La Somme de Trois Carrés

Li Ma.
Sujet proposé par : Y. Benoist.

avril 2007

Introduction

Étant donné un entier positif n, on s'intéresse au nombre des solutions entières de l'équation $x^2 + y^2 + z^2 = n$. Pour un certain diviseur d de n, on voit que les solutions entières (x, y, z) avec $\mathrm{pgcd}(x, y, z) = d$ sont en bijection avec les solutions entières de l'équation $x^2 + y^2 + z^2 = \frac{n}{d^2}$, donc on peut s'intéresser seulement aux solutions entières primitives, i.e., avec $\mathrm{pgcd}(x, y, z) = 1$.

Le but du texte est de montrer un résultat de Gauss, qui relie le nombre R_n des solutions entières primitives au nombres $h(-4n)$ des classes de formes quadratiques binaires primitives de discriminant $-4n$. Plus précisément, on montrera que, pour $n > 4$, $R_n/h(-4n)$ vaut 12 si $n \equiv 1, 2 \pmod 4$, vaut 8 si $n \equiv 3 \pmod 8$ et vaut 0 si $n \equiv 7 \pmod 8$. On ne regarde pas le cas où 4 divise n, car un argument modulo 4 implique immédiatement que R_n vaut 0 dans ce cas.

Dans la première partie, on établira une relation entre R_n et l'ensemble des triplets $(\Lambda, \mathfrak{b}, \overline{w})$, où Λ est un $\mathbb{Z}$-module libre de rang 2, $\mathfrak{b}$ est une forme bilinéaire de déterminant n sur Λ, et $\overline{w}$ est un élément de $\Lambda/n\Lambda^*$, tel que $\overline{\mathfrak{b}}(\overline{w}, \overline{w}) = \overline{-1} \in \mathbb{Z}/n\mathbb{Z}$. L'idée cruciale de cette partie est la suivante. Soit v une solution entière primitive, que l'on voit comme un vecteur dans $\mathbb{R}^3$, on note $\mathcal{P}$ le plan orthogonal de v dans $\mathbb{R}^3$. Alors v est déterminé (à une action de $\mathrm{SO}_3(\mathbb{Z})$ près) par la structure de trois éléments : l'intersection de $\mathcal{P}$ et $\mathbb{Z}^3$, la projection orthogonale de $\mathbb{Z}^3$ sur $\mathcal{P}$, et la "première couche" de $\mathbb{Z}^3$ le long de v.

Dans la deuxième partie, on comptera les classes des triplets $(\Lambda, \mathfrak{b}, \overline{w})$. Pour cela, on oubliera d'abord la composant $\overline{w}$. Comme on a une application canonique π qui envoie la classe de $(\Lambda, \mathfrak{b}, \overline{w})$ sur la classe de $(\Lambda, \mathfrak{b})$, il suffit de calculer le cardinal des fibres et de l'image. On introduira alors la "théorie de genres" pour les décrire. Un "genre" (de discriminant D) est une collection des formes quadratiques primitives de discriminant D qui représentent les mêmes valeurs dans $(\mathbb{Z}/D\mathbb{Z})^*$. On verra que l'image de π correspond juste à un genre de discriminant $-4n$ (si $n \equiv 1, 2 \pmod 4$) ou $-n$ (si $n \equiv 3 \pmod 4$). On donnera aussi une formule qui relie le nombre des classes de formes quadratiques dans un genre de discriminant D et le nombre $h(D)$, d'où on peut déduire une formule reliant le nombre des classes des triplets $(\Lambda, \mathfrak{b}, \overline{w})$ à $h(D)$.

Enfin, on combinera les résultats des deux parties et un petit lemme reliant $h(-n)$ à $h(-4n)$ pour obtenir la conclusion.

Dans le texte, rien n'est admis d'avance, sauf les résultats fondamentaux d'algèbre et le théorème de Dirichlet. Les outils importants sont : théorème de la base adaptée pour les $\mathbb{Z}$-modules ; lemme de Minkowski ; la structure de groupe sur les classes de formes quadratiques ; symbole de Jacobi et la loi de réciprocité quadratique de Gauss.

Table des matières

Introduction **1**

1 Première Partie **4**
1.1 Réseaux et formes bilinéaires 4
1.2 Énoncé du Théorème 5
1.3 Construction de ϕ 6
1.4 Injectivité de ϕ 9
1.5 Lemme de Minkowski 10
1.6 Surjectivité de ϕ 13

2 Deuxième Partie **16**
2.1 Classes de Formes Quadratiques 16
2.2 Théorie des Genres 22
2.3 Symbole de Jacobi 25
2.4 Théorie des Genres - Suite 28
2.5 Énoncés des Théorèmes 30
2.6 Preuve de Théorème 2.5.1 31
2.7 Preuve de Théorème 2.5.2 36

3 Conclusion **37**

1 Première Partie

On fixe un entier $n > 0$. Dans ce texte, toutes les formes bilinéaires sont symétriques et entières, sauf mention explicite.

1.1 Réseaux et formes bilinéaires

Soient Λ un $\mathbb{Z}$-module libre de rang 2, et $\mathfrak{b} : \Lambda \times \Lambda \to \mathbb{Z}$ une forme bilinéaire sur Λ. On suppose que $\mathfrak{b}$ est définie positive, de déterminant n et primitive. C'est-à-dire, si $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ est la matrice de $\mathfrak{b}$ dans une base de Λ, alors on a $a > 0$, $ac - b^2 = n$ et $\mathrm{pgcd}(a, b, c) = 1$. On note Λ^* le dual de Λ.

Proposition 1.1.1. *Il existe un morphisme injectif $\eta : \Lambda \hookrightarrow \Lambda^*$, telle que $\eta(v) = \mathfrak{b}(v, \cdot)$. Désormais, on identifie Λ avec $\mathrm{Im}(\eta)$. Dans cette identification, on a : $n\Lambda^* \subseteq \Lambda \subseteq \Lambda^*$.*

Démonstration η est bien un morphisme de $\mathbb{Z}$-modules. Il est injectif car $\mathfrak{b}$ est de déterminant non nul (et donc non dégénérée).

Soit (e_1, e_2) une base de Λ. On vérifie facilement que

$$\forall \lambda \in \Lambda^*, n\lambda = (c\lambda(e_1) - b\lambda(e_2))\eta(e_1) + (-b\lambda(e_1) + a\lambda(e_2))\eta(e_2).$$

Donc on a $n\Lambda^* \subseteq \Lambda$.

□

Comme $n\Lambda^* \subseteq \Lambda$, on a le quotient $\Lambda/n\Lambda^*$ et une forme bilinéaire $\overline{\mathfrak{b}}$: $(\Lambda/n\Lambda^*) \times (\Lambda/n\Lambda^*) \to \mathbb{Z}/n\mathbb{Z}$ définie par : $\overline{\mathfrak{b}}(\overline{u}, \overline{v}) = \overline{\mathfrak{b}(u, v)}$, où pour x entier, la notation $\overline{x}$ désigne la réduction de x modulo n, et pour u dans Λ, $\overline{u}$ est l'image de u dans $\Lambda/n\Lambda^*$. On voit que $\overline{\mathfrak{b}}$ est bien définie, car n divise $\mathfrak{b}(u, v)$ pour tout (u, v) dans $(\Lambda \times n\Lambda^*) \bigcup (n\Lambda^* \times \Lambda)$.

Lemme 1.1.1. *Soit $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ la matrice de $\mathfrak{b}$ dans une base de Λ, alors on a*

- $\mathrm{card}(\Lambda^*/\Lambda) = \mathrm{card}(\Lambda/n\Lambda^*) = n$,
- *les $\mathbb{Z}$-modules Λ^*/Λ et $\Lambda/n\Lambda^*$ sont isomorphes,*
- $\det(\mathfrak{b}|_{n\Lambda^*}) = n^3$.

Démonstration Soient (e_1, e_2) la base de Λ, et (f_1, f_2) la base duale de Λ^*. Alors on a $(e_1, e_2) = (f_1, f_2)\begin{pmatrix} a & b \\ b & c \end{pmatrix}$.

Comme $\Lambda \subseteq \Lambda^*$ sont des $\mathbb{Z}$-modules, il existe $\alpha_1, \alpha_2 \in \Lambda^*$ et $d_1, d_2 \in \mathbb{N}$, tels que (α_1, α_2) soit une base de Λ^*, d_1 divise d_2 et $(d_1\alpha_1, d_2\alpha_2)$ soit une base de Λ. Alors il existe $P, Q \in \mathrm{GL}_2(\mathbb{Z})$, telles que

$$\begin{aligned} (f_1, f_2) &= (\alpha_1, \alpha_2)P \\ (d_1\alpha_1, d_2\alpha_2) &= (e_1, e_2)Q \end{aligned}$$

Donc on a

$$(d_1\alpha_1, d_2\alpha_2) = (\alpha_1, \alpha_2)P\begin{pmatrix} a & b \\ b & c \end{pmatrix}Q.$$

Comme α_1, α_2 est une base de Λ^*, on a

$$P\begin{pmatrix} a & b \\ b & c \end{pmatrix}Q = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}.$$

En prenant la valeur absolue du déterminant, on a $d_1d_2 = n$. Comme Λ^*/Λ est isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}$, on a $\mathrm{card}(\Lambda^*/\Lambda) = d_1d_2 = n$.

De plus, on sait que $(n\alpha_1, n\alpha_2) = (d_1\alpha_1, d_2\alpha_2)\begin{pmatrix} d_2 & 0 \\ 0 & d_1 \end{pmatrix}$ est une base de $n\Lambda^*$, donc on a $\Lambda/n\Lambda^* \simeq \mathbb{Z}/d_2\mathbb{Z} \oplus \mathbb{Z}/d_1\mathbb{Z} \simeq \Lambda^*/\Lambda$.

Enfin, soit M la matrice de $\mathfrak{b}$ dans la base (α_1, α_2). Alors la matrice de $\mathfrak{b}|_{n\Lambda^*}$ est $\begin{pmatrix} d_2 & 0 \\ 0 & d_1 \end{pmatrix} M \begin{pmatrix} d_2 & 0 \\ 0 & d_1 \end{pmatrix}$, donc on a $\det(\mathfrak{b}|_{n\Lambda^*}) = n^2\det\mathfrak{b} = n^3$.

□

1.2 Énoncé du Théorème

On note $\mathfrak{R}_n$ l'ensemble des solutions entières primitives de l'équation $x^2 + y^2 + z^2 = n$, i.e.,

$$\mathfrak{R}_n := \{(x, y, z) \in \mathbb{Z}^3 : \mathrm{pgcd}(x, y, z) = 1, x^2 + y^2 + z^2 = n\}.$$

Le groupe $\mathrm{SO}_3(\mathbb{Z})$ agit sur $\mathfrak{R}_n$ par l'action usuelle, et on note $\mathfrak{r}_n := \mathfrak{R}_n/\mathrm{SO}_3(\mathbb{Z})$ l'ensemble des orbites sous cette action.

On note $\mathfrak{E}_n$ l'ensemble des triplets $(\Lambda, \mathfrak{b}, \overline{w})$, où

– Λ est un $\mathbb{Z}$-module libre de rang 2, qui est **orienté**, i.e., qui est muni d'une orientation,
– $\mathfrak{b}$ est une forme bilinéaire sur Λ, définie positive, de déterminant n et primitive,
– $\overline{w}$ est un élément de $\Lambda/n\Lambda^*$ (avec $w \in \Lambda$), tel que $\overline{b}(\overline{w}, \overline{w}) = \overline{-1}$.

Deux triplets $(\Lambda, \mathfrak{b}, \overline{w}), (\Lambda', \mathfrak{b}', \overline{w'}) \in \mathfrak{E}_n$ sont dits "isomorphes", s'il existe une application $\psi : \Lambda \to \Lambda'$, telle que
– ψ est un isomorphisme de $\mathbb{Z}$-modules, et préserve l'orientation,
– pour tout $u, v \in \Lambda$, on a $\mathfrak{b}(u, v) = \mathfrak{b}'(\psi(u), \psi(v))$,
– $\overline{\psi(w)} = \overline{w'}$ (cette condition est bien définie, car ψ induit un isomorphisme entre $n\Lambda^*$ et $n\Lambda'^*$).

Il est facile de voir que l'isomorphisme de triplets défini ci-dessus est une relation d'équivalence. On note $\mathfrak{e}_n$ l'ensemble des classes d'équivalence sous cette relation.

Maintenant on peut énoncer le théorème principal de la première partie.

Théorème 1.2.1. *Il existe une bijection $\phi : \mathfrak{r}_n \to \mathfrak{e}_n$.*

On va montrer ce théorème par 3 étapes :
1. Construire une application $\phi : \mathfrak{r}_n \to \mathfrak{e}_n$.
2. Montrer que ϕ est injective.
3. Montrer que ϕ est surjective.

On introduit d'abord les idées. Pour un élément v de $\mathfrak{R}_n$, on prend le plan orthogonal de v dans $\mathbb{R}^3$, noté $\mathcal{P}$. Il se découle alors que v est déterminé (à une action de $\mathrm{SO}_3(\mathbb{Z})$ près) par la structure de trois éléments : l'intersection de $\mathcal{P}$ et $\mathbb{Z}^3$, la projection orthogonale de $\mathbb{Z}^3$ sur $\mathcal{P}$, et la "première couche" de $\mathbb{Z}^3$, i.e., les points dans $\mathbb{Z}^3$ qui ont la plus petite distance strictement positive à $\mathcal{P}$ le long de v. Les trois choses correspondent respectivement à Λ, $\mathfrak{b}$ et $\overline{w}$ d'un triplet dans $\mathfrak{E}_n$. On montre l'injectivité en déduisant une transformation orthogonale sur $\mathbb{Z}^3$ d'un isomorphisme de triplets, et on montre le surjectivité en rétablisant le module $\mathbb{Z}^3$ (avec le produit euclidien) à partir d'un triplet dans $\mathfrak{E}_n$, à l'aide de lemme de Minkowski.

1.3 Construction de ϕ

On construit d'abord une application $\Phi : \mathfrak{R}_n \to \mathfrak{e}_n$. Dans la suite, on note $\langle \cdot, \cdot \rangle$ le produit scalaire euclidien sur $\mathbb{R}^3$.

Soit $v = (x, y, z)$ dans $\mathfrak{R}_n$. On prend le plan orthogonal $\mathcal{P}_v := \{u \in \mathbb{R}^3 : \langle u, v \rangle = 0\}$. Pour chaque u dans $\mathbb{R}^3$, on note $\pi_v(u)$ la projection orthogonale de u sur $\mathcal{P}_v$. On définit $\Phi(v)$ comme la classe d'équivalence de $(\Lambda_v, \mathfrak{b}_v, \overline{w_v})$, où

- $\Lambda_v = \pi_v(\mathbb{Z}^3)$, avec l'orientation induite par v,
- $\mathfrak{b}_v = n\langle \cdot, \cdot \rangle$,
- $w_v = \pi_v(w_0)$, où $w_0 \in \mathbb{Z}^3$ satisfait $\langle w_0, v \rangle = 1$ (par égalité de Bézout, un tel w_0 existe toujours).

