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

III. Formes irréductibles à discriminant positif

Éric KERN

Nous ne considérerons plus désormais que des formes quadratiques irréductibles à discriminant $D > 0$, donc $\sqrt{D} \notin \mathbb{N}$ et par suite $D \geq 5$.

A. Formes réduites :

Définition :
On dit qu'un nombre quadratique réel x est réduit si :

$$-1 < x^\sigma < 0 < 1 < x$$

On dira qu'une forme primitive irréductible de discriminant positif est réduite si sa première racine est un quadratique (réel) réduit.

Remarque : *Si x et y sont réduits et si $\partial x = \partial y$, on a $x = y$.*

En effet on a $y = x + a$, avec $a \in \mathbb{Z}$ donc $a = 0$, puisque $-1 < x^\sigma < 0$ et $-1 < y^\sigma < 0$.

Proposition :
Si x est un quadratique réel réduit alors $x_1 = \partial x$ est aussi réduit (et de même discriminant que x).

On a $x_1 = 1/(x - a) = \partial x > 1$ avec $a = [x] \geq 1$. Or $x^\sigma - a < -a \leq -1$, donc $-1 < x_1^\sigma < 0$, de sorte que x_1 est réduit.

Soient x un nombre quadratique réel et $f = [A, B, C]$ la forme primitive associée. Posons $P(t) = At^2 + Bt + C = f(t, 1)$. Si x est réduit, x est la plus grande racine de f, donc $A > 0$. La condition $-1 < x^\sigma < 0$ s'écrit donc $P(-1) > 0$ et $P(0) < 0$, soit $A - B + C > 0$ et $C < 0$. La condition $1 < x$ s'écrit $P(1) < 0$ soit $A + B + C < 0$. Ces deux dernières conditions s'écrivent aussi $B < A + C < -B$, ce qui signifie que $B < 0$ et que $|A + C| < |B|$. Donc :

Pour qu'une forme primitive irréductible $f = [A, B, C]$ de discriminant $D > 0$ soit réduite il faut et il suffit que l'on ait :

$$A > 0\ ,\ C < 0\ ,\ B < 0\ ,\ |A + C| < |B|$$

Si f est réduite on a donc $D = B^2 + 4A|C| \leq B^2 + 4$, donc $B^2 \leq D - 4$. On en déduit donc que pour un discriminant $D > 0$ donné il n'y a qu'un nombre fini de

valeurs possibles pour B et pour chacune de ces valeurs de B il n'y a qu'un nombre fini de valeurs possibles pour A et pour C. Donc :

Il n'y a qu'un nombre fini de réduites de discriminant $D > 0$ donné.

Comme le nombre de réduits de discriminant donné D est fini, ∂ est donc une permutation de l'ensemble de ces réduites, qui les décompose donc en cycles disjoints. Si x est réduit il existe donc un entier $p > 0$ tel que $\partial^p x = x$. Le plus petit de ces entiers s'appellera la période de x.

Proposition :
Pour qu'un quadratique réel x soit réduit il faut et il suffit que son développement en fractions continues soit périodique, i.e. $x = [\overline{b_1, \cdots, b_p}] = [b_1, \cdots, b_p, b_1, \cdots]$.

Si x est réduit, il existe un $p > 0$ tel que $x = \partial^p x$, d'où $x_n = \partial^n x = \partial^{n+p} x = x_{n+p}$ et par suite $a_{n+p} = a_n$ car $a_n = [x_n]$.
Réciproquement (Euler) supposons que $x = [\overline{b_1, \cdots, b_p}] = [b_1, \cdots, b_p, b_1, \cdots]$ et montrons que x est réduit. Comme $b_i \geq 1$ on a $x > 1$. D'autre part si on pose $G = T(b_1, \cdots, b_p) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on a $G \cdot x = x$ donc aussi $cx^2 + (d-a)x - b = 0$.
Or on a $c > 0$ et $b > 0$,donc le produit des racines de cette dernière équation est < 0. On a donc $x^\sigma < 0$. Si on pose $y = [\overline{b_p, b_1, \cdots, b_{p-1}}]$, les mêmes considérations s'appliquent à y et on a $\partial y = x$, en particulier on aura $y^\sigma - [y] < -1$ donc $-1 < 1/(y^\sigma - [y]) = x^\sigma < 0$, de sorte que x est réduit.

