Premiers de la forme $x^2 + ny^2$

Remarque : en vue de généraliser l'énoncé de descente, on est amené à considérer les formes quadratiques de discriminant fixé. Pour se ramener à un nombre fini, Lagrange a introduit la notion de forme quadratique réduite, notion qui ne concerne que les formes quadratiques définies positives, cas auquel on se restreindra dans la suite.

Définition 0.1. — Une forme quadratique primitive définie positive $ax^2+bxy+cy^2$ est dite *réduite* si

$$|b| \leq a \leq c, \text{ et } b \geq 0 \text{ si } |b| = a \text{ ou } a = c.$$

Remarque : $x^2 + ny^2$ est une forme réduite de discriminant $-4n$. Plus généralement pour $D \equiv 0 \mod 4$ (resp. $D \equiv 1 \mod 4$), la forme $x^2 - \frac{D}{4}y^2$ (resp. $x^2+xy+\frac{1-D}{4}y^2$) est une forme réduite de discriminant D que l'on appelle **la forme principale** de discriminant D.

Théorème 0.2. — *Toute forme quadratique primitive définie positive est proprement équivalente à une unique forme réduite.*

Preuve : Soit $\tau_f = \frac{-b+i\sqrt{D}}{2a}$ l'élément du demi-plan de Poincaré $\mathcal{H}$ associé à f. On vérifie alors que pour $g = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$, $\tau_{g.f} = g.\tau_f$ où on rappelle que l'action de g sur $\mathcal{H}$ est donnée par la formule $g.z = \frac{pz+q}{rz+s}$. Ainsi deux formes quadratiques f, g sont proprement équivalente si et seulement si τ_f et τ_g sont dans la même classe dans $\mathcal{H}/SL_2(\mathbb{Z})$. D'après l'exercice **??**, un domaine fondamental de $\mathcal{H}/SL_2(\mathbb{Z})$ est donné par l'intérieur du domaine $-1/2 \leq \mathrm{Re}\,(z) \leq 1/2$ et $|z| \geq 1$ ce qui donne en regardant : la partie réelle, $|b| \leq a$, et le module, $b^2 - D \geq 4a^2$. Si on est sur le bord du domaine, $|\mathrm{Re}\, z| = 1/2$ soit $|b| = a$, on prend le bord gauche i.e. $\mathrm{Re}\, z = -1/2$ et donc $b = a$; sur $|z| = 1$, on prend de même le bout du cercle de gauche, i.e. $\mathrm{Re}\, z \leq 0$ et donc $b \geq 0$.
Remarque : si $f(x, y) = ax^2 + bxy + cy^2$ est une forme réduite de discriminant D alors $-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$ et donc $|a| \leq \sqrt{-D/3}$ ce qui donne un nombre fini de couples (a, b) et donc aussi de triplets (a, b, c). Ainsi pour $D < 0$, on notera $h(D)$ **le nombre de formes quadratiques primitives positives définies réduites de discriminant** D.

Théorème 0.3. — *(**Landau** cf.* [**1**] *p.31) Pour $n \in \mathbb{N}$, on a*

$$h(-4n) = 1 \Leftrightarrow n = 1, 2, 3, 4, 7.$$

Preuve : Pour $n = 1, 2, 3, 4, 7$, on regarde pour tout $0 \leq a \leq \sqrt{4n/3}$ et $|b| \leq a$ si $(b^2+4n)/4a$ appartient à $\mathbb{Z}$ et on vérifie que les seules solutions sont x^2+ny^2. Pour $n \notin \{1, 2, 3, 4, 7\}$, l'idée est de construire une forme réduite de discriminant $-4n$ distincte de $x^2 + ny^2$ de sorte que $h(-4n) > 1$.

Supposons que n n'est pas la puissance d'un nombre premier, i.e. $n = ac$ avec $1 < a < c$ et $a \wedge c = 1$; la forme $ax^2 + cy^2$ est alors réduite de discriminant $-4ac = -4n$.

Pour $n = 2^r$ et $r \geq 4$, alors $4x^2+4xy+(2^{r-2}+1)y^2$ est primitive, réduite et de discriminant $4^2 - 4.4(2^{r-2} + 1) = -16.2^{r-2} = -4n$. Pour $n = 8$, on calcule $h(-32) = 2$.