Dans la suite, on va vérifier que Φ est bien définie, et qu'elle induit une application $\phi : \mathfrak{r}_n \to \mathfrak{e}_n$. On établit d'abord deux lemmes.

Lemme 1.3.1. *Pour $v \in \mathfrak{R}_n$, on a $n\Lambda_v^* = \mathbb{Z}^3 \bigcap \mathcal{P}_v$.*

Démonstration D'une part, soit u un élément de $\mathbb{Z}^3 \bigcap \mathcal{P}_v$, on a alors $u(\pi_v(x)) = n\langle u, x \rangle \in n\mathbb{Z}$ pour tout x dans $\mathbb{Z}^3$, donc u est dans $n\Lambda_v^*$.

D'autre part, soit λ dans Λ_v^*. On pose

$$u = (\lambda(\pi_v(1,0,0)), \lambda(\pi_v(0,1,0)), \lambda(\pi_v(0,0,1))) \in \mathbb{Z}^3,$$

alors u est dans $\mathcal{P}_v$, car $\langle u, v \rangle = \lambda(\pi_v(v)) = \lambda(0) = 0$. De plus, on a $n\lambda(\pi_v(x)) = n\langle u, x \rangle = n\langle u, \pi_v(x) \rangle = \mathfrak{b}_v(u, \pi_v(x))$ pour tout x dans $\mathbb{Z}^3$, donc $n\lambda = u \in \mathbb{Z}^3 \bigcap \mathcal{P}$.

□

Lemme 1.3.2. *Soit v dans $\mathbb{Z}^3$, écrivons $v = (x, y, z)$ avec x, y, z dans $\mathbb{Z}$. Si $\mathrm{pgcd}(x, y, z) = 1$, alors v peut s'étendre en une base de $\mathbb{Z}^3$.*

Démonstration Comme $\mathbb{Z}v$ est un sous-$\mathbb{Z}$-module de $\mathbb{Z}^3$ de rang 1, il existe une base (v_1, v_2, v_3) de $\mathbb{Z}^3$ et un entier positif d, tels que $\mathbb{Z}v = \mathbb{Z}(dv_1)$. Mais alors d divise v, et donc on a $d = 1$ car $\mathrm{pgcd}(x, y, z) = 1$. On en déduit que (v, v_2, v_3) est une base de $\mathbb{Z}^3$.

□

Proposition 1.3.1. *Pour tout v dans $\mathfrak{R}_n$, on a*

- *$\Phi(v)$ est un élément de $\mathfrak{e}_n$, et il est bien défini (i.e. ne dépend pas du choix de w_0 dans la définition).*
- *Pour tout g dans SO_3, on a $\Phi(gv) = \Phi(v)$.*

Démonstration Soit $v = (x, y, z) \in \mathfrak{R}_n$.Par le lemme précédent, v s'étend en une base (v, v_2, v_3) de $\mathbb{Z}^3$. De plus, on peut supposer que $\det(v, v_2, v_3) = 1$, quitte à remplacer v_3 par $-v_3$.

Il est facile de voir qu'on a des isomorphismes de $\mathbb{Z}$-modules $\Lambda_v \simeq \mathbb{Z}^3/\mathbb{Z}v \simeq \mathbb{Z}v_2 \oplus \mathbb{Z}v_3$, donc Λ_v est un $\mathbb{Z}$-module libre de rang 2. De plus, $(\pi_v(v_2), \pi_v(v_3))$ est une base positive de Λ_v, car $\det(v, v_2, v_3) = 1$.

Pour tout w dans $\mathbb{R}^3$, on a $\pi_v(w) = w - \frac{\langle w,v\rangle}{\langle v,v\rangle} v = w - \frac{\langle w,v\rangle}{n} v$. Alors pour $u_1, u_2 \in \mathbb{Z}^3$, on a

$$\mathfrak{b}_v(\pi_v(u_1), \pi_v(u_2)) = n\langle \pi_v(u_1), \pi_v(u_2)\rangle = n\langle u_1, u_2\rangle - \langle u_1, v\rangle\langle u_2, v\rangle \in \mathbb{Z}.$$

Donc $\mathfrak{b}_v$ est une forme bilinéaire sur Λ_v. $\mathfrak{b}_v$ est définie positive car $\langle \cdot, \cdot \rangle$ l'est. La matrice de $\mathfrak{b}_v$ dans la base $(\pi_v(v_2), \pi_v(v_3))$ est

$$B = \begin{pmatrix} n\langle v_2, v_2\rangle - \langle v_2, v\rangle^2 & n\langle v_2, v_3\rangle - \langle v_2, v\rangle\langle v_3, v\rangle \\ n\langle v_2, v_3\rangle - \langle v_2, v\rangle\langle v_3, v\rangle & n\langle v_3, v_3\rangle - \langle v_3, v\rangle^2 \end{pmatrix}.$$

Notons $A = (v, v_2, v_3)$, alors $\det B = n \cdot \det({}^tAA) = n \cdot \det(A)^2 = n$. Soit p un nombre premier quelconque. Supposons que p divise tous les coefficients de B, alors p divise $\det B = n = \langle v, v\rangle$. Donc p divise aussi $\langle v_2, v\rangle$, car p divise $n\langle v_2, v_2\rangle - \langle v_2, v\rangle^2$. De même, p divise $\langle v_3, v\rangle$. Mais alors p divise la première ligne de ${}^tAA$, cela contredit le fait que $\det({}^tAA) = 1$.

On en conclut que $\mathfrak{b}_v$ est définie positive, de déterminant n et primitive.

On vérifie ensuite que $\overline{w_v} = \overline{\pi_v(w_0)}$ est bien définie. Soit w_1 un élément de $\mathbb{Z}^3$ tel que $\langle w_1, v\rangle = 1$, alors $\langle w_1 - w_0, v\rangle$ est nul. Donc on a

$$\pi_v(w_1) - \pi_v(w_0) = \pi_v(w_1 - w_0) = w_1 - w_0 \in \mathbb{Z}^3 \bigcap \mathcal{P}_v = n\Lambda^*$$

d'après le lemme précédent, i.e., $\overline{\pi_v(w_1)} = \overline{\pi_v(w_0)}$. De plus, on a

$$\overline{\mathfrak{b}}(\overline{w_v}, \overline{w_v}) = \overline{\mathfrak{b}(\pi_v(w_0), \pi_v(w_0))} = \overline{n\langle w_0, w_0\rangle - \langle w_0, v\rangle^2} = \overline{-1}.$$

Donc on a montré que $\Phi(v) \in \mathfrak{e}_n$ est bien défini.

Enfin, soit g un élément de $\mathrm{SO}_3(\mathbb{Z})$, alors l'application $u \mapsto g(u)$ est bien un isomorphisme de $(\Lambda_v, \mathfrak{b}_v, \overline{w_v})$ vers $(\Lambda_{gv}, \mathfrak{b}_{gv}, \overline{w_{gv}})$.

□

Grâce à la proposition précédente, on peut définir $\phi([v]) = \Phi(v)$ pour tout v dans $\mathfrak{R}_n$, où $[v] \in \mathfrak{r}_n$ est l'orbite de v. Cela définit bien une application de $\mathfrak{r}_n$ dans $\mathfrak{e}_n$.

1.4 Injectivité de ϕ

L'injectivité de ϕ est donnée par la proposition suivante.

Proposition 1.4.1. *Soient v, v' deux éléments de $\mathfrak{R}_n$. Si $(\Lambda_v, \mathfrak{b}_v, \overline{w_v})$ et $(\Lambda_{v'}, \mathfrak{b}_{v'}, \overline{w_{v'}})$ sont isomorphes, alors il existe $P \in SO_3(\mathbb{Z})$, telle que $Pv = v'$.*

Démonstration Soit ψ un isomorphisme de $(\Lambda_v, \mathfrak{b}_v, \overline{w_v})$ vers $(\Lambda_{v'}, \mathfrak{b}_{v'}, \overline{w_{v'}})$. Soit (f_1, f_2) une base de $n\Lambda_v^*$, alors $(\psi(f_1), \psi(f_2))$ est une base de $n\Lambda_{v'}^*$. Soit f_3 dans $\mathbb{Z}^3$ tel que $\langle f_3, v\rangle = 1$, alors on peut supposer que $w_v = \pi_v(f_3)$. On pose $f'_i = \psi(f_i)$ pour $i = 1, 2$, et $f'_3 = \psi(w_v) + \frac{v'}{n}$.

Soit w dans $\mathbb{Z}^3$ tel que $\langle w, v'\rangle = 1$, alors $\overline{\pi_{v'}(w)} = \overline{w_{v'}} = \overline{\psi(w_v)}$. Comme $\pi_{v'}(w) = w - \frac{\langle w,v'\rangle}{n} v' = w - \frac{v'}{n}$, on a $f'_3 - w \in n\Lambda_{v'}^* \subseteq \mathbb{Z}^3$. Donc f'_3 est dans $\mathbb{Z}^3$, et $\langle f'_3, v'\rangle = 1$.

Il est facile de voir que les f_i forment une base de $\mathbb{Z}^3$. En fait, chaque $u \in \mathbb{Z}^3$ s'écrit uniquement sous la forme $kf_3 + u_0$ avec $k \in \mathbb{Z}$ et $u_0 \in n\Lambda_v^*$ (i.e., avec $k = \langle u, v\rangle$ et $u_0 = u - kf_3$), donc $\mathbb{Z}^3 = n\Lambda_v^* \oplus \mathbb{Z}f_3 = \mathbb{Z}f_1 \oplus \mathbb{Z}f_2 \oplus \mathbb{Z}f_3$.

De même, les f'_i forment aussi une base de $\mathbb{Z}^3$.

Il existe donc une matrice $P \in \mathrm{GL}_3(\mathbb{Z})$, telle que $P(f_1, f_2, f_3) = (f'_1, f'_2, f'_3)$. On va montrer qu'en fait P est dans $\mathrm{SO}_3(\mathbb{Z})$.

Comme ψ préserve l'orientation, on sait que $\det(f_1, f_2, v)$ et $\det(f'_1, f'_2, v')$ ont même signe. Mais $f_3 - \frac{v}{n} = \pi(f_3)$ est une combinaison ($\mathbb{Q}$-)linéaire de f_1, f_2, donc $\det(f_1, f_2, f_3)$ et $\det(f_1, f_2, v)$ ont même signe. De même, $\det(f'_1, f'_2, f'_3)$ et $\det(f'_1, f'_2, v')$ ont même signe. On voit alors que $\det(f_1, f_2, f_3)$ et $\det(f'_1, f'_2, f'_3)$ ont même signe, i.e., P est dans $\mathrm{SL}_3(\mathbb{Z})$. De plus, pour tout i, j dans $\{1, 2\}$, on a

$$\begin{aligned}
\langle f_i, f_j\rangle &= \frac{1}{n}\mathfrak{b}_v(f_i, f_j) = \frac{1}{n}\mathfrak{b}_{v'}(f'_i, f'_j) = \langle f'_i, f'_j\rangle \\
\langle f_i, f_3\rangle &= \frac{1}{n}\langle f_i, w_v\rangle = \frac{1}{n}\mathfrak{b}_{v'}(f'_i, \psi(w_v)) = \langle f'_i, f'_3\rangle \\
\langle f_3, f_3\rangle &= \langle w_v, w_v\rangle + \frac{1}{n^2}\langle v, v\rangle = \langle \psi(w_v), \psi(w_v)\rangle + \frac{1}{n^2}\langle v', v'\rangle = \langle f'_3, f'_3\rangle
\end{aligned}$$

Donc P préserve la distance euclidienne, i.e., P est dans $\mathrm{SO}_3(\mathbb{Z})$.

Écrivons $v = af_1 + bf_2 + nf_3$ avec a, b dans $\mathbb{Z}$, alors on a

$$\begin{aligned} & af'_1 + bf'_2 + nf'_3 - v' \\ = \ & a\psi(f_1) + b\psi(f_2) + n\psi(\pi(f_3)) \\ = \ & \psi(\pi(af_1 + bf_2 + nf_3)) \\ = \ & \psi(\pi(v)) \ = \ \psi(0) \ = \ 0, \end{aligned}$$

donc $v' = af'_1 + bf'_2 + nf'_3 = Pv$.

$\square$

Avant montrer la surjectivité de ϕ, on introduit le lemme de Minkowski.

1.5 Lemme de Minkowski

Définition 1.5.1. *Une matrice symétrique définie positive* $\begin{pmatrix} a & b \\ b & c \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z})$, *où a, b, c sont des entiers, est dite* ***réduite****, si on a* $2|b| \leq a \leq c$.

Lemme 1.5.1. *Soit $M \in \mathrm{M}_2(\mathbb{Z})$ une matrice réduite. Écrivons* $M = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ *avec a, b, c des entiers, alors on a* $a \leq \frac{2}{\sqrt{3}}\sqrt{det(M)}$. *En particulier, si le déterminant de M est 1, alors on a* $M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Démonstration Comme $\det(M) = ac - b^2 \geq \frac{3}{4}a^2$, on a $a \leq \frac{2}{\sqrt{3}}\sqrt{\det(M)}$. Si $\det(M)$ est 1, alors on a $a \leq \frac{2}{\sqrt{3}}$, donc $a = 1$. Comme $2|b| \leq a = 1$, on a $b = 0$, et alors $c = 1$.

$\square$

Lemme 1.5.2. *Soient E un $\mathbb{Z}$-module libre de rang 2 et $\beta : E \times E \to \mathbb{Z}$ une forme bilinéaire définie positive sur E. Alors il existe une base de E, telle que la matrice de β dans cette base est une matrice réduite.*

Démonstration On peut supposer que E soit $\mathbb{Z}^2$.

Comme β est définie positive, on sait que $a := \min\{\beta(\tilde{v}, \tilde{v}) : \tilde{v} \in E\}$ est un entier positif. Alors il existe v dans E, tel que $a = \beta(v, v)$. Écrivons $v = (x, y)$ avec x, y dans $\mathbb{Z}$, alors on a $\mathrm{pgcd}(x, y) = 1$. Par égalité de Bézout, il existe v' dans $\mathbb{Z}^2$, tel que (v, v') est une base de $\mathbb{Z}^2$. La matrice de β dans la base (v, v') s'écrit donc comme $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ avec b, c dans $\mathbb{Z}$.

Quitte à remplacer v' par $v' + kv$ pour un certain entier k, on peut supposer que $2|b| \leq a$. De plus, par la définition de a, on a $a \leq c$ car $c = \beta(v', v')$ est un élément de $\{\beta(\tilde{v}, \tilde{v}) : \tilde{v} \in E\}$.

Donc la matrice $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ est réduite, et (v, v') est la base voulue.

$\square$

Proposition 1.5.1. *(Lemme de Minkowski) Soient E un $\mathbb{Z}$-module libre de rang 3 et $\beta : E \times E \to \mathbb{Z}$ une forme bilinéaire définie positive sur E, de déterminant 1. Alors il existe une base de E, telle que la matrice de β dans cette base est* $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Démonstration On peut supposer que E soit $\mathbb{Z}^3$.

