RÉSOLUTION DE L'ÉQUATION DIOPHANTIENNE DU SECOND DEGRÉ (SUITE)

II. Généralités sur les formes quadratiques binaires

Éric KERN

A. Définitions et premières propriétés :

Définition :
Une forme quadratique (binaire entière) est un polynôme $f \in \mathbb{Z}[x,y]$ homogène du second degré, autrement dit

$$f(x,y) = f \cdot \begin{pmatrix} x \\ y \end{pmatrix} = Ax^2 + Bxy + Cy^2 \quad \textit{avec} \quad A,B,C \in \mathbb{Z}$$

On écrira simplement de façon abrégée $f = [A,B,C]$, si aucune confusion n'est possible.

La donnée de $f = [A,B,C]$ étant équivalente à celle du polynôme $P(t) = At^2 + Bt + C$, il est raisonnable de transporter à la forme quadratique f les définitions en usage pour le polynôme $P(t)$. Ainsi $D = B^2 - 4AC$ s'apelle le discriminant de f, si $\sqrt{D} \notin \mathbb{N}$ la forme f est dite irréductible et si $\operatorname{pgcd}(A,B,C) = 1$, la forme f est dite primitive. Enfin on donne aisément la définition de la première et de la deuxième racine de f.

Si ρ est un nombre quadratique, l'unique forme irréductible et primitive f telle que ρ soit la première racine de f sera dite associée à ρ.

On pourra vérifier le tableau de correspondance suivant :

Correspondance entre nombres quadratiques et formes :

$$\begin{array}{cccccc}
[A,B,C] & \leftrightarrow & \rho, & [-A,-B,-C] & \leftrightarrow & \rho^\sigma, \\
[-A,B,-C] & \leftrightarrow & -\rho, & [A,-B,C] & \leftrightarrow & -\rho^\sigma, \\
[-C,-B,-A] & \leftrightarrow & 1/\rho, & [C,B,A] & \leftrightarrow & 1/\rho^\sigma, \\
[C,-B,A] & \leftrightarrow & -1/\rho, & [-C,B,-A] & \leftrightarrow & -1/\rho^\sigma.
\end{array}$$

La matrice

$$M = M(f) = \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}$$

s'appelle la matrice de f. On a donc :

$$D = B^2 - 4AC = -4\det(M)$$

On rappelle que le discriminant D de f vérifie :

$$D = 0 \mod 4 \qquad \text{ou} \qquad D = 1 \mod 4$$

ceci suivant que B est pair ou impair.

Soit $D \in \mathbb{Z}$ vérifiant $D = 0 \mod 4$ ou $D = 1 \mod 4$. Si $D = 0 \mod 4$, alors $f = [1, 0, -D/4]$ est une forme quadratique primitive de discriminant D. Si $D = 1 \mod 4$, alors $f = [1, -1, (1-D)/4]$ est une forme quadratique primitive de discriminant D.
Dans les deux cas f s'appelle la forme quadratique principale de discriminant D.

Si $T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{Z})$ et si $f = [A, B, C]$, on définit une nouvelle forme $f1 = f \cdot T = [A_1, B_1, C_1]$ par

$$f_1 \cdot \begin{pmatrix} x \\ y \end{pmatrix} = f \cdot \begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix} = f \cdot \left(T \begin{pmatrix} x \\ y \end{pmatrix} \right) = (f \cdot T) \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

Un petit calcul donne

$$\begin{aligned} A_1 &= A\alpha^2 + B\alpha\gamma + C\gamma^2 = f(\alpha, \gamma) \\ B_1 &= 2A\alpha\beta + B(\alpha\delta + \beta\gamma) + 2C\gamma\delta \\ C_1 &= A\beta^2 + B\beta\delta + C\delta^2 = f(\beta, \delta) \end{aligned}$$

En outre on a :

$$M(f_1) = M(f \cdot T) = {}^tTM(f)T$$

Par suite si $D1 = B_1^2 - 4A_1C_1$ est le discriminant de $f1$, $D = B^2 - 4AC$ le discriminant de f, $\Delta = \det(T)$, on a

$$D_1 = D \cdot \Delta^2$$

et en particulier, si $T \in \mathrm{GL}(2, \mathbb{Z})$, on a $D_1 = D$, i.e. les formes f et $f \cdot T$ ont même discriminant.Comme on a aussi $(f \cdot T_1) \cdot T_2 = f \cdot (T_1 T_2)$ on en déduit que $\mathrm{GL}(2, \mathbb{Z})$ opère à droite sur les formes quadratiques par $(f, T) \mapsto f \cdot T$. En outre cette opération est aussi une opération sur les formes de discriminant D donné.

