CHAPITRE 3

Formes quadratiques binaires entières

RÉFÉRENCE : Le livre de Gauss déjà cité.

1. Vocabulaire des formes

Définition 3.1. *Une forme quadratique binaire entière est une fonction $q : \mathbb{Z}^2 \to \mathbb{Z}$ telle qu'il existe $a, b, c \in \mathbb{Z}$ vérifiant*

$$q(x, y) = ax^2 + bxy + cy^2, \ \ \forall x, y \in \mathbb{Z}.$$

Dans tout ce chapitre, nous appellerons simplement "forme" une "forme quadratique binaire entière". Remarquons que si q est comme dans la définition ci-dessus, on a

$$a = q(1, 0), \ b = q(0, 1), \text{ et } \ a + b + c = q(1, 1).$$

La forme q est donc uniquement déterminée par le triplet $(a, b, c) \in \mathbb{Z}^3$, c'est pourquoi nous la désignerons souvent simplement par le symbole (a, b, c), à la manière de Gauss [1]. On note $\mathcal{Q}(\mathbb{Z}^2)$ l'ensemble des formes, c'est un groupe abélien pour l'addition évidente des fonctions.

La forme (a, b, c) est dite *primitive* si a, b, c sont premiers entre eux dans leur ensemble. Autrement dit, une forme est primitive si elle n'est pas égale à nq où $n \geq 2$ et $q \in \mathrm{Q}(\mathbb{Z}^2)$. L'étude de toutes les formes se ramenant trivialement à celle des formes primitives, on se concentrera parfois sur ces dernières, notamment lorsque cela allègera les énoncés.

Définition 3.2. *On dit que la forme q représente l'entier $n \in \mathbb{Z}$ s'il existe $(x, y) \in \mathbb{Z}^2$ tel que $q(x, y) = n$. Si $n = 0$, on requiert de plus que $(x, y) \neq (0, 0)$.*

On dit que q représente primitivement l'entier $n \in \mathbb{Z}$ s'il existe $x, y \in \mathbb{Z}$ premiers entre eux tels que $q(x, y) = n$.

Déterminer l'ensemble des entiers représentés par une forme donnée est la motivation principale de ce chapitre. Pour les formes du type $x^2 + dy^2$, ce problème a été soulevé au chapitre précédent, et d'autres formes quadratiques annexes sont alors apparues, ce qui justifie en partie (suivant Lagrange) que l'on s'y intéresse dans cette généralité. Par exemple, la forme $x^2 + 5y^2$ s'est trouvée accompagnée de la forme $2x^2 + 2xy + 3y^2$, l'une et l'autre représentant alors exclusivement les premiers p tels que $\left(\frac{-5}{p}\right) = 1$.

1. Le lecteur qui étudiera Gauss prendra garde qu'il ne considère que des formes du type $ax^2 + 2bxy + cy^2$ avec $a, b, c \in \mathbb{Z}$, et qu'il note donc (a, b, c) ce que nous notons $(a, 2b, c)$.

Notons que si l'on connaît tous les entiers primitivement représentés par q, alors on connaît tous les entiers représentés par q, de sorte que l'on se concentrera souvent sur ceux-ci. Une forme peut cependant représenter un même entier primitivement et non primitivement : la forme $(1,0,1)$ représente 25 primitivement et non primitivement (et 4 uniquement non primitivement). Remarquons enfin que si un nombre premier est représenté par q, il l'est nécessairement primitivement.

Une quantité fondamentale attachée à une forme est son discriminant.

Définition 3.3. *Le discriminant de la forme $q = (a,b,c)$ est l'entier* $\mathrm{disc}(q) = b^2 - 4ac$.

Par exemple, le discriminant de x^2+dy^2 est $-4d$. On constate aussi que x^2+5y^2 et $2x^2+2xy+3y^2$ sont toutes deux de discriminant -20. De même, les formes $(1,0,11)$ et $(3,2,4)$ rencontrées dans l'étude des premiers de la forme x^2+11y^2 sont toutes deux de discriminant -44.

Nous verrons par la suite que le discriminant d'une forme détermine grandement les propriétés des entiers qu'elle représente. La question la plus élémentaire est celle de leur signe.

Proposition 3.4. (Signe du trinôme) *Soit q une forme de discriminant D.*

(i) q représente 0 si, et seulement si, D est un carré,

(ii) $D \leq 0$ si, et seulement si, les entiers non nuls représentés par q sont tous de même signe.

Démonstration — Écrivons $q=(a,b,c)$. Supposons d'abord $a=0$. Dans ce cas q représente 0, $D=b^2$ est un carré, et $q(x,y)=bxy+cy^2$. Cela montre (i). De plus on a $D\leq 0$ si, et seulement si, on a $b=0$, soit $q(x,y)=cy^2$, ce qui entraîne (ii).

Supposons maintenant $a\neq 0$. En particulier $q(x,y)=0$ avec $(x,y)\neq 0$ entraîne $y\neq 0$. Considérons l'identité remarquable ("forme canonique")

$$4aq(x,y) = (2ax+by)^2 - Dy^2. \tag{2}$$

On en déduit que q représente 0 si, et seulement si, D est un carré dans $\mathbb{Q}$, ou ce qui revient au même si D est un carré dans $\mathbb{Z}$ (car $\overline{\mathbb{Z}}\cap\mathbb{Q}=\mathbb{Z}$!). Le sens $\Rightarrow$ du (ii) s'ensuit également car si $D\leq 0$ et $q(x,y)\neq 0$ alors $aq(x,y)>0$. Pour la réciproque, on considère $(x,y)=(-b,2a)$. □

Cela nous conduit à une discussion sur l'involution sur les formes $q=(a,b,c)\mapsto -q=(-a,-b,-c)$. Bien sûr, $\mathrm{disc}(q)=\mathrm{disc}(-q)$ et cette involution échange formes à valeurs ≥ 0 et formes à valeurs ≤ 0. Ainsi, dans l'étude des formes de discriminant <0 (qui ne représentent pas 0), on ne perdra rien à ne considérer que des formes (a,b,c) à valeurs positives, ou ce qui revient au même telles que $a>0$.

Convention : *Dorénavant, nous supposerons toujours qu'une forme de discriminant <0 est positive. Autrement dit, si (a,b,c) est une forme telle que $b^2-4ac<0$, on supposera de plus que $a>0$.*

La théorie des formes de discriminant <0 s'avèrera sensiblement plus simple. En effet, considérons par exemple le problème algorithmique consistant à déterminer

tous les entiers positifs représentés par une forme $q = (a, b, c)$ de discriminant $D < 0$. L'identité (2) montre que $q(x, y) = n$ entraîne

$$|y| \leq \sqrt{\frac{4an}{-D}} \text{ et } |2ax + by| \leq \sqrt{4an},$$

en particulier il n'y a qu'un nombre fini de couples (x, y) à tester pour résoudre $q(x, y) = n$. Quand $D > 0$ ce n'est plus vrai. Par exemple l'équation de "Pell-Fermat" $x^2 - 2y^2 = 1$ admet une infinité de solutions $(x, y) \in \mathbb{Z}^2$ (Exercice 3.7).

2. Notions d'équivalence entre deux formes

Suivant Lagrange, étudions maintenant les formes obtenues par changement de variables à coefficients entiers à partir d'une forme donnée. C'est une question tout à fait importante car les entiers représentés par la forme obtenue seront évidemment parmi ceux représentés par la forme dont on est parti, et qu'en particulier deux formes obtenues par changement de variable réversible représentent les même entiers.