Comme β est définie positive, on a $a := \min\{\beta(\tilde{v}, \tilde{v}) : \tilde{v} \in E\}$ est un entier positif. Alors il existe v dans E, tel que $a = \beta(v, v)$. Écrivons $v = (x, y, z)$ avec x, y, z dans $\mathbb{Z}$, alors on a $\mathrm{pgcd}(x, y, z) = 1$. Par lemme 1.3.2, il existe v', v'' dans E, tels que (v, v', v'') est une base de E. La matrice de β dans la base (v, v', v''), notée M, s'écrit donc comme $\begin{pmatrix} a & d & f \\ d & b & e \\ f & e & c \end{pmatrix}$ avec b, c, d, e, f dans $\mathbb{Z}$.

Posons $P := \begin{pmatrix} a & d & f \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, alors on a $\det(P) = a$ et l'égalité suivante

$$ {}^tP \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} P = aM, $$

ici on a posé $A := \begin{pmatrix} ab - d^2 & ae - df \\ ae - df & ac - f^2 \end{pmatrix}$. En prenant les déterminants, on a $\det(A) = a \cdot \det(M) = a$.

Par le lemme précédent, il existe une matrice T dans $\mathrm{GL}_2(\mathbb{Z})$, telle que ${}^tTAT$ est une matrice réduite.

On pose $Q := \begin{pmatrix} 1 & 0 \\ 0 & T \end{pmatrix}$, alors Q est dans $\mathrm{GL}_2(\mathbb{Z})$. Notons $(u, u', u'') := (v, v', v'')Q$ et M' la matrice de β dans la base (u, u', u''). Écrivons $M' = \begin{pmatrix} a' & d' & f' \\ d' & b' & e' \\ f' & e' & c' \end{pmatrix}$ avec a', b', c', d', e', f' des entiers, on a alors

$$M' = {}^tQMQ = \begin{pmatrix} a & \begin{pmatrix} d & f \end{pmatrix} T \\ {}^tT \begin{pmatrix} d \\ f \end{pmatrix} & {}^tT \begin{pmatrix} b & e \\ e & c \end{pmatrix} T \end{pmatrix},$$

donc on a $a' = a$ et $(d', f') = (d, f)T$. Posons $P' := \begin{pmatrix} a' & d' & f' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, alors on voit que $QP' = \begin{pmatrix} a' & \begin{pmatrix} d' & f' \end{pmatrix} \\ 0 & T \end{pmatrix} = PQ$.

Notons $A' := \begin{pmatrix} a'b' - d'^2 & a'e' - d'f' \\ a'e' - d'f' & a'c' - f'^2 \end{pmatrix}$. On a l'égalité suivante

$$\begin{aligned} {}^tP' \begin{pmatrix} 1 & 0 \\ 0 & A' \end{pmatrix} P' &= aB' = {}^tQ(aB)Q = {}^tQ\,{}^tP \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} PQ \\ &= {}^tP'\,{}^tQ \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} QP'. \end{aligned}$$

Comme $\det(P') = a'$ n'est pas nul, P' est inversible (en tant que matrice sur $\mathbb{Q}$). Donc on a

$$\begin{pmatrix} 1 & 0 \\ 0 & A' \end{pmatrix} = {}^tQ \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} Q = \begin{pmatrix} 1 & 0 \\ 0 & {}^tTAT \end{pmatrix}.$$

On en déduit que $A' = {}^tTAT$ est réduite et de déterminant a. Par lemme 1.5.1, on a $a'b' - d'^2 \leq \frac{2}{\sqrt{3}}\sqrt{a}$.

Soient k, t des entiers tels que $2|d' + ka'| \leq a'$ et $2|f' + ta'| \leq a'$. Notons $(w, w', w'') = (u, u', u'') \begin{pmatrix} 1 & k & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et M'' la matrice de β dans la base

(w, w', w''). Écrivons $M'' = \begin{pmatrix} a'' & d'' & f'' \\ d'' & b'' & e'' \\ f'' & e'' & c'' \end{pmatrix}$ avec $a'', b'', c'', d'', e'', f''$ des entiers, alors on a $a'' = a' = a$, $d'' = d' + ka'$, $f'' = f' + ta'$, $b'' = b' + 2ka'$, d'où on peut déduire les inégalités suivantes

$$\begin{aligned} \max(2|d''|, 2|f''|) &\leq a \\ a''b'' - d''^2 = a'b' - d'^2 - (ka')^2 &\leq \frac{2}{\sqrt{3}}\sqrt{a}. \end{aligned}$$

De plus, on sait que $a \leq b''$ car $b'' = \beta(w'', w'') \in \{\beta(\tilde{v}, \tilde{v}) : \tilde{v} \in E\}$. Donc on a $\frac{2}{\sqrt{3}}\sqrt{a} \geq a''b'' - d''^2 \geq \frac{3}{4}a^2$, i.e., $a \leq \frac{4}{3}$. Alors $a = a'' = 1$, et $d'' = f'' = 0$.

La matrice M'' s'écrit donc comme $\begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}$ avec $N \in \mathrm{M}_2(\mathbb{Z})$ une matrice définie positive et de déterminant 1. Par le lemme précédent, on peut supposer que N est réduite. Par lemme 1.5.1, on a $N = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, et donc $M'' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, i.e., (w, w', w'') est la base voulue.

□

1.6 Surjectivité de ϕ

Lemme 1.6.1. *Soit $(\Lambda, \mathfrak{b}, \overline{w})$ dans $\mathfrak{E}_n$. Alors le groupe $\Lambda/n\Lambda^*$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, et $\overline{w}$ en est un générateur.*

Démonstration Comme $\overline{\mathfrak{b}}(\overline{w}, \overline{w}) = \overline{-1}$, on a $\overline{\mathfrak{b}}(\overline{kw}, \overline{w}) = \overline{-k} \neq \overline{0}$ pour tout entier k tel que $0 < k < n$. Donc $\overline{kw}$ n'est pas nul pour tout $0 < k < n$. Or, le cardinal de $\Lambda/n\Lambda^*$ est n, d'où le résultat.

□

Maintenant on peut montrer la surjectivité de ϕ.

Proposition 1.6.1. *Soit $(\Lambda, \mathfrak{b}, \overline{w})$ un élément de $\mathfrak{E}_n$. Alors il existe $v \in \mathfrak{R}_n$, tel que $(\Lambda, \mathfrak{b}, \overline{w})$ et $(\Lambda_v, \mathfrak{b}_v, \overline{w_v})$ sont isomorphes.*

Démonstration Soit (f_1, f_2) une base positive de $n\Lambda^*$. Choisissons un relevé $w \in \Lambda$ de $\overline{w}$ et écrivons $nw = af_1 + bf_2$ avec a, b dans $\mathbb{Z}$. Remarquons que $\mathrm{pgcd}(n, a, b) = 1$. En fait, soit d un entier tel que d divise n, a, b et $d > 1$, alors on a $\frac{n}{d}w = \frac{a}{d}f_1 + \frac{b}{d}f_2 \in n\Lambda^*$. Mais cela contredit le lemme précédent.

Introduisons un $\mathbb{Z}$-module libre de rang 3 de base $(\tilde{f}_1, \tilde{f}_2, \tilde{f}_3)$, et définissons une forme bilinéaire $\beta(\cdot,\cdot)$ sur ce module, par les formules suivantes : pour tout i, j dans $\{1, 2\}$, on pose

$$\begin{aligned}
\beta(\tilde{f}_i, \tilde{f}_j) &= \frac{1}{n}\mathfrak{b}(f_i, f_j) \\
\beta(\tilde{f}_i, \tilde{f}_3) &= \frac{1}{n}\mathfrak{b}(f_i, w) \\
\beta(\tilde{f}_3, \tilde{f}_3) &= \frac{1}{n}(\mathfrak{b}(w, w) + 1).
\end{aligned}$$

Posons $\tilde{v} := n\tilde{f}_3 - a\tilde{f}_1 - b\tilde{f}_2$, alors on a

$$\begin{aligned}
\beta(\tilde{v}, \tilde{v}) &= n(\mathfrak{b}(w, w) + 1) - 2\mathfrak{b}(af_1 + bf_2, w) + \frac{1}{n}\mathfrak{b}(af_1 + bf_2, af_1 + bf_2) \\
&= n\mathfrak{b}(w, w) + n - 2\mathfrak{b}(nw, w) + \frac{1}{n}\mathfrak{b}(nw, nw) \\
&= n.
\end{aligned}$$

De même, on calcule que $\beta(\tilde{v}, \tilde{f}_i) = 0$ pour $i = 1, 2$, et que $\beta(\tilde{v}, \tilde{f}_3) = 1$.

On va montrer que β est définie positive et $\det\beta = 1$. Comme

$$\begin{aligned}
\beta(\tilde{f}_1, \tilde{f}_1) &= \frac{1}{n}\mathfrak{b}(f_1, f_1) > 0 \\
\det\begin{pmatrix} \beta(\tilde{f}_1, \tilde{f}_1) & \beta(\tilde{f}_1, \tilde{f}_2) \\ \beta(\tilde{f}_2, \tilde{f}_1) & \beta(\tilde{f}_2, \tilde{f}_2) \end{pmatrix} &= \frac{1}{n^2}(\mathfrak{b}(f_1, f_1)\mathfrak{b}(f_2, f_2) - \mathfrak{b}(f_1, f_2)^2) > 0,
\end{aligned}$$

il suffit de montrer que $\det\beta = 1$. Or, on a

$$\begin{aligned}
n^2\det\beta &= \det\begin{pmatrix} \beta(\tilde{f}_1, \tilde{f}_1) & \beta(\tilde{f}_1, \tilde{f}_2) & \beta(\tilde{f}_1, n\tilde{f}_3) \\ \beta(\tilde{f}_2, \tilde{f}_1) & \beta(\tilde{f}_2, \tilde{f}_2) & \beta(\tilde{f}_2, n\tilde{f}_3) \\ \beta(n\tilde{f}_3, \tilde{f}_1) & \beta(n\tilde{f}_3, \tilde{f}_2) & \beta(n\tilde{f}_3, n\tilde{f}_3) \end{pmatrix} \\
&= \det\begin{pmatrix} \beta(\tilde{f}_1, \tilde{f}_1) & \beta(\tilde{f}_1, \tilde{f}_2) & \beta(\tilde{f}_1, \tilde{v}) \\ \beta(\tilde{f}_2, \tilde{f}_1) & \beta(\tilde{f}_2, \tilde{f}_2) & \beta(\tilde{f}_2, \tilde{v}) \\ \beta(\tilde{v}, \tilde{f}_1) & \beta(\tilde{v}, \tilde{f}_2) & \beta(\tilde{v}, \tilde{v}) \end{pmatrix} \\
&= n \cdot \det\begin{pmatrix} \frac{1}{n}\mathfrak{b}(f_1, f_1) & \frac{1}{n}\mathfrak{b}(f_1, f_2) \\ \frac{1}{n}\mathfrak{b}(f_2, f_1) & \frac{1}{n}\mathfrak{b}(f_2, f_2) \end{pmatrix} \\
&= \frac{1}{n}\det(b|_{n\Lambda^*}).
\end{aligned}$$

Par lemme 1.1.1, on a $\det(b|_{n\Lambda^*}) = n^3$, donc $\det\beta$ vaut 1.

Par lemme de Minkowski, il existe une base (e_1, e_2, e_3) de $\mathbb{Z}\tilde{f}_1 \oplus \mathbb{Z}\tilde{f}_2 \oplus \mathbb{Z}\tilde{f}_3$, telle que la matrice de β dans cette base est $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Dans la suite, on identifie (e_1, e_2, e_3) avec la base canonique de $\mathbb{Z}^3$, et β s'identifie donc au produit scalaire euclidien $\langle \cdot, \cdot \rangle$. De plus, on peut supposer que $\det(\tilde{f}_1, \tilde{f}_2, \tilde{f}_3) > 0$, quitte à remplacer e_1 avec $-e_1$.

Comme on a $\langle \tilde{v}, \tilde{v} \rangle = n$ et $\tilde{v} = n\tilde{f}_3 - a\tilde{f}_1 - b\tilde{f}_2$ avec $\mathrm{pgcd}(n, a, b) = 1$, $\tilde{v}$ est bien un élément de $\mathfrak{R}_n$.

On va montrer que $(\Lambda_{\tilde{v}}, \mathfrak{b}_{\tilde{v}}, \overline{w_{\tilde{v}}})$ et $(\Lambda, \mathfrak{b}, \overline{w})$ sont isomorphes. Notons que

$$\begin{array}{rcl} n\Lambda_{\tilde{v}}^* & = & \{u \in \mathbb{Z}^3 : \beta(u, \tilde{v}) = 0\} \\ & = & \{p\tilde{f}_1 + q\tilde{f}_2 + r\tilde{f}_3 : \beta(p\tilde{f}_1 + q\tilde{f}_2 + r\tilde{f}_3, \tilde{v}) = 0\} \\ & = & \{p\tilde{f}_1 + q\tilde{f}_2 + r\tilde{f}_3 : r = 0\} \\ & = & \mathbb{Z}\tilde{f}_1 \oplus \mathbb{Z}\tilde{f}_2, \end{array}$$

on a donc un isomorphisme $\psi : n\Lambda_{\tilde{v}}^* \mapsto n\Lambda^*$, tel que $\psi(\tilde{f}_i) = f_i$ pour $i = 1, 2$. On a encore $\langle \tilde{f}_3, \tilde{v} \rangle = 1$, donc $\overline{w_{\tilde{v}}} = \overline{\pi_{\tilde{v}}(\tilde{f}_3)}$. Par lemme 1.6.1, $\overline{\pi_{\tilde{v}}(\tilde{f}_3)}$ et $\overline{w}$ sont respectivement des générateurs de $\Lambda_{\tilde{v}}/n\Lambda_{\tilde{v}}^*$ et de $\Lambda/n\Lambda^*$, et on a

$$\psi(n\pi_{\tilde{v}}(\tilde{f}_3)) = \psi(\pi_{\tilde{v}}(\tilde{v} + a\tilde{f}_1 + b\tilde{f}_2)) = \psi(a\tilde{f}_1 + b\tilde{f}_2) = nw,$$

donc ψ s'étend à un isomorphisme de $\Lambda_{\tilde{v}}$ à Λ, que l'on note aussi ψ, tel que $\psi(\pi_{\tilde{v}}(\tilde{f}_3)) = w$. On a donc $\overline{\psi(w_{\tilde{v}})} = \overline{w}$.

De plus, $\det(\tilde{f}_1, \tilde{f}_2, \tilde{v})$ est positif car $\det(\tilde{f}_1, \tilde{f}_2, \tilde{f}_3)$ l'est. Donc $(\tilde{f}_1, \tilde{f}_2)$ est une base positive de $n\Lambda_{\tilde{v}}^*$. Comme $(\psi(\tilde{f}_1), \psi(\tilde{f}_2)) = (f_1, f_2)$ est aussi une base positive de $n\Lambda^*$, on voit que ψ préserve l'orientation.

Il reste donc à montrer que $\mathfrak{b}_{\tilde{v}}(x, y) = \mathfrak{b}(\psi(x), \psi(y))$ pour tout $x, y \in \Lambda_{\tilde{v}}$. Mais cela découle juste de la construction de β.

