55376
1988
11

N° d'ordre 1426

THESE

présentée à

L'UNIVERSITE DES SCIENCES ET TECHNIQUES DE LILLE FLANDRES ARTOIS

pour obtenir

le titre de Docteur de 3ème cycle

Spécialité : Mathématiques Pures

par

M'ZARI Mohamed

POINTS DE HEEGNER ET CORPS QUADRATIQUES

Soutenue le 28 juin 1988 devant la Commission d'Examen :

Présidente et Rapporteur : N. ZINN-JUSTIN (Université de Lille Flandres Artois)
Membres : L. GRUSON (Université de Lille Flandres Artois)
P. SATGE (Université de Caen)
M. HUTTNER (Université de Lille Flandres Artois)

55 376
1988
11

N° d'ordre 1426

THESE

présentée à

L'UNIVERSITE DES SCIENCES ET TECHNIQUES DE LILLE FLANDRES ARTOIS

pour obtenir

le titre de Docteur de 3ème cycle

Spécialité : Mathématiques Pures

par

M'ZARI Mohamed

POINTS DE HEEGNER ET CORPS QUADRATIQUES

Soutenue le 28 juin 1988 devant la Commission d'Examen :

Présidente et Rapporteur : N. ZINN-JUSTIN (Université de Lille Flandres Artois)
Membres : L. GRUSON (Université de Lille Flandres Artois)
P. SATGE (Université de Caen)
M. HUTTNER (Université de Lille Flandres Artois)

A mes parents

A Christine, Sophia et Samy

A ma famille

Je remercie vivement Madame Nicole Zinn-Justin pour l'aide qu'elle m'a apportée tout au long de ce travail. Sa très grande disponibilité, ses suggestions et ses conseils m'ont permis de mener à bien ce travail. Je lui exprime ici ma profonde gratitude.

Je remercie beaucoup Monsieur Philippe Satgé pour les discussions très enrichissantes que j'ai eues avec lui, pour l'accueil chaleureux qu'il m'avait réservé à Caen et d'avoir accepté de faire partie du jury. Cette thèse lui doit beaucoup.

Je remercie également Monsieur Laurent Gruson de m'avoir honoré de sa présence dans le jury.

Un grand merci aussi à Monsieur Marc Huttner pour ses conseils, ses encouragements et d'avoir accepté de faire partie du jury.

Je tiens à remercier Madame Raymonde Bérat pour sa gentillesse, sa patience, sa bonne humeur et tout le soin apporté à la dactylographie de cette thèse. Mes remerciements vont également à toutes les personnes ayant participé à sa réalisation matérielle.

Enfin, je ne saurais oublier d'associer à mes remerciements tous les membres de l'U.F.R. de Mathématiques de l'Université des Sciences et Techniques de Lille Flandres Artois, pour la sympathie et la gentillesse dont ils m'ont fait preuve.

TABLE DES MATIERES

INTRODUCTION

Soit $Y_0(N)$ la courbe $H/\Gamma_0(N)$, où H est le demi-plan de Poincaré et

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbf{Z}) | c \equiv 0 \bmod (N) \right\}, \ N \text{étant un entier} \geq 1 .$$

Au point de vue analytique, un point de Heegner de $Y_0(N)$ est un point z de H défini modulo $\Gamma_0(N)$, quadratique, tel que : $\Delta(z) = \Delta(Nz)$ (si $Az^2 + Bz + C = 0$ avec A, B et C des entiers tels que $(A,B,C) = 1$, on notera $\Delta(z) = B^2 - 4AC$) (cf. [6]). D'après l'interprétation des points de $Y_0(N)$ en terme de classes d'isomorphie de couples de courbes elliptiques $(E \xrightarrow{\alpha} E')$, liées par une isogénie α de noyau cyclique de degré N, les points de Heegner sont considérés comme des couples de courbes elliptiques $(E \xrightarrow{\alpha} E')$, N-isogènes telles que E et E' aient la même multiplication complexe, par un ordre $\mathcal{O}_f$ de l'anneau des entiers d'un corps quadratique imaginaire (cf. [3]).

Dans ce travail, on va s'intéresser à la détermination des points de Heegner de discriminant D, avec D fondamental, impair et $(D,N) = 1$.

On va établir une identification entre ces points et les triplets $(\mathcal{O}, \eta, [a])$; où $\mathcal{O}$ est l'anneau des entiers du corps quadratique $K = Q(\sqrt{D})$ (l'ordre maximal), η est un idéal entier primitif de norme N et $[a]$ la classe d'un idéal a.

On va étudier quelques exemples de détermination de ces points (cas où $N = 1$; 2^n; 3^n, n étant un entier ≥ 1 et D un discriminant tel que $h(D)$ est un nombre premier ou $h(D) = 1$). Les résultats vont nous conduire à établir un algorithme concernant les discriminants, pour lesquels il existe des représentants des classes d'idéaux, qui sont des puissances successives d'un idéal de norme un nombre premier. D'une façon générale, on peut étendre cet algorithme à tous les discriminants :

$$cl(Q(\sqrt{D})) = \{[\mathcal{P}_1], \ldots, [\mathcal{P}_1^{r_1}]; [\mathcal{P}_2], \ldots, [\mathcal{P}_2^{r_2}], \ldots, [\mathcal{P}_s], \ldots, [\mathcal{P}_s^{r_s}]\}$$

où les $\mathcal{P}_i$ sont des idéaux de norme un nombre premier et les r_i des entiers tels que $\sum_{i=1}^{s} r_i = h(D)$.

CHAPITRE I

LA COURBE $Y_0(N)$

1 - Définitions.

Soient N un entier ≥ 1, $\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbf{Z}) | c \equiv 0 \bmod (N)\}$ et H le demi-plan de Poincaré. $\Gamma_0(N)$ agit sur H de la façon suivante :

$$\rho : \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \to \rho(\gamma) : (z \to \frac{az+b}{cz+d}) \in Aut(H) .$$

ρ est un homomorphisme dont le noyau est $\{\pm id\}$.

Deux points z et z' de H sont équivalents modulo $\Gamma_0(N)$ ssi il existe $\overline{\gamma} \in \Gamma_0(N)/\{\pm id\}$ telle que $z' = \rho(\gamma)(z)$. Dans la suite, on confondra $\rho(\gamma)$ avec $\overline{\gamma}$.

On pose :

$$Y_0(N) = H/\Gamma_0(N)$$

H étant muni de la topologie usuelle, alors $Y_0(N)$ muni de la topologie quotient est un espace séparé non compact.

2 - Compactification de $Y_0(N)$.

L'ensemble des pointes relativement à $\Gamma_0(N)$ (les points de $\mathbf{R} \cup \{\infty\}$ fixés par des éléments paraboliques de $\Gamma_0(N)$) est $Q \cup \{\infty\}$. Cet ensemble est $\Gamma_0(N)$-invariant. On démontre que : (voir, App. (1) et (2)).

$Q \cup \{\infty\}/\Gamma_0(N)$ est isomorphe (au point de vue ensembliste) à $\bigcup_{\substack{d/N \\ d>0}} (\mathbf{Z}/f_d\mathbf{Z})^*$ où $f_d = (d, N/d)$ et la correspondance est donnée par l'application :

$$\frac{m}{n}(m, n \in \mathbf{Z}, (m,n) = 1) \to m\frac{n}{d} \bmod (f_d); d = (n, N) .$$

Le nombre des pointes modulo $\Gamma_0(N)$ est :

$$\sum_{d/n} \varphi(f_d) = \prod_{\substack{p^\nu \| N \\ \nu \geq 1}} \left(p^{[\nu/2]} + p^{[(\nu-1)/2]}\right)$$

où φ est la fonction d'Euler.

En particulier, $Q \cup \{\infty\}/\Gamma_0(1) = \{\infty\}$ et $Q \cup \{\infty\}/\Gamma_0(p) = \{0, \infty\}$, p étant un nombre premier.

Soit $H^* = H \cup Q \cup \{\infty\}$, *on pose :*

$$X_0(N) = H^*/\Gamma_0(N) = Y_0(N) \cup \left(Q \cup \{\infty\}/\Gamma_0(N)\right) .$$

$X_0(N)$ muni de la topologie usuelle est un espace séparé, compact. De plus, on démontre qu'il existe une "structure complexe" définie sur $X_0(N)$ et que $X_0(N)$ muni de cette structure complexe est une surface de Riemann compacte (App. (3) ou [1], p. 10-18).

3 - Corps des fonctions sur $X_0(N)$: $\mathbf{C}(X_0(N))$.

On sait que $\mathbf{C}(j)$ est le corps des fonctions sur $X_0(1)$, (les fonctions méromorphes sur H invariantes par $\Gamma_0(1)$) où j est l'invariant modulaire.

Par conséquent, le corps des fonctions invariantes par

$$\Gamma = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma_0(1) \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$$

est $\mathbf{C}(j_N)$ où $j_N(z) = j(Nz)$. Comme $\Gamma_0(N) = \Gamma_0(1) \cap \Gamma$, donc $\mathbf{C}(X_0(N)) = \mathbf{C}(j, j_N)$. On sait que j et j_N sont reliées par une équation modulaire $F_N(u,v) \in \mathbf{Z}[u,v]$ telle que $F_N(j, j_N) = 0$. La détermination explicite de cette équation est souvent difficile : Les coefficients augmentent très rapidement avec N, (voir [2]).

Exemples :

$$\begin{aligned} F_2(u,v) &= u^3 + v^3 - (uv)^2 + 3^4 \cdot 5^3 \cdot 4027uv + 2^4 \cdot 3 \cdot 31uv(u+v) \\ &\quad - 2^4 \cdot 3^4 \cdot 5^3(u^2+v^2) + 2^8 \cdot 3^7 \cdot 5^6(u+v) - 2^{12} \cdot 3^9 \cdot 5^9 \end{aligned}$$

$$\begin{aligned} F_3(u,v) &= u(u + 2^{15} \cdot 3 \cdot 5^3)^3 + v(v + 2^{15} \cdot 3 \cdot 5^3)^3 - u^3v^3 \\ &\quad + 2^3 \cdot 3^2 \cdot 31u^2v^2(u+v) - 2^2 \cdot 3^3 \cdot 9907uv(u^2+v^2) \\ &\quad + 2 \cdot 3^4 \cdot 13 \cdot 193 \cdot 6367u^2v^2 + 2^{16} \cdot 3^5 \cdot 5^3 \cdot 17 \cdot 263uv(u+v) \\ &\quad - 2^{31} \cdot 5^6 \cdot 22973uv \end{aligned}$$

Soit la courbe $Z_0(N)$: $F_N(u,v) = 0$, alors $Z_0(N)$ est un modèle plane de la courbe $X_0(N)$.

$$\begin{aligned} \theta : X_0(N) &\to Z_0(N) \\ z &\to (j(z), j(Nz)) \end{aligned}$$

Bien sûr, $Z_0(N)$ n'est pas un bon modèle de $X_0(N)$ (on peut avoir $\theta(z_1) = \theta(z_2)$ et $z_1 \not\equiv z_2$: z_1 (resp. Nz_1) $\Gamma_0(1)$-équivalent à z_2 (resp. Nz_2) et z_1 n'est pas $\Gamma_0(N)$-équivalent à z_2); (voir [6]). (Pour trouver une équation de la courbe $X_0(N)$, voir [7]).

4 - Interprétation des points de $Y_0(N)$ comme des couples de courbes elliptiques.

Proposition. *$Y_0(N)$ classifie les classes d'isomorphie de couples $(E \xrightarrow{\alpha} E')$ de courbes elliptiques liées par une isogénie α cyclique d'ordre N. (i.e on*

a une correspondance entre les points z de $Y_0(N)$ et les classes d'isomorphie de couples $(E \xrightarrow{\alpha} E')$ de courbes elliptiques, où α est un morphisme analytique tel que $\ker\alpha \simeq \mathbf{Z}/N\mathbf{Z}$).

■ Rappelons que : Toute courbe elliptique E sur $\mathbf{C}$ peut être définie comme un tore complexe de dimension 1 : $E(\mathbf{C}) \simeq \mathbf{C}/L$ où L est un réseau de période. Deux courbes elliptiques sur $\mathbf{C}$ sont isomorphes ssi les réseaux de période sont homothétiques.

• Soit $z \in H$, alors à z correspond le couple de courbes elliptiques : $(\mathbf{C}/L_z \xrightarrow{N} \mathbf{C}/L_{Nz})$ où $L_z = \mathbf{Z} + z\mathbf{Z}$ et $L_{Nz} = \mathbf{Z} + Nz\mathbf{Z}$ sont des réseaux de $\mathbf{C}$.

Si $z' = \frac{az+b}{cz+d}$ avec $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, alors $(cz+d)L_{z'} = L_z$ et $(cz+d)L_{Nz'} = L_{Nz}$. Par conséquent, les couples $(\mathbf{C}/L_z \xrightarrow{N} \mathbf{C}/L_{Nz})$ et $(\mathbf{C}/L_{z'} \xrightarrow{N} \mathbf{C}/L_{Nz'})$ appartiennent à la même classe d'isomorphie.

• Réciproquement, soit $(E \xrightarrow{\alpha} E')$ un couple de courbes elliptiques liées par une isogénie α telle que $\ker\alpha \simeq \mathbf{Z}/N\mathbf{Z}$. On pose $E \simeq \mathbf{C}/L$ et $E' \simeq \mathbf{C}/L'$, alors α est induit par une homothétie $z \to \lambda z$ avec $\lambda \in \mathbf{C}$ et $\lambda L \subset L'$. On pose $L'' = \lambda L$, alors on a $L'' \subset L'$ et $L'/L'' \simeq \mathbf{Z}/N\mathbf{Z}$. Comme $E \simeq \mathbf{C}/L \simeq \mathbf{C}/L''$, donc quitte à changer L par L'', on peut supposer qu'on a le couple suivant :

$$(\mathbf{C}/L \xrightarrow{id} \mathbf{C}/L') \text{ avec } L'/L \simeq \mathbf{Z}/N\mathbf{Z}\,.$$

D'après le théorème des diviseurs élémentaires, on démontre qu'il existe une $\mathbf{Z}$-base (w_1, w_2) de L telle que $(w_1, \frac{w_2}{N})$ soit une $\mathbf{Z}$-base de L' et $\mathrm{Im}(\frac{w_1}{w_2}) > 0$.

Ainsi, on obtient le couple : $(\mathbf{C}/w_1\mathbf{Z}+w_2\mathbf{Z} \xrightarrow{id} \mathbf{C}/w_1\mathbf{Z}+\frac{w_2}{N}\mathbf{Z})$, qui appartient à la même classe que le couple : $(\mathbf{C}/\mathbf{Z}+\frac{w_1}{w_2}\mathbf{Z} \xrightarrow{id} \mathbf{C}/\frac{1}{N}\mathbf{Z}+\frac{w_1}{w_2}\mathbf{Z})$. Par conséquent, on peut supposer qu'on a le couple suivant :

$$(\mathbf{C}/L_z \xrightarrow{N} \mathbf{C}/L_{Nz}),\ \text{où } z = w_1/w_2,\ z \in H\,.$$

Lemme. *z est unique modulo* $\Gamma_0(N)$.

■ Supposons qu'il existe deux $\mathbf{Z}$-bases (w_1, w_2) et (w_1', w_2') de L, telles que $(w_1, w_2/N)$ et $(w_1', w_2'/N)$ soient deux $\mathbf{Z}$-bases de L', avec w_1/w_2, w_1'/w_2' deux éléments de H. Alors, il existe

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(1)$$

telle que : $w_1' = aw_1 + b(w_2/N)$ et $w_2'/N = cw_1 + d(w_2/N)$. Par conséquent, on a : $w_1' = aw_1 + (b/N)w_2$ et $w_2' = Ncw_1 + dw_2$, avec b/N un entier, puisque (w_1, w_2) et (w_1', w_2') sont deux $\mathbf{Z}$-bases de L. D'où $z' = w_1'/w_2' = \gamma(w_1/w_2)$ avec

$$\gamma = \begin{pmatrix} a & b/N \\ Nc & d \end{pmatrix} \in \Gamma_0(N) .$$

Ce lemme achève la preuve de la proposition. ■

CHAPITRE II

POINTS DE HEEGNER DE $Y_0(N)$

1 - Points de Heegner, au point de vue analytique.