Les conditions ci-dessus montre que $f = [A, B, C]$ est réduite si et seulenent si $g = [-C, B, -A]$ est réduite. Or si x est la première racine de f, alors $-1/x^\sigma$ est la première racine de g donc :

Un nombre quadratique réel x est réduit si et seulement si $-1/x^\sigma$ est réduit et ces deux nombres ont même discriminant.

Proposition :
Si x est un quadratique réel réduit posons $x^* = -1/x^\sigma$, qui est donc aussi un réduit. Si $y = \partial x$, on a $\partial(y^*) = x^*$ et $a = [x] = [y^*]$

On a $y = 1/(x-a)$ avec $a = [x] \geq 1$. D'où $a < y^* = -x^\sigma + a < a + 1$, donc $a = [y^*]$. En outre $\partial(y^*) = -1/(y^* - a) = -1/x^\sigma = x^*$.

Proposition :
Soit $x = [\overline{a_0, \cdots, a_r}]$, un réduit. Alors $y = -1/x^\sigma = [\overline{a_r, \cdots, a_0}]$.

Posons $x_n = \partial^n x$ et $y_n = \partial^n y$. On a la situation suivante, la flèche représentant l'opération ∂ :

$$x_0 \xrightarrow{a_0} x_1 \xrightarrow{a_1} \cdots \longrightarrow x_{r-1} \xrightarrow{a_{r-1}} x_r \xrightarrow{a_r} x_0$$

donc aussi, d'après la proposition précédente :

$$(x_0)^* \xleftarrow{a_0} (x_1)^* \xleftarrow{a_1} \cdots \longleftarrow (x_{r-1})^* \xleftarrow{a_{r-1}} (x_r)^* \xleftarrow{a_r} (x_0)^*$$

d'où la conclusion puisque $(x_0)^* = x^* = y$.

Remarque : Ce résultat a d'importantes conséquences, que nous n'exploiterons pas dans cet article (c'était pour le plaisir du codage en TEXde la démonstration).

B. Théorème de périodicité de Lagrange :

Soient $f = [A, B, C]$ une forme primitive irréductible de discriminant $D > 0$ et x la première racine de f. On posera : $f_n = \partial^n f = [A_n, B_n, C_n]$ et $x_n = \partial^n x$ de sorte que x_n est la première racine de f_n. On désignera par $x = [a_0, \cdots, a_n, \cdots]$ le développement en fraction continue de x, de sorte que $a_n = [x_n]$.

Théorème de périodicité de Lagrange :
Avec les hypothèses et les notations ci-dessus, il existe un r tel que x_r soit réduit. Le développement en fraction continue de x est donc périodique à partir de r, c'est à dire, $x = [a_0, \ldots, a_{r-1}, \overline{b_1, \cdots, b_p}]$.