□

On a bien montré que ϕ est une bijection de $\mathfrak{r}_n$ dans $\mathfrak{e}_n$. En particulier, on a $\mathrm{card}(\mathfrak{r}_n) = \mathrm{card}(\mathfrak{e}_n)$.

Terminons cette partie par une relation entre $\mathrm{card}(\mathfrak{r}_n)$ et $\mathrm{card}(\mathfrak{R}_n)$.

Proposition 1.6.2. *Si $n > 3$, alors pour tout v dans $\mathfrak{R}_n$, on a* $\mathrm{card}([v]) = 24$*, où $[v] \in \mathfrak{r}_n$ est l'orbite de v sous l'action de* $\mathrm{SO}_3(\mathbb{Z})$*.*

Démonstration Comme $\mathrm{card}(\mathrm{SO}_3(\mathbb{Z})) = 24$, il suffit de montrer que, pour tout v dans $\mathfrak{R}_n$, le stabilisateur de v est constitué seulement par $\mathrm{Id} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Soient v dans $\mathfrak{R}_n$ et g dans $\mathrm{SO}_3(\mathbb{Z})$, tels que $gv = v$. Montrons que $g = \mathrm{Id}$. Écrivons $v = (x, y, z)$ avec x, y, z dans $\mathbb{Z}$, on a trois cas :

Si les valeurs absolues de x, y, z sont non nulles et deux-à-deux différentes, alors il est évident que $g = \mathrm{Id}$.

Si $|x|$ est nulle, alors on a $y^2 + z^2 = n$ et $\mathrm{pgcd}(y, z) = 1$. On en déduit que $|y|, |z|$ sont non nulles et différentes (car $n > 3$). Donc $g = \begin{pmatrix} \epsilon & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ avec ϵ dans $\{\pm 1\}$, et alors $g = \mathrm{Id}$.

Si $|x|, |y|, |z|$ sont non nulles mais $|x| = |y|$, alors on a $2x^2 + z^2 = n$ et $\mathrm{pgcd}(x, z) = 1$. On en déduit que $|x|, |z|$ sont différentes (car $n > 3$). Notons $\epsilon := x/y \in \{\pm 1\}$, alors on a $g = \mathrm{Id}$ ou $g = \begin{pmatrix} 0 & \epsilon & 0 \\ \epsilon & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Donc $g = \mathrm{Id}$.

□

Par la proposition précédente, on a $\mathrm{card}\mathfrak{R}_n = 24\mathrm{card}\mathfrak{r}_n = 24\mathrm{card}\mathfrak{e}_n$. Donc pour compter $\mathfrak{R}_n$, il suffit de compter $\mathfrak{e}_n$.

2 Deuxième Partie

2.1 Classes de Formes Quadratiques

Soit D un entier négatif tel que $D \equiv 0, 1 \pmod 4$. Notons

$$\mathcal{Q}(D) := \{aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y] : a > 0, b^2 - 4ac = D, \mathrm{pgcd}(a, b, c) = 1\}.$$

Le groupe $\mathrm{SL}_2(\mathbb{Z})$ agit sur $\mathcal{Q}(D)$ de façon suivante :

$$\begin{aligned} & \begin{pmatrix} p & q \\ r & s \end{pmatrix} \cdot (aX^2 + bXY + cY^2) \\ = \quad & a(pX + qY)^2 + b(pX + qY)(rX + sY) + c(rX + sY)^2. \end{aligned}$$

On note $\mathcal{C}(D)$ l'ensemble des orbites sous cette action.

Proposition 2.1.1. *Le cardinal de $\mathcal{C}(D)$ est fini.*

Démonstration Soit $aX^2 + bXY + cY^2$ une forme dans $\mathcal{Q}(D)$ avec a, b, c des entiers. On pose $M_f := \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ (si b est pair) ou $\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$ (si b est impair) , alors M_f peut être vue comme une forme bilinéaire sur $\mathbb{Z}^2$. Par lemme 1.5.2, on sait que M_f est équivalente à une matrice réduite de déterminant $-\frac{D}{4}$ ou $-D$.

Par lemme 1.5.2, on voit facilement qu'il n'existe qu'un nombre fini de matrices réduites de déterminant $-\frac{D}{4}$ ou $-D$. Par définition, on voit aussi que deux formes f, g dans $\mathcal{Q}(D)$ sont dans le même orbite si M_f et M_g sont équivalentes. Donc $\mathcal{C}(D)$ est fini.

$\square$

Dans la suite, on note $h(D) = \mathrm{card}\ \mathcal{C}(D)$.

Le but du reste de cette partie est de construire une certaine structure de groupe sur $\mathcal{C}(D)$. Pour cela, on introduira d'abord le groupe de classes d'idéaux $Pic(D)$, et on trouvera une bijection entre $\mathcal{C}(D)$ et $Pic(D)$, ainsi la structure de groupe sur $Pic(D)$ induira une structure de groupe sur $\mathcal{C}(D)$.

Notons τ l'élément de $\{0, 1\} \subseteq \mathbb{Z}$ tel que $\tau \equiv D \pmod 2$, et $\delta := \frac{-\tau + \sqrt{D}}{2}$, alors on a $\delta^2 + \tau\delta + \frac{\tau - D}{4} = 0$. Introduisons l'anneau $O_D := \mathbb{Z}[\delta]$ et le corps $K_D = \mathbb{Q}(\delta)$.

Définition 2.1.1. *Un **idéal fractionaire** de O_D est un sous-O_D-module non nul de type fini de K_D. Pour I, J des idéaux fractionaires de O_D, on définit le **produit** de I, J comme*

$$IJ := \{\sum_{k=1}^{r} i_k j_k : r \in \mathbb{N}, i_k \in I, j_k \in J\}.$$

*Un idéal fractionaire I est dit **inversible**, s'il existe un idéal fractionaire J, tel que $IJ = O_D$.*

Il est immédiat que tout idéal fractionaire est libre de rang 2 en tant que $\mathbb{Z}$-module, et que le produit de deux idéaux fractionaires est encore un idéal fractionaire. On vérifie facilement que $IJ = JI$, $O_D I = I$ et $I(JK) = (IJ)K$ pour I, J, K des idéaux fractionaires, donc les idéaux fractionaires inversibles forment un groupe commutatif, que l'on note $\mathcal{J}(D)$, et O_D en est l'élément neutre. Notons $\mathcal{P}(D) := \{\lambda O_D : \lambda \in K_D^*\}$, alors $\mathcal{P}(D)$ est un sous-groupe distingué de $\mathcal{J}(D)$. On pose $Pic(D) := \mathcal{J}(D)/\mathcal{P}(D)$.

Pour tout idéal fractionaire de O_D, on pose $I^* := \{\alpha \in K_D : \alpha I \subseteq O_D\}$. Dans la suite, on écrit $\lfloor x, y \rfloor$ pour $\mathbb{Z}x \oplus \mathbb{Z}y$ si x, y sont des éléments de K_D linéairement indépendents sur $\mathbb{Q}$.

Lemme 2.1.1. *Soit I un idéal fractionaire de O_D.*

- *Il existe λ dans K_D^* et a, b dans $\mathbb{Z}$, tel que $a > 0$, $4a$ divise $b^2 - D$ et qu'on a $I = \lambda\lfloor a, \frac{-b+\sqrt{D}}{2}\rfloor$.*
- *Avec les notations ci-dessus, on a $I^* = \frac{1}{\lambda a}\lfloor a, \frac{b+\sqrt{D}}{2}\rfloor$, donc I^* est encore un idéal fractionaire.*
- *Avec les notations ci-dessus, il y a équivalence entre*
  1. *I est inversible*
  2. *$a, b, \frac{b^2-D}{4a}$ sont premiers entre eux*

Démonstration Comme $K_D = \mathrm{Frac}(O_D)$ et I est engendré (en tant que O_D-module) par un nombre fini d'éléments de K_D, on sait qu'il existe λ_0 dans K_D^*, tel que $\lambda_0 I$ est inclus dans O_D. On peut donc supposer que I est un idéal de O_D.

On définit des morphismes de $\mathbb{Z}$-modules $p_i : O_D \to \mathbb{Z}$ $(i = 1, 2)$ par $p_1(x + y\delta) = x$ et $p_2(x + y\delta) = y$ pour tout x, y dans $\mathbb{Z}$. Posons $H_i = p_i(I)$, alors les H_i sont des idéaux de $\mathbb{Z}$. Notons que $H_1 \subseteq H_2$. En fait, soit $x + y\delta$ dans I, alors $z := (x + y\delta)(\delta + \tau)$ est dans I, et on a $p_2(z) = x$. Écrivons $H_2 = \mathbb{Z}g$ avec g un entier non nul, alors on a $g^{-1}I \subseteq O_D$ et $p_2(g^{-1}I) = \mathbb{Z}$. Donc on peut supposer que $p_2(I) = \mathbb{Z}$, quitte à remplacer I par gI.

Il existe donc un entier b tel que $\frac{-b+\sqrt{D}}{2}$ est dans I. Écrivons $I \bigcap \mathbb{Z} = \mathbb{Z}a$ avec a un entier positif, alors on a $I = \lfloor a, \frac{-b+\sqrt{D}}{2}\rfloor$. Comme I est un idéal, on a $\delta\frac{-b+\sqrt{D}}{2} = ca + d\frac{-b+\sqrt{D}}{2}$ avec c, d des entiers, d'où on déduit que $\delta - d = \frac{b+\sqrt{D}}{2}$ et $ca = \frac{D-b^2}{4}$. Donc a divise $\frac{b^2-D}{4}$.

Soient u, v, w des entiers tels que $\mathrm{pgcd}(u, v, w) = 1$ et $w \neq 0$, alors on a

$$\begin{aligned}
& \frac{u+v\delta}{w} \in I^* \\
\Leftrightarrow \quad & \begin{cases} \frac{u+v\delta}{w} \cdot a \in O_D \\ \frac{u+v\delta}{w} \cdot \frac{-b+\sqrt{D}}{2} \in O_D \end{cases} \\
\Leftrightarrow \quad & \begin{cases} w|ua, \ w|va \\ w|u - \frac{b+\tau}{2}v, \ w|\frac{-b+\tau}{2}u + \frac{D-\tau}{4}v \end{cases} \\
\Leftrightarrow \quad & \begin{cases} w|\mathrm{pgcd}(u,v)a \\ w|u - \frac{b+\tau}{2}v, \ w|\frac{b^2-D}{4}v \end{cases} \\
\Leftrightarrow \quad & w|a, \ w|u - \frac{b+\tau}{2}v \\
\Leftrightarrow \quad & \frac{u+v\delta}{w} \in \frac{1}{a}\lfloor a, \frac{b+\sqrt{D}}{2} \rfloor.
\end{aligned}$$

Donc on a $I^* = \frac{1}{a}\lfloor a, \frac{b+\sqrt{D}}{2} \rfloor$, et on voit que c'est encore un idéal fractionaire.

Comme I est inversible si et seulement si $II^* = O_D$, on a

$$\begin{aligned}
& \text{I est inversible} \\
\Leftrightarrow \quad & \frac{1}{a}(\mathbb{Z}a^2 + \mathbb{Z}a\frac{-b+\sqrt{D}}{2} + \mathbb{Z}a\frac{b+\sqrt{D}}{2} + \mathbb{Z}\frac{b^2-D}{4}) = O_D \\
\Leftrightarrow \quad & \mathbb{Z}a + \mathbb{Z}b + \mathbb{Z}\frac{b^2-D}{4a} + \mathbb{Z}\frac{-b+\sqrt{D}}{2} = O_D \\
\Leftrightarrow \quad & \mathrm{pgcd}(a, b, \frac{b^2-D}{4a}) = 1.
\end{aligned}$$

□

Le lemme suivant donnera une bijection entre $\mathcal{C}(D)$ et $Pic(D)$.

Lemme 2.1.2. *Soient f, g dans $\mathcal{Q}(D)$. Écrivons $f = aX^2 + bXY + cY^2$ et $g = a'X^2 + b'XY + c'Y^2$ avec a, b, c, a', b', c' des entiers. Alors il y a équivalence entre*

1. *il existe P dans $\mathrm{SL}_2(\mathbb{Z})$, tel que $f = P \cdot g$,*
2. *il existe λ dans K_D^*, tel que $\lfloor a, \frac{-b+\sqrt{D}}{2} \rfloor = \lambda \lfloor a', \frac{-b'+\sqrt{D}}{2} \rfloor$.*

Démonstration On note γ (resp. γ') la racine du polynôme $f(X,1)$ (resp. $g(X,1)$) telle que la partie imaginaire de γ (resp. de γ') est positive.

D'une part, soit P dans $\mathrm{SL}_2(\mathbb{Z})$, tel que $f = P \cdot g$. Écrivons $P = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$, alors on a $f(\gamma,1) = g(p\gamma + q, r\gamma + s)$, donc on a $\gamma' = \frac{p\gamma+q}{r\gamma+s}$ car la partie imaginaire de ce dernier est positive. En posant $\lambda := \frac{a}{a'}(r\gamma + s)$, on a

$$\lambda \lfloor a', \frac{-b' + \sqrt{D}}{2} \rfloor = a \lfloor r\gamma + s, p\gamma + q \rfloor = a \lfloor 1, \gamma \rfloor = \lfloor a, \frac{-b + \sqrt{D}}{2} \rfloor.$$

D'autre part, soit λ dans K_D^*, tel que $\lfloor a, \frac{-b+\sqrt{D}}{2} \rfloor = \lambda \lfloor a', \frac{-b'+\sqrt{D}}{2} \rfloor$. Alors il existe une matrice $P \in \mathrm{GL}_2(\mathbb{Z})$, telle que $\begin{pmatrix} \lambda \frac{-b'+\sqrt{D}}{2} \\ \lambda a' \end{pmatrix} = P \begin{pmatrix} \frac{-b+\sqrt{D}}{2} \\ a \end{pmatrix}$. Par orientation, on voit que P est dans $\mathrm{SL}_2(\mathbb{Z})$. Écrivons $P = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$, on a alors $\gamma' = \frac{p\gamma+q}{r\gamma+s}$, d'où on conclut que $f = P \cdot g$, car ce dernier est dans $\mathcal{Q}(D)$ et sa racine de partie imaginaire positive est juste γ.

$\square$

Grâce aux deux lemmes précédents, il existe une unique bijection $\Gamma : \mathcal{C}(D) \to Pic(D)$ qui envoie la classe d'une forme $f = aX^2 + bXY + cY^2$ sur la classe de l'idéal fractionaire $\lfloor a, \frac{-b+\sqrt{D}}{2} \rfloor$. On a donc une structure de groupe sur $\mathcal{C}(D)$ induite par la structure de groupe sur $Pic(D)$, i.e., on pose $F \cdot G = \Gamma^{-1}(\Gamma(F)\Gamma(G))$ pour tout F, G dans $\mathcal{C}(D)$, et l'élément neutre est donné par $\Gamma^{-1}(e)$, où e est l'élément neutre de $Pic(D)$. Dans la suite, on va toujours munir $\mathcal{C}(D)$ de cette structure de groupe.