Soit z un nombre quadratique imaginaire, alors z est solution d'une équation : $Az^2 + Bz + C = 0$, avec A, B, C des entiers, $(A, B, C) = 1$ et $B^2 < 4AC$.

On note $\Delta(z) = B^2 - 4AC$, le discriminant de z. $\Delta(z)$ est un entier négatif, non carré parfait.

Lemme. *Soit z un nombre quadratique imaginaire, alors pour tout $z' \in \Gamma_0(N)(z)$, on a : $\Delta(z) = \Delta(z')$ et $\Delta(Nz) = \Delta(Nz')$.*

Définition. *Soit z un point de $Y_0(N)$, z est un point de Heegner de $Y_0(N)$ si $\Delta(z) = \Delta(Nz)$.*

(D'après le lemme précédent, cette définition a bien un sens).

Proposition 1. *Soit z un point de $Y_0(N)$, si z est un point de Heegner de $Y_0(N)$ alors z est solution d'une équation $Az^2 + Bz + C = 0$, avec A, B, C des entiers, $(A, B, C) = 1$ et $A \equiv 0$ mod(N).*

■ Soit z un point de Heegner de $Y_0(N)$, alors z satisfait une équation : $Az^2 + Bz + C = 0$, avec A, B, C des entiers, $(A, B, C) = 1$ et $\Delta(z) = B^2 - 4AC = \Delta(Nz)$. Nz est solution de l'équation : $A(Nz)^2 + BN(Nz) + N^2C = 0$, on pose $D = (A, BN, N^2C)$. Comme $\Delta(Nz) = \frac{N^2\Delta(z)}{D^2} = \Delta(z)$, donc $D = N$. D'où $A \equiv 0 \bmod(N)$ et l'équation de Nz est :

$$\frac{A}{N}(Nz)^2 + B(Nz) + NC = 0 .$$ ■

Remarque : Si $A \equiv 0 \bmod(N)$ alors $\Delta(z) \equiv B^2 \bmod(4N)$; par conséquent, si D est un discriminant, alors pour qu'il existe un point de Heegner z de $Y_0(N)$ tel que $\Delta(z) = D$, il est nécessaire que D soit un carré modulo $4N$.

On verra dans la suite que cette condition est nécessaire et suffisante pour certains discriminants.

2 - Points de Heegner, en terme de couples de courbes elliptiques.

Avant de donner l'interprétation des points de Heegner en terme de couples de courbes elliptiques, on va rappeler quelques notions :

— Soit D un discriminant négatif, si D est fondamental (i.e. pour tout discriminant négatif $D' \neq D$, le nombre $\sqrt{D/D'}$ n'est pas rationnel), alors à D

correspond $\mathcal{O}$ l'anneau des entiers d'un corps quadratique imaginaire K, tel que le discriminant de $\mathcal{O}$ soit égal à D. Si D n'est pas fondamental (i.e. il existe un entier $g > 1$ tel que $D = g^2 D_1$, avec D_1 un discriminant fondamental), alors à D correspond un ordre α de l'anneau des entiers $\mathcal{O}$ d'un corps quadratique imaginaire K, tel que le discriminant de $\mathcal{O}$ soit égal à D_1. Dans ce cas, on a : $|\mathcal{O}/\alpha| = g$ et si $(1, \omega)$ est une $\mathbf{Z}$-base de $\mathcal{O}$ alors, $(1, g\omega)$ sera une $\mathbf{Z}$-base de α; (voir [4], p. III 26). En plus, si $h(D)$ et $h(D_1)$ désignent le nombre des classes d'idéaux de α et $\mathcal{O}$ respectivement, on démontre que :

$$\infty > h(D) = g h(D_1) \cdot \prod_{p/g} \{1 - \left(\frac{D_1}{p}\right) \frac{1}{p}\} \geq h(D_1) \,,$$

où p est premier et (-) désigne le symbole de Legendre (voir [5]).

— Soit E une courbe elliptique à multiplication complexe : $E(\mathbf{C}) \simeq \mathbf{C}/L$ où L est un réseau de $\mathbf{C}$ tel que $\mathrm{End}(L) \neq \mathbf{Z}$, alors on sait que $\mathrm{End}(E)$ est isomorphe à un ordre α de l'anneau des entiers d'un corps quadratique et L est homothétique à un idéal a de α.

Réciproquement, soit K un corps quadratique imaginaire, $\mathcal{O}_K$ l'anneau des entiers de K, $\mathcal{O}_f$ un ordre de $\mathcal{O}_K$ avec $f = |\mathcal{O}_K/\mathcal{O}_f|$, h_f le nombre des classes d'idéaux de $\mathcal{O}_f$; alors il existe exactement h_f courbes elliptiques E non isomorphes telles que : $\mathrm{End}(E) \simeq \mathcal{O}_f$.

Si E et E' sont deux courbes elliptiques à multiplication complexe isogènes : $E(\mathbf{C}) \simeq \mathbf{C}/L$, $E'(\mathbf{C}) \simeq \mathbf{C}/L'$, alors $\mathrm{End}_Q(L) = \mathrm{End}_Q(L') = K$, un corps quadratique imaginaire, où $\mathrm{End}_Q(L) = \mathrm{End}\, L \otimes_{\mathbf{Z}} Q$. Par conséquent, $\mathrm{End}(E) \simeq \alpha$, $\mathrm{End}(E') \simeq \beta$ où α et β sont deux ordres de l'anneau des entiers de K, et L (resp. L') est homothétique à un idéal de α (resp. de β), (voir [4], p. III 25-27).

Proposition 2. *Soient D un discriminant négatif, on pose $D = g^2 D_1$ où D_1 est un discriminant fondamental (on peut avoir éventuellement $g = 1$), $\mathcal{O}$ l'anneau des entiers d'un corps quadratique imaginaire K de discriminant D_1, α l'ordre de $\mathcal{O}$ d'indice g. Alors z est un point de Heegner de $Y_0(N)$ de discriminant $\Delta(z) = D$ ssi $End(\mathbf{C}/L_z)$ et $End(\mathbf{C}/L_{Nz})$ sont isomorphes au même ordre α.*

■ Soit z un point de Heegner de $Y_0(N)$ de discriminant D, d'après l'interprétation des points de $Y_0(N)$, vue au 1$^{\text{er}}$ chap., à z correspond le couple : $(\mathbf{C}/L_z \xrightarrow{N} \mathbf{C}/L_{Nz}) \cdot \mathbf{C}/L_z$ et $\mathbf{C}/L_{Nz}$ étant isogènes, donc $\mathrm{End}_Q(L_z) = \mathrm{End}_Q(L_{Nz}) = Q(z) =$

$Q(Nz) = K$. Or $\Delta(z) = \Delta(Nz) = D$, donc $\mathrm{End}(L_z) = \mathrm{End}(L_{Nz}) = \alpha$. D'où $\mathrm{End}(\mathbf{C}/L_z)$ et $\mathrm{End}(\mathbf{C}/L_{Nz})$ sont isomorphes à l'ordre α. La réciproque est immédiate. ∎

Conséquences :

— Les points de Heegner de $Y_0(N)$ peuvent être interprétés comme des couples de courbes elliptiques liées par une isogénie α cyclique d'ordre N, $(E \xrightarrow{\alpha} E')$ tels que E et E' aient la même multiplication complexe.

— Soient K un corps quadratique imaginaire de discriminant D, $\mathcal{O}$ l'anneau des entiers, $z \in Y_0(N)$, $z : (E \xrightarrow{\alpha} E')$; alors z est un point de Heegner de $Y_0(N)$ de discriminant D ssi E et E' sont à multiplication complexe par $\mathcal{O}$ (l'ordre maximal).

Dans notre étude, on va s'intéresser à la recherche des points de Heegner de $Y_0(N)$ de discriminant D, avec D fondamental, $(D, N) = 1$ et D impair ($D \equiv 1 \bmod (4)$), en travaillant sur les couples de courbes elliptiques liées par une isogénie α cyclique d'ordre N et ayant la même multiplication complexe.

3 - Points de Heegner, comme des triplets $(\mathcal{O}, \eta, [a])$.

Dans la suite, K désignera un corps quadratique imaginaire de discriminant D vérifiant les conditions ci-dessus, $\mathcal{O}$ l'anneau des entiers de K, cl_K le groupe des classes d'idéaux et $h = |cl_K|$.

Proposition 3. *On a la correspondance suivante :*

$$\left\{ \begin{array}{l} \textit{Les points de Heegner de } Y_0(N) \\ \textit{de discriminant } D \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \textit{Les paires } (\mathcal{A}, \eta) \\ \textit{avec } \mathcal{A} \in cl_K \textit{ et } \eta \textit{ un idéal} \\ \textit{entier primitif de norme } N \end{array} \right\}$$

$$(\mathbf{C}/a \xrightarrow{id} \mathbf{C}/a\eta^{-1}) \leftarrow ([a], \eta)$$

où a est un idéal fractionnaire de $\mathcal{O}$, $[a] \in cl_K$ et η est un idéal entier primitif (i.e. $\eta \subset \mathcal{O}$ et η n'est pas divisible comme idéal par tout entier > 1).

∎ • Soit z un point de Heegner de $Y_0(N)$ de discriminant D, alors on peut supposer que $z : (\mathbf{C}/L \xrightarrow{id} \mathbf{C}/L')$ où L et L' sont des idéaux fractionnaires de $\mathcal{O}$, tels que : $L \subset L'$ et $L'/L \simeq \mathbf{Z}/N\mathbf{Z}$.

En effet, considérons $z : (\mathbf{C}/L \xrightarrow{\alpha} \mathbf{C}/L')$ avec $\ker\alpha \simeq \mathbf{Z}/N\mathbf{Z}$ et L, L' deux réseaux de $\mathbf{C}$. On a $\mathrm{End}_Q(L) = \mathrm{End}_Q(L') = K$, donc il existe λ, λ', w, w' des complexes tels que $L = \lambda L_\omega$, $L' = \lambda' L_{\omega'}$ et $Q(w) = Q(w') = K$. Par ailleurs, il existe n, n' des entiers tels que nw et $n'w'$ appartiennent à $\mathcal{O}$. Donc quitte à remplacer L et L' par des homothétiques convenables, on peut supposer que L et L' sont des réseaux de K et il existe deux entiers n et n' tels que $nL \subset \mathcal{O}$ et $n'L' \subset \mathcal{O}$. Comme $\mathrm{End}(L) = \mathrm{End}(L') = \mathcal{O}$, donc L et L' sont des $\mathcal{O}$-modules de K. Par conséquent, L et L' sont des idéaux fractionnaires de $\mathcal{O}$. Par ailleurs, L et L' sont liés par une isogénie cyclique d'ordre N, donc il existe $\lambda \in \mathbf{C}$ tel que $\lambda L \subset L'$ et $|L'/\lambda L| = N$. D'où quitte à remplacer L par λL, on peut supposer que $z : (\mathbf{C}/L \xrightarrow{id} \mathbf{C}/L')$ avec $L'/L \simeq \mathbf{Z}/N\mathbf{Z}$ et $L \subset L' \subset K$.

$*$ On pose $\eta = LL'^{-1}$, alors η est un idéal entier de $\mathcal{O}$, primitif, de norme N.

En effet, $\eta = LL'^{-1} \subset L'L'^{-1} = \mathcal{O}$, puisque $L \subset L'$; donc η est un idéal entier. D'autre part, on a : $\mathcal{O}/\eta \simeq L'/L \simeq \mathbf{Z}/N\mathbf{Z}$, d'où la norme de η est N et η est primitif. En effet, supposons qu'il existe un entier n tel que $(n) = n\mathcal{O}$ divise η; alors il existe un idéal entier $\mathcal{D}$ tel que $\eta = (n)\mathcal{D}$, ce qui entraîne que $\frac{1}{n}L \subset L'$. Soient (w_1, w_2) et $(w_1, \frac{w_2}{N})$ deux $\mathbf{Z}$-bases de L et L' respectivement; alors il existe a et b deux entiers tels que : $\frac{w_1}{n} = aw_1 + b\frac{w_2}{N}$, ce qui entraîne que $(N - anN)w_1 - bnw_2 = 0$, par conséquent $n = 1$. D'où η est primitif.

• On pose $a = L$, alors a est un idéal fractionnaire de $\mathcal{O}$ et $L' = a\eta^{-1}$. Par conséquent on a, $z : (\mathbf{C}/a \xrightarrow{id} \mathbf{C}/a\eta^{-1})$, où a et η vérifient les conditions de la proposition.

• Réciproquement, soient a un idéal fractionnaire de $\mathcal{O}$ et η un idéal entier primitif, de norme N; alors les courbes elliptiques $\mathbf{C}/a$ et $\mathbf{C}/a\eta^{-1}$ ont la même multiplication complexe par $\mathcal{O}$ et l'isogénie : $\mathbf{C}/a \to \mathbf{C}/a\eta^{-1}$ induite par $id_{\mathbf{C}}$ définit un point de Heegner de $Y_0(N)$.

$*$ Montrons qu'un tel point ne dépend que de K, de η et de $[a]$:

Supposons que (a_1, η_1) et (a_2, η_2) définissent le même point de Heegner de $Y_0(N)$, alors les deux couples $(\mathbf{C}/a_1 \xrightarrow{id} \mathbf{C}/a_1\eta_1^{-1})$ et $(\mathbf{C}/a_2 \xrightarrow{id} \mathbf{C}/a_2\eta_2^{-1})$ appartiennent à la même classe. Ce qui entraîne qu'il existe un complexe λ tel que $a_2 = \lambda a_1$ et $a_2\eta_2^{-1} = \lambda a_1\eta_1^{-1}$ (en fait, $\lambda \in K$). D'où $[a_1] = [a_2]$ et $\eta_1 = \eta_2$; ce qui achève la démonstration de la proposition 3. ∎

Remarque : D'après la proposition 3, l'existence des points de Heegner de $Y_0(N)$ de discriminant D est liée à l'existence des idéaux η. Pour un idéal η, il existe h points de Heegner et comme η est de norme N, donc il y a au plus un nombre fini de tels points.

4 - L'existence des idéaux η.

Proposition 4. *On pose :* $N = p_1^{r_1}.....p_s^{r_s}$ *où les* p_i *sont des nombres premiers distincts et les* r_i *des entiers* ≥ 1.

Alors η *existe ssi pour tout* $i = 1, \ldots, s$, *on a* $(\frac{D}{p_i}) = 1$, *où (-) est le symbole de Legendre.*

Dans le cas où $(\frac{D}{p_i}) = 1$ *pour tout* i, *il existe* 2^s *idéaux* η.

■ Soit p un nombre premier, alors on sait que : ou p reste inerte (i.e. (p) est un idéal premier) $\Leftrightarrow (\frac{D}{p}) = -1$, ou p se décompose (i.e. $(p) = \mathcal{P}\mathcal{P}'$ avec $\mathcal{P}, \mathcal{P}'$, deux idéaux premiers) $\Leftrightarrow (\frac{D}{p}) = 1$, ou p se ramifie (i.e. $(p) = \mathcal{P}^2$ avec $\mathcal{P}$ un idéal premier) $\Leftrightarrow p$ divise D.

Puisque $(D, N) = 1$, donc pour tout $i = 1, \ldots, s$, p_i ne se ramifie pas.