Comme $x_m = a_m + 1/x_{m+1}$ et $x_m^\sigma = a_m + 1/x_{m+1}^\sigma$, dire que $x_{m+1}^\sigma < 0$ signifie que que $x_m^\sigma < a_m < x_m$, autrement dit que les entiers séparent les racines de f_m et que x_m est la plus qrande racine de f_m. Montrons que s'il en est ainsi, il en est de même pour x_{m+1} et que x_{m+2} est réduit. Comme $a_{m+1} \geq 1$ on a $1/x_{m+2}^\sigma = x_{m+1}^\sigma - a_{m+1} < 0 - 1 = -1$, donc $-1 < x_{m+2}^\sigma < 0 < 1 < x_{m+2}$ et par suite x_{m+2} est réduit. De plus comme $x_{m+1}^\sigma < 0$, on a bien $x_{m+1}^\sigma < a_{m+1} < x_{m+1}$. Montrons qu'il existe effectivement un m tel que $x_{m+1}^\sigma < 0$. Supposons $x_{m+1}^\sigma > 0$ pour tout m. On ne peut avoir $0 < x_{m+1}^\sigma < 1$, car alors $x_{m+2}^\sigma = 1/(x_{m+1}^\sigma - a_{m+1}) < 0$. Comme $x_m^\sigma = a_m + 1/x_{m+1}^\sigma > 1$ pour tout m on a donc $[x_m^\sigma] = a_m = [x_m]$ pour tout m donc $x = [a_0, a_1, \cdots] = x^\sigma$, ce qui est contradictoire.

Remarque :

(i) $sgn(A_{n+2}) = -sgn(x_{n+2}^\sigma . sgn(A_n)$

(ii) Si s est le plus petit entier $t.q. x_s$ soit réduit alors si $1 \leq n < (s-1)$ on a $sgn(A_{n+2} = -sgn(A_n)$, $B_n \neq 0$ etc...

Théorème :
Avec les notations ci-dessus, soit p la période du développement en fractions continues de x, i.e. p est le plus petit entier positif tel que $a_n = a_{n+p}$ pour n assez grand. Soit $r \geq 0$ un indice dans la partie périodique de x. Posons

$$T_1 = T(a_0, \cdots, a_{r-1}) \quad et \quad H = T(a_r, \cdots, a_{r+p-1})$$

Pour que $G \in \mathrm{GL}(2, \mathbb{Z})$ soit tel que $G \cdot x = x$, i.e. $f * G = f$, il faut et il suffit que l'on ait $G = \epsilon T_1 H^n T_1^{-1}$ avec $\epsilon = \pm 1$ et $n \in \mathbb{Z}$ qui sont déterminés de façon unique par ces conditions. En outre on a $\det(G) = (-1)^{n+p}$.

Démontrons d'abord le résultat si x est réduit et si l'on prend $r = 0$ i.e. $T_1 = I$. Il faut donc montrer que tout $G \in \mathrm{GL}(2, \mathbb{Z})$ tel que $G \cdot x = x$ s'écrit de façon unique sous la forme $G = \epsilon H^n$ avec $\epsilon = \pm 1$, $n \in \mathbb{Z}$, $H = T(a_0, \cdots, a_{p-1})$, et réciproquement. On a $x = x_p = \partial^p x$, donc $H \cdot x = x_p = x$ et on a donc aussi $(\epsilon H^n) \cdot x = x$ si $\epsilon = \pm 1$ et $n \in \mathbb{Z}$, d'où la réciproque dans le cas considéré. Montrons