Fixons donc q une forme, ainsi que u, v deux éléments de $\mathbb{Z}^2$. La fonction

$$(x, y) \mapsto q(xu + yv),\ \mathbb{Z}^2 \to \mathbb{Z},$$

est alors une nouvelle forme. Concrètement, si l'on écrit $u = (\alpha, \gamma)$ et $v = (\beta, \delta)$, on trouve simplement la forme $q(\alpha x + \beta y, \gamma x + \delta y)$, de sorte que l'on a simplement opéré le changement de variables $(x, y) \mapsto (\alpha x + \beta y, \gamma x + \delta y)$. La notation matricielle suivante sera parfois commode.

NOTATION : Si $(x, y) \in \mathbb{Z}^2$, on pose $q(\begin{pmatrix} x \\ y \end{pmatrix}) = q(x, y)$, autrement dit on voit les éléments de $\mathbb{Z}^2$ comme des vecteurs colonnes. Si u et v sont comme ci-dessus on a donc la relation

$$q(xu + yv) = q(x \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} + y \begin{pmatrix} \beta \\ \delta \end{pmatrix}) = q(P \begin{pmatrix} x \\ y \end{pmatrix})$$

où $P = \mathrm{Mat}(u, v) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ est la matrice des vecteurs u et v dans la base canonique de $\mathbb{Z}^2$.

Proposition-Définition 3.5. *Si $q \in \mathrm{Q}(\mathbb{Z}^2)$ et $M \in \mathrm{M}_2(\mathbb{Z})$ on note $q \cdot M$ la forme $(x, y) \mapsto q(M \begin{pmatrix} x \\ y \end{pmatrix})$. Pour tout $M, N \in \mathrm{M}_2(\mathbb{Z})$ et tout $q \in \mathrm{Q}(\mathbb{Z}^2)$, on a la relation $(q \cdot M) \cdot N = q \cdot (MN)$.*

Le cas le plus important de changement de coordonnées est celui où u, v est une $\mathbb{Z}$-base de $\mathbb{Z}^2$, ou ce qui revient au même si le déterminant de $P = \mathrm{Mat}(u, v)$ vaut ± 1 (i.e. $P \in \mathrm{GL}_2(\mathbb{Z})$), car alors ce changement de variables est réversible : $q = (q \cdot P) \cdot P^{-1}$. Dans ce cas, la forme obtenue renferme à bien des égards la même information que la forme q, et selon la définition suivante sera dite *équivalente* à q. On rappelle que

$$\mathrm{SL}_2(\mathbb{Z}) := \{P \in \mathrm{GL}_2(\mathbb{Z}) \mid \det(P) = 1\},$$

c'est donc un sous-groupe distingué d'indice 2 de $\mathrm{GL}_2(\mathbb{Z})$. On dira qu'une $\mathbb{Z}$-base u, v de $\mathbb{Z}^2$ est directe si $\det(u, v) = +1$.

Définition 3.6. *Deux formes q et q' sont dites équivalentes (resp. proprement équivalentes) s'il existe une $\mathbb{Z}$-base u, v de $\mathbb{Z}^2$ (resp. une $\mathbb{Z}$-base directe) telle que $q'(x, y) = q(xu + vy)$ pour tout $x, y \in \mathbb{Z}$. Il revient au même de dire qu'il existe $P \in \mathrm{GL}_2(\mathbb{Z})$ (resp. $P \in \mathrm{SL}_2(\mathbb{Z})$) tel que $q' = q \cdot P$.*

On notera $q \sim q'$ (resp. $q \overset{+}{\sim} q'$) si q et q' sont équivalentes (resp. proprement équivalentes). Ce sont des relations d'équivalence sur $\mathrm{Q}(\mathbb{Z}^2)$. En effet, la relation (3.5) signifie que $(P, q) \mapsto q \cdot P$ est une action à droite du groupe $\mathrm{GL}_2(\mathbb{Z})$ (resp. $\mathrm{SL}_2(\mathbb{Z})$) sur $\mathrm{Q}(\mathbb{Z}^2)$ dont les orbites sont les classes d'équivalence (resp. d'équivalence propre). Notons que $q \overset{+}{\sim} q'$ entraîne évidemment $q \sim q'$. En particulier, l'ensemble des classes d'équivalence (resp. d'équivalence propre) de formes est une partition de $\mathrm{Q}(\mathbb{Z}^2)$.

La notion d'équivalence est due à Lagrange et celle d'équivalence propre à Gauss. Même si la première est la plus naturelle dans les questions de représentation des entiers, c'est la seconde qui permettra de comprendre les propriétés les plus fines des formes, comme l'a vu Gauss. L'intérêt des de la notion d'équivalence propre n'apparaîtra clairement que plus tard dans le cours, lorsque sera discutée la notion de composition des formes.

Lemme 3.7. (Équivalences élémentaires) *Pour tout $a, b, c \in \mathbb{Z}$, on a $(a, b, c) \sim (a, -b, c)$ et*

$$(a, b, c) \overset{+}{\sim} (c, -b, a) \overset{+}{\sim} (a, b + 2a, c + b + a) \overset{+}{\sim} (a, b - 2a, c - b + a).$$

Démonstration — En effet, cela découle des changements de variables $(x, y) \mapsto (x, -y)$ (qui change l'orientation), $(x, y) \mapsto (y, -x)$, $(x + y, y)$ et $(x - y, y)$ (qui la préservent), qui correspondent aussi respectivement aux matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

□

Par exemple, la forme $(5, 6, 2)$ est proprement équivalente à $(1, 0, 1)$. On peut en effet le voir en appliquant les équivalences élémentaires suivantes : $(5, 6, 2) \overset{+}{\sim} (2, -6, 5) \overset{+}{\sim} (2, -2, 1) \overset{+}{\sim} (1, 2, 2) \overset{+}{\sim} (1, 0, 1)$.

Proposition 3.8. *Deux formes équivalentes représentent les mêmes entiers, primitivement ou non, et ce le même nombre de fois. De plus, elles sont simultanément primitives. Enfin, deux formes équivalentes ont même discriminant.*

Démonstration — Le premier point de la proposition est évident : si $P \in \mathrm{GL}_2(\mathbb{Z})$ alors

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto P^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$$

définit une bijection entre les $(x, y) \in \mathbb{Z}^2$ tels que $q(x, y) = n$ et les $(x', y') \in \mathbb{Z}^2$ tels que $(q \cdot P)(x', y') = n$, son inverse étant $\begin{pmatrix} x' \\ y' \end{pmatrix} \mapsto P \begin{pmatrix} x' \\ y' \end{pmatrix}$. Comme $u \in \mathbb{Z}^2$ est primitif si et seulement s'il n'est pas de la forme mv avec $v \in \mathbb{Z}^2$ et $m \geq 2$,

on voit de plus que u est primitif si, et seulement si, Pu l'est. La seconde assertion découle de ce que si $m \in \mathbb{Z}$, $q \in \mathrm{Q}(\mathbb{Z}^2)$ et $M \in \mathrm{M}_2(\mathbb{Z})$, alors $(mq) \cdot P = m(q \cdot P)$. La dernière assertion découle de la proposition suivante et de ce que le déterminant d'un élément de $\mathrm{GL}_2(\mathbb{Z})$ est toujours ± 1. □

Proposition 3.9. *Si q est une forme et $P \in \mathrm{M}_2(\mathbb{Z})$, alors* $\mathrm{Mat}(q \cdot P) = {}^tP \,\mathrm{Mat}(q)\, P$. *En particulier,* $\mathrm{disc}(q \cdot P) = \det(P)^2 \mathrm{disc}(q)$.