On remarquera que l'on a

$$f \cdot T = f \cdot (-T)$$

Proposition :
Soient $f = [A, B, C]$ une forme quadratique, $G \in \mathrm{GL}(2, \mathbb{Z})$, $f_1 = [A_1, B_1, C_1] = f \cdot G$, alors $\mathrm{pgcd}(A, B, C) = \mathrm{pgcd}(A_1, B_1, C_1)$. *En particulier f est primitive si et seulement si f_1 est primitive.*

Les formules ci-dessus montre que l'on a : $A_1\mathbb{Z} + B_1\mathbb{Z} + C_1\mathbb{Z} \subset A\mathbb{Z} + B\mathbb{Z} + C\mathbb{Z}$. Comme $f = f_1 \cdot G^{-1}$ on a aussi $A\mathbb{Z} + B\mathbb{Z} + C\mathbb{Z} \subset A_1\mathbb{Z} + B_1\mathbb{Z} + C_1\mathbb{Z}$, donc aussi $A_1\mathbb{Z} + B_1\mathbb{Z} + C_1\mathbb{Z} = A\mathbb{Z} + B\mathbb{Z} + C\mathbb{Z}$.

Cas particuliers :

i)Si $T = T(a)$ on a : $f_1 = f \cdot T(a) = [Aa^2 + Ba + C, B + 2Aa, A]$ soit :

$$A_1 = Aa^2 + Ba + C = \frac{B_1^2 - D}{4A}$$
$$B_1 = B + 2Aa$$
$$C_1 = A$$

ii)Si $T = \Delta(a)$ on a : $f_1 = f \cdot T(a) = [A, B + 2Aa, Aa^2 + Ba + C]$ soit :

$$A_1 = A$$
$$B_1 = B + 2Aa$$
$$C_1 = Aa^2 + Ba + C = \frac{B_1^2 - D}{4A}$$

Ces deux dernières formules seront très utiles par la suite.

A coté de cette opération (la seule utilisée dans la littérature) il existe une deuxième opération naturelle de $\mathrm{GL}(2,\mathbb{Z})$ sur les formes quadratiques définie par :

$$f * T = \det(T) f \cdot T$$

les deux opérations coïncidant donc si on se restreint à $\mathrm{SL}(2,\mathbb{Z})$.

On dira que deux formes f et g sont strictement équivalentes s'il existe un $T \in \mathrm{SL}(2,\mathbb{Z})$ tel que $f = f * T = f \cdot T$. Nous nous refuserons de parler des cas d'équivalence non stricte.

L'intérêt de la considération de $f * T$ au lieu de $f \cdot T$ provient du résultat suivant :

Proposition :
Soient $f = [A, B, C]$ est une forme quadratique irréductible de discriminant D, ρ la première racine de f. Si $T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z})$ et si on pose $\epsilon = \det(T), f_1 = f * T^{-1} = [A_1, B_1, C_1]$ on a :

$$N(\alpha\rho + \beta) = \epsilon\frac{C_1}{A}, N(\gamma\rho + \delta) = \epsilon\frac{A_1}{A}, T \cdot \rho - T \cdot \rho^\sigma = \frac{\sqrt{D}}{A_1}$$

et $T \cdot \rho$ est la première racine de $f_1 = f * T^{-1}$.

On a $T^{-1} = \epsilon\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$, donc

$$A_1 = \epsilon(A\delta^2 - B\gamma\delta + C\gamma^2) \text{ et } C_1 = \epsilon(A\beta^2 - B\alpha\beta + C\alpha^2)$$

Or on a $\alpha\rho+\beta = \dfrac{(-B\alpha+2A\beta)+\alpha\sqrt{D}}{2A}$ donc

$$N(\alpha\rho+\beta) = \frac{B^2\alpha^2-4AB\alpha\beta+4A^2\beta^2-\alpha^2D}{4A^2} = \frac{4AC\alpha^2-4AB\alpha\beta+4A^2\beta^2}{4A^2} = \epsilon\frac{C_1}{A}$$

De même on obtient $N(\gamma\rho+\delta) = \epsilon\dfrac{A_1}{A}$. Enfin on a

$$T\cdot\rho - T\cdot\rho^\sigma = \frac{\alpha\rho+\beta}{\gamma\rho+\delta} - \frac{\alpha\rho^\sigma+\beta}{\gamma\rho^\sigma+\delta} = \frac{\epsilon(\rho-\rho^\sigma)}{N(\gamma\rho+\delta)} = \frac{\sqrt{D}}{A_1}$$

