Caractères de Kronecker et évaluations de formes quadratiques

Lemme 12.
• *Soit q une forme* **primitive** *et m un entier* **non nul** *; il existe (x, y) de la forme $(1, y)$ ou $(x, 1)$ tel que $q(x, y)$ soit premier à m. En particulier, il existe un entier premier à m proprement représenté par q.*
• *Si m est premier à un discriminant quadratique Δ, alors toute forme de discriminant Δ représentant m est primitive.*

Preuve.
• Soient a, b, c les coefficients de q ; on va montrer qu'il existe $u \in \mathbb{Z}$ tel que l'un des deux polynômes aX^2+bX+c ou $a+bX+cX^2$ prend en u une valeur non nulle modulo p pour tout premier p divisant m : il s'en suivra que $q(u, 1)$ ou $q(1, u)$ est inversible modulo m. Désignons par f un quelconque de ces deux polynômes ; f n'est pas nul dans $\mathbb{F}_p[X]$ (sinon p diviserait a, b, c contredisant le fait que q est primitive), de degré ≤ 2 donc il admet au plus deux racines dans $\mathbb{F}_p$. Si $p > 2$, il existe donc $u_p \in \mathbb{Z}$ tel que $f(u_p) \not\equiv 0 \pmod p$. Reste à examiner le cas $p = 2$; si $aX^2 + bX + c$ s'annule sur $\mathbb{F}_2$, on a nécessairement $aX^2 + bX + c \bmod 2 = X(X + 1)$; dans ce cas, $a + bX + cX^2 \bmod 2 = 1 + X$ prend une valeur non nulle sur $\mathbb{F}_2$; dans tous les cas, pour l'un des deux polynômes f, il existe $u_2 \in \mathbb{Z}$ tel que $f(u_2) \not\equiv 0 \pmod 2$. Le théorème chinois fournit l'existence d'un $u \in \mathbb{Z}$ tel que $f(u) \not\equiv 0 \pmod p$ pour tout $p \mid m$.
• On a $m = ax^2 + bxy + cy^2$ avec $b^2 - 4ac = \Delta$; si d est un diviseur commun à a, b, c, il divise m et Δ, donc $d = \pm 1$. □

A plusieurs reprises, nous allons utiliser le fait que pour tous $x, y \in \mathbb{Z}$:

$$(\heartsuit) \qquad \chi_{-4}(x^2+y^2) \in \{0,1\}, \qquad \chi_8(x^2-2y^2) \in \{0,1\}, \qquad \chi_{-8}(x^2+2y^2) \in \{0,1\}$$

ou encore, de manière uniforme pour $D \in \{-4, \pm 8\}$, en faisant intervenir la forme quadratique $x^2 - \frac{D}{4}y^2$ de discriminant D :

$$\chi_D\Big(x^2 - \frac{D}{4}y^2\Big) \in \{0,1\}$$

Definition 2 (du signe $\chi_{D_i}(q)$)**.**
Soit D un discriminant quadratique fondamental (positif ou négatif) et $D = D_1 \cdots D_k$ sa décomposition en discriminants quadratiques fondamentaux élémentaires premiers deux à deux. Pour une forme quadratique $q(x, y) = ax^2 + bxy + cy^2$ de discriminant D, on définit $\chi_{D_i}(q) \in \{\pm 1\}$ par :

$$\boxed{\chi_{D_i}(q) = \begin{cases} \chi_{D_i}(a) & \text{si } a \wedge D_i = 1 \\ \chi_{D_i}(c) & \text{si } c \wedge D_i = 1 \end{cases}}$$

En particulier, pour la forme neutre q_0 :

$$\chi_{D_i}(q_0) = 1$$

Justifions la validité de cette définition. Montrons tout d'abord que $\chi_{D_i}(ac) \in \{0, 1\}$. Puisque $4ac \equiv b^2 \bmod D$, c'est immédiat si D_i est impair. Si $D_i \in \{-4, \pm 8\}$, b est pair, $b = 2b'$, et en écrivant $D = D_i D'$ avec $D' \equiv 1 \bmod 4$, on a

$$ac = b'^2 - \frac{D_i}{4}D' \equiv \begin{cases} b'^2 + 1 \bmod 4 & \text{si } D_i = -4 \\ b'^2 - 2 \bmod 8 & \text{si } D_i = 8 \\ b'^2 + 2 \bmod 8 & \text{si } D_i = -8 \end{cases}$$

d'où $\chi_{D_i}(ac) \in \{0, 1\}$ d'après $(\heartsuit)$.
De ce résultat $\chi_{D_i}(ac) \in \{0, 1\}$, on en déduit, lorsque $a \wedge D_i = c \wedge D_i = 1$, que $\chi_{D_i}(a) = \chi_{D_i}(c)$ et donc que la définition encadrée a du sens dans ce cas là.
Enfin, l'une des deux alternatives $a \wedge D_i = 1$ ou $c \wedge D_i = 1$ se produit toujours. En effet, D_i est d'une part un diviseur de $D = b^2 - 4ac$, et d'autre part, au signe près, soit un nombre premier p soit une puissance de $p = 2$; l'éventualité $a \wedge D_i \neq 1$ et $c \wedge D_i \neq 1$ conduirait alors à ce que p divise a, b, c, contredisant le caractère primitif de (a, b, c).