Démonstration — Si $q = (a, b, c)$, posons $\mathrm{Mat}(q) = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$. On a $\mathrm{disc}(q) = -\det(\mathrm{Mat}(q))$. On conclut par l'identité matricielle $2q(x, y) = {}^t\begin{pmatrix} x \\ y \end{pmatrix} \mathrm{Mat}(q) \begin{pmatrix} x \\ y \end{pmatrix}$, valable pour tout $x, y \in \mathbb{Z}$. □

Observons que deux formes de même discriminant ne sont pas nécessairement équivalentes. Par exemple, les deux formes $(1, 0, 5)$ et $(2, 2, 3)$ ont même discriminant -20. La seconde représente 2 mais pas la première, car 2 n'est pas de la forme x^2+5y^2 avec $x, y \in \mathbb{Z}$.

3. Entiers représentés par une forme, d'après Lagrange

Théorème 3.10. (Lagrange) *Soient $D, n \in \mathbb{Z}$. Il y a équivalence entre :*

(i) D est un carré modulo $4n$,

(ii) il existe une forme de discrimininant D qui représente primitivement n.

En effet, supposons que D est un carré modulo $4n$. On peut donc trouver $b, c \in \mathbb{Z}$ tels que $D = b^2 - 4nc$. Mais alors la forme $q = (n, b, c)$ est de discrimimant D, et représente primitivement $n = q(1, 0)$. On a montré (i) implique (ii).

La réciproque, d'apparence moins intéressante, est plus difficile. Nous aurons besoin des deux lemmes suivants. On dira qu'un vecteur $(x, y) \in \mathbb{Z}^2$ est primitif si x et y sont premiers entre eux.

Lemme 3.11. *Tout vecteur primitif $u \in \mathbb{Z}^2$ se complète en une $\mathbb{Z}$-base directe u, v de $\mathbb{Z}^2$.*

Démonstration — En effet, écrivons $u = (x, y)$. Soient $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha x + \beta y = 1$ (Bézout). On constate que

$$\det \begin{pmatrix} x & -\beta \\ y & \alpha \end{pmatrix} = 1$$

donc (x, y) et $(-\beta, \alpha)$ forment une $\mathbb{Z}$-base directe de $\mathbb{Z}^2$. □

Lemme 3.12. (Lemme clé) *L'entier $n \in \mathbb{Z}$ est primitivement représenté par la forme q si, et seulement si, $q \overset{+}{\sim} (n, b, c)$, avec de plus $-|n| < b \leq |n|$ si $n \neq 0$.*

Démonstration — Une forme du type (n, b, c) représente primitivement l'entier n car $q(1, 0) = n$, ainsi donc que toute forme équivalente. Réciproquement, soient q une forme et $n = q(u)$ avec u primitif. D'après le lemme précédent, on peut compléter le vecteur u en une $\mathbb{Z}$-base u, v de $\mathbb{Z}^2$ telle que $\det(u, v) = 1$. Si q' est la forme $q'(x, y) = q(ux + vy)$ alors $q' \overset{+}{\sim} q$ et $q' = (n, *, *)$. Cela conclut le cas $n = 0$, puis le cas $n \neq 0$ en appliquant de manière répétée les équivalences propres élémentaires (Lemme 3.7). □

Terminons la démonstration du théorème de Lagrange. Supposons que n est primitivement représenté par une forme q. Le lemme précédent assure que l'on a $q \overset{+}{\sim} (n, b, c)$ pour certains $b, c \in \mathbb{Z}$. D'après la proposition 3.8, $\mathrm{disc}(q) = b^2 - 4nc$. En particulier, $\mathrm{disc}(q)$ est un carré modulo $4n$. □

Le théorème de Lagrange se précise quand n est un nombre premier. Rappelons que si une forme représente un nombre premier, elle le représente primitivement : si $q(x, y)$ est premier alors (x, y) est nécessairement primitif.

Théorème 3.13. *Soient $D \in \mathbb{Z}$ et p un nombre premier tels que D est un carré modulo $4p$. Alors à équivalence près, p est représenté par une unique forme de discriminant D.*

Démonstration — Soit q une forme qui représente le nombre premier p. D'après la remarque ci-dessus, q représente p primitivement. Le lemme 3.11 montre donc l'existence de $b, c \in \mathbb{Z}$ tels que $q \sim (q, b, c)$ et $0 \leq b \leq p$ (utiliser $(u, v, w) \sim (u, -v, w)$). Supposons maintenant $(p, b, c) \sim (p, b', c')$ avec $0 \leq b, b' \leq p$, et $c, c' \in \mathbb{Z}$. On va montrer $b = b'$ et $c = c'$. En prenant les discriminants on a l'égalité

$$D = b^2 - 4pc = (b')^2 - 4pc'.$$

Il suffit donc de montrer $b = b'$. On a $b^2 = (b')^2 \bmod 4p$. Les carrés de $0, 1, 2$ étant distincts modulo 8, le théorème est vrai pour $p = 2$. La relation $b^2 \equiv (b')^2 \bmod p$ entraîne $b' \equiv \pm b \bmod p$ car p est premier. Les inégalités $0 \leq b, b' \leq p$ assurent alors $b = b'$ ou $b = p - b'$. Ce dernier cas ne se produit pas si $p > 2$ car la congruence $b^2 \equiv (b')^2 \bmod 4$ entraîne $b \equiv b' \bmod 2$. □

Ces résultats justifient grandement une étude plus fine des classes d'équivalence de formes de discriminant donné, qui sera l'objet du paragraphe suivant.

Remarque 3.14. Si p est impair alors D est un carré modulo $4p$ si, et seulement si, $D \equiv 0, 1 \bmod 4$ et D est un carré modulo p. Enfin, D est un carré modulo 8 si, et seulement si, $D \equiv 0, 1, 4 \bmod 8$.

4. L'ensemble des classes de formes de discriminant donné

Constatons que si D est le discriminant d'une forme, on a la congruence

$$D \equiv 0, 1 \bmod 4.$$

Réciproquement, si $D \equiv 0, 1 \bmod 4$, alors D est le discriminant de la forme

$$\begin{cases} x^2 - \frac{D}{4}y^2, & \text{si } \ D \equiv 0 \bmod 4, \\ \\ x^2 + xy + \frac{1-D}{4}y^2, & \text{si } \ D \equiv 1 \bmod 4. \end{cases}$$

Cette forme est appelée *forme principale* de discriminant D. Il y en a bien sûr beaucoup d'autres, par exemple toutes les formes équivalentes à la forme principale, et la question restante abordée ici est de toutes les classifier à équivalence près. La forme principale se distingue par la propriété suivante.

Proposition 3.15. *Une forme représente* 1 *si, et seulement si, elle est équivalente à la forme principale de même discriminant.*

Démonstration — Il est évident que la forme principale représente 1. Réciproquement, si une forme q de discriminant D représente 1 elle le représente primitivement, et elle est donc équivalente à $(1, b, c)$ avec $b \in \{0, 1\}$ par le lemme 3.12. Cette forme est aussi de discriminant D, d'où la congruence $b \equiv D \bmod 2$. Il y a donc une seule possibilité pour b, et donc une seule pour $c = \frac{b^2-D}{4}$: c'est la forme principale. □

On fixe dorénavant un entier $D \equiv 0, 1 \bmod 4$. On conserve de plus la convention du paragraphe précédent : si $D < 0$ on ne considère que des formes positives. Le résultat suivant, dû à Lagrange, est central dans la théorie des formes.

