Introduction :

Nous allons montrer que pour résoudre l'équation $ax^2 + bxy + cy^2 = m$ (E) (avec $b^2 - 4ac = D$ non carré ; $a > 0$; $m > 0$), il suffit de savoir accomplir les tâches suivantes :

a) Trouver les unités de norme ± 1 de l'anneau $\mathcal{O}_M$ (stabilisateur de $M = \mathbb{Z} \oplus \mathbb{Z}\left(\frac{-b+\sqrt{D}}{2a}\right)$)

b) Faire la liste des modules $A \subseteq \mathcal{O}_M$ associés à $\mathcal{O}_K$ et de norme m

c) Extraire de cette liste les modules strictement semblables à M^{-1}

Nous allons donner une preuve constructive du point a) (théorème de Dirichlet quadratique) à l'aide de fractions continuées.
Un calcul direct fournira le point b).
Le point c) relève également des fractions continuées.

En dernière partie, nous nous intéresserons à la structure des idéaux premiers de $\mathcal{O}_K$ (l'anneau des entiers d'un corps quadratique), puis au nombre d'idéaux de norme donnée afin d'obtenir une majoration du nombre de solutions non associées de l'équation (E).

I) Modules complets

1) Apparition des corps quadratiques

Soit à résoudre $\varphi(x,y) = ax^2 + bxy + cy^2 = m$ où $(a,b,c) \in \mathbb{Z}^3$

avec $a > 0$; $PGCD(a;b;c) = 1$ et $\text{Disc}\,\varphi = b^2 - 4ac$ n'est pas un carré dans $\mathbb{Z}$.

Factorisons φ : $\varphi(x,y) = a\left(\left(x + \frac{b}{2a}y\right)^2 - D\frac{y^2}{4a^2}\right)$ où $D = \text{Disc}\,\varphi$

On peut factoriser dans le corps K de $\mathbb{C}$ obtenu en ajoutant à $\mathbb{Q}$ une racine de l'équation $X^2 - D$; en écrivant $D = f^2 d$ où $f \in \mathbb{N}^*$ et $d \in \mathbb{Z}$, d sans facteur carré.

$K = \mathbb{Q}(\sqrt{d})$ est un corps quadratique, c'est à dire un $\mathbb{Q}$ espace vectoriel de dimension 2

On a $K = \mathbb{Q} \oplus \mathbb{Q}\sqrt{d}$.

On peut factoriser φ dans K :

$$\varphi(x,y) = a\left(x - \frac{-b+\sqrt{D}}{2a}y\right)\left(x - \frac{-b-\sqrt{D}}{2a}y\right) \quad (\text{où } \sqrt{D} = f\sqrt{d})$$

En notant σ le $\mathbb{Q}$-morphisme de $\mathbb{Q}(\sqrt{d})$ tel que $\sigma(\sqrt{d}) = -\sqrt{d}$

et $\alpha = \frac{-b+\sqrt{D}}{2a}$ on a :

$$\varphi(x,y) = a(x - \alpha y)(x - \alpha^\sigma y) = a\,N(x - \alpha y) = a\,N(\xi)$$

(où $N(x) = x x^\sigma$, $x \in K$ et la norme de K sur $\mathbb{Q}$)

Le problème $\varphi(x,y) = m$ revient donc à chercher les nombres $\xi \in \mathbb{Z} \oplus \mathbb{Z}\alpha$ tels que $N(\xi) = \frac{m}{a}$.

2) Modules, ordres, anneaux de stabilisateurs, discriminant, norme, produit.

Definition : Un module complet de K est un sous $\mathbb{Z}$-module de rang 2 de K.

Soit $\xi \in \mathbb{Z} \oplus \mathbb{Z}\alpha = M$ (M est un module complet) avec $N(\xi) = \frac{m}{a}$

Si $w \in \mathbb{Q}(\sqrt{d})$ est de norme 1 et si $w\xi \in M$ on a également $N(w\xi) = \frac{m}{a}$

donc $w\xi$ sera aussi solution de $N(\xi) = \frac{m}{a}$.

Soit donc $\mathcal{O}_\Pi = \{w \in K / w\Pi \subset \Pi\}$ est appellé anneau des stabilisateurs de Π

On dit que Π est associé à $\mathcal{O}_\Pi$.

On appelle ordre de K un sous-anneau de K qui est un module complet.

Lemme I.1):

Soit $\mathcal{O}$ un ordre de K :

1) Si $\mathcal{O}_K$ est l'anneau des entiers de K sur $\mathbb{Z}$ alors $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z} w$ ($\mathcal{O}_K$ est un ordre)
avec $w = \frac{1+\sqrt{d}}{2}$ si $d \equiv 1 [4]$ et $w = \sqrt{d}$ si $d \equiv 2$ ou $3 [4]$

2) Il existe $f \geq 1$ entier appelé conducteur de $\mathcal{O}$ tel que $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z} fw = \mathcal{O}_f$

3) Si $w \in \mathcal{O}$ $w \neq 0$ on a $\frac{N(w)}{w} \in \mathcal{O}$

4) Soit $\mathcal{O}^*$ le groupe des unités de $\mathcal{O}$ alors $\mathcal{O}^* = \{\varepsilon \in \mathcal{O} / N(\varepsilon) = \pm 1\}$

5) Si Π est un module complet et $\alpha \in K$ alors $\mathcal{O}_{\alpha\Pi} = \mathcal{O}_\Pi$

6) Si $\Pi = \mathbb{Z} \oplus \mathbb{Z}\alpha$ est un module complet et si $P_\alpha = uX^2 + vX + w \in \mathbb{Z}[X]$ est le polynôme minimal de α alors $\mathcal{O}_\Pi = \mathbb{Z} \oplus \mathbb{Z} u\alpha$.

Définition : Si Π est un module complet on note Π^σ le conjugué de M par
$\Pi^\sigma = \{m^\sigma, m \in \Pi\}$

Propriété 1) : Π^σ est un module complet ; tout ordre $\mathcal{O}$ est égal à son conjugué $\mathcal{O}^\sigma = \mathcal{O}$.

Démonstration : D'après le lemme 1) il existe $f \geq 1$ tel que $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z} fw$
et $(fw)^\sigma = fw^\sigma$ vaut soit $-fw$ (si $d \equiv 2, 3 [4]$) soit $f - fw$ (si $d \equiv 1 [4]$) donc est un élément de $\mathcal{O}$, on a donc $\mathcal{O}_\Pi = \mathcal{O}_{\Pi^\sigma}$ (on a $\mathcal{O}_{\Pi^\sigma} = (\mathcal{O}_\Pi)^\sigma = \mathcal{O}_\Pi$) □

Définition : Soit $M = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2$ un module complet
$D(\alpha_1, \alpha_2) = \det\left(\mathrm{Tr}(\alpha_i \alpha_j)\right)_{1 \leq i,j \leq 2}$ est appelé discriminant du module Π noté $\mathrm{Disc}\, M$. La remarque qui suit justifi cette écriture.

Remarque : Si β_1, β_2 une autre base de Π et $C \in Gl_2(\mathbb{Z})$ tel que
$\begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = C \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$ alors $D(\beta_1, \beta_2) = (\det C)^2 D(\alpha_1, \alpha_2)$ mais $\det C = \pm 1$
donc $D(\beta_1, \beta_2) = D(\alpha_1, \alpha_2) = \mathrm{Disc}\, \Pi$.

Lemme 2): Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique

1) Si $\Pi = \mathbb{Z} \oplus \mathbb{Z}\alpha$ est un module complet de K avec $P_\alpha = uX^2 + vX + w \in \mathbb{Z}[X]$ polynôme minimal de α alors $\mathrm{Disc}\,\Pi = (v^2 - 4uw)/u^2$

2) $\mathrm{Disc}\,\mathcal{O}_f = f^2 \mathrm{disc}\,\mathcal{O}_K$ et $\mathrm{disc}\,\mathcal{O}_K = d$ si $d \equiv 1\ [4]$

$\mathrm{disc}\,\mathcal{O}_K = 4d$ si $d \equiv 2,3\ [4]$

3) Deux ordre ayant le même discriminant sont égaux.

Démonstration:

1) $\mathrm{Disc}\,\Pi = \begin{vmatrix} \mathrm{Tr}\,1 & \mathrm{Tr}\,\alpha \\ \mathrm{Tr}\,\alpha & \mathrm{Tr}\,\alpha^2 \end{vmatrix} = \begin{vmatrix} 2 & -\frac{v}{u} \\ \frac{v}{u} & \frac{v^2}{u^2} - \frac{2w}{u} \end{vmatrix} = \frac{v^2 - 4uw}{u^2}$ car $\mathrm{Tr}\,\alpha^2 = \mathrm{Tr}\left(\frac{-v\alpha - w}{u}\right) = \frac{-v}{u}\mathrm{Tr}\,\alpha - \frac{w}{u}\mathrm{Tr}\,1$

2) Si $d \equiv 1\ [4]$ $\mathcal{O}_f = \mathbb{Z} + \mathbb{Z} f\omega$ on a

$\omega = \frac{1+\sqrt{d}}{2}$ et $P_{f\omega} = X^2 - fX + \frac{1-d^2}{4} f^2$ donc $\mathrm{Disc}\,\mathcal{O}_f = 4f^2 d$ lorsque $f = 1$

$\mathrm{Disc}\,\mathcal{O}_K = 4d$ (Lemme I.1)

Si $d \equiv 2,3\ [4]$ $\mathcal{O}_f = \mathbb{Z} \oplus \mathbb{Z} f\omega$ on a $\omega = \sqrt{d}$ et $P_{f\omega} = X^2 - df^2$ donc $\mathrm{Dis}\,\mathcal{O}_f = 4f^2 d$

3) Car ils ont même conducteur. □

Définition:

Si $\Pi = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2$ un module complet et $\mathcal{O}_\Pi = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$

Soit $A \in Gl_2(\mathbb{Q})$ telle que $\begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$

Par définition $N(\Pi) = |\det A|$.

Remarque: Si l'on change de base pour Π et $\mathcal{O}_\Pi$ ($\Pi = \mathbb{Z}\alpha'_1 \oplus \mathbb{Z}\alpha'_2$ et $\mathcal{O}_\Pi = \mathbb{Z}\omega'_1 \oplus \mathbb{Z}\omega'_2$)

on a $\begin{pmatrix} \alpha'_1 \\ \alpha'_2 \end{pmatrix} = C \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$ et $\begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} = D \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$ avec C et $D \in Gl_2(\mathbb{Z})$ on a

$\det CAD^{-1} = \pm \det A$ et $\begin{pmatrix} \alpha'_1 \\ \alpha'_2 \end{pmatrix} = CAD^{-1} \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix}$

Lemme 3): Si Π est un module complet

1) Si $\lambda \neq 0$ $N(\lambda\Pi) = |N(\lambda)|\, N(\Pi)$

2) Si $\Pi = \mathbb{Z} \oplus \mathbb{Z}\alpha$ et $P_\alpha = uX^2 + vX + w$ alors $N(\Pi) = \frac{1}{u}$ (où $P_\alpha = P_{\text{minimal de } \alpha}$)

3) $\mathrm{Disc}\,\Pi = N(\Pi)^2\, \mathrm{Dis}\,\mathcal{O}_\Pi$

Exemple: Soit $\varphi(x,y) = ax^2+bxy+cy^2$ $(a>0$; $pgcd(a;b;c)=1$ et $D=b^2-4ac$ n'a carré)

on a $P_\alpha = aX^2+bX+c$ où $M = \mathbb{Z}\oplus\mathbb{Z}\alpha$ avec $\alpha = \frac{-b+\sqrt{D}}{2a}$, donc $N(M) = \frac{1}{a}$

et $\mathrm{Disc}\, M = \frac{b^2-4ac}{a^2} = N(M)^2 . \mathrm{Disc}\, \mathcal{O}_M$ donc $b^2-4ac = \mathrm{Disc}\, \mathcal{O}_M$.

