Mémoire de Master 2

Genre des courbes modulaires

Vincent AIDE

25 octobre 2013

Mémoire encadré par Samuel BOISSIÈRE

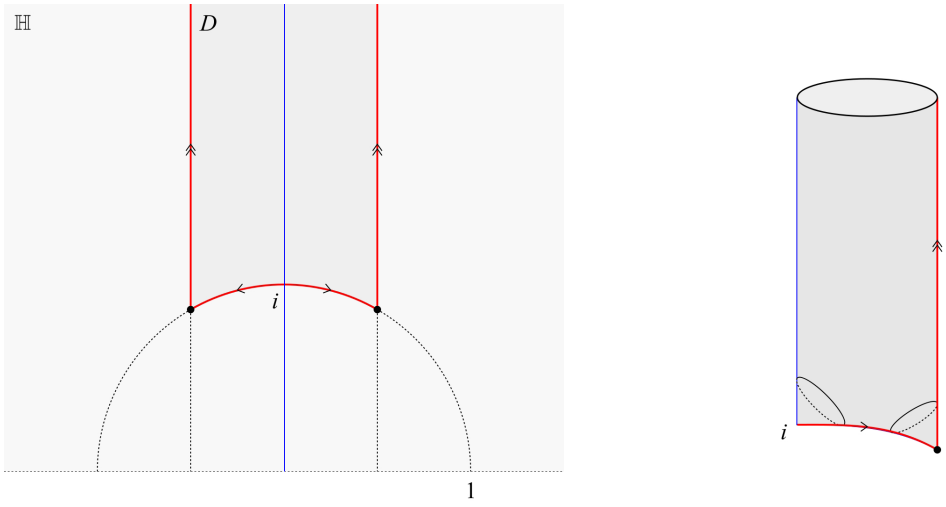


FIGURE 1 – Courbe Modulaire $SL_2(\mathbb{Z})\backslash\mathbb{H}$ et son domaine fondamental D [1]

[1] Guillaume BRUNERIE http ://www.eleves.ens.fr/home/brunerie/docs/tipe-reseaux-unitaires.pdf

Table des matières

1 Introduction

L'objet de ce mémoire est la construction d'une surface de Riemann $Y(\Gamma)$ appelée courbe modulaire comme étant le quotient du demi-plan de Poincaré $\mathbb{H}$ sous l'action homographique d'un sous-groupe Γ d'indice fini de $SL_2(\mathbb{Z})$. Cette surface n'étant pas compacte on rajoutera des points appelés pointes ou cusps pour obtenir une surface compacte $X(\Gamma)$ appelée courbe modulaire compactifiée ou, en fonction du contexte, simplement courbe modulaire. On pourra ainsi s'intéresser au genre de cette surface pour obtenir une formule exprimant ce genre en fonction de l'indice de Γ, du nombre de points Γ-elliptiques de $\mathbb{H}$ et du nombre de pointes. On appliquera ensuite cette formule aux surfaces $X(\Gamma(N))$ et $X(\Gamma_0(N))$ associées aux sous groupes de congruences $\Gamma(N)$ et $\Gamma_0(N)$ et on pourra exprimer le genre de ces surfaces directement en fonction de l'entier N.

2 Rappels et notations

2.1 Rappels sur les surfaces de Riemann

Définition 2.1.1. *Soit X est un espace topologique, on appelle carte de X tout homéomorphisme $\varphi : U \to V$ où U est un ouvert de X et V un ouvert de $\mathbb{C}$. L'ouvert U est alors appelé le domaine de la carte φ.*

Définition 2.1.2. *Une carte $\varphi : U \to V$ est dite centrée en $P \in X$ si $P \in U$ et $\varphi(P) = 0$.*

Remarque 2.1.1. *Soit $\varphi : U \to V$ une carte de X et $U_1 \subset U$ un ouvert, alors $\varphi_{|U_1} : U_1 \to \varphi(U_1)$ est une carte de X. On dit que $\varphi_{|U_1}$ est une sous-carte de X.*

Définition 2.1.3. *Soit $\varphi_1 : U_1 \to V_1$ et $\varphi_2 : U_2 \to V_2$ deux cartes de X. On dit que φ_1 et φ_2 sont compatibles si soit $U_1 \cap U_2 = \emptyset$ soit $\varphi_2 \circ \varphi_1^{-1} : \varphi_1(U_1 \cap U_2) \to \varphi_2(U_1 \cap U_2)$, ainsi que son inverse, sont holomorphes.*

Définition 2.1.4. *Un atlas $\mathcal{A}$ est un ensemble de cartes de X compatibles deux à deux telles que leurs domaines recouvrent X.*

Remarque 2.1.2. *Soit $\mathcal{A} = \{\varphi_i : U_i \to V_i\}$ un atlas de X et Y un ouvert de X alors l'ensemble $\mathcal{A}_Y = \left\{\varphi_{i\,|Y\cap U_i} : Y \cap U_i \to \varphi_i(Y \cap U_i)\right\}$ de sous-cartes de X est un atlas sur Y.*

Définition 2.1.5. *Deux atlas $\mathcal{A}$ et $\mathcal{B}$ sont équivalents si chaque carte de $\mathcal{A}$ est compatible avec toutes les cartes de $\mathcal{B}$.*

Définition 2.1.6. *Une structure complexe sur X est une classe d'équivalence d'atlas sur X.*

Définition 2.1.7. *Une surface de Riemann X est un espace topologique connexe, séparé muni d'une structure complexe.*

Définition 2.1.8. *Soit $f : X \to Y$ une application entre deux surfaces de Riemann, on dit que f est holomorphe en $P \in X$ s'il existe une carte (U_1, φ_1) de X avec $P \in U_1$ et une carte (U_2, φ_2) de Y avec $f(P) \in U_2$ telle que la composée $\varphi_2 \circ f \circ \varphi_1^{-1}$ soit holomorphe en $\varphi_1(P)$. De manière équivalente, puisque les cartes sont compatibles, f est holomorphe en $P \in X$ si et seulement si pour toute carte (U_1, φ_1) de X avec $P \in U_1$ et (U_2, φ_2) de Y avec $f(P) \in U_2$, la composée $\varphi_2 \circ f \circ \varphi_1^{-1}$ est holomorphe en $\varphi_1(P)$. Si W est un ouvert de X, on dit que f est holomorphe sur W si elle est holomorphe en tout point de W, en particulier f est holomorphe si elle est holomorphe sur X.*

Proposition 2.1.1. *Soit $f : X \to Y$ une application non constante entre deux surfaces de Riemann et W un ouvert de X. Si f est holomorphe sur W alors en tout point $P \in W$ il existe un unique entier $m \geq 1$ tel que pour toute carte (U_2, φ_2) de Y centrée en $f(P)$ il existe une carte (U_1, φ_1) de X centrée en P telle que $\forall z \in \varphi_1(U_1)$, $\varphi_2 \circ f \circ \varphi_1^{-1}(z) = z^m$.*

Démonstration. Soit $\varphi_2 : U_2 \to V_2$ une carte de Y centrée en $f(P)$, d'après la remarque 2.1.2 on peut trouver une carte $\phi : U \to V$ centrée en P telle que $U \subset W$. L'application f est donc holomorphe sur U et ainsi $\varphi_2 \circ f \circ \phi^{-1}$ est holomorphe sur l'ouvert $V \subset \mathbb{C}$ contenant 0. De plus, puisque X est connexe, f est non constante sur U. On pose $T = \varphi_2 \circ f \circ \phi^{-1}$ alors puisque $T(0) = 0$ et T n'est pas constante il existe un disque ouvert D centré en 0 tel que l'on puisse écrire $\forall z \in D$, $T(z) = z^m S(z)$ avec S une application holomorphe sur D, $S(0) \neq 0$ et $m \geq 1$ l'ordre de T en 0 (cf. [7] p.251). Puisque $S(0) \neq 0$ et S est holomorphe sur D il existe un disque ouvert $D' \subset D$ centré en 0 tel que S ne s'annule pas sur D'. Il existe donc une fonction R holomorphe sur D' telle que $\forall z \in D'$, $R(z)^m = S(z)$ (cf. [7] p.319). On pose $\forall z \in D'$, $\eta(z) = zR(z)$, on a alors $T(z) = (\eta(z))^m$, η est holomorphe sur D' et $\eta'(0) = R(0) \neq 0$ donc d'après le théorème d'inversion locale (cf. [7] p.257) il existe un voisinage V_0 ouvert de 0 tel que $\eta : V_0 \to \eta(V_0)$ soit biholomorphe. On pose $U_1 = \phi^{-1}(V_0)$ et $\varphi_1 = \eta \circ \phi$ alors $\varphi_1 : U_1 \to \varphi_1(U_1) = \eta(V_0)$ est une carte de X centrée en P compatible avec ϕ. De plus on a

$$\begin{aligned} \forall z \in \varphi_1(U_1),\ \varphi_2 \circ f \circ \varphi_1^{-1}(z) &= \varphi_2 \circ f \circ \phi^{-1} \circ \eta^{-1}(z) \\ &= T(\eta^{-1}(z)) \\ &= \eta(\eta^{-1}(z))^m \\ &= z^m \end{aligned}$$

L'unicité vient du fait que si l'on peut écrire $\varphi_2 \circ f \circ \varphi_1^{-1}(z) = z^m$ alors tous les points proches de $f(P)$ possèdent exactement m antécédents proches de P donc m dépend uniquement des propriétés de f autour de P. □

Définition 2.1.9. *L'entier m est appelé la multiplicité de f en P et est noté $mult_f(P)$.*

Proposition 2.1.2. *Soit $f : X \to Y$ et $g : Y \to Z$ deux applications non constantes entre surfaces de Riemann. Soit $P \in X$, si f est holomorphe sur un ouvert W contenant P et g holomorphe sur un ouvert W' tel que $f(W) \subset W'$ alors $g \circ f$ est holomorphe sur W et $mult_{g \circ f}(P) = mult_f(P) \times mult_g(f(P))$.*

Démonstration. On pose $m = \text{mult}_g(f(P))$ et $n = \text{mult}_f(P)$. Soit (U_2, φ_2) une carte centrée en $g(f(P))$ de Z alors il existe une carte (U_1, φ_1) de Y centrée en $f(P)$ telle que $\forall z \in \varphi_1(U_1)$, $\varphi_2 \circ g \circ \varphi_1^{-1}(z) = z^m$. La carte (U_1, φ_1) est centrée en $f(P)$ donc il existe

une carte (U_3, φ_3) de X centrée en P telle que $\forall z \in \varphi_3(U_3)$, $\varphi_1 \circ f \circ \varphi_3^{-1}(z) = z^n$. Ainsi $\forall z \in \varphi_3(U_3)$,

$$\begin{aligned}\varphi_2 \circ g \circ f \circ \varphi_3^{-1}(z) &= \varphi_2 \circ g \circ \varphi_1^{-1} \circ \varphi_1 \circ f \circ \varphi_3^{-1}(z) \\ &= \varphi_2 \circ g \circ \varphi_1^{-1}(z^n) \\ &= (z^n)^m \\ &= z^{nm}\end{aligned}$$

donc $\text{mult}_{g\circ f}(P) = nm$ □

Proposition 2.1.3. *Soit $f : X \to Y$ une application non constante holomorphe entre deux surfaces de Riemann compactes et soit $y \in Y$ alors la quantité $d_y(f) = \sum_{P\in f^{-1}(y)} mult_f(P)$ est constante et ne dépend pas de y. La quantité $d_y(f)$ est appelée le degré de f que l'on note* $\deg(f)$.

L'idée de la preuve (cf. [4],p.47) est de montrer que l'application $\phi : Y \to \mathbb{N}$ telle que $\phi(y) = d_y(f)$ est localement constante on aura alors que ϕ est constante par connexité de Y.

3 Construction des courbes modulaires $Y(\Gamma)$ et $X(\Gamma)$

3.1 Action de $SL_2(\mathbb{Z})$ sur le demi-plan de Poincaré

Définition 3.1.1. *On appelle demi-plan de Poincaré l'ensemble* $\mathbb{H} = \{z \in \mathbb{C}, \Im(z) > 0\}$.

On rappelle que $SL_2(\mathbb{Z})$ et ses sous-groupes sont tous des sous-groupes discrets de $SL_2(\mathbb{R})$. Dans la suite $SL_2(\mathbb{Z})$ sera noté $\Gamma(1)$ et Γ désignera un sous-groupe de $\Gamma(1)$ d'indice fini.

Proposition 3.1.1. *Le groupe Γ agit continuement sur $\mathbb{H}$ par l'action homographique*

$$\begin{gathered}\Gamma \times \mathbb{H} \longrightarrow \mathbb{H} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, z \longmapsto \frac{az+b}{cz+d}\end{gathered}$$

Démonstration. Soit $z \in \mathbb{H}$ alors

$$\Im(\frac{az+b}{cz+d}) = \frac{(ad-bc)\Im(z)}{|cz+d|^2} > 0$$

De plus $I.z = z$ et si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ et $\gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma$ alors

$$(\gamma\gamma').z = \frac{(aa'+bc')z + ab' + bd'}{(ca'+c'd)z + cb' + dd'}$$

et

$$\gamma.(\gamma'.z) = \frac{a(a'z+b') + b(c'z+d')}{c(a'z+b') + d(c'z+d')} = \frac{(aa'+bc')z + ab' + bd'}{(ca'+c'd)z + cb' + dd'} = (\gamma\gamma').z$$

Puisque que Γ est discret et que l'application de $\mathbb{H}$ dans lui même qui à z associe $\frac{az+b}{cz+d}$ est continue, l'action de Γ sur $\mathbb{H}$ est continue.