Pour $n = p^r$ avec p premier impair. Si on a $n + 1 = ac$ avec $1 < a < c$ et $a \wedge c = 1 =$: $ax^2 + 2xy + cy^2$ est réduite de discriminant $2^2 - 4ac = 4 - 4(n + 1) = -4n$. Comme $n + 1$ est pair, il reste alors à considérer le cas $n + 1 = 2^s$: si $s \geq 6$ alors $8x^2 + 6xy + (2^{s-3} + 1)y^2$

est primitive réduite de discriminant $-4n$. Reste alors à traiter les cas de $n = 15$ et 31 : 15 n'étant pas premier, il a déjà été traité et pour $n = 31$, on calcule $h(-4.31) = 3$.
Remarque : ainsi pour $n = 7$, l'étape de descente du début est vraie de sorte que l'on obtient

$$p = x^2 + 7y^2 \Leftrightarrow (\frac{-n}{7}) = 1 \Leftrightarrow p \equiv 1, 9, 11, 15, 23, 25 \mod 28.$$

Pour avancer sur les autres cas, Lagrange a introduit la notion suivante.

Définition 0.4. — Deux formes quadratiques primitives définies positives de discriminant D sont dites de même genre si elles représentent les mêmes valeurs dans $(\mathbb{Z}/D\mathbb{Z})^\times$.

Exemples : pour $D = -20$, $x^2 + 5y^2$ représente $1, 9 \in (\mathbb{Z}/20\mathbb{Z})^\times$ et $2x^2 + 2xy + 3y^2$ représente $3, 7 \in (\mathbb{Z}/20\mathbb{Z})^\times$. Pour $D = -56$, on a

$$\begin{array}{rll} x^2 + 14y^2,\ 2x^2 + 7y^2 & \text{représentent} & 1, 9, 14, 23, 25, 29 \in (\mathbb{Z}/56\mathbb{Z})^\times \\ 3x^2 \pm 2xy + 5y^2 & \text{représentent} & 3, 5, 13, 19, 27, 45 \in (\mathbb{Z}/56\mathbb{Z})^\times \end{array}$$

On observe donc que les genres ne sont pas forcément réduit à un élément. Cependant il semble que les valeurs représentées forment des ensembles disjoints ce qui est confirmé par la proposition suivante.

Proposition 0.5. — *Soit $D < 0$ tel que $D \equiv 0, 1 \mod 4$. On note $\chi : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ l'homomorphisme défini par le symbole de Jacobi cf.* **??**, *i.e. $\chi(\bar{n}) = (\frac{D}{n})$ où $n \in \bar{n}$ est impair* [(1)].

(i) Les valeurs de $(\mathbb{Z}/D\mathbb{Z})^\times$ représentées par la forme principale de discriminant D est un sous groupe $H \subset \operatorname{Ker} \chi$.

(ii) Les valeurs de $(\mathbb{Z}/D\mathbb{Z})^\times$ représentées par une forme primitive définie positive de discriminant D forment une classe dans $\operatorname{Ker} \chi / H$.

Preuve : Soit m premier à D qui est représenté par une forme $f(x, y)$ de discriminant D : montrons que $\bar{m} \in \operatorname{Ker} \chi$. On a $m = d^2 m'$ où m' est proprement représentée par $f(x, y)$. On a $\chi(m) = \chi(m')$ et d'après **??**, D est un résidu quadratique modulo m, i.e. $D = b^2 - km$. Si m est impair alors d'après les propriétés élémentaires du symbole de Jacobi on a $\chi(m) = (\frac{D}{m}) = (\frac{b^2}{m}) = 1$. Si m est pair alors d'après **??**, on a $D \equiv 1 \mod 8$ de sorte que $\chi(\bar{2}) = 1$ et on se ramène aisément au cas impair.

(i) D'après ce qui précède $H \subset \operatorname{Ker} \chi$; pour $D = -4n$ l'identité remarquable

$$(cx - ndy)^2 + n(dx + cy)^2 = (x^2 + ny^2)(c^2 + nd^2)$$

montre que H est un sous-groupe. Pour $D \equiv 1 \mod 4$, l'argument est différent : l'égalité

$$4\big(x^2 + xy + \frac{1 - D}{4} y^2\big) \equiv (2x + y)^2 \mod D$$

montre que H est le sous-groupe des carrés de $(\mathbb{Z}/D\mathbb{Z})^\times$.