D'autre part si $P(t) = At^2+Bt+C$ et $P_1(t) = A_1t^2+B_1t+C_1$ on a, en remarquant que $f_1\cdot T = \epsilon f$:

$$P_1(T\cdot\rho) = \frac{1}{(\gamma\rho+\delta)^2} f_1\cdot\begin{pmatrix}\alpha\rho+\beta\\ \gamma\rho+\delta\end{pmatrix} = \frac{1}{(\gamma\rho+\delta)^2}(f_1\cdot T)\begin{pmatrix}\rho\\1\end{pmatrix} = \frac{\epsilon}{(\gamma\rho+\delta)^2}P(\rho) = 0$$

donc $T\cdot\rho$ est une racine de f_1, donc la première racine de f_1, car $T\cdot\rho - T\cdot\rho^\sigma = \dfrac{\sqrt{D}}{A_1}$.

Corollaire :
Soient f et f_1 deux formes quadratiques irréductibles de même discriminant D, ρ la première racine de f et ρ_1 la première racine de f_1. Si $T\in \mathrm{GL}(2,\mathbb{Z})$ on a :

$$f * T = f_1 \Longleftrightarrow \rho = T\cdot\rho_1$$

La proposition précédente montre que si $f*T = f_1$, on a bien $\rho = T\cdot\rho_1$. Réciproquement, si $\rho = T\cdot\rho_1$, en posant $f = [A,B,C]$ et $f_2 = [A_2,B_2,C_2] = f_1 * T^{-1}$, la proposition précédente montre que :

$$\rho = \frac{-B+\sqrt{D}}{2A} = \frac{-B_2+\sqrt{D}}{2A_2}$$

donc $A = A_2, B = B_2$ donc aussi $C = C_2$ et par suite $f = f_2 = f_1 * T^{-1}$, donc $f_1 = f*T$.

B. Dérivée d'une forme quadratique irréductible

Formes quadratiques irréductibles à discriminant positif :

Ce qui précède permet de définir de façon naturelle la notion de dérivée d'une forme quadratique irréductible à discriminant positif.

Définition :
Si f est une forme quadratique irréductible de discriminant $D>0$ on pose

$$\partial f = f * T([\rho])$$

ρ étant la première racine de f.
De cette manière, si $n \geq 0$ est un entier, $\partial^n \rho$ est la première racine de $\partial^n f$.

En raison de leur importance, explicitons les formules qui donnent la dérivée d'une forme irréductible $f = [A, B, C]$ à discriminant $D > 0$.

Soit $\rho = \dfrac{-B + \sqrt{D}}{2A}$, posons $a = [\rho]$, alors $f_1 = [A_1, B_1, C_1] = \partial f$ est donnée par :

$$\begin{aligned} C_1 &= -A \\ B_1 &= -(B + 2Aa) \\ A_1 &= -(Aa^2 + Ba + C) = \frac{B_1^2 - D}{4A} \end{aligned}$$

Ceci permet donc d'obtenir l'algorithme suivant :

Algorithme : (j' ♡)

Si on pose $f = f_0 = [A_0, B_0, -A_{-1}]$, alors $f_n = \partial^n f = [A_n, B_n, -A_{n-1}]$ et f_n est obtenu par :

$$\begin{aligned} B_{n+1} &= -(B_n + 2A_n a_n) \\ A_{n+1} &= \frac{B_{n+1}^2 - D}{4A_n} \end{aligned}$$

avec

$$a_n = \left[\frac{-B_n + \sqrt{D}}{2A_n}\right]$$

Si ρ est la première racine de f on a alors $\rho = [a_0, a_1, \cdots]$.

Enfin on a :

$$f * T(a_0, \cdots, a_{n-1}) = f_n$$

L'intérêt de cet algorithme réside dans le fait qu'à partir d'un certain rang il se répète périodiquement, qu'il est aisé de déterminer le début de la partie périodique ainsi que la période. La démonstration de ce fait (théorème de périodicité de Lagrange) sera effectuée ultérieurement.

