Formes quadratiques (Leçon 1)

Jorge Jiménez Urroz
(Universitat Politècnica de Catalunya)

Cimpa École, Bamako, Novembre 2010

Préliminaires

Définition

Une forme quadratique *est une fonction polynomiale homogène du second degré à coefficients dans* $\mathbb{Z}$,

$$f(x,y) = ax^2 + bxy + cy^2, \qquad a,b,c \in \mathbb{Z},$$

qui sera notée $f = \langle a,b,c\rangle$.

Question: Quels sont les entiers que f représente?

- $f(x,y) = 2x^2 - 6xy + 2y^2 = \langle 2,-6,2\rangle$.

Définition

La forme $\langle a,b,c\rangle$ *est dite* primitive *si* $pgcd(a,b,c) = 1$

- $f(x,y) = x^2 + y^2 = \langle 1,0,1\rangle$) ne représente eaucun entier négatif.

Définition

La forme $\langle a,b,c\rangle$ *est dite* définie *si* $\Delta = b^2 - 4ac < 0$ *avec* $a > 0$ *(et* $c > 0$*). Elle est dite* indéfinie *si* $\Delta > 0$.

$$4af(x,y) = 4a(ax^2 + bxy + cy^2) = (2ax + by)^2 - \Delta y^2.$$

- $f_1(x,y) = x^2 + 3y^2$ ne représente pas l'entier 2.

- $f_2(x,y) = 4x^2 + 14xy + 13y^2$, non plus.

Si on fait le changement de variables $x = 2x' - y'$, $y = -x' + y'$, nous avons $f_2(x,y) = f_1(x',y')$, et f et f' représentent le même ensemble d'entiers.

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \text{ et } \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Nous voulons faire un changement de variables pour trouver la forme la plus facile possible pour les calculs. Ce changement de variables doit impliquer une matrice inversible. Posons

$$\mathrm{GL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} : \alpha\delta - \beta\gamma = \pm 1 \right\},$$

et

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} : \alpha\delta - \beta\gamma = 1 \right\}.$$

Définition

A chaque forme $f = \langle a, b, c\rangle$, on associe la matrice

$$M_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

Alors on a

$$f(x, y) = (x, y) M_f \begin{pmatrix} x \\ y \end{pmatrix}.$$

Observation: $\Delta = -4\det(M_f)$.

Chaque $A \in \mathrm{GL}_2(\mathbb{Z})$ agit sur f et donne une autre forme f' dont la matrice associée est

$$M_{f'} = A M_f A^t.$$

En particulier, $\Delta_f = \Delta_{f'}$.

Définition

Etant donné un discriminant Δ, nous appelons $\mathcal{F}_\Delta$ l'ensemble des formes quadratiques de discriminant Δ.

Observation Tout entier $\Delta \equiv 0, 1 \pmod 4$ est discriminant d'une forme quadratique.

Définition

Etant donné un discriminant Δ, la forme quadratique principale I de discriminant Δ est

$$I = \begin{cases} \langle 1, 0, -\Delta/4\rangle & \text{si } \Delta \equiv 0 \pmod 4, \\ \langle 1, 1, (1-\Delta)/4\rangle & \text{si } \Delta \equiv 1 \pmod 4. \end{cases}$$

Définition

Un entier Δ est un discriminant fondamental *s'il est discriminant d'une forme quadratique primitive et seulement de formes quadratiques primitives.*

Il y a deux possibilités:

- $\Delta \equiv 1 \pmod 4$ avec Δ sans facteur carré,
- $\Delta/4 \equiv 2, 3 \pmod 4$ avec $\Delta/4$ sans facteur carré.