□

On notera $\Gamma\backslash\mathbb{H}$ l'ensemble quotient des orbites pour l'action homographique de Γ sur $\mathbb{H}$, $\pi_\Gamma : \Gamma \longrightarrow \Gamma\backslash\mathbb{H}$ la projection canonique, $\Gamma_z = \mathrm{Stab}_\Gamma(z)$ le stabilisateur de z sous l'action de Γ et $Z(\Gamma) = \Gamma \cap \{\pm I\}$ le centre de Γ.

Définition 3.1.2. *On appelle domaine fondamental de Γ un ouvert connexe D de $\mathbb{H}$ tel que D ne possède pas deux points Γ-équivalent pour l'action homographique et tel que la restriction de π_Γ à $\overline{D}$ soit surjective.*

On trouvera la preuve des deux propositions suivantes dans [2] p.32

Proposition 3.1.2. *On pose $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\rho = \exp(2i\pi/6)$ on a*

$$a) Stab_{\Gamma(1)}(i) = \{\pm I, \pm S\}$$
$$b) Stab_{\Gamma(1)}(\rho) = \left\{\pm I, \pm TS, \pm (TS)^2\right\}$$
$$c) Stab_{\Gamma(1)}(\rho^2) = \left\{\pm I, \pm ST, \pm (ST)^2\right\}$$

.

Proposition 3.1.3. *L'ensemble $D = \{z \in \mathbb{H}, |z| > 1, -1/2 < \Re(z) < 1/2\}$ est un domaine fondamental pour $\Gamma(1)$ (cf figure 1) et deux points z et z' de $\overline{D}$ sont $\Gamma(1)$-équivalent si et seulement si $|z| = 1$ et $z' = Sz$ ou $\Re(z) = \pm 1/2$ et $z' = Tz$. De plus si $z \in \overline{D}$ et $Stab_{\Gamma(1)}(z) \neq \{\pm I\}$ alors $z \in \{i, \rho, \rho^2\}$.*

Définition 3.1.3. *Une matrice $\gamma \in SL_2(\mathbb{Z})$ est dite elliptique si $|\,Tr(\gamma)\,| < 2$.*

Définition 3.1.4. *Un élément $z \in \mathbb{H}$ est un point Γ-elliptique si son stabilisateur sous Γ contient une matrice elliptique.*

Proposition 3.1.4. *Un point z appartenant à $\mathbb{H}$ est $\Gamma(1)$-elliptique si et seulement si il est $\Gamma(1)$-équivalent à i ou à ρ.*

Démonstration. Soit z un point $\Gamma(1)$-elliptique alors il existe une matrice elliptique γ_e tel que $z = \gamma_e z$. De plus il existe z' dans la clôture du domaine fondamental D tel que $z = \gamma z'$ donc $\gamma^{-1}\gamma_e\gamma \in \Gamma_{z'}$. Puisque $\gamma_e \neq \pm I$, $\Gamma_{z'} \neq \{\pm I\}$ et donc, d'après la proposition 3.1.3, $z' \in \{i, \rho, \rho^2\}$ et ainsi z est $\Gamma(1)$-équivalent à i ou à ρ. Inversement pour tout $\gamma \in \Gamma(1)$ on a $(\gamma S\gamma^{-1})\gamma i = \gamma i$ et $(\gamma TS\gamma^{-1})\gamma\rho = \gamma\rho$ et puisque S et TS sont elliptiques il en est de même de $\gamma TS\gamma^{-1}$ et $\gamma TS\gamma^{-1}$. □

Proposition 3.1.5. *Soit $z \in \mathbb{H}$ un point Γ-elliptique. Si z est $\Gamma(1)$-équivalent à i alors $\Gamma_z/Z(\Gamma)$ est fini, cyclique d'ordre 2 et si z est $\Gamma(1)$-équivalent à ρ, le groupe $\Gamma_z/Z(\Gamma)$ est fini, cyclique d'ordre 3.*

Démonstration. Supposons que $z = \gamma_1 i$ avec $\gamma_1 \in \Gamma(1)$ alors $\Gamma_z \subset \gamma_1 \mathrm{Stab}_{\Gamma(1)}(i)\gamma_1^{-1} = \left\{\pm I, \pm\gamma_1 S\gamma_1^{-1}\right\}$. Puisque z est un point Γ-elliptique $\gamma_1 S\gamma_1^{-1}$ ou $-\gamma_1 S\gamma_1^{-1}$ sont dans Γ_z donc $\Gamma_z/Z(\Gamma) = \left\{\overline{I}, \overline{\gamma_1 S\gamma_1^{-1}}\right\}$ et puisque $(\gamma_1 S\gamma_1^{-1})^2 = -I$, $\Gamma_z/Z(\Gamma)$ est fini et cyclique d'ordre 2. De même si $z = \gamma_1\rho$ puisque $\mathrm{Stab}_{\Gamma(1)}(\rho) = \{\pm I, \pm TS, \pm(TS)^2\}$ et $(TS)^4 = -TS$ on a que $\Gamma_z/Z(\Gamma)$ est fini et cyclique d'ordre 3. □

3.2 Topologie et structure complexe sur $\Gamma\backslash\mathbb{H}$

On munit désormais $\Gamma\backslash\mathbb{H}$ de la topologie quotient, c'est-à-dire que U est un ouvert de $\Gamma\backslash\mathbb{H}$ si et seulement si $\pi_\Gamma^{-1}(U)$ est un ouvert de $\mathbb{H}$. On souhaite montrer que $\Gamma\backslash\mathbb{H}$ est une surface de Riemann appelée courbe modulaire et notée $Y(\Gamma)$, pour cela on va montrer que la topologie quotient est séparée et définir une structure complexe.

Définition 3.2.1. *Soit G un groupe agissant sur un espace topologique X, l'action de G sur X est dite proprement discontinue si pour tout x et y dans X il existe un voisinage V_x de x et un voisinage V_y de y tel que l'ensemble $\{g \in G, gV_x \cap V_y \neq \emptyset\}$ est fini.*

Proposition 3.2.1. *Soit Γ un sous groupe de $\Gamma(1)$ on a*

a) $\forall x \in \mathbb{H}$, $Stab_\Gamma(x)$ *est un sous-groupe fini.*

b) $\forall x \in \mathbb{H}$, *il existe un voisinage U qui vérifie* : $\gamma \in \Gamma$ *et* $U \cap \gamma U \neq \emptyset \Leftrightarrow \gamma \in Stab_\Gamma(x)$

c) $\forall x, y \in \mathbb{H}$ *tels que x et y ne soient pas dans la même Γ-orbite , il existe U voisinage de x et V voisinage de y tel que* $\forall \gamma \in \Gamma, V \cap \gamma U = \emptyset$.

Démonstration. *a*) Puisque que Γ est discret, l'action de Γ sur $\mathbb{H}$ est proprement discontinue (cf[5] p.17) donc il existe un voisinage V_x de x tel que l'ensemble $\{\gamma \in \Gamma, V_x \cap \gamma V_x \neq \emptyset\}$ est fini. On a alors $\mathrm{Stab}_\Gamma(x) \subset \{\gamma \in \Gamma, V_x \cap \gamma V_x \neq \emptyset\} < \infty$.
b) On peut écrire

$$\{\gamma \in \Gamma, V_x \cap \gamma V_x \neq \emptyset\} = \{\gamma_i, 1 \leq i \leq n\}$$

avec

$$\{\gamma_i, 1 \leq i \leq n\} \cap \mathrm{Stab}_\Gamma(x) = \{\gamma_1, \dots \gamma_s\}$$

Pour chaque $i > s$ on choisit deux voisinages disjoints V_i de x et W_i de $\gamma_i x$ et on pose

$$U = V_x \bigcap_{i>s} (V_i \cap \gamma_i^{-1} W_i)$$

On a alors pour $i > s$, $\gamma_i U \subset W_i$ et $U \subset V_i$ et U est un voisinage ouvert de x car c'est une intersection finie d'ouverts d'où le résultat puisque V_i et W_i sont disjoints.
c) On choisit V_x voisinage de x et V_y voisinage de y tels que $\{\gamma \in \Gamma, V_y \cap \gamma V_x \neq \emptyset\}$ est fini on peut alors écrire $\{\gamma \in \Gamma, V_y \cap \gamma V_x \neq \emptyset\} = \{\gamma_i, 1 \leq i \leq n\}$. Puisque x et y ne sont pas sur la même orbite $\gamma_i x \neq y$ on peut donc choisir deux voisinages disjoints U_i de $\gamma_i x$ et V_i de y. On pose

$$U = V_x \bigcap_{1 \leq i \leq n} \gamma_i^{-1} U_i, \; V = V_y \bigcap_{1 \leq i \leq n} V_i$$

Alors U et V sont des voisinages ouverts respectivement de x et de y et $\forall \gamma \in \Gamma, \; \gamma U \cap V = \emptyset$. □

Proposition 3.2.2. *L'espace topologique $\Gamma\backslash\mathbb{H}$ est connexe et séparé.*

Démonstration. $\Gamma\backslash\mathbb{H}$ est connexe car $\mathbb{H}$ est connexe. Soit x et y dans $\mathbb{H}$ qui ne sont pas Γ-équivalents alors d'après la proposition 3.2.1c) il existe U voisinage ouvert de x et V voisinage ouvert de y tels que $\forall \gamma \in \Gamma, V \cap \gamma U = \emptyset$ donc $\pi_\Gamma(U)$ et $\pi_\Gamma(V)$ sont disjoints et ouverts car $\pi_\Gamma^{-1}(\pi_\Gamma(U)) = \bigcup_{\gamma \in \Gamma} \gamma U$ est un ouvert de $\mathbb{H}$ et de même pour $\pi_\Gamma(V)$. □

On va maintenant définir des cartes sur $\Gamma\backslash\mathbb{H}$. Soit $a = \pi_\Gamma(z_0) \in \Gamma\backslash\mathbb{H}$ alors d'après la proposition 3.2.1.b il existe V un voisinage de z_0 tel que $V \cap \gamma V \neq \emptyset \Leftrightarrow \gamma \in \mathrm{Stab}_\Gamma(z_0)$. On pose $U = \pi_\Gamma(V)$, alors $\pi_\Gamma^{-1}(U) = \bigcup_{\gamma\in\Gamma} \gamma V$ donc U est ouvert. On a de plus $\bigcup_{\gamma\in\Gamma} \gamma V = \bigsqcup_{i\in I}(\gamma_i\Gamma_{z_0})V$. D'après la proposition 3.1.3 soit $\mathrm{Stab}_\Gamma(z_0) \subset \{\pm I\}$, soit z_0 est $\Gamma(1)$-équivalent à i ou à ρ et donc, d'après les propositions 3.1.4 et 3.3.9, Γ-elliptique. On va donc distinguer ces trois cas disjoints pour construire des cartes centrées en a.

Proposition 3.2.3. *Si $Stab_\Gamma(z_0) \subset \{\pm I\}$, la restriction $\pi_\Gamma : V \longrightarrow U$ définit un homéomorphisme d'inverse noté ψ_a*

Démonstration. Si $\pi_\Gamma(x) = \pi_\Gamma(y)$ avec x et y dans V alors $x = \gamma y$ et donc $V \cap \gamma V \neq \emptyset$ ce qui implique $\gamma \in \Gamma_{z_0}$ donc $\gamma = \pm I$ et $x = y$. Ainsi $\pi_\Gamma : V \longrightarrow \pi_\Gamma(V)$ est bijective, de plus par définition π_Γ est continue et est ouverte car si O est un ouvert inclus dans V alors $\pi_\Gamma^{-1}(\pi_\Gamma(O)) \cap V = \bigcup \gamma O \cap V$ est un ouvert de V. □

Dans le cas où $\mathrm{Stab}_\Gamma(z_0) \subset \{\pm I\}$ on choisira (U, ψ_a) comme carte locale en a. Supposons maintenant que z_0 est Γ-elliptique.

Lemme 3.2.1. *Si $z_0 \in \mathbb{H}$, on note $D(0,1)$ le disque ouvert unité alors l'application*

$$\begin{aligned} \lambda : \mathbb{H} &\longrightarrow D(0,1) \\ z &\longmapsto \frac{z - z_0}{z - \bar{z_0}} \end{aligned}$$

est bi-holomorphe.

Démonstration. L'application λ est bien définie car

$$|\lambda(z)|^2 = \frac{|z - z_0|^2}{|z - \bar{z_0}|^2} = \frac{(\Re z - \Re z_0)^2 + (\Im z - \Im z_0)^2}{(\Re z - \Re z_0)^2 + (\Im z + \Im z_0)^2} < 1$$

On considère l'application

$$\begin{aligned} \lambda^{-1} : D(0,1) &\longrightarrow \mathbb{H} \\ z &\longmapsto \frac{z\bar{z_0} - z_0}{z - 1} \end{aligned}$$

λ^{-1} est bien définie car $\Im(\lambda^{-1}(z)) = \frac{\Im(z_0)(1-|z|^2)}{|z-1|^2} > 0$, de plus $\forall z \in \mathbb{H},\ \lambda^{-1}(\lambda(z)) = z$ et $\forall z \in D(0,1),\ \lambda(\lambda^{-1}(z)) = z$. Ainsi λ est bijective d'inverse λ^{-1} et il est clair qu'elles sont toutes les deux holomorphes. □

Proposition 3.2.4. *Si z_0 est $\Gamma(1)$-équivalent à i alors il existe un voisinage $U_a \subset U$ de a et V_0 de 0 tel que l'application*

$$\begin{aligned} \phi_a : U_a &\longrightarrow V_0 \\ \pi_\Gamma(z) &\longmapsto (\lambda(z))^2 \end{aligned}$$

est un homémorphisme.