Le discriminant de $\mathcal{O}_M$ est le même que celui de la forme binaire dont il provient. De plus $N(\varphi) = \frac{m}{a}$ s'écrit $N(\varphi) = m\, N(M)$

Définition: M_1 et M_2 deux modules complets, M_1M_2 est le sous-groupe additif de K engendré par $\{xy \,/\, x\in M_1$ et $y\in M_2\}$ pour $M_1 = \mathbb{Z}\alpha_1\oplus\mathbb{Z}\beta_1$ et $M_2 = \mathbb{Z}\alpha_2\oplus\mathbb{Z}\beta_2$ on a $M_1M_2 = \mathbb{Z}\alpha_1\alpha_2 + \mathbb{Z}\beta_2\alpha_1 + \mathbb{Z}\beta_1\alpha_2 + \mathbb{Z}\beta_1\beta_2$ ceci montre que c'est un module qui est complet car $\alpha_1\alpha_2$ et $\alpha_2\beta_2$ sont $\mathbb{Q}$-linéairement indépendants

Lemme 6) En notant M_f les modules complets associés à l'ordre $\mathcal{O}_f$ (rel que $\mathcal{O}_M = \mathcal{O}_f$)

1) M_f est un groupe abélien d'élément neutre $\mathcal{O}_f$ et $M^{-1} = \frac{1}{N(M)} M^\sigma$

2) $N : M \longrightarrow N(M)$ est morphisme du groupe M_f vers $\mathbb{Q}_+^*$

$M_f \longrightarrow \mathbb{Q}_+^*$

Démonstration:

on a $M\in M_f \Rightarrow M^\sigma \in M_f$ (propriété 1)

$M = \mathbb{Z}\alpha\oplus\mathbb{Z}\beta = \alpha(\mathbb{Z}\oplus\mathbb{Z}\gamma)$ où $\gamma = \beta/\alpha$ alors $MM^\sigma = \alpha\alpha^\sigma(\mathbb{Z}\oplus\mathbb{Z}\gamma)(\mathbb{Z}\oplus\mathbb{Z}\gamma^\sigma)$

$= N(\alpha)(\mathbb{Z}\oplus\mathbb{Z}\gamma+\mathbb{Z}\gamma^\sigma+\mathbb{Z}\gamma\gamma^\sigma)$

Mais $P_\gamma = uX^2+vX+w$ est le polynôme minimal de γ on a $\gamma+\gamma^\sigma = -\frac{v}{u}$

$\gamma\gamma^\sigma = N(\gamma) = \frac{w}{u}$ donc $MM^\sigma = N(\alpha)(\mathbb{Z}\frac{1}{u}\oplus\mathbb{Z}\gamma) = \frac{N(\alpha)}{u}(\mathbb{Z}\oplus\mathbb{Z}u\gamma) = \frac{N(\alpha)}{u}\mathcal{O}_f$

or $N(M) = |N(\alpha)|\, N(\mathbb{Z}\oplus\mathbb{Z}\gamma) = |N(\alpha)|\cdot\frac{1}{u}$ d'où

$$MM^\sigma = N(M)\mathcal{O}_f$$

Soient alors $M_1, M_2 \in M_f \Rightarrow N(M_1M_2)\cdot\mathcal{O}_{M_1M_2} = M_1M_2\cdot(M_1M_2)^\sigma = M_1M_1^\sigma M_2M_2^\sigma$

$= N(M_1)\mathcal{O}_f N(M_2)\mathcal{O}_f = N(M_1)N(M_2)\mathcal{O}_f$ d'où $\mathcal{O}_{M_1M_2} = r\mathcal{O}_f$ avec $r = \frac{N(M_1)N(M_2)}{N(M_1M_2)} \in \mathbb{Q}_+^*$

en prenant la norme $N(\mathcal{O}_{n_1 n_2}) = N(r\mathcal{O}_f)$ soit $1 = r^2$ donc $r = 1$

on a donc $\mathcal{O}_{n_1 n_2} = \mathcal{O}_f$ et N est un morphisme. Enfin $\mathcal{O}_f$ est l'élément neutre de Π_f car $n \subset n.\mathcal{O}_f \subset n$ donc $n.\mathcal{O}_f = n$. □

Définition : n_1 et n_2 sont dits semblables s'il existe $\alpha \neq 0 \in K$ tel que $n_1 = \alpha n_2$

il s'ensuit que $\mathcal{O}_{n_1} = \mathcal{O}_{n_2} = \mathcal{O}_f$, c'est une relation d'équivalence sur Π_f compatible avec la structure de groupe de Π_f. Le groupe quotient noté G_f est le groupe des classes de modules associés à $\mathcal{O}_f$

De même n_1 et n_2 sont strictement semblables si il existe $\alpha \neq 0$ et $N(\alpha) > 0$ tel que $n_1 = \alpha n_2$.

Théorème (" de la correspondance entre classes de nombres et de modules ")

Si $n > 0$ $\xi \longrightarrow \xi n^{-1} = A$ définit par passage au quotient une bijection entre les classes strictes d'association de nombre $\left\{ \xi \in M \atop N(\xi) = n N(M) \right\} \left([\xi] = \{ w\xi / w \in \mathcal{O}_M^* \text{ et } N(w) = 1 \} \right)$ et les modules complets A vérifiant : $\begin{cases} A \subset \mathcal{O}_M \\ \mathcal{O}_A = \mathcal{O}_M \\ N(A) = n \\ A \sim_s M^{-1} \end{cases}$

Démonstration :

Si $w \in \mathcal{O}_M^* / N(w) = 1$ alors $w\xi M^{-1} = \xi M^{-1}$ (car $wM^{-1} = M^{-1}$)

donc $[\xi] \longrightarrow \xi n^{-1}$ est bien définie

on a $\xi n^{-1} \subset \mathcal{O}_M$ (facile) et on a $\mathcal{O}_{\xi n^{-1}} = \mathcal{O}_{n^{-1}} = \mathcal{O}_M$

De plus $N(\xi n^{-1}) = N(\xi)/N(M) = \frac{n N(M)}{N(M)} = n$.

Montrons l'injectivité de l'application :

Si $\xi_1 n^{-1} = \xi_2 n^{-1} \Leftrightarrow \xi_1 \xi_2^{-1} n^{-1} = n^{-1} \Leftrightarrow \xi_1 \xi_2^{-1} \in \mathcal{O}_M^*$ mais $N(\xi_2) = N(\xi_2) \Rightarrow N(\xi_1 \xi_2^{-1}) = 1$

donc $(\xi_1) = (\xi_2)$

Si A vérifie les quatre conditions, il existe $\alpha \in K / N(\alpha) > 0$ tel que $A = \alpha n^{-1}$

Puisque $\alpha n^{-1} \subset \mathcal{O}_M \Rightarrow \alpha n^{-1} n \subset n \Rightarrow \alpha \in n$

Puisque $N(\alpha M^{-1}) = m$ on a $N(\alpha M^{-1}) = \frac{|N(\alpha)|}{N(M)} = m \Rightarrow N(\alpha) = m N(M)$ □

Nous disposons maintenant d'une méthode pour résoudre $\varphi(m,y) = m$ $(m>0)$

1) Trouver les unités de norme ± 1 de $\mathcal{O}_\Pi$ où $\Pi = \mathbb{Z} \oplus \mathbb{Z}\alpha$ $\left(\alpha = \frac{-b+\sqrt{D}}{2a}\right)$

2) Faire la liste des modules $A \subseteq \mathcal{O}_\Pi$ / $N(A) = m$

3) Extraire de cette liste les modules strictement semblables à Π^{-1}.

Le point 2) résulte du théorème suivant.

Théorème 2) "de la détermination des modules $A \subset \mathcal{O}_\Pi$, de norme m, et associés à $\mathcal{O}_\Pi$".

Soit $\mathcal{O}$ un ordre de K avec $\mathrm{Disc}\,\mathcal{O} = D$

Les modules A associés à $\mathcal{O}$, inclus dans $\mathcal{O}$ et de norme $n \geq 1$ sont fournis par les quadruplets $(s,u,v,w) \in \mathbb{N}^2 \times \mathbb{Z}^2$ tels que

$$\begin{cases} A = us\left(\mathbb{Z} \oplus \mathbb{Z}\left(\frac{-v+\sqrt{D}}{2u}\right)\right) \\ v^2 - 4uw = D \\ -u < v \leq u \\ \mathrm{pgcd}(u,v,w) = 1 \\ us^2 = m \end{cases}$$

Démonstration :

Soit $\mathcal{O}$ un ordre de K de discriminant D et soit $A \subseteq \mathcal{O}$ un module complet associé à $\mathcal{O}$ de norme m.

Soit $G = A \cap \mathbb{Z}$ et un sous groupe de $\mathbb{Z}$; $G \neq 0$ car si $\alpha \neq 0$, $\alpha \in A$ alors $\alpha \in \mathcal{O}$ donc $\alpha\alpha^\sigma \in \mathcal{O}$ et $\alpha\alpha^\sigma = N(\alpha) \in A \cap \mathbb{Z}$ ainsi $G = \mathbb{Z}h$, $h \geq 1$ est un sous groupe de rang 1 de A

Le théorème de la base incomplète montre que $A = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2$ et $G = \mathbb{Z} \cap \alpha_1$

Il $\mathbb{Z}h = \mathbb{Z} \cap \alpha_1$ on en déduit $n = h$ et $\alpha_1 = 1$ donc $A = \mathbb{Z}h \oplus \mathbb{Z}\alpha_2 = h\left(\mathbb{Z} + \mathbb{Z}\frac{\alpha_2}{h}\right)$

Le nombre $\gamma = \frac{\alpha_2}{h}$ est de forme précise : Soit $P_\gamma = uX^2 + vX + w$ son polynôme minimal

$v^2 - 4uw$ est le discriminant de $\mathcal{O}_{\mathbb{Z} \oplus \mathbb{Z}\gamma}$ donc de $\mathcal{O}$: $v^2 - 4uw = D$.

Plus $N(A) = m = h^2 N(\mathbb{Z} \oplus \mathbb{Z}\gamma) = \frac{h^2}{u}$ donc $mu = h^2$ et $\gamma = \frac{-v \pm \sqrt{D}}{2u}$, mais

$\mathbb{Z} \oplus \mathbb{Z}\gamma$ ne change pas si l'on change γ en $-\gamma$ ou si l'on translate γ d'un entier (ces deux opérations n'altèrent pas $\mathrm{Disc}(\gamma)$ on peut donc

Supposons que $\gamma = \frac{-v \pm \sqrt{D}}{2u}$ avec $-u < v \leq u$, par ailleurs $\forall \gamma \in A \subseteq \mathcal{O}$

et $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}u\gamma$ donc $\forall \gamma = m + nu\gamma$ et $k = nu$, u divise k, soit

$k = us$ $(s \geq 1)$. Ainsi à A on peut associer le quadruplet demandé.

Réciproquement soit (s,u,v,w) un tel quadruplet, posons $A = us\left(\mathbb{Z} \oplus \mathbb{Z}\left(\frac{-v+\sqrt{D}}{2u}\right)\right)$

alors $\mathcal{O}_A = \mathbb{Z} \oplus \mathbb{Z}\left(\frac{-v+\sqrt{D}}{2u}\right)$, le polynôme minimal de $\gamma = \frac{-v+\sqrt{D}}{2u}$

étant $P_\gamma = uX^2 + vX + w$. De plus on a $\mathrm{Disc}\,\mathcal{O}_A = D = v^2 - 4uw$ donc $\mathcal{O}_A = \mathcal{O}$.

$N(A) = u^2 s^2 \cdot \frac{1}{u} = us^2 = m$ en écrivant $A = s\left(\mathbb{Z} + \mathbb{Z}\left(\frac{-v+\sqrt{D}}{2u}\right)\right)$ on voit que

$A \subseteq \mathcal{O}_A = \mathcal{O}$

□

Le point 1) de la méthode de résolution de $\varphi(x,y) = m$ $(m > 0)$

résulte des fractions continuées que nous allons étudier en deuxième partie.

II) Fractions continuées et théorème de Dirichlet des unités pour un ordre d'un corps quadratique.

i) Calcul des réduites

Si $x \in \mathbb{R}$ $x>0$ on pose $x_0 = x$ et $u_0 = [x]$ (partie entière de x)

- si $x - u_0 = 0$ on s'arrête sinon
- on calcule $x_1 = \frac{1}{x-u_0} > 1$ de sorte que $x = u_0 + \frac{1}{x_1}$, puis on calcule $u_1 = [x_1] \geq 1$
- si $x_1 - u_1 = 0$ on s'arrête sinon on continue ...

Le procédé s'arrête dès que $x_n \in \mathbb{N}$ dans ce cas $x = u_0 + \cfrac{1}{u_1 + \cfrac{1}{\ddots u_{n-1} + \frac{1}{u_n}}}$

La suite finie ou non de u_n est le développement en fraction continue de x notée $[u_0, u_1, \dots, u_n, \dots]$ les u_n sont les quotients incomplets, $u_0 \geq 0$, $u_1 \geq 1$.

les x_n sont les quotients complets : $x_n = u_n + \frac{1}{x_{n+1}}$

la $n^{ième}$ réduite est le rationnel $[u_0, \dots, u_n] = u_0 + \cfrac{1}{u_1 + \cfrac{1}{\ddots u_{n-1} + \frac{1}{u_n}}}$

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$ on associe une bijection f de $\mathbb{R} \cup \{\infty\}$:

$$f : A \longrightarrow \tilde{A} : x \longrightarrow \begin{cases} \frac{ax+b}{cx+d} & \text{si } x \neq -\frac{d}{c} \\ \frac{a}{c} & \text{si } x = \infty \end{cases}$$

. On vérifie que f est un morphisme de groupe.