Etant donnés une matrice $A \in \mathrm{GL}_2(\mathbb{Z})$ et un discriminant Δ, nous avons

$$\begin{aligned} T_A : \quad & F_\Delta \to F_\Delta \\ & f \to T_A(f) = f'. \end{aligned}$$

Définition

Deux formes $f, g \in F_\Delta$ sont équivalentes, *en symboles $f \sim g$, s'il existe $A \in \mathrm{GL}_2(\mathbb{Z})$ tel que $T_A(f) = g$.*
Si $A \in \mathrm{SL}_2(\mathbb{Z})$, on dit que la forme f est proprement équivalente *à la forme g, en symboles $f \approx g$.*

Observation: $\sim$ et $\approx$ sont des relations d'équivalence. On note respectivement $\mathrm{Cl}(\Delta)$ l'ensemble des classes d'équivalence par rapport à $\sim$, et $\mathrm{Cl}^+(\Delta)$ l'ensemble des classes d'équivalence par rapport à $\approx$.

Si $T_A(f) = \langle a', b', c' \rangle$ et $A = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$, alors

$$\begin{cases} a' &= f(\alpha, \gamma), \\ b' &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, \\ c' &= f(\beta, \delta). \end{cases}$$

Etant donnée une forme $f \in \mathcal{F}_\Delta$, nous voulons trouver la forme équivalente (ou proprement équivalente) à f la plus utile.

Formes définies positives

Nous voulons les coefficients de $\langle a, b, c \rangle$ les plus petits possibles. Si la forme est définie positive, il existe m ayant la propriété

$$m = \min\{f(x, y) \, : \, x, y \in \mathbb{Z}\}.$$

Il est clair que si $m = f(\alpha, \gamma)$, alors $\text{pgcd}(\alpha, \gamma) = 1$ et on peut trouver β, δ telle que $\alpha\delta - \beta\gamma = 1$. Posons $A = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$ et appelons $T_A(f) = \langle a', b', c' \rangle$. Nous avons $a \leq c$, et voulons rendre $|b|$ le plus petit possible.

Définition

Une forme quadratique définie positive $f = \langle a, b, c \rangle$ est réduite *si $|b| \leq a \leq c$ et si de plus $b \geq 0$ lorsque $|b| = a$ ou lorsque $c = a$.*

Proposition

Il existe une forme quadratique réduite dans chaque classe de formes quadratiques définies positives proprement équivalentes.

Démonstration: Choisissons $\langle a', b', c' \rangle = T_A(f)$ avec $a' = \min\{f(x, y) \, : \, x, y \in \mathbb{Z}\}$. Si $|b'| \leq a$, c'est fini. Sinon, nous considérons l'unique entier δ tel que $|-b' + 2a'\delta| \leq a'$, et la matrice $B = M_\delta A'$ ou $M_\delta = \begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix}$ et $A' = \begin{pmatrix} -\beta & -\delta \\ \alpha & \gamma \end{pmatrix}$. La forme $T_B(f)$ est réduite.

Vous remarquerez que $g = T_{A'}(f) = \langle c', -b', a' \rangle$ et $T_{M_\delta}(g) = \langle a', -b + 2a'\delta, c' + b'\delta + a'\delta^2 \rangle$.

Exercice: Finissez la démonstration.

Théorème

Les seules formes de l'ensemble des formes réduites qui sont équivalentes entre elles sont $\langle a, -b, a \rangle \approx \langle a, b, a \rangle$ et $\langle a, -a, c \rangle \approx \langle a, a, c \rangle$.

Démonstration: Soit $\langle a, b, c \rangle$ et $\langle a', b', c' \rangle$ deux formes réduites équivalentes avec $a \geq a'$. Alors, $a' = a\alpha^2 + b\alpha\gamma + c\gamma^2$, et $a \geq a\alpha^2 + b\alpha\gamma + c\gamma^2 \geq a(\alpha^2 + \gamma^2) - |b||\alpha\gamma| \geq a|\alpha\gamma|$, de sorte que $\alpha^2 + \gamma^2 \geq 2|\alpha\gamma|$.

Cette inégalité est possible seulement si $\{\alpha, \gamma\} \subset \{0, 1, -1\}$. Si $\alpha = 0$, alors $b' = -b \pm 2c\delta$, $a' = c$, et nous arrivons a f_1. Si $\gamma = 0$, alors $b' = b \pm 2a\delta$, $a' = a$, et nous arrivons à f_2. Finalement, si $|\alpha\gamma| = 1$, alors $a = a' = a \pm b + c$, et nous avons $\langle a, \pm a, a \rangle$.

