Cours d'Arithmétique M1 Paris 7
J-F. Mestre.

1 Formes quadratiques

Définitions.- *a) Une forme quadratique entière binaire est une forme quadratique de la forme* $f(x,y) = ax^2 + bxy + cy^2$*, avec* $a, b, c \in \mathbf{Z}$*. Son discriminant* D_f *est l'entier* $b^2 - 4ac$*. C'est un nombre* $\equiv 0$ *ou* $1 \mod 4$*. La forme* f *est dite* **indéfinie** *si* D_f *est* > 0*, et* **définie** *sinon.*

b) Soit D *un entier* $\equiv 0$ *ou* $1 \mod 4$*. La* **forme unité** *de discriminant* D *est* $X^2 - \frac{D}{4}Y^2$ *si* $D \equiv 0 \mod 4$ *et* $X^2 + XY + \frac{1-D}{4}Y^2$ *si* $D \equiv 1 \mod 4$*.*

c) Soit n *un entier. On dit que* f *représente* n *s'il existe* $x, y \in \mathbf{Z}$ *tels que* $f(x,y) = n$*.*

Notations.- Dans ce qui suit, on note (a,b,c) la forme quadratique $aX^2 + bXY + cY^2$, et on pose

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Si D est un entier, on note $Q(D)$ l'ensemble des formes quadratiques $f = (a,b,c)$, a, b, c premiers entre eux, avec $a > 0$ si $D < 0$, de discriminant D. D'après ce qui précède, $Q(D) \neq \emptyset \Leftrightarrow D \equiv 0$ ou $1 \mod 4$.

Proposition.- *Le groupe* $\mathbf{GL}_2(\mathbf{Z})$ *agit à droite sur* $Q(D)$ *par* $(f^M)(x,y) = f(M \begin{pmatrix} x \\ y \end{pmatrix})$.

Remarques.- 1) Comme $\{\pm I\}$ agit trivialement sur $Q(D)$, l'action ci-dessus se factorise à travers $\mathbf{PGL}_2(\mathbf{Z})$.

2) Si $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, et si $f = (a,b,c)$, on a $f^M = (A,B,C)$, où $A = f(\alpha,\gamma)$ et $C = f(\beta,\delta)$.

3) Si f représente un entier n, toute forme g dans la même orbite que f sous l'action de $\mathbf{GL}_2(\mathbf{Z})$ représente également n. Plus précisément, si $f(x,y) = n$, on a $f^M(M^{-1}(\begin{smallmatrix} x \\ y \end{smallmatrix})) = n$.

4) On a $(a,b,c)^T = (a, b+2a, a+b+c)$, $(a,b,c)^S = (c, -b, a)$.

5) Attention: (a,b,c) et $(a,-b,c)$ sont conjuguées modulo $\mathbf{GL}_2(\mathbf{Z})$ (via la matrice $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$) mais en général ne le sont pas modulo $\mathbf{SL}_2(\mathbf{Z})$.

Néanmoins, (a,a,c) et $(a,-a,c)$ sont conjuguées modulo $\mathbf{SL}_2(\mathbf{Z})$ (via T^{-1}), ainsi que (a,b,a) et $(a,-b,a)$ (via S).

6) si $D < 0$, et si $f = (a,b,c)$ avec $a > 0$, pour tout $M \in \mathbf{GL}_2(\mathbf{Z})$, $f^M = (a', b', c')$, avec $a' > 0$. Ceci n'est plus vrai si $D > 0$.

7) D_f est l'opposé du déterminant de la matrice $A_f = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$ associée à la forme bilinéaire symétrique ϕ_f telle que $\phi_f(v,v) = 2f(v)$.

Proposition.- *Soit* n *un entier sans facteur carré représenté par* f *forme binaire entière. Il existe* $M \in \mathbf{SL}_2(\mathbf{Z})$ *telle que* $f^M = (n, *, *)$*.*

Si $n = f(x,y)$, comme n est sans facteur carré, x et y sont premiers entre eux, d'où d'après Bezout une matrice $M = \begin{pmatrix} x & * \\ y & * \end{pmatrix}$ dans $\mathbf{SL}_2(\mathbf{Z})$; D'après ce qui précède, $g = f^M = (n, *, *)$.

Proposition.- *Soit $D \equiv 0$ ou $1 \mod 4$, et p un nombre premier impair premier à D. Alors $\left(\frac{D}{p}\right) = 1$ si et seulement s'il existe $f \in Q(D)$ représentant p.*

S'il existe $f \in Q(D)$ représentant p, il existe $g \in Q(D)$ telle que $g = (p, b, c)$; donc $D = b^2 - 4pc$, et D est un carré non nul $\mod p$. Réciproquement, si $D = u^2 - kp$, quitte à changer u en $u + p$, on peut supposer que k est pair, donc $\equiv 0 \mod 4$. La forme $(p, u, k/4)$ est dans $Q(D)$ et représente p.