d'abord l'unicité. Si $\epsilon_1 H^n = \epsilon_2 H^m$, quitte à échanger n et m on peut supposer $n \leq m$ et alors $I = \epsilon_1\epsilon_2 H^{m-n}$. Or si on pose $H^{m-n} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, on a $\gamma > 0$ si $(m-n) > 0$ (ceci est une propriété des $T(a_0, \cdots, a_k)$), donc $n = m$ et par suite aussi $\epsilon_1 = \epsilon_2$.
Montrons maintenant l'existence. Soit $G \in \mathrm{GL}(2, \mathbb{Z})$ tel que $G \cdot x = x$. Si $\det(G) = -1$, on sait que p est impair donc que $\det(H) = -1$. Or G est de la forme ϵH^n si et seulement si il en est ainsi pour GH et on a $\det(GH) = 1$. On peut donc désormais supposer que $\det(G) = 1$. Or on sait que G s'écrit de façon unique $G = G(t,u) = \begin{pmatrix} (1/2)(t - Bu) & -Cu \\ Au & (1/2)(t + Bu) \end{pmatrix}$, où t et u sont solutions entières de $t^2 - Du^2 = 4$. Si $u = 0$ on a $t = \pm 2$, donc $G = \pm I$ ce qui démontre l'existence dans ce cas. Supposons maintenant $u \neq 0$, donc $t \neq 0$. Vérifions d'abord que l'une des matrices $G, G^{-1}, -G, -G^{-1}$ est de la forme $G_1 = G(t_1, u_1)$ avec $t_1 > 0$, $u_1 > 0$. En effet comme $\det(G) = 1$ et $G = G(t,u)$ on a $G^{-1} = G(t, -u)$, donc aussi $-G = G(-t, -u)$ et $-G^{-1} = G(-t, u)$, d'où le résultat. Il suffit donc de démontrer le résultat lorsque $t > 0$ et $u > 0$. Comme f est réduite on a $A > 0$, $B < 0$ et $C < 0$, donc $\alpha > 0, \beta > 0, \gamma > 0$ En outre $\alpha\delta = 1 + \beta\gamma > 0$, donc $\delta > 0$. On sait que l'on peut écrire $G = T(b_0, \cdots, b_s)\Delta(a)$, avec $b_i \geq 1$ si $i \geq 1$. Si on pose $G_2 = T(b_0, \cdots, b_s) = \begin{pmatrix} \alpha_2 & \beta_2 \\ \gamma_2 & \delta_2 \end{pmatrix}$ on a $G = \begin{pmatrix} \alpha_2 & \beta_2 + a\alpha_2 \\ \gamma_2 & \delta_2 + a\gamma_2 \end{pmatrix}$. Comme $\delta > 0$ on a $a \geq 0$, car $\gamma_2 > 0$ et $\gamma_2 \geq \delta_2 \geq 0$. Or $\Delta(a) \cdot x = [a + a_0, a_1, \cdots]$ et comme $a + a_0 \geq 1$ on a aussi $G \cdot x = [b_0, \cdots b_s, a + a_0, a_1, a_2, \cdots] = \overline{[a_0, \cdots, \alpha_{p-1}]}$ ceci n'est possible que si $a = 0$ et s'il existe un $n \geq 1$ tel que $(b_0, \cdots, b_s) = (a_0, \cdots, a_{np-1})$, autrement dit on a $G_2 = T(a_0, \cdots, a_{np-1}) = H^n$ et on a $G = G_2 \cdot \Delta(0) = G_2$. Le résultat est donc démontré lorsque x est réduit et si $r = 0$. Passons au cas général. On a $x = T_1 \cdot x_r$. Dire que $G \cdot x = x$ équivaut à dire que $(T_1^{-1} G T_1) \cdot x_r = x_r$, donc que $T_1^{-1} G T_1 = \epsilon H^n$ ou encore que $G = \epsilon T_1 H^n T_1^{-1}$.

On en déduit aussi la structure du groupe $\mathcal{G} = \{G \in \mathrm{SL}(2, \mathbb{Z}) \mid f * G = f\}$. Posons, en reprenant les notations ci-dessus, $H_+ = H$ si $\det(H) = 1$ i.e. si p est pair et $H_+ = H^2$ si $\det(H) = -1$ i.e. si p est impair. On remarquera que si q est la plus petite période paire du développement en fraction continue de x, on a : $H_+ = T(a_r, \cdots, a_{r+q-1})$. On posera en outre $G_+ = T_1 H_+ T_1^{-1}$.

On a $G \in \mathcal{G}$ si et seulement si G est de la forme $G = \epsilon T_1 H_+^n T_1^{-1} = \epsilon G_+^n$ avec $\epsilon = \pm 1$ et $n \in \mathbb{Z}$, cette écriture étant unique. En particulier $(\epsilon, n) \mapsto \epsilon G_+^n$ est un isomorphisme du groupe $\{1, -1\} \times \mathbb{Z}$ sur $\mathcal{G}$.