$*$ Supposons qu'il existe $i_0 \in \{1, \ldots, s\}$ tel que (p_{i_0}) est un idéal premier. On a $N(\eta) = N$, donc $(N) = \eta\overline{\eta}$, où $\overline{\eta}$ est le conjugué de η. Comme (p_{i_0}) divise (N) et (p_{i_0}) est premier donc (p_{i_0}) divise η ou $\overline{\eta}$; ce qui est contradictoire avec le fait que η et $\overline{\eta}$ sont primitifs. Par conséquent, pour que η existe, il faut que les p_i se décomposent, pour tout $i = 1, \ldots, s$.

$*$ Montrons qu'il existe 2^s idéaux η, dans le cas où les p_i se décomposent :

Posons $(p_1) = \mathcal{P}_1\mathcal{P}'_1$, $(p_2) = \mathcal{P}_2\mathcal{P}'_2, \ldots, (p_s) = \mathcal{P}_s\mathcal{P}'_s$, la décomposition en idéaux premiers des (p_i). Comme $N(\eta) = N$, donc pour tout $i = 1, \ldots, s$, on a : $\mathcal{P}_i$ divise η ou $\mathcal{P}'_i$ divise η (le "ou" est exclusif, puisque η est primitif).

Si $s = 1$, on a $\eta = \mathcal{P}_1^{r_1}$ ou $\eta = \mathcal{P}_1'^{r_1}$, soit 2 idéaux.

Si $s = 2$, on a $\eta = \mathcal{P}_1^{r_1}\mathcal{P}_2^{r_2}$ ou $\eta = \mathcal{P}_1^{r_1}\mathcal{P}'^{r_2}_2$ ou $\eta = \mathcal{P}'^{r_1}_1\mathcal{P}_2^{r_2}$ ou $\eta = \mathcal{P}'^{r_1}_1\mathcal{P}'^{r_2}_2$, soit 4 idéaux.

Supposons qu'à l'ordre $s-1$, on a 2^{s-1} idéaux η; soit $\eta_1, \eta_2, \ldots, \eta_{2^{s-1}}$. Alors à l'ordre s, les idéaux η sont :

$$\eta_1\mathcal{P}_s^{r_s}, \eta_2\mathcal{P}_s^{r_s}, \ldots, \eta_{2^{s-1}}\mathcal{P}_s^{r_s}; \eta_1\mathcal{P}'^{r_s}_s, \ldots, \eta_{2^{s-1}}\mathcal{P}'^{r_s}_s$$

soit 2^s idéaux. D'où la proposition 4. ■

Remarque.

Si tous les p_i divisant N, se décomposent, pour $i = 1, \ldots, s$; alors on a 2^s idéaux η. Par conséquent, il existe $2^s h$ points de Heegner de $Y_0(N)$ de discriminant D. Par contre, s'il existe un p tel que p reste inerte, alors $Y_0(N)$ n'admet pas de point de Heegner de discriminant D.

5 - Une caractérisation des idéaux primitifs.

Proposition 5. *On a la correspondance suivante :*

$$\left\{ \begin{array}{l} a \text{ un idéal entier primitif} \\ \text{de } \mathcal{O}, \text{ de norme } A \end{array} \right\} \Longleftrightarrow \left\{ \begin{array}{l} \beta \text{ une solution de la congruence :} \\ B^2 \equiv D \mod (4A) \text{ dans } \mathbf{Z}/2A\mathbf{Z} \end{array} \right\}$$

$$a = \left(A, \frac{\beta + \sqrt{D}}{2} \right)_{\mathbf{Z}-\text{base}} \longleftarrow \beta \, .$$

■ • D'abord, on va démontrer que si a est un idéal primitif de norme A, alors il existe $\alpha \in a$ tel que $a = (A, \alpha)$, une $\mathbf{Z}$-base.

On a $N(a) = A$, donc $(A) = a\overline{a}$. Soit k un entier > 1; si $A/k \in a$, alors il existe un idéal entier $\mathcal{D}$ tel que $\overline{a} = (k)\mathcal{D}$. Or $\overline{a}$ est primitif, puisque a l'est; donc $A/k \notin a$ pour tout entier $k > 1$.

Soit (w_1, w_2) une $\mathbf{Z}$-base de a; comme $A \in a$ et $A/k \notin a$ pour tout $k > 1$, donc il existe deux entiers a et b tels que : $A = aw_1 + bw_2$ et $(a, b) = 1$.

D'après Bezout, il existe deux entiers c et d tels que la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ soit unimodulaire. On prend : $\alpha = cw_1 + dw_2$, d'où (A, α) est une $\mathbf{Z}$-base de a.

$*$ a étant primitif de norme A, donc il existe $\alpha \in a$ tel que $a = (A, \alpha)$. On pose : $\alpha = a + b\frac{1+\sqrt{D}}{2}$ où a et$b$ sont des entiers. On a $N(a) = \left\| \begin{matrix} A & 0 \\ a & b \end{matrix} \right\| = A|b| = A$, donc $|b| = 1$; d'où quitte à remplacer α par $(-\alpha)$ dans le cas où $b = -1$, on peut écrire : $\alpha = \frac{\beta+\sqrt{D}}{2}$ avec β un entier tel que $|\beta| < 2A$. Comme $\frac{\beta+\sqrt{D}}{2} \in a$, par passage aux normes, on a : A divise $\frac{\beta^2-D}{4}$; par conséquent, $\beta^2 \equiv D \mod (4A)$. D'où $a = (A, \frac{\beta+\sqrt{D}}{2})$ avec β une solution de la congruence : $B^2 \equiv D \mod (4A)$ dans $\mathbf{Z}/2A\mathbf{Z}$.

• Récriproquement, soit $\beta \in \mathbf{Z}/2A\mathbf{Z}$ tel que $\beta^2 \equiv D \bmod (4A)$. On pose $a = \left(A, \frac{\beta+\sqrt{D}}{2}\right)$, alors a est bien de norme A. Montrons qu'il est primitif. Supposons qu'il existe un entier k tel que (k) divise a, alors il existe a et b deux entiers tels que $\frac{\beta+\sqrt{D}}{2} = k\left(a + b\frac{1+\sqrt{D}}{2}\right)$, d'où $k = \pm 1$. Par conséquent, a est primitif. Ce qui prouve la proposition 5. ∎

Remarques :

— Soit s le nombre des diviseurs premiers de N, on sait que le nombre des solutions de la congruence : $\beta^2 \equiv D \bmod (4N)$ dans $\mathbf{Z}/2N\mathbf{Z}$ est $\prod_{\substack{p/N \\ p \text{ premier}}} \left(1 + (\frac{D}{p})\right)$, puisque $(N, D) = 1$.

Ce nombre est égal à 2^s (resp. zéro) si tous les p se décomposent (resp. s'il existe un p qui reste inerte). Ce qui justifie la cohérence entre l'existence des solutions β et les idéaux η.

— Si D est un carré modulo $4N$, alors la congruence : $\beta^2 \equiv D \bmod (4N)$ admet 2^s solutions β dans $\mathbf{Z}/2N\mathbf{Z}$. D'où il existe $2^s h$ points de Heegner de $Y_0(N)$ de discriminant D. Ce qui prouve que le fait que D soit un carré modulo $4N$ est une condition nécessaire et suffisante pour l'existence des points de Heegner de discriminant D (rappelons que D est fondamental, $D \equiv 1 \bmod (4)$ et $(D, N) = 1$).

6 - Détermination analytique des points de Heegner.

On suppose que D est un carré modulo (4N), soient alors $\beta_0 \in \mathbf{Z}/2N\mathbf{Z}$ tel que $\beta_0^2 \equiv D \bmod (4N)$, $\eta_0 = \left(N, \frac{\beta_0+\sqrt{D}}{2}\right)$ l'idéal primitif correspondant à la solution β_0 et a un idéal appartenant à une certaine classe du groupe cl_K. On veut déterminer le point z de H, défini modulo $\Gamma_0(N)$, correspondant à la classe d'isomorphie du couple $(\mathbf{C}/a \xrightarrow{id} \mathbf{C}/a\eta_0^{-1})$.

— D'abord, on va démontrer qu'on peut supposer que a est primitif et $a \subset \eta_0$ (i.e. il existe un idéal $\mathcal{B} \subset \eta_0$, primitif, tel que $[a] = [\mathcal{B}]$) :

Soit $cl_K = \{[a_1], [a_2], \ldots, [a_h]\}$, où les a_i pour $i = 1, \ldots, h$ constituent un système complet de représentants des classes d'idéaux de K. On peut supposer que les a_i sont primitifs, quitte à les remplacer par des idéaux primitifs équivalents.

On pose $\mathcal{B}_i = a_i\eta_0$, alors on a $cl_K = \{[\mathcal{B}_i],\ i = 1, \ldots, h\}$.

Si les $\mathcal{B}_i$ sont primitifs, alors le problème est résolu.

Supposons par exemple, que $\mathcal{B}_1$ est non primitif, donc il existe un nombre premier p tel que (p) divise $\mathcal{B}_1$. Comme a_1 est primitif et tout idéal premier divisant η_0 provient d'un nombre premier qui se décompose, donc p se décompose. Par conséquent, il existe un idéal $\mathcal{P}$ premier, tel que $\mathcal{P}$ divise η_0 et $\overline{\mathcal{P}}$ divise a_1. D'où, — en utilisant le fait que les puissances de η_0 sont primitives — quitte à multiplier les a_i par une puissance convenable de η_0 et à prendre la partie primitive, on peut supposer que les $\mathcal{B}_i$ sont primitifs et $\mathcal{B}_i \subset \eta_0$.

— Soit le couple $(\mathbf{C}/a \overset{id}{\to} \mathbf{C}/a\eta_0^{-1})$ avec a primitif et $a \subset \eta_0$, on pose $N(a) = A$. D'après la proposition 5, il existe un entier $B \in \mathbf{Z}/2A\mathbf{Z}$ avec $B^2 \equiv D \bmod (4A)$ tel que $a = \left(A, \frac{B+\sqrt{D}}{2}\right)$. Comme $a \subset \eta_0$ et a primitif, donc $a\eta_0^{-1}$ est un idéal entier primitif et $A \equiv 0 \bmod (N)$. Par conséquent, il existe un entier B' tel que $a\eta_0^{-1} = \left(\frac{A}{N}, \frac{B'+\sqrt{D}}{2}\right)$. On va démontrer qu'on peut prendre $B' = B$ et que $B \equiv \beta_0 \bmod (2N)$:

On a $a \subset a\eta_0^{-1}$, donc il existe deux entiers x et y tels que :
$\frac{B+\sqrt{D}}{2} = x\frac{A}{N} + y\frac{B'+\sqrt{D}}{2}$ ce qui entraîne que $y = 1$ et donc $B \equiv B' \bmod (2\frac{A}{N})$. D'où, on peut prendre $B' = B$.

On sait que $a \subset \eta_0$, donc il existe deux entiers x et y tels que :
$\frac{B+\sqrt{D}}{2} = xN + y\frac{\beta_0+\sqrt{D}}{2}$, ce qui entraîne que $y = 1$ et donc $B \equiv \beta_0 \bmod (2N)$.

Par conséquent, on a :

$$(\mathbf{C}/a \overset{id}{\to} \mathbf{C}/a\eta_0^{-1}) \simeq (\mathbf{C}/L_z \overset{N}{\to} \mathbf{C}/L_{Nz}) \text{ où } z = \frac{B+\sqrt{D}}{2A}.$$

Ce qui entraîne que z est solution de l'équation quadratique : $Az^2 - Bz + C = 0$, où C est un entier tel que $D = B^2 - 4AC$, $A > 0$, $A \equiv 0 \bmod (N)$ et $B \equiv \beta_0 \bmod (2N)$.

Finalement, on vérifie facilement, que si $z' = \gamma(z)$ avec $\gamma \in \Gamma_0(N)$, alors z' sera solution d'une équation : $A'^2z'^2 - B'z' + C' = 0$ avec $A' \equiv 0 \bmod (N)$ et $B' \equiv B \equiv \beta_0 \bmod (2N)$. D'où on a la proposition suivante :

Proposition 6. *Un point de Heegner de $Y_0(N)$ de discriminant D a toujours une représentation du type : $(\mathbf{C}/a \overset{id}{\to} \mathbf{C}/a\eta^{-1})$ avec $\eta = \left(N, \frac{\beta+\sqrt{D}}{2}\right)$, $a = \left(A, \frac{B+\sqrt{D}}{2}\right)$, et $a\eta^{-1} = \left(\frac{A}{N}, \frac{B+\sqrt{D}}{2}\right)$, où $\beta \in \mathbf{Z}/2N\mathbf{Z}$, $\beta^2 \equiv D \bmod (4N)$, $A = N(a)$, $A \equiv 0 \bmod (N)$ et $B \equiv \beta \bmod (2N)$. Dans ce cas, le point z de H correspondant est : $z = \frac{B+\sqrt{D}}{2A}$.*

Réciproquement, soit $z \in H$, un point de Heegner de $Y_0(N)$; alors z est solution d'une équation quadratique : $Az^2 + Bz + C = 0$ tel que $D = B^2 - 4AC$ et $A \equiv 0 \bmod (N)$. La classe de la forme $[A, B, C]$ détermine la classe de a et la classe de B modulo $2N$, détermine l'idéal η.

7 - Structure rationnelle sur $Y_0(N)$. Points de Heegner.

Soit K un corps extension de Q, il existe une structure Q- rationnelle sur $Y_0(N)$ caractérisée par : un point z de $Y_0(N)$ est rationnel sur K ssi on peut trouver dans l'ensemble des couples de courbes elliptiques correspondant à z un représentant $(E \xrightarrow{\alpha} E')$ tel que E', E et α soient définies sur K.

Soit $z \in H$, quadratique de discriminant Δ, d'après la théorie des corps de classes, le corps $Q(z, j(z))$ dépend de Δ plutôt que de z, c'est le corps des classes de l'anneau $\mathbf{Z} + \frac{1}{2}(\Delta + \sqrt{\Delta})\mathbf{Z}$.

Conséquence.

Soit z un point de Heegner de $Y_0(N)$ de discriminant D, alors on a :

$$z : \left(\mathbf{C}/L_z \xrightarrow{N} \mathbf{C}/L_{Nz}\right) \text{ avec } \Delta(z) = \Delta(Nz) = D \, .$$

L_z et L_{Nz} sont des idéaux de $\mathcal{O}$.

Par conséquent, z est rationnel sur $K(j(\mathcal{O}))$, le corps des classes de Hilbert de K, $(K = Q(\sqrt{D}))$.

CHAPITRE III

CALCUL DES POINTS DE HEEGNER DE $Y_0(N)$

1 - Méthode de détermination.

Soient N un entier ≥ 1 et D un discriminant fondamental tel que $(D, N) = 1$ et $D \equiv 1 \bmod (4)$. Si D n'est pas un carré modulo $4N$, alors $Y_0(N)$ n'admet pas de point de Heegner de discriminant D. Dans le cas contraire, $Y_0(N)$ admet $2^s h(D)$ points de Heegner où s est le nombre des diviseurs premiers distincts de N et $h(D)$ est le nombre des classes d'idéaux de $K = Q\sqrt{D})$.

Pour déterminer ces points (définis modulo $\Gamma_0(N)$), il faut, pour chaque idéal $\eta = (N, \frac{\beta+\sqrt{D}}{2})$ où $\beta \in \mathbf{Z}/2N\mathbf{Z}$ et $\beta^2 \equiv D \bmod (4N)$, trouver un système complet de représentants des classes d'idéaux de K : $a_1, \ldots, a_{h(D)}$, avec $a_i = \left(A_i, \frac{B_i+\sqrt{D}}{2}\right)$, $A_i \equiv 0 \bmod (N)$ et $B_i \equiv \beta \bmod (2N)$ pour $1 \leq i \leq h(D)$. Ainsi, relativement à un idéal η les points de Heegner sont : $\frac{B_i+\sqrt{D}}{2A_i} \bmod (\Gamma_0(N))$, $1 \leq i \leq h(D)$.