Proposition.- *Soit f et g dans $Q(D)$ représentant un nombre premier p impair premier à D. Alors f et g sont conjuguées modulo $\mathbf{GL}_2(\mathbf{Z})$. Si $g = (a, b, c)$, g ou $(a, -b, c)$ est conjuguée à f modulo $\mathbf{SL}_2(\mathbf{Z})$.*

On peut supposer $g = (p, b, c)$ et $f = (p, b', c')$. Par suite, $b^2 - 4pc = b'^2 - 4pc'$, soit $4p(c' - c) = (b' - b)(b' + b)$. Donc b et b' ont même parité, et par exemple $b \equiv b' \mod p$; donc $b' = b + 2kp$; les formes g^{T^k} et f ont les mêmes deux premiers coefficients, donc elles sont égales, et f et g sont congrues modulo $\mathbf{SL}_2(\mathbf{Z})$. Si on a $b \equiv -b' \mod p$, on en déduit de même que f et $(p, -b, c)$ sont congrues modulo $\mathbf{SL}_2(\mathbf{Z})$.

Notation.- On note $H(D)$ l'ensemble des orbites des éléments de $Q(D)$ sous l'action de $\mathbf{SL}_2(\mathbf{Z})$.

Définition.- *On suppose $D < 0$; une forme $f \in Q(D)$ est dite* **réduite** *si $|b| \leq a \leq c$.*

Proposition.- *Soit $f(x, y) = ax^2 + bxy + cy^2$ une forme quadratique définie réduite. Alors:*
1) $a = \inf f(x, y)$,
2) $ac = \inf f(x, y) f(z, t)$, avec $xt - yz \neq 0$,
3) Si $|b| < a < c$, pour tous (x, y) tels que $xy \neq 0$, on a $f(x, y) > c$. De plus, on a $f^M = f$ si et seulement si $M = \pm I$.

On a $f(x, 0) = x^2 a$, $f(0, y) = y^2 c$, et, pour $xy \neq 0$,

$$f(x, y) \geq ax^2 - |b||x||y| + cy^2 \geq ax^2 - |b||x||y| + cy^2 - a(|x| - |y|)^2 \geq (2a - |b|)|x||y| + (c - a)y^2 \geq a - |b| + c.$$

Théorème.- *Soit $D < 0$ et $D \equiv 0$ ou $1 \mod 4$.*
1) $H(D)$ est fini non vide. Son nombre d'éléments $h(D)$ est appelé le nombre de classes de D.
2) Tout élément de $H(D)$ contient une forme quadratique réduite. Plus précisément, pour toute forme quadratique Q de discriminant D, il existe un élément g dans le groupe engendré par S et T tel que Q^g soit réduite.
3) Soient $f = (a, b, c)$ et g deux formes quadratiques de $Q(D)$ distinctes et réduites. Elles sont équivalentes modulo $\mathbf{SL}_2(\mathbf{Z})$ si et seulement l'une des inégalités $|b| \leq a \leq b$ est une égalité. On a alors $g = (a, -b, c)$.

On montre d'abord 2), par utilisations successives de S et T: si $|a| > |c|$, on utilise T, si $|b| > |a|$, on ramène par une puissance convenable de T (a, b, c) à $(a, b', *)$, avec $|b'| \leq |a|$. La suite des b est décroissante, donc stationnaire. Pour démontrer 1), il suffit donc de montrer que le nombre de formes réduites est fini.
Soit $f = (a, b, c)$ réduite.
On a $|b| \leq a \leq c$, donc $|D| = 4ac - b^2 \geq 3b^2$, et $|b| \leq \sqrt{\frac{|D|}{3}}$. Il y a donc un nombre fini de valeurs de b possibles; comme $4ac = b^2 - D$, on a donc pour chaque valeur de b un nombre fini de valeurs possibles pour (a, c), et $H(D)$ est fini.
Le point 3) se déduit immédiatement de la proposition précédente.

Théorème.- *Le groupe $\mathbf{SL}_2(\mathbf{Z})$ est engendré par S et T.*
Notons H le sous-groupe de $\mathbf{SL}_2(\mathbf{Z})$ engendré par S et T. Soit $Q(x, y) = x^2 + 4y^2$, $g \in \mathbf{SL}_2(\mathbf{Z})$, et $Q' = Q^g$. Il existe $h \in H$ tel que Q'^h est réduite, donc, d'après le théorème précédent, $Q'^h = Q$, soit $Q^{gh} = Q$. On a donc $gh = \pm I$. Or $-I = S^2$, d'où le résultat.

1.1 Corollaires

Proposition.- *Soit D tel que $h(D) = 1$, et p un nombre premier impair premier à D; les trois assertions suivantes sont équivalentes:*

i) p est représentable par toute forme de discriminant D,

ii) p est représentable par la forme unité de $Q(D)$,

iii) D est un carré $\bmod p$.