Démonstration. On note W_r le disque ouvert de centre 0 de rayon $r > 0$ et Γ_{z_0} le stabilisateur de z_0 sous Γ. Puisque $\lambda(z_0) = 0$ il existe un $r > 0$ tel que $\lambda^{-1}(W_r) \subset V$. On pose $U_a = \pi_\Gamma(\lambda^{-1}(W_r))$, alors U_a est un voisinage de a inclus dans U. Le stabilisateur Γ_{z_0} est un sous-groupe de $SL_2(\mathbb{Z})$ donc si on identifie λ à la matrice $\begin{pmatrix} 1 & -z_0 \\ 1 & -\bar{z_0} \end{pmatrix} \in GL_2(\mathbb{C})$, $\lambda\Gamma_{z_0}\lambda^{-1}$ est un sous groupe de $GL_2(\mathbb{C})$. De plus ce sous-groupe agit sur $D(0,1)$ via $(\lambda\gamma\lambda^{-1}, z) \longmapsto (\lambda\gamma\lambda^{-1})z$. Pour $\gamma \in \Gamma_{z_0}$ fixé on considère l'application

$$\begin{aligned} f_\gamma : D(0,1) &\longrightarrow D(0,1) \\ z &\longmapsto \lambda\gamma\lambda^{-1}z \end{aligned}$$

alors f est bi-holomorphe de réciproque

$$\begin{aligned} f_\gamma^{-1} : D(0,1) &\longrightarrow D(0,1) \\ z &\longmapsto \lambda\gamma^{-1}\lambda^{-1}z \end{aligned}$$

De plus $f_\gamma(0) = f_\gamma^{-1}(0) = 0$, en appliquant le lemme de Schwarz à f_γ et à f_γ^{-1} on a $|f_\gamma(z)| = |z|$ et $f_\gamma(z) = \exp(2i\theta(\gamma))z$ avec $0 \leq \theta(\gamma) < \pi$. Montrons que $\theta(\gamma) \in \frac{\pi}{2}\mathbb{Z}$. D'après la proposition 3.1.5 $\Gamma_{z_0}/Z(\Gamma)$ est cyclique d'ordre 2, de générateur noté $\overline{\gamma_0}$. Puisque $f_{-\gamma} = f_\gamma$ il suffit de vérifier que $\theta(I)$ et $\theta(\gamma_0)$ sont dans $\frac{\pi}{2}\mathbb{Z}$. Si on se donne $z \neq 0$, on a $f_I(z) = z$ donc $\theta(I) = 0$ et $z = f_{\gamma_0^2}(z) = f_{\gamma_0} \circ f_{\gamma_0}(z) = \exp(4i\theta(\gamma_0))z$ donc $\exp(4i\theta(\gamma_0)) = 1$ et $\theta(\gamma_0) \in \frac{\pi}{2}\mathbb{Z}$. Ainsi $\forall \gamma \in \Gamma_{z_0}, f_\gamma$ est une rotation de centre 0 et d'angle $2\pi k/2$ avec $k \in \mathbb{Z}$. Puisque f_γ est une rotation, $\lambda^{-1}(W_r)$ est stable sous l'action de Γ_{z_0} et W_r est stable sous l'action de $\lambda\Gamma_{z_0}\lambda^{-1}$. Puisque $V \cap \gamma V \neq \emptyset \Rightarrow \gamma \in \Gamma_{z_0}$, U_a est homéomorphe à $\Gamma_{z_0}\backslash\lambda^{-1}(W_r)$ via $\eta_1 : \pi_\Gamma(z) \longmapsto \pi_{\Gamma_{z_0}}(z)$. De plus $\Gamma_{z_0}\backslash\lambda^{-1}(W_r)$ est homéomorphe à $\lambda\Gamma_{z_0}\lambda^{-1}\backslash W_r$ via $\eta_2 : \pi_{\Gamma_{z_0}}(z) \longmapsto \pi_{\lambda\Gamma_{z_0}\lambda^{-1}}(\lambda z)$. On considère l'application

$$\begin{aligned} \eta_3 : \lambda\Gamma_{z_0}\lambda^{-1}\backslash W_r &\longrightarrow W_{r^2} \\ \pi(w) &\longmapsto w^2 \end{aligned}$$

L'application $w \mapsto w^2$ de W_r dans W_{r^2} est surjective, ouverte et invariante par rotation de centre 0 et d'angle $2\pi k/2$ de plus si $w_1^2 = w_2^2$ alors $|w_1| = |w_2|$ et $\mathrm{Arg}(w_2) = \mathrm{Arg}(w_1) + 2k\pi/2$ donc l'application η_3 définit un homéomorphisme. En posant $V_0 = W_{r^2}$, on a $\phi_a = \eta_3 \circ \eta_2 \circ \eta_1$ donc ϕ_a est un homéomorphisme. □

Dans le cas où z_0 est $\Gamma(1)$-équivalent à i on choisira (U_a, ϕ_a) comme carte centrée en a.

Proposition 3.2.5. *Si z_0 est $\Gamma(1)$-équivalent à ρ alors il existe un voisinage $U_a \subset U$ de a et V_0 de 0 tel que l'application*

$$\begin{aligned} \varphi_a : U_a &\longrightarrow V_0 \\ \pi_\Gamma(z) &\longmapsto (\lambda(z))^3 \end{aligned}$$

est un homémorphisme.

Démonstration. On reprend la démonstration précédente en sachant que $\Gamma_{z_0}/Z(\Gamma)$ est cyclique d'ordre 3, on aura alors f_γ est une rotation de centre 0 et d'angle $2k\pi/3$. □

Dans le cas où z_0 est $\Gamma(1)$-équivalent à ρ on choisira (U_a, φ) comme carte centrée en a.

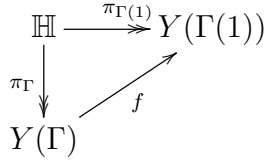
Proposition 3.2.6. *L'ensemble $\mathcal{A} = \{\psi_a, \phi_a, \varphi_a, a \in \Gamma/\mathbb{H}\}$ est un atlas sur $Y(\Gamma)$*

Démonstration. Puisque les domaines des cartes de $\mathcal{A}$ recouvrent $Y(\Gamma)$ il reste à montrer que ses cartes sont compatibles. Soit $a = \pi_\Gamma(z_1)$ et $b = \pi_\Gamma(z_2)$, on note $U_1 = \pi_\Gamma(V_1)$ et $U_2 = \pi_\Gamma(V_2)$. On suppose $U_1 \cap U_2 \neq \emptyset$. Montrons que ψ_a et ψ_b sont compatibles. On pose $f = \psi_b \circ \psi_a^{-1} : \psi_a(U_1 \cap U_2) \subset V_1 \longrightarrow \psi_b(U_1 \cap U_2) \subset V_2$. On pose $W_1 = \psi_a(U_1 \cap U_2)$ et $W_2 = \psi_b(U_1 \cap U_2)$ alors W_1 est un ouvert inclus dans V_1 et W_2 est un ouvert inclus dans V_2. Si $z \in W_1$ alors il existe $z' \in W_2$ tel que $\bar{z} = \bar{z'}$ et donc $z' = \gamma_z z$. Ainsi $f(z) = \psi_b \circ \psi_a^{-1}(z) = \psi_b \circ \psi_a^{-1}(\psi_a(\bar{z})) = \psi_b(\bar{z}) = \psi_b(\bar{z'}) = \psi_b(\bar{\gamma_z} z) = \gamma_z z$. Montrons que f est holomorphe sur toutes les composantes connexes de W_1 qui sont des ouverts dans W_1 on aura alors que f est holomorphe sur W_1 . Soit C une telle composante connexe, on pose $C' = f(C)$ alors, puisque f est continue et ouverte, C' est connexe et ouvert dans W_2. Or $C' \subset \pi_\Gamma^{-1}(U_1 \cap U_2) \subset \pi_\Gamma^{-1}(U_1) = \bigcup_{\gamma \in \Gamma} \gamma V_1 = \bigsqcup_{i \in I} (\gamma_i \Gamma_{z_0}) V_1$ avec γ_i les représentants des classes de Γ/Γ_{z_0}. Puisque C' est connexe il existe un γ_{i_0} tel que $C' \subset \gamma_{i_0} \Gamma_{z_0} V_1 \subset \gamma_{i_0} \{\pm I\} V_1$. Donc si $z \in C$ alors $f(z) = \gamma_z z = \pm \gamma_{i_0} z' = \gamma_{i_0} z'$ avec $z' \in V_1$ et ainsi $\gamma_{i_0}^{-1} \gamma_z \in \Gamma_{z_0}$ donc $\gamma_z = \pm \gamma_{i_0}$ et $f(z) = \gamma_{i_0} z$. Ainsi f est holomorphe sur C. Pour la compatibilité des autres cartes cf [5].

□

Proposition 3.2.7. *La surface $Y(\Gamma)$ n'est pas compacte.*

Démonstration. Commençons par montrer que $Y(\Gamma(1))$ n'est pas compacte (cf figure 1). D'après la propostion 3.1.3 $Y(\Gamma(1))$ est homéomorphe via la projection $\pi_{\Gamma(1)}$ à l'ensemble
$D' = D \cup \{z \in \mathbb{C}, \Re z = 1/2, \Im z \geq \Im \rho\} \cup \{z \in \mathbb{C}, |z| = 1, 0 \leq \Re z \leq \Re \rho, \Im z > 0\}$ où D est le domaine fondamental de $\Gamma(1)$. Puisque D' n'est pas compacte, $Y(\Gamma(1))$ n'est pas compacte. D'après le théorème de factorisation il existe une unique application surjective $f : Y(\Gamma) \to Y(\Gamma(1))$ tel que le diagramme suivant commute :



On a alors $\forall z \in \mathbb{H}$, $f(\bar{z}^\Gamma) = \bar{z}^{\Gamma(1)}$. Si U est un ouvert de $Y(\Gamma(1))$ alors $\pi_\Gamma^{-1}(f^{-1}(U)) = \pi_{\Gamma(1)}^{-1}(U)$ donc f est continue et puisque la topologie sur $Y(\Gamma(1))$ est séparée $Y(\Gamma)$ n'est pas compacte car sinon $Y(\Gamma(1)) = f(Y(\Gamma))$ serait compacte. □

3.3 Topologie et structure complexe sur $\Gamma\backslash\mathbb{H}^\star$

Pour rendre compacte $Y(\Gamma)$ on va ajouter des points à $\mathbb{H}$ qu'on appelera des pointes (ou cusps) et dans la suite une pointe pourra désigné un point ou son orbite selon le contexte. On pose $\mathbb{H}^\star = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$. On identifie géométriquement le point ∞ au point $i\infty$ et on étend l'action de Γ sur $\mathbb{H}$ à $\mathbb{H}^\star$ de la manière suivante : $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \begin{cases} \frac{a}{c} & \text{si } c \neq 0 \\ \infty & \text{si } c = 0 \end{cases}$ et $\begin{pmatrix} a & b \\ c & d \end{pmatrix} r = \begin{cases} \frac{ar+b}{cr+d} & \text{si } r \neq \frac{-d}{c} \\ \infty & \text{si } r = \frac{-d}{c} \end{cases}$ si $r \in \mathbb{Q}$.

On va maintenant étendre la topologie de $\mathbb{H}$ en une topologie sur $\mathbb{H}^\star$ qui sera séparée :
- les voisinages des points z de $\mathbb{H}$ sont ceux donnés par la topologie usuelle de $\mathbb{C}$.
- Un système fondamental de voisinages de ∞ est donné par les demi-plans :
$\{z \in \mathbb{H}, \Im z > M\} \cup \{i\infty\}$, $M > 0$.
- Un système fondamental de voisinages de $r \in \mathbb{Q}$ est donné par les $C \cup \{r\}$ où C est un disque ouvert contenu dans $\mathbb{H}$ et tangent en r à l'axe réel.

Proposition 3.3.1. *L'action de Γ sur $\mathbb{H}^\star$ est continue.*

Démonstration. D'après la proposition 3.1.1 il reste à vérifier que pour tout $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ l'application $z \mapsto \gamma z$ est continue sur $\mathbb{Q} \cup \{\infty\}$. On fixe un tel γ en supposant $c \neq 0$ alors dans ce cas si $V_M = \{z \in \mathbb{H}, \Im z > M\}$ on a

$$\gamma^{-1}(V_M) = \left\{ z \in \mathbb{H}, \frac{\Im(z)}{|cz+d|^2} > M \right\}$$

qui est le disque ouvert de $\mathbb{H}$ de rayon $1/(2Mc^2)$ tangent en $-d/c$, en effet

$$\begin{aligned}
\Im(z)/|cz+d|^2 > M &\Leftrightarrow M(c^2\Im(z)^2 + c^2\Re(z)^2 + 2cd\Re(z) + d^2) - \Im(z) < 0 \\
&\Leftrightarrow \Im(z)^2 + \Re(z)^2 + \frac{2d\Re(z)}{c} + \frac{d^2}{c^2} - \frac{\Im(z)}{Mc^2} + \frac{1}{(2Mc^2)^2} < \frac{1}{(2Mc^2)^2} \\
&\Leftrightarrow |z - (\frac{-d}{c} + \frac{i}{2Mc^2})|^2 < \frac{1}{(2Mc^2)^2} \\
&\Leftrightarrow d(z, -\frac{d}{c} + \frac{i}{2Mc^2}) < \frac{1}{(2Mc^2)}
\end{aligned}$$

De plus si $U_q = C_r \cup \{q\}$ est un voisinage de $q \in \mathbb{Q}$ avec C_r de rayon r et $q \neq \frac{a}{c}$ alors, puisque qu'une homographie préserve les cercles, $\gamma^{-1}(U_q) = U_{q'}$ avec $q' = \gamma^{-1}q$ et si $q = \frac{a}{c}$ alors $\gamma^{-1}(U_q) = V_{1/2rc^2} \cup \{\infty\}$. □

Proposition 3.3.2. *L'action de $\Gamma(1)$ sur les pointes est transitive et l'application $\pi_{\Gamma(1)} : \overline{D} \cup \{\infty\} \longrightarrow \Gamma(1)\backslash\mathbb{H}^\star$, où D est le domaine fondamental de $\Gamma(1)$, est surjective.*

Démonstration. Si $\frac{n}{m} \in \mathbb{Q}$ avec $m \wedge n = 1$ alors $\begin{pmatrix} a & b \\ n & -m \end{pmatrix} \frac{n}{m} = \infty$ avec $-a$ et $-b$ des coefficients de Bezout de m et n. Ainsi l'action sur les pointes est bien transitive donc si z est une pointe alors $\bar{z} = \bar{\infty}$. □

On note désormais $X(\Gamma) = \Gamma\backslash\mathbb{H}^\star$ que l'on munit de la topologie quotient. On appelle courbe modulaire compactifiée la surface de Riemann $X(\Gamma)$.