Théorème 3.16. (Lagrange) *Soit $D \in \mathbb{Z}$. À équivalence (propre ou non) près, il n'y a qu'un nombre fini de formes de discriminant D.*

Nous supposerons que D n'est pas un carré, cas en fait beaucoup plus simple et pour lequel nous renvoyons aux exercices. Il suffit de démontrer le lemme de réduction suivant.

Lemme 3.17. (Réduction de Lagrange) *Toute forme de discriminant D non carré est proprement équivalente à une forme (a, b, c) avec $-|a| < b \leq |a| \leq |c|$. Une telle forme satisfait $1 \leq |a| \leq \sqrt{\frac{|D|}{3}}$.*

Le théorème 3.16 s'ensuit car il n'y a qu'un nombre fini de triplets (a, b, c) satisfaisant les conditions ci-dessus et la relation $b^2 - 4ac = D$. Observons en effet que si $-|a| < b < |a| \leq |c|$ et $D = b^2 - 4ac$, on a

$$4|a|^2 \leq 4|ac| = |b^2 - D| \leq |a|^2 + |D|,$$

ce qui montre aussi la seconde assertion.

Démonstration — (du lemme 3.17) Soit q une forme de discriminant D. Soit $\mathcal{V}$ l'ensemble des valeurs absolues des entiers représentés primitivement par q. Comme

D n'est pas un carré, on a $0 \notin \mathcal{V}$ d'après la proposition 3.4, et il est de plus évident que $\mathcal{V} \neq \emptyset$. Il existe donc $u \in \mathbb{Z}^2$ primitif tel que $a = q(u)$ satisfait $|a| = \mathrm{Min}\mathcal{V}$. Le lemme 3.10 assure alors qu'il existe $b, c \in \mathbb{Z}$ tels que

$$q \overset{+}{\sim} (a, b, c) \quad \text{et}, \quad -|a| < b \leq |a|.$$

Mais c est représenté primitivement par (a, b, c), et donc par q, d'où l'inégalité $|a| \leq |c|$. □

En guise de seconde démonstration du théorème ci-dessus, donnons un algorithme permettant, étant donnée une forme (a, b, c), de trouver une forme (a', b', c') qui lui est proprement équivalente et qui satisfait de plus $-|a'| < |b| \leq |a'| \leq |c|$. On suppose donc que ces inégalités ne sont pas toutes satisfaites ; nous allons définir une forme (a', b', c') qui est élémentairement proprement équivalente à (a, b, c) et telle que $|a'| + |b'| < |a| + |b|$, ce qui concluera :

- Si $|c| < |a|$ on pose $(a', b', c') = (c, -b, a)$.
- Si $|c| \geq |a|$ et $|b| > |a|$, on pose $(a', b', c') = (a, b \pm 2a, c + a \pm b)$ le signe $\pm$ étant uniformément choisi, et choisi de sorte que $|b \pm a| < |b|$. C'est possible car $a \neq 0$ (D n'est pas un carré).
- Si $|c| \geq |a|$ et $b = -|a|$ on pose $(a', b', c') = (a, \pm a, c)$.

Définition 3.18. *On désigne par* $\mathrm{Cl}(D)$ (resp. $\mathrm{P}(D)$) *l'ensemble des classes d'équivalence propre de formes (resp. de formes primitives) de discriminant D, supposées de plus positives si $D < 0$. On note enfin* $\mathrm{h}(D) = |\mathrm{P}(D)|$.

En particulier, on a $\mathrm{h}(D) = 1$ si, et seulement si, toute forme primitive de discriminant D est proprement équivalente à la forme principale. Observons que si d est le pgcd de a, b, c, alors d divise tous les entiers représentés par (a, b, c) et d^2 divise D. En particulier, si un nombre premier p est représenté par une forme non primitive de discriminant D, alors p divise D. On déduit de cela, du théorème 3.13, et de la remarque 3.14 le :

Corollaire 3.19. *Supposons* $\mathrm{h}(D) = 1$. *Alors tout nombre premier impair p tel que* $\left(\frac{D}{p}\right) = 1$ *est représenté par la forme principale de discriminant D.*

Proposition 3.20. *Si* $|D| \leq 11$ *et D n'est pas un carré alors on a* $\mathrm{h}(D) = 1$.

Comme D n'est pas un carré et $D \equiv 0, 1 \bmod 4$, l'hypothèse $|D| \leq 11$ affirme simplement que D est dans la liste $\{-11, -8, -7, -4, -3, 5, 8\}$.

Démonstration — La seconde assertion découle du théorème 3.13. Vérifions la première. Si $|D| < 12$ alors $\sqrt{\frac{|D|}{3}} < 2$. Toute forme de discriminant D est donc équivalente à une forme (a, b, c) avec $a = \pm 1$. Si $a = 1$, et en particulier si $D < 0$ par convention, une telle forme représente 1 et le corollaire découle alors de la proposition 3.15. Il ne reste donc qu'à traiter les cas $D > 0$, i.e. $D = 5, 8$, et $a = -1$.

Si $D = 5$, cela conduit aux deux formes $(1, 1, -1)$ et $(-1, 1, 1)$, qui sont en fait proprement équivalentes car $(a, b, c) \overset{+}{\sim} (c, -b, a)$ en général. Si $D = 11$, on obtient les deux formes $(1, 0, -2)$ et $(-1, 0, 2)$, qui sont aussi proprement équivalentes ! En effet, le lemme 3.7 justifie la suite d'équivalences propres suivante :

$$(-1, 0, 2) \overset{+}{\sim} (-1, -2, 1) \overset{+}{\sim} (1, 2, -1) \overset{+}{\sim} (1, 0, -2).$$

□

Notons que cela fournit une autre démonstration du théorème des deux carrés de Fermat, qui en est le cas $D = -4$. Cela montre aussi qu'un nombre premier impair p est de la forme $a^2 + ab + 3b^2$ (resp. $a^2 + ab + 2b^2$, resp. $a^2 + ab + b^2$) si, et seulement si, -11 (resp. -7, resp. -3) est un carré modulo p.

Le problème de déterminer si deux formes satisfaisant les conditions du lemme 3.17 sont équivalentes ou non est en fait sensiblement plus simple lorsque $D < 0$, et nous allons nous concentrer sur ce cas par la suite.

5. Détermination de Cl(D) lorsque le discriminant D est négatif, d'après Gauss

Définition 3.21. (Gauss) *Une forme (a, b, c) de discriminant < 0 est dite* réduite *(au sens de Gauss) si $-a < b \leq a \leq c$, et si de plus $b \geq 0$ dans le cas où $a = c$.*

Comme $(a, b, a) \overset{+}{\sim} (a, -b, a)$ (équivalence élémentaire) le lemme 3.17 entraîne que toute forme de discriminant < 0 est proprement équivalente à une forme réduite. L'algorithme du paragraphe précédent donne même une suite d'équivalences propres élémentaires permettant de passer d'une forme quelconque à une forme réduite.

Théorème 3.22. (Réduction de Gauss) *Une forme de discriminant < 0 est proprement équivalente à une unique forme réduite.*

L'existence a déjà été justifiée ci-dessus, il n'y a donc qu'à vérifier l'unicité.

Lemme 3.23. *(Les deux premières valeurs primitives d'une forme réduite) Soit $q = (a, b, c)$ une forme réduite. L'entier a est le plus petit entier (primitivement) représenté par q, de plus il y a deux cas :*

(i) Si $a < c$ alors $a = q(u)$ pour exactement 2 vecteurs $u \in \mathbb{Z}^2$, à savoir $u = \pm(1, 0)$. Dans ce cas, c est la seconde valeur représentée primitivement par q. De plus, $c = q(v)$ pour exactement 2 vecteurs primitifs $v \in \mathbb{Z}^2$, à moins que $b = a$ auquel cas il y en a 4.

