}}^i; X)} = \prod_{p\leq Y} \mu(\mathcal{U}_p)$$

La limite en $Y \to \infty$ donne :

$$\limsup_{X\to\infty} \frac{N(\mathcal{U} \cap V_{\mathbf{Z}}^i; X)}{N(V_{\mathbf{Z}}^i; X)} \leq \prod_{p} \mu(\mathcal{U}_p).$$

Reste à obtenir une borne inférieure ; pour cela on remarque que $\bigcap_{p\leq Y} \mathcal{U}_p \subset \mathcal{U} \cup \bigcup_{p>Y} \mathcal{Z}_p$; cela nous permet d'estimer le reste en Y :

$$\lim_{X\to\infty} \frac{N(\mathcal{U} \cap V_{\mathbf{Z}}^i; X)}{X} \geq \frac{\pi^2}{12 n_i} \prod_{p\leq Y} (1-p^{-2})(1-p^{-3}) + \mathcal{O}(\sum_{p>Y} p^{-3}).$$

Ainsi la limite $Y \to \infty$ donne :

$$N_i(X) = \frac{1}{2n_i\zeta(3)} X + o(X),$$

ce qui termine la preuve du théorème de Davenport-Heilbronn.

Cas quadratique

On va effectuer le même travail dans le cas quadratique en exploitant la correspondance de Gauss, ce qui va nous permettre, à partir de la formule de Siegel sur le nombres de classes de formes quadratiques, pas forcément primitives, de discriminant borné, de retrouver la somme restreinte aux formes primitives et de calculer un équivalent de la somme des cardinaux des groupes

de classes d'idéaux des corps quadratiques. En effet, cette somme s'obtient à partir de la précédente tout simplement en se restreignant aux discriminants *fondamentaux*, i.e. sans facteurs carrés autres qu'éventuellement 4. Cette restriction va faire apparaître, comme dans le cas cubique, un terme de densité.

Le caractère primitif en p d'une forme quadratique s'exprime localement par $(a,b,c) \neq 0$ dans $\mathbf{Z}/p\mathbf{Z}$; il est clair que la densité des formes primitives en p est $1-p^{-3}$. De plus, cette relation de congruence sur les coefficients est bien linéaire en les coefficients comme dans le cas cubique ; des arguments analogues permettent alors de retrouver le facteur $1/\zeta(3)$ obtenu par la méthode analytique comme $\prod_p 1-p^{-3}$, en se restreignant aux classes de formes primitives dans la formule $\sum_{D\leq N} h_{-D} \sim \frac{\pi}{18} N^{3/2}$.
En effet on a, comme dans le cas cubique, une estimation uniforme du nombre de formes non primitives en p et de discriminant $-D \leq X$ en $O(X^{3/2}/p^3)$, puisqu'à toute forme non primitive en p, de discriminant $-D \leq X$, on associe une forme de discriminant $D' = D/p^2$; celles-ci sont en nombre au plus $(X/p^2)^{3/2}$. Ainsi, par un calcul parfaitement analogue à celui effectué dans le cas cubique, on arrive à obtenir le facteur $1/\zeta(3)$, qui s'interprète heuristiquement comme la densité globale des formes primitives.

La maximalité d'une forme se traduit simplement par le fait que le discriminant soit sans facteurs carrés autres qu'éventuellement 4 : la non-maximalité en $p=2$ se traduit donc par $2^4|D$, et en $p \neq 2$ par $p^2|D$. Soit, comme dans le cas cubique, $\mathcal{U}_p$ l'ensemble des formes non maximales en p : la condition $f \in \bigcap_p \mathcal{U}_p$ correspond exactement à la condition D est un discriminant fondamental.
On calcule alors la densité locale de $\mathcal{U}_p$:

Lemme 19. *Dans le cas quadratique* $\mu(\mathcal{U}_p) = 1 - p^{-2} - p^{-3} + p^{-4}$.