(ii) Commençons par prouver le lemme suivant :

Lemme 0.6. — *Soit $f(x, y)$ une forme quadratique et M un entier alors $f(x, y)$ représente proprement un nombre premier à M.*

[(1)] Le point essentiel est de voir que le symbole de Jacobi ne dépend que de la classe modulo D

Preuve : Soit $f(x,y) = ax^2 + bxy + cy^2$; on a $f(1,0) = a$, $f(0,1) = c$ et $f(1,1) = a+b+c$ de sorte que comme a, b, c sont premiers entre eux, pour tout p premier, il existe $x \wedge y = 1$ tels que $f(x,y)$ est premier à p. Le résultat découle alors simplement d'une application du théorème chinois.

Supposons $D = -4n$, d'après le lemme précédent pour $M = 4n$ et **??**, on peut supposer que $f(x,y) = ax^2 + bxy + cy^2$ avec a premier à $4n$; $f(x,y)$ étant de discriminant $-4n$, b est pair et s'écrit $2b'$ et donc

$$af(x,y) = (ax + b'y)^2 + ny^2.$$

Comme a est premier à $4n$, les valeurs prises par $f(x,y)$ appartiennent à $\bar{a}^{-1}H$: réciproquement si $\bar{c} \in \bar{a}^{-1}H$ alors $ac \equiv z^2 + nw^2 \mod 4n$. En posant $y = w$ et $ax + b'y = z$, on a $f(x,y) \equiv c \mod 4n$ de sorte que les valeurs prises sont exactement $\bar{a}^{-1}H$.

Si $D \equiv 1 \mod 4$, on écrit $f(x,y) = ax^2 + bxy + cy^2$ avec $a \wedge D = 1$ sous la forme $4af(x,y) = (2ax + by)^2 - Dy^2 \equiv (2ax + by)^2 \mod D$ et comme $4a$ est premier à D, les valeurs prises par $f(x,y)$ sont dans $(\overline{4a})^{-1}H$ où on rappelle que H est le sous-groupe des carrés de $(\mathbb{Z}/D\mathbb{Z})^\times$. L'inclusion réciproque se montre aisément comme précédemment.
Remarque : ainsi pour H' une classe dans $\operatorname{Ker}\chi/H$, le genre de H' est l'ensemble des formes quadratiques réduites de discriminant D dont les valeurs représentées sont $H' \subset \operatorname{Ker}\chi \subset (\mathbb{Z}/D\mathbb{Z})^\times$.
Remarque : si le genre de la forme principale est réduit à un seul élément, l'étape de descente se résoud alors simplement en terme de congruences. On a déjà vu que c'était le cas pour $n = 5$ et on peut montrer que ce cas favorable se produit pour $n = 6, 10, 13, 15, 21, 22, 30$, ce qui donne les résultats suivants :

$$\begin{array}{rcl}
p = x^2 + 5y^2 & \Leftrightarrow & p \equiv 1, 9 \mod 20 \\
p = x^2 + 6y^2 & \Leftrightarrow & p \equiv 1, 7 \mod 24 \\
p = x^2 + 10y^2 & \Leftrightarrow & p \equiv 1, 9, 11, 19 \mod 40 \\
p = x^2 + 13y^2 & \Leftrightarrow & p \equiv 1, 9, 17, 25, 29, 49 \mod 52 \\
p = x^2 + 15y^2 & \Leftrightarrow & p \equiv 1, 19, 31, 49 \mod 60 \\
p = x^2 + 21y^2 & \Leftrightarrow & p \equiv 1, 25, 37 \mod 84 \\
p = x^2 + 22y^2 & \Leftrightarrow & p \equiv 1, 9, 15, 23, 25, 31, 47, 49, 71, 81 \mod 88 \\
p = x^2 + 30y^2 & \Leftrightarrow & p \equiv 1, 31, 49, 79 \mod 120
\end{array}$$

Les questions en suspens sont alors de savoir caractériser tous les n pour lesquels le genre de la forme principale est réduite à un élément puis de trouver une nouvelle idée pour traiter les autres cas.

Références

[1] D. Cox. *Primes of the form $x^2 + ny^2$*. Pure and applied mathematics. 1989.