Formes quadratiques à discriminant négatif :

Transcrivons aussi la notion de dérivée des nombres quadratiques non réels aux formes quadratiques. Soient ρ un nombre quadratique non réel (donc de discriminant $D < 0$) et $f = [A, B, C]$ la forme quadratique (primitive) associée. On a donc $D = B^2 - 4AC$, donc aussi $4AC = B^2 + |D| > 0$ et par suite A et C sont non nuls et de même signe. Dire que $\rho \in \Pi_+$ (resp. $\rho \in \Pi_-$) siginifie que $A > 0$ (resp. $A < 0$) , donc que f est une forme quadratique définie positive (resp. négative). Enfin on a :

$$|\rho| = \frac{C}{A} \quad \text{et} \quad \Re(\rho) = -\frac{B}{2A}$$

Définition :
Soit $f = [A, B, C]$ une forme quadratique primitive de discriminant $D < 0$. Si $A > 0$, on dira que f est réduite si on a :

$$A \leq C \quad et \quad -A \leq B < A \quad avec\ en\ outre\ \ B \leq 0 \quad si \quad A = C$$

Si $A < 0$, f sera dite réduite si $-f$ est réduite.Ainsi, si ρ est la première racine de f, f est réduite si et seulement si ρ est réduit.

Transcrivons maintenant la définition de la dérivée des nombres quadratiques non réels. Soit ρ un tel nombre et suposons ρ non réduit et $\rho \in \Pi_+$. Posons $\rho_1 = \partial\rho = a - 1/\rho$. Soient $f = [A, B, C]$ et $f_1 = [A_1, B_1, C_1]$ les formes primitives associées à ρ et ρ_1. On a $\rho = \dfrac{-1}{z - a}$ donc $\rho = G \cdot \rho_1$ avec $G = \begin{pmatrix} 0 & -1 \\ 1 & -a \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$ donc aussi :

$$f_1(x, y) = f(-y, x - ay) = Cx^2 + (-B - 2aC)xy + (Ca^2 + Ba + A)y^2$$

de sorte que $[A_1, B_1, C_1] = [C, -B - 2aC, Ca^2 + Ba + A]$. Reste à déterminer comment on calcule a. On détermine a par la condition $-1/2 < \Re(\rho_1) \leq 1/2$ ce qui s'écrit $-A_1 < -B_1 \leq A_1$ soit $-C \leq B_1 < C$. En outre on a $B_1 = -B \bmod 2C$ et ces deux dernières conditions déterminent entièrement B_1 et on a alors $a = -\dfrac{B_1 + B}{2C}$.

Définition :
Soit $f = [A, B, C]$ un forme quadratique primitive de discriminant $D < 0$. On définit $\partial f = f_1 = [A_1, B_1, C_1]$ de la manière suivante : Si $A > 0$ et si f n'est pas réduite on définit B_1 par les conditions :

$$-C \leq B_1 < C \ , \ B_1 = -B \bmod 2C$$

et on pose :

$$b = \frac{B_1 + B}{2C} \ , \ A_1 = C \ , \ C_1 = Cb^2 - Bb + A = \frac{B_1^2 + |D|}{4C}$$

de sorte que $f_1 = f * \Theta(b)$ avec $\Theta(b) = \begin{pmatrix} 0 & -1 \\ 1 & b \end{pmatrix}$
Si f est réduite on pose $\partial f = f$. Enfin si $A < 0$ on pose $\partial f = -\partial(-f)$. Donc si ρ est la première racine de f alors $\partial^n\rho$ est la première racine de $\partial^n f$.

Les résultats obtenus pour les nombres quadratiques non réels se transposent en des résultats sur les formes quadratiques primitives à discriminant négatif.Ainsi si $f = [A, B, C]$ est une telle forme et si on pose $f_n = [A_n, B_n, C_n] = \partial^n f$, il existe un entier $n \geq 0$ tel que f_n soit réduite et f_n est alors l'unique réduite strictement équivalente à f.

En outre soit $n \geq 1$. Si $A_n > \sqrt{|D|}$ on a $A_{n+1} < A_n/2$. Si $0 < A_n \leq \sqrt{|D|}$ alors f_n ou f_{n+1} est réduite.On tombe donc sur une réduite avec au plus $\log_2(|C|/\sqrt{|D|})+2$ dérivations.

C. Généralités sur la représentation des formes quadratiques

Définition :
Soient $f = [A, B, C]$ une forme quadratique et $x, y, R \in \mathbb{Z}$. Si

$$f(x, y) = Ax^2 + Bxy + Cy^2 = R$$

on dit que (x, y) est une représentation de R par f. Si de plus $\operatorname{pgcd}(x, y) = 1$ *on dit que (x, y) est une représentation propre de R par f.*
On dit alors aussi que f représente (resp. représente proprement) R.