Remarque :

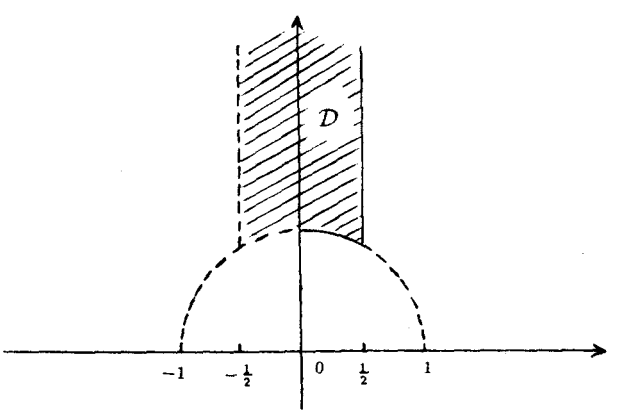
Si D est un carré modulo $4N$ et $h(D) = 1$, alors les points de Heegner sont : $\frac{\beta+\sqrt{D}}{2N} \bmod \Gamma_0(N)$, où β est une solution dans $\mathbf{Z}/2N\mathbf{Z}$ de la congruence $\beta^2 \equiv D \bmod (4N)$.

2 - Exemples.

2.1 - Cas : $N = 1$.

Un domaine fondamental de $Y_0(1)$ est donné par :

$$\mathcal{D} = \{z \in H/|z| \geq 1,\ -\frac{1}{2} < \mathrm{Rez} \leq \frac{1}{2} \quad \text{et} \quad \mathrm{Rez} \geq 0 \quad \text{quand} \quad |z| = 1\}\ .$$



Dans ce cas particulier, la congruence $\beta^2 \equiv D \bmod (4)$, admet une seule solution dans $\mathbf{Z}/2\mathbf{Z}$: $\beta = 1$, soit $\eta = \mathcal{O}$. Par conséquent, $Y_0(1)$ admet $h(D)$ points de Heegner pour tout discriminant D (en fait, ce sont les éléments de H définis modulo $\Gamma_0(1)$, quadratiques, de discriminant D).

2.1.1 - Si $h(D) = 1$, $Y_0(1)$ admet un seul point de Heegner de discriminant D : $\frac{1+\sqrt{D}}{2} \bmod \Gamma_0(1)$.

Exemples :

$$D = -3\ ; -7\ ; -11\ ; -19\ ; -43\ ; -67\ ; -163\ .$$

(ce sont les seuls discriminants).

2.1.2 - Si $h(D) \geq 2$, il faut trouver un système complet de représentants primitifs des classes d'idéaux : $a_1, \ldots, a_{h(D)}$. Si $a_i = \left(A_i, \frac{B_i+\sqrt{D}}{2}\right)$, les points de Heegner sont : $\frac{B_i+\sqrt{D}}{2A_i} \bmod \Gamma_0(1)$, $1 \leq i \leq h(D)$.

Exemples.

$\underline{D = -15.}$

On a : $h(-15) = 2$ et $cl(Q(\sqrt{-15})) = \{[\mathcal{O}], [\mathcal{P}]\}$, où $\mathcal{P} = (2, \frac{1+\sqrt{-15}}{2})$.

Par conséquent, les points de Heegner sont :

$\frac{1+\sqrt{-15}}{2}$ et $\frac{1+\sqrt{-15}}{4} \bmod \Gamma_0(1)$.

$\underline{D = -23.}$

On a : $h(-23) = 3$ et $cl(Q(\sqrt{-23})) = \{[\mathcal{O}], [\mathcal{P}], [\mathcal{P}']\}$, où
$\mathcal{P} = \left(2, \frac{1+\sqrt{-23}}{2}\right)$ et $\mathcal{P}' = (3, \frac{1+\sqrt{-23}}{2})$.

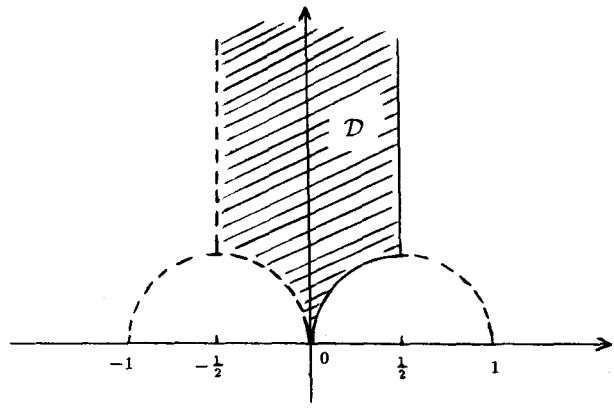
Par conséquent, les points de Heegner sont :

$$\frac{1+\sqrt{-23}}{2},\ \frac{1+\sqrt{-23}}{4},\ \text{et}\ \frac{1+\sqrt{-23}}{6} \bmod \Gamma_0(1)\ .$$

2.2 - Cas : $N = 2$.

Un domaine fondamental de $Y_0(2)$ est donné par :

$$\mathcal{D} = \{z \in H / -\frac{1}{2} < \text{Rez} \leq \frac{1}{2}\ ,\quad |z - \frac{1}{2}| \geq \frac{1}{2}\quad \text{et}\quad |z + \frac{1}{2}| > \frac{1}{2}\}\ .$$



Pour qu'il existe des points de Heegner de $Y_0(2)$, il faut et il suffit que $D \equiv 1 \bmod (8)$.

Soit $D \equiv 1 \bmod (8)$, les solutions de la congruence : $\beta^2 \equiv D \bmod (8)$, dans $\mathbf{Z}/4\mathbf{Z}$ sont (± 1) . D'où les idéaux primitifs de norme 2 sont :

$$\eta_1 = (2, \frac{1+\sqrt{D}}{2}) \quad \text{et} \quad \eta_1' = (2, \frac{-1+\sqrt{D}}{2}) .$$

2.2.1 - Si $h(D) = 1$, $Y_0(2)$ admet deux points de Heegner : $\frac{\pm 1+\sqrt{D}}{4} \bmod \Gamma_0(2)$.

Exemple : $D = -7$ (c'est le seul exemple).

2.2.2 - Si $h(D) \geq 2$, soient $a_1, \ldots, a_{h(D)}$, un système complet de représentants des classes d'idéaux de $Q(\sqrt{D})$, relativement à η_1, i.e. $a_i = (A_i, \frac{B_i+\sqrt{D}}{2})$ avec $A_i \equiv 0 \bmod (2)$ et $B_i \equiv 1 \bmod (4)$. En posant $a_i' = (A_i, \frac{-B_i+\sqrt{D}}{2})$, on remarque que $a_i a_i' = (A_i)$ et $-B_i \equiv -1 \bmod (4)$. D'où les a_i', $i = 1, \ldots, h(D)$ constituent un système complet de représentants des classes d'idéaux de $Q(\sqrt{D})$, relativement à η_1'. Par conséquent, les points de Heegner sont :

$$\frac{\pm B_i + \sqrt{D}}{2A_i} \bmod \Gamma_0(2), 1 \leq i \leq h(D) .$$

On remarque que η_1 et η_1' sont non principaux, d'où :

Si $h(D) = q$ un nombre premier, alors $cl(Q(\sqrt{D})) = \{[\eta_1], [\eta_1^2], \ldots, [\eta_1^q]\}$. Comme η_1 est primitif et tous les nombres premiers qui divisent N se décomposent, alors toutes les puissances de η_1 sont primitives, donc on peut écrire :

$\eta^i = (2^i, \frac{B_i+\sqrt{D}}{2})$ avec $B_i^2 \equiv D \bmod (2^{i+2})$, $B_i \in \mathbf{Z}/2^{i+1}\mathbf{Z}$ et $B_i \equiv 1 \bmod (4)$, pour $1 \leq i \leq q$, en posant $B_1 = 1$. Par conséquent, les points de Heegner sont : $\frac{\pm B_i+\sqrt{D}}{2^{i+1}} \bmod \Gamma_0(2)$, $1 \leq i \leq q$. Ainsi pour trouver les points de Heegner, il suffit de trouver les B_i. Mais, comme $B_i^2 \equiv B_{i-1}^2 \bmod (2^{i+1})$ et $B_i \equiv B_{i-1} \equiv 1 \bmod (4)$, donc $B_i \equiv B_{i-1} \bmod (2^i)$. On vérifie facilement que : $B_i = B_{i-1} + 2^i k$ avec $k = 0$, ± 1 ou ± 2 . D'où la proposition suivante :

Proposition 1. *Les points de Heegner de $Y_0(2)$ de discriminant D avec $h(D) = q$, un nombre premier sont : $\frac{\pm B_i+\sqrt{D}}{2^{i+1}} \bmod \Gamma_0(2)$, où $(B_i)_{1\leq i\leq q}$ vérifie : $B_1 = 1$, $B_i^2 \equiv D \bmod (2^{i+2})$, $B_i \in \mathbf{Z}/2^{i+1}\mathbf{Z}$ et $B_i \equiv B_{i-1} \bmod (2^i)$.*

Soit $1 \leq i \leq q-1$ fixé, pour trouver B_{i+1}, connaissant B_i, il suffit de trouver un entier $k = 0$, ± 1 ou ± 2 tel que : $(B_i + 2^{i+1}k)^2 \equiv D \bmod (2^{i+3})$. Ainsi, on prendra : $B_{i+1} = B_i + 2^{i+1}k$.

Exemples :

$D = -15$, $h(-15) = 2$.

On trouve : $B_1 = B_2 = 1$. D'où les points de Heegner sont :

$$\frac{\pm 1 + \sqrt{-15}}{4} \text{ et } \frac{\pm 1 + \sqrt{-15}}{8} \bmod \Gamma_0(2) .$$

$D = -23$, $h(-23) = 3$.

On trouve : $B_1 = 1$, $B_2 = -3$ et $B_3 = 3$. D'où les points de Heegner sont :

$$\frac{\pm 1 + \sqrt{-23}}{4}, \frac{\pm 3 + \sqrt{-23}}{8} \text{ et } \frac{\pm 3 + \sqrt{-23}}{16} \bmod \Gamma_0(2) .$$

$D = -47$, $h(-47) = 5$.

On trouve : $B_1 = B_2 = 1$, $B_3 = -7$ et $B_4 = B_5 = 9$.

D'où les points de Heegner sont :

$$\frac{\pm 1 + \sqrt{-47}}{4} ; \frac{\pm 1 + \sqrt{-47}}{8} ; \frac{\pm 7 + \sqrt{-47}}{16} ;$$

$$\frac{\pm 9 + \sqrt{-47}}{32} \text{ et } \frac{\pm 9 + \sqrt{-47}}{64} \bmod \Gamma_0(2) ,$$

2.3 - Cas : $N = 2^n, n \geq 1$.

Pour qu'il existe des points de Heegner de $Y_0(2^n)$ *de discriminant* D, *il faut et il suffit que* $D \equiv 1 \bmod (8)$.

Soit $D \equiv 1 \bmod (8)$, *soient* $(\pm B_n)$ *les solutions de la congruence :* $B^2 \equiv D \bmod (2^{n+2})$, *dans* $\mathbf{Z}/2^{n+1}\mathbf{Z}$, *avec* $B_n \equiv 1 \bmod (4)$. *Les idéaux primitifs de norme* 2^n *sont alors :*

$$\eta_n = (2^n, \frac{B_n + \sqrt{D}}{2}) \text{ et } \eta_n' = (2^n, \frac{-B_n + \sqrt{D}}{2}) ;$$

D'après la proposition 1, on a : $B_n = B_{n-1} + 2^n k$ *où* $k = 0, \pm 1$ *ou* ± 2, *tel que :*

$$B_n^2 \equiv D \bmod (2^{n+2}) .$$

2.3.1 - *Si* $h(D) = 1$,

les points de Heegner de $Y_0(2^n)$ sont :
$\frac{\pm B_n + \sqrt{D}}{2^{n+1}} \bmod \Gamma_0(2^n)$.

Exemple : $\underline{D = -7.}$

Si $n = 2$, on trouve $B_2 = -3$; d'où, les points de Heegner de $Y_0(4)$ sont :

$$\frac{\pm 3 + \sqrt{-7}}{8} \bmod \Gamma_0(4) .$$

Si $n = 3$, on trouve $B_3 = -3$; d'où, les points de Heegner de $Y_0(8)$ sont :

$$\frac{\pm 3 + \sqrt{-7}}{16} \bmod \Gamma_0(8) .$$

2.3.2 - Si $h(D) \geq 2$, alors $\eta_1 = (2, \frac{1 \pm \sqrt{D}}{2})$ est un idéal non principal, d'où :

Si $h(D) = q$, **un nombre premier,** alors $cl(Q(\sqrt{D})) = \{[\eta_1], \ldots, [\eta_1^q]\}$.

On a $\eta_n = (2^n, \frac{B_n + \sqrt{D}}{2})$, avec $B_n \equiv D \bmod (2^{n+2})$, $B_n \in \mathbf{Z}/2^{n+1}\mathbf{Z}$ et $B_n \equiv 1 \bmod (4)$.

On pose : $\eta_{n+i} = \eta_n \eta_1^i = \eta_1^{n+i} = (2^{n+i}, \frac{B_{n+i} + \sqrt{D}}{2})$, pour $0 \leq i \leq q-1$, alors on a : $2^{n+i} \equiv 0 \bmod (2^n)$, $B_{n+i} \equiv B_n \bmod (2^{n+i})$ et $cl(Q(\sqrt{D})) = \{[\eta_n], [\eta_{n+1}], \ldots, [\eta_{n+q-1}]\}$.

Par conséquent, les points de Heegner sont :

$$\frac{\pm B_{n+i} + \sqrt{D}}{2^{n+i+1}} \bmod \Gamma_0(2^n) .$$

D'où la proposition suivante :

Proposition 2. *Les points de Heegner de $Y_0(2^n)$ de discriminant D, avec $h(D) = q$ un nombre premier sont :*

$$\frac{\pm B_{n+i} + \sqrt{D}}{2^{n+i+1}} \bmod \Gamma_0(2^n),\ \textit{où}\ (B_{n+i})_{0 \le i \le q-1}\ \textit{vérifie}\ :$$

$$B_{n+i}^2 \equiv D \bmod (2^{n+i+2}),\ B_{n+i} \in \mathbf{Z}/2^{n+i+1}\mathbf{Z} \quad \textit{et} \quad B_{n+i} \equiv 1 \bmod (4)\ .$$

Pour trouver les B_j, il suffit d'appliquer l'algorithme de la proposition 1.

Remarque : La proposition 1 est un cas particulier de la proposition 2.

Exemples :

$\underline{D = -15}$, $h(-15) = 2$.

Pour $n = 2$, on trouve $B_2 = 1$, $B_3 = -7$. D'où les points de Heegner de $Y_0(4)$ sont :

$$\frac{\pm 1 + \sqrt{-15}}{8} \text{ et } \frac{\pm 7 + \sqrt{-15}}{16} \bmod \Gamma_0(4)\ .$$

Pour $n = 3$, on trouve : $B_3 = B_4 = -7$.

D'où les points de Heegner de $Y_0(8)$ sont :

$$\frac{\pm 7 + \sqrt{-15}}{16} \text{ et } \frac{\pm 7 + \sqrt{-15}}{32} \bmod \Gamma_0(8)\ .$$

$\underline{D = -23}$, $h(-23) = 3$.

Pour $n = 2$, on trouve $B_2 = B_3 = -3$ et $B_4 = 13$.