$\ker f = \mathbb{R}^* Id$ donc $Im f \cong \frac{GL_2(\mathbb{R})}{\mathbb{R}^*} = PGL_2(\mathbb{R})$ est le groupe de homographies.

Posons $A_0 = \begin{pmatrix} u_0 & 1 \\ 1 & 0 \end{pmatrix}$ et $H_{n+1} = H_n \times U_{n+1}$, $n \geq 0$ où $U_n = \begin{pmatrix} U_n & 1 \\ 1 & 0 \end{pmatrix}$

Comme $\det H_0 = -1$ on voit que $\det H_n = (-1)^{n+1}$.

Notons $H_n = \begin{pmatrix} P_n & p_n \\ Q_n & q_n \end{pmatrix}$

Posons $[u_0;\dots;u_n;a] = u_0 + \dfrac{1}{\dots + u_n + \frac{1}{a}}$ $(a \neq 0)$ alors

Proposition : 1)

$\widetilde{H}_n(x) = [u_0;\dots;u_n;x]$ pour $n \geq 0$ et $x > 0$

Démo : si $n=0$ on a $\widetilde{H}_0(x) = \dfrac{u_0 x + 1}{x} = u_0 + \dfrac{1}{x} = [u_0;x]$

Si c'est vrai jusqu'au rang n $[u_0;\dots;u_n;u_{n+1};a] = [u_0;\dots;u_{n+1};\frac{1}{a}]$

$= \widetilde{H}_n\left(u_{n+1} + \frac{1}{a}\right)$ (car $u_{n+1} \geq 0$)

$= \widetilde{H}_n\left(\dfrac{u_{n+1}a + 1}{a}\right) = \widetilde{H}_n \circ \widetilde{U}_{n+1}(x)$

$= \widetilde{H_n \times U_{n+1}}(x) = \widetilde{H}_{n+1}(x)$

Si $x \to +\infty$ on a $\widetilde{H}_n(+\infty) = [u_0;\dots;u_n] = \dfrac{P_n}{Q_n}$

On a $H_{n+1} = \begin{pmatrix} P_{n+1} & p_{n+1} \\ Q_{n+1} & q_{n+1} \end{pmatrix} = \begin{pmatrix} P_n & p_n \\ Q_n & q_n \end{pmatrix} \times \begin{pmatrix} u_{n+1} & 1 \\ 1 & 0 \end{pmatrix}$ donc

$$\begin{cases} P_{n+1} = P_n u_{n+1} + p_n \ , \ p_{n+1} = P_n \\ Q_{n+1} = Q_n u_{n+1} + q_n \ , \ q_{n+1} = Q_n \end{cases}$$

Soit pour $n \geq 2$ $\begin{cases} P_n = P_{n-1} u_n + P_{n-2} \\ Q_n = Q_{n-1} u_n + Q_{n-2} \end{cases}$

Si on pose $P_{-1} = 1$ $P_{-2} = 0$ $Q_{-1} = 0$ $Q_{-2} = 1$ ces formules sont vraies pour $n \geq 0$.

On a $P_n Q_{n-1} - P_{n-1} Q_n = \pm 1$

On vérifie que $\widetilde{H}_n^{-1}(x) = \dfrac{Q_{n-1}x - P_{n-1}}{-Q_n x + P_n}$

q) de suite $(P_n)_{n\geq 0}$ et $(Q_n)_{n\geq 0}$

On a $Q_0 = 1$ $Q_1 = u_1 \geq 1$ $Q_2 = u_2 Q_1 + Q_0 = u_2 Q_1 + 1 > u_2 Q_1 \geq Q_1$ donc $Q_2 > Q_1$

on voit alors que $1 = Q_0 \leq Q_1 < Q_2 \cdots < Q_{n-1} < Q_n < \cdots$

on en déduit que $\begin{cases} Q_{n+2} = u_{n+2} Q_{n+1} + Q_n \geq Q_{n+1} + Q_n > 2Q_n & n \geq 1 \\ Q_2 = u_2 Q_1 + Q_0 \geq Q_1 + Q_0 \geq 2Q_0 \end{cases}$

d'où $Q_{2n} > 2^n$ pour $n \geq 2$

$Q_{2n+1} > 2^n$ pour $n \geq 1$

Soit encore $Q_n Q_{n+1} > 2^n$ $(n \geq 1)$

Pour la suite (P_n) :

$P_0 = u_0 \geq 0$; $P_1 = 1 + u_0 u_1 > u_0 u_1 \geq u_0 = P_0$; $P_2 = P_1 u_2 + P_0 \geq P_1 + P_0 \geq P_1$

$P_3 = P_2 u_3 + P_1 \geq P_2 u_3 + 1 > P_2$ donc

$0 \leq u_0 = P_0 < P_1 \leq P_2 < P_3 < \dots < P_{n-1} < P_n < \dots$

on a d'autre part $P_n P_{n+1} > 2^{n-1}$ $n \geq 2$.

Proposition 2) Si α est irrationnel positif alors $\left| \frac{P_n}{Q_n} - \alpha \right| < \frac{1}{2^n}$ $(n \geq 1)$

Démonstration :

on a $\tilde{H}_n(\alpha) = \frac{P_n \alpha + P_{n-1}}{Q_n \alpha + Q_{n-1}}$ donc $\tilde{H}_n'(\alpha) = \frac{(-1)^{n+1}}{(Q_n \alpha + Q_{n-1})^2}$ donc $\tilde{H}_n$ est monotone (si $\alpha \in \mathbb{R}$)

• Si n est pair $\tilde{H}_n$ est strictement décroissante donc $\alpha_{n+1} < u_{n+2} + \frac{1}{u_{n+2}} < +\infty$ implique :

$\tilde{H}_n(+\infty) < \tilde{H}_n\left(u_{n+2} + \frac{1}{u_{n+2}}\right) < \tilde{H}_n(\alpha_{n+1})$. Soit $\frac{P_n}{Q_n} < \frac{P_{n+2}}{Q_{n+2}} < \alpha$.

• Si n est impair $\tilde{H}_n$ est strictement croissante et cette fois $\frac{P_n}{Q_n} > \frac{P_{n+2}}{Q_{n+2}} > \alpha$.

Cela prouve que $\left(\frac{P_{2n}}{Q_{2n}}\right)_{n \geq 0}$ est croissante et majorée par α, que $\left(\frac{P_{2n+1}}{Q_{2n+1}}\right)_{n \geq 0}$ est décroissante et minorée par α, mais de plus $\left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| = \left| \frac{(-1)^n}{Q_n Q_{n+1}} \right| = \frac{1}{Q_n Q_{n+1}} < \frac{1}{2^n}$

$n \geq 1$, donc ces suites sont adjacentes de limite commune α, il s'ensuit que $\forall n \geq 1$

$\left| \frac{P_n}{Q_n} - \alpha \right| \leq \left| \frac{P_n}{Q_n} - \frac{P_{n+1}}{Q_{n+1}} \right| < \frac{1}{2^n}$ on peut donc écrire :

$$\alpha = \lim_{n \to +\infty} \frac{P_n}{Q_n} = \lim_{n \to +\infty} [u_0; \dots, u_n] = [u_0; \dots, u_n \dots]$$

□

Lemme 1) (Unicité)

Si $x = v_0 + \cfrac{1}{v_1 + \cfrac{1}{v_2 + \cfrac{1}{\ddots + \frac{1}{z}}}}$ avec $v_0 \geq 0$ $v_i \geq 1$ $(i \geq 1)$ avec $z > 1$

alors $[v_0; \dots; v_n]$ est la $n^{ième}$ réduite de x et z son $(n+1)^{ième}$ quotient complet.

Démonstration :

Posons pour $i = 0; \dots; n$ $y_i = v_i + \cfrac{1}{v_{i+1} + \ddots \cfrac{1}{v_n + \frac{1}{z}}}$; on a $y_i = v_i + \frac{1}{y_{i+1}} > 1$, en prenant $y_{n+1} = z > 1$

$y_0 = x = v_0 + \frac{1}{y_1}$ montre que $v_0 = \lfloor x \rfloor$, premier quotient incomplet de x et y_1 premier quotient complet. $y_1 = v_1 + \frac{1}{y_2}$ et $y_2 > 1$ etc... cela se poursuit jusqu'à $y_n = v_n + \frac{1}{z}$ montrant que v_n est quotient incomplet, et z le $(n+1)^{ième}$ quotient complet □

Proposition 3) (Développement d'un rationnel)

1) Pour $x > 0$ rationnel, de développement $[u_0; \dots; a_n]$, on a $u_n \geq 2$

2) Deux fractions finies différentes, représentent le même rationnel si seulement pour :

$[u_0; \dots u_{n-2}; u_{n-1} + 1] = [u_0; \dots; u_{n-2}; u_{n-1}; 1] = x$.

La première écriture est le développement en fraction continue de x, les réduites respectives :

$\frac{P_i}{Q_i}$ et $\frac{P'_i}{Q'_i}$ sont les mêmes pour $i \leq n-2$ et $\frac{P_{n-1}}{Q_{n-1}} = \frac{P'_{n-1} + P'_{n-2}}{Q'_{n-1} + Q'_{n-2}} = \frac{P'_n}{Q'_n}$

Démonstration :

1) Si $x = \frac{p_0}{q_0}$ on a $p_0 = u_0 q_0 + q_1$, $q_1 < q_0 \dots$ et $q_{n-1} = u_n q_n + q_{n+1}$ avec $q_{n+1} = 0$;

Comme $q_n < q_{n-1}$ nécessairement $u_n \geq 2$.

2) Supposons $[u_0; \dots, u_n) = [v_0; \dots; v_m] = x$ et soient x_i, y_i les quotients complets successifs

on a pour tout i : $x = u_0 + \cfrac{1}{\ddots u_i + \frac{1}{x_i}} = v_0 + \cfrac{1}{\ddots v_i + \frac{1}{x_i}}$ pour $i \leq m$; $i \leq n$

en appliquant le lemme tant que $x_i > 1$ et $y_i > 1$ on aura $u_0 = v_0, \dots, u_i = v_i$ comme quotients incomplets du développement de x et $x_i = y_i$, si cela a lieu jusqu'à $i = k-1$

alors x_k ou y_k vaut 1, supposons par exemple $x_k = 1$ alors $k = n$ (sinon l'égalité

$1 = r_k = u_k + \frac{1}{r_{k+1}}$ implique $u_k < 1$ et $x_n = u_n = 1$ d'où $y_{n-1} = x_{n-1} = u_{n-1} + \frac{1}{x_n} = u_{n-1} + 1$

Si $m = n-1$ on a $v_{n-1} = u_{n-1} + 1$, sinon $m \geq n$ $y_{n-1} = v_{n-1} + \frac{1}{y_n} = u_{n-1} + 1$

impose $y_n = 1 = x_n$ donc $m = n$ et les fractions sont les mêmes □.

Lemme 2):

Soit $F \in \mathbb{Q}_2(Z)$, $\tilde{F}(z) = \frac{Pz + P'}{Qz + Q'}$, on suppose $Q > Q' > 0$, P et P' positifs, alors pour tout $z > 1$ $\frac{P'}{Q'}$ et $\frac{P}{Q}$ sont deux réduite consécutive de $\tilde{F}(z)$ et z est le quotient complet suivant.

Démonstration:

On a $PQ' - QP' = \pm 1$. Par ailleurs $\frac{P}{Q}$ admet deux représentations (Proposition 3) dont la longueur diffère d'une unité: on choisit celle $[u_0, \dots, u_n]$ pour laquelle $PQ' - QP' = (-1)^{n+1}$

on a $\frac{P_n}{Q_n} = \frac{P}{Q}$ donc $P = P_n$ et $Q = Q_n$ on $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^n = PQ' - P'Q = P_n Q' - P' Q_n$

d'où : $P_n (Q_{n-1} - Q') = Q_n (P_{n-1} - P')$ donc $Q_n \mid Q_{n-1} - Q'$ mais $Q_{n-1} - Q' \leq Q_n - Q' < Q_n$

et finalement $Q' = Q_{n-1}$ et $P' = P_{n-1}$ alors $\tilde{F}(z) = \tilde{H}_n(z) = u_0 + \cfrac{1}{\ddots u_n + \frac{1}{z}}$

en appliquant le lemme 2) $[u_0, \dots, u_n] = \frac{P}{Q}$ et la $n^{\text{ième}}$ réduite de $\tilde{F}(z)$ et z est le quotient complet suivant □.