Définition 2.1.2. *Quand $D \equiv 0 \pmod 4$ (resp. $D \equiv 1 \pmod 4$), on appelle la* ***forme principale*** *la forme $X^2 + \frac{-D}{4} Y^2$ (resp. $X^2 + XY + \frac{1-D}{4} Y^2$).*

Par définition, la classe de la forme principale est juste l'élément neutre du groupe $\mathcal{C}(D)$.

Maintenant on va donner une propriété importante du groupe $\mathcal{C}(D)$.

Proposition 2.1.2. *Soient f_1, f_2, f_3 dans $\mathcal{Q}(D)$, telles que $[f_1][f_2] = [f_3]$, où $[f_i] \in \mathcal{C}(D)$ est la classe de f_i. Alors il existe deux formes bilinéaires (pas nécéssairment symétriques) ρ_1, ρ_2 sur $\mathbb{Z}^2$, telles que pour tout u, v dans $\mathbb{Z}^2$, on a $f_1(u)f_2(v) = f_3(\rho_1(u,v), \rho_2(u,v))$.*

Avant démontrer cette proposition, on introduit la "norme absolue".

Définition 2.1.3. *Soient I un idéal fractionaire de O_D et (α, β) une $\mathbb{Z}$-base de I, alors (α, β) est aussi une $\mathbb{Q}$-base de K_D. Donc il existe une unique matrice P dans $\mathrm{GL}_2(\mathbb{Q})$, telle que $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = P \begin{pmatrix} 1 \\ \delta \end{pmatrix}$. On définit alors la **norme absolue** de I, notée $\mathrm{N}(I)$, comme la valeur absolue du déterminant de P.*

Il est facile de voir que la norme absolue est bien définie pour tout idéal fractionaire. Notons σ le seule automorphime non trivial de K_D, i.e., la conjugué complexe.

Lemme 2.1.3. *Soient I, J des idéaux fractionaires inversibles de O_D et λ dans K_D^*. On a les égalités suivantes*

1. $\mathrm{N}(\lambda I) = \lambda\sigma(\lambda)\mathrm{N}(I)$,
2. $I\sigma(I) = \mathrm{N}(I)O_D$,
3. $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

Démonstration Soient (α, β) une $\mathbb{Z}$-base de I et P dans $\mathrm{GL}_2(\mathbb{Q})$ telle que $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = P \begin{pmatrix} 1 \\ \delta \end{pmatrix}$. Alors $(\lambda\alpha, \lambda\beta)$ est une $\mathbb{Z}$-base de λI, et on a $\begin{pmatrix} \lambda\alpha \\ \lambda\beta \end{pmatrix} = \lambda P \begin{pmatrix} 1 \\ \delta \end{pmatrix} = PQ \begin{pmatrix} 1 \\ \delta \end{pmatrix}$, où Q est la matrice de λ dans la $\mathbb{Q}$-base $(1, \delta)$ de K_D. On a donc $\mathrm{N}(\lambda I) = |\det(PQ)| = |\det(P)||\det Q|$. Notons que $\det(Q)$ est exactement $\mathrm{N}_Q^{K_D}(\lambda)$, qui est positif et peut être écrit comme $\lambda\sigma(\lambda)$, d'où 1.

Par lemme 2.1.1, on peut écrire $I = \mu I_0$ avec μ dans K_D^* et $I_0 = \lfloor a, \frac{-b+\sqrt{D}}{2} \rfloor$, où a, b sont des entiers tels que a est positif, a divise $\frac{b^2-D}{4}$ et $\mathrm{pgcd}(a, b, \frac{b^2-D}{4a}) = 1$. On sait que $I_0^* = \frac{1}{a}\sigma(I_0)$, et on vérifie facilement que $\mathrm{N}(I_0) = a$. Donc $I_0\sigma(I_0) = \mathrm{N}(I_0)I_0I_0^* = \mathrm{N}(I_0)O_D$, et 2 découle de 1.

Enfin, on a $\mathrm{N}(IJ)O_D = (IJ)\sigma(IJ) = (I\sigma(I))(J\sigma(J)) = \mathrm{N}(I)\mathrm{N}(J)O_D$, d'où 3.

□

On munit K_D avec l'orientation telle que $(1, \delta)$ est une base positive.

Proposition 2.1.3. *Soient I un idéal fractionaire de O_D et (α, β) une base positive de I. On pose $f(X, Y) := \frac{1}{\mathrm{N}(I)}\mathrm{N}_{\mathbb{Q}}^{K_D}(X\alpha - Y\beta)$, alors Γ^{-1} envoie la classe de I sur la classe de f.*

Démonstration Par le lemme précédent, on peut remplacer I par un idéal fractionaire quelconque dans la classe de I, et on peut remplacer (α, β) par une base positive quelconque de I.

Soit g dans $\mathcal{Q}(D)$ tel que Γ envoie la classe de g sur la classe de I. Écrivons $g = aX^2 + bXY + cY^2$ avec a, b, c des entiers. Par lemme 2.1.1, on peut supposer que $I = \lfloor a, \frac{-b+\sqrt{D}}{2} \rfloor$, et que $(\alpha, \beta) = (a, \frac{-b+\sqrt{D}}{2})$, car cette dernière est aussi une base positive de I.

On voit alors que $f(X,Y) = \frac{1}{a}\mathrm{N}_{\mathbb{Q}}^{K_D}(aX + \frac{b-\sqrt{D}}{2}Y) = aX^2 + bXY + cY^2 = g(X,Y)$ (notons que $\mathrm{N}(I) = a$).

$\square$

Maintenant proposition 2.1.2 est claire. Soit I_i un idéal fractionaire dans la classe $\Gamma([f_i])$ $(i = 1, 2)$, alors $I_3 := I_1 I_2$ est dans la classe $\Gamma([f_3])$. Soit (α_i, β_i) une base positive de I_i $(i = 1, 2, 3)$. Pour tout u_1, u_2 dans $\mathbb{Z}^2$, posons $\gamma_i = (\alpha_i, -\beta_i)u_i$ (i=1,2), $\gamma_3 = \gamma_1\gamma_2$, et écrivons $\gamma_3 = (\alpha_3, -\beta_3)\begin{pmatrix} p \\ q \end{pmatrix}$. On pose alors $\rho_1(u_1, u_2) = p$, $\rho_2(u_1, u_2) = q$. Il est immédiat qu'elles sont des formes bilinéaires sur $\mathbb{Z}^2$, et pour tout u_1, u_2 dans $\mathbb{Z}^2$, on a

$$f_1(u_1)f_2(u_2) = \frac{\mathrm{N}_{\mathbb{Q}}^{K_D}(\gamma_1)}{\mathrm{N}(I_1)} \cdot \frac{\mathrm{N}_{\mathbb{Q}}^{K_D}(\gamma_2)}{\mathrm{N}(I_2)} = \frac{\mathrm{N}_{\mathbb{Q}}^{K_D}(\gamma_3)}{\mathrm{N}(I_3)} = f_3(\rho_1(u_1, u_2), \rho_2(u_1, u_2)).$$

2.2 Théorie des Genres

On pose les mêmes hypothèses sur D que dans le paragraphe précédent.

Définition 2.2.1. *Soient $f(X,Y)$ un élément de $\mathcal{Q}(D)$ et m un entier. On dit que m est **repésenté** par f, s'il existe des entiers x, y, tels que $m = f(x,y)$. On dit que m est **représenté proprement** par f, s'il existe des entiers x, y, tels que $m = f(x,y)$ et $\mathrm{pgcd}(x,y) = 1$. Dans ces cas, on dit aussi que f **représente** (resp. **représente proprement**) m.*

*Un élément de $\mathbb{Z}/D\mathbb{Z}$ est dit **représenté** par f, s'il admet un relevé dans $\mathbb{Z}$, qui est représenté par f.*

Remarque Si m est un élément de $\mathbb{Z}/D\mathbb{Z}$ et f un élément de $\mathcal{Q}(D)$, alors il y a équivalence entre

1. m est représenté par f,

2. il existe deux éléments u, v de $\mathbb{Z}/D\mathbb{Z}$, tels que $m = f(u, v)$.

Par définition, on voit facilement que deux formes quadratiques équivalentes repésentent (resp. représentent proprement) les mêmes entiers, et *a fortiori* représentent les mêmes éléments dans $\mathbb{Z}/D\mathbb{Z}$.

Lemme 2.2.1. *Soient $f = aX^2 + bXY + cY^2$ un élément de $\mathcal{Q}(D)$ et m un entier. Si m est représenté proprement par f, alors il existe $u, v \in \mathbb{Z}$, tels que $mX^2 + uXY + vY^2$ et f sont équivalentes.*

Démonstration Soit p, q des entiers tels que $\mathrm{pgcd}(p, q) = 1$ et $m = f(p, q)$. Par égalité de Bézout, il existe deux entiers r, s, tels que $ps - qr = 1$. Alors la forme $\begin{pmatrix} p & r \\ q & s \end{pmatrix} \cdot f$ convient.

□

Lemme 2.2.2. *Soient C dans $\mathcal{C}(D)$ et M un entier non nul. Alors il existe $f = aX^2 + bXY + cY^2$ dans C, telle que* $\mathrm{pgcd}(a, M) = 1$.

Démonstration Soit $f = aX^2 + bXY + cY^2$ une forme dans C, avec a, b, c des entiers. Par le lemme précédent, il suffit de montrer que f représente un nombre premier avec M. Par le lemme chinois, on peut supposer que M soit premier. Mais alors au moins un des trois nombres $f(1, 0)$, $f(0, 1)$, $f(1, 1)$ est premier avec M, car on a $\mathrm{pgcd}(a, b, c) = 1$.

□

Proposition 2.2.1. *On rappelle la définition de forme principale.*

1. *Les éléments de $(\mathbb{Z}/D\mathbb{Z})^*$ représentés par la forme principale forment un sous-groupe de $(\mathbb{Z}/D\mathbb{Z})^*$, que l'on note H désormais.*
2. *Pour chaque f dans $\mathcal{Q}(D)$, les éléments de $(\mathbb{Z}/D\mathbb{Z})^*$ représentés par f forment une classe modulo H.*

Démonstration Pour tout f dans $\mathcal{Q}(D)$, notons $[f] \in \mathcal{C}(D)$ la classe de f.

Notons f_0 la forme principale et H l'ensemble des éléments représentés par f_0. Comme $[f_0]$ est l'élément neutre du groupe $\mathcal{C}(D)$, on a $[f_0][f_0] = [f_0]$. Par proposition 2.1.2, on voit que H est une partie multiplicative de

$(\mathbb{Z}/D\mathbb{Z})^*$. Comme $(\mathbb{Z}/D\mathbb{Z})^*$ est un groupe fini, on sait que H en est un sous-groupe.

De même, pour tout f dans $\mathcal{Q}(D)$, notons G l'ensemble des éléments de $(\mathbb{Z}/D\mathbb{Z})^*$ représentés par f, alors on déduit de l'égalité $[f_0][f] = [f]$ que G contient au moins une classe modulo H (car G n'est pas vide). Or, on a encore $[f][f]^{-1} = [f_0]$, d'où on déduit que $\mathrm{card}(G) \leq \mathrm{card}(H)$. Donc G est exactement une classe modulo H.

$\square$

Grâce à la proposition précédente, la relation "représenter les même valeurs dans $(\mathbb{Z}/D\mathbb{Z})^*$" est bien une relation d'équivalence sur $\mathcal{Q}(D)$. On définit donc un "genre" comme une classe d'équivalence sous cette relation. On dit aussi un "genre de discriminant D" quand on veut expliciter l'entier D.

Comme les formes équivalentes représentent les mêmes éléments dans $(\mathbb{Z}/D\mathbb{Z})^*$, ils sont dans le même genre. Donc chaque genre est formé par quelque classes de formes, et on a une application $\Psi : \mathcal{C}(D) \to (\mathbb{Z}/D\mathbb{Z})^*/H$, qui à chaque classe de formes associe la classe modulo H qu'elle représente.

Proposition 2.2.2. *Ψ est un morphisme de groupes.*

Démonstration C'est une conséquence de proposition 2.1.2.

$\square$

Corollaire 2.2.1. *Tous les genres sont formés du même nombre de classes de formes.*

Démonstration Les genres sont juste les fibres de Ψ.

$\square$

Notre but est de calculer exactement le nombre des genres, i.e., le cardinal de l'image de Ψ. Pour décrire $\mathrm{Im}\Psi$, on introduit d'abord le symbole de Jacobi.

2.3 Symbole de Jacobi

Soit p un nombre premier impair.

Définition 2.3.1. *Soit k un entier. Notons $\overline{k}$ la réduction de k modulo p. On définit le **symbole de Legendre**, noté $\left(\frac{k}{p}\right)$, par la formule suivante*

$$\left(\frac{k}{p}\right) = \begin{cases} 0, & si\ \overline{k} = \overline{0} \in \mathbb{F}_p \\ 1, & si\ \overline{k}\ est\ un\ carré\ non\ nul\ dans\ \mathbb{F}_p \\ -1, & si\ \overline{k}\ n'est\ pas\ carré\ dans\ \mathbb{F}_p \end{cases}.$$

Proposition 2.3.1. *Soit p un nombre premier impair. Alors on a*

1. $\left(\frac{k_1}{p}\right) = \left(\frac{k_2}{p}\right)$ *si* $k_1 \equiv k_2 \pmod{p}$,
2. $\left(\frac{k_1 k_2}{p}\right) = \left(\frac{k_1}{p}\right)\left(\frac{k_2}{p}\right)$ *pour tout* k_1, k_2 *dans* $\mathbb{Z}$,
3. $\left(\frac{k^2}{p}\right) = 1$ *pour tout entier k premier avec p,*
4. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,
5. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Démonstration Rappelons que $\mathbb{F}_p^*$ est un groupe cyclique, d'où 1,2,3,4.

Montrons 5. Soit ζ une racine 8-ième primitive de l'unité dans une extension de $\mathbb{F}_p$, alors on a $\zeta^4 = -1$, i.e., $\zeta^2 + \zeta^{-2} = 0$. Posons $\xi := \zeta + \zeta^{-1}$, alors $\xi^2 = 2 \in \mathbb{F}_p$. Donc $\left(\frac{2}{p}\right) = 1$ si et seulement si ξ est dans $\mathbb{F}_p$. Or, cela est encore équivalent à $\xi^p = \xi$, i.e., $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$. Comme on a $\zeta^4 = -1$, on voit que

$$\zeta^p + \zeta^{-p} = \begin{cases} \zeta + \zeta^{-1}, & si\ p \equiv 1, 7 \pmod{8} \\ -\zeta - \zeta^{-1}, & si\ p \equiv 3, 5 \pmod{8} \end{cases},$$

d'où le résultat.

□

Pour le symbole de Legendre, on a la "loi de réciprocité quadratique de Gauss", qui est donné par la proposition suivante.

Proposition 2.3.2. *Soient p, q deux nombres premiers impairs différents. Alors on a* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Démonstration Soit ζ une racine q-ième de l'unité dans une extension de $\mathbb{F}_p$. On voit alors que $\left(\frac{x}{q}\right)$ et ζ^x sont bien définis pour tout x dans $\mathbb{F}_q$ (en prenant un relevé de x dans $\mathbb{Z}$). On pose $G := \sum_{x\in\mathbb{F}_q} \left(\frac{x}{q}\right)\zeta^x$.