Proposition 3.3.3. *L'espace topologique $X(\Gamma)$ est connexe et séparé.*

Démonstration. Puisque $\mathbb{H}^\star$ est connexe pour la topologie définie plus haut il en est de même pour $X(\Gamma)$. Soit $x = \pi_\Gamma(z_1)$ et $y = \pi_\Gamma(z_2)$, puisque la topologie sur $Y(\Gamma)$ est séparée il reste à examiner le cas z_1 et z_2 sont deux pointes et le cas z_1 est une pointe et $z_2 \in \mathbb{H}$ (cf [5] p.27).

□

Proposition 3.3.4. *La surface $X(\Gamma)$ est compacte.*

Démonstration. Puisque Γ est d'indice fini m on peut écrire $\Gamma(1) = \bigsqcup_{i=1}^{m} \Gamma\gamma_i$. On pose alors $D' = \bigcup_{i=1}^{m} \gamma_i(\overline{D} \cup \{\infty\})$ avec D le domaine fondamental de $\Gamma(1)$. Puisque $\overline{D} \cup \{\infty\}$ est compacte et l'action de $\Gamma(1)$ sur $\mathbb{H}^\star$ est continue D' est compacte. Soit $\bar{z} \in X(\Gamma)$ alors il existe $z' \in \overline{D} \cup \{\infty\}$ tel que $z = \gamma z'$ avec $\gamma \in \Gamma(1)$. Il existe alors $1 \leq i \leq m$ tel que $\gamma \in \Gamma\gamma_i$ et donc z est Γ-équivalent à un élément de D'. Ainsi $\pi_\Gamma(D') = X(\Gamma)$ et puisque π_Γ est continue et que la topologie sur $X(\Gamma)$ est séparée, $X(\Gamma)$ est compacte. $\square$

On va maintenant définir une structure complexe sur $X(\Gamma)$, puisque $X(\Gamma) = Y(\Gamma) \sqcup \pi_\Gamma(\{cusps\})$ il reste à définir des cartes centrées en $a \in \pi_\Gamma(\{cusps\})$. Soit $a = \pi_\Gamma(z_0)$ avec $z_0 = \mathbb{Q} \cup \{\infty\}$ tel que $\sigma z_0 = \infty$, $\sigma \in \Gamma(1)$.

Proposition 3.3.5. *Il existe un voisinage U_a de a et un entier $h \in \mathbb{N}^\star$ qui dépend de a tel que l'application suivante définisse un homéomorphisme*

$$\begin{aligned} \eta_a : U_a &\longrightarrow D(0, e^{-4\pi/h}) \\ \pi_\Gamma(z) &\longmapsto \begin{cases} \exp(2i\pi\sigma z/h) & z \neq z_0 \\ 0 & z = z_0 \end{cases} \end{aligned}$$

Démonstration. On a $\sigma\Gamma_{z_0}\sigma^{-1} \subset \mathrm{Stab}_{\Gamma(1)}(\infty) = \{\pm T^m, m \in \mathbb{Z}\}$ donc

$$\frac{\sigma\Gamma_{z_0}\sigma^{-1}}{\{\pm I\}} \subset \{T^m, m \in \mathbb{Z}\}$$

Ce dernier groupe étant cyclique il existe un entier $h \geq 0$ tel que

$$\frac{\sigma\Gamma_{z_0}\sigma^{-1}}{\{\pm I\}} = \left\{(T^h)^m, m \in \mathbb{Z}\right\}$$

Puisque Γ est d'indice fini il contient une puissance non nulle de $\sigma^{-1}T\sigma$ donc $h \neq 0$. Ainsi

$$\sigma\Gamma_{z_0}\sigma^{-1}.\{\pm I\} = \left\{\pm T^{hm}, m \in \mathbb{Z}\right\}$$

On pose maintenant $V = \{z \in \mathbb{C}, \Im z > 2\} \cup \{\infty\}$, $V' = \sigma^{-1}(V)$ et $U_a = \pi_\Gamma(V')$ alors U_a et un voisinage de a. Montrons maintenant que $V \cap \gamma V \neq \emptyset \Leftrightarrow \gamma \in \Gamma_\infty$, Supposons que $\gamma z \in V$ avec $z \in V$ et $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ alors

$$2 \leq \Im(\gamma z) = \frac{\Im(z)}{|cz+d|^2} \leq \frac{1}{|c|^2\Im(z)} \leq \frac{1}{2|c|^2}$$

donc $c = 0$ et $\gamma = \pm T^m$ donc $\gamma \in \Gamma_\infty$. Pour l'autre implication il suffit de remarquer que $\Im(T^m z) = \Im(z)$. Ainsi puisque $\sigma^{-1}\mathrm{Stab}_{\Gamma(1)}(\infty)\sigma \subset \mathrm{Stab}_{\Gamma(1)}(z_0)$ on a

$$V' \cap \gamma V' \neq \emptyset \Leftrightarrow \gamma \in \Gamma_{z_0}$$

Puisque $\sigma\Gamma_{z_0}\sigma^{-1} \subset \left\{\pm T^{hm}, m \in \mathbb{Z}\right\}$, V' est stable sous l'action de Γ_{z_0} et V est stable sous l'action de $\sigma\Gamma_{z_0}\sigma^{-1}$. Comme dans la démonstration de la proposition 3.1.1, U_a est

homéomorphe via η_1 à Γ_{z_0}/V' qui est homéomorphe à $\sigma\Gamma_{z_0}\sigma^{-1}/V$ via η_2. On considère maintenant l'application

$$\begin{aligned} \eta : V &\longrightarrow D(0, e^{-4\pi/h}) \\ z &\longrightarrow \begin{cases} \exp(2i\pi z/h) & z \neq \infty \\ 0 & z = \infty \end{cases} \end{aligned}$$

Alors η est surjective et $\eta(\sigma\gamma_{z_0}\sigma^{-1}z) = \eta(z)$ si $\gamma_{z_0} \in \Gamma_{z_0}$, donc η induit une application $\eta_3 : \sigma\Gamma_{z_0}\sigma^{-1}/V \longrightarrow D(0, e^{-4\pi/h})$. De plus η_3 est injective et η est continue et ouverte pour la topologie de $\mathbb{H}^\star$ donc η_3 définit un homéomorphisme et on alors $\eta_a = \eta_3 \circ \eta_2 \circ \eta_1$ est un homéomorphisme. □

Proposition 3.3.6. *L'ensemble $\mathcal{B} = \mathcal{A} \cup \{\eta_a, a \in \pi_\Gamma(\{cusps\})\}$ est un atlas sur $X(\Gamma)$.*

Démonstration. D'après la proposition 3.2.6 il reste à montrer que chaque cartes de $\mathcal{B}$ qui ne sont pas dans $\mathcal{A}$ sont compatibles entre elles et avec chaque cartes de $\mathcal{A}$ (cf[5]). □

Proposition 3.3.7. *Soit $\pi_\Gamma : \mathbb{H}^\star \to X(\Gamma)$ l'application quotient qui à un élément de $\mathbb{H}^\star$ associe son orbite sous Γ, alors π_Γ est holomorphe sur l'ouvert $\mathbb{H}$.*

Démonstration. Soit $z_0 \in \mathbb{H}$ si $\Gamma_{z_0} \subset Z(\Gamma)$ alors il existe un voisinage V de z_0 et une carte $\psi : \pi_\Gamma(V) \to V$ tel que $\psi \circ \pi_\Gamma(z) = z$ pour tout z dans V. Ainsi π_Γ est holomorphe en z_0. De même si z_0 est un point elliptique alors il existe une carte $\phi : U \to V$ avec $U \subset \pi_\Gamma(V)$ tel que $\phi \circ \pi_\Gamma(z) = (\lambda(z))^m$ et $z \mapsto (\lambda(z))^m$ est holomorphe en z_0. □

Remarque 3.3.1. *Puisque $z \mapsto \begin{cases} \exp(2i\pi\sigma z/h) & z \neq z_0 \\ 0 & z = z_0 \end{cases}$ n'est pas holomorphe en z_0, l'application π_Γ n'est pas holomorphe sur les cusps.*

Proposition 3.3.8. *Soit $z \in \mathbb{H}$, Si z est $\Gamma(1)$-équivalent à i alors $mult_{\pi_{\Gamma(1)}}(z) = 2$, si z est $\Gamma(1)$-équivalent à ρ alors $mult_{\pi_{\Gamma(1)}}(z) = 3$ sinon $mult_{\pi_{\Gamma(1)}}(z) = 1$.*

Démonstration. Par définition de la structure complexe sur $Y(\Gamma)$, il existe une carte ϕ centrée en $\pi_{\Gamma(1)}(z)$ tel que sur un voisinage de z on puisse écrire $\phi \circ \pi_{\Gamma(1)}(\omega) = (\lambda(w))^m$, avec $m = 2$ si z est $\Gamma(1)$-équivalent à i et $m = 3$ si z est $\Gamma(1)$-équivalent à ρ, et $\phi \circ \pi_{\Gamma(1)}(\omega) = \omega$ si z n'est pas elliptique. □

Proposition 3.3.9. *Soit $z \in \mathbb{H}$ un point $\Gamma(1)$-elliptique, sont équivalents :*

i) z est Γ-elliptique
ii)$\Gamma_z \neq Z(\Gamma)$
iii) $mult_{\pi_\Gamma}(z) \neq 1$

Démonstration. Montrons que *i)* $\Leftrightarrow$ *ii)*. La matrice $\pm I$ n'est pas elliptique d'où la première implication, maintenant si $\Gamma_z \neq Z(\Gamma)$ alors il existe $\gamma \in \Gamma, \gamma \neq \pm I$ tel que $\gamma z = z$. Si z est $\Gamma(1)$-équivalent à i alors il existe $\gamma_1 \in \Gamma(1)$ tel que $\gamma_1 i = z$ et donc $\gamma_1^{-1}\gamma\gamma_1 \in Stab_{\Gamma(1)}(i) - \{\pm I\} = \{\pm S\}$. Puisque $Tr(\gamma) = Tr(\gamma_1^{-1}\gamma\gamma_1)$ et $|Tr(\pm S)| < 2$, γ est elliptique. De même si z est $\Gamma(1)$-équivalent à ρ puisque $Stab_{\Gamma(1)}(\rho) \setminus \{\pm I\} = \{\pm TS, \pm(TS)^2\}$.

Montrons maintenant que *ii)* $\Leftrightarrow$ *iii)*. Si $\Gamma_z = Z(\Gamma)$ alors par définition de la structure complexe sur $X(\Gamma)$ il existe une carte (U, φ) avec $\pi_\Gamma(z) \in U$ tel que sur un voisinage de z on puisse écrire $\varphi \circ \pi_\Gamma \circ Id_{\mathbb{C}}(\omega) = \omega$ donc $\text{mult}_{\pi_\Gamma}(z) = 1$. Maintenant si $\Gamma_z \neq Z(\Gamma)$ alors z est Γ-elliptique et par définition de la structure complexe sur $X(\Gamma)$ il existe une carte (U, φ) avec $\pi_\Gamma(z) \in U$ telle que sur un voisinage de z on puisse écrire

$$\varphi \circ \pi_\Gamma(\omega) = (\frac{w - z}{w - \bar{z}})^m$$

avec $m = 2$ ou $m = 3$, donc $\text{mult}_{\pi_\Gamma}(z) = m \neq 1$. □

4 Genre des courbes modulaires $X(\Gamma)$

4.1 Genre d'une surface de Riemann et triangulation

Dans ce qui suit X désignera une surface de Riemann compacte.