Proposition 3) (Legendre)

Si le rationnel $\frac{p}{q}$ réalise $|x - \frac{p}{q}| < \frac{1}{2q^2}$ alors $\frac{p}{q}$ est réduite de x.

Démonstration:

Si $\frac{p}{q} > x$ (resp $\frac{p}{q} < x$) on représente $\frac{p}{q}$ par le développement $[u_0, \dots, u_n]$ pour lequel $\tilde{H}_n(z) = \frac{P_n z + P_{n-1}}{Q_n z + Q_{n-1}}$ est croissante (resp décroissante): $\tilde{H}_n(1) = \frac{P_n + P_{n-1}}{Q_n + Q_{n-1}}$ est entre $\tilde{H}_n(0) = \frac{P_{n-1}}{Q_{n-1}}$ et $\tilde{H}_n(\infty) = \frac{P_n}{Q_n} = \frac{p}{q}$ mais $\left| \tilde{H}_n(1) - \frac{P_n}{Q_n} \right| = \frac{1}{Q_n (Q_n + Q_{n-1})} \geq \frac{1}{2Q_n^2}$

et l'hypothèse $\left| x - \frac{P_n}{Q_n} \right| < \frac{1}{2Q_n^2}$ montre que x se trouve entre $\frac{P_n}{Q_n}$ et $\tilde{H}_n(1)$ donc entre $\tilde{H}_n(\infty)$ et $\tilde{H}_n(1)$; il existe donc $z > 1$ tel que $\tilde{H}_n(z) = x$.

Si $Q_n > Q_{n-1} > 0$ on peut appliquer le lemme 2) et conclure que $\frac{P_n}{Q_n} = \frac{p}{q}$ est réduite de x.

Ceci a lieu pour $n \geq 2$. Si $n=1$ on aura soit $\frac{p}{q} = a_0 + \frac{1}{a_1}$ avec $a_1 \geq 2$ donc $Q_1 = a_1 \geq 2 > Q_0$ donc le lemme 2) s'applique, soit $\frac{p}{q} = a_0 + 1 \in \mathbb{N}$. Il reste donc à étudier le cas $\frac{p}{q} = a \in \mathbb{N}$: $a - \frac{1}{2} < x < a + \frac{1}{2}$ implique que soit $\lfloor x \rfloor = a = \frac{p}{q}$ soit $\lfloor x \rfloor = a-1$ d'où $x = a-1 + \frac{1}{x_1}$ avec $x_1 = \frac{1}{x - a + 1}$ et on vérifie $\lfloor x_1 \rfloor = 1$ donc $a-1+1 = a$ est bien réduite de x.

Définition : x et y deux irrationnels positifs x et y sont dits équivalents s'ils ont même développement en fraction continue à partir d'un certain rang.
La relation $x \sim y$ est une relation d'équivalence.

Proposition 4) (Caractérisation de l'équivalence)
Soient x et y deux irrationnels positifs :
$x \sim y \iff$ il existe $F \in GL_2(\mathbb{Z})$ telle que $F(x) = y$

Preuve : • Si $x \sim y$, $x = [a_0; a_1, a_2, \dots]$ et $y = [b_0; \dots, b_j, \dots]$, $\exists m, n$ entiers positifs tels que $\forall j \geq 0$ $a_{n+j} = b_{m+j}$ donc $x = H_n(x_{n+1})$ et $y = K_m(y_{m+1})$ où $x_{n+1} = [a_{n+1}, \dots] = [b_{m+1}, \dots] = y_{m+1}$
donc $y = \widetilde{K_m}(x_{n+1}) = \widetilde{K_m H_n^{-1}}(x)$.

• Réciproquement si $y = \widetilde{F}(x) = \frac{ax+b}{cx+d}$, on peut supposer $cx+d > 0$, $y > 0 \Rightarrow ax+b > 0$
On a $x = \widetilde{H_n}(x_{n+1})$ donc $y = \widetilde{F_x H_n}(x_{n+1}) = \frac{(aP_n + bQ_n)x_{n+1} + aP_{n-1} + bQ_{n-1}}{(cP_n + dQ_n)x_{n+1} + cP_{n-1} + dQ_{n-1}} = \frac{R_n x_{n+1} + R_{n-1}}{S_n x_{n+1} + S_{n-1}}$

Comme $\frac{P_n}{Q_n} \xrightarrow[n \to +\infty]{} x$ et que $ax+b > 0$ on a $a\frac{P_n}{Q_n} + b > 0$ à partir d'un certain rang et $Q_n > 0$ implique $R_n = aP_n + bQ_n > 0$ pour n grand, de même $cx+d > 0 \Rightarrow S_n = cP_n + dQ_n > 0$ (pour n grand)
Si on trouve n tel que $S_n > S_{n-1} > 0$ on applique le lemme 2) et on en déduira que x_{n+1} est quotient complet de y donc que $x \sim y$, on déjà $S_{n-1} > 0$ pour n grand et $S_n > S_{n-1}$ s'écrit $c(P_n - P_{n-1}) > d'(Q_{n-1} - Q_n)$.
Soit $c\frac{P_n - P_{n-1}}{Q_n - Q_{n-1}} > -d$. Posons $F_n(z) = \frac{P_n z - P_{n-1}}{Q_n z - Q_{n-1}}$ alors $\det f_n = (-1)^n$ et F_n est sans pôle

sur $[t;+\infty[$:

Il faut donc voir si : $c.F_n(t) > -d$

- si $c>0$, pour n impair F_n est décroissante donc $F_n(t) \geqslant F_n(+\infty) = \frac{P_n}{Q_n} \longrightarrow x$ et comme $n > -\frac{d}{c}$, on est assuré que $F_n(t) > -\frac{d}{c}$ pour n impair assez grand

- si $c<0$, pour n pair f_n croissante donc $F_n(t) \leqslant F_n(+\infty) = \frac{P_n}{Q_n} \longrightarrow x < -\frac{d}{c}$ donc $F_n(t) < -\frac{d}{c}$ pour n pair assez grand.

- si $c=0$, $ct+d>0 \Rightarrow d>0$ donc $c.F_n(t) > -d$.

3) Nombre quadratique réel et développements périodiques -

Définition : Soit x un irrationnel strictement positif. Si le développement de x est $x = [u_0; \dots; u_r; u_{r+1}; \dots; u_{r+t}; u_{r+1}; \dots; u_{r+t}; \dots] \quad (u_{r+kt+j} = u_{r+j}$ pour $k \geqslant 1$ et $1 \leqslant j \leqslant t)$

x est dit périodique : $[u_0; \dots; u_r]$ est la partie irrégulière et $[u_{r+1}; \dots; u_{r+t}]$ est la période, de longueur $t \geqslant 1$.

Proposition 5) (Euler)

Tout irrationnel périodique est un nombre quadratique réel.

Démonstration :

$x = [u_0; \dots; u_r; \overline{u_{r+1}; \dots; u_{r+t}}]$, on a $x = \widetilde{H}_{r+1}(x_{r+1}) = \widetilde{H}_{r+t+1}(x_{r+t+1})$ mais

$x_{r+t+1} = [u_{r+t+1}; \dots] = [u_{r+1}; \dots] = x_{r+1}$, de sorte que $x = \widetilde{H}_{r+1}(x_{r+1}) = \widetilde{H}_{r+t+1}(x_{r+1})$

et $x = \widetilde{H_{r+1} \times H_{r+t+1}^{-1}}(x) = \frac{axc+b}{cx+d}$ où $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ donc $cx^2 + (d-a)x - b = 0 \quad (c \neq 0)$ □

En fait la réciproque est vraie, c'est l'objet de la prochaine proposition.

Proposition 6) :

Soit $x > 0$ un irrationnel de $\mathbb{Q}(\sqrt{d})$ de discriminant $D = Disc(x) = b^2 - 4ac$ ($P_x = ax^2 + bx + c$)

1) $\forall n \geqslant 0 \quad x_n \notin \mathbb{Q}$ et $Disc(x_n) = D$

2) Si $P_{x_n} = a_n X^2 + b_n X + c_n$ alors $\pm P_{x_{n+1}} = P_{x_n}(u_n)X^2 + (b_n + 2a_n u_n)X + a_n$

Preuve :

$x_n = u_n + \frac{1}{x_{n+1}} = u_n + y$ avec $y = x_n - u_n \in \mathbb{Q}(\sqrt{d})$; $P_y = a_n X^2 + (b_n + 2a_n u_n)X + c_n + (b_n + a_n u_n)u_n$

En effet $y \notin \mathbb{Q}$, $P_y(y)=0$ et P_y est primitif car si d divise ses coefficient $d|a_n$; $d|b_n+2a_nu_n$ (donc $d|b_n$) et $d|c_n+(b_n+a_nu_n)u_n$ alors $d|c_n$ donc $d|PGCD(a_n,b_n,c_n)=1$. De plus $Disc\ y=(b_n+2a_nu_n)^2-4a_n(c_n+(b_n+a_nu_n)u_n)$

$=b_n^2-4a_nc_n=D$

Si $P_y=aX^2+bX+c$ alors $\pm P_{\frac{1}{y}}=cX^2+bX+a$ (selon le signe de c).

De plus $Disc(cX^2+bX+a)=b^2-4ac=Disc(y)$ comme $c_n+(b_n+a_nu_n)v_n=P_{a_n}(v_n)$ ceci achève la preuve. ▷.

Définition: Soit $x\in\mathbb{Q}(\sqrt{d})$, $x\notin\mathbb{Q}$ si $x>1$ et $-1<x^\sigma<0$ x est dit réduit.

Proposition 7):
Soit $x>0$ un irrationnel de $\mathbb{Q}(\sqrt{d})$ alors x est périodique simple si et seulement si x est périodique réduit.

Preuve:
1) Montrons en premier lieu que si x est réduit, tous ses quotients complets le sont, pour cela il suffit de montrer que x_n réduit implique x_{n+1} réduit or $x_{n+1}=\frac{1}{x_n-u_n}$ $x_{n+1}^\sigma=\frac{1}{x_n^\sigma-u_n}$

on a $x_n^\sigma<0$ (on montre que $x_n^\sigma-u_n<0$ donc $x_{n+1}^\sigma<0$.

$x_{n+1}^\sigma>-1 \Leftrightarrow u_n-x_n^\sigma>1 \Leftrightarrow x_n^\sigma+1<u_n$ mais $x_n^\sigma+1<1$ et $1\leq u_n$ c'est donc vrai ($u_n\geq 1$ car $x_n>1$ par hypothèse).

$x_{n+1}>1$ car c'est un quotient complet d'irrationnel.

b) Si x est périodique réduit et possède une partie irrégulière de longueur t:

$x=[u_0;\dots u_r;\overline{u_{r+1};\dots u_{r+t}}]$ on a $x_{r+t+1}=x_{r+1}$ donc en redescendant:

$x_r=u_r+\frac{1}{x_{r+1}}$ d'où $x_r^\sigma=u_r+\frac{1}{x_{r+1}^\sigma}$ $x_{r+t}=u_{r+t}+\frac{1}{x_{r+t+1}}$ d'où $x_{r+t}^\sigma=u_r+\frac{1}{x_{r+t+1}^\sigma}$

et $|x_r^\sigma-x_{r+t}^\sigma|=|u_r-u_{r+t}|$. Mais comme $-1<x_r^\sigma$; $x_{r+t}^\sigma<0$ d'après a) ceci n'est possible que si $u_r=u_{r+t}$ donc aussi: $x_r^\sigma=x_{r+t}^\sigma$ et $x_r=x_{r+t}$, donc la partie irrégulière serait de longueur $r-1$, impossible.

c) Si x périodique simple $x=[\overline{u_0;\dots;u_{t-1}}]$ de période $t\geq 1$, $u_t=u_0\Rightarrow u_0\geq 1$ donc $x>1$

$x_t=x_0=x\Rightarrow x=\tilde{H}_t(x_t)=\tilde{H}_t(x)=\frac{P_tx+P_{t-1}}{Q_tx+Q_{t-1}}$ donc x est racine de $f=Q_tX^2+(Q_{t-1}-P_t)X-P_{t-1}$

donc x^σ est aussi racine de f ; or $f(-1) = Q_t - Q_{t-1} + P_t - P_{t-1} > 0$ et $f(0) = -P_{t-1} < 0$

donc f s'annule entre -1 et 0 : $-1 < x^\sigma < 0$ donc x est réduit. □.