Démonstration. On suppose ici $p \neq 2$; le cas $p=2$ étant évident. Il s'agit alors de compter les triplets (a,b,c) tels que $p^2|b^2-4ac$; cela dépend donc des classes résiduelles de (a,b,c) dans $(\mathbf{Z}/p^2\mathbf{Z})$. On commence par fixer b : s'il est divisible par p, 4 étant inversible, on doit avoir $ac=0$ donc soit $(a,c) \in ((\mathbf{Z}/p\mathbf{Z})^\times)^2$, soit $a=0$, soit $c=0$: ce cas nous donne alors $p((p-1)^2+2p^2-1) = 3p^3-2p^2-p$ possibilités. Si b est inversible modulo p^2, b^2 aussi, et en fixant un a inversible on a une unique solution c, ce qui donne $(p^2-p)^2$ solutions. Au final on a $p^4+p^3-p^2$ formes correspondant à un discriminant non maximal en p, pour un total de p^6 formes ; ce qui donne la densité annoncée. □

Chaque condition de congruence en p se traduit par un nombre fini de conditions de congruences sur les coefficients, i.e. être égaux modulo p à une des solutions de $b^2-4ac=0$ dans $\mathbf{Z}/p^2\mathbf{Z}$. Il s'ensuit, en prenant l'intersection

sur tous les p premiers :

$$\limsup_{X\to\infty} \frac{N(\mathcal{U}\cap V^i_{\mathbf{Z}};X)}{N(V^i_{\mathbf{Z}};X)} \leq \prod_p \mu(\mathcal{U}_p),$$

où $\mathcal{U}$ désigne l'ensemble des formes dont le discriminant est fondamental. Il reste alors à obtenir une borne inférieure ; afin de s'assurer que les conditions de congruence imposées ne "raréfient" pas trop l'ensemble des points considérés. Ces estimations peuvent s'obtenir en contrôlant le reste effectif obtenu à l'aide du principe de Lipschitz, en estimant la taille des projections de l'ensemble de points considéré ; nous ne donnerons pas les détails du calcul.
Ceci nous permet d'obtenir (dans le cas imaginaire uniquement) :

$$\sum_{K\in\mathcal{K}_X} h(K) = \prod_{p\in\mathbf{P}} (1-p^{-2}-p^{-3}+p^{-4})\frac{\pi}{18}X^{3/2}+o(X^{3/2}).$$

Conclusion

En fait, on dispose actuellement d'une conjecture qui généraliserait le théorème de Davenport-Heilbronn ; elle affirme la chose suivante : si $N_n(X)$ est le nombre de corps de nombres de degré n, dont la cloture galoisienne a pour groupe de Galois $\mathfrak{S}_n$(il s'agit de ce qu'on pourrait appeler le cas "standard"), alors la limite $c_n = \lim_{X\to\infty} \frac{N_n(X)}{X}$ existe, et elle prédit même la valeur de c_n :

$$c_n = \frac{r_2(\mathfrak{S}_n)}{2n!} \prod_{p\in\mathbf{P}} \sum_{k=0}^{n} \frac{q(k;n-k) - q(k-1;n-k+1)}{p^k},$$

où l'on définit $r_2(\mathfrak{S}_n)$ comme le nombre d'éléments de *2-torsion* de $\mathfrak{S}_n$, i.e. le nombre d'éléments de $\mathfrak{S}_n$ dont l'ordre est une puissance de 2 ; et les $q(i;j)$ comme le nombre de partitions de i en moins de j parties. Pour $n = 2$, le résultat est trivial ; pour $n = 3$ il s'agit du théorème de Davenport-Heilbronn. Les cas $n = 4, 5$ ont été résolus par Bhargava dans sa thèse en 2001. Cependant, pour $n \geq 6$, cette question reste ouverte et donne toujours lieu à de nombreuses recherches.

Références

[1] Karim Belabas. Paramétrisation de structures algébriques et densité de discriminants. 2004.

[2] Dorian M. Goldfeld. A simple proof of siegel's theorem. 1973.

[3] Jacob Tsimerman Manjul Bhargava, Arul Shankar. On the Davenport Heilbronn theorems and second order terms. 2012.

[4] Daniel A. Marcus. *Number Fields*. 1977.

[5] Pierre Samuel. *Théorie Algébrique Des Nombres*. 1967.

[6] Carl Ludwig Siegel. The average measure of quadratic forms with given determinant and signature. 1944.