On a :

$$G_+ = T(a_0, \cdots, a_{r+q-1}) T(a_0, \cdots, a_{r-1})^{-1} = T(a_0 \cdots, a_{r+q-1}, 0, -a_{r-1}, \cdots, -a_0, 0)$$

En outre il est aisé de vérifier que G_+ ne dépend que de f et pas de l'indice particulier r choisi. On aura intérêt à prendre le plus petit r tel que x_r soit réduit.

C. Résolution pour les formes de discriminant positif :

Soient $f = [A, B, C]$ une forme irréductible de discriminant $D > 0$, $R \in \mathbb{Z}$, $R \neq 0$. On sait que l'on est ramené à chercher les solutions propres avec f primitive. Nous nous placerons désormais dans cette situation.

Soit x la première racine de f et $x = [a_0, a_1, \cdots]$ le développement en fraction continue de x. On posera $x_n = \partial^n x$ et $f_n = [A_n, B_n, C_n] = [A_n, B_n, -A_{n-1}] = \partial^n f$. On sait comment calculer les f_n et les a_n qui sont périodiques à partir d'un certain rang et l'on sait comment déterminer le début de la partie périodique ainsi que la période.

Soit G_+ défini par la méthode exposée ci-dessus. Si (X, Y) est une solution en entiers de $f(X, Y) = R$, les solutions de la classe de (X, Y) sont donc les $\pm(X_n, Y_n)$ définis par $\begin{pmatrix} X_n \\ Y_n \end{pmatrix} = G_+^n \begin{pmatrix} X \\ Y \end{pmatrix}$ avec $n \in \mathbb{Z}$. Contrairement au cas du discriminant négatif, les classes de solutions sont donc infinies. Posons $\tau = \mathrm{tr}(G_+)$. Comme $\det(G_+) = 1$ on a $G_+^2 - \tau G_+ + I = 0$, donc aussi $G_+^{n+2} - \tau G_+^{n+1} + G_+^n = 0$, de sorte que l'on a aussi $(X_{n+2}, Y_{n+2}) - \tau(X_{n+1}, Y_{n+1}) + (X_n, Y_n) = 0$, ce qui permet de calculer par une récurrence double les (X_n, Y_n) quand on connaît (X_0, Y_0) et (X_1, Y_1).

Soit $g = [R, S, L]$ obtenu par la méthode générale du principe de résolution de l'équation du second degré (voir partie II B).

Il s'agit de savoir si f et g sont strictement équivalentes et, lorsqu'il en est ainsi de trouver un $T \in \mathrm{SL}(2, \mathbb{Z})$ tel que $f * T = g$, ce qui permet de trouver une solution propre (X, Y) de $f(X, Y) = R$, par $\begin{pmatrix} X \\ Y \end{pmatrix} = T \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Soient y la première racine de g et $y = [b_0, b_1, \cdots]$ le développement en fractions continues de y. On posera $y_n = \partial^n y$ et $g_n = [R_n, S_n, L_n] = [R_n, S_n, -R_{n-1}] = \partial^n g$.

Or on sait que f et g sont strictement équivalentes si et seulement si il existe un $r \geq 0$ et un $s \geq 0$ tels que $r + s$ soit pair et $f_r = g_s$ (condition de Scheffler) (partie I E). Lorsqu'il en est ainsi posons $T_1 = T(a_0, \cdots, a_{r-1})$ et $T_2 = T(b_0, \cdots, b_{s-1})$. On a donc $f * T_1 = f_r = g_s = gT_2$, donc aussi $f * T = g$ avec $T = T_1 T_2^{-1}$ et on a

$$T = T(a_0, \cdots, a_{r-1}) T(b_0, \cdots, b_{s-1})^{-1} = T(a_0, \cdots, a_{r-1}, 0, -b_{s-1}, \cdots, -b_0, 0)$$

En outre comme $r + s$ est pair on a $T \in \mathrm{SL}(2, \mathbb{Z})$.