(ii) Si $a = c$ alors $a = q(u)$ pour exactement 4 vecteurs primitifs $u \in \mathbb{Z}^2$, à moins que $b = a$ auquel cas il y en a 6.

Démonstration — Observons déjà que le seul vecteur $(x, y) \in \mathbb{Z}^2$ primitif tel que $y = 0$ est $\pm(1, 0)$ et qu'alors $q(\pm 1, 0) = a$. Considérons maintenant l'identité

$$4aq(x, y) = (2ax + by)^2 - Dy^2$$

pour $(x, y) \in \mathbb{Z}^2$. Si $|y| \geq 2$, on constate que $aq(x, y) \geq -D = 4ac - b^2$. Mais $b^2 \leq a^2 \leq ac$ comme q est réduite, et donc $q(x, y) \geq 3c > c$ dès que $|y| \geq 2$. Considérons donc pour finir le cas $y = \pm 1$, qui se ramène à $y = 1$. Comme $-a < b \leq a$, on a $|2ax + b| \geq |b|$ pour tout $x \in \mathbb{Z}$, avec égalité si, et seulement si, $x = 0$, ou $b = a$ et $x = -1$. Ainsi, pour tout $x \in \mathbb{Z}$,

$$q(x, 1) \geq \frac{b^2 - D}{4a} = c,$$

avec égalité si, et seulement si, $x = 0$, ou $b = a$ et $x = -1$. Le lemme en découle. □

Retournons à la démonstration de l'unicité dans le théorème 3.22. Soient $q = (a, b, c)$ et $q' = (a', b', c')$ deux formes réduites. On suppose d'abord seulement q et q' équivalentes. Comme deux formes équivalentes représentent primitivement les même valeurs, et chacune le même nombre de fois, on a $a = a'$ (même minimum). De plus, on a $c = c'$. En effet, soit a est représenté exactement deux fois auquel cas $c = c'$ est la seconde valeur primitive de q et q' d'après le lemme ci-dessus (i), soit a est représenté 4 ou 6 fois auquel cas on a $c = a = a' = c'$ d'après le (ii). En prenant le discriminant, on obtient de plus $b^2 = (b')^2$, et donc $b = \pm b'$.

Si l'on a $c = a$, l'inégalité $b, b' \geq 0$ entraîne $b = b'$. On peut donc supposer $a < c$: q et q' sont dans le cas (i) du lemme ci-dessus. On en déduit que l'on a $b = a$ si, et seulement si, $b' = a'$, et on peut donc supposer enfin que l'on a $b, b' \neq a$. Ainsi,a et c sont représentés primitivement par q et q', et ce exactement deux fois chacun, nécessairement par $\pm(1, 0)$ pour a et $\pm(0, 1)$ pour c. On a donc $q'(x, y) = q(xu+yv)$ avec $u = \pm(1, 0)$ et $v = \pm(0, 1)$. Comme $q'(x, y) = q'(-x, -y)$, on peut supposer que l'on a $u = (1, 0)$. Supposons enfin que q et q' sont *proprement* équivalentes. On a alors de plus $\det(u, v) = 1$. Cela entraîne $v = (0, 1)$, et donc $q = q'$. □

Remarque 3.24. On pourra consulter les exercices pour un point de vue plus "géométrique" sur ce résultat, basé sur l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur le demi-plan de Poincaré.

Ce résultat a de multiples applications. Il permet tout d'abord de parler de *la forme réduite* d'une classe d'équivalence propre de formes, puisque qu'elle est unique. Il donne surtout un algorithme simple pour calculer $\mathrm{Cl}(D)$ pour $D < 0$ donné : il suffit de déterminer le nombre de triplets $(a, b, c) \in \mathbb{Z}^3$ définissant une forme réduite de discriminant D. On pourra procéder comme suit : pour chaque $b \in \mathbb{Z}$ tel que $b \equiv D \bmod 2$ et tel que $|b| \leq \sqrt{\frac{-D}{3}}$ on factorisera $\frac{b^2-D}{4}$ sous la forme ac avec $|b| \leq a \leq c$.

Par exemple, nous avons vu que $\mathrm{h}(D) = 1$ si $|D| \leq 11$. D'après l'algorithme ci-dessus, nous pouvons maintenant calculer sans difficulté $\mathrm{h}(D)$ pour des petites valeurs de $|D|$.

Exemple 3.25. Prenons l'exemple $D = -20$, de sorte que $\sqrt{\frac{-D}{3}} < 3$. Les formes réduites (a, b, c) de ce discriminant satisfont donc $|b| \leq 2$ et b pair. Si $b = 0$ alors $-4ac = -20$ et donc $a = 1$ et $c = 5$: c'est la forme principale $(1, 0, 5)$. Sinon $a = 2$ et donc $b = 2$, puis $c = \frac{b^2-D}{4a} = 3 \geq a$: c'est la forme $(2, 2, 3)$. Ces deux formes sont bien réduites, et donc non proprement équivalentes d'après Gauss. On aurait pu arguer plus directement ici que $(1, 0, 5)$ et $(2, 2, 3)$ sont non équivalentes

car 2 est représenté par la seconde et non par la première. En guise d'application du théorème 3.13, on retrouve le fait que si p est premier impair, $D = -20$ est un carré modulo p (i.e. -5 est un carré modulo p), si, et seulement si, p est de la forme $x^2 + 5y^2$ ou $2x^2 + 2xy + 3y^2$, et que ces deux cas se produisent exclusivement.

D	h(D)	Formes réduites primitives
-15	2	$(1,1,4)$, $(2,1,2)$
-20	2	$(1,0,5)$, $(2,2,3)$
-23	3	$(1,1,6)$, $(2,\pm1,3)$
-24	2	$(1,0,6)$, $(2,0,3)$
-31	3	$(1,1,8)$, $(2,\pm1,4)$
-32	2	$(1,0,8)$, $(3,2,3)$
-35	2	$(1,1,9)$, $(3,1,3)$
-36	2	$(1,0,9)$, $(2,2,5)$
-39	4	$(1,1,10)$, $(2,\pm1,5)$, $(3,3,4)$
-40	2	$(1,0,10)$, $(2,0,5)$
-44	3	$(1,0,11)$, $(3,\pm2,4)$
-47	5	$(1,1,12)$, $(2,\pm1,6)$, $(3,\pm1,4)$
-48	2	$(1,0,12)$, $(3,0,4)$

TABLE 1. Formes réduites primitives de discriminant $-48 \leq D < 0$ tel que h(D) $\neq 1$

Étant donné le critère 3.19, il est naturel de se demander quels sont les $D < 0$ tels que h(D) $= 1$. Nous avons déjà vu que c'est toujours le cas si $|D| \leq 11$, on vérifie de même que :

Proposition 3.26. *On a* h(D) $= 1$ *pour tout discriminant D dans la liste suivante :*

$$\{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}.$$

DÉMONSTRATION — On peut supposer $|D| \geq 12$. Soit (a, b, c) une forme réduite d'un tel discriminant. On a $b \equiv D \bmod 2$ et $b^2 \leq a^2 \leq -D/3$. Notons que $[\sqrt{\frac{-D}{3}}]$ vaut 7 si $D = -163$, 4 si $D = -67$, 3 si $D = -43$, 2 si $D = -19$. Si $D = -19, -27, -43, -47$ et -163, on vérifie que pour tout b tel que $b^2 \leq -D/3$ et $b \equiv D \bmod 2$, le nombre $\frac{b^2-D}{4}$ est premier, ce qui force $a = 1$. Par exemple pour $D = -163$ on a $b \in \{\pm1, \pm3, \pm5, \pm7\}$ et on constate que

$$\frac{1+163}{4} = 41, \quad \frac{9+163}{4} = 43, \quad \frac{25+163}{4} = 47, \quad \text{et} \quad \frac{49+163}{4} = 53$$

qui sont tous premiers. Si $D = 12, -16, -28$, donc $b = 0, \pm2$, on constate que dans tous les cas $\frac{b^2-D}{4}$ est soit premier soit une puissance de 2, ce qui force encore $a = 1$. □

On prétend que Gauss, par examen de ses tables, avait conjecturé que les $D < 0$ tels que $\mathrm{h}(D) = 1$ sont ceux de la proposition précédente [2]. Ce problème, dit "du nombre de classes 1", a par la suite suscité une multitude de recherches en théorie des nombres. Il a été démontré 150 ans plus tard par Heegner, en 1952. Sa démonstration comportait certains points obscurs, éclaircis par Stark en 1967. Baker en a donné aussi une démonstration différente en 1966. Ces démonstrations dépassent malheureusement le cadre de ce cours.