D'où les points de Heegner de $Y_0(4)$ sont :

$$\frac{\pm 3 + \sqrt{-23}}{8}\ ;\ \frac{\pm 3 + \sqrt{-23}}{16} \text{ et } \frac{\pm 13 + \sqrt{-23}}{32} \bmod \Gamma_0(4)\ .$$

Pour $n = 3$, on trouve : $B_3 = -3$, $B_4 = 13$ et $B_5 = -19$.

D'où les points de Heegner de $Y_0(8)$ sont :

$$\frac{\pm 3 + \sqrt{-23}}{16}\ ;\ \frac{\pm 13 + \sqrt{-23}}{32} \quad \text{et} \quad \frac{\pm 19 + \sqrt{-23}}{64} \bmod \Gamma_0(8)\ .$$

$\underline{D = -47}$, $h(-47) = 5$.

Pour $n = 2$, on trouve : $B_2 = 1$, $B_3 = -7$, $B_4 = B_5 = 9$ et $B_6 = -55$.

D'où les points de Heegner de $Y_0(4)$ sont :

$$\frac{\pm 1+\sqrt{-47}}{8}\ ;\ \frac{\pm 7+\sqrt{-47}}{16}\ ;\ \frac{\pm 9+\sqrt{-47}}{32}\ ;$$
$$\frac{\pm 9+\sqrt{-47}}{64}\quad \text{et}\quad \frac{\pm 55+\sqrt{-47}}{128} \bmod \Gamma_0(4)\ .$$

Pour $n=3$, on trouve $B_3=-7$, $B_4=B_5=9$ et $B_6=B_7=-55$.

D'où les points de Heegner de $Y_0(8)$ sont :

$$\frac{\pm 7+\sqrt{-47}}{16}\ ;\ \frac{\pm 9+\sqrt{-47}}{32}\ ;\ \frac{\pm 9+\sqrt{-47}}{64}\ ;$$
$$\frac{\pm 55+\sqrt{-47}}{128}\quad \text{et}\quad \frac{\pm 55+\sqrt{-47}}{256} \bmod \Gamma_0(8)\ .$$

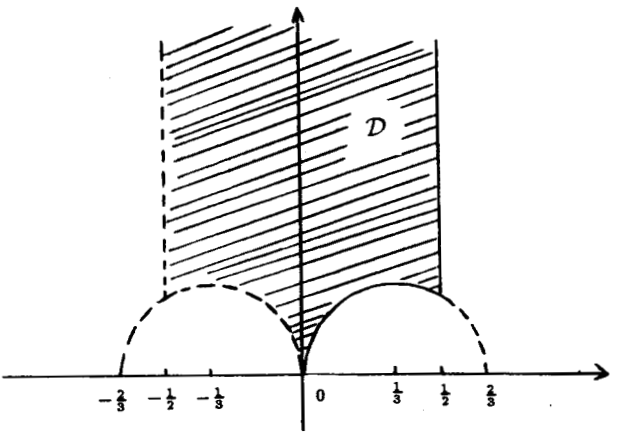
Remarque :

Si $w_1, w_2, \ldots, w_r$ sont les points de Heegner de $Y_0(2^n)$ de discriminant D, alors $(r-1)$ points parmi eux, sont des points de Heegner de $Y_0(2^{n+1})$.

2.4 - Cas : $N=3$.

Un domaine fondamental de $Y_0(3)$ est donné par :

$$\mathcal{D}=\{z\in H/\ -\frac{1}{2}<\mathrm{Re}z\leq\frac{1}{2},\ |z-\frac{1}{3}|\geq\frac{1}{3}\ \text{et}\ |z+\frac{1}{3}|>\frac{1}{3}\}\ .$$



Pour qu'il existe des points de Heegner de $Y_0(3)$ de discriminant D, il faut et il suffit que D soit un carré mod(12); mais, comme $D\equiv 1 \bmod (4)$ et $(D,3)=1$, donc il faut que $D\equiv 1 \bmod (12)$.

Soit $D \equiv 1 \bmod (12)$; les solutions dans $\mathbf{Z}/6\mathbf{Z}$ de la congruence : $\beta^2 \equiv D \bmod (12)$, sont : (± 1). D'où, les idéaux primitifs de norme 3 sont :

$$\eta_1 = (3, \frac{1+\sqrt{D}}{2}) \text{ et } \eta_1' = (3, \frac{-1+\sqrt{D}}{2}) .$$

2.4.1 - Si $h(D) = 1$, alors $Y_0(3)$ admet deux points de Heegner : $\frac{\pm 1 \pm \sqrt{D}}{6} \bmod \Gamma_0(3)$.

Exemple : $D = -11$. (C'est le seul exemple).

2.4.2 - Si $h(D) \geq 2$, alors $|D| > 12$, ce qui entraîne que η_1 est non principal; d'où :

Si $h(D) = q$**, un nombre premier,** alors $cl(Q(\sqrt{D})) = \{[\eta_1], [\eta_1^2], \ldots, [\eta_1^q]\}$, et on a : $\eta_1^i = (3^i, \frac{B_i+\sqrt{D}}{2})$ avec $B_i^2 \equiv D \bmod (4.3^i)$, $B_i \equiv 1 \bmod (6)$ et $B_i \in \mathbf{Z}/2 \cdot 3^i\mathbf{Z}$, pour $i = 1, \ldots, q$, en posant $B_1 = 1$.

Par conséquent, les points de Heegner sont :

$$\frac{\pm B_i + \sqrt{D}}{2 \cdot 3^i} \bmod \Gamma_0(3),\ 1 \leq i \leq q .$$

Méthode pour trouver B_i**, connaissant** B_{i-1}**.**

On a : $B_i^2 \equiv B_{i-1}^2 \bmod (4 \cdot 3^{i-1})$; comme $B_i \equiv B_{i-1} \equiv 1 \bmod (3)$, donc 3 ne divise pas $B_i + B_{i-1}$. D'autre part, $B_i \equiv B_{i-1} \bmod (2)$. Par conséquent, $B_i \equiv B_{i-1} \bmod (2 \cdot 3^{i-1})$. On vérifie facilement qu'on peut prendre $B_i = B_{i-1} + 2 \cdot 3^{i-1}k$, où $k = 0$ ou ± 1 tel que $B_i^2 \equiv D \bmod (4 \cdot 3^i)$. D'où la proposition suivante :

Proposition 3. *Les points de Heegner de* $Y_0(3)$ *de discriminant* D*, avec* $h(D) = q$*, un nombre premier sont :*

$$\frac{\pm B_i + \sqrt{D}}{2 \cdot 3^i} \bmod \Gamma_0(3), \quad \textit{où } (B_i)_{1 \leq i \leq q} \quad \textit{vérifie :}$$

$B_1 = 1$, $B_i^2 \equiv D \bmod (4 \cdot 3^i)$, $B_i \in \mathbf{Z}/2 \cdot 3^i\mathbf{Z}$ *et* $B_i \equiv B_{i-1} \bmod (2 \cdot 3^{i-1})$.

Soit $1 \leq i \leq q-1$ *fixé, pour trouver* B_{i+1} *connaissant* B_i*, il suffit de trouver un entier* $k = 0$ *ou* ± 1 *tel que :* $(B_i + 2 \cdot 3^i k)^2 \equiv D \bmod (4.3^{i+1})$. *Ainsi, on prendra :* $B_{i+1} = B_i + 2.3^i k$.

Exemples :

$\underline{D = -23}$, $h(-23) = 3$.

On trouve : $B_1 = 1$, $B_2 = 7$ et $B_3 = 25$.

D'où, les points de Heegner de $Y_0(3)$ sont :

$$\frac{\pm 1 + \sqrt{-23}}{6} \; ; \; \frac{\pm 7 + \sqrt{-23}}{18} \text{ et } \frac{\pm 25 + \sqrt{-23}}{54} \bmod \Gamma_0(3) \, .$$

$\underline{D = -35}$, $h(-35) = 2$.

On trouve : $B_1 = B_2 = 1$.

D'où, les points de Heegner de $Y_0(3)$ sont :

$$\frac{\pm 1 + \sqrt{-35}}{6} \text{ et } \frac{\pm 1 + \sqrt{-35}}{18} \bmod \Gamma_0(3) \, .$$

$\underline{D = -47}$, $h(-47) = 5$.

On trouve : $B_1 = 1$, $B_2 = -5$, $B_3 = 13$, $B_4 = 67$ et $B_5 = 229$.

D'où, les points de Heegner sont :

$$\frac{\pm 1 + \sqrt{-47}}{6} \; ; \; \frac{\pm 5 + \sqrt{-47}}{18} \; ; \; \frac{\pm 13 + \sqrt{-47}}{54} \; ;$$
$$\frac{\pm 67 + \sqrt{-47}}{162} \text{ et } \frac{\pm 229 + \sqrt{-47}}{486} \bmod \Gamma_0(3) \, .$$

2.5 - Cas : $N = 3^n$, $n \geq 1$.

Pour qu'il existe des points de Heegner de $Y_0(3^n)$, de discriminant D, il faut et il suffit que $D \equiv 1 \bmod (12)$.

Soit $D \equiv 1 \bmod (12)$**;** soient $(\pm B_n)$ les solutions dans $\mathbf{Z}/2.3^n\mathbf{Z}$ de la congruence : $B^2 \equiv D \bmod (4.3^n)$, avec $B_n \equiv 1 \bmod (6)$. Les idéaux primitifs de norme 3^n sont alors :

$$\eta_n = (3^n, \frac{B_n + \sqrt{D}}{2}) \text{ et } \eta'_n = (3^n, \frac{-B_n + \sqrt{D}}{2}) \, .$$

D'après le proposition 3, on peut prendre $B_n = B_{n-1} + 2 \cdot 3^{n-1} k$, avec $k = 0$ ou ± 1, tel que :

$$B_n^2 \equiv D \bmod (4 \cdot 3^n) \, .$$

2.5.1 - Si $h(D) = 1$, les points de Heegner de $Y_0(3^n)$ sont :
$\frac{\pm B_n + \sqrt{D}}{2 \cdot 3^n} \bmod \Gamma_0(3^n)$.

2.5.2 - Si $h(D) = q$, un nombre premier, alors par un raisonnement analogue au cas où $N = 2^n$, on obtient la proposition suivante :

Proposition 4. *Les points de Heegner de $Y_0(3^n)$ de discriminant D, avec $h(D) = q$, un nombre premier sont :*

$$\frac{\pm B_{n+i} + \sqrt{D}}{2 \cdot 3^{n+i}} \bmod \Gamma_0(3^n), \text{ où } (B_{n+i})_{0 \leq i \leq q-1} \text{ vérifie :}$$

$$B_{n+i}^2 \equiv D \bmod (4 \cdot 3^{n+i}), B_{n+i} \in \mathbf{Z}/2 \cdot 3^{n+i}\mathbf{Z} \text{ et } B_{n+i} \equiv 1 \bmod (6) .$$

Pour trouver les B_j, il suffit d'appliquer l'algorithme de la proposition 3.

Remarque : La proposition 3 est un cas particulier de la proposition 4. Si $h(D) = 1$, la proposition 4 reste valable.

Exemples :

$\underline{D = -11}$, $h(-11) = 1$.

Pour $n = 2$, on trouve : $B_1 = -5$.

D'où, les points de Heegner de $Y_0(9)$ sont :

$$\frac{\pm 5 + \sqrt{-11}}{18} \bmod \Gamma_0(9) .$$

Pour $n = 3$, on trouve : $B_3 = -23$.

D'où, les points de Heegner de $Y_0(27)$ sont :

$$\frac{\pm 23 + \sqrt{-11}}{54} \bmod \Gamma_0(27) .$$

$\underline{D = -23}$, $h(-23) = 3$.

Pour $n = 2$, on trouve : $B_2 = 7$, $B_3 = B_4 = 25$.

D'où, les points de Heegner de $Y_0(9)$ sont :

$$\frac{\pm 7 + \sqrt{-23}}{18} ; \frac{\pm 25 + \sqrt{-23}}{54} \text{ et } \frac{\pm 25 + \sqrt{-23}}{162} \bmod \Gamma_0(9) .$$

Pour $n = 3$, on trouve : $B_3 = B_4 = 25$ et $B_5 = 187$.

D'où, les points de Heegner de $Y_0(27)$ sont :

$$\frac{\pm 25 + \sqrt{-23}}{54} ; \frac{\pm 25 + \sqrt{-23}}{162} \text{ et } \frac{\pm 187 + \sqrt{-23}}{486} \bmod \Gamma_0(27) .$$

$D = -35$, $h(-35) = 2$.

Pour $n = 2$, on trouve : $B_2 = 1$ et $B_3 = -17$.

D'où, les points de Heegner de $Y_0(9)$ sont :

$$\frac{\pm 1 + \sqrt{-35}}{18} \quad \text{et} \quad \frac{\pm 17 + \sqrt{-35}}{54} \bmod \Gamma_0(9) .$$

Pour $n = 3$, on trouve : $B_3 = B_4 = -17$.

D'où, les points de Heegner de $Y_0(27)$ sont :

$$\frac{\pm 17 + \sqrt{-35}}{54} \quad \text{et} \quad \frac{\pm 17 + \sqrt{-35}}{162} \bmod \Gamma_0(27) .$$

3 - Algorithme et applications.

3.1 - Remarque.

Dans les cas précédents, toute l'information nécessaire pour déterminer les points de Heegner de $Y_0(N)$ de discriminant D, avec : $N = 2^n$ ou 3^n, $n \geq 1$ et $h(D)$ un nombre premier, est contenue dans les nombres B_i. Mais, ce qui joue un rôle important dans cette détermmination, est le fait que des représentants des classes d'idéaux de $Q(\sqrt{D})$, peuvent s'écrire sous forme d'une puissance d'un idéal de norme un nombre premier et non la condition que $h(D)$ soit un nombre premier.

3.2 - Algorithme.

Dans ce paragraphe, on va généraliser la méthode de détermination des points de Heegner, décrite dans les cas précédents, pour N un entier > 1 et D un discriminant tel que $h(D) > 1$ et $cl(Q(\sqrt{D})) = \{[\mathcal{P}], [\mathcal{P}^2], \ldots, [\mathcal{P}^{h(D)}]\}$ où $\mathcal{P}$ est un idéal de norme un nombre premier.

Soient $N = p_1^{r_1} \ldots . p_s^{r_s}$, la décomposition de N en nombres premiers et D un carré modulo $4N$. On pose $\mathcal{P} = (p, \frac{\alpha \pm \sqrt{D}}{2})$, où p est un nombre premier, $\alpha^2 \equiv D \bmod (4p)$ et $\alpha \in \mathbf{Z}/2p\mathbf{Z}$.

Soient $(\pm B_{0,i})_{1 \leq i \leq 2^{s-1}}$, les solutions dans $\mathbf{Z}/2N\mathbf{Z}$, de la congruence : $B^2 \equiv D \bmod (4N)$, (on verra plus loin, le choix des $B_{0,i}$).

Alors, les idéaux primitifs de norme N sont :

$$\eta_{0,i} = \left(N, \frac{B_{0,i} + \sqrt{D}}{2}\right) \quad \text{et} \quad \eta'_{0,i} = \left(N, \frac{-B_{0,i} + \sqrt{D}}{2}\right)$$
$$i = 1, 2, \ldots, 2^{s-1} .$$

Pour construire des représentants primitifs, des classes d'idéaux de $Q(\sqrt{D})$ satisfaisant les conditions de Heegner par rapport à un idéal primitif de norme N, on est amené à envisager les deux cas suivants :

1^er^ cas : p ne divise pas DN, ou p divise N.

Dans ce cas, p se décompose : $(p) = \mathcal{P}\overline{\mathcal{P}}$ avec $\overline{\mathcal{P}} = \left(p, \frac{-\alpha+\sqrt{D}}{2}\right)$.