Proposition 4.1.1 (cf [4])**.** *Tout surface de Riemann compacte est homéomorphe à un tore à g trous, $g \geq 0$ étant unique.*

Définition 4.1.1. *On appelle genre d'une surface de Riemann compacte l'entier g.*

Définition 4.1.2. *Une triangulation de X est une décomposition de X en sous-ensembles fermés qui sont chacun homéomorphes à un triangle tels que deux triangles sont soit disjoints soit s'intersectent en un seul coté ou bien en un seul sommet.*

Définition 4.1.3. *Soit X une surface de Riemann compacte avec une triangulation qui comporte V sommets, E cotés et F et faces. On appelle caractéristique d'Euler le nombre $\chi(X) = V - E + F$.*

Proposition 4.1.2 (cf[4] p.51)**.** *La caractéristique d'Euler ne dépend pas de la triangulation choisie et l'on a $\chi(X) = 2 - 2g$.*

4.2 Calcul du genre de la surface $X(\Gamma(1))$

Proposition 4.2.1. *La surface $X(\Gamma(1))$ est de genre nul.*

Démonstration. On calcule le genre g de $X(\Gamma(1))$ par triangulation. D'après la proposition 3.3.2, l'ensemble

$$D \cup \{z \in \mathbb{C}, \Re z = 1/2, \Im z \geq \Im \rho\} \cup \{z \in \mathbb{C}, |z| = 1, 0 \leq \Re z \leq \Re \rho, \Im z > 0\} \cup \{\infty\}$$

est homéomorphe via $\pi_{\Gamma(1)}$ à $X(\Gamma(1))$ où D est le domaine fondamental de $\Gamma(1)$ sur $\mathbb{H}$ donc $X(\Gamma(1))$ est homéomorphe à la surface S obtenue par recollement, symétriquement par rapport à l'axe imaginaire, des cotés opposés b et des cotés a de la figure 2. On peut trianguler cette surface en se donnant un point $z_0 \in D,\ 0 < \Re(z_0) < 1/2$ et en la décomposant en quatre triangles (cf figure 2) :

Triangle 1 : $(i, i\infty, \rho)$
Triangle 2 : $(i, i\infty, z_0)$
Triangle 3 : (i, z_0, ρ)
Triangle 4 : $(i\infty, z_0, \rho)$

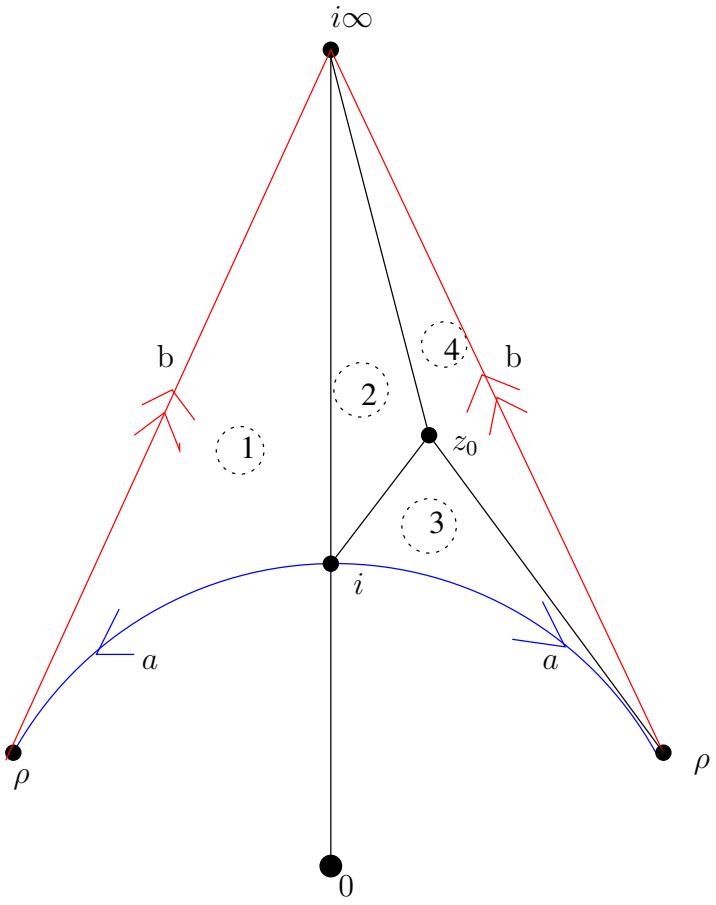


FIGURE 2 –

On a alors $2-2g=\chi(S)=4-6+4=2$ donc $g=0$.

□

4.3 Formule sur le genre de la surface $X(\Gamma)$

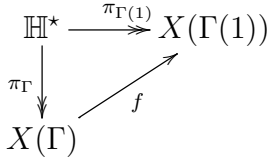
Proposition 4.3.1. *Soit Γ un sous-groupe de $\Gamma(1)$ d'indice fini m. On note $\overline{\Gamma(1)} = \frac{\Gamma(1)}{\{\pm I\}}$ et $\overline{\Gamma}$ l'image de Γ dans $\overline{\Gamma(1)}$, alors l'indice $\left[\overline{\Gamma(1)} : \overline{\Gamma}\right]$ est égal à m si $-I \in \Gamma$ et $m/2$ sinon.*

Démonstration. On note $M = \{\pm I\}$ et ρ_M la projection canonique de $\Gamma(1)$ dans M et $\overline{\Gamma}\backslash\overline{\Gamma(1)}$ l'ensemble des classes à droite de $\overline{\Gamma(1)}$ suivant le sous-groupe $\overline{\Gamma}$. On considère l'ensemble $E = \{M\Gamma\gamma, \gamma \in \Gamma(1)\}$ et l'application

$$\begin{aligned} f : \overline{\Gamma}\backslash\overline{\Gamma(1)} &\to E \\ \overline{\Gamma}\rho_M(\gamma) &\mapsto M\Gamma\gamma \end{aligned}$$

Puisque $M\Gamma\gamma_1 = M\Gamma\gamma_2$ si et seulement si $\Gamma\gamma_1 = \pm\Gamma\gamma_2$, f est bien définie et bijective. Le sous groupe Γ est d'indice fini m donc on peut écrire $\Gamma(1) = \bigsqcup_{i=1}^{m} \Gamma\gamma_i$ avec $\gamma_i \in \Gamma(1)$, on a alors $E = \{M\Gamma\gamma_i, 1 \leq i \leq m\}$. Ainsi l'indice $\left[\overline{\Gamma(1)} : \overline{\Gamma}\right]$ est fini et est égal au cardinal de E. Si $-I \in \Gamma$ alors $M\Gamma\gamma_1 = M\Gamma\gamma_2$ si et seulement si $\Gamma\gamma_1 = \Gamma\gamma_2$ donc Card $E = m$. Maintenant supposons que $-I$ n'appartient pas à Γ on a alors $\Gamma\gamma_i \cap \Gamma(-\gamma_i) = \emptyset$ donc chaque γ_i et son opposé représentent deux classes distinctes. Si on fixe $1 \leq i \leq m$ et qu'on se donne un $1 \leq j \leq m$ avec $j \neq i$ et tel que $\Gamma\gamma_j \neq \Gamma(-\gamma_i)$ alors $\Gamma(-\gamma_j) \notin \{\Gamma\gamma_i, \Gamma(-\gamma_i)\}$. Ainsi m est pair et en réindexant les γ_i on peut écrire $\Gamma(1) = \bigsqcup_{i=1}^{m/2} \Gamma\gamma_i \sqcup \Gamma(-\gamma_i)$. Puisque $M\Gamma\gamma_1 = M\Gamma\gamma_2$ si et seulement si $\Gamma\gamma_1 = \pm\Gamma\gamma_2$, Card $E = m/2$. □

Soit $\pi_{\Gamma(1)}$ (resp π_Γ) l'application quotient qui à un élément de $\mathbb{H}^\star$ associe son orbite sous $\Gamma(1)$ (resp Γ). D'après le théorème de factorisation il existe une unique application $f : X(\Gamma) \to X(\Gamma(1))$ telle que le diagramme suivant commute :



On a alors $\forall z \in \mathbb{H}^\star$, $f(\bar{z}^\Gamma) = \bar{z}^{\Gamma(1)}$ en particulier z est une pointe si et seulement si $f(\bar{z}^\Gamma) = \bar{\infty}$ (cf proposition 3.3.2).

Proposition 4.3.2. *Soit Γ un sous-groupe de $\Gamma(1)$ d'indice fini m. L'application quotient $f : X(\Gamma) \to X(\Gamma(1))$ est non constante et holomorphe.*

Démonstration. L'action de $\Gamma(1)$ sur $\mathbb{H}^\star$ n'est pas transitive donc f n'est pas constante. Soit $z_0 \in \mathbb{H}$, on pose $a = \pi_\Gamma(z_0)$ et $b = \pi_{\Gamma(1)}(z_0)$ supposons que z_0 n'est pas Γ-elliptique alors si z_0 n'est pas $\Gamma(1)$-elliptique il existe une carte ψ_b de $X(\Gamma(1))$ et ψ_a de $X(\Gamma)$ tel que sur un voisinage de z_0 on puisse écrire $\psi_b \circ f \circ \psi_a^{-1}(z) = z$ et si z_0 est $\Gamma(1)$-elliptique on pourra écrire $\phi_b \circ f \circ \psi_a^{-1}(z) = (\lambda(z))^m$. De même si z_0 est Γ-elliptique on pourra écrire sur un voisinage de 0, $\phi_b \circ f \circ \phi_a^{-1}(z) = z$. Enfin si z_0 est une pointe on pourra écrire $\eta_b \circ f \circ \eta_a^{-1}(z) = z^h$. □

On a vu que π_Γ n'est pas holomorphe sur les pointes (cf remarque 3.3.1) seulement puisque f est holomorphe sur $X(\Gamma)$ on peut parler de multiplicité de f en tout point de $X(\Gamma)$. La proposition suivante exprime la multiplicité de f en fonction des multiplicités de $\pi_{\Gamma(1)}$ et π_Γ sur les points qui ne sont pas des cusps.

Proposition 4.3.3. *Soit Γ un sous-groupe de $\Gamma(1)$ d'indice fini m, on a la formule*

$$\forall z \in \mathbb{H},\ mult_{\pi_{\Gamma(1)}}(z) = mult_f(\bar{z}^\Gamma) \times mult_{\pi_\Gamma}(z)$$

Démonstration. D'après la proposition 3.3.7 π_Γ est holomorphe sur l'ouvert $\mathbb{H}$, f est holomorphe sur $\pi_\Gamma(\mathbb{H})$ qui est ouvert car $\pi_\Gamma^{-1}(\pi_\Gamma(\mathbb{H})) = \mathbb{H}$ et $f \circ \pi_\Gamma = \pi_{\Gamma(1)}$ donc d'après la proposition 2.1.2 on a la formule $\forall z \in \mathbb{H}$, $\mathrm{mult}_{\pi_{\Gamma(1)}}(z) = \mathrm{mult}_f(\bar{z}^\Gamma) \times \mathrm{mult}_{\pi_\Gamma}(z)$. □

Théorème 4.3.1. *Soit Γ un sous-groupe de $\Gamma(1)$ d'indice fini m. On note*

$\mu_2 =$ *le nombre de points Γ-elliptiques, inéquivalents et de multiplicité 2 pour π_Γ*
$\mu_3 =$ *le nombre de points Γ-elliptiques, inéquivalents et de multiplicité 3 pour π_Γ*
$\mu_\infty =$ *le nombre de cusp Γ-inéquivalents.*

Alors le genre de $X(\Gamma)$ est donné par

$$g = \begin{cases} 1 + m/12 - \mu_2/4 - \mu_3/3 - \mu_\infty/2 & si - I \in \Gamma \\ 1 + m/24 - \mu_2/4 - \mu_3/3 - \mu_\infty/2 & sinon \end{cases}$$

Démonstration. En utilisant la formule de Riemann-Hurwitz (cf.[4] p.52) avec l'application quotient $f : X(\Gamma) \to X(\Gamma(1))$ on a

$$g(X(\Gamma)) = g(X(\Gamma(1))) + 1 - \deg(f) + \frac{1}{2} \sum_{P \in X(\Gamma)} (\mathrm{mult}_f(P) - 1)$$

La surface $X(\Gamma(1))$ est de genre 0 donc

$$g(X(\Gamma)) = 1 - \deg(f) + \frac{1}{2} \sum_{P \in X(\Gamma)} (\mathrm{mult}_f(P) - 1)$$

Calculons maintenant le dernier terme de cette somme :

$$\begin{aligned} \sum_{P \in X(\Gamma)} (\mathrm{mult}_f(P) - 1) &= \sum_{P \in \pi_\Gamma(\mathbb{H})} (\mathrm{mult}_f(P) - 1) + \sum_{P \in \pi_\Gamma(\{\mathrm{cusp}\})} (\mathrm{mult}_f(P) - 1) \\ &= \sum_{P \in \pi_\Gamma(\mathbb{H})} (\mathrm{mult}_f(P) - 1) + \sum_{P \in f^{-1}(\infty)} \mathrm{mult}_f(P) - \mathrm{Card}(\pi_\Gamma(\{\mathrm{cusp}\})) \\ &= \sum_{P \in \pi_\Gamma(\mathbb{H})} (\mathrm{mult}_f(P) - 1) + \deg(f) - \mu_\infty \end{aligned}$$

Soit $z \in \mathbb{H}$ qui n'est pas un point $\Gamma(1)$-elliptique, alors d'après la proposition 3.3.8 $\mathrm{mult}_{\pi_{\Gamma(1)}}(z) = 1$ ce qui implique d'après la proposition 4.3.3 que $\mathrm{mult}_f(\bar{z}^\Gamma) = 1$. Ainsi $\sum_{P \in \pi_\Gamma(\mathbb{H})}(\mathrm{mult}_f(P) - 1) = \sum_{P \in \pi_\Gamma(\{\text{points } \Gamma(1)\text{-elliptique}\})}(\mathrm{mult}_f(P) - 1)$.