Théorème 3.27. *(Stark, Heegner,Baker) Si $D < 0$, alors $\mathrm{h}(D) = 1$ si, et seulement si, D est l'un des treize discriminants de la proposition 3.26.*

Gauss avait aussi conjecturé $\mathrm{h}(D) \to \infty$ si $D \to -\infty$, ce qui a aussi été démontré (et bien avant le résultat ci-dessus !) par Hecke-Deuring-Heilbronn. Siegel a même démontré

$$\log \mathrm{h}(D) \underset{-D\to+\infty}{\sim} \frac{1}{2}\log(|D|).$$

Mentionnons enfin que le cas $D > 0$ est assez différent : on conjecture aussi depuis Gauss que l'on a $\mathrm{h}(D) = 1$ pour une infinité de $D > 0$, mais c'est un problème toujours ouvert.

6. Classes ambiguës de discriminant négatif

Terminons ce chapitre par une discussion sur la différence entre équivalence et équivalence propre. On définit *l'opposée de la forme* $q = (a, b, c)$ comme étant la forme de même discriminant

$$q^{\mathrm{opp}} = (a, -b, c) = q \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Bien sûr $(q^{\mathrm{opp}})^{\mathrm{opp}} = q$. Comme $\mathrm{SL}_2(\mathbb{Z})$ est distingué dans $\mathrm{GL}_2(\mathbb{Z})$, on constate que $q \overset{+}{\sim} q'$ entraîne $q^{\mathrm{opp}} \overset{+}{\sim} (q')^{\mathrm{opp}}$, de sorte que si C est une classe d'équivalence propre de formes alors $C^{\mathrm{opp}} = \{q^{\mathrm{opp}}, q \in C\}$ en est aussi une.

Lemme 3.28. *$C \mapsto C^{\mathrm{opp}}$ est une involution de $\mathrm{Cl}(D)$ dont les orbites sont exactement les classes d'équivalence de formes de discriminant D.*

Démonstration — Il est évident que l'application $C \mapsto C^{\mathrm{opp}}$ est involutive : $(C^{\mathrm{opp}})^{\mathrm{opp}} = C$. Ses orbites sont alors par définition de la forme $C \cup C^{\mathrm{opp}}$. Mais une telle partie est la classe d'équivalence toute entière de n'importe qu'elle forme de C car $\mathrm{GL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \mathrm{SL}_2(\mathbb{Z})$. □

2. Mentionnons cependant que Gauss ne considère que les discriminants $\equiv 0 \bmod 4$ dans ses Disquisitionnes, pour lequel le problème est une conséquence simple de l'analyse des formes ambiguës.

Définition 3.29. *Une forme est dite*[3] *ambiguë si elle est proprement équivalente à son opposée. Une classe $C \in \mathrm{Cl}(D)$ est dite ambiguë si $C^{\mathrm{opp}} = C$.*

Il découle de cette définition qu'une forme primitive est ambiguë si, et seulement si, sa classe d'équivalence propre est ambiguë. Le lemme élémentaire précédent montre que pour déterminer les classes d'équivalence (non propre) de formes primitives de discriminant D il suffit de déterminer les classes d'équivalence propre de discriminant D et parmi celles-ci de regrouper chaque classe non ambiguë avec son opposée. En particulier, le nombre de classes d'équivalence de formes primitives de discriminant D vaut

$$\frac{\mathrm{h}(D) + a(D)}{2}$$

où $a(D)$ désigne le nombre de classes ambiguës de $\mathrm{P}(D)$. Gauss a déterminé $a(D)$ pour tout D, mais nous nous restreindrons pour simplifier au cas où $D < 0$. Nous désignerons par $t(N)$ le nombre de diviseurs premiers distincts de l'entier N. Par exemple, $t(12) = 2$.

Théorème 3.30. (Gauss) *On suppose $D < 0$.*

(i) Une forme réduite (a, b, c) de discriminant D est ambiguë si, et seulement si, $b = 0$, $b = a$ ou $c = a$.

(ii) Il y a exactement 2^{t-1} classes ambiguës dans $\mathrm{P}(D)$ où $t = t(D)$, à moins que $D \equiv 4 \bmod 16$ (resp. $D \equiv 0 \bmod 32$) auquel cas $t = t(D) - 1$ (resp. $t = t(D) + 1$).

Démonstration — En effet, soit (a, b, c) la forme réduite d'une classe ambiguë. Elle est donc proprement équivalente à son opposée, qui est $(a, -b, c)$. Si $c > a$ et $b \neq a$ c'est encore une forme réduite, ce qui force $b = -b$ par le théorème 3.22, et donc $b = 0$. Ainsi, soit $b = a$, soit $b = 0$, soit $c = a$. Réciproquement $(a, 0, c)$ est égale à son opposée, $(a, a, c) \overset{+}{\sim} (a, a - 2a, c + a - a) = (a, -a, c)$, et $(a, b, a) \overset{+}{\sim} (a, -b, a)$, ce qui conclut le premier point.

Comme toute classe ambiguë contient une et une seule forme réduite ambiguë par le théorème 3.22, il ne reste qu'à dénombrer les formes réduites primitives décrites au (i). Constatons que $(a, b, a) \overset{+}{\sim} (a, b - 2a, 2a - b) \overset{+}{\sim} (2a - b, 2a - b, a)$, de sorte que les formes réduites (a, b, c) telles que $b = a$ ou $c = a$ sont en bijection naturelle avec les formes (a, a, c) telles que $1 \leq a \leq 2c$. Écartons enfin définitivement le cas $D = -4$ qui est trivial car $\mathrm{h}(-4) = 1$.

Soit $S(D)$ l'ensemble des couples (u, v) d'entiers positifs premiers entre eux tels que $-D = 4uv$. Cet ensemble est non vide si et seulement si $D \equiv 0 \bmod 4$, auquel cas il a exactement $|S(D)| = 2^{t(\frac{D}{4})}$ éléments (pourquoi ?). Notons que si $(u, v) \in S(D)$, alors $(v, u) \in S(D)$, et que de plus $(u, v) \neq (v, u)$ car $D \neq -4$, il y a donc exactement $\frac{|S(D)|}{2}$ formes réduites primitives du type $(a, 0, c)$.

3. On prendra garde, si l'on lit Gauss, que sa définition d'une forme ambiguë n'est pas équivalente à celle donnée ici. Pour lui, une forme (a, b, c) est dite ambiguë si $b \equiv 0 \bmod a$; par exemple (a, b, a) n'est pas en général ambiguë dans son sens mais elle l'est avec la définition ici. Par contre, les deux définitions de classe ambiguë coïncident.