Exemple : Si $f = [1, 0, 1]$, i.e. $f(x, y) = x^2 + y^2$, alors $(1, 1)$ est une représentation propre de 2 par f, $(2, 2)$ est une représentation de 8 par f, 8 n'est pas représenté proprement par f, 3 n'est pas représenté par f, $(5, 5)$ est une représentation de 50 par f et $(1, 7)$ est une représentation propre de 50 par f.

Si f est une forme quadratique et si $T \in \mathrm{GL}(2, \mathbb{Z})$, f et $f \cdot T$ représentent les mêmes nombres

En effet $\binom{x}{y} \mapsto T\binom{x}{y}$ est une bijection de $\mathbb{Z}^2$ sur $\mathbb{Z}^2$.

Proposition :
Soient $(x, y) \in \mathbb{Z}^2$, $T \in \mathrm{GL}(2, \mathbb{Z})$. Si $\binom{x_1}{y_1} = T\binom{x}{y}$, on a $\operatorname{pgcd}(x_1, y_1) = \operatorname{pgcd}(x, y)$.

Comme $x_1 = ax + by, y_1 = cx + dy$ a $x_1\mathbb{Z} + y_1\mathbb{Z} \subset x\mathbb{Z} + y\mathbb{Z}$. Mais on a aussi $\binom{x}{y} = T^{-1}\binom{x_1}{y_1}$ donc $x\mathbb{Z} + y\mathbb{Z} \subset x_1\mathbb{Z} + y_1\mathbb{Z}$ et par suite $x_1\mathbb{Z} + y_1\mathbb{Z} = x\mathbb{Z} + y\mathbb{Z}$.

Théorème des représentations propres :
Soient f une forme quadratique irréductible et $R \in \mathbb{Z}, R \neq 0$. Alors R est proprement représenté par f si et seulement si il existe $T \in \mathrm{SL}(2, \mathbb{Z})$ tel que :

$$(*) \qquad f * T = [R, S, L] \text{ , avec } -|R| < S \leq |R|$$

En outre $T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto T\binom{1}{0} = \binom{\alpha}{\gamma}$ est alors une bijection entre l'ensemble des $T \in \mathrm{SL}(2, \mathbb{Z})$ vérifiant $(*)$ et l'ensemble des représentations propres de R par f.

Tout d'abord remarquons que si $T \in \mathrm{SL}(2, \mathbb{Z})$ vérifie $g = f * T = [R, S, L]$ et si on pose $\binom{x}{y} = T\binom{1}{0}$, on a $R = g(1, 0) = f(x, y)$. Comme $\operatorname{pgcd}(x, y) = \operatorname{pgcd}(1, 0) = 1$, (x, y) est une représentation propre de R par f.

Réciproquement soit (α,γ) une représentation propre de R par $f=[A,B,C]$. Comme $\mathrm{pgcd}(\alpha,\gamma)=1$ il existe $\beta,\delta\in\mathbb{Z}$ tels que $\alpha\delta-\beta\gamma=1$, donc $T_1=\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}\in \mathrm{SL}(2,\mathbb{Z})$ et si on pose $g_1=[A_1,B_1,C_1]=f*T_1$ on a $A_1=g_1(1,0)=f(\alpha,\gamma)=R$, donc $g_1=[R,B_1,C_1]$. Si $a\in\mathbb{Z}$ on a

$$g_2=f*T_1\Delta(a)=f*T_2=g_1*\Delta(a)=[R,B_1+2Ra,Ra^2+B_1a+C_1]$$

Il existe donc un unique $a\in\mathbb{Z}$ tel que $-|R|<B_1+2Ra\leq|R|$ et si pour cette valeur de a on pose $S=B_1+2Ra, L=Ra^2+B_1a+C_1$ on a trouvé on forme quadratique $g=[R,S,L]$, avec $-|R|<S\leq|R|$ et un $T=T_2\in\mathrm{SL}(2,\mathbb{Z})$ tels que $g=f*T$. En outre on a $T\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}\alpha\\\gamma\end{pmatrix}$.