D'après la proposition 3.1.4, $z \in \mathbb{H}$ est un point $\Gamma(1)$-elliptique $\Leftrightarrow \bar{z}^{\Gamma(1)} \in \left\{\pi_{\Gamma(1)}(i), \pi_{\Gamma(1)}(\rho)\right\}$, donc

$$\sum_{P \in \pi_\Gamma(\{\text{points } \Gamma(1)\text{-elliptique}\})} (\text{mult}_f(P) - 1) = \sum_{P \in f^{-1}(\bar{i})} (\text{mult}_f(P) - 1) + \sum_{P \in f^{-1}(\bar{\rho})} (\text{mult}_f(P) - 1)$$

Si $\bar{z}^{\Gamma(1)} = \bar{i}^{\Gamma(1)}$ alors $\text{mult}_{\pi_{\Gamma(1)}}(z) = \text{mult}_{\pi_{\Gamma(1)}}(i) = 2$ donc d'après la proposition 4.3.3 soit $\text{mult}_f(\bar{z}^\Gamma) = 1$ et $\text{mult}_{\pi_\Gamma}(z) = 2$, soit $\text{mult}_f(\bar{z}^\Gamma) = 2$ et $\text{mult}_{\pi_\Gamma}(z) = 1$, il s'ensuit d'après la proposition 3.3.9 que

$$f^{-1}(\bar{i}) = f^{-1}(\bar{i}) \cap [\pi_\Gamma(\{z \in \mathbb{H},\ \text{mult}_{\pi_\Gamma}(z) = 2\}) \sqcup \pi_\Gamma(\{z \in \mathbb{H},\ \text{mult}_{\pi_\Gamma}(z) = 1\})]$$

D'après la proposition 3.3.9, un point de multiplicité 2 pour π_Γ est Γ-elliptique donc il y a μ_2 points qui vérifient le premier cas. Ainsi

$$\begin{aligned}\deg(f) &=^{\text{def}} \sum_{P \in f^{-1}(\bar{i})} \text{mult}_f(P) \\ &= \mu_2 + 2 \times \text{Card}(\left\{P \in f^{-1}(\bar{i}), \text{mult}_f(P) = 2\right\})\end{aligned}$$

Ainsi

$$\begin{aligned}\sum_{P \in f^{-1}(\bar{i})} (\text{mult}_f(P) - 1) &= (2-1) \times \text{Card}(\left\{P \in f^{-1}(\bar{i}), \text{mult}_f(P) = 2\right\}) \\ &= (\deg(f) - \mu_2)/2\end{aligned}$$

De même si $\bar{z}^{\Gamma(1)} = \bar{\rho}^{\Gamma(1)}$, comme $\text{mult}_{\pi_{\Gamma(1)}}(\rho) = 3$, on a

$$\sum_{P \in f^{-1}(\bar{\rho})} (\text{mult}_f(P) - 1) = (3-1) \times ((\deg(f) - \mu_3)/3) = \frac{2}{3}(\deg(f) - \mu_3)$$

En résumé

$$\begin{aligned}g &= 1 - \deg(f) + \frac{1}{2}\left[\frac{1}{2}(\deg(f) - \mu_2) + \frac{2}{3}(\deg(f) - \mu_3) + \deg(f) - \mu_\infty\right] \\ &= 1 + \deg(f)/12 - \mu_2/4 - \mu_3/3 - \mu_\infty/2\end{aligned}$$

On fixe $z_0 \in \mathbb{H}$ un point qui n'est pas $\Gamma(1)$-elliptique ce qui implique que $\forall \bar{z}^\Gamma \in f^{-1}(\bar{z_0})$, $\text{mult}_f(\bar{z}^\Gamma) = 1$. Ainsi $\deg(f) = \text{Card}(f^{-1}(\bar{z_0}))$. On note $M = \{\pm I\}$ et on considère l'application $\tilde{g} : \frac{\Gamma(1)}{M} \to f^{-1}(\bar{z_0})$ induite par la surjection $g : \Gamma(1) \to f^{-1}(\bar{z_0})$ telle que $g(\gamma) = \pi_\Gamma(\gamma z_0)$. On a le diagramme suivant où ρ_M est la projection canonique de $\Gamma(1)$ dans $\frac{\Gamma(1)}{M}$:

$$\begin{array}{ccc} \Gamma(1) & \xrightarrow{g} & f^{-1}(\bar{z_0}) \\ {\scriptstyle \rho_M}\downarrow & \nearrow_{\tilde{g}} & \\ \frac{\Gamma(1)}{M} & & \end{array}$$

On note maintenant $\overline{\Gamma(1)} = \frac{\Gamma(1)}{M}$, $\overline{\Gamma} = \rho_M(\Gamma)$ et on considère $\overline{\Gamma}\backslash\overline{\Gamma(1)}$ l'ensemble des classes à droite de $\overline{\Gamma(1)}$ suivant le sous-groupe $\overline{\Gamma}$ et on note $\bar{m}$ son indice. Puisque

$g(\gamma_1) = g(\gamma_2)$ si $\gamma_2 \in \pm\Gamma\gamma_1$ on peut considérer l'application $\hat{g} : \overline{\Gamma}\backslash\overline{\Gamma(1)} \to f^{-1}(\bar{z_0})$ telle que $\hat{g}(\overline{\Gamma}\rho_M(\gamma_1)) = \tilde{g}(\rho_M(\gamma_1))$. Elle est surjective puisque $\tilde{g}$ est surjective et si $\pi_\Gamma(\gamma_1 z_0) = \pi_\Gamma(\gamma_2 z_0)$ dans $f^{-1}(\bar{z_0})$ alors il existe $\gamma \in \Gamma$ tel que $\gamma_2 z_0 = \gamma(\gamma_1 z_0) = \gamma\gamma_1\ z_0$ donc $z_0 = \gamma_2^{-1}\gamma\gamma_1\ z_0$ c'est à dire $\gamma_2^{-1}\gamma\gamma_1 \in \mathrm{Stab}_{\Gamma(1)}(z_0)$ donc $\gamma_2^{-1}\gamma\gamma_1 = \pm I$. Ainsi $\rho_M(\gamma_2) = \rho_M(\gamma\gamma_1) = \rho_M(\gamma)\rho_M(\gamma_1)$ donc $\overline{\Gamma}\rho_M(\gamma_1) = \overline{\Gamma}\rho_M(\gamma_2)$ et $\hat{g}$ est bijective ce qui implique que $\bar{m} = \mathrm{Card}(f^{-1}(\bar{z_0})) = \deg(f)$. D'après la proposition 4.3.1 $\bar{m}$ est égal à m si $-I$ appartient à Γ et à $m/2$ sinon d'où le résultat. □

5 Application aux surfaces $X(N)$ et $X_0(N)$

Dans ce qui suit, on notera φ l'indicatrice d'Euler et $a \wedge b$ le PGCD de a et b.

5.1 Sous-groupes de congruence de $SL_2(\mathbb{Z})$

Définition 5.1.1. *Soit N un entier plus grand que 1, on appelle N-ième sous groupe principale de congruence le sous groupe, noté $\Gamma(N)$, de $\Gamma(1)$ formé des classes de matrices congrues modulo N à la matrice identité, c'est à dire l'ensemble*

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1), a \equiv d \equiv 1 \mod (N), c \equiv b \equiv 0 \mod (N) \right\}$$

Proposition 5.1.1. *Le groupe $SL_2(\mathbb{Z}/N\mathbb{Z})$ est fini de cardinal $N^3 \prod_{p|N} \frac{p^2-1}{p^2}$.*

Démonstration. Pour les détails de la démonstration on pourra regarder [5] p.105 : En écrivant $N = \prod p_i^{r_i}$ il suffit de prouver les quatre résultats suivants :

1) $GL_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod GL_2(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$
2) $|GL_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p)$
3) $|GL_2(\mathbb{Z}/p^r\mathbb{Z})| = (p^{r-1})^4(p^2-1)(p^2-p)$
4) $|GL_2(\mathbb{Z}/p^r\mathbb{Z})| = \varphi(p^r)\,|SL_2(\mathbb{Z}/p\mathbb{Z})|$

□

Proposition 5.1.2. *Soit $N > 1$, le sous-groupe principale de congruence $\Gamma(N)$ est normal et d'indice fini égal à $N^3 \prod_{p|N} \frac{p^2-1}{p^2}$.*

Démonstration. On vérifie facilement que $\forall \gamma_N \in \Gamma(N), \forall \gamma \in \Gamma(1), \gamma_N\gamma\gamma_N^{-1} \in \Gamma(N)$. On considère maintenant l'application

$$\lambda_N : \Gamma(1) \to SL_2(\mathbb{Z}/N\mathbb{Z})$$
$$\gamma \mapsto \bar{\gamma}^N$$

alors λ_N est un morphisme de groupe de noyau $\Gamma(N)$. Montrons qu'il est surjectif, on se donne $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ tel que $\det A \equiv 1[N]$. Il existe alors $k \in \mathbb{Z}$ tel que

$ad-bc-Nk=1$. D'après le théorème chinois il existe $n\in\mathbb{Z}$ tel que pour tout p premier qui divise c mais pas N on ait $n\equiv(1-d)N^{-1} \mod(p)$ et pour p qui divise c et N on ait $n\equiv 0 \mod(p)$. Il en découle que $c\wedge d+nN=1$, et en remplaçant d par $d+nN$ on peut supposer que $c\wedge d=1$. Il existe alors $u,v\in\mathbb{Z}$ tel que $k=uc+vd$, on pose maintenant $B=\begin{pmatrix} a-vN & b+uN \\ c & d\end{pmatrix}$. On a alors $\det B=ad-bc-N(vd+cu)=1$ donc $B\in\Gamma(1)$ et $\lambda_N(B)=A$. Ainsi $\frac{\Gamma(1)}{\Gamma(N)}\cong SL_2(\mathbb{Z}/N\mathbb{Z})$ et $|SL_2(\mathbb{Z}/N\mathbb{Z})|=N^3\prod_{p|N}\frac{p^2-1}{p^2}$ donc $[\Gamma(1):\Gamma(N)]=N^3\prod_{p|N}\frac{p^2-1}{p^2}$. □

Définition 5.1.2. *On appelle sous-groupe de congruence un sous-groupe de* $\Gamma(1)$ *qui contient le sous-groupe* $\Gamma(N)$ *pour au moins un entier* N.

Proposition 5.1.3. *L'ensemble* $\Gamma_0(N)=\left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\Gamma(1), c\equiv 0 \mod(N)\right\}$ *est un sous-groupe de congruence d'indice fini égal à* $N\prod_{p|N}\frac{p+1}{p}$.

Démonstration. Il est claire que $\Gamma(N)\subset\Gamma_0(N)$, considérons l'application

$$\begin{aligned} f:\Gamma_0(N)\backslash\Gamma(1)&\longrightarrow\lambda_N(\Gamma_0(N))\backslash SL_2(\mathbb{Z}/N\mathbb{Z})\\ \Gamma_0(N)\gamma&\longmapsto\lambda_N(\Gamma_0(N))\lambda_N(\gamma)\end{aligned}$$

qui provient du diagramme commutatif suivant :

$$\begin{array}{ccc}\Gamma(1) & \xrightarrow{\lambda_N} & SL_2(\mathbb{Z}/N\mathbb{Z})\\ \downarrow{\scriptstyle \pi_{\Gamma_0(N)}} & & \downarrow{\scriptstyle \pi_{\lambda(\Gamma_0(N))}}\\ \Gamma_0(N)\backslash\Gamma(1) & \xrightarrow{f} & \lambda_N(\Gamma_0(N))\backslash SL_2(\mathbb{Z}/N\mathbb{Z})\end{array}$$

f est bien défine car si $\gamma_1\in\Gamma_0(N)\gamma_2$ alors, puisque λ_N est un morphisme de groupe, $f(\Gamma_0(N)\gamma_1)=f(\Gamma_0(N)\gamma_2)$. L'application f est surjective car λ_N est surjective et si $f(\Gamma_0(N)\gamma_1)=f(\Gamma_0(N)\gamma_2)$ alors $\lambda_N(\gamma_1)=\lambda_N(\gamma_0)\lambda_N(\gamma_2)=\lambda_N(\gamma_0\gamma_2)$ donc $\gamma_1(\gamma_0\gamma_2)^{-1}\in\ker\lambda_N\subset\Gamma_0(N)$. Ainsi $\Gamma_0(N)\gamma_1=\Gamma_0(N)\gamma_2$ et f est bijective donc

$$[\Gamma(1):\Gamma_0(N)]=[SL_2(\mathbb{Z}/N\mathbb{Z}):\lambda_N(\Gamma_0(N))]=\frac{|SL_2(\mathbb{Z}/N\mathbb{Z})|}{|\lambda_N(\Gamma_0(N))|}.$$

Il est facile de voir que $\lambda_N(\Gamma_0(N))=\left\{\begin{pmatrix} a & b\\ 0 & a^{-1}\end{pmatrix}, a\in(\mathbb{Z}/N\mathbb{Z})^\times, b\in\mathbb{Z}/N\mathbb{Z}\right\}$ donc $|\lambda_N(\Gamma_0(N))|=N\varphi(N)=N\times N\prod_{p|N}\frac{p-1}{p}$. Ainsi

$$[\Gamma(1):\Gamma_0(N)]=\frac{N^3\prod_{p|N}\frac{p^2-1}{p^2}}{N^2\prod_{p|N}\frac{p-1}{p}}=N\prod_{p|N}\frac{p+1}{p}$$

□

On va maintenant essayer de trouver des représentants des classes à gauche de l'ensemble $\Gamma_0(N)\backslash\Gamma(1)$ qui serviront à déterminer le nombre de points elliptiques. Dans la suite p désigne un nombre premier et r un entier supérieur ou égal à 1.

Proposition 5.1.4. *Supposons que $N = p^r$ alors l'ensemble*

$$A_N = \{(c,d) \in \mathbb{N}^\star \times \mathbb{N}^\star, c \wedge d = 1, d|N, 0 < c \leq N/d\}$$

est fini de cardinal $p^r \dfrac{p+1}{p} = N \displaystyle\prod_{p|N} \frac{p+1}{p} = [\Gamma(1) : \Gamma_0(N)]$.