Pour $i \in \{1, 2, \ldots, 2^{s-1}\}$ fixé, on pose :

$$\eta_{j,i} = \eta_{0,i}\mathcal{P}^j \quad \text{et} \quad \eta'_{j,i} = \eta'_{0,i}\overline{\mathcal{P}}^j \ ; \ 0 \leq j \leq h(D) - 1 .$$

Alors on a :

$$\begin{aligned} cl(\mathbf{Q}(\sqrt{D})) &= \{[\eta_{j,i}], \quad 0 \leq j \leq h(D) - 1\} \\ &= \{[\eta'_{j,i}], \quad 0 \leq j \leq h(D) - 1\} . \end{aligned}$$

Maintenant, on va voir les conditions qu'il faut poser sur $B_{0,i}$, pour que, pour tout $1 \leq j \leq h(D) - 1$, les idéaux $\eta_{j,i}$ et $\eta'_{j,i}$ soient primitifs.

Puisque $\eta_{0,i}, \eta'_{0,i}, \mathcal{P}$ et $\overline{\mathcal{P}}$ sont primitifs, donc $\eta_{j,i}$ (resp. $\eta'_{j,i}$) est non primitif ssi $\overline{\mathcal{P}}$ divise $\eta_{0,i}$ (resp. $\mathcal{P}$ divise $\eta'_{0,i}$).

Conséquence :

— Si p ne divise pas DN, alors $\eta_{j,i}$ et $\eta'_{j,i}$ sont primitifs pour tout $1 \leq j \leq h(D) - 1$ ($B_{0,i}$ est donc choisi, d'une façon arbitraire).

— Si p divise N, on choisit $B_{0,i}$ tel que $B_{0,i} \equiv \alpha \bmod (2p)$. Ce qui entraîne que $\mathcal{P}$ divise $\eta_{0,i}$ et $\overline{\mathcal{P}}$ divise $\eta'_{0,i}$. Ainsi, pour tout $1 \leq j \leq h(D) - 1$, $\eta_{j,i}$ et $\eta'_{j,i}$ sont primitifs.

D'où : en choisissant, pour tout $1 \leq i \leq 2^{s-1}$, les $B_{0,i}$ telles que $B_{0,i} \equiv \alpha \bmod (2p)$ (resp. d'une manière arbitraire), dans le cas où p divise N (resp. p ne divise pas ND); pour tout $1 \leq j \leq h(D) - 1$ et $1 \leq i \leq 2^{s-1}$, on peut écrire :

$$\eta_{j,i} = \left(Np^j, \frac{B_{j,i} + \sqrt{D}}{2}\right) \quad \text{et} \quad \eta'_{j,i} = \left(Np^j, \frac{-B_{j,i} + \sqrt{D}}{2}\right) ,$$

où
$$B_{j,i}^2 \equiv D \bmod (4Np^j), \quad B_{j,i} \in \mathbf{Z}/2Np^j\mathbf{Z}$$
$$B_{j,i} \equiv B_{0,i} \bmod (2N)$$
$$\text{et } B_{j,i} \equiv \alpha \bmod (2p)\,.$$

Par conséquent, les points de Heegner de $Y_0(N)$ de discriminant D sont :

$$\frac{\pm B_{j,i} + \sqrt{D}}{2Np^j} \bmod \Gamma_0(N), \quad 1 \leq i \leq 2^{s-1}, \quad 0 \leq j \leq h(D) - 1\,.$$

Maintenant, on se propose de trouver une relation entre $B_{j,i}$ et B_{j+1+i}, pour tout $0 \leq j \leq h(D) - 2$ et $i \in \{1, 2, \ldots, 2^{s-1}\}$ fixé : Vu les conditions que doivent satisfaire les $B_{j,i}$, on a : $B_{j+1+i} \equiv B_{j,i} \bmod (2Np^j)$.

On vérifie facilement qu'on peut prendre :

$B_{j+1,i} = B_{j,i} + 2Np^j k$, où $k = 0, \pm 1, \ldots,$ ou $\pm p$ tel que :
$(B_{j,i} + 2Np^j k)^2 \equiv D \bmod (4Np^{j+1})$ et $B_{j,i} + 2Np^j k \equiv \alpha \bmod (2p)$.
(un tel k existe).

$2^{\text{ème}}$ cas : p divise D.

Dans ce cas, $h(D) = 2$, $p \neq 2$ et $(p) = \mathcal{P}^2$ où $\mathcal{P} = \left(p, \frac{p+\sqrt{D}}{2}\right)$.

Pour $i \in \{1, 2, \ldots, 2^{s-1}\}$ fixé, on pose :

$$\eta_{1,i} = \eta_{0,i}\mathcal{P} \quad \text{et} \quad \eta'_{1,i} = \eta'_{0,i}\mathcal{P}\,.$$

Alors, on a :
$$cl(Q(\sqrt{D})) = \{[\eta_{0,i}], [\eta_{1,i}]\}$$
$$= \{[\eta'_{0,i}], [\eta'_{1,i}]\}\,.$$

Puisque $\eta_{0,i}$, $\eta'_{0,i}$ et $\mathcal{P}$ sont primitifs et p ne divise pas N, donc $\eta_{1,i}$ et $\eta'_{1,i}$ sont primitifs. Par conséquent, on peut écrire :

$$\eta_{1,i} = \left(pN, \frac{B_{1,i} + \sqrt{D}}{2}\right) \quad \text{et} \quad \eta'_{1,i} = \left(pN, \frac{-B_{1,i} + \sqrt{D}}{2}\right)$$

où
$$B_{1,i}^2 \equiv D \bmod (4Np), \quad B_{1,i} \in \mathbf{Z}/2Np\mathbf{Z}$$
$$B_{1,i} \equiv B_{0,i} \bmod (2N)$$
$$\text{et } B_{1,i} \equiv 0 \bmod (p)\,.$$

D'où, les points de Heegner de $Y_0(N)$ de discriminant D sont :

$$\frac{\pm B_{j,i}+\sqrt{D}}{2Np^j} \bmod \Gamma_0(N) \quad 1 \leq i \leq 2^{s-1}, \quad j = 0, 1 .$$

Vu les conditions que satisfait $B_{1,i}$, pour déterminer cette dernière, il suffit de trouver un entier $k \in \{0, \pm 1, \pm 2, \ldots, \pm p\}$ tel que $B_{0,i} + 2Nk \equiv 0 \bmod (p)$. Dans ce cas, on peut prendre $B_{1,i} = B_{0,i} + 2Nk$. D'où, on a la proposition suivante :

Proposition 5. (Proposition principale).

• *Soient N un entier > 1, D un discriminant tel que : $h(D) > 1$ et $cl(Q(\sqrt{D})) = \{[\mathcal{P}], \ldots, [\mathcal{P}^{h(D)}]\}$, où $\mathcal{P} = \left(p, \frac{\alpha+\sqrt{D}}{2}\right)$ avec p un nombre premier, $\alpha^2 \equiv D \bmod (4p)$ et $\alpha \in \mathbf{Z}/2p\mathbf{Z}$. On suppose que D est un carré modulo $4N$, soient $(\pm B_{0,i})_{1 \leq i \leq 2^{s-1}}$ les solutions dans $\mathbf{Z}/2N\mathbf{Z}$, de la congruence : $B^2 \equiv D \bmod (4N)$; on prendra $B_{0,i} \equiv \alpha \bmod (2p)$, si p divise N (s étant le nombre des diviseurs premiers de N).*

Alors, les points de Heegner de $Y_0(N)$ de discriminant D sont :

$$\frac{\pm B_{j,i}+\sqrt{D}}{2Np^j} \bmod \Gamma_0(N), \quad 1 \leq i \leq 2^{s-1}, \quad 0 \leq j \leq h(D)-1 ,$$

où $(B_{j,i})_{\substack{1 \leq i \leq 2^{s-1} \\ 1 \leq j \leq h(D)-1}}$ vérifie :

$$\begin{cases} B_{j,i}^2 \equiv D \bmod (4Np^j) \\ B_{j,i} \in \mathbf{Z}/2Np^j\mathbf{Z} \\ B_{j,i} \equiv B_{0,i} \bmod (2N) \\ B_{j,i} \equiv \alpha \bmod (2p) . \end{cases}$$

• *Etant donné $1 \leq i \leq 2^{s-1}$ et $0 \leq j \leq h(D)-2$, pour déterminer $B_{j+1,i}$ connaissant $B_{j,i}$, il suffit de trouver un entier $k = 0, \pm 1, \ldots,$ ou $\pm p$, tel que : $(B_{j,i} + 2Np^jk)^2 \equiv D \bmod (4Np^{j+1})$ et $B_{j,i} + 2Np^jk \equiv \alpha \bmod (2p)$. Ainsi, on prendra : $B_{j+1,i} = B_{j,i} + 2Np^jk$.*

Remarques :

— Les entiers $B_{0,i}$ de la proposition 5 peuvent aussi être déterminés d'une façon algorithmique. Dans les exemples suivants (cf. 3.3 - Applications.), on considère $1 \leq B_{0,i} < 2N$.

— Les propositions précédentes sont des cas particuliers de la proposition 5 ($p = 2, \alpha = 1$ (resp. $p = 3, \alpha = 1$) pour les exemples où $N = 2^n$, $n \geq 1$ (resp. $N = 3^n$, $n \geq 1$)).

— On peut étendre la méthode décrite dans la proposition 5 à tous les discriminants D :

$$cl(\mathbf{Q}(\sqrt{D})) = \{[\mathcal{P}_1], \ldots, [\mathcal{P}_1^{r_1}]; [\mathcal{P}_2], \ldots, [\mathcal{P}_2^{r_2}]; [\mathcal{P}_s], \ldots, [\mathcal{P}_s^{r_s}]\}$$

où les $\mathcal{P}_i$ sont des idéaux de norme un nombre premier et les r_i des entiers tels que $\sum_{i=1}^{s} r_i = h(D)$.

3.3 - Applications.

Convention : Pour les discriminants D et les entiers N suivants, les points de Heegner $\frac{\pm B_{j,i} + \sqrt{D}}{2Np^j}$ sont désignés par des couples $(\pm B_{j,i}; 2Np^j)$, $1 \leq i \leq 2^{s-1}$, $0 \leq j \leq h(D) - 1$.

Exemple 1 : $D = -39$, $h(-39) = 4$, $p = 2$, $\alpha = 1$.

Pour $N = 2$, les points de Heegner sont :

$$(\pm 1; 4),\ (\pm 5; 8),\ (\pm 5; 16) \text{ et } (\pm 5; 32)\ .$$

Pour $N = 4$, les points de Heegner sont :

$$(\pm 5; 8),\ (\pm 5; 16),\ (\pm 5; 32) \text{ et } (\pm 37; 64)\ .$$

Pour $N = 5$, les points de Heegner sont :

$$(\pm 1; 10),\ (\pm 1; 20),\ (\pm 21; 40) \text{ et } (\pm 21; 80)\ .$$

Pour $N = 8$, les points de Heegner sont :

$$(\pm 5; 16),\ (\pm 5; 32),\ (\pm 37; 64) \text{ et } (\pm 101; 128)\ .$$

Pour $N = 10$, les points de Heegner sont :

$$(\pm 1; 20),\ (\pm 21; 40),\ (\pm 21; 80),\ (\pm 101; 160),$$
$$(\pm 9; 20),\ (\pm 29; 40),\ (\pm 69; 80),\ \text{et } (\pm 69; 160)\ .$$

Exemple 2 : $\underline{D = -47}$, $h(-47) = 5$, $p = 2$, $\alpha = 1$.

Pour $\underline{N = 2}$, les points de Heegner sont :

$$(\pm 1; 4),\ (\pm 1; 8),\ (\pm 9; 16),\ (\pm 9; 32),\ \text{et}\ (\pm 9; 64)\,.$$

Pour $\underline{N = 3}$, les points de Heegner sont :

$$(\pm 1; 6),\ (\pm 1; 12),\ (\pm 1; 24),\ (\pm 25; 48),\ \text{et}\ (\pm 73; 96)\,.$$

Pour $\underline{N = 4}$, les points de Heegner sont :

$$(\pm 1; 8),\ (\pm 9; 16),\ (\pm 9; 32),\ (\pm 9; 64),\ \text{et}\ (\pm 73; 128)\,.$$

Pour $\underline{N = 6}$, les points de Heegner sont :

$$(\pm 1; 12),\ (\pm 1; 24),\ (\pm 25; 48),\ (\pm 73; 96),\ (\pm 73; 192),$$
$$(\pm 5; 12),\ (\pm 17; 24),\ (\pm 41; 48),\ (\pm 41; 96),\ \text{et}\ (\pm 137; 192)\,.$$

Pour $\underline{N = 7}$, les points de Heegner sont :

$$(\pm 3; 14),\ (\pm 17; 28),\ (\pm 17; 56),\ (\pm 73; 112),\ \text{et}\ (\pm 73; 224)\,.$$

Pour $\underline{N = 8}$, les points de Heegner sont :

$$(\pm 9; 16),\ (\pm 9; 32),\ (\pm 9; 64),\ (\pm 73; 128),\ \text{et}\ (\pm 201; 256)\,.$$

Pour $\underline{N = 9}$, les points de Heegner sont :

$$(\pm 5; 18),\ (\pm 5; 36),\ (\pm 41; 72),\ (\pm 41; 144),\ \text{et}\ (\pm 41; 288)\,.$$

Exemple 3 : $\underline{D = -87}$, $h(-87) = 6$, $p = 2$, $\alpha = 1$.

Pour $\underline{N = 2}$, les points de Heegner sont :

$$(\pm 1; 4),\ (\pm 5; 8),\ (\pm 13; 16),\ (\pm 13; 32),\ (\pm 13; 64),\ \text{et}\ (\pm 13; 128)\,.$$

Pour $\underline{N = 4}$, les points de Heegner sont :

$$(\pm 5; 8),\ (\pm 13; 16),\ (\pm 13; 32),\ (\pm 13; 64),\ (\pm 13; 128),\ \text{et}\ (\pm 141; 256)\,.$$

Pour $N = 7$, les points de Heegner sont :

$(\pm 5; 14)$, $(\pm 5; 28)$, $(\pm 5; 56)$, $(\pm 61; 112)$, $(\pm 173; 224)$, et $(\pm 397; 448)$.

Pour $N = 8$, les points de Heegner sont :

$(\pm 13; 16)$, $(\pm 13; 32)$, $(\pm 13; 64)$, $(\pm 13; 128)$, $(\pm 141; 256)$, et $(\pm 397; 512)$.

Exemple 4 : $D = -91$, $h(-91) = 2$, $p = 7$, $\alpha = 7$.

Pour $N = 5$, les points de Heegner sont :

$(\pm 3; 10)$ et $(\pm 7; 70)$.

Exemple 5 : $D = -95$, $h(-95) = 8$, $p = 2$, $\alpha = 1$.

Pour $N = 2$, les points de Heegner sont :

$(\pm 1; 4)$, $(\pm 1; 8)$, $(\pm 1; 16)$, $(\pm 17; 32)$,
$(\pm 17; 64)$, $(\pm 81; 128)$, $(\pm 81; 256)$, et $(\pm 337; 512)$.

Pour $N = 3$, les points de Heegner sont :

$(\pm 1; 6)$, $(\pm 1; 12)$, $(\pm 1; 24)$, $(\pm 1; 48)$,
$(\pm 49; 96)$, $(\pm 145; 192)$, $(\pm 337; 384)$, et $(\pm 337; 768)$.

Pour $N = 4$, les points de Heegner sont :

$(\pm 1; 8)$, $(\pm 1; 16)$, $(\pm 17; 32)$, $(\pm 17; 64)$,
$(\pm 81; 128)$, $(\pm 81; 256)$, $(\pm 337; 512)$, et $(\pm 849; 1024)$.