Montrons enfin que si

$$g_i=[R,S_i,L_i]=f*T_i\ ,T_i\in\mathrm{SL}(2,\mathbb{Z}),-|R|<S_i\leq|R|\text{ pour }i=1,2$$

et si $\begin{pmatrix}\alpha\\\gamma\end{pmatrix}=T_1\begin{pmatrix}1\\0\end{pmatrix}=T_2\begin{pmatrix}1\\0\end{pmatrix}$ alors $T_1=T_2$. On a $T_i=\begin{pmatrix}\alpha&\beta_i\\\gamma&\delta_i\end{pmatrix}$ pour $i=1,2$ et comme $\det(T_1)=\det(T_2)=1$ on a aussi $\alpha(\delta_1-\delta_2)-\gamma(\beta_1-\beta_2)=0$. Puisque $\mathrm{pgcd}(\alpha,\gamma)=1$ on a $\delta_2=\delta_1+a\gamma,\beta_2=\beta_1+a\alpha$ avec $a\in\mathbb{Z}$, i.e. $T_2=T_1\Delta(a)$. On a donc aussi

$$g_2=g_1*\Delta(a)=[R,S_1+2Ra,Ra^2+S_1a+L_1]=[R,S_2,L_2]$$

donc $a=0$ car $-|R|<S_i\leq|R|$ pour $i=1,2$, de sorte que $T_1=T_2$. □

Remarque : Si $g=[R,S,L]=f*T=[A,B,C]*T$ avec $T\in\mathrm{GL}(2,\mathbb{Z})$, on a aussi $\mathrm{pgcd}(A,B,C)=\mathrm{pgcd}(R,S,L)$. En outre f et g ont alors même discriminant $D=B^2-4AC=S^2-4RL$. En particulier on aura : $S^2=D\mod 4|R|$.

Principes pour la résolution de l'équation du second degré :

Soient $f=[A,B,C]$ une forme quadratique irréductible, $R\in\mathbb{Z}$, $R\neq 0$.On cherche les représentations de R par f, autrement dit on cherche les $(x,y)\in\mathbb{Z}^2$ tels que

$$(*)\qquad f(x,y)=Ax^2+Bxy+Cy^2=R$$

Si $a=\mathrm{pgcd}(A,B,C)$, quitte à diviser par a, ce qui remplace R par R/a qui doit donc être entier, on peut supposer que f est primitive : c'est ce que nous supposerons désormais.

Si on pose $a=\mathrm{pgcd}(x,y)$ et $(x,y)=(ax_1,ay_1)$, l'équation $(*)$ s'écrit aussi $f(x_1,y_1)=R/a^2$, de sorte que R/a^2 doit être un entier. En cherchant tous les

entiers $a > 0$ tels que $R/a^2 \in \mathbb{Z}$, on est donc ramené à chercher les représentations propres de R par f, i.e. on se ramène au cas $\text{pgcd}(x, y) = 1$.

Le problême des représentations propres sera résolu de la manière suivante :

Soit $D = B^2 - 4AC$ le discriminant de f, donc $\sqrt{D} \notin \mathbb{Z}$. On cherche d'abord les $S \in \mathbb{Z}$ vérifiant :

$$(**) \qquad S^2 = D \mod 4|R| \ , \ -|R| < S \leq |R|$$

Si S est une solution on pose $L = \dfrac{S^2 - D}{4R}$ et on ne garde que les S vérifiant en outre $\text{pgcd}(R, S, L) = 1$. On pose alors $g = [R, S, L]$, qui est donc une forme quadratique primitive de discriminant D.

On cherche alors si f et g sont strictement équivalentes. Dans ce cas on cherche un $T \in \text{SL}(2, \mathbb{Z})$ tel que $f * T = g$. Alors si on pose $\begin{pmatrix} x \\ y \end{pmatrix} = T \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ (la première colonne de T), (x, y) est une représentation propre de R par f, deux valeurs distinctes de S donnant deux solutions distinctes de $(*)$.

Si (x, y) est une solution (non nécessairement propre) de $(*)$ obtenue par le procédé ci-dessus, on détermine le groupe $\mathcal{G} = \{G \in \text{SL}(2, \mathbb{Z}) \mid f = f * G\}$. Alors si $G \in \mathcal{G}$ et si on pose $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = G \begin{pmatrix} x \\ y \end{pmatrix}$, (x_1, y_1) est encore une solution de $(*)$, puisque $(f * G) * T = f * T = g$. On dira d'ailleurs que (x_1, y_1) et (x, y) sont deux solutions de même classe.

Par ce procédé on obtient toutes les solutions de $(*)$, réparties en classes disjointes. On peut n'avoir qu'une seule classe (ou aucune si $(*)$ n'a pas de solution).

Remarques :

1) Si (x, y) est une solution alors $(-x, -y)$ est dans la classe de (x, y). En effet $-I \in \mathcal{G}$.

2) Si $D < -4$ une classe contient exactement deux solutions $\pm(x, y)$. En effet on sait que dans ce cas on a $\mathcal{G} = \{I, -I\}$.