Comment pouvons-nous trouver la valeur minimale de $f(x,y)$? Dans ce qui suit, on va donner un algorithme standard pour trouver cette valeur:

- Si $f = \langle a,b,c\rangle$ n'est pas réduite, alors il existe un entier unique δ telle que $|-b+2c\delta| \leq c$.
- Considérons $A = \begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix}$ et $T_A(f) = \langle c, -b+2c\delta, a+b\delta+c\delta^2\rangle = f'$.
- Si $c \leq a+b\delta+c\delta^2$, c'est terminé. Sinon, nous répétons avec f'.

Observation Vous constaterez que si f' n'est pas réduite, alors $0 < c' < c$, de sorte que le processus se terminera après un nombre fini d'étapes.

Proposition

Soit $\langle a,b,c\rangle$ une forme définie positive réduite. Alors,

- $|b| \leq \sqrt{\Delta/3}$ *et* $b \equiv \Delta \pmod 2$,
- $a|(b^2-\Delta)/4$,
- $|b| \leq a \leq (b^2-\Delta)/(4a)$.

Corollaire

Pour $\Delta < 0$, les ensembles $\mathrm{Cl}(\Delta)$ et $\mathrm{Cl}(\Delta)^+$ sont finis de cardinalités h_Δ et h_Δ^+ respectivement.

Nous pouvons utiliser cette proposition, pour trouver toutes les formes quadratiques réduites définies positives.

Algorithme calculant toutes les formes quadratiques definies positives réduites de discriminant donné.

Soit

$$B = \{0 \leq b \leq \sqrt{|\Delta|/3}, b \equiv \Delta \pmod 2\},$$

et pour $b \in B$ posons

$$A_b = \{a \,|\, (b^2-\Delta)/4, |b| \leq a \leq (b^2-\Delta)/(4a)\}.$$

Alors,

$$h_\Delta^+ = \sum_{b\in B}\sum_{a\in A_b} n(a,b),$$

où

$$n(a,b) = \begin{cases} 1 & \text{si } b=0 \text{ ou si } a \in \{b,(b^2-\Delta)/4a\}, \\ 2 & \text{sinon.} \end{cases}$$

Exemple.

$\Delta = -264 = 4(-2\cdot 3\cdot 11)$

b	$(b^2-\Delta)/4$	a	c
0	66	$1,2,3,6$	$66,33,22,11$
2	67		
4	70	$5,7$	$14,10$
6	75		
8	82		

Par conséquent $h_\Delta^+ = 8$, et

$$Cl(\Delta)^+ = \left\{ \begin{array}{llll} \langle 1,0,66\rangle, & \langle 2,0,33\rangle, & \langle 3,0,22\rangle, & \langle 6,0,11\rangle, \\ \langle 5,4,14\rangle, & \langle 5,-4,14\rangle, & \langle 7,4,10\rangle, & \langle 7,-4,10\rangle \end{array} \right\}.$$

Nous avons $\langle a,-b,c\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\langle a,b,c\rangle$. Donc

$\langle 5,4,14\rangle \sim \langle 5,-4,14\rangle$, $\langle 7,4,10\rangle \sim \langle 7,-4,10\rangle$, et $h_\Delta = 6$.

Formes indéfinies

Définition

Une forme quadratique indéfinie $f = \langle a, b, c\rangle$ est dite réduite *si*

- $0 < b < \sqrt{\Delta}$,
- $\sqrt{\Delta} - b < 2|a| < \sqrt{\Delta} + b$.

Observations: Si $\langle a, b, c\rangle$ est réduite, $\langle c, b, a\rangle$ l'est aussi. En outre, $|a| < \sqrt{\Delta}$, $|c| < \sqrt{\Delta}$ et $ac < 0$. Remarquons que

$$(\sqrt{\Delta} - b)(\sqrt{\Delta} + b) = \Delta - b^2 = -4ac = 2|a| \cdot 2|c|$$

Proposition

Si $|a| \leq |c|$ et $\sqrt{\Delta} - 2|a| < b < \sqrt{\Delta}$, alors $\langle a, b, c\rangle$ est réduite.