Pour $N = 6$, les points de Heegner sont :

$(\pm 1; 12)$, $(\pm 1; 24)$, $(\pm 1; 48)$, $(\pm 49; 96)$, $(\pm 145; 192)$,
$(\pm 337; 384)$, $(\pm 337; 768)$, $(\pm 337; 1536)$, $(\pm 5; 12)$, $(\pm 17; 24)$,
$(\pm 17; 48)$, $(\pm 17; 96)$, $(\pm 17; 192)$, $(\pm 209; 384)$, $(\pm 593; 768)$, et $(\pm 1361; 1536)$.

Pour $N = 8$, les points de Heegner sont :

$$(\pm 1; 16),\ (\pm 17; 32),\ (\pm 17; 64),\ (\pm 81; 128),$$
$$(\pm 81; 256),\ (\pm 337; 512),\ (\pm 849; 1024) \text{ et } (\pm 849; 2048)\ .$$

Pour $N = 9$, les points de Heegner sont :

$$(\pm 7; 18),\ (\pm 25; 36),\ (\pm 25; 72),\ (\pm 97; 144),$$
$$(\pm 241; 288),\ (\pm 529; 576),\ (\pm 1105; 1152),\ \text{et } (\pm 1105; 2304)\ .$$

Remarques :

— Dans les exemples précédents, pour un discriminant D donné, on a fait varier l'entier N de 2 à 10.

— Pour d'autres applications, voir "Calcul effectif des points de Heegner de $Y_0(N)$", travail à paraître.

4 - Exemple de discriminant ne satisfaisant pas l'algorithme.

$D = -195$ et $N = 7$.

On a $h(-195) = 4$ et $cl(Q(\sqrt{-195})) = \{[\mathcal{O}], [\mathcal{P}_1], [\mathcal{P}_2], [\mathcal{P}_3]\}$, où :

$$\mathcal{O} = (1, \frac{1+\sqrt{-195}}{2})\ ;\ \mathcal{P}_1 = (3, \frac{3+\sqrt{-195}}{2})\ ;$$

$$\mathcal{P}_2 = (5, \frac{5+\sqrt{-195}}{2}) \quad \text{et} \quad \mathcal{P}_3 = (7, \frac{1+\sqrt{-195}}{2})\ .$$

On vérifie facilement, que $[\mathcal{P}_1^2] = [\mathcal{P}_2^2] = [\mathcal{P}_3^2] = [\mathcal{O}]$; ce qui prouve qu'on ne peut pas trouver des représentants des classes d'idéaux sous forme d'une puissance d'un idéal.

Les idéaux primitifs de norme 7 sont :

$$\mathcal{P}_3 = (7, \frac{1+\sqrt{-195}}{2}) \quad \text{et} \quad \mathcal{P}'_3 = (7, \frac{-1+\sqrt{-195}}{2})\ .$$

On peut écrire :

$$cl(Q(\sqrt{-195})) = \{[\mathcal{P}_3]; [\mathcal{P}_1\mathcal{P}_3]; [\mathcal{P}_2\mathcal{P}_3]; [\mathcal{P}_3^2]\}$$
$$= \{[\mathcal{P}'_3]; [\mathcal{P}_1\mathcal{P}'_3]; [\mathcal{P}_2\mathcal{P}'_3]; [\mathcal{P}'^2_3]\}\ .$$

où
$$\mathcal{P}_1\mathcal{P}_3,\ \mathcal{P}_1\mathcal{P}_3' = (21, \frac{\pm 15 + \sqrt{-195}}{2})$$
$$\mathcal{P}_2\mathcal{P}_3,\ \mathcal{P}_2\mathcal{P}_3' = (35, \frac{\pm 15 + \sqrt{-195}}{2})\ ;$$
$$\mathcal{P}_3^2,\ \mathcal{P}_3'^2 = (49, \frac{\pm 1 + \sqrt{-195}}{2})\ .$$

Par conséquent, les points de Heegner de $Y_0(7)$ de discriminant (-195) sont :

$$\frac{\pm 1 + \sqrt{-195}}{14}\ ;\ \frac{\pm 15 + \sqrt{-195}}{42}\ ;\ \frac{\pm 15 + \sqrt{-195}}{70}\ ;\ \frac{\pm 1 + \sqrt{-195}}{98} \mod \Gamma_0(7)\ .$$

5 - Table des discriminants satisfaisant l'algorithme.

Pour $|D| \leq 503$, $D \equiv 1 \bmod (4)$ et $h(D) > 1$, le tableau suivant, donne un idéal $\mathcal{P} = (p, \frac{\alpha + \sqrt{D}}{2})$ tel que : $cl(Q(\sqrt{D})) = \{[\mathcal{P}^i],\quad 1 \leq i \leq h(D)\}$. Un tel idéal n'existe pas pour $D = -195$; -399 ; -455 et -483.

$-D$	$h(D)$	p	α	$-D$	$h(D)$	p	α	$-D$	$h(D)$	p	α
15	2	2	1	195	4	×	×	355	4	7	3
23	3	2	1	199	9	2	1	359	19	2	1
31	3	2	1	203	4	3	1	367	9	2	1
35	2	3	1	211	3	5	3	371	8	3	1
39	4	2	1	215	14	2	1	379	3	5	1
47	5	2	1	219	4	5	1	383	17	2	1
51	2	3	3	223	7	2	1	391	14	7	1
55	4	2	1	227	5	3	1	395	8	3	1
59	3	3	1	231	12	2	1	399	16	×	×
71	7	2	1	235	2	5	5	403	2	13	13
79	5	2	1	239	15	2	1	407	16	2	1
83	3	3	1	247	6	2	1	411	6	5	3
87	6	2	1	251	7	3	1	415	10	2	1
91	2	7	7	255	12	2	1	419	9	3	1
95	8	2	1	259	4	5	1	427	2	7	7
103	5	2	1	263	13	2	1	431	21	3	1
107	3	3	1	267	2	3	3	435	4	2	1
111	8	2	1	271	11	2	1	439	15	2	1
115	2	5	5	283	3	7	5	443	5	3	1
119	10	3	1	287	14	3	1	447	14	2	1
123	2	3	3	291	4	5	3	451	6	7	5
127	5	2	1	295	8	2	1	455	20	×	×
131	5	3	1	299	8	5	1	463	7	2	1
139	3	5	1	303	10	2	1	467	7	3	1
143	10	2	1	307	3	7	1	471	16	2	1
151	7	2	1	311	19	2	1	479	25	2	1
155	4	3	1	319	10	2	1	483	4	×	×
159	10	2	1	323	4	3	1	487	7	2	1
167	11	2	1	327	12	2	1	491	9	3	1
179	5	3	1	331	3	5	3	499	3	5	1
183	8	2	1	335	18	2	1	503	21	3	1
187	2	11	11	339	6	5	1	×	×	×	×
191	13	2	1	347	5	3	1	×	×	×	×

APPENDICE

LA COURBE $Y_0(N)$

1 - Classification des éléments de $SL_2(\mathbf{R})$.

Regardons d'abord, $GL_2(\mathbf{C})$ agissant sur $\mathbf{C} \cup \{\infty\}$.

D'après la théorie de Jordon, toute matrice de $GL_2(\mathbf{C})$ est semblable (ou conjuguée) à une matrice de l'un des trois types suivants :

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}, \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}, \quad \text{avec} \quad \lambda \neq \mu \; ; \; \lambda \neq 0 \text{ et } \mu \neq 0 \; .$$

Par conséquent, la transformation de $\mathbf{C} \cup \{\infty\}$ associée à la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{C})$ est conjuguée, soit à l'identité, soit à la transformation : $z \to z + \frac{1}{\lambda}$, soit à la transformation : $z \to cz$ avec $c \neq 1$.

Définition 1. *Si la transformation est conjuguée à : $z \to z + \frac{1}{\lambda}$, elle est dite parabolique.*

Si la transformation est conjuguée à : $z \to cz$ avec :

$$\begin{cases} |c| = 1, \textit{ elle est dite elliptique.} \\ c > 0, \textit{ elle est dite hyperbolique.} \\ \textit{Sinon, elle est dite loxodromique.} \end{cases}$$

Remarque : Le nombre des points de $\mathbf{C} \cup \{\infty\}$ fixés par un élément de $GL_2(\mathbf{C})$ est un ou deux, selon les cas ci-dessus.

Revenons à $SL_2(\mathbf{R})$, la classification est décrite par la proposition suivante :

Proposition 1. *Soit $\gamma \in SL_2(\mathbf{R})$, $\gamma \neq \pm id$, alors :*

γ est parabolique ssi $|tr\,\gamma| = 2$.

γ est elliptique ssi $|tr\,\gamma| < 2$.

γ est hyperbolique ssi $|tr\,\gamma| > 2$.

Il n'y a pas d'élément loxodromique.

Maintenant, on va préciser cette classification par rapport aux points fixes des transformations :

Proposition 2. *Soit $\gamma \in SL_2(\mathbf{R})$, $\gamma \neq \pm id$, alors :*
γ est parabolique ssi γ a un seul point fixe sur $\mathbf{R} \cup \{\infty\}$.
γ est elliptique ssi γ un a un point fixe z sur H et l'autre point fixe est $\overline{z}$.
γ est hyperbolique ssi γ a deux points fixes sur $\mathbf{R} \cup \{\infty\}$.

Définition 2. *Soit Γ un sous-groupe discret de $SL_2(\mathbf{R})$. Un point z de H est dit elliptique relativement à Γ, s'il est fixé par un élément γ de Γ (γ est alors elliptique).*

Un point z de $\mathbf{R} \cup \{\infty\}$ est une pointe relativement à Γ, s'il est fixé par un élément parabolique de Γ (z est l'unique point fixe d'un élément γ de Γ).

Proposition 3. *L'ensemble des pointes (resp. des points elliptiques) est Γ-invariant.*

2 - Les pointes relativement à $\Gamma_0(N)$.

Proposition 1. *L'ensemble des pointes relativement à $\Gamma_0(N)$ est $Q \cup \{\infty\}$.*

■ — On va d'abord démontrer cette proposition, dans le cas où $N = 1$.

Soit $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, T est un élément parabolique de $\Gamma_0(1)$, qui stabilise l'∞; donc l'∞ est une pointe relativement à $\Gamma_0(1)$. L'orbite de l'∞ est :

$$\Gamma_0(1)(\infty) = \left\{ \frac{a}{c} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(1) \right\} = Q .$$

Soit s une pointe relativement à $\Gamma_0(1)$, $s \neq \infty$; donc s est racine de $\begin{pmatrix} a & b \\ c & d \end{pmatrix} s = s$, avec $a + d = \pm 2$. Ce qui entraîne que s vérifie l'équation : $cz^2 + (d-a)z - b = 0$, le discriminant vaut $(d-a)^2 + 4bc = 0$; donc $s \in Q$.

D'où, l'ensemble des pointes relativement à $\Gamma_0(1)$ est $Q \cup \{\infty\}$; de plus, elles sont toutes $\Gamma_0(1)$-équivalentes à l'∞.

— Pour $N > 1$, on a $\Gamma_0(N) \subset \Gamma_0(1)$, et on démontre que :

$$[\Gamma_0(1) : \Gamma_0(N)] = N \prod_{p/N} (1 + \frac{1}{p}) = \mu .$$

Si s est une pointe relativement à $\Gamma_0(N)$, alors il existe $\gamma \in \Gamma_0(N)$ parabolique, telle que $\gamma(s) = s$; mais $\gamma \in \Gamma_0(1)$, donc s est une pointe relativement à $\Gamma_0(1)$. D'où {Les pointes relativement à $\Gamma_0(N)$} $\subset \mathbf{Q} \cup \{\infty\}$.

Si $s \in Q \cup \{\infty\}$, alors il existe $\gamma \in \Gamma_0(1)$ parabolique telle que $\gamma(s) = s$. Or, si $\gamma \in \Gamma_0(1)$, alors $\gamma^\mu \in \Gamma_0(N)$ et on a $\gamma^\mu(s) = s$. D'où, il suffit de démontrer que γ^μ est parabolique :

Si $s \in Q \cup \{\infty\}$, donc il existe $g \in \Gamma_0(1)$ telle que $g(\infty) = s$. Ce qui entraîne que $g^{-1}\gamma g$ stabilise l'∞. Or, $\mathrm{stab}_{\Gamma_0(1)}(\infty) = \left\{ \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} | h \in \mathbf{Z} \right\}$, donc il existe $h \in \mathbf{Z}$ tel que γ est semblable à $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$. Ce qui entraîne que γ^μ est semblable à $\begin{pmatrix} 1 & h\mu \\ 0 & 1 \end{pmatrix}$. Par conséquent, γ^μ est parabolique; d'où s est une pointe relativement à $\Gamma_0(N)$. ∎

Proposition 2. *$Q \cup \{\infty\}/\Gamma_0(N)$ est isomorphe (au point de vue ensembliste) à $\bigcup_{\substack{d/N \\ d>0}} (\mathbf{Z}/f_d\mathbf{Z})^*$ où $f_d = (d, \frac{N}{d})$.*

∎ On a :

$$\begin{aligned} Q \cup \{\infty\} &= \cup_{d/N} \{ \frac{m}{n} / m, n \in \mathbf{Z} \ ; \ (m,n) = 1 \text{ et } d = (N,n) \} \\ &= \cup_{d/N} X_d \qquad \text{(réunion disjointe).} \end{aligned}$$

— $\mathrm{Orb}(\infty) = \{ \frac{a}{c} \mid (a,c) = 1 \text{ et } c \equiv 0 \bmod (N) \} = X_N$, donc tous les rationnels, dont le dénominateur est divisible par N, sont $\Gamma_0(N)$-équivalents à l'∞.

— $\mathrm{Orb}(0) = \{ \frac{a}{c} \mid (a,c) = 1 \text{ et } (c,N) = 1 \} = X_1$, donc tous les rationnels dont le dénominateur est premier avec N, sont $\Gamma_0(N)$-équivalents à 0.

— Soient d un diviseur de N différent de 1 et de N, et $\frac{m}{n} \in X_d$; alors on vérifie facilement que $\Gamma_0(N)(X_d) \subset X_d$ et $\left(\frac{mn}{d}, f_d\right) = 1$.

On va démontrer que deux éléments $\frac{m}{n}$ et $\frac{m'}{n'}$ de X_d sont $\Gamma_0(N)$-équivalents ssi $\frac{mn}{d} \equiv \frac{m'n'}{d} \bmod (f_d)$:

• Si $\frac{m'}{n'} \in \mathrm{Orb}(\frac{m}{n})$, alors il existe x, y, z et t, des entiers tels que : $xt - yz = 1$, $z \equiv 0 \bmod (N)$, $m' = xm + yn$ et $n' = zm + tn$.

D'où, $\frac{m'n'}{d} = (xm + yn)(zm + tn)/d \equiv tx\frac{mn}{d} \equiv \frac{mn}{d} \bmod (f_d)$.

• La réciproque est une conséquence du lemme suivant :

Lemme. *Soient $\frac{x}{kd}$ et $\frac{\alpha}{d}$ deux éléments de X_d.*

Si $xk \equiv \alpha \bmod (f_d)$, alors $\frac{x}{kd}$ et $\frac{\alpha}{d}$ sont $\Gamma_0(N)$-équivalents.

■ On a : $(x, kd) = 1$ et $(\alpha, d) = 1$, donc il existe des entiers X, Y, U et V tels que $Xx + Ykd = 1$ et $\alpha U + Vd = 1$. Par conséquent, $\frac{x}{kd} = \begin{pmatrix} x & -Y \\ kd & X \end{pmatrix}(\infty) = f(\infty)$, $\frac{\alpha}{d} = \begin{pmatrix} \alpha & -V \\ d & U \end{pmatrix}(\infty) = g(\infty)$.