Premièrement, on montre que $G^2 = \left(\frac{-1}{q}\right) q$, où la notation q désigne à la fois l'entier q et l'image de q dans $\mathbb{F}_p$. En fait, on a

$$G^2 = \sum_{x,y\in\mathbb{F}_q} \left(\frac{xy}{q}\right)\zeta^{x+y} = \sum_{x\in\mathbb{F}_q} \zeta^x \sum_{y\in\mathbb{F}_q^*} \left(\frac{(x-y)y}{q}\right) = \left(\frac{-1}{q}\right) \sum_{x\in\mathbb{F}_q} \zeta^x G_x,$$

où $G_x = \sum_{y\in\mathbb{F}_q^*} \left(\frac{1-xy^{-1}}{q}\right)$. Or, on a $G_0 = q-1$ et $G_x = \sum_{x\in\mathbb{F}_p\setminus\{1\}} \left(\frac{x}{q}\right) = -1$ pour tout x dans $\mathbb{F}_q^*$, car les nombres de carrés et de non carrés dans $\mathbb{F}_q$ sont égaux. On en déduit que $\left(\frac{-1}{q}\right) G^2 = q - 1 - \sum_{x\in\mathbb{F}_q^*} \zeta^x = q$. En particulier, G n'est pas nul car p, q sont différents.

Deuxièmement, on va montrer que $G^{p-1} = \left(\frac{p}{q}\right)$. En fait, comme G est dans un corps de caratéristique p, on a

$$G^p = \sum_{x\in\mathbb{F}_q} \left(\frac{x}{q}\right)\zeta^{px} = \sum_{x\in\mathbb{F}_q} \left(\frac{p^{-1}x}{q}\right)\zeta^x = \left(\frac{p^{-1}}{q}\right) \sum_{x\in\mathbb{F}_q} \left(\frac{x}{q}\right)\zeta^x = \left(\frac{p}{q}\right) G,$$

où la notation p désigne à la fois l'entier p et l'image de p dans $\mathbb{F}_q$. Comme G n'est pas nul, on a la formule voulue.

Le résultat découle alors des deux formules ci-dessus.

$\square$

Définition 2.3.2. *Soient m un entier positif impair et k un entier. Si la décomposition de m en nombres premiers est $m = p_1 \cdots p_r$ avec les p_i premiers, alors le* ***symbole de Jacobi****, noté $\left(\frac{k}{m}\right)$, est défini comme $\prod_{i=1}^{r} \left(\frac{k}{p_i}\right)$, où les $\left(\frac{k}{p_i}\right)$ sont les symbols de Legendre.*

Remarque Quand m est premier, le symbole de Jacobi coïncide avec le symbole de Legendre. Donc on ne distingue pas les deux désormais.

Proposition 2.3.3. *Soient m, m' des entiers positifs impairs. Alors on a*

1. $\left(\frac{k_1}{m}\right) = \left(\frac{k_2}{m}\right)$ *si* $k_1 \equiv k_2 \pmod{m}$,
2. $\left(\frac{k_1 k_2}{m}\right) = \left(\frac{k_1}{m}\right)\left(\frac{k_2}{m}\right)$ *pour tout* k_1, k_2 *dans* $\mathbb{Z}$,
3. $\left(\frac{k}{mm'}\right) = \left(\frac{k}{m}\right)\left(\frac{k}{m'}\right)$ *pour tout entier* k,
4. $\left(\frac{k^2}{m}\right) = 1$ *pour tout entier* k *premier avec* m,
5. $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$,
6. $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$,
7. $\left(\frac{m}{m'}\right)\left(\frac{m'}{m}\right) = (-1)^{\frac{(m-1)(m'-1)}{4}}$ *si* m *et* m' *sont premiers entre eux.*

Démonstration 1,2,3,4 sont clairs par définition.

Écrivons $m = \prod_{i=1}^{r} p_i$ et $m' = \prod_{j=1}^{s} q_j$, avec p_i, q_j les nombres premiers impairs. Comme on a

$$\begin{aligned} \frac{p-1}{2} + \frac{q-1}{2} &\equiv \frac{pq-1}{2} \pmod{2} \\ \frac{p^2-1}{8} + \frac{q^2-1}{8} &\equiv \frac{(pq)^2-1}{8} \pmod{2} \end{aligned}$$

pour p, q des nombres impairs, on peut montrer les formules suivantes par récurrence

$$\begin{aligned} \sum_{i=1}^{r} \frac{p_i-1}{2} &\equiv \frac{m-1}{2} \pmod{2} \\ \sum_{i=1}^{r} \frac{p_i^2-1}{8} &\equiv \frac{m^2-1}{8} \pmod{2} \\ \sum_{i=1}^{r}\sum_{j=1}^{s} \frac{(p_i-1)(q_j-1)}{4} &\equiv \frac{(m-1)(m'-1)}{4} \pmod{2}. \end{aligned}$$

Avec les propositions 2.3.1 et 2.3.2, on en déduit 5,6,7.

□

Proposition 2.3.4. *Il existe un unique caractère $\chi : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$, qui vérifie la condition suivante : pour chaque entier positif m premier avec $2D$, on a $\chi(\overline{m}) = \left(\frac{D}{m}\right)$, où $\overline{m}$ est la réduction de m modulo D.*

Démonstration Il suffit de montrer que, pour deux entiers positifs impairs M, N tels que $M \equiv N \pmod D$, on a $\left(\frac{D}{M}\right) = \left(\frac{D}{N}\right)$.

Écrivons $D = -2^k d$ avec k un entier non négatif et d un entier positif impair. Par la proposition précédente, on a

$$\left(\tfrac{D}{M}\right) = (-1)^{\frac{M-1}{2}}(-1)^{\frac{M^2-1}{8}k}\left(\tfrac{d}{M}\right) = (-1)^{\frac{(M-1)(d+1)}{4}}(-1)^{\frac{M^2-1}{8}k}\left(\tfrac{M}{d}\right).$$

De même, on a une formule similaire pour $\left(\frac{D}{N}\right)$. Comme $M \equiv N \pmod D$, on a $\left(\frac{M}{d}\right) = \left(\frac{N}{d}\right)$. De plus, comme $D \equiv 0, 1 \pmod 4$, on vérifie facilement que 8 divise $(M-N)(d+1)$ et que 16 divise $(M^2 - N^2)k$, d'où le résultat.

$\square$

Désormais, on note toujours χ le caractère dans la proposition précédente.

2.4 Théorie des Genres - Suite

Rappelons que $\Psi : \mathcal{C}(D) \to (\mathbb{Z}/D\mathbb{Z})^*/H$ est un morphisme de groupe, qui à chaque classe de formes associe la classe modulo H qu'elle représente, et que le nombre de genres et card(ImΨ) sont égaux. Maintenant on peut décrire ImΨ.

Proposition 2.4.1. *Pour un entier k, on note $\overline{k} \in \mathbb{Z}/D\mathbb{Z}$ la réduction de k modulo D. Soit m un entier tel que $\overline{m}$ est dans $(\mathbb{Z}/D\mathbb{Z})^*$, alors les deux conditions suivantes sont équivalentes :*

1. *il existe $f \in \mathcal{Q}(D)$, telle que $\overline{m}$ est représenté par f,*
2. *$\overline{m}$ est dans* $\ker(\chi)$.

Démonstration "1 implique 2" : Par hypothèse, il existe un entier M tel que $M \equiv m \pmod D$ et $M = f(x, y)$ avec $f = aX^2 + bXY + cY^2$ un élément de $\mathcal{Q}(D)$ et x, y des entiers. On peut supposer que M soit impair (si M est pair, alors D est impair, et on utilise le lemme chinois) et que x, y soient premiers entre eux (quitte à diviser x, y par pgcd(x, y)).

Par lemme 2.2.1, on peut encore supposer que $a = M$. Alors on a $D = b^2 - 4Mc$, donc $\chi(\overline{m}) = \left(\frac{D}{M}\right) = \left(\frac{b^2}{M}\right) = 1$, i.e., $\overline{m}$ est dans $\ker(\chi)$.

"2. implique 1." : Par théorème de Dirichlet, il existe un nombre premier impair P, tel que $\overline{P} = \overline{m}$. Par hypothèse, on a $\left(\frac{D}{P}\right) = 1$, donc il existe des entiers b, c, tels que $b^2 = D + Pc$. Quitte à remplacer b avec $b + P$, on peut supposer que $b \equiv D \pmod 2$. Alors 4 divise c, et on a $\overline{m} = \overline{P} = f(\overline{1}, \overline{0})$ avec $f = PX^2 + bXY + \frac{c}{4}Y^2$ dans $\mathcal{Q}(D)$.

$\square$

Par la proposition précédente, on sait que H est un sous-groupe de $\ker(\chi)$, et $\mathrm{Im}\Psi = \ker(\chi)/H$.

Pour un entier k non nul, on pose $r(k)$ le nombre de nombres premiers impairs divisant k. Si 16 ne divise pas D, on note

$$\mu(D) = \begin{cases} r(D), & \textit{si } D \equiv 1 \pmod 4 \textit{ ou } D \equiv 4 \pmod{16} \\ r(D) + 1, & \textit{si } D \equiv 8, 12 \pmod{16} \end{cases}$$

Proposition 2.4.2. *Si* 16 *ne divise pas D, alors le nombre des genres de discriminant D est* $2^{\mu(D)-1}$.

Démonstration Par la proposition 2.2.2 et son corollaire, on sait que le nombre des genres est juste $\mathrm{card}(\mathrm{Im}\Psi)$, donc il suffit de compter $\ker(\chi)/H$.

Pour simplifier les notations, on écrit r, μ pour $r(D), \mu(D)$ dans la suite. Soit $D = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition en nombres premiers de D, avec α un entier non négatif, p_i des nombres premiers impairs différents et α_i des entiers positifs. Notons $p_0 := 2$ et $\alpha_0 := \alpha$.

On note $G := (\mathbb{Z}/D\mathbb{Z})^*$ et $G_i := (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$ pour $0 \leq i \leq r$. Par le lemme chinois, le groupe G est isomorphe à $\oplus_{i=0}^r G_i$. Dans la suite, on identifie chaque G_i avec son image dans G.

Posons $H_i := H \bigcap G_i$ pour $0 \leq i \leq r$, alors H_i est un sous-groupe de G_i, et on a $\oplus_{i=0}^r H_i \subseteq H$. D'autre part, soit m dans H, alors par le lemme chinois on voit que la projection de m sur G_i est encore dans H, donc on a $\oplus_{i=0}^r H_i \supseteq H$, alors $H = \oplus_{i=0}^r H_i$.

Pour un indice $i \neq 0$, on voit par un argument modulo $p_i^{\alpha_i}$ que H_i coïncide avec l'ensemble des carrés de G_i. Notons $[G_i : H_i] := \frac{\mathrm{card}(G_i)}{\mathrm{card}(H_i)}$ l'indice de H_i dans G_i, alors on a $[G_i : H_i] = 2$ car G_i est cyclique.

Pour $i = 0$, on calcule $[G_0 : H_0]$ dans les trois cas suivants.

Si $\alpha = 0$, alors on a $\mathrm{card}(G_0) = 1$, et donc $[G_0 : H_0]$ est bien sûr 1.

Si $\alpha = 2$, alors on a $G_0 = \{\overline{1}, \overline{1 + \frac{D}{2}}\} \subseteq G$, et on vérifie facilement que $\overline{1 + \frac{D}{2}}$ est dans H si et seulement si $D \equiv 4 \pmod{16}$. Donc $[G_0 : H_0]$ vaut 1 si $D \equiv 4 \pmod{16}$, et vaut 2 sinon.

Si $\alpha = 3$, alors on a $G_0 = \{\overline{1}, \overline{1 + \frac{D}{4}}, \overline{1 + \frac{D}{2}}, \overline{1 + \frac{3D}{4}}\} \subseteq G$, et on vérifie facilement que $\overline{1 + \frac{D}{4}}$ est dans H mais $\overline{1 + \frac{D}{2}}$ ne l'est pas. Donc $[G_0 : H_0]$ vaut 2.

Comme on a $[G : H] = \prod_{i=0}^{r} [G_i : H_i]$, on voit que $[G : H]$ vaut exactement 2^μ. On a aussi $[G : \ker(\chi)] = 2$ (car χ est surjective et $\mathrm{card}(\mathrm{Im}\chi) = 2$), donc le nombre des genres est

$$\mathrm{card}(\mathrm{Im}\Psi) = \mathrm{card}(\ker(\chi)/H) = [\ker(\chi) : H] = \frac{[G : H]}{[G : \ker(\chi)]} = 2^{\mu-1}.$$

□

Corollaire 2.4.1. *Si* 16 *ne divise pas* D*, alors chaque genre est formé de* $\frac{h(D)}{2^{\mu(D)-1}}$ *classes de formes.*

Démonstration Ce résultat découle du corollaire 2.2.1.

□

2.5 Énoncés des Théorèmes

On fixe encore un entier $n > 0$. On rappelle la définition de $\mathfrak{e}_n$ dans 1.2.

On note $\mathfrak{F}_n$ l'ensemble des couples $(\Lambda, \mathfrak{b})$, où
- Λ est un $\mathbb{Z}$-module libre orienté de rang 2,
- $\mathfrak{b}$ est une forme bilinéaire sur Λ, définie positive, de déterminant n et primitive.

Deux couples $(\Lambda, \mathfrak{b}), (\Lambda', \mathfrak{b}') \in \mathfrak{F}_n$ sont dites "isomorphes", s'il existe une application $\psi : \Lambda \to \Lambda'$, telle que :
- ψ est un isomorphisme de $\mathbb{Z}$-modules, et préserve l'orientation,
- pour tout $u, v \in \Lambda$, on a $\mathfrak{b}(u, v) = \mathfrak{b}'(\psi(u), \psi(v))$.

Il est facile de voir que l'isomorphisme de couples défini ci-dessus est une relation d'équivalence. On note $\mathfrak{f}_n$ l'ensemble des classes d'équivalence sous cette relation.

Soient $(\Lambda, \mathfrak{b}, \overline{w}), (\Lambda', \mathfrak{b}', \overline{w'})$ deux éléments de $\mathfrak{E}_n$. S'ils sont isomorphes au sens de 1.2, alors les couples $(\Lambda, \mathfrak{b}), (\Lambda', \mathfrak{b}')$ sont isomorphes en tant qu'éléments de $\mathfrak{F}_n$. On a donc une application canonique $\pi : \mathfrak{e}_n \to \mathfrak{f}_n$, telle que $\pi([(\Lambda, \mathfrak{b}, \overline{w})]) = [(\Lambda, \mathfrak{b})]$ pour tout $(\Lambda, \mathfrak{b}, \overline{w})$ dans $\mathfrak{E}_n$, où $[(\Lambda, \mathfrak{b}, \overline{w})]$ (resp. $[(\Lambda, \mathfrak{b})]$) est la classe d'équivalence de $(\Lambda, \mathfrak{b}, \overline{w})$ (resp. de $(\Lambda, \mathfrak{b})$) dans $\mathfrak{E}_\mathfrak{n}$ (resp. dans $\mathfrak{F}_\mathfrak{n}$).