Afin d'étudier le nombre des formes primitives de discriminant D du type (a, a, c) avec $1 \leq a \leq 2c$, considérons l'ensemble $T(D)$ des couples (u, v) d'entiers positifs premiers entre eux tels que $-D = u(4v - u)$. Si $D \equiv 1 \bmod 4$, on constate que toute décomposition $-D = rs$ avec r et s positifs premiers entre eux satisfait $-r \equiv s \bmod 4$ et $\mathrm{pgcd}(r, \frac{r+s}{4}) = 1$, de sorte que $|T(D)| = 2^{t(D)}$. On verifierait de même au cas par cas que : (i) si $D \equiv 4, 8 \bmod 16$, ou si $D \equiv 16 \bmod 32$, alors $T(D) = \emptyset$, (ii) si $D \equiv 12 \bmod 16$ alors $|T(D)| = 2^{t(D)-1}$, et (iii) si $D \equiv 0 \bmod 32$ alors $|T(D)| = 2^{t(D)}$.

Considérons l'involution $(u, v) \mapsto (4v - u, v)$ de $T(D)$. Elle n'a pas de point fixe car $D \neq -4$. Il en résulte qu'exactement la moitié des $(u, v) \in T(D)$ satisfont $u < 4v - u$, c'est-à-dire $u < 2v$. Comme $D \neq -4$, la forme $(2c, 2c, c)$ n'est pas primitive et donc l'ensemble des formes réduites primitives de discriminant D du type (a, a, c) ou (a, b, a) a exactement $\frac{|T(D)|}{2}$ éléments. Le nombre total de formes réduites ambiguës est donc dans tous les cas

$$a(D) = \frac{|S(D)| + |T(D)|}{2},$$

d'où l'on déduit le théorème. □

Ainsi que nous le verrons plus tard, Gauss a défini une loi de groupe abélien naturelle sur $\mathrm{P}(D)$, basée sur sa *composition des formes*. Elle s'exprime naturellement grâce à l'arithmétique des corps quadratiques, c'est pourquoi nous repoussons temporairement sa description. L'élément neutre s'avèrera être la classe d'équivalence propre de la forme principale, et C^{opp} l'inverse de la classe C. Le résultat ci-dessus s'interprêtera alors comme la détermination des éléments de carré 1 de $\mathrm{P}(D)$, en particulier $t = 1$ si, et seulement si, $\mathrm{h}(D)$ est impair !

Exemple 3.31. Soit $D = -44$. La méthode de Gauss démontre que les formes réduites de discriminant -44 sont $(1, 0, 11)$, $(2, 2, 6)$ et $(3, \pm 2, 4)$. En particulier $|\mathrm{Cl}(-44)| = 4$. La forme $(2, 2, 6)$ n'est pas primitive, de sorte que $\mathrm{h}(-44) = 3$. La forme $(1, 0, 11)$ est évidemment ambiguë, et les deux formes $(3, \pm 2, 4)$ sont opposées l'une de l'autre. À équivalence près il y a donc exactement deux formes de discriminant -44 : $(1, 0, 11)$ et $(3, 2, 4)$. On déduit du théorème 3.13 le résultat suivant, annoncé au chapitre précédent : si $p > 2$ est un nombre premier tel que $\left(\frac{-11}{p}\right) = 1$ alors p est exclusivement de la forme $x^2 + 11y^2$ ou de la forme $3x^2 + 2xy + 4y^2$, avec $x, y \in \mathbb{Z}$. Comme nous l'avions observé, il y a statistiquement $2/3$ de ces nombres premiers qui sont du second type : bien que nous ne pourrons le démontrer ici, ce phénomène est en fait relié à l'apparition des deux formes équivalentes $(3, \pm 2, 4)$ mais non proprement équivalentes.

7. Exercices

Exercice 3.1. *Montrer que tout nombre premier* $\equiv 1 \bmod 4$ *est de la forme* $5x^2 + 16xy + 13y^2$ *avec* $x, y \in \mathbb{Z}$.

Exercice 3.2. (Discriminants fondamentaux) *Soit* $D \in \mathbb{Z}$ *un entier non nul. On dit que* D *est un discriminant si c'est le discriminant d'une forme. On dit que* D *est un discriminant fondamental si de plus toute forme de discriminant* D *est primitive.*

(i) Montrer que D *est un discriminant si, et seulement si,* $D \equiv 0, 1 \bmod 4$.

(ii) Montrer que D est un discriminant fondamental si, et seulement si, :
(a) $D \equiv 1 \bmod 4$ et D est sans facteur carré,
(b) $D \equiv 0 \bmod 4$, $D/4 \equiv 2, 3 \bmod 4$, et $D/4$ est sans facteur carré.

(iii) Montrer que $|\mathrm{Cl}(D)| = \sum_{D'} \mathrm{h}(D')$ où D' parcourt les discriminant d divisant D et tels que D/d est un carré.

Exercice 3.3. *(i) Déterminer (des représentants de) $\mathrm{Cl}(-20)$ ainsi que ses classes ambiguës.*

(ii) Soit p un nombre premier impair tel que $\left(\frac{-5}{p}\right) = 1$. Montrer que p est soit de la forme $a^2 + 5b^2$, soit de la forme $2a^2 + 2ab + 3b^2$, et ce exclusivement.

(iii) (suite) Montrer que le premier cas se produit si, et seulement si, $p \equiv 1 \bmod 4$.

(iv) Donner des exemples.

Exercice 3.4. *(i) Déterminer $\mathrm{Cl}(-44)$ ainsi que ses classes ambiguës.*

(ii) Soit p un nombre premier impair tel que $\left(\frac{-11}{p}\right) = 1$. Montrer que p est soit de la forme $a^2 + 11b^2$, soit de la forme $3a^2 + 2ab + 4b^2$, et ce exclusivement.

(iii) Donner des exemples.

Exercice 3.5. *Démontrer que si p est un nombre premier tel que $\left(\frac{-84}{p}\right) = 1$ alors p est représenté par une et une seule des formes $(1, 0, 21)$, $(2, 2, 11)$, $(5, 4, 5)$ et $(3, 0, 7)$.*

Exercice 3.6. *Déterminer $\mathrm{Cl}(-56)$ ainsi que les classes ambiguës de ce discriminant. Comparer avec l'exercice 2.11.*

Exercice 3.7. *(i) On suppose $D < 0$. Trouver toutes les representations de 1 par la forme principale de discriminant D.*

(ii) En considérant les entiers $a_n, b_n \in \mathbb{Z}$ tels que $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$, montrer que $x^2 - 2y^2$ représente une infinité de fois 1 et -1.

Exercice 3.8. *Soit $\mathrm{G} \subset \mathrm{SL}_2(\mathbb{Z})$ le sous-groupe engendré par les éléments $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. On se propose de montrer que $\mathrm{G} = \mathrm{SL}_2(\mathbb{Z})$.*

(i) En utilisant l'algorithme de réduction de Lagrange, et que $\mathrm{h}(-4) = 1$, montrer que toute matrice dans $\mathrm{M}_2(\mathbb{Z})$ symétrique positive et de déterminant 1 est de la forme ${}^tPP$ où $P \in \mathrm{G}$.

(ii) Montrer que si $P \in \mathrm{SL}_2(\mathbb{Z})$ est tel que ${}^tPP = \mathrm{I}_2$ alors $P \in \mathrm{G}$.

(iii) Conclure.