Démonstration. Pour $d|p^r$ fixé on a p^r possibilités pour c si $d = 1$ et si $d = p^i$ on a $\varphi(p^{r-i})$ possibilités pour c. Ainsi

$$|A_{p^r}| = p^r + \sum_{i=1}^{r} \varphi(p^{r-i}) = p^r + p^{r-1} = p^r \frac{p+1}{p}$$

□

Proposition 5.1.5. *Pour chaque couple (c,d) de A_{p^r} on fixe deux entiers a et b tels que $ad - bc = 1$, on a alors*

$$\Gamma(1) = \bigsqcup_{(c,d)\in A_{p^r}} \Gamma_0(p^r) \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \bigsqcup_{(c,d)\in A_{p^r}} \begin{pmatrix} d & b \\ c & a \end{pmatrix} \Gamma_0(p^r)$$

Démonstration. On va montrer que ces représentants sont inéquivalents par multiplication à gauche par des éléments de $\Gamma_0(p^r)$ puis que leur nombre est exactement l'indice de $\Gamma_0(p^r)$. Soit $(c,d) \in A_{p^r}$ et $(c',d') \in A_{p^r}$, supposons qu'il existe $\begin{pmatrix} \alpha & \beta \\ kp^r & \gamma \end{pmatrix} \in \Gamma_0(p^r)$ et $k \in \mathbb{Z}$ tels que

$$\begin{pmatrix} \alpha & \beta \\ kp^r & \gamma \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

on a alors $d' = kp^r b + \gamma d$ et $d = -kp^r b' + \alpha d'$ d'où $d|d'$ et $d'|d$ donc $d = d'$. On a également $c' = kp^r a + \gamma c$ donc on peut écrire

$$\begin{pmatrix} c' \\ d \end{pmatrix} = \begin{pmatrix} c' \\ d' \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} kp^r \\ \gamma \end{pmatrix}$$

d'où

$$\begin{pmatrix} kp^r \\ \gamma \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \begin{pmatrix} c' \\ d' \end{pmatrix} = \begin{pmatrix} dc' - cd' \\ -bc' + ad' \end{pmatrix} = \begin{pmatrix} dc' - cd \\ -bc' + ad \end{pmatrix}$$

Ainsi $c - c' = k(p^r/d)$ donc $c \equiv c' \mod (p^r/d)$ et puisque $0 < c, c' \leq p^r/d$ on a $c = c'$. De la même manière on montre que si $\begin{pmatrix} d' & b' \\ c' & a' \end{pmatrix} \in \begin{pmatrix} d & b \\ c & a \end{pmatrix} \Gamma_0(p^r)$ alors $(c,d) = (c',d')$. D'après le proposition précédente $|A_{p^r}| = [\Gamma(1) : \Gamma_0(p^r)]$ d'où le résultat. □

Remarque 5.1.1. *Les représentants définis plus haut sont aussi inéquivalents pour un entier $N > 0$ quelconque. Dans le Shimura [8] p.25 il est dit que $|A_N| = N \prod_{p|N} \frac{p+1}{p}$ et ainsi que la proposition précédente se généralise pour un entier $N > 0$ quelconque ce qui est faux car par exemple pour $N = 6$ on remarque que $|A_6| = 11$ mais que $[\Gamma(1) : \Gamma_0(6)] = 6 \prod_{p|6} \frac{p+1}{p} = 12$.*

Plutôt que d'essayer de corriger cette erreur et de trouver des représentants pour N quelconque on se contentera de supposer que N est une puissance d'un nombre premier puis on contournera le problème en utilisant la décomposition $N = \prod_i p_i^{r_i}$ (cf le résultat suivant et la démonstration de la proposition 5.3.3).

Proposition 5.1.6. *Soit $N = \prod_{i=1}^n p_i^{r_i}$, l'application*

$$\begin{aligned} \phi : \Gamma_0(N) \backslash \Gamma(1) &\longrightarrow \prod_{i=1}^n \Gamma_0(p_i^{r_i}) \backslash \Gamma(1) \\ \Gamma_0(N)\gamma &\longmapsto (\Gamma_0(p_1^{r_1})\gamma, \ \dots \ , \Gamma_0(p_n^{r_n})\gamma) \end{aligned}$$

est bijective

Démonstration. Puisque $\Gamma_0(N) \subset \Gamma_0(p_i^{r_i})$, l'application ϕ est bien définie. Supposons $\phi(\Gamma_0(N)\gamma_1) = \phi(\Gamma_0(N)\gamma_2)$ alors $\gamma_1\gamma_2^{-1} \in \cap_i \Gamma_0(p_i^{r_i}) = \Gamma_0(N)$ donc $\Gamma_0(N)\gamma_1 = \Gamma_0(N)\gamma_2$ et ϕ est injective. On a de plus

$$|\prod_{i=1}^n \Gamma_0(p_i^{r_i}) \backslash \Gamma(1)| = \prod_{i=1}^n [\Gamma(1) : \Gamma_0(p_i^{r_i})] = \prod_{i=1}^n p_i^{r_i} \frac{p_i + 1}{p_i} = [\Gamma(1) : \Gamma_0(N)]$$

donc ϕ est bijective. □

Dans la suite on notera $X(N)$ la surface $X(\Gamma(N))$ et $X_0(N)$ la surface $X(\Gamma_0(N))$.

5.2 Genre de la surface $X(N)$

Lemme 5.2.1. *Soit G un groupe agissant transitivement sur un ensemble X et H un sous-groupe normal de G d'indice fini. Soit $x_0 \in X$, on note $G_0 = Stab_G(x_0)$ et $H_0 = Stab_H(x_0)$, alors le nombre d'orbites de l'action de H sur X est $\dfrac{[G : H]}{[G_0 : H_0]}$.*

Démonstration. Puisque H est normal et d'indice fini dans G, H_0 est normal et d'indice fini dans G_0 (en effet $H_0 = G_0 \cap H$). On note $H\backslash X$ l'ensemble des orbites de l'action de H sur X, $\rho_H : G \longrightarrow \frac{G}{H}$ et $\rho_{H_0} : G_0 \longrightarrow \frac{G_0}{H_0}$ les projections canoniques. On a alors le diagramme suivant :

$$\begin{array}{ccc} G_0 & \xrightarrow{\rho_H} & \rho_H(G_0) \\ {\scriptstyle \rho_{H_0}}\downarrow & \nearrow_{\widetilde{\rho_H}} & \\ \frac{G_0}{H_0} & & \end{array}$$

Si $\widetilde{\rho_H}(g_0H_0) = \widetilde{\rho_H}(l_0H_0)$ alors $g_0H = l_0H$ donc $g_0l_0^{-1} \in H \cap G_0 = H_0$ et $g_0H_0 = l_0H_0$. Ainsi $\widetilde{\rho_H}$ est bijective et $\rho_H(G_0)$ est un groupe fini d'ordre $[G_0 : H_0]$. On note $\frac{G}{H}/\frac{G_0}{H_0}$ l'ensemble des classes à gauche de $\frac{G}{H}$ suivant le sous-groupe $\rho_H(G_0)$ et on considère l'application

$$\begin{aligned} f : \frac{G}{H}/\frac{G_0}{H_0} &\longrightarrow H\backslash X \\ (gH)\rho_H(G_0) &\mapsto \mathrm{orb}_H(gx_0) \end{aligned}$$

Montrons que f est bien définie et bijective. Elle est bien définie car si $(g_1H)\rho_H(G_0) = (g_2H)\rho_H(G_0)$ alors il existe $h \in H$ et $g_0 \in G_0$ tels que $g_2 = hg_1g_0$ on a alors $g_2x_0 = hg_1g_0x_0 = hg_1x_0 = h(g_1x_0)$ et ainsi $\mathrm{orb}_H(g_1x_0) = \mathrm{orb}_H(g_2x_0)$. Puisque G agit transitivement sur X, f est surjective. Enfin si $\mathrm{orb}_H(g_1x_0) = \mathrm{orb}_H(g_2x_0)$ alors il existe $h \in H$ tel que $g_1x_0 = hg_2x_0$ donc $g_0 = g_1^{-1}hg_2$ appartient à G_0 et, puisque H est normal, $g_2H = g_1g_0H = g_1Hg_0H$ d'où $(g_1H)\rho_H(G_0) = (g_2H)\rho_H(G_0)$ et f est injective. Ainsi d'après la formule des indices

$$|H\backslash X| = \frac{[G:H]}{|\rho_H(G_0)|} = \frac{[G:H]}{[G_0:H_0]}$$

□

Proposition 5.2.1. *On a* $g(X(N)) = \begin{cases} 0 & si\, N \leq 2 \\ 1 + N^2\dfrac{(N-6)}{24}\displaystyle\prod_{p|N}\frac{p^2-1}{p^2} & si\, N > 2 \end{cases}$

Démonstration. Montrons qu'il n'existe pas de point $\Gamma(N)$-elliptique, on aura alors $\mu_2 = \mu_3 = 0$. S'il existe $\gamma \in \Gamma(N)$ matrice elliptique avec $\gamma z = z$, $z \in \mathbb{H}$, alors d'après la proposition 3.1.4 z est $\Gamma(1)$-équivalent à i ou à ρ donc γ est conjuguée à une matrice du stabilisateur de i ou ρ or d'après la proposition 3.1.2 aucun élément différent de $\pm I$ de ces deux stabilisateurs n'appartient à $\Gamma(N)$ qui est un sous groupe normal donc $\gamma \notin \Gamma(N)$.
Déterminons maintenant le nombre μ_∞ de cusps $\Gamma(N)$-inéquivalents en utilisant le lemme 5.2.1. On prend $G = \frac{\Gamma(1)}{\{\pm I\}}$ et $H = \frac{\Gamma(N)}{\{\pm I\}}$ l'image de $\Gamma(N)$ dans G, $X = \{\text{cusp}\}$ et $x_0 = \infty$. Le groupe $\Gamma(1)$ agit transitivement sur X donc G agit transitivement sur X par l'action $\bar{g}.x = gx$. On note $G_\infty = \mathrm{Stab}_G(\infty)$ et $H_\infty = \mathrm{Stab}_H(\infty)$. Puisque que $\Gamma(N)$ est normal, H est normal, de plus d'après la proposition 4.3.1 H est d'indice fini.

Montrons que $[G_\infty : H_\infty] = N$, pour cela on pose $M = \{\pm I\}$ et $A_m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$. On sait déjà que $\mathrm{Stab}_{\Gamma(1)}(\infty) = \{\pm A_m, m \in \mathbb{Z}\}$ et donc $\mathrm{Stab}_{\Gamma(N)}(\infty) = \{\pm A_m, m \in \mathbb{Z}, N|m\}$. Maintenant si $\pm A_m \in \mathrm{Stab}_{\Gamma(1)}(\infty)$ alors il existe $0 \leq k \leq N-1$ tel que $\bar{k}^N = \bar{m}^N$ et l'on a $\pm A_m = A_k \pm A_{m-k}$ avec $\pm A_{m-k} \in \mathrm{Stab}_{\Gamma(N)}(\infty)$. De plus si $A_{k'} = A_k \pm A_m$ avec $\bar{m}^N = 0$ et $0 \leq k, k' \leq N-1$ alors $k' = k \pm m$ donc $k' = k$. Ainsi

$$\mathrm{Stab}_{\Gamma(1)}(\infty) = \bigsqcup_{k=0}^{N-1} A_k\, \mathrm{Stab}_{\Gamma(N)}(\infty)$$

Cette égalité modulo M donne

$$G_\infty = \bigsqcup_{k=0}^{N-1} (A_kM)H_\infty$$

et donc l'indice de H_∞ dans G_∞ est N. On a ainsi d'après le lemme 5.2.1

$$\mu_\infty = \frac{[G:H]}{[G_\infty:H_\infty]} = \frac{[G:H]}{N}$$

c'est à dire, puisque $[G : H]$ est égal à $[\Gamma(1) : \Gamma(N)]/2$ si $N > 2$ et $[\Gamma(1) : \Gamma(N)]$ sinon,

$$\mu_\infty = \begin{cases} 3 & \text{si } N = 2 \\ \dfrac{N^2}{2} \displaystyle\prod_{p|N} \dfrac{p^2-1}{p^2} & \text{si } N > 2 \end{cases}$$

On obtient alors le résultat en appliquant le théorème 4.3.1 .

□

On pourra se reporter à l'exemple 5.3.1 pour quelques valeurs de $g(X(N))$.

5.3 Genre de la surface $X_0(N)$

Soit p un nombre premier, on définit deux nombres ϵ_p et η_p de la manière suivante :

$$\epsilon_p = \begin{cases} 0 & \text{si } p \equiv 3 \mod (4) \\ 1 & \text{si } p = 2 \\ 2 & \text{si } p \equiv 1 \mod (4) \end{cases} \quad \text{et } \eta_p = \begin{cases} 0 & \text{si } p \equiv 2 \mod (3) \\ 1 & \text{si } p = 3 \\ 2 & \text{si } p \equiv 1 \mod (3) \end{cases}$$

Lemme 5.3.1. *Soit p un nombre premier impair, $r \in \mathbb{N}^\star$ et $a \in \mathbb{Z}$ tels que p ne divise pas a. Si a est un carré modulo p^m alors a est un carré modulo p^{2m}.*

Démonstration. Soit x une racine carrée de a modulo p^m alors $p^m | a - x^2$. Puisque p ne divise pas a, x est inversible dans $\mathbb{Z}/p^m\mathbb{Z}$, on peut donc poser $y = (2x)^{-1} \frac{a-x^2}{p^m}$ et $x' = x + yp^m$ alors $x'^2 = x^2 + 2xyp^m + y^2p^{2m} \equiv x^2 + 2xyp^m \equiv a \mod (p^{2m})$ donc a est un carré modulo p^{2m}. □

Lemme 5.3.2. *Soit p un nombre premier impair, $r \in \mathbb{N}^\star$ et $a \in \mathbb{Z}$ tels que p ne divise pas a. Le nombre de racine du polynôme $X^2 - a$ dans $\mathbb{Z}/p^r\mathbb{Z}$ est le même que dans $\mathbb{Z}/p\mathbb{Z}$. De plus ce polynôme n'admet aucune racine double dans $\mathbb{Z}/p^r\mathbb{Z}$ ni dans $\mathbb{Z}/p\mathbb{Z}$*

Démonstration. Si $X^2 - a$ avait une racine double x alors $(X^2 - a)'(x) = 0$ donc $2x = 0$ et puisque 2 est inversible $x = 0$ d'où $a = 0$ et $p|a$ ce qui est faux par hypothèse. Maintenant si a est un carré modulo p^r alors c'est un carré modulo p^s, pour tout $1 \leq s \leq r$ et si a est un carré modulo p alors d'après le lemme précédent c'est un carré modulo p^{2^k} pour tout $k \in \mathbb{Z}$. Puisqu'il existe k tel que $r \leq 2^k$, a est un carré modulo p^r. □

Proposition 5.3.1. *Soit r un entier supérieur ou égal à 1 alors, dans $\mathbb{Z}/p^r\mathbb{Z}$, le polynôme $X^2 + 1$ admet exactement ϵ_p racines si 4 ne divise pas p^r et 0 racine sinon. De plus si $p > 2$ le polynôme $X^2 + 3$ admet exactement η_p racines si 9 ne divise pas p^r et 0 racine sinon.*

Démonstration. Si $p > 2$ alors -1 est un carré modulo p si et seulement si $p = 1 \mod (4)$ (cf [6] p.75). D'après le lemme précédent $X^2 + 1$ n'a pas de racine double donc le nombre de racine dans $\mathbb{Z}/p\mathbb{Z}$ est ϵ_p qui est, d'après le lemme précédent, aussi le nombre de racine dans $\mathbb{Z}/p^r\mathbb{Z}$. Maintenant si $p = 2$, $X^2 + 1$ a une unique racine dans $\mathbb{Z}/p\mathbb{Z}$ qui est 1, et si $x^2 + 1 \equiv 0 \mod (2^r)$ alors $x^2 \equiv -1 \mod (4)$ et $x^2 \equiv 1 \mod (4)$ car $2|x - 1$ implique $4|(x + 1)(x - 1) = x^2 - 1$. Puisque $1 \neq -1 \mod (4)$, $X^2 + 1$ n'a pas de racine dans $\mathbb{Z}/2^r\mathbb{Z}$ si $r > 1$.