3) Si $D = -4$ donc $B = 2b$, une classe contient quatre solutions :

$$\pm(x, y) \ , \ \pm(-bx - Cy, Ax + by)$$

En effet dans ce cas on a $\mathcal{G} = \{I, -I, G, -G\}$ avec $G = \begin{pmatrix} -b & -C \\ A & b \end{pmatrix}$

4) Si $D = -3$ donc $B = 2b + 1$, une classe contient six solutions :

$$\pm(x, y) \ , \ \pm(-bx - Cy, Ax + (b + 1)y) \ , \ \pm(-(b + 1)x - Cy, Ax + by)$$

En effet dans ce cas on a $\mathcal{G} = \{I, -I, G, -G, G^2, -G^2\}$ ($G^3 = -I$) avec

$$G = G(1,1) = \begin{pmatrix} -b & -C \\ A & b+1 \end{pmatrix} \text{ et } G^2 = G(-1,1) = \begin{pmatrix} -(b+1) & -C \\ A & b \end{pmatrix}$$

D. Formes de discriminant négatif

Soient $f = [A, B, C]$ une forme à discriminant négatif, $R \in \mathbb{Z}$, $R \neq 0$. On sait que l'on est ramené à chercher les solutions propres avec f primitive. En outre quitte à changer de signe on peut supposer que $A > 0$, i.e. f définie positive donc $R > 0$ s'il y a au moins une solution. Nous nous placerons désormais dans cette situation.

On calcule d'abord $n \geq 0$ tel que $r = \partial^n f$ soit réduite. Ceci donne $a_0, \cdots, a_{n-1}$ tels que $T_1 = \Theta(a_0) \cdots \Theta(a_{n-1}) = \Theta(a_0, \cdots, a_{n-1})$ vérifie $f * T_1 = r$.

Soit $g = [R, S, L]$ obtenue par la méthode générale exposée ci-dessus. Soit $m \geq 0$ tel que $r_1 = \partial^m g$ soit réduite. On sait que f et g sont strictement équivalentes ssi $r = r_1$. Lorsqu'il en est ainsi ceci donne $b_0, \cdots, b_{m-1}$ tels que $T_2 = \Theta(b_0, \cdots, b_{m-1})$ vérifie $g * T_2 = r$.

En posant $T = T_1 T_2^{-1}$ on obtient donc un $T \in \mathrm{SL}(2, \mathbb{Z})$ tel que $f * T = g$, et on sait comment en déduire une solution (x, y). En outre on a déjà vu comment on en déduisait (suivant la valeur du discriminant D de f) la classe de solutions de (x, y).

La partie la plus délicate (sans logiciel de calcul formel) est la recherche des solutions de $S^2 = D \mod 4R$ vérifiant $-R < S \leq R$.

Exemple numérique : (Calculs effectués par MAPLE)

On cherche les solutions entières de :

$$f(x, y) = 5x^2 + 6xy + 2y^2 = 1850 = 2 \cdot 5^2 \cdot 37 = R$$

On a $f = [5, 6, 2]$ et $D = 6^2 - 4 \cdot 5 \cdot 2 = -4$.

Rappelons que si (x, y) est une solution alors la classe des solutions de (x, y) est l'ensemble à 4 éléments $\{\pm(x, y), \pm(-3x - 2y, 5x + 2y)\}$. En outre si $g = [R, S, L]$ est une forme de discriminant D alors g est primitive. En effet si $a = \mathrm{pgcd}(R, S, L)$ on a $-4 = a^2 D_1$ où D_1 est un discriminant. Or $D_1 = -4/a^2$. Si $a \neq 1$ on a $a = 2$ et $D_1 = -1$ qui n'est pas un discriminant.

Remarquons aussi que $[1, 0, 1]$ est l'unique réduite $r = [A, B, C]$ de discriminant $D = -4$ avec $A > 0$ (à titre purement indicatif). En effet on a $|B| \leq A \leq C$, donc $4A^2 \leq 4AC = B^2 + 4 \leq A^2 + 4$ donc $3A^2 \leq 4$, donc $A = 1$. Or B est pair et $|B| \leq 1$, donc $B = 0$ et par suite $C = 1$. Toute forme $[A_1, B_1, C_1]$ de discriminant -4 avec $A_1 > 0$ sera donc strictement équivalente à $[1, 0, 1]$, donc aussi à $[5, 6, 2]$.