Proposition 8)

i) Tout réduit de discriminant D s'écrit de façon unique $x = \frac{B + \sqrt{D}}{2A}$ où

$\begin{cases} D = B^2 + 4AC \\ PGCD(A,B,C) = 1 \\ A,B,C > 0 \end{cases}$ et $P_x = AX^2 - BX - C$. Un tel nombre est toujours réduit.

ii) Le nombre de réduits de discriminant D ne dépasse pas $\frac{1}{2}[\sqrt{D}]^2$

iii) Si $P_{x_n} = A_n X^2 - B_n X - C_n$ est le polynôme minimal du $n^{ième}$ quotient complet x_n du réduit x alors :

- $A_{n+1} = -A_n u_n^2 - B_n u_n - C_n = -P_{x_n}(u_n)$
- $B_{n+1} = 2A_n u_n - B_n$
- $C_{n+1} = A_n$

iv) x réduit équivaut à x périodique simple.

Démo :

i) Soit x réduit $P_x = aX^2 + bX + c$ donc $x = \frac{-b \pm \sqrt{D}}{2a}$; comme $-1 < x^\sigma < 0$ et $1 < x$, on a

$x + x^\sigma = -\frac{b}{a} > 0$ donc $b < 0$ et $x x^\sigma = \frac{c}{a} < 0$ donc $c < 0$ en posant

$A = a \quad B = -b \quad C = -c$ on voit que $x = \frac{B \pm \sqrt{D}}{2A}$ et $D = b^2 - 4ac = B^2 + 4AC$

enfin $\frac{B - \sqrt{D}}{2A} < \frac{B + \sqrt{D}}{2A}$ et le fait que $x^\sigma < x$ montrent que $x = \frac{B + \sqrt{D}}{2A}$; il est clair que $PGCD(A,B,C) = PGCD(a;b;c) = 1$, on exprime $-1 < x^\sigma < 0$ par $P_x(-1) > 0$ ($P_x(0) = -c < 0$) soit $A - B - c < 0$ soit $A + B - c > 0$, on exprime $x > 1$ par $P_x(1) < 0$ (1 est entre les racines) soit $A - B - c < 0$

donc $|A - c| < B$.

Réciproquement $x = \frac{B + \sqrt{D}}{2A}$ a pour polynôme minimal $P_x = AX^2 - BX - C$, son conjugué est $x^\sigma = \frac{B - \sqrt{D}}{2A} < x$; pour voir que x est réduit il suffit donc d'établir que 0 et 1 sont entre les racines et que $P_x(-1) \geq 0$. On $P_x(0) = -C < 0$; $P_x(1) = A - B - C < 0$ et $P_x(-1) = A + B - C > 0$

ii) on a pour $x = \frac{B + \sqrt{D}}{2A}$ réduit ; $D = B^2 + 4AC \geq (A - C)^2 + 4AC = (A + C)^2$ donc $A + C \leq \sqrt{D}$

donc $1 \leq A \leq [\sqrt{D}]$ et $1 \leq C \leq [\sqrt{D}]$; comme un tel choix de A et C fixe aussi B

il y a au plus $(\sqrt{D})^2$ réduits possibles.

De $A+C \leq \lfloor \sqrt{D} \rfloor$ on a qu'il y a au plus $\sum_{n=1}^{\lfloor \sqrt{D} \rfloor - 1} n$ choix de couple (A, C)

donc moins de $\frac{(\lfloor \sqrt{D} \rfloor - 1)\lfloor \sqrt{D} \rfloor}{2} < \frac{1}{2}(\sqrt{D})^2$ réduit possible

iii) D'après la Prop 6) : x_n étant réduit on a $x_n^\sigma < 0$ et $-1 < x_n$

donc $P_{n-1}(u_n) < 0$ d'où le signe et la valeur de A_{n+1}.

iv) La prop 7) montre qu'un réduit est périodique, mais si $x = \frac{B+\sqrt{D}}{2A}$ et réduit ses quotients complets le sont aussi et comme il y a un nombre fini de réduits possibles, nécessairement il existe $m > n$ tels que $x_m = x_n$ donc x est périodique □.

Théorème (Lagrange)

Soit x un irrationnel strictement positif de $\mathbb{Q}(\sqrt{d})$ alors l'un de quotients complets x_n de x est réduit.

Preuve: Soit $x = [u_0; u_1; \dots; u_n; \dots]$

$x_n = \widetilde{H}_{n-1}^{-1}(x) = -\frac{Q_{n-1}x - P_{n-1}}{Q_n x - P_n} = -\frac{Q_{n-1}}{Q_n}\left(\frac{x - \frac{P_{n-1}}{Q_{n-1}}}{x - \frac{P_n}{Q_n}}\right)$, soit en conjuguant

$x_n^\sigma = -\frac{Q_{n-1}}{Q_n}\left(\frac{x^\sigma - \frac{P_{n-1}}{Q_{n-1}}}{x^\sigma - \frac{P_n}{Q_n}}\right)$. Or $\frac{P_n}{Q_n} \longrightarrow x$ et $x \neq x^\sigma$ donc

$\frac{x^\sigma - \frac{P_{n-1}}{Q_{n-1}}}{x^\sigma - \frac{P_n}{Q_n}} \longrightarrow \frac{x^\sigma - x}{x^\sigma - x} = 1$ cela prouve que, Q_n étant positif strictement

$x_n^\sigma < 0$ pour n grand. Montrons que $x_n^\sigma + 1 > 0$ pour n grand :

$$x_n^\sigma + 1 = 1 - \frac{Q_{n-1}x^\sigma - P_{n-1}}{Q_n x^\sigma - P_n} = 1 - \frac{Q_{n-1}}{Q_n}\left(\frac{x^\sigma - \frac{P_{n-1}}{Q_{n-1}}}{x^\sigma - \frac{P_n}{Q_n}}\right) = 1 - \frac{Q_{n-1}}{Q_n} + \frac{Q_{n-1}}{Q_n}\left(\frac{\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}}}{x^\sigma - \frac{P_n}{Q_n}}\right)$$

$$= 1 - \frac{Q_{n-1}}{Q_n} + \frac{1}{Q_n^2}\left(\frac{\pm 1}{x^\sigma - \frac{P_n}{Q_n}}\right) = \frac{1}{Q_n}\left(Q_n - Q_{n-1} + \frac{1}{Q_n}\left(\frac{\mp 1}{x^\sigma - \frac{P_n}{Q_n}}\right)\right).$$

On $\frac{1}{Q_n} \to 0$ et $\frac{1}{x^\sigma - \frac{P_n}{Q_n}} \to \frac{1}{x^\sigma - x}$ donc $\frac{1}{Q_n} \cdot \frac{\pm 1}{x^\sigma - \frac{P_n}{Q_n}} \to 0$ et comme

$Q_n > Q_{n-1}$ on a $x_n^\sigma + 1 > 0$ pour n grand. □

Conséquence : x est donc périodique.

4) Application au théorème des unités "quadratique"

Rappel : Si $d \equiv 2,3 \ [4]$ $w = \sqrt{d}$ $P_w = X^2 - d$; $T_n(w) = 0$; $N(w) = -d$ $\mathrm{Disc}(\mathcal{O}_f) = 4df^2$

Si $d \equiv 1 \ [4]$ $w = \frac{1+\sqrt{d}}{2}$ $P_w = X^2 - X - \frac{d-1}{4}$ $T_n(w) = 1$; $N(w) = -\left(\frac{d-1}{4}\right)$; $\mathrm{Dis}\, \mathcal{O}_f = df^2$.

Théorème (Legendre)

Soit $\mathcal{O}_f$ un ordre du corps quadratique réel $K = \mathbb{Q}(\sqrt{d})$ et $D = f^2 \mathrm{Disc}(\mathcal{O}_K)$

i) $-f w^\sigma = -\frac{f T_n(w) + \sqrt{D}}{2} > 0$

ii) Si $f = 1$ et $d = 5$: $-f w^\sigma = [\overline{u_1; \dots; u_t}] = [\overline{1}]$ sinon

ii') $-f w^\sigma = [u_0; \overline{u_1, \dots, u_t}]$ avec $u_t = 2a_0 + f T_n(w)$, de plus le deux réduits :

$[\overline{u_1, u_2 \dots, u_{t-1}}]$ et $[\overline{u_{t-1}; \dots; u_2, u_1}]$ sont égaux $u_{t-i} = u_i$ pour $1 \leq i \leq t-1$

et si $x_i = \frac{B_i + \sqrt{D}}{2A_i}$ est le $i^{\text{ième}}$ quotient complet de $-f w^\sigma$ on a pour $1 \leq i \leq t-1$

$A_{t-i} = A_i = C_{i+1}$ et $B_{t-i} = B_{i+1}$.

iii) Si $\frac{P_n}{Q_n}$ et la $n^{\text{ième}}$ réduite de $-f w^\sigma$ alors $\gamma = P_{t-1} + Q_{t-1} f w$ est une unité de l'anneau $\mathcal{O}_f$, sa norme est $(-1)^t$.

Preuves : a) Soit $P_0 = A_0 X^2 - B_0 X - C_0$ le polynôme minimal de $-f w^\sigma$: $A_0 = 1$ car $-f w^\sigma \in \mathcal{O}_K$, $B_0 = T_n(-f w^\sigma) = -f T_n(w)$; $-C_0 = N(-f w^\sigma) = f^2 N(w)$

$A_0 = 1$ $B_0 = -f T_n(w)$ $C_0 = -f^2 N(w)$ donc $-f w^\sigma = \left(-f T_n w \pm \sqrt{D}\right)/2$ mais $-f w^\sigma = f\sqrt{d}$

or $f(\sqrt{d} - 1)/2$ est positif d'où le signe + et $-f w^\sigma = \left(-f T_n w + \sqrt{D}\right)/2$

ii) $-f w^\sigma = a_0 + \frac{1}{a_1}$ donc $x_1 = \frac{-1}{f w^\sigma + a_0}$; $x_1^\sigma = \frac{-1}{f w + a_0} < 0$ car $a_0 + f w > 0$ et $|x_1^\sigma| = \frac{1}{a_0 + f w} < 1$

puisque $a_0 + f w \geq f w \geq w > 1$:

Si $d \equiv 2,3 \ [4]$ $w = \sqrt{d} \geq \sqrt{2} > 1$; Si $d \equiv 1 \ [4]$ $w = \left(\frac{1+\sqrt{d}}{2}\right) \geq \left(\frac{1+\sqrt{5}}{2}\right) > 1$

u_1 étant réduit on a $C_1 > 0$ et $C_1 = 1$ $B_1 = 2A_0 u_0 - B_0$; $A_1 = -P_0(u_0)$

donc $A_1 = -(u_0^2 + f u_0 T_n w + f^2 w w^\sigma) = -N(u_0 + f w)$

De $D = B_t^2 + 4C_t$ on déduit $B_t < \sqrt{D}$ et $|C_t - A_t| \leq B_t$:

$C_t - A_t = D - \frac{B_t^2 - 4}{4} < B_t$ donc $D < 4B_t + B_t^2 + 4 = (B_t + 2)^2$ et $\sqrt{D} < B_t + 2$

et $-f w^\sigma = -\frac{f T_n(w) + \sqrt{D}}{2} < -\frac{f T_n(w) + B_t}{2} + 1$ mais $\sqrt{D} > B_t$ donc

$-f w^\sigma > -\frac{f T_n w + B_t}{2}$.