Maintenant on peut énoncer les théorèmes principaux de la deuxième partie.

Théorème 2.5.1. *On suppose que* 4 *ne divise pas* n.

- *Quand* $n \equiv 1, 2 \pmod 4$, *il existe une bijection entre* $\mathfrak{f}_n$ *et* $\mathcal{C}(-4n)$, *et dans cette bijection* $\mathrm{Im}(\pi)$ *correspond à un certain genre de discriminant* $-4n$, *qui représente* $\overline{-1+2n} \in \mathbb{Z}/4n\mathbb{Z}$.
- *Quand* $n \equiv 3 \pmod 4$, *il existe une bijection entre* $\mathfrak{f}_n$ *et la réunion disjointe de* $\mathcal{C}(-4n)$ *et* $\mathcal{C}(-n)$. *Si* $n \equiv 3 \pmod 8$, *alors dans cette bijection* $\mathrm{Im}(\pi)$ *correspond à un certain genre de discriminant* $-n$, *qui représente* -2 *; si* $n \equiv 7 \pmod 8$, *alors* $\mathrm{Im}(\pi)$ *est vide.*

Théorème 2.5.2. *On suppose que* 4 *ne divise pas* n *et que* $n > 4$. *Pour chaque* $[(\Lambda, \mathfrak{b})]$ *dans* $\mathrm{Im}(\pi)$, *il existe* $2^{r(n)-1}$ *éléments différents* $[(\Lambda, \mathfrak{b}, \overline{w})]$ *de* $\mathfrak{e}_n$, *tels que* $\pi([(\Lambda, \mathfrak{b}, \overline{w})]) = [(\Lambda, \mathfrak{b})]$.

2.6 Preuve de Théorème 2.5.1

Soit D un entier vérifiant les hypothèses de 2.1. On rappelle la définition et les propiétés du caractère $\chi : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$.

Lemme 2.6.1. *Pour un entier* k, *on note* $\overline{k}$ *la réduction de* k *modulo* D.

Quand $D \equiv 0 \pmod 4$, *écrivons* $D = -4m$ *avec* m *dans* $\mathbb{N}$, *alors on a*

$$\begin{aligned}\chi(\overline{-1}) &= -1\\ \chi(\overline{-1+2m}) &= \begin{cases}1, & si\ m \equiv 1,2 \pmod 4\\ -1, & si\ m \equiv 0,3 \pmod 4\end{cases}.\end{aligned}$$

Si m *est pair, on a*

$$\begin{aligned}\chi(\overline{-1+m}) &= \begin{cases}1, & si\ m \equiv 2 \pmod 4\\ -1, & si\ m \equiv 0 \pmod 4\end{cases}\\ \chi(\overline{1+3m}) &= -1.\end{aligned}$$

Si $m \equiv 1 \pmod 4$*, on a*

$$\begin{aligned}\chi(\overline{(-1+m)/4}) &= -\chi(\overline{(-1+9m)/4}), \text{ pour } m \equiv 5 \pmod 8\\ \chi(\overline{(-1+5m)/4}) &= -\chi(\overline{(-1+13m)/4}), \text{ pour } m \equiv 1 \pmod 8.\end{aligned}$$

Si $m \equiv 3 \pmod 4$*, on pose* $t = 3, 11$ *si* $m \equiv 7 \pmod 8$ *et* $t = 7, 15$ *si* $m \equiv 3 \pmod 8$*, alors on a*

$$\chi(\overline{(-1+tm)/4}) = -1.$$

Quand $D \equiv 1 \pmod 4$*, écrivons* $D = -m$ *avec* m *dans* $\mathbb{N}$*, alors on a*

$$\chi(\overline{-2}) = \begin{cases} 1, & si\ m \equiv 3 \pmod 8 \\ -1, & si\ m \equiv 7 \pmod 8 \end{cases}.$$

Démonstration Quand on suppose $D \equiv 0 \pmod 4$ et $D = -4m$, on a

$$\begin{aligned}\chi(\overline{-1}) &= \left(\tfrac{-4m}{4m-1}\right) = \left(\tfrac{-1}{4m-1}\right) = -1\\ \chi(\overline{-1+2m}) &= \left(\tfrac{-4m}{2m-1}\right) = \left(\tfrac{-2}{2m-1}\right) = \begin{cases} 1, & si\ m \equiv 1, 2 \pmod 4 \\ -1, & si\ m \equiv 0, 3 \pmod 4 \end{cases}.\end{aligned}$$

Si m est pair, on a

$$\begin{aligned}\chi(\overline{-1+m}) &= \left(\tfrac{-4m}{m-1}\right) = \left(\tfrac{-1}{m-1}\right) = \begin{cases} 1, & si\ m \equiv 2 \pmod 4 \\ -1, & si\ m \equiv 0 \pmod 4 \end{cases}\\ \chi(\overline{-1+3m}) &= \left(\tfrac{-4m}{3m-1}\right) = \left(\tfrac{-3}{3m-1}\right) = -1.\end{aligned}$$

Si $m \equiv 1 \pmod 4$, on pose $t = 1, 9$ pour $m \equiv 5 \pmod 8$ et $t = 5, 13$ pour $m \equiv 1 \pmod 8$, alors on a

$$\chi(\overline{(-1+tm)/4}) = \left(\frac{-4m}{(-1+tm)/4}\right) = \left(\frac{-t}{(-1+tm)/4}\right) = (-1)^{\frac{tm+5}{8}}.$$

Si $m \equiv 3 \pmod 4$, avec la notation de l'énoncé, on a

$$\chi(\overline{(-1+tm)/4}) = \left(\frac{-4m}{(-1+tm)/4}\right) = \left(\frac{-t}{(-1+tm)/4}\right) = -1.$$

Quand on suppose $D \equiv 1 \pmod 4$ et $D = -m$, alors on a

$$\chi(\overline{-2}) = \left(\tfrac{-m}{m-2}\right) = \left(\tfrac{-2}{m-2}\right) = \begin{cases} 1, & si\ m \equiv 3 \pmod 8 \\ -1, & si\ m \equiv 7 \pmod 8 \end{cases}.$$

□

Maintenant on peut démontrer théorème 2.5.1. Pour u dans $\mathfrak{F}_n$ et v dans $\mathcal{Q}(-4n)$ (ou $\mathcal{Q}(-n)$), on note $[u]$ et $[v]$ leur classes d'équivalence dans $\mathfrak{F}_n$ et dans $\mathcal{Q}(-4n)$ (ou $\mathcal{Q}(-n)$), respectivement.

Cas 1 Dans ce cas on suppose que $n \equiv 1, 2 \pmod 4$.

On construit d'abord une application $\varphi : \mathfrak{f}_n \to \mathcal{C}(-4n)$. Soient $(\Lambda, \mathfrak{b})$ un élément de $\mathfrak{F}_n$ et $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ la matrice de $\mathfrak{b}$ dans une base positive de Λ. Comme on a $ac - b^2 = n \equiv 1, 2 \pmod 4$, l'un de a, c est impair. On pose alors $\varphi([(\Lambda, \mathfrak{b})]) = [aX^2 + 2bXY + cY^2]$. Il est facile de voir que φ est bien définie et injective.

Montrons que φ est surjecctive. Soit $f = aX^2 + bXY + cY^2$ un élément de $\mathcal{Q}(-4n)$ avec a, b, c des entiers, alors b est pair car $b^2 - 4ac = -4n$. Donc la matrice $M := \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ peut être vue comme une forme bilinéaire primitive sur $\mathbb{Z}^2$. On a alors $\varphi([(\mathbb{Z}^2, M)]) = [f]$.

Donc φ est une bijection entre $\mathfrak{f}_n$ et $\mathcal{C}(-4n)$. Notons que pour $(\Lambda, \mathfrak{b})$ dans $\mathfrak{F}_n$, $[(\Lambda, \mathfrak{b})]$ est dans $\mathrm{Im}(\pi)$ si et seulement s'il existe w dans Λ, tel que $\mathfrak{b}(w, w) \equiv -1 \pmod n$. On note $\overline{k}$ la réduction de k modulo $4n$ pour tout entier k, alors un élément C de $\mathcal{C}(-4n)$ est dans $\varphi(\mathrm{Im}(\pi))$ si et seulement si au moins un des 4 éléments $\overline{-1}$, $\overline{-1+n}$, $\overline{-1+2n}$, $\overline{-1+3n}$ est représenté par les formes dans C.

Notons que $\overline{-1+2n} \in (\mathbb{Z}/4n\mathbb{Z})^*$ est toujours représenté par une forme dans $\mathcal{Q}(-4n)$ car on a $\chi(\overline{-1+2n}) = 1$. Donc il existe un certain genre G de discriminant $-4n$, tel que les formes dans G représentent $\overline{-1+2n}$. On a alors $G \subseteq \varphi(\mathrm{Im}(\pi))$.

On va montrer qu'en fait on a $G = \psi(\mathrm{Im}(\pi))$. Soit f dans $\mathcal{Q}(-4n)$ tels que $[f]$ est dans $\varphi(\mathrm{Im}(\pi))$, il suffit de montrer que $[f]$ est dans G.

Quand $n \equiv 2 \pmod 4$, on sait que $\chi(\overline{-1}) = \chi(\overline{-1+3n}) = -1$. Comme $[f]$ est dans $\varphi(\mathrm{Im}(\pi))$, f représente $\overline{-1+2n}$ ou $\overline{-1+n}$. Or, on a

$$\overline{-1+n} \cdot \overline{-1+2n}^{-1} = \overline{-1+n} \cdot \overline{-1+2n} = \overline{1+n},$$

Donc $\overline{-1+n}$ et $\overline{-1+2n}$ sont dans la même classe modulo H, car $\overline{1+n}$ est représenté par la forme principale. On en conclut qu'en tout cas f représente $\overline{-1+2n}$, et alors f est dans G.

On suppose maintenant que $n \equiv 1 \pmod 4$. Comme on a $\chi(\overline{-1}) = -1$ et $[f] \in \varphi(\mathrm{Im}(\pi))$, f représente $\overline{-1+n}$, $\overline{-1+2n}$ ou $\overline{-1+3n}$. Si f représente $\overline{-1+2n}$, on a bien $f \in G$. Si f représente $\overline{-1+3n}$, alors f représente aussi

$\overline{-1+n}$, car on a $\overline{-1+n} = \overline{-1+3n} \cdot \overline{1+n}$ avec $\overline{1+n}$ représenté par la forme principale. Donc on peut supposer que f représente $\overline{-1+n}$.

Écrivons $f = aX^2 + bXY + cY^2$ avec a, b, c des entiers. Alors b est pair. Par lemme 2.2.2, on peut supposer que a soit impair. Quitte à changer (X, Y) par $(X+Y, Y)$, on peut supposer que $\frac{b}{2}$ soit impair. Comme on a $ac - (\frac{b}{2})^2 = n \equiv 1 \pmod 4$, on voit que $c \equiv 2 \pmod 4$. Soient x, y des entiers tels que $\overline{f(x,y)} = \overline{-1+n}$. Par réduction modulo 2, on sait que 2 divise x. Par réduction modulo 4, on sait que 2 divise y.

Notons $w := f(\frac{x}{2}, \frac{y}{2})$, alors $\overline{w}$ est représenté par f, et on a $4w \equiv -1 + n \equiv -1 \pmod n$, i.e., $\overline{w}$ est l'un des 4 éléments $\overline{(-1+n)/4}$, $\overline{(-1+5n)/4}$, $\overline{(-1+9n)/4}$, $\overline{(-1+13n)/4}$. Quitte à remplacer $\frac{x}{2}$ par $\frac{x}{2}+n$, on peut supposer que $\overline{w}$ est dans $(\mathbb{Z}/4n\mathbb{Z})^*$.

Or, par le lemme précédent, on sait qu'en tout cas il existe au plus un des 4 éléments ci-dessus, qui est dans $(\mathbb{Z}/4n\mathbb{Z})^*$ et représenté par une forme de $\mathcal{Q}(-4n)$. Comme $\tilde{w} := \overline{-1+2n} \cdot \overline{(1+n)/2}^2 \in (\mathbb{Z}/4n\mathbb{Z})^*$ est représenté par les formes dans G et la réduction de $4\tilde{w}$ modulo n vaut -1, on a $\overline{w} = \tilde{w}$. Donc $\overline{w}$ et $\overline{-1+2n}$ sont dans la même classe modulo H, et on a $f \in G$ car f représente $\overline{w}$.

On conclut que $G = \varphi(\mathrm{Im}(\pi))$.

Cas 2 Dans ce cas on suppose que $n \equiv 3 \pmod 4$.

On construit d'abord une application $\varphi : \mathfrak{f}_n \to \mathcal{C}(-4n) \bigcup \mathcal{C}(-n)$. Soient $(\Lambda, \mathfrak{b})$ un élément de $\mathfrak{F}_n$ et $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ la matrice de $\mathfrak{b}$ dans une base positive de Λ. On pose alors

$$\varphi([(\Lambda, \mathfrak{b})]) = \begin{cases} [\frac{a}{2}X^2 + bXY + \frac{c}{2}Y^2] \in \mathcal{C}(-n), & \textit{si } a, c \textit{ sont pairs} \\ [aX^2 + 2bXY + cY^2] \in \mathcal{C}(-4n), & \textit{sinon} \end{cases}.$$

Il est facile de voir que φ est bien définie et injective.

Montrons que φ est surjective. Soit $f = aX^2 + bXY + cY^2$ un élément de $\mathcal{Q}(-4n) \bigcup \mathcal{Q}(-n)$ avec a, b, c des entiers. Si f est dans $\mathcal{Q}(-4n)$, alors b est pair car $b^2 - 4ac = -4n$, et on pose $M := \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$; si f est dans $\mathcal{Q}(-n)$, alors

b est impair car $b^2 - 4ac = -n \equiv 1 \pmod 4$, et on pose $M := \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$. On voit qu'en tout cas M peut être vue comme une forme bilinéaire primitive sur $\mathbb{Z}^2$, et qu'on a $\psi([(\mathbb{Z}^2, M)]) = [f]$.

Donc φ est une bijection entre $\mathfrak{f}_n$ et $\mathcal{C}(-4n) \bigcup \mathcal{C}(-n)$. On va montrer que $\mathcal{C}(-4n) \bigcap \varphi(\mathrm{Im}(\pi))$ est vide. Pour tout entier k, notons $\overline{k}$ la réduction de k modulo $4n$, alors il suffit de montrer qu'aucun des 4 éléments $\overline{-1}$, $\overline{-1+n}$, $\overline{-1+2n}$, $\overline{-1+3n}$ n'est représenté par aucune forme dans $\mathcal{Q}(-4n)$.

Par l'absurde, supposons qu'une forme f dans $\mathcal{Q}(-4n)$ représente l'un des 4 éléments ci-dessus. Par lemme 2.6.1 appliqué à $D = -4n$, $\overline{-1}$ et $\overline{-1+2n}$ ne sont pas représentés par f. Si $\overline{-1+n}$ est représenté par f, alors $\overline{-1+3n}$ l'est aussi, car on a $\overline{-1+3n} = \overline{-1+n} \cdot \overline{1+n}$ avec $\overline{1+n}$ représenté par la forme principale. Donc on peut supposer que f représente $\overline{-1+3n}$.