Expliquons comment on peut déterminer si la condition de Scheffler est vérifiée ou non. On commence par déterminer le plus petit r_0 tel que f_{r_0} soit réduite, ainsi que la période p de f, ce qui implique le calcul de la partie périodique $f_{r_0}, \cdots, f_{r_0+p-1}$ de f. On désigne par s le plus petit indice tel que g_s soit réduite. On regarde alors s'il existe un indice r avec $r_0 \leq r < r_0 + p$ tel que $f_r = g_s$. Si ce n'est pas le cas il n'y a pas de solution associée à g. Sinon on distingue deux cas.

• Si $r + s$ est pair on a trouvé r et s qui donne une solution associée à g.

• Si $r+s$ est impair on doit distinguer suivant la parité de la période p de f. Si p est pair il n'y a pas de solution associée à g, sinon en remarquant que $r+p+s$ est alors pair, il suffit de remplacer r par $r+p$ pour obtenir une solution associée à g.

Remarque : L'idéal est de posséder un logiciel de calcul formel tel que MAPLE ou autre pour programmer l'algorithme. J'ai toutefois, il y a un certain nombre d'années programmé l'algorithme sur une calculette programmable en Basic (bon courage).

Avant de donner (quand-même) un exemple numérique, terminons par une remarque qui n'est pas sans intérêt. Il arrive assez souvent que au lieu d'être amené à résoudre $f(X,Y)=R$, on soit ammené à résoudre $f(X,Y)=\pm R$. Avec ce qui a été dit jusqu'à présent on devrait, en toute logique, résoudre séparément les équations $f(X,Y)=R$ et $f(X,Y)=-R$. Or dans chacun de ces cas on est amené à chercher d'abord les S vérifiant $-|R|<S\leq|R|$ et $S^2=D \bmod 4|R|$. Ceci donne donc les mêmes S pour chacun des cas et en outre, si $g=[R,S,L]$ dans un cas, on devra examiner $g_1=[-R,S,-L]$ dans l'autre cas. Ceci n'est pas très gratifiant.

Une remarque assez simple permet de traiter simultanément les deux cas. N'oublions pas que pour trouver la classe des solutions de $f(X,Y)=R$ associées à $g=[R,S,L]$, il suffit d'en trouver une et que ceci se fait en cherchant **un** $T\in \mathrm{SL}(2,\mathbb{Z})$. La méthode exposée ci-dessus nous permet (s'il existe) de trouver un tel $T=T_1T_2^{-1}$ lorsque la condition de Scheffler $r+s$ pair est vérifiée. On peut alors espérer et c'est ce que nous allons monter, que si $r+s$ est impair, la même constuction donne une solution de la classe des solutions de $f(X,Y)=-R$ associée à $g_1=[-R,S,-L]$.

Si T_1 et T_2 sont construits par la méthode exposée ci-dessus et si $T=T_1T_2^{-1}$ on a donc $f*T=g$ et $\det(T)=-1$. On a donc aussi $f\cdot T=-g=[-R,-S,-L]$. Posons alors $J=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ de sorte que $\det(J)=-1$ et $g\cdot J=[-R,S,-L]=g_1$. On a donc det(TJ)=1, donc $TJ\in \mathrm{SL}(2,\mathbb{Z})$ et $g\cdot J=g_1$, de sorte que

$$f*(TJ)=f\cdot(TJ)=(f\cdot T)\cdot J=g_1$$

Donc $\begin{pmatrix}X\\Y\end{pmatrix}=TJ\begin{pmatrix}1\\0\end{pmatrix}$ fournit une solution de la classe des solutions (propres) associée à g_1.Or on a $\begin{pmatrix}1\\0\end{pmatrix}=J\begin{pmatrix}1\\0\end{pmatrix}$, donc $\begin{pmatrix}X\\Y\end{pmatrix}=T\begin{pmatrix}1\\0\end{pmatrix}$, fournit bien une solution (propre) de $f(X,Y)=-R$ associée à $g_1=[-R,S,-L]$. On a donc bien trouvé une méthode qui résout simultanément $f(X,Y)=R$ et $f(X,Y)=-R$.