D'autre part :

$$\begin{cases} A_{t+1} = A_1 \\ B_{t+1} = B_1 \\ C_{t+1} = C_1 \end{cases} \text{ donc } \begin{cases} -u_t^2 + u_t B_t + C_t = -N(u_0 + f w) \\ 2u_t A_t - B_t = 2u_0 + f T_n(w) \\ A_t = 1 \end{cases}$$

Exprimons maintenant A_n, C_n, B_n avec les réduits $\frac{P_n}{Q_n}$:

$$u_n = \widehat{H_{n-1}}^{-1}(-f w^\sigma) = \frac{Q_{n-2}(-f w^\sigma) - P_{n-2}}{-Q_{n-1}(-f w^\sigma) + P_{n-1}} = \frac{-P_{n-1}P_{n-2} - Q_{n-1}Q_{n-2} f^2 N(w) + E}{N(P_{n-1} + Q_{n-1} f w)}$$

où $E = -P_{n-2}Q_{n-1} f w - P_{n-1}Q_{n-2} f w^\sigma = (-1)^n f w - P_{n-1}Q_{n-2} f T_n(w)$ mais comme $f w = \frac{f T_n(w) + \sqrt{D}}{2}$

$$u_n = \frac{-P_{n-1}P_{n-2} - Q_{n-1}Q_{n-2} f^2 N(w) + (-1)^n \times \left(\frac{f T_n(w) + \sqrt{D}}{2}\right) - P_{n-1}Q_{n-2} f T_n(w)}{N(P_{n-1} + Q_{n-1} f w)}$$

On en déduit :

$$A_n = (-1)^n N(P_{n-1} + Q_{n-1} f w)$$

$$B_n = 2(-1)^n (P_{n-1}P_{n-2} + Q_{n-1}Q_{n-2} f^2 N(w) + f P_{n-1}Q_{n-2} T_n(w)) + f T_n(w)$$

$$C_n = (-1)^{n-1} N(P_{n-2} + Q_{n-2} f w) \quad (\text{car } C_n = A_{n-1})$$

Si $n = t$ on a $A_t = 1$ donc $N(P_{t-1} + Q_{t-1} f w) = (-1)^t$ □

Théorème des unités de Dirichlet (Cas quadratique)

Soit $\mathcal{O}=\mathcal{O}_f$ un ordre de $\mathbb{Q}(\sqrt{d})$ avec $-f\omega^\sigma=[u_0;\overline{u_1;\dots,u_t}]$

Si $\frac{P_{t-1}}{Q_{t-1}}$ est la $(t-1)^{ième}$ réduite $\gamma_0=\gamma_f=P_{t-1}+Q_{t-1}f\omega$ et $N(\gamma_0)=(-1)^t$ alors

1) γ_0 est la plus petite unité de $\mathcal{O}$ supérieure à 1 (c'est l'unité fondamentale de $\mathcal{O}$) et si $\gamma>1$ est une unité alors $\gamma=\gamma_0^n=P_{nt-1}+Q_{nt-1}f\omega \quad n\geq 1$

2) $\mathcal{O}^*=\pm(\gamma_0)^{\mathbb{Z}}=\{\pm(\gamma_0)^n / n\in\mathbb{N}\}$

3) $\mathcal{O}_1^*/\mathcal{O}_p^*$ est cyclique d'ordre 1, où $\gamma_1=\gamma_f$.

Démonstration :

i) Soit $E=\{\gamma\in\mathcal{O}^* / \gamma>1\}$. Si $\gamma=x+yf\omega\in E$ on a $y>0$ car $\omega-\omega^\sigma=2\sqrt{d}$ ou $\sqrt{d}>0$

donc $\gamma-\gamma^\sigma=\gamma\pm\frac{1}{\gamma}>0 \Rightarrow yf(\omega-\omega^\sigma)>0$ et $y>0$; $\frac{1}{\gamma}=|\gamma^\sigma|=|x+yf\omega^\sigma|<1$

$\Rightarrow x>-1-yf\omega^\sigma$, donc on va prouver que $x>0$ sauf dans un seul cas :

* Si $f\neq 1$ ou $d\neq 5$ on a déjà prouvé que $f\omega^\sigma\leq -1$ donc $x>-1-yf\omega^\sigma\geq -1+y\geq 0$ et $x>0$.

* Sinon $f=1$ et $d=5$ et $x>-1+y(\sqrt{5}-1)/2$; si $y\geq 2$ alors $x>-1+\sqrt{5}+1=\sqrt{5}-2>0$

si $y=1$ et $x>-1+\left(\frac{\sqrt{5}-1}{2}\right)\neq 0{,}76$ donc $x\geq 0$ et si $x=0$ c'est que $\gamma=\gamma_0$

Donc on a $x>0$ et $y>0$ (sauf lorsque $\gamma=\gamma_0$ avec $d=5$ et $f=1$)

Hormis ce cas nous allons montrer que $\frac{x}{y}$ est réduite de $-f\omega^\sigma$:

- Si $\frac{x}{y}>-f\omega^\sigma$: $\left|-f\omega^\sigma-\frac{x}{y}\right|=\left|\frac{x+yf\omega^\sigma}{y}\right|=\frac{1}{y|x+fwy|}<\frac{1}{2y^2}$ si

$2<\frac{x}{y}+fw$ mais $\frac{x}{y}+fw>-\omega^\sigma+fw\geq -\omega^\sigma+\omega$ et $-\omega^\sigma+\omega$ vaut soit $2\sqrt{d}>2$

soit $\sqrt{d}$ (si $d\equiv 1[4]$) auquel cas $d\geq 5$ donc $\sqrt{d}\geq\sqrt{5}>2$. Dans tous les cas $-\omega^\sigma+\omega>2$ et le théorème de Legendre montre que $\frac{x}{y}$ est réduite de $-f\omega^\sigma$

• Si $\frac{x}{y} < -f_w^\sigma$: $\left|\frac{-1}{f_w^\sigma} - \frac{y}{x}\right| = \frac{|x+yf_w^\sigma|}{|xf_w^\sigma|} = \frac{1}{x|f_w^\sigma|x+yf_w|} \leq \frac{1}{2y^2}$

si : $2 < |f_w^\sigma| \cdot |1 + \frac{y}{x} f_w| = -f_w^\sigma + \frac{y}{x}(-f_w^\sigma) f_w$ ce qui est vrai puisque :

$-f_w^\sigma + \frac{y}{x}(-f_w^\sigma) f_w > -f_w^\sigma + f_w > w - w^\sigma > 2$ Legendre $\Rightarrow$ $\frac{y}{x}$ est réduite

de $-\frac{1}{f_w^\sigma}$ donc $\frac{x}{y}$ est réduite de $-f_w^\sigma$. En effet si $x > 1$ et $x = [a_0; a_1, \ldots]$

alors $\frac{1}{x} = [0; a_0, \ldots] = [v_0; v_1 \ldots]$; appelons H_n et $\frac{p_n}{q_n}$ les matrices et réduites

associés à x, V_n et $\frac{P_n}{q_n}$ celles relatives à $\frac{1}{x}$ on a :

$V_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $V_1 = V_0 H_0 \Rightarrow V_{n+1} = V_0 H_n$ donc $\widetilde{H}_n(+\infty) = \frac{P_n}{q_n}$ donc

$\widetilde{V}_{n+1}(+\infty) = \widetilde{V}_0\left(\frac{P_n}{q_n}\right)$; Soit $\frac{P_{n+1}}{q_{n+1}} = \frac{q_n}{p_n}$.

Ainsi dans les deux cas $\frac{x}{y}$ est réduite de $-f_w^\sigma$ donc il existe $n \geq 0$ tel que

$\frac{x}{y}$ soit la réduite de $\frac{P_n}{Q_n}$ de $-f_w^\sigma$. On PGCD$(P_n, Q_n) = 1$ et PGCD$(x, y) = 1$.

donc $x = P_n$ et $y = Q_n$ et $\gamma = P_n + Q_n f_w$ comme $N(\delta) = \pm 1 = N(P_n + Q_n f_w) = (-1)^{n-1} A_{n-1}$

$\Rightarrow$ $A_{n-1} = 1$ et ceci ne se produit que pour $n = t, 2t, \ldots, kt, \ldots$

donc $\in \{P_{nt-1} + Q_{nt-1} f_w \mid n \geq 1\}$

$(\gamma_\theta^n)_{n \geq 1}$ et $(P_{nt-1} + Q_{nt-1} f_w)$ sont strictement croissantes on a donc

$\gamma_\theta^n = P_{nt-1} + Q_{nt-1} f_w \quad \forall n \geq 1$.

ii) Soit $\gamma \in \mathcal{O}^*$, si $\gamma > 1$ on a $\gamma = \gamma_\theta^n$, $n \geq 0$ si $0 < \gamma < 1 \Rightarrow \alpha = \frac{1}{\gamma} \in \mathcal{O}^*$

et $\alpha > 1$ donc $\alpha = \gamma_\theta^n$ $n \geq 1$ $\gamma = \gamma_\theta^n$ $m \leq -1$ si $\gamma < 0$ donc $\beta = -\gamma \in \mathcal{O}^*$ et $\beta > 0$

d'où $\gamma = -\gamma_\theta^n$, $n \in \mathbb{Z}$.

5 Application à la recherche de modules de norme donnée.

Proposition : Méthode $m = us^2$

Soit $\mathcal{O}$ un ordre de $K = \mathbb{Q}(\sqrt{d})$ avec $\mathrm{Disc}\,\mathcal{O} = D$
Les modules A associés à $\mathcal{O}$, inclus dans $\mathcal{O}$ et de norme $m \geq 1$ sont fournis par les quadruplets $(s,u,v,w) \in \mathbb{N}^2 \times \mathbb{Z}^2$ tels que

$$\begin{cases} A = us\left(\mathbb{Z} \oplus \mathbb{Z}\left(\dfrac{-v+\sqrt{D}}{2u}\right)\right) \\ v^2 - 4uw = D \\ -u < v \leq u \\ \mathrm{PGCD}(u,v,w) = 1 \\ us^2 = m \end{cases}$$

Preuve :

$G = A \cap \mathbb{Z}$ est un sous groupe de $\mathbb{Z}$; $G \neq 0$ car si $\alpha \neq 0$ $\alpha \in A$ alors $\alpha \in \mathcal{O}$ donc $\alpha^\sigma \in \mathcal{O}$
et $\alpha\alpha^\sigma = N(\alpha) \in A \cap \mathbb{Z}$ ainsi $G = \mathbb{Z}h$ $(h \geq 1)$ est un sous groupe de rang 1 de A
donc $A = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2$ et $G = \mathbb{Z}n\alpha_1$ de $\mathbb{Z}h = \mathbb{Z}n\alpha_1$ il vient $n = h$ $\alpha_1 = 1$

donc $A = \mathbb{Z}h \oplus \mathbb{Z}\alpha_2 = h\left(\mathbb{Z} \oplus \mathbb{Z}\dfrac{\alpha_2}{h}\right)$.

Soit $P_\gamma = uX^2 + vX + w$, $v^2 - 4uw = \mathrm{Disc}\,\mathcal{O}_{\mathbb{Z}\oplus\mathbb{Z}\gamma} = \mathrm{Disc}\,(\mathcal{O}) = D$

De plus $N(A) = m = h^2 N(\mathbb{Z} \oplus \mathbb{Z}\gamma) = \dfrac{h^2}{u}$ donc $m = h^2$ et $\gamma = -\dfrac{v \pm \sqrt{D}}{2u}$

mais $\mathbb{Z} \oplus \mathbb{Z}\gamma$ ne change pas si l'on change γ en $-\gamma$ ou si l'on translate γ d'un entier, on peut supposer $\gamma = -\dfrac{v \pm \sqrt{D}}{2u}$ avec $-u < v \leq u$, par ailleurs
$h\gamma \in A \subseteq \mathcal{O}$ et $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}u\gamma$ donc $h\gamma = m + nu\gamma$ et $h = nu \Rightarrow u \mid h$.

soit $h = us$ $(s \geq 1)$.