Soit $\gamma \in \Gamma_0(1)$ telle que $\frac{x}{kd} = \gamma(\frac{\alpha}{d})$. On a $f(\infty) = \gamma g(\infty) \Leftrightarrow g^{-1}\gamma^{-1}f(\infty) = \infty \Leftrightarrow g^{-1}\gamma^{-1}f = \delta_h = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \Leftrightarrow \gamma^{-1} = g\delta_h f^{-1} = \begin{pmatrix} * & * \\ d(X - dhk - kU) & * \end{pmatrix}$. D'où $\gamma \in \Gamma_0(N)$ ssi $X - dhk - kU \equiv 0 \bmod (\frac{N}{d})$.

Si on prend $h \equiv 0 \bmod (\frac{N}{d})$, alors le problème revient à trouver

X et U tels que : $X \equiv kU \bmod (\frac{N}{d})$, $Xx \equiv 1 \bmod (kd)$ et $\alpha U \equiv 1 \bmod (d)$.

Soient U, V, X et Y des entiers fixés tels que : $\alpha U + Vd = 1$ et $Xx + Ykd = 1$; il s'agit de trouver deux entiers X' et Y' tels que : $X'x + Y'kd = 1$ et $X' \equiv kU \bmod (\frac{N}{d})$:

On pose $X = kU + m$; $m \neq 0$, puisque $(X, k) = 1$. Alors, on a : $Xx + Ykd = 1 \Leftrightarrow (kU + m)x + Ykd = 1 \Leftrightarrow k(xU + Yd) + xm = 1$. En plus, il existe un entier r tel que $m = rf_d$; en effet, $xX = xkU + xm$, $xX \equiv 1 \bmod (f_d)$, $xkU \equiv \alpha U \bmod (f_d)$ et $(x, f_d) = 1$.

On pose $d' = \frac{N}{d}$, alors on a : $(k, \frac{d'}{f_d}) = 1$ et $(\frac{d'}{f_d}, \frac{d}{f_d}) = 1$. Donc il existe deux entiers p et q tels que $pk\frac{d}{f_d} + q\frac{d'}{f_d} = 1$; d'où, on a : $k(xU + Yd) + rf_d x = 1 \Leftrightarrow k(xU + Yd) + rf_d x(pk\frac{d}{f_d} + q\frac{d'}{f_d}) = 1 \Leftrightarrow x(kU + rqd') + kd(Y + xrp) = 1$.

On pose : $X' = kU + rqd'$ et $Y' = Y + xrp$, d'où le résultat.

— Soit l'application :

$$\begin{aligned} \psi : X_d &\to (\mathbf{Z}/f_d\mathbf{Z})^* \\ \frac{m}{n} &\to \frac{mn}{d} \bmod (f_d) . \end{aligned}$$

ψ est surjective : soit $\alpha \in (\mathbf{Z}/f_d\mathbf{Z})^*$; à α on assorie $\frac{\alpha \bmod (f_d)}{d}$ tel que $(\alpha \bmod (f_d), d) = 1$.

D'où $\psi(X_d/\Gamma_0(N)) \simeq (\mathbf{Z}/f_d\mathbf{Z})^*$; par conséquent,

$$Q \cup \{\infty\}/\Gamma_0(N) = \cup d/N(X_d/\Gamma_0(N)) \simeq \cup d/N(\mathbf{Z}/f_d\mathbf{Z})^* . \qquad ■$$

Remarque : $Q \cup \{\infty\}/\Gamma_0(1) = \{\infty\}$.

Si N est premier, $Q \cup \{\infty\}/\Gamma_0(N) = \{0, \infty\}$.

Proposition 3.

$$|Q \cup \{\infty\}/\Gamma_0(N)| = \sum_{d/N} \varphi(f_d) = \prod_{p^\mu \| N} \left(p^{[\nu/2]} + p^{[(\nu-1)/2]}\right) .$$

■ — Soit $g(N) = \sum_{d/N} \varphi(f_d)$; g est multiplicative, en effet : soient $N_1, N_2 \in \mathbf{N}^*$ tels que $(N_1, N_2) = 1$, on a :

$$g(N_1 N_2) = \sum_{d/N_1 N_2} \varphi(f_d) = \sum_{d_1/N_1, d_2/N_2} \varphi(f_{d_1 d_2}) .$$

On vérifie facilement que $f_{d_1 d_2} = (d_1 d_2, \frac{N_1 N_2}{d_1 d_2}) = f_{d_1} \cdot f_{d_2}$; d'où,

$$g(N_1 N_2) = \sum_{d_1/N_1} \varphi(f_{d_1}) \cdot \sum_{d_2/N_2} \varphi(f_{d_2}) = g(N_1) \cdot g(N_2) .$$

— Soit p^ν une puisance d'un nombre premier, démontrons que $g(p^\nu) = p^{[\nu/2]} + p^{[(\nu-1)/2]}$:

• Si ν est pair,

$$\begin{aligned} g(p^\nu) &= 1 + \varphi(f_p) + \ldots + \varphi(f_{p^{\nu/2}}) + \ldots + \varphi(f_{p^\nu}) \\ &= 1 + \varphi(p) + \ldots + \varphi(p^{(\nu/2)-1}) + \varphi(p^{\nu/2}) + \varphi(p^{(\nu/2)-1} + \ldots + \varphi(p) + 1 \\ &= 2(1 + (p-1) + (p^2 - p) + \ldots + p^{(\nu/2)-1} - p^{(\nu/2)-2}) + p^{\nu/2} - p^{(\nu/2)-1} \\ &= p^{\nu/2} + p^{(\nu/2)-1} = p^{[\nu/2]} + p^{[(\nu-1)/2]} . \end{aligned}$$

• Si ν est impair,

$$\begin{aligned} g(p^\nu) &= 1 + \varphi(f_p) + \ldots + \varphi(f_{p^{[\nu/2]}}) + \ldots + \varphi(f_{p^\nu}) \\ &= 2(1 + (p-1) + (p^2 - p) + \ldots + p^{[\nu/2]} - p^{[\nu/2]-1}) \\ &= 2p^{[\nu/2]} = p^{[\nu/2]} + p^{[(\nu-1)/2]} . \end{aligned}$$

D'où la proposition. ■

3 - $X_0(N)$ comme surface de Riemann compacte.

Proposition 1. *$X_0(N)$ muni de la topologie usuelle est un espace compact.*

■ — D'abord, on va démontrer que $X_0(1)$ est compact : un domaine fondamental de $Y_0(1)$ est donné par :

$$\mathcal{D} = \{z \in H / |z| \geq 1,\ -\frac{1}{2} < \mathrm{Re}\, z \leq \frac{1}{2} \text{ et } |z| > 1 \text{ si } \mathrm{Re}\, z < 0\} .$$

En identifiant, les points situés sur la frontière de $\mathcal{D}$ par : $z \to \frac{1}{z}$ et $z \to -\frac{1}{z}$, $Y_0(1)$ est une surface de Riemann. En complétant cette surface par $(i\infty)$; $X_0(1)$ est une sphère de Riemann.

— Soient π (resp. π') la projection de H^* sur $X_0(1)$ (resp. $X_0(N)$) :

$$\begin{array}{ccc} H^* & \xrightarrow{\pi} & X_0(1) \\ & \searrow^{\pi'} & \uparrow \varphi \\ & & X_0(N) \end{array}$$

π et π' sont continues et ouvertes, donc φ est continue.

On va recouvrir $X_0(1)$, puis $X_0(N)$ à l'aide de voisinages des éléments de H^* :

Pour $z \in H$, soit v_z un voisinage ouvert de z tel que $\overline{v}_z$ soit compact.

Pour l'∞, soit $v_\infty = \{w \in H / \operatorname{Im} w > r\} \cup \{\infty\}$, v_∞ est un voisinage ouvert de l'∞.

Pour $z \in Q$, il existe $g \in \Gamma_0(1)$ tel que $g^{-1}(\infty) = z$, soit alors $v_z = g^{-1}(v_\infty)$; v_z est un voisinage ouvert de z, puisque g est continue.

Il est clair que $X_0(1) \subset \cup_{z \in H^*} \pi(v_z)$; puisque $X_0(1)$ est compact, de ce recouvrement on peut extraire un recouvrement fini, soit $X_0(1) \subset \cup_{i=1}^{p} \pi(v_{z_i})$. On va s'arranger pour remplacer les v_{z_i} par des compacts :

Si $z_i \in H$, on prendra $\overline{v}_{z_i}$ qui est compact.

Si $z_i = \infty$, il est clair que tout élément de v_∞ est $\Gamma_0(1)$-équivalent à un élément de $\tilde{v}_\infty = \{w \in H / -\frac{1}{2} \leq \operatorname{Re} w \leq \frac{1}{2} \text{ et } \operatorname{Im} w \geq r\} \cup \{\infty\}$. Donc $\pi(v_\infty) \subset \pi(\tilde{v}_\infty)$ et $\tilde{v}_\infty$ est compact.

Si $z_i \in Q$, il existe $g \in \Gamma_0(1)$ telle que $g(\infty) = z_i$; on prendra $\tilde{v}_{z_i} = g(\tilde{v}_\infty)$, qui est compact.

Ainsi, on a : $X_0(1) \subset \cup_{i=1}^{p} \pi(K_i)$, où les K_i sont des compacts. Or, $X_0(N) = \varphi^{-1}(X_0(1)) = \cup_{i=1}^{p} \varphi^{-1}(\pi(K_i))$. Comme $[\Gamma_0(1) : \Gamma_0(N)] = \mu < \infty$; donc $\Gamma_0(1) = \cup_{k=1}^{\mu} \Gamma_0(N)\gamma_k$, en posant $\Gamma_0(1)/\Gamma_0(N) = \{\gamma_1, \ldots, \gamma_\mu\}$. D'où , $\varphi^{-1}\pi(K_i) = \cup_{k=1}^{\mu} \pi'\gamma_k(K_i)$; ce qui entraîne que $X_0(N) \subset \cup_{i=1}^{p} \cup_{k=1}^{\mu} \pi'\gamma_k(K_i)$. Or $\pi'\gamma_k(K_i)$ est compact, donc $X_0(N)$ est compact. Ainsi les pointes relativement à $\Gamma_0(N)$ apparaissent comme les points de compactification de $Y_0(N)$. ∎

Proposition 2. *Il existe une famille $(U_\alpha, p_\alpha)_{\alpha\in I}$ avec I un ensemble d'indices, où $\{U_\alpha\}_{\alpha\in I}$ est un recouvrement ouvert de $X_0(N)$ et p_α est un homéomorphisme de U_α dans un ouvert de $\mathbf{C}$, tels que : si $U_\alpha \cap U_\beta \neq \emptyset$, alors l'application :*

$$p_\beta \circ p_\alpha^{-1} : p_\alpha(U_\alpha \cap U_\beta) \to p_\beta(U_\alpha \cap U_\beta) \quad \textit{est holomorphe.}$$

■ Soit π la projection : $H^* \to X_0(N)$; pour tout point $w \in H^*$, on pose : $\Gamma_w = \{\gamma \in \Gamma_0(N)/\gamma(w) = w\}$.

On peut démontrer qu'il existe un voisinage ouvert U de w tel que $\Gamma_w = \{\gamma \in \Gamma_0(N)/\gamma(U) \cap U \neq \emptyset\}$, voir [1].

D'où on a l'injection naturelle : $U/\Gamma_w \to X_0(N)$ et U/Γ_w est un voisinage ouvert de $\pi(w)$ dans $X_0(N)$.

— Si w n'est ni une pointe ni un point elliptique, alors $\Gamma_w = \{\pm \mathrm{id}\}$, et, par conséquent, l'application $\pi : U \to U/\Gamma_w$ est un homéomorphisme. D'où pour tels points, on peut prendre comme recouvrement $(U/\Gamma_w, \pi^{-1})$.

— Si w est un point elliptique, alors on sait que $\overline{\Gamma}_w = \Gamma_w/\{\pm\mathrm{id}\}$ est un groupe cyclique fini, soit n son ordre. Soit λ un isomorphisme analytique de H dans D, le disque unité, tel que $\lambda(w) = 0$; alors $\lambda\overline{\Gamma}_w\lambda^{-1}$ est constitué des transformations :

$$u \to \xi^k u \quad \text{où} \quad \xi = e^{\frac{2i\pi}{n}} \; ; \; k = 0, \ldots, n-1 \; .$$

Par conséquent, si on définit l'application $p : U/\Gamma_w \to \mathbf{C}$ par :

$$p(\pi(z)) = \lambda(z)^n \; ,$$

alors p est un homéomorphisme de U/Γ_w dans un ouvert de $\mathbf{C}$. D'où, pour tels points, on peut prendre comme recouvrement $(U/\Gamma_w, p)$.

— Si w est une pointe, soit $\rho \in \Gamma_0(1)$ telle que $\rho(w) = \infty$, alors $\rho\Gamma_w\rho^{-1}$ stabilise l'∞; donc il existe un nombre positif h tel que :

$$\rho\Gamma_w\rho^{-1} = \left\{ \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m / m \in \mathbf{Z} \right\} \; .$$

Par conséquent, on peut définir un homéomorphisme p de U/Γ_w dans un ouvert de $\mathbf{C}$ par :

$$p(\pi(z)) = \exp\left(\frac{2i\pi\rho(z)}{h}\right) \; .$$

D'où, pour tels points, on peut prendre comme recouvrement $(U/\Gamma_w, p)$.

Pour achever la démonstration, on vérifie facilement la dernière condition de la proposition.

$X_0(N)$ muni de cette structure complexe est donc une surface de Riemann compacte, puisque c'est un espace topologique séparé, connexe et compact. ■

Références

[1] G. SHIMURA, Introduction to the arithmetic theory of automorphic functions.

[2] P. COHEN, On the coefficients of the transformation polynomials for the elliptic modular function; *Math. Proc. Camb. Phil. Soc. (1984), 94, 389-402.*

[3] Benedict H. GROSS and Don B. ZAGIER, Heegner points and derivatives of L-series; *Invent. Math. (1986), 84, 225-320.*

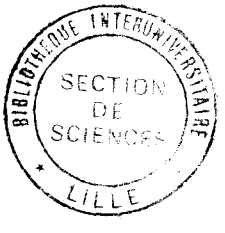
[4] A. ROBERT, Elliptic curves, *Lecture Notes in Mathematics.*

[5] LANDAU, Vorlesungen über Zahlentheorie, *Bd 1, Satz 214 and Satz 209.*

[6] B.J. BIRCH, Heegner points of elliptic curves,*Symp. Math. (1975), 15, 441-445.*

[7] A. OGG, Survey of modular functions of one variable.

[8] B. GROSS, Heegner points on $X_0(N)$. *In : Modular forms (ed. R.A. Rankin), 87 - 106, Chichester : Ellis Horwood 1984.*



RÉSUMÉ

Dans ce travail, on s'intéresse à la détermination des points de Heegner de $Y_0(N)$, de discriminant D, avec D fondamental, impair et $(D, N) = 1$. $Y_0(N)$ étant la courbe $H/\Gamma_0(N)$.

On présente différentes interprétations des points de Heegner; en particulier, la correspondance entre ces points et les triplets $(\mathcal{O}, \eta, [a])$, où $\mathcal{O}$ est l'anneau des entiers du corps quadratique imaginaire $K = Q(\sqrt{D})$, η est un idéal entier primitif de norme N et $[a]$ la classe d'un idéal a.

L'étude de quelques exemples de détermination va nous conduire à établir un algorithme concernant les discriminants, pour lesquels il existe des représentants des classes d'idéaux, qui sont des puissances successives d'un idéal de norme un nombre premier.

MOTS CLÉS : **Courbes elliptiques - Courbes modulaires - Points de Heegner - Discriminants - Classes d'idéaux.**