Toujours en reprenant les notations ci-dessus, posons $G_0=T_1HT_1^{-1}$ et soit p la période de f, de sorte que $G_+=G_0$ si p est pair et $G_+=G_0^2$ si p est impair. On sait que $f*G_0=f$.

Exemple numérique : (Calculs effectués par MAPLE)

On cherche les solutions entières de :

$$f(x,y) = 12x^2 - 26xy + 11y^2 = \pm 81 = \pm R$$

On a $f = [12, -26, 11]$ et $D = 4.(13^2 - 12 \cdot 11) = 4 \cdot 37 = 148$.

Effectuons le développement de $f = [12, -26, 11]$. 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	12	-26	11	1
1	3	2	-12	1
2	7	-8	-3	1
3	4	-6	-7	2
4	3	-10	-4	3
5	7	-8	-3	1

La période $p = 3$ de f est donc impaire. On obtient donc :

$$G_0 = T(1,1,1,2,3,0,-1,-1,0) = \begin{pmatrix} 19 & -11 \\ 12 & -7 \end{pmatrix} \quad \text{et} \quad G_+ = G_0^2 = \begin{pmatrix} 229 & -132 \\ 144 & -83 \end{pmatrix}$$

Les $a \geq 1$ tels que $a^2 | R$ sont $a = 1$,$a = 3$ et $a = 9$.

1) Solutions (X, Y) avec $\text{pgcd}(X, Y) = 1$. On doit résoudre $(R = 81)$

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

On trouve $S = \pm 38$.

• $S = -38$ donc $g = [R, S, L] = [81, -38, 4]$ et $\text{pgcd}(R, S, L) = 1$.

n	R_n	S_n	L_n	b_n
0	81	-38	4	0
1	-4	38	-81	3
2	3	-14	4	4
3	4	-10	-3	

Donc pas de solution associée à g (et à $g_1 = [-R, S, -L]$).

• $S = 38$ donc $g = [R, S, L] = [81, 38, 4]$ et $\text{pgcd}(R, S, L) = 1$.

n	R_n	S_n	L_n	b_n
0	81	38	4	-1
1	-47	124	-81	1
2	4	-30	47	5
3	3	-10	-4	

Donc $r=4$, $s=3$ est une condition de Scheffler pour f et g avec $r+s=7$ impair. $T(1,1,1,2,0,-5,-1,1,0)\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}10\\7\end{pmatrix}$. Donc $(X,Y)=(10,7)$ est une solution associée à g_1 donc $f(X,Y)=-R$. Si on pose $\begin{pmatrix}X_n\\Y_n\end{pmatrix}=G_+^n\begin{pmatrix}X\\Y\end{pmatrix}$ pour $n\in\mathbb{Z}$ alors $\pm(X_n,Y_n)$ la classe des solutions associées à g_1. On a donc $f(X_n,Y_n)=-R=-81$.
On a $G_0\begin{pmatrix}X\\Y\end{pmatrix}=\begin{pmatrix}113\\71\end{pmatrix}$. Donc si on pose $(X,Y)=(113,71)$ alors (X,Y) est une solution associée à g donc $f(X,Y)=R$. Si on pose $\begin{pmatrix}X_n\\Y_n\end{pmatrix}=G_+^n\begin{pmatrix}X\\Y\end{pmatrix}$ pour $n\in\mathbb{Z}$ alors $\pm(X_n,Y_n)$ la classe des solutions associées à g_1. On a donc $f(X_n,Y_n)=R=81$.
Tableau des premières valeurs :