Exercice 3.9. *Soit* $\mathbb{H} = \{\tau \in \mathbb{C}, \mathrm{Im}(\tau) > 0\}$ *le demi-plan de Poincaré. Si* g *désigne l'élément* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *de* $\mathrm{SL}_2(\mathbb{R})$*, et si* τ *est dans* $\mathbb{H}$*, on pose* $g \cdot \tau = \frac{a\tau+b}{c\tau+d}$*.*

(i) Montrer la relation $\mathrm{Im}\ g \cdot \tau = \frac{\mathrm{Im}\,\tau}{|c\tau+d|^2}$*.*

(ii) Vérifier que $(g, \tau) \mapsto g \cdot \tau$ *définit une action de* $\mathrm{SL}_2(\mathbb{R})$ *sur* $\mathbb{H}$*.*

(iii) Vérifier que les transformations de $\mathbb{H}$ *définies par* $\tau \mapsto \tau + 1$ *et* $\tau \mapsto -\frac{1}{\tau}$ *sont induites par des éléments de* $\mathrm{SL}_2(\mathbb{Z})$*.*

Soit D *l'ensemble des éléments* τ *de* $\mathbb{H}$ *vérifiant soit* $-\frac{1}{2} < \mathrm{Re}\,\tau \leq \frac{1}{2}$ *et* $|\tau| > 1$*, soit* $0 \leq \mathrm{Re}\,\tau \leq \frac{1}{2}$ *et* $|\tau| = 1$ *(faire un dessin).*

(iv) Montrer que pour tout $\tau \in \mathbb{H}$*, l'orbite de* τ *sous l'action de* $\mathrm{SL}_2(\mathbb{Z})$ *rencontre* D*. On pourra considérer* $g \in \mathrm{SL}_2(\mathbb{Z})$ *tel que* $\mathrm{Im}\ g \cdot \tau$ *est maximal.*

(v) Soient $\tau \in$ D *et* $g \in \mathrm{SL}_2(\mathbb{Z})$ *tels que* $g \cdot \tau \in$ D*. Vérifier que l'on a* $g \cdot \tau = \tau$*.*

(vi) En déduire que pour tout $\tau \in \mathbb{H}$*, l'orbite de* τ *sous l'action de* $\mathrm{SL}_2(\mathbb{Z})$ *rencontre un et un seul point dans* D*.*

(vii) Si $q = (a, b, c)$ *est une forme de discriminant* < 0*, montrer qu'il existe un unique* $\tau(q) \in \mathbb{H}$ *tel que* $q(x, y) = a(x - \tau(q)y)(x - \overline{\tau(q)}y)$ *pour tout* $(x, y) \in \mathbb{Z}^2$*.*

(viii) Vérifier que si $P \in \mathrm{SL}_2(\mathbb{Z})$ *et* $\mathrm{disc}\, q < 0$ *on a* $\tau(q \cdot P) = P^{-1} \cdot \tau(q)$*.*

(ix) En déduire une autre démonstration du théorème 3.22.

Exercice 3.10. (Polarisation d'une forme) *Soit* q *une forme. Si* $u, v \in \mathbb{Z}^2$ *on note* $f(u, v) \in \mathbb{Z}$ *l'unique élément tel que* $q(xu + yv) = q(u)x^2 + f(u, v)xy + q(v)y^2$*, autrement dit*

$$f(u, v) = q(u + v) - q(u) - q(v).$$

Montrer que $f : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}, (u, v) \mapsto f(u, v)$ *est une application* $\mathbb{Z}$*-bilinéaire, symétrique et paire (i.e.* $f(u, u) \in 2\mathbb{Z}\ \forall u \in \mathbb{Z}$*), qui détermine* q *en retour par la formule* $q(u) = \frac{f(u,u)}{2}$ *pour tout* $u \in \mathbb{Z}^2$*.*

Exercice 3.11. (Formes de discriminant carré)

(i) Montrer qu'une forme de discriminant k^2 *avec* $k \geq 1$ *entier est équivalente à* $(0, k, c)$ *pour un unique entier* $0 \leq c \leq k - 1$*.*

(ii) Montrer qu'une forme de discriminant 0 *est équivalente à* $(0, 0, c)$ *pour un unique entier* $c \in \mathbb{Z}$*.*

Exercice 3.12. (Groupe orthogonal d'une forme) *Si* q *est une forme, on définit son groupe orthogonal par* $\mathrm{O}(q) = \{P \in \mathrm{GL}_2(\mathbb{Z}), q \cdot P = q\}$*, ainsi que* $\mathrm{SO}(q) = \mathrm{O}(q) \cap \mathrm{SL}_2(\mathbb{Z})$*.*

(i) Vérifier que $\mathrm{O}(q)$ *est un sous-groupe de* $\mathrm{GL}_2(\mathbb{Z})$ *contenant* $\pm\mathrm{I}_2$*.*

(ii) Montrer que $\mathrm{O}(q) \neq \mathrm{SO}(q)$ *si, et seulement si,* q *est ambiguë.*

(iii) Comparer $\mathrm{O}(q)$ *et* $\mathrm{O}(q')$ *si* q *et* q' *sont équivalentes, ou si* $q' = mq$ *avec* $m \neq 0$*.*

On suppose maintenant $D = \mathrm{disc}(q) < 0$.

(iv) Montrer que $\mathrm{O}(q)$ *est discret dans* $\mathrm{M}_2(\mathbb{R})$ *et qu'il est conjugué à un sous-groupe de* $\mathrm{O}_2(\mathbb{R})$.

(v) En déduire que $\mathrm{O}(q)$ *est fini, et que si* q *est ambiguë alors* $\mathrm{O}(q)$ *est un produit semi-direct de* $\mathbb{Z}/2\mathbb{Z}$ *par son sous-groupe* $\mathrm{SO}(q)$.

(vi) Montrer que si $P \in \mathrm{SO}(q)$ *fixe un élément non nul de* $\mathbb{Z}^2$ *alors* $P = \mathrm{I}_2$.

(vii) Supposons q *primitive et réduite. Montrer que* $\mathrm{SO}(q) = \{\pm I_2\}$ *à moins que* $D = -3$ *(resp.* $D = -4$*) auquel cas il est cyclique d'ordre* 6 *(resp.* 4*).*

(viii) Décrire explicitement $\mathrm{O}(q)$ *si* q *est réduite.*

Exercice 3.13. *Soient* p *un nombre premier et* q *une forme de discriminant* $D < 0$ *représentant* p. *On se propose de déterminer l'ensemble* $R = \{u \in \mathbb{Z}^2, q(u) = p\}$ *de toutes les représentations de* p *par* q. *Soit* b *l'unique entier tel que* $b^2 \equiv D \bmod 4p$ *et* $0 \leq b \leq p$ *(justifier).*

(i) Montrer que $\forall u \in R$, *il existe un unique* $P \in \mathrm{GL}_2(\mathbb{Z})$ *tel que* $q \cdot P = (p, b, \frac{b^2-D}{4p})$ *et* $P((1,0)) = u$.

(ii) Vérifier que l'action de $\mathrm{GL}_2(\mathbb{Z})$ *sur* $\mathbb{Z}^2$ *induit une action de* $\mathrm{O}(q)$ *sur* R.

(iii) En déduire que si $u \in R$, *alors* $R = \{P(u) \mid P \in \mathrm{O}(q)\}$.

(iv) En déduire que $|R| = |\mathrm{O}(q)|$, *à moins que* q *ne soit ambiguë et qu'il existe une symétrie* $s \in \mathrm{O}(q)$ *fixant un élément de* R, *auquel cas* $|R| = |\mathrm{SO}(q)|$.

(v) (suite) Montrer que ce second cas se produit si, et seulement si, p *divise* D.