Comme dans la démonstration de proposition 2.6.1, on peut trouver un entier w représenté par f, tel que la réduction de w modulo $4n$ est dans $(\mathbb{Z}/4n\mathbb{Z})^*$, et qu'on a $4w \equiv -1 \pmod{4n}$. Or, cela contredit lemme 2.6.1 appliqué à $D = -4n$.

On en déduit que $\varphi(\mathrm{Im}(\pi)) \subseteq \mathcal{C}(-n)$. Pour tout entier k, notons maintenant $\overline{k}$ la réduction de k modulo n, alors pour une forme f dans $\mathcal{Q}(D)$, $[f]$ est dans $\varphi(\mathrm{Im}(\pi))$ si et seulement si f représente $\overline{-1}/2$, ou de façon équivalente, si et seulement si f représente $\overline{-2}$ (notons que 2 est dans $(\mathbb{Z}/n\mathbb{Z})^*$).

Le résultat découle donc du lemme 2.6.1 appliqué à $D = -n$.

□

On a donc démontré théorème 2.5.1.

Corollaire 2.6.1. *Quand* $n \equiv 1, 2 \pmod 4$, *on a* $\mathrm{card}(\mathrm{Im}(\pi)) = \frac{h(-4n)}{2^{r(n)}}$ *;*
Quand $n \equiv 3 \pmod 8$, *on a* $\mathrm{card}(\mathrm{Im}(\pi)) = \frac{h(-n)}{2^{r(n)-1}}$ *;*
Quand $n \equiv 7 \pmod 8$, *on a* $\mathrm{card}(\mathrm{Im}(\pi)) = 0$.

Démonstration C'est une conséquence de corollaire 2.4.1.

□

2.7 Preuve de Théorème 2.5.2

On pose les mêmes hypothèses sur n que dans l'énoncé de théorème 2.5.2. Dans ce paragraphe, on fixe un élément de $\mathrm{Im}(\pi)$, que l'on écrit comme $[(\Lambda, \mathfrak{b})]$ avec $(\Lambda, \mathfrak{b})$ dans $\mathfrak{F}_n$. On pose $F := \pi^{-1}([(\Lambda, \mathfrak{b})])$, alors théorème 2.5.2 est équivalent à dire que $\mathrm{card}(F) = 2^{r(n)-1}$.

Considérons l'ensemble $W := \{\overline{w} \in \Lambda/n\Lambda^* : \overline{\mathfrak{b}}(\overline{w}, \overline{w}) = \overline{-1} \in \mathbb{Z}/n\mathbb{Z}\}$. On a une application $\tau : W \to F$, telle que $\tau(\overline{w}) = [(\Lambda, \mathfrak{b}, \overline{w})]$. On voit facilement que τ est bien définie.

La démonstration de théorème 3 est donnée par les deux propositions suivantes.

Proposition 2.7.1. *On a* $\mathrm{card}(W) = 2\mathrm{card}(F)$.

Démonstration Notons Id l'application identitée sur Λ. On va montrer que les seules isomorphismes de $(\Lambda, \mathfrak{b})$ vers lui-même sont $\pm\mathrm{Id}$.

Soit η un isomorphisme de $(\Lambda, \mathfrak{b})$ vers lui-même. On fixe une base positive de Λ, et on note $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ (resp. $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$) la matrice de η (resp. de $\mathfrak{b}$) dans cette base. Comme η est un isomorphisme, on a $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ et $\mathfrak{b}(u, v) = \mathfrak{b}(\eta(u), \eta(v))$ pour tout u, v dans Λ, i.e.,

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} s & -q \\ -r & p \end{pmatrix}.$$

On en déduit que $2br = a(s-p)$ et $cr = -aq$, i.e., $\frac{r}{a} = \frac{s-p}{2b} = \frac{-q}{c}$ (on n'écarte pas le cas $b = 0$). Comme $\mathrm{pgcd}(a, 2b, c)$ divise 2, il existe un entier t, tel que $r = \frac{a}{2}t$, $s - p = bt$, $-q = \frac{c}{2}t$. Donc on a

$$1 = ps - qr = p(p + bt) + \frac{ac}{4}t^2 = (p + \frac{bt}{2})^2 + \frac{n}{4}t^2.$$

Comme on a supposé que $n > 4$, on voit que $t = 0$. Donc on a $q = r = 0$ et $p = s = \pm 1$, i.e., $\eta = \mathrm{Id}$ ou $\eta = -\mathrm{Id}$.

On conclut que pour tout ω, ω' dans W, $\tau(\omega) = \tau(\omega')$ est équivalent à $\omega' = \pm\omega$. Il suffit donc de montrer que pour tout ω dans W, on a $\omega \neq -\omega$. Or, $\omega = -\omega$ implique que

$$\overline{0} = \overline{\mathfrak{b}}(\omega, 2\omega) = 2\overline{\mathfrak{b}}(\omega, \omega) = \overline{2},$$

i.e., $n = 2$. Cela contredit l'hypothèse $n > 4$.

□

Proposition 2.7.2. *On a* $\mathrm{card}(W) = 2^{r(n)}$.

Démonstration Comme $[(\Lambda, \mathfrak{b})]$ est dans $\mathrm{Im}(\pi)$, on sait qu'il existe un élément ω de $\Lambda/n\Lambda^*$, tel que $(\Lambda, \mathfrak{b}, \omega)$ est dans $\mathfrak{E}_n$. Par lemme 1.6.1, on sait que $\Lambda/n\Lambda^*$ est un groupe cyclique d'ordre n engendré par ω. Or, pour un entier k, $k\omega$ est dans W si et seulement si $\overline{b}(k\omega, k\omega) = \overline{-1}$, i.e., $k^2 \equiv 1 \pmod{n}$. On en déduit que $\mathrm{card}(W)$ est juste le nombre des éléments d'ordre 2 du groupe $(\mathbb{Z}/n\mathbb{Z})^*$.

Comme 4 ne divise pas n, on peut écrire $n = \epsilon \prod\limits_{i=1}^{r(n)} p_i^{\alpha_i}$ avec p_i des nombres premiers impairs différents, α_i des entiers positifs et ϵ dans $\{1, 2\}$. Par le lemme chinois, $(\mathbb{Z}/n\mathbb{Z})^*$ est isomorphe à $\oplus_{i=1}^{r(n)} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$. Comme le groupe $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$ est cyclique d'ordre pair, il admet exactement 2 éléments d'ordre 2. On a donc $\mathrm{card}(W) = 2^{r(n)}$.

□

On a démontré théorème 2.5.2.

Par théorème 2.5.2 et corollaire 2.6.1, on a

$$\mathrm{card}\mathfrak{e}_n = 2^{r(n)-1}\mathrm{card}(\mathrm{Im}(\pi)) = \begin{cases} \frac{h(-4n)}{2}, & si\ n \equiv 1, 2 \pmod{4} \\ h(-n), & si\ n \equiv 3 \pmod{8} \\ 0, & si\ n \equiv 7 \pmod{8} \end{cases} .$$

3 Conclusion

Lemme 3.0.1. *Soit n un entier tel que $n > 4$ et $n \equiv 3 \pmod{8}$, alors on a $h(-4n) = 3h(-n)$.*

Démonstration On construit une application $\Theta : \mathcal{C}(-4n) \to \mathcal{C}(-n)$. Soit f un élément de $\mathcal{Q}(-4n)$, que l'on voit comme une forme quadratique sur $\mathbb{Z}^2$. Comme le $\mathbb{F}_2$-espace vectoriel $\mathbb{Z}^2/2\mathbb{Z}^2$ est de dimension 2, il y a 3 éléments non nuls dedans. f induit une $\mathbb{F}_2$-forme quadratique sur $\mathbb{Z}^2/2\mathbb{Z}^2$, notée $\overline{f}$, par la formule suivante : $\overline{f}(\overline{u}) = \overline{f(u)}$. On voit facilement que $\overline{f}$ est en fait une forme linéaire, elle est non nulle car f est primitive. Donc le noyau de

$\overline{f}$ est de dimension 1, i.e., il existe un unique élément non nul L de $\mathbb{Z}^2/2\mathbb{Z}^2$, tel que L est dans $\ker(\overline{f})$.

Notons $\Lambda := \mathbb{Z}^2 \bigcup \frac{1}{2}L = \frac{1}{2} \cdot \cup\ker(\overline{f})$, alors Λ est un $\mathbb{Z}$-module, et on a $\mathbb{Z}^2 \subsetneq \Lambda \subsetneq \frac{1}{2}\mathbb{Z}^2$. Donc il existe (e_1, e_2) une base de $\mathbb{Z}^2$, tel que $(e_1, \frac{1}{2}e_2)$ est une base de Λ. Écrivons $f(X \cdot e_1 + Y \cdot e_2) = aX^2 + bXY + cY^2$ avec a, b, c des entiers, alors b est pair car $b^2 - 4ac$ vaut $-4n$, et c est pair car $\overline{e_2} \in \mathbb{Z}^2/2\mathbb{Z}^2$ est dans $\ker(\overline{f})$. Donc on a $(\frac{b}{2})^2 - ac = -n \equiv -3 \pmod 8$, et on en déduit que $\frac{b}{2}$ est impair, a est impair et 4 divise c. Notons g la forme quadratique sur Λ induite par f, alors on a $g(X \cdot e_1, Y \cdot \frac{1}{2}e_2) = aX^2 + \frac{b}{2}XY + \frac{c}{4}Y^2$ est un élément de $\mathcal{Q}(-n)$. On définit donc $\Theta([f]) = [g]$, où $[f]$ (resp. $[g]$) est la classe de f (resp. de g) modulo $\mathrm{SL}_2(\mathbb{Z})$ dans $Q(-4n)$ (resp. dans $Q(-n)$). Il est facile de voir que Θ est bien définie. On va montrer que Θ est une application 3-à-1, i.e., pour chaque C dans $\mathcal{C}(-n)$, on a $\mathrm{card}(\Theta^{-1}\{C\}) = 3$.

Soit $g = aX^2 + bXY + cY^2$ un élément de $Q(-n)$, que l'on voit comme une forme quadratique sur $\mathbb{Z}^2$. Alors on a $b^2 - 4ac = -n \equiv -3 \pmod 8$, donc a, b, c sont impairs. Si f est un élément de $Q(-4n)$ tel que $\Theta([f]) = [g]$, alors par construction de Θ, on peut identifier f avec la restriction de g sur un sous-$\mathbb{Z}$-module de $\mathbb{Z}^2$, noté Γ, tel que $2\mathbb{Z}^2 \subsetneq \Gamma \subsetneq \mathbb{Z}^2$. Mais il n'existe que 3 tels Γ (car $\mathbb{Z}^2/2\mathbb{Z}^2$ est un $\mathbb{F}_2$-espace vectoriel de dimension 2), i.e., $\Gamma_1 = \mathbb{Z}(2,0) \oplus \mathbb{Z}(0,1)$, $\Gamma_2 = \mathbb{Z}(1,0) \oplus \mathbb{Z}(0,2)$, $\Gamma_3 = \mathbb{Z}(1,1) \oplus \mathbb{Z}(-1,1)$, donc il suffit de montrer que la classe de $f_i := g|_{\Gamma_i}$ sont dans $\Theta^{-1}([g])$, et que les $[f_i]$ sont différentes.

On vérifie facilement que

$$\begin{aligned} f_1(X \cdot (2,0) + Y \cdot (0,1)) &= 4aX^2 + 2bXY + cY^2 \\ f_2(X \cdot (1,0) + Y \cdot (0,2)) &= aX^2 + 2bXY + 4cY^2 \\ f_3(X \cdot (1,1) + Y \cdot (-1,1)) &= (a+b+c)X^2 + 2(c-a)XY + (a-b+c)Y^2 \end{aligned}$$

sont des formes primitives, et donc par construction de Θ on a $\Theta([f_i]) = [g]$. Il reste à montrer que les $[f_i]$ sont différentes.

Supposons qu'on a $[f_1] = [f_2]$, alors il existe une matrice $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ dans $\mathrm{SL}_2(\mathbb{Z})$, telle que

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} \begin{pmatrix} 4a & b \\ b & c \end{pmatrix} = \begin{pmatrix} a & b \\ b & 4c \end{pmatrix} \begin{pmatrix} s & -q \\ -r & p \end{pmatrix}.$$

On en déduit que $2br = a(s-4p)$ et $cr = -aq$, i.e., $\frac{r}{a} = \frac{s-4p}{2b} = \frac{-q}{c}$ (on n'écarte pas le cas $b = 0$). Comme on a $\mathrm{pgcd}(a, 2b, c) = 1$, il existe un entier t, tel que $r = at$, $s - 4p = 2bt$, $-q = ct$. Donc on a

$$1 = ps - qr = p(4p + 2bt) + act^2 = (2p + \frac{bt}{2})^2 + \frac{n}{4}t^2.$$

Comme on a supposé que $n > 4$, on voit que $t = 0$. Mais alors on a $1 = 4p^2$, contradiction.

On conclut que $[f_1]$ et $[f_2]$ sont différentes. On montre pareillement que $[f_1] \neq [f_3]$ et $[f_2] \neq [f_3]$.

Donc Θ est bien une application 3-à-1, et on a $h(-4n) = 3h(-n)$.

$\square$

Théorème de Trois Carrés Soit n un entier tel que $n > 4$ et 4 ne divise pas n. Alors le nombre des solutions entières primitives, noté R_n, est donné par

$$R_n = \rho(n)h(-4n),$$

où

$$\rho(n) = \begin{cases} 12, & si\ n \equiv 1, 2 \pmod 4 \\ 8, & si\ n \equiv 3 \pmod 8 \\ 0, & si\ n \equiv 7 \pmod 8 \end{cases}.$$

Démonstration Par le résultat de la première partie, on a

$$R_n = \mathrm{card}(\mathfrak{R}_n) = 24\mathrm{card}(\mathfrak{e}_n).$$

Par le résultat de la deuxième partie, on a

$$\mathrm{card}\mathfrak{e}_n = \begin{cases} \frac{h(-4n)}{2}, & si\ n \equiv 1, 2 \pmod 4 \\ h(-n), & si\ n \equiv 3 \pmod 8 \\ 0, & si\ n \equiv 7 \pmod 8 \end{cases}.$$

En utilisant le lemme précédent, on obtient la formule voulue.

$\square$

Corollaire Un entier positif peut s'écrire comme la somme de trois carrés si et seulement s'il n'est pas de la forme $n = 4^k(8b + 7)$, où k, b sont des entiers non négatifs.

Démonstration Il suffit de remarquer que, quand on a $n = x^2 + y^2 + z^2$ avec 4 divise n, alors x, y, z sont tous pairs par un argument modulo 4.

$\square$

Références

[1] D. A. Cox, *Primes of the forme* $x^2 + ny^2$, §1 à 4 et 7, John Wiley & Sons, 1989.

[2] E. Grosswald, *Representations of integers as sums of squares*, chap.4, Springer-Verlag, 1985.

[3] C. F. Gauss, *Disquisitiones arithmeticae*, Leipzig, 1801.