Réciproquement :

Soit (s,u,v,w) un tel quadruplet. Posons $A = us\left(\mathbb{Z} \oplus \mathbb{Z}\cdot\dfrac{v+\sqrt{D}}{2u}\right)$

alors $\mathcal{O}_\pi = \mathbb{Z} \oplus \mathbb{Z}\left(\dfrac{v+\sqrt{D}}{2u}\right)$ $\quad P_\gamma = uX^2 + vX + w$ où $\gamma = -\dfrac{v+\sqrt{D}}{2u}$

De plus on a $\mathrm{Disc}\,\mathcal{O}_A = D = v^2 - 4uw$ donc $\mathcal{O}_A = \mathcal{O}$. $N(A) = u^2 s^2 \cdot \frac{1}{u} = us^2 = m$

donc $A = s\left|\, \mathbb{Z} \oplus \mathbb{Z}\left(\frac{v+\sqrt{D}}{2u}\right)\right.$ on a donc $A \subseteq \mathcal{O}_A = \mathcal{O}$. □

III) Méthode de résolution de $ax^2+bx+c=m$ (cas b^2-4ac non carré positif)

Commençons par deux lemmes caractérisant la similitude de deux modules :

Lemme 1) Similitudes pour $D>0$ et $N(\gamma_f) = -1$:

Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique réel et soit $\mathcal{O}$ un ordre de K dont l'unité fondamentale γ_f est de norme -1.

a) $\mathbb{Z}\oplus\mathbb{Z}\alpha$ et $\mathbb{Z}\oplus\mathbb{Z}\beta$ deux modules associés à $\mathcal{O}_f$ (avec α et $\beta > 0$) sont strictement semblables si et seulement si α et β ont même cycle de réduits.

b) Si $\alpha, \alpha_1, \dots, \alpha_n$ sont les quotients complets successifs de α :

$$\mathbb{Z}\oplus\mathbb{Z}\alpha = \frac{1}{\alpha_1 \cdots \alpha_n}\left(\mathbb{Z}\oplus\mathbb{Z}\alpha_n\right) = \frac{1}{Q_{n-1}\alpha_n + Q_{n-2}}\left(\mathbb{Z}\oplus\mathbb{Z}\alpha_n\right)$$

Preuve

a) Il suffit de montrer le résultat suivant :

$\mathbb{Z}\oplus\mathbb{Z}\alpha$ semblable à $\mathbb{Z}\oplus\mathbb{Z}\beta \iff \exists H \in GL_2(\mathbb{Z}) \,/\, \tilde{H}(\beta) = \alpha$ et dans ce cas

$$\mathbb{Z}\oplus\mathbb{Z}\alpha = \frac{1}{c\beta+d}\left(\mathbb{Z}\oplus\mathbb{Z}\beta\right) \quad \left(\text{où } H = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)$$

En effet :

Si $A = \mathbb{Z}\oplus\mathbb{Z}\alpha$ est semblable à $B = \mathbb{Z}\oplus\mathbb{Z}\beta$ il existe $\xi \in K$ tel que $B = \xi A$ donc $(\xi, \xi\alpha)$ est une base de B et il existe $H = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ telle que $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \beta \\ 1 \end{pmatrix} = \begin{pmatrix} \xi\alpha \\ \xi \end{pmatrix}$ soit $a\beta + b = \xi\alpha$ et $c\beta + d = \xi$ donc

$$\tilde{H}(\beta) = \frac{a\beta+b}{c\beta+d} = \alpha \text{ et } A = \frac{1}{\xi}B$$

réciproquement si $\alpha = \frac{a\beta+b}{c\beta+d}$ avec $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ écrivons

$$A = \frac{a\beta+b}{c\beta+d}\left(\mathbb{Z}(c\beta+d)\oplus\mathbb{Z}(a\beta+b)\right) = \frac{1}{c\beta+d}\left(\mathbb{Z}\oplus\mathbb{Z}\beta\right) \text{ donc}$$

$\{c\beta+d\,;\, a\beta+b\}$ est une base de $\mathbb{Z}\oplus\mathbb{Z}\beta$

b) $\alpha = \widetilde{H_{n-1}}(\alpha_n) = \dfrac{P_{n-1}\alpha_n + P_{n-2}}{Q_{n-1}\alpha_n + Q_{n-2}}$ donc $V_\Phi V_\alpha = \dfrac{1}{Q_{n-1}\alpha_n + Q_{n-2}}(V_\Phi Z_{\alpha_n})$

mais $H_n = H_{n-1} \times \begin{pmatrix} u_n & 1 \\ 1 & 0 \end{pmatrix}$ donc $H_{n-1}^{-1} H_n = \begin{pmatrix} u_n & 1 \\ 1 & 0 \end{pmatrix}$ donc en α_n cela donne

$\alpha_{n-1} = \dfrac{u_n \alpha_n + 1}{\alpha_n}$ donc $V_\Phi V_{\alpha_{n-1}} = \dfrac{1}{\alpha_n}(V_\Phi V_{\alpha_n})$.

Lemme 2) Similitudes pour $D>0$ et $N(\gamma_j) = +1$

Si $N(\gamma_j) = 1$ alors

a) $Z_\Phi V_\alpha$ et $Z_\Phi V_\beta$ semblable $\Leftrightarrow$ α et β ont même cycle de réduits

si $\alpha, \alpha_1, \dots, \alpha_n$ et $\beta, \beta_1, \dots, \beta_m$ sont les quotients complets successifs

tels que $\alpha_n = \beta_m$ on a $Z_\Phi V_\alpha = \dfrac{\beta_1 \dots \beta_m}{\alpha_1 \dots \alpha_n}(Z_\Phi V_\beta)$

b) La similitude est stricte si et seulement si $N\left(\dfrac{\beta_1 \dots \beta_m}{\alpha_1 \dots \alpha_n}\right) > 0$

c) De plus si $N(\alpha_i) < 0$ on a $N(\alpha_{i+1}) < 0$.

Preuve :

$\alpha_i = u_i + \dfrac{1}{\alpha_{i+1}}$ donc $\dfrac{1}{\alpha_{i+1}} = -u_i + \alpha_i$ $\quad \dfrac{1}{N(\alpha_{i+1})} = N(\alpha_i - u_i) = (\alpha_i - u_i)(\alpha_i^\sigma - u_i^\sigma)$

$= N(\alpha_i) - u_i \mathrm{Tr}(\alpha_i) + u_i^2$. Soit $P_{\alpha_i} = a_i X^2 + b_i X + c_i$ $\quad N(\alpha_i) = \dfrac{c_i}{a_i}$ $\quad \mathrm{Tr}(\alpha_i) = -\dfrac{b_i}{a_i}$

donc $\dfrac{1}{N(\alpha_{i+1})} = \dfrac{c_i}{a_i} + u_i \dfrac{b_i}{a_i} + u_i^2 = \dfrac{1}{a_i} P_{\alpha_i}(u_i)$. On a $0 \leq u_i < \alpha_i$ donc si $N(\alpha_i) < 0$

c'est que $\alpha_i^\sigma < 0$ (c'est le cas si α_i est réduit) donc u_i est entre les racines de

P_{α_i} et $\dfrac{1}{N(\alpha_{i+1})} < 0$ par contre si $N(\alpha_i) > 0$ tout dépend de la position de α_i^σ

par rapport à u_i $\square$.

La méthode de résolution :

Soit à résoudre $\varphi(x,y) = ax^2 + bxy + cy^2 = m$ $(a>0)$ $(m>0)$ $\operatorname{pgcd}(a,b,c)=1$ $b^2-4ac>0$ non carré.

1) $D = b^2 - 4ac = g^2 d$ où d est sans facteur carré

On cherche le conducteur de l'ordre $\mathcal{O}_n$ (où $\Pi = \mathbb{Z} \oplus \mathbb{Z}\alpha$; $\alpha = -\frac{b+\sqrt{D}}{2a}$)

Soit $\mathcal{O}_n = \mathcal{O}_f = \mathbb{Z}$ Dis $\mathcal{O}_n = g^2 d = \begin{cases} (g/\ell)^2 d & \text{si } d \neq 1 [4] \\ \ell^2 g^2 d & d \equiv 1 [4] \end{cases}$

donc $f = g$ si $d \equiv 1 [4]$ et $f = \frac{g}{2}$ si $d \equiv 2,3 [4]$

2) Soit $\Pi = \mathbb{Z} \oplus \mathbb{Z}\alpha$ où $\alpha = -\frac{b+\sqrt{D}}{2a}$ donc $N(\Pi) = \frac{1}{a}$

$\Pi^{-1} = a(\mathbb{Z} \oplus \mathbb{Z}\mu)$ avec $\pm\mu = \frac{b+\sqrt{D}}{2a}$ le signe étant choisi pour que $\mu > 0$

3) Développer μ en fraction continue.

4) Avec la méthode $m = us^2$ calculer le module $A_i = u_i s_i (\mathbb{Z} \oplus \mathbb{Z}\delta_i) \subset \mathcal{O}_f$ de norme m.

5) Développer chaque δ_i en fraction continue et comparer au développement de μ

6) Calculer $N(\gamma_f)$ pour savoir si similitudes larges et strictes coïncident.

7) Pour chaque A_i trouvé strictement semblable à Π^{-1}, déterminer ξ_i tel que $A_i = \xi_i \Pi^{-1}$. (vérifier que $N(\xi_i) = \frac{m}{a}$)

8) Déterminer les unités de $\mathcal{O}_f$ de norme 1

9) En déduire le classe $\xi_i \mathcal{O}_f^*$ correspondant aux ξ_i

10) Revenir aux solutions en x, y :

Pour chaque $\eta = u + v\sqrt{d} \in \xi_i U$ écrire $\eta = x - y\alpha$ le couple (x,y) est la solution correspondant à η.

Exemple :

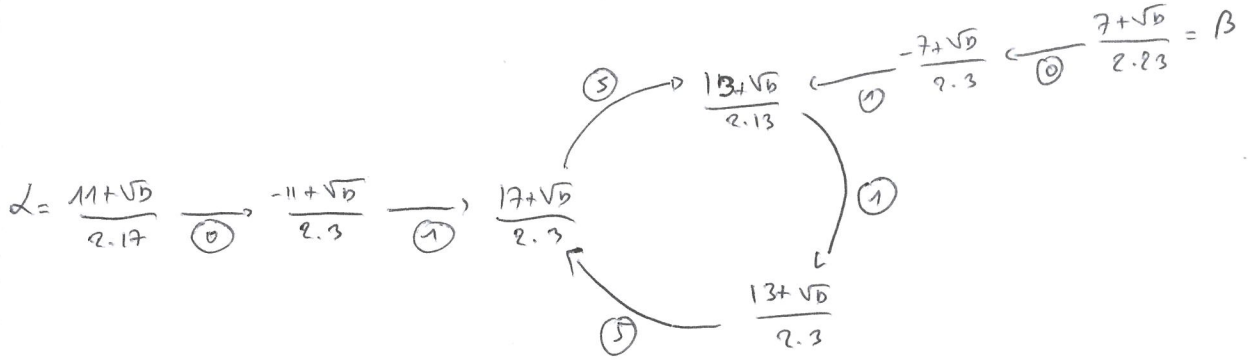
Supposons qu'une équation aboutisse aux résultats suivant :

$K = \mathbb{Q}(\sqrt{13})$ $\quad w = \frac{1+\sqrt{13}}{2}$ $\quad D_K = 13$ $\quad \gamma_1 = 1+w = \frac{3+\sqrt{13}}{2}$ est de norme -1

Pour $p = 5$ on a $D = 25 \times 13 = 325$ on trouve $\gamma_5 = 18 + \sqrt{D} = \gamma_1^3$ et $N(\gamma_5) = -1$

Prenons comme module $A = \mathbb{Z} \oplus \mathbb{Z}\left(\frac{11+\sqrt{D}}{2\times 17}\right)$ et $B = \mathbb{Z} \oplus \mathbb{Z}\left(\frac{7+\sqrt{D}}{2\times 23}\right)$ on obtient

α $\qquad$ β



$$\mathbb{Z} \oplus \mathbb{Z}\alpha = \frac{\beta_1 \beta_2}{\alpha_1 \alpha_2 \alpha_3}\left(\mathbb{Z} \oplus \mathbb{Z}\beta\right) \quad \text{avec} \quad \xi = \frac{-7+\sqrt{D}}{2\cdot 3} \cdot \frac{2\times 3}{-11+\sqrt{D}} \cdot \frac{2\times 3}{17+\sqrt{D}}$$

$\xi = \frac{-81+5\sqrt{D}}{34}$ $\quad$ on a $N(\xi) = -\frac{23}{17}$

$\xi\gamma_5$ est un rapport de similitude stricte.

$\xi\gamma_5 = \frac{167+9\sqrt{D}}{34}$.

IV) Structure des idéaux premiers

Soit $\mathfrak{P}$ un idéal premier non nul de $\mathcal{O}_K$; $\mathfrak{P} \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$ premier

(car $xy \in \mathfrak{P} \cap \mathbb{Z} \Rightarrow xy\mathcal{O}_K \cdot y\mathcal{O}_K \subseteq \mathfrak{P} = \mathfrak{P} \mid xy\mathcal{O}_K \Rightarrow \mathfrak{P} \mid x\mathcal{O}_K$ ou $\mathfrak{P} \mid y\mathcal{O}_K \Rightarrow x \in \mathfrak{P}$ ou $y \in \mathfrak{P}$)

donc il existe un nombre premier $p \in \mathbb{N}$ tel que $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$, on dit que $\mathfrak{P}$ est au dessus de p.