Lemme 13.
Dans le contexte de la définition précédente, on a :

$$\chi_{D_i}(q)\ \chi_{D_i}(q(x, y)) \in \{0, 1\}$$

En particulier, pour toute évaluation $q(x, y)$ **première à** *D_i :*

$$\chi_{D_i}(q(x, y)) = \chi_{D_i}(q)$$

Preuve.
Tout repose sur (♡) et surtout sur l'égalité :

$$(\star) \qquad a(ax^2+bxy+cy^2) = \Big(ax+\frac{b}{2}y\Big)^2 - \frac{b^2-4ac}{4}y^2 = \Big(ax+\frac{b}{2}y\Big)^2 - \frac{D}{4}y^2$$

On distingue les deux cas suivants :
• $D \equiv 1 \bmod 4$. En multipliant par 4 l'égalité $(\star)$ et en notant $z = 2ax+by$:

$$4aq(x,y) = z^2 - Dy^2 \equiv z^2 \bmod D$$

En conséquence $\chi_{D_i}(a)\ \chi_{D_i}(q(x,y)) \in \{0,1\}$. Idem avec c à la place de q d'où le résultat.
• $D \equiv 0 \bmod 4$. Dans ce cas, b est pair et $(\star)$ peut s'écrire, en notant $z = ax+\frac{b}{2}y$:

$$aq(x,y) = z^2 - \frac{D}{4}y^2$$

ce qui conduit, en écrivant $D = D_iD'$ avec $D' \equiv 1 \bmod 4$, à :

$$aq(x,y) \equiv \begin{cases} z^2 \bmod D_i & \text{si } D_i \notin \{-4, \pm 8\} \\ z^2+y^2 \bmod D_i & \text{si } D_i = -4 \\ z^2-2y^2 \bmod D_i & \text{si } D_i = 8 \\ z^2+2y^2 \bmod D_i & \text{si } D_i = -8 \end{cases}$$

Dans tous les cas, on a $\chi_{D_i}(a)\ \chi_{D_i}(q(x,y)) \in \{0,1\}$. Idem avec c à la place de q d'où le résultat. □

Théorème 4.
Soit D un discriminant quadratique fondamental (positif ou négatif) et $D = D_1 \cdots D_k$ sa décomposition en discriminants quadratiques fondamentaux élémentaires premiers deux à deux.

(i) Pour toute forme quadratique binaire $q(x,y) = ax^2+bxy+cy^2$ de discriminant D, il existe une valeur $q(x,y)$ première à D.

(ii) Tout couple (D_i, q) où q est une forme quadratique de discriminant D, détermine un signe

$$\chi_{D_i}(q) \in \{\pm 1\}$$

tel que :

$$\chi_{D_i}(q(x,y)) = \chi_{D_i}(q) \qquad \text{pour n'importe quelle valeur } q(x,y) \text{ première à } D_i$$

(iii) Pour toute forme quadratique q de discriminant D, on a :

$$\chi_D(q) \overset{\text{def}}{=} \chi_{D_1}(q) \cdots \chi_{D_k}(q) = 1$$

Preuve.
(i) Toute forme quadratique dont le discriminant est un discriminant quadratique fondamental est primitive. On peut alors appliquer le lemme (12) à $m = D$.
(ii) Lemme précédent.
(iii) Soit donc $m = q(x,y)$ premier à D ; il faut démontrer que $\chi_D(m) = 1$. Soit $d = \gcd(x,y)$ et $x = dx'$, $y = dy'$ avec $x' \wedge y' = 1$. On a alors $m = d^2m'$ avec $m' = q(x',y')$ et donc $\chi_D(m) = \chi_D(m')$. Il faut donc montrer que $\chi_D(m') = 1$ et il suffit de montrer que $\chi_D(p) = 1$ pour tout diviseur premier p de m' (si $m' = 1$, c'est évident).
Et cette fois, l'avantage de m' sur m c'est que m' est proprement représenté par q en (x',y') ; ceci permet de définir $\varphi \in \mathrm{SL}_2(\mathbb{Z})$ par :

$$\varphi = \begin{bmatrix} x' & u \\ y' & v \end{bmatrix} \quad \text{où } u,v \text{ sont tels que} \quad \begin{vmatrix} x' & u \\ y' & v \end{vmatrix} = 1$$

La forme forme quadratique $q \circ \varphi$ est de discriminant D et son coefficient en x^2 i.e. $(q \circ \varphi)(e_1)$ est $q(x',y') = m'$ de sorte que D est un carré modulo $4m'$. Soit p un diviseur premier de m'. Si p est impair, on a $\chi_D(p) = 1$; si $p = 2$, alors D est un carré modulo 8 et est impair donc :

$$\chi_D(2) = (-1)^{\frac{D^2-1}{8}} = 1$$

□