	$f(X_n,Y_n)=81$			$f(X_n,Y_n)=-81$	
n	X_n	Y_n	n	X_n	Y_n
4	51358576625	32296315511	4	4250565754	2672924791
3	351787577	221218019	3	29114830	18308563
2	2409617	1515263	2	199426	125407
1	16505	10379	1	1366	859
0	113	71	0	10	7
-1	-7	-13	-1	94	163
-2	-1135	-1969	-2	13714	23791
-3	-165703	-287461	-3	2002150	3473323
-4	-24191503	-41967337	-4	292300186	507081367

2) Solutions (X,Y) avec $\text{pgcd}(X,Y)=3$.
On remplace R par $R/3^2=9=R'$. On doit résoudre $(R=9)$

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

On trouve $S=\pm 2$.

• $S=-2$ donc $g=[R,S,L]=[9,-2,-4]$ et $\text{pgcd}(R,S,L)=1$.

n	R_n	S_n	L_n	b_n
0	9	-2	-4	0
1	4	2	-9	1
2	3	-10	-4	

Donc $r=4$, $s=2$ est une condition de Scheffler pour f et g avec $r+s=6$ pair. $T(1,1,1,2,0,-1,0,0)\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}5\\3\end{pmatrix}$. Donc $(X,Y)=3\cdot(5,3)=(15,9)$ est une solution avec $\text{pgcd}(X,Y)=3$ associée à g donc $f(X,Y)=R=81$.
Si on pose $\begin{pmatrix}X_n\\Y_n\end{pmatrix}=G_+^n\begin{pmatrix}X\\Y\end{pmatrix}$ pour $n\in\mathbb{Z}$ alors $\pm(X_n,Y_n)$ la classe des solutions associées à g. On a donc $f(X_n,Y_n)=R=81$.

On a $G_0\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 186 \\ 117 \end{pmatrix}$. Donc si on pose $(X, Y) = (186, 117)$ alors (X, Y) est une solution avec $\text{pgcd}(X, Y) = 3$ associée à g_1 donc $f(X, Y) = -R = -81$.
Si on pose $\begin{pmatrix} X_n \\ Y_n \end{pmatrix} = G_+^n \begin{pmatrix} X \\ Y \end{pmatrix}$ pour $n \in \mathbb{Z}$ alors $\pm(X_n, Y_n)$ la classe des solutions associées à g_1. On a donc $f(X_n, Y_n) = R = -81$.
Tableau des premières valeurs :

	$f(X_n, Y_n) = 81$			$f(X_n, Y_n) = -81$	
n	X_n	Y_n	n	X_n	Y_n
4	6991993743	4396843737	4	84482600010	53126018757
3	47892615	30116781	3	578675094	363893913
2	328047	206289	2	3963714	2492541
1	2247	1413	1	27150	17073
0	15	9	0	186	117
-1	-57	-99	-1	6	9
-2	-8337	-14463	-2	690	1197
-3	-1217145	-2111499	-3	100734	174753
-4	-177694833	-308264391	-4	14706474	25512741

• $S = 2$ donc $g = [R, S, L] = [9, 2, -4]$ et $\text{pgcd}(R, S, L) = 1$.

n	R_n	S_n	L_n	b_n
0	9	2	-4	0
1	4	-2	-9	1
2	7	-6	4	

Donc pas de solution associée à g (et à $g_1 = [-R, S, -L]$).

3) Solutions (X, Y) avec $\text{pgcd}(X, Y) = 9$.
On remplace R par $R/9^2 = 1 = R'$. On doit résoudre $(R = 1)$

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

On trouve $S = 0$.

• $S = 0$ donc $g = [R, S, L] = [1, 0, -37]$ et $\text{pgcd}(R, S, L) = 1$.

n	R_n	S_n	L_n	b_n
0	1	0	-37	6
1	1	-12	-1	

Donc pas de solution associée à g (et à $g_1 = [-R, S, -L]$).

K.E.