Lemme.- Soit $D \equiv 1 \mod 4$ négatif; on a $(\frac{D}{p}) = (-1)^{\varepsilon(p)}(\frac{|D|}{p}) = (\frac{p}{|D|})$.

Exemple 1.- Soit $D = -4$; les formes quadratiques réduites de $Q(-4)$ vérifient

$$\begin{cases} |b| \leq \sqrt{4/3} \\ b \equiv 0 \mod 2 \\ 4ac = 4 + b^2 \end{cases},$$

d'où $b = 0$, $a = c = 1$. Donc $H(-4) = \{x^2 + y^2\}$. On retrouve le fait que $p \equiv 1 \mod 4$ ssi p est somme de deux carrés.

Exemple 2.- On vérifie de même que $h(-3) = 1$. Donc un nombre premier impair $p \neq 3$ s'écrit $x^2 + xy + y^2$ si et seulement si $p \equiv 1 \mod 3$.

Exemple 3.- De même, $h(-7) = 1$; donc p impair différent de 7 s'écrit $x^2 + xy + 2y^2$ ssi $p \equiv 1, 2, 4 \mod 7$.

Exemple 4.- On vérifie encore que $h(-8) = 1$. Or

$$(\frac{-8}{p}) = (\frac{-1}{p})(\frac{2}{p}) = (-1)^{\varepsilon(p)}(-1)^{\omega(p)}.$$

Donc $(\frac{D}{p}) = 1$ si et seulement si $(-1)^{\varepsilon(p)} = (-1)^{\omega(p)}$, soit ssi $p \equiv 1$ ou $3 \mod 8$. Par suite, un nombre premier impair p est de la forme $x^2 + 2y^2$ si et seulement si il est congru à 1 ou $3 \mod 8$.

Problématique générale.- Soit f une forme quadratique entière. Peut-on déterminer quels nombres premiers p elle représente par des congruences sur p? Par exemple, si $f = x^2 + y^2$, f représente p impair ssi $p \equiv 1 \mod 4$.

Lemme: $d < 0$, $d \equiv 1 \mod 4$; on a $(D/p) = 1$ ssi $(p/|D|) = 1$.

Proposition.- *Soit f quadratique binaire entière de discriminant $d < 0$. Si $h(d) = 1$, les nombres premiers représentant p sont donnés en terme de congruence $\bmod d$ (par exemple, si d est impair, ssi $(p/|d|) = 1$; si d est pair, la loi de réciprocité quadratique permet également de déterminer les dites congruences.)*

En particulier, via Dirichlet, **si f est de discriminant d et si $h(d) = 1$, il existe une infinité de nombres premiers représentés par f.**

Même si $h(d) \neq 1$, il peut encore arriver que l'on puisse classifier p en termes de congruence: par exemple, soit $d = -15$; soit $f_1 = x^2 + xy + 4y^2$ et $f_2 = 2x^2 + xy + 2y^2$ les deux formes quadratiques réduites de discriminant -15. On vérifie facilement que les nombres premiers p (premiers à 30) représentés par f_1 sont ceux $\equiv 1$ ou $4 \mod 15$ et ceux représentés par f_2 sont ceux $\equiv 2$ ou $8 \mod 15$.

Ici encore, via Dirichlet, on en déduit qu'il existe une infinité de p représentés par f_1 (resp. par f_2).

Néanmoins, en général, les p représentés par une forme quadratique f ne peuvent pas être décrits en termes de congruence modulo le discriminant de f. Par exemple, si $d = -23$, on peut montrer que pour tout x carré $\bmod 23$, il existe des $p \equiv x \mod 23$ représentés par n'importe laquelle des trois formes réduites de discriminant -23.

(Il reste vrai qu'une telle forme quadratique représente une infinité de nombres premiers, mais c'est plus difficile (conséquence par exemple du théorème de Cebotarev).)

Théorème (admis pour l'implication directe) Baker, Heegner-Stark: *on a $h(d) = 1$ ssi*

$d = -3, -4, -7, -8, -11, -19, -47, -67, -163$ *et aussi* $d = -12, -27, -16, -28$.

Lemme.- *Si p est représenté par la forme quadratique unité de discriminant d, et si $(p, d) = 1$, on a $p \geq (|d| + 1)/4$ si d est impair et $p \geq (1 + |d|/4)$ si $d \equiv 0 \mod 4$.*

Corollaire.- *Si $h(D) = 1$, et si $(D/p) = 1$, alors $p \geq (|D| + 1)/4$.*

Théorème (polynômes d'Euler).- *Soit $f(x) = x^2+x+a$, $a \geq 3$, $a \neq 7$;$f(x)$ est premier pour $0 \leq x \leq a-2$ ssi $h(1 - 4a) = 1$.*

Par exemple, $x^2 + x + 41$ est un nombre premier pour $-1 \leq x \leq 39$.