Effectuons la réduction de $f = [5, 6, 2]$. On posera $f_n = [A_n, B_n, C_n] = \partial^n f$. On obtient :

n	A_n	B_n	C_n	a_n
0	5	6	2	1
1	2	-2	1	-1
2	1	0	1	

$$T_1 = \Theta(1, -1) = \begin{pmatrix} -1 & 1 \\ 1 & -2 \end{pmatrix}$$

Les $a \geq 1$ tels que $a^2 | R$ sont $a = 1$ et $a = 5$.

1) Solutions (x, y) avec $\text{pgcd}(x, y) = 1$. On doit résoudre ($R = 1850$)

$$S^2 = D \bmod 4R, -R < S \leq R$$

On trouve $S = \pm 86, \pm 1714$.

• $S = 86$ ce qui donne $L = 1$.

n	R_n	S_n	L_n	a_n
0	1850	86	1	43
1	1	0	1	

$$T_2 = \Theta(43) = \begin{pmatrix} 0 & -1 \\ 1 & 43 \end{pmatrix}, \quad T = T_1 T_2^{-1} = \begin{pmatrix} -44 & -1 \\ 45 & 1 \end{pmatrix}$$

D'où la classe de solutions : $\{\pm(-44, 45), \pm(42, -85)\}$
• $S = -86$ ce qui donne $L = 1$.

n	R_n	S_n	L_n	a_n
0	1850	-86	1	-43
1	1	0	1	

$$T_2 = \Theta(-43) = \begin{pmatrix} 0 & -1 \\ 1 & -43 \end{pmatrix}, \quad T = T_1 T_2^{-1} = \begin{pmatrix} 42 & -1 \\ -41 & 1 \end{pmatrix}$$

D'où la classe de solutions : $\{\pm(42, -41), \pm(-44, 87)\}$
• $S = 1714$ ce qui donne $L = 397$.

n	R_n	S_n	L_n	a_n
0	1850	1714	397	2
1	397	126	10	-6
2	10	-6	1	3
3	1	0	1	

$$T_2 = \Theta(2, -6, 3) = \begin{pmatrix} 6 & 19 \\ -13 & -41 \end{pmatrix}, \quad T = T_1 T_2^{-1} = \begin{pmatrix} 54 & 25 \\ -67 & -31 \end{pmatrix}$$

D'où la classe de solutions : $\{\pm(-54,-67),\pm(-28,69)\}$
• $S=-1714$ ce qui donne $L=397$.

n	R_n	S_n	L_n	a_n
0	1850	-1714	397	-2
1	397	126	10	6
2	10	-6	1	-3
3	1	0	1	

$$T_2=\Theta(-2,6,-3)=\begin{pmatrix}-6 & 19\\ -13 & 41\end{pmatrix},\quad T=T_1T_2^{-1}=\begin{pmatrix}-28 & 13\\ 15 & 7\end{pmatrix}$$

D'où la classe de solutions : $\{\pm(-28,15),\pm(54,-95)\}$

2) Solutions (x,y) avec $\text{pgcd}(x,y)=5$.
On remplace R par $R/5^2=74=R'$. On doit résoudre $(R=74)$

$$S^2=D \bmod 4R, -R<S\leq R$$

On trouve $S=\pm 62$.
• $S=62$ ce qui donne $L=13$.

n	R_n	S_n	L_n	a_n
0	74	62	13	2
1	13	-10	2	-3
2	2	-2	1	-1
3	1	0	1	

$$T_2=\Theta(2,-3,-1)=\begin{pmatrix}3 & -2\\ -7 & 5\end{pmatrix},\quad T=T_1T_2^{-1}=\begin{pmatrix}2 & 1\\ -9 & -4\end{pmatrix}$$

D'où la classe de solutions : $\{\pm 5\cdot(2,-9),\pm 5\cdot(12,-17)\}=\{\pm(10,45),\pm(60,-85)\}$
• $S=-62$ ce qui donne $L=13$.

n	R_n	S_n	L_n	a_n
0	74	-62	13	-2
1	13	10	2	2
2	2	-2	1	-1
3	1	0	1	

$$T_2=\Theta(2,2,-1)=\begin{pmatrix}-2 & 3\\ -5 & 7\end{pmatrix},\quad T=T_1T_2^{-1}=\begin{pmatrix}-2 & 1\\ -3 & 1\end{pmatrix}$$

D'où la classe de solutions : $\{\pm 5\cdot(-2,-3),\pm 5\cdot(12,-19)\}=\{\pm(10,45),\pm(60,-95)\}$

Il y a donc 24 solutions réparties en 6 classes de 4 éléments chacune.

K.E.