Proposition

Toute forme quadratique indéfinie f de discrminant Δ est proprement équivalente à une forme réduite de même discrminant.

Démonstration: Si $\langle a, b, c\rangle$ n'est pas réduite, on chosit δ tel que $\sqrt{\Delta} - 2|c| < -b + 2c\delta < \sqrt{\Delta}$. Donc,

$$\langle c, -b + 2c\delta, a - b\delta + c\delta^2\rangle = \begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix} \langle a, b, c\rangle$$

et si $|a - b\delta + c\delta^2| < |c|$ le processus est répété.

Corollaire

Pour $\Delta > 0$, $\mathrm{Cl}(\Delta)$ et $\mathrm{Cl}(\Delta)^+$ sont finis du cardinalité h_Δ et h_Δ^+ respectivement.

Exemple.

$\Delta = 316 = 4 \cdot 79$

b	$\sqrt{\Delta} - b$	$\sqrt{\Delta} + b$	$\lvert a\rvert$	$\lvert c\rvert$
2	$15, 77$	$19, 77$		
4	$13, 77$	$21, 77$		
6	$11, 77$	$23, 77$	$7, 10$	$10, 7$
8	$9, 77$	$25, 77$	$7, 9$	$9, 7$
10	$7, 77$	$27, 77$	$6, 9$	$9, 6$
12	$5, 77$	$29, 77$		
14	$3, 77$	$31, 77$	$2, 3, 5, 6, 10, 15$	$15, 10, 6, 5, 3, 2$
16	$1, 77$	$33, 77$	$1, 3, 5, 15$	$15, 5, 3, 1$

Les formes réduites sont:

$\langle \pm 7, 6, \mp 10\rangle$, $\langle \pm 10, 6, \mp 7\rangle$, $\langle \pm 7, 8, \mp 9\rangle$, $\langle \pm 9, 8, \mp 7\rangle$
$\langle \pm 6, 10, \mp 9\rangle$, $\langle \pm 9, 10, \mp 6\rangle$, $\langle \pm 2, 14, \mp 15\rangle$, $\langle \pm 15, 14, \mp 2\rangle$,
$\langle \pm 3, 14, \mp 10\rangle$, $\langle \pm 10, 14, \mp 3\rangle$, $\langle \pm 5, 14, \mp 6\rangle$, $\langle \pm 6, 15, \mp 5\rangle$,
$\langle \pm 1, 16, \mp 15\rangle$, $\langle \pm 15, 16, \mp 1\rangle$, $\langle \pm 3, 16, \mp 5\rangle$, $\langle \pm 5, 16, \mp 3\rangle$

Définition

Les formes $\langle a, b, a' \rangle$ *et* $\langle a', b', c' \rangle$ *sont dites* adjacentes par la droite *si* $b + b' \equiv 0 \pmod{2a'}$. *Les formes* $\langle c', b, c \rangle$ *et* $\langle a', b', c' \rangle$ *sont dites* adjacentes par la gauche *si* $b + b' \equiv 0 \pmod{2c'}$.

Proposition

Soit $f = \langle a, b, c \rangle$ *une forme quadratique indéfinie réduite. Alors, il existe une forme équivalente à* f *adjacente par la droite et une autre forme équivalente à* f *et adjacente par la gauche.*

Démonstration: Nous considérons $b + b' \equiv 0 \pmod{2ac}$, et les matrices $\begin{pmatrix} 0 & -1 \\ 1 & -(b+b')/2c \end{pmatrix}$ et $\begin{pmatrix} -(b+b')/2a & -1 \\ 1 & 0 \end{pmatrix}$.

Observation: L'esemble des formes quadratiques réduites de discriminant $\Delta > 0$ peut être partionné en cycles de formes adjacentes par la droite (ou par la gauche).

Théorème

Soit f *et* f' *deux formes quadratiques indéfinies réduites. Alors,* $f \approx f' \iff$ *toutes les deux appartiennent au même cycle.*

Une implication est déjà démontrée. Pour l'autre nous avons besoin des nombres quadratiques.