Réciproquement l'idéal $\mathcal{O}_K p$ se décompose en $\mathcal{O}_K p = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$; en prenant les normes $p^2 = \prod_{i=1}^{r} N(\mathfrak{P}_i)^{e_i}$; on $N(\mathfrak{P}_i) \in \mathbb{N}$ et $N(\mathfrak{P}_i) \geq 2$ (car $\mathfrak{P}_i \subseteq \mathcal{O}_K$ et $N(\mathfrak{P}_i) = [\mathcal{O}_K : \mathfrak{P}_i]$ donc $N(\mathfrak{P}_i) = 1 \Rightarrow \mathfrak{P}_i = \mathcal{O}_K$) de sorte que trois cas peuvent se produire:

$r=1$ et $e_1 = 1$ $\mathcal{O}_K p = \mathfrak{P}$ est premier de norme p^2: on dit que p est inerte

$r=1$ et $e_1 = 2$ $\mathcal{O}_K p = \mathfrak{P}^2$ avec $N(\mathfrak{P}) = p$ on dit que p est ramifié

$r=2$ alors $e_1 = e_2 = 1$ $\mathcal{O}_K p = \mathfrak{P}_1 \cdot \mathfrak{P}_2$ avec $N(\mathfrak{P}_1) = N(\mathfrak{P}_2) = p$ $\mathfrak{P}_1 \neq \mathfrak{P}_2$ on dit que p est décomposé

Examinons le cas où $p \neq 2$:

Remarquons que $\dfrac{\mathcal{O}_K}{p\mathcal{O}_K} \cong \dfrac{\mathbb{Z} \oplus \mathbb{Z}\sqrt{d}}{(p)}$ (si $d \equiv 1 [4]$ alors $a + b\left(\dfrac{1+\sqrt{d}}{2}\right)$ (avec b impair) est congru à $a + \left(\dfrac{b+p}{2}\right)\left(1+\sqrt{d}\right) \in \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$)

On $\mathbb{Z} \oplus \mathbb{Z}\sqrt{d} \cong \dfrac{\mathbb{Z}[X]}{(X^2 - d)}$ d'où $\dfrac{\mathcal{O}_K}{p\mathcal{O}_K} \cong \dfrac{\mathbb{Z}[X]}{(p, X^2-d)} \cong \dfrac{\frac{\mathbb{Z}[X]}{(p)}}{(X^2 - \bar{d})} \cong \dfrac{\mathbb{F}_p[X]}{(X^2 - \bar{d})}$

On p est décomposé (resp inerte, se ramifie) signifie que $\dfrac{\mathcal{B}_K}{p\mathcal{O}_K}$ est produit de deux corps (resp est un corps, a des éléments nilpotents)

Ceci signifie donc que le polynôme $X^2 - \bar{d} \in \mathbb{F}_p[X]$ est produit de deux facteurs distincts (resp est irréductible, est un carré). Or ceci se produit si $\bar{d}$ est un carré non nul de $\mathbb{F}_p$ (resp n'est pas un carré de $\mathbb{F}_p$, est nul dans $\mathbb{F}_p$)

Cas $p = 2$:

Si: $d \equiv 2,3 [4]$ $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$ $\dfrac{\mathcal{O}_K}{2\mathcal{O}_K} \cong \dfrac{\mathbb{F}_2[X]}{(X^2 - \bar{d})}$. Or $X^2 - \bar{d} = X^2$ ou $X^2 + 1 = (X+1)^2$

et est donc un carré. Ainsi 2 se ramifie dans $\mathcal{O}_K$

Si $d \equiv 1 [4]$ $\frac{1+\sqrt{d}}{2}$ admet $X^2 - X - \frac{d-1}{4}$ pour polynôme minimal d'où

$\frac{\mathcal{O}_K}{2\mathcal{O}_K} \simeq \frac{\mathbb{F}_2[X]}{(X^2 - X - \delta)}$ $\left(\text{où } \delta = \left(\frac{d-1}{4}\right)\right)$. Pour $d \equiv 1 [8]$ on a $\delta = 0$ et

$X^2 - X - \delta = X(X-1)$ donc 2 est décomposé

Si $d \equiv 5 [8]$ on a $\delta = 1$ et $X^2 - X - \delta = X^2 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$ donc 2 est inerte.

V) Le caractère χ_K et le nombre d'idéaux de norme donnée

Définition: Soit $\chi_K : \mathbb{Z} \to \{-1, 0, 1\}$ définie par $\chi_K(p) = 1$ si p est décomposé

$\chi_K(p) = -1$ si p est inerte ; $\chi_K(p) = 0$ si p est ramifié.

Soit I_n l'ensemble des idéaux de norme n et $X_n = \#I_n$. Soit $\mathfrak{p} \in I_p$ ($\mathfrak{p}$ premier) alors

$\mathfrak{p}$ est premier car si $\mathfrak{p} = Q_1 Q_2$ on a $N(\mathfrak{p}) = p = N(Q_1)N(Q_2) \Rightarrow N(Q_1) = 1$ ou $N(Q_2) = 1$

donc $Q_1 = \mathcal{O}_K$ ou $Q_2 = \mathcal{O}_K$ on a alors $X_p = 1 + \chi_K(p)$ en effet :

Si p est inerte $X_p = 0$ et $1 + \chi_K(p) = 1 - 1 = 0$

Si p est décomposé $X_p = 2$ et $1 + \chi_K(p) = 1 + 1 = 2$

Si p est ramifié $X_p = 1$ et $1 + \chi_K(p) = 1 + 0 = 1$

Montrons $X_{p^n} = 1 + \chi_K(p) + \chi_K(p)^2 + \dots + \chi_K(p)^n$

Démonstration: $n = 1$ c'est vrai.

- Si p inerte. Soit $I \in I_{p^{n+1}}$: $I = \prod_{\mathfrak{p} \mid I} \mathfrak{p}^{v_{\mathfrak{p}}(I)} \Rightarrow p^{n+1} = \prod_{\mathfrak{p} \mid I} N(\mathfrak{p})^{v_{\mathfrak{p}}(I)} \Rightarrow N(\mathfrak{p})$ est une puissance de p mais un seul idéal premier $\mathfrak{p}$ divise I et il est de norme p^2 car p inerte :

$I = \mathfrak{p}^{v_{\mathfrak{p}}(I)}$ et $p^{n+1} = p^{2v_{\mathfrak{p}}(I)} \Rightarrow n+1$ est pair ainsi $X_{p^{n+1}} = 0$ si $n+1$ impair et $X_{p^{n+1}} = 1$ si $n+1$ pair ce qui donne $1 + \chi_K(p) + \chi_K(p)^2 + \dots + \chi_K(p)^n$ on a donc $\forall n$ $X_{p^n} = \frac{1 + (-1)^n}{2}$ si p inerte.

- Si p est décomposé :

Si $N(I) = p^{n+1}$ si $\mathfrak{p} \mid I$ $\mathfrak{p} = \mathfrak{p}_1$ ou $\mathfrak{p} = \mathfrak{p}_2$ l'un des deux idéaux de norme p. Si $\mathfrak{p}_1 \mid I$ alors $J = I\mathfrak{p}_1^{-1}$ est un idéal de norme p^n et il y en a X_{p^n} ; Si $\mathfrak{p}_1 \nmid I$ alors $\mathfrak{p}_2^{n+1} = I$ au total $X_{p^{n+1}} = X_{p^n} + 1$ ($X_{p^n} = n+1$)

- Si p ramifié :

$N(I) = p^{n+1}$ et $\mathfrak{p} \mid I$ $N(J = I\mathfrak{p}^{-1}) = p^n$ et $X_{p^{n+1}} = X_{p^n}$. ($X_{p^n} = 1$)

Nous savons $\gamma_\kappa(1)=1$ et $\gamma_\kappa(p^n)=\gamma_\kappa(p)^n$ on a donc $\chi_{p^n}=\sum_{d\mid p^n}\gamma_\kappa(d)$

On va étendre cette formule par multiplication :

$n\longmapsto \chi_n$ est multiplicative : Si $m_1\wedge m_2=1 \Rightarrow \chi_{m_1m_2}=\chi_{m_1}\chi_{m_2}$

En effet soit $\varphi : \mathcal{I}_{m_1}\times\mathcal{I}_{m_2}\longrightarrow \mathcal{I}_{m_1m_2}$ définie par $\varphi(\mathcal{I}_1,\mathcal{I}_2)=\mathcal{I}_1\cdot\mathcal{I}_2$

- φ est surjective : Soit $\mathcal{I}=\prod_{\mathfrak{p}\mid\mathcal{I}}\mathfrak{p}^{v_\mathfrak{p}(\mathcal{I})}\in\mathcal{I}_{m_1m_2}$ si $\mathfrak{p}\mid\mathcal{I}$ alors $N(\mathfrak{p})\mid m_1m_2 \Rightarrow$

$N(\mathfrak{p})\mid m_1$ ou $N(\mathfrak{p})\mid m_2 \Rightarrow \mathcal{I}=\prod_{N(\mathfrak{p})\mid m_1}\mathfrak{p}^{v_\mathfrak{p}(\mathcal{I})}\prod_{N(\mathfrak{p})\mid m_2}\mathfrak{p}^{v_\mathfrak{p}(\mathcal{I})}=\mathcal{I}_1\cdot\mathcal{I}_2$ donc $m_1m_2=N(\mathcal{I}_1)N(\mathcal{I}_2)$

et comme $N(\mathcal{I}_1)\wedge m_2=N(\mathcal{I}_2)\wedge m_2=1 \Rightarrow N(\mathcal{I}_1)=m_1 \quad N(\mathcal{I}_2)=m_2$ donc $\mathcal{I}=\varphi(\mathcal{I}_1,\mathcal{I}_2)$

- φ injective : Soit $\mathcal{I}=\prod_{N(\mathfrak{p})\mid m_1}\mathfrak{p}^{v_\mathfrak{p}(\mathcal{I})}\prod_{N(\mathfrak{p})\mid m_2}\mathfrak{p}^{v_\mathfrak{p}(\mathcal{I})}$; $\mathcal{I}=\mathcal{J}_1\mathcal{J}_2$ pour $N(\mathfrak{p})\mid m_1$ ou $\mathfrak{p})\mathcal{J}_1$

car sinon $\mathfrak{p}\mid\mathcal{J}_2$ donc $N(\mathfrak{p})\mid N(\mathcal{J}_2)=m_2 \Rightarrow \mathfrak{p}^{v_\mathfrak{p}(\mathcal{I})}\mid\mathcal{J}_1$, de même pour $\mathcal{J}_2$ d'où $\mathcal{J}_1=\prod_{N(\mathfrak{p})\mid m_1}\mathfrak{p}^{v_\mathfrak{p}(\mathcal{I})}$

On définit $\gamma_\kappa(m)=\prod_{\mathfrak{p}\mid m}\gamma_\kappa(\mathfrak{p}^{v_\mathfrak{p}(m)})=\prod_{\mathfrak{p}\mid m}\gamma_\kappa(\mathfrak{p})^{v_\mathfrak{p}(n)}$ si $m=\prod_{\mathfrak{p}\mid m}\mathfrak{p}^{v_\mathfrak{p}(n)}$

La fonction $n\longmapsto \psi_n=\sum_{d\mid n}\gamma_\kappa(d)$ est multiplicative :

en effet γ_κ l'est et si $m_1\wedge m_2=1$: $\gamma_\kappa(m_1m_2)=\prod_{\mathfrak{p}\mid m_1m_2}\gamma_\kappa(\mathfrak{p})^{v_\mathfrak{p}(m_1m_2)}=\prod_{\mathfrak{p}\mid m_1m_2}\gamma_\kappa(\mathfrak{p})^{v_\mathfrak{p}(m_1)+v_\mathfrak{p}(m_2)}$

$=\prod_{\mathfrak{p}\mid m_1}\gamma_\kappa(\mathfrak{p})^{v_\mathfrak{p}(m_1)}\cdot\prod_{\mathfrak{p}\mid m_2}\gamma_\kappa(\mathfrak{p})^{v_\mathfrak{p}(m_2)}=\gamma_\kappa(m_1)\gamma_\kappa(m_2)$ et $\psi_{m_1m_2}=\sum_{d\mid m_1m_2}\gamma_\kappa(d)=\sum_{d_1\mid m_1,\,d_2\mid m_2}\gamma_\kappa(d_1d_2)$

$=\sum_{d_1\mid m_1,\,d_2\mid m_2}\gamma_\kappa(d_1)\gamma_\kappa(d_2)=\sum_{d_1\mid m_1}\gamma_\kappa(d_1)\cdot\sum_{d_2\mid m_2}\gamma_\kappa(d_2)=\psi_{m_1}\psi_{m_2}$

$\psi_1(\mathfrak{p}^m)=\chi_1(\mathfrak{p}^m)$ $\forall\mathfrak{p}\ \forall m\ \forall n$ donc $\chi_n=\psi_n$.

On a montré :

Proposition : $\chi_n=\sum_{d\mid n}\gamma_\kappa(d)$

Remarque : on peut majorer le nombre de solutions non associées de $\varphi(x,y)=m$ par χ_m et

$\chi_m\leq\sum_{d\mid m}1=d(m)$ (nombre de diviseurs de m)