On s'intéresse maintenant au polynôme X^2+3. Si $p=3$ alors X^2+3 a une unique racine dans $\mathbb{Z}/3\mathbb{Z}$ qui est 0 et n'a aucune racine dans $\mathbb{Z}/3^r\mathbb{Z}$, $r>1$ car si $x^2+3\equiv 0 \mod (3^r)$ alors $x^2\equiv -3 \mod (9)$ et $x^2\equiv 0 \mod (9)$ en effet $x\equiv 0 \mod (3)$ implique $x^2\equiv 0 \mod (9)$ et $x^2+3\equiv 0 \mod (3^r)$ implique $x^2+3\equiv 0 \mod (3)$. Si $p>3$ alors d'après le théorème de réciprocité quadratique (cf [1] p.166) on a

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=\begin{cases} -\left(\frac{-1}{p}\right)\left(\frac{p}{3}\right) & \text{si } p=3 \mod (4) \\ \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right) & \text{sinon} \end{cases} =\left(\frac{p}{3}\right)$$

où pour un entier a et un nombre premier p

$$\left(\frac{a}{p}\right)=\begin{cases} 0 & \text{si } a=0 \\ 1 & \text{si } a \text{ est un carré dans } \mathbb{Z}/p\mathbb{Z} \\ -1 & \text{sinon} \end{cases}$$

est le symbole de Legendre. Ainsi, puisque p est un carré dans $\mathbb{Z}/3\mathbb{Z}$ si et seulement si $p\equiv 1 \mod (3)$ et que X^2+3 n'a pas de racine double, on a que le polynôme X^2+3 admet η_p racines dans $\mathbb{Z}/p\mathbb{Z}$ et aussi dans $\mathbb{Z}/p^r\mathbb{Z}$ d'après le lemme précédent. □

Proposition 5.3.2. *Soit r un entier supérieur ou égal à 1 alors, dans $\mathbb{Z}/p^r\mathbb{Z}$, le polynôme X^2-X+1 admet exactement η_p racines si 9 ne divise pas p^r et 0 racine sinon.*

Démonstration. Regardons en premier le cas $p=2$: le polynôme X^2-X+1 n'a pas de racine dans $\mathbb{Z}/2\mathbb{Z}$ ce qui implique qu'il n'en a pas non plus dans $\mathbb{Z}/2^r\mathbb{Z}$. Supposons $p>2$ alors le discriminant de X^2-X+1 est -3, on a donc

$$\begin{aligned} -3 \text{ est un carré dans } \mathbb{Z}/p^r\mathbb{Z} &\Leftrightarrow \exists x\in\mathbb{Z}/p^r\mathbb{Z} \text{ tel que } -3=x^2 \\ &\Leftrightarrow X^2-X+1=(X-2^{-1}(1+x))(X-2^{-1}(1-x)) \\ &\Leftrightarrow X^2-X+1=(X-x_1)(X-x_2) \\ &\Leftrightarrow X^2-X+1 \text{ a au moins une racine} \end{aligned}$$

Ainsi si $-3\neq 0$ est un carré dans $\mathbb{Z}/p^r\mathbb{Z}$ alors X^2-X+1 a deux racines distinctes, si $-3=0$ il a une unique racine double et si -3 n'est pas un carré il a aucune racine. Puisque $-3=0$ si et seulement si $p^r=3$ on obtient le résultat d'après la proposition précédente. □

Proposition 5.3.3. *Le nombre μ_2 de points $\Gamma_0(N)$-elliptiques, inéquivalents et de multiplicité 2 est donné par*

$$\mu_2=\begin{cases} 0 & si\ N\equiv 0 \mod (4) \\ \prod_{p|N}\epsilon_p & sinon \end{cases}$$

Démonstration. Supposons d'abord que $N=p^r$. On rappelle que (cf proposition 5.1.5)

$$\Gamma(1)=\bigsqcup_{(c,d)\in A_N}\Gamma_0(N)\begin{pmatrix} a & b \\ c & d\end{pmatrix} \text{ avec } A_N=\{(c,d)\in\mathbb{N}^\star\times\mathbb{N}^\star, c\wedge d=1, d|N, 0<c\leq N/d\}$$

a et b étant fixés pour chaque (c,d). On pose alors

$$\gamma_{(c,d)} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ et } E_2(N) = \{\text{points } \Gamma_0(N) \text{ -elliptiques, inéquivalents et de multiplicité } 2\}$$

Montrons que l'on a $E_2(N) = \left\{\gamma_{(c,1)}i, 0 < c \leq N, c^2+1 \equiv 0 \mod (N)\right\}$. Soit $z \in E_2$ alors il existe $\gamma_0 \in \Gamma_0(N)$ tel que $z = \gamma_0 z$ et, puisque z est en particulier $\Gamma(1)$-elliptique de multiplicité 2, $z = \gamma_1 i$ avec $\gamma_1 \in \Gamma(1)$, d'où $\gamma_1^{-1}\gamma_0\gamma_1 \in \mathrm{Stab}_{\Gamma(1)}(i)$ donc $\gamma_1^{-1}\gamma_0\gamma_1 \in \{\pm S\}$. Il existe $(c,d) \in A_N$ tel que $\gamma_1 \in \Gamma_0(N)\gamma_{(c,d)}$ donc $\gamma_{(c,d)} \pm S\gamma_{(c,d)}^{-1} \in \Gamma_0(N)$ c'est-à-dire

$$\begin{pmatrix} ac+bd & -(a^2+b^2) \\ c^2+d^2 & -(ac+bd) \end{pmatrix} \in \Gamma_0(N)$$

d'où

$$c^2 + d^2 \equiv 0 \mod (N)$$

Montrons que $d = 1$: Pour cela supposons qu'il existe un nombre premier p qui divise d alors $c^2 \equiv 0 \mod (p)$ donc $p|c$ impossible car $c \wedge d = 1$. On a donc $c^2+1 \equiv 0 \mod (N)$, $0 < c \leq N$ et $\gamma_{(c,d)} = \gamma_{(c,1)}$ donc $z \in \Gamma_0(N)\gamma_{(c,1)}i$ et z est $\Gamma_0(N)$-équivalent à $\gamma_{(c,1)}i$.
Inversement si $c^2 + 1 \equiv 0 \mod (N)$ alors

$$\gamma_{(c,1)}S\gamma_{(c,1)}^{-1} \in \Gamma_0(N) \text{ et } \gamma_{(c,1)}S\gamma_{(c,1)}^{-1}\gamma_{(c,1)}i = \gamma_{(c,1)}i$$

D'après la proposition 3.3.8 $\gamma_{(c,1)}i$ est de multiplicité 2 pour $\pi_{\Gamma(1)}$ donc d'après la proposition 4.3.3 $\gamma_{(c,1)}i$ est de multiplicité 1 ou 2 pour $\pi_{\Gamma_0(N)}$ mais $\gamma_{(c,1)}i$ est $\Gamma_0(N)$-elliptique donc d'après la proposition 3.3.9 sa multiplicité est différente de 1. Maintenant si $\gamma_{(c_1,1)}i = \gamma_0\gamma_{(c_2,1)}i$ avec $0 < c_1, c_2 \leq N$ tel que $c_1^2 + 1 \equiv 0 \mod (N)$ et $c_2^2 + 1 \equiv 0 \mod (N)$ alors $\gamma_{(c,1)}^{-1}\gamma_0\gamma_{(c_2,1)} \in \mathrm{Stab}_{\Gamma(1)}(i)$ et donc $c_1 \equiv c_2 \mod (N)$ ou $c_1c_2 + 1 \equiv 0 \mod (N)$. On obtient alors dans les deux cas $c_1 \equiv c_2 \mod (N)$ et donc $c_1 = c_2$ et ainsi les points $\gamma_{(c,1)}i$ sont inéquivalents sous $\Gamma_0(N)$.
Ainsi d'après la proposition 5.3.1 on a :

$$\mu_2 = |E_2(N)| = |\left\{c \in \mathbb{N}^\star, c \leq N, c^2+1 \equiv 0 \mod (N)\right\}| = \begin{cases} 0 & \text{si } p^r \equiv 0 \mod (4) \\ \epsilon_p & \text{sinon} \end{cases}$$

On va maintenant se ramener au cas où N est quelconque pour cela on suppose que $N = \prod_{i=1}^{n} p_i^{r_i}$ et on pose

$$\begin{aligned} f : E_2(N) &\longrightarrow \prod_{i=1}^{n} E_2(p_i^{r_i}) \\ \gamma i &\longmapsto (\gamma_1 i, \ \ldots \ , \gamma_n i) \end{aligned}$$

où $\gamma_i = \gamma_{(c_i,d_i)}$ est le représentant de la classe de γ modulo $\Gamma_0(p_i^{r_i})$. Vérifions que f est bien définie et bijective : si $\gamma_0\gamma i = \gamma i$ avec $\gamma_0 \in \Gamma_0(N) \subset \Gamma_0(p_i^{r_i})$ alors si $\gamma = M_i\gamma_i$ avec $M_i \in \Gamma_0(p_i^{r_i})$ on a $M_i^{-1}\gamma_0 M_i\gamma_i i = \gamma_i i$ donc $\gamma_i i \in E_2(p_i^{r_i})$ et $\gamma_i = \gamma_{(c_i,1)}$. Maintenant supposons que $f(\gamma i) = f(\gamma' i)$ alors $\gamma_{(c_i,1)}i = \gamma_{(c_i',1)}i$ donc $c_i = c_i'$ et puisque d'après la proposition 5.1.6 ϕ est injective $\gamma = \gamma'$ modulo $\Gamma_0(N)$ donc $\gamma i = \gamma' i$. Enfin si on

se donne $\gamma_{(c_i,1)} \in \Gamma_0(p_i^{r_i})$, $1 \leq i \leq n$ avec $c_i^2 + 1 = 0 \mod (p_i^{r_i})$ alors, puisque ϕ est surjective(cf proposition 5.1.6), il existe $\gamma \in \Gamma(1)$ tel que $\gamma = \gamma_{(c_i,1)}$ modulo $\Gamma_0(p_i^{r_i})$ ce qui implique, puisque $\gamma_{(c_i,1)} S \gamma_{(c_i,1)}^{-1} \in \Gamma_0(p_i^{r_i})$, que $\gamma S \gamma^{-1} \in \bigcap_i \Gamma_0(p_i^{r_i}) = \Gamma_0(N)$. Ainsi $\gamma i \in E_2(N)$ et f est surjective. On a donc $|E_2(N)| = \prod_{i=1}^n |E_2(p_i^{r_i})|$ d'où le résultat. □

Lemme 5.3.3. *Soit c_1 et c_2 deux entiers tels que $0 < c_1, c_2 \leq N$, $c_1^2 - c_1 + 1 \equiv 0 \mod (N)$ et $c_2^2 - c_2 + 1 \equiv 0 \mod (N)$ alors $c_1 = c_2$ si $c_1 c_2 - c_2 + 1 \equiv 0 \mod (N)$ ou $c_1 c_2 - 2c_2 + 1 \equiv 0 \mod (N)$.*

Démonstration. Si $N = 2$ ou $N = 3$ la vérification se fait facilement, on peut donc supposer $N > 3$. Si un nombre premier p diviserait N et c_1 alors, puisque $c_1^2 - c_1 + 1 \equiv 0 \mod (N)$, on aurait $1 \equiv 0 \mod (p)$ ce qui est impossible donc $c_2 \wedge N = 1$, de même $c_1 \wedge N = 1$. On peut donc supposer que c_1 et c_2 appartiennent à $(\mathbb{Z}/N\mathbb{Z})^\times$. Supposons que c_1 n'est pas congru à c_2 modulo N alors c_1 et c_2 sont les deux racines distinctes du polynômes $X^2 - X + 1$ dans le corps $(\mathbb{Z}/N\mathbb{Z})^\times$ donc $c_1 c_2 \equiv 1 \mod (N)$ et $c_1 + c_2 \equiv 1 \mod (N)$ (relation coefficients-racines). Dans le cas où $c_1 c_2 - c_2 + 1 \equiv 0 \mod (N)$ on obtient $c_2 \equiv 2 \mod (N)$ et $c_1 \equiv -1 \mod (N)$ donc $3 = 0 \mod (N)$ ce qui implique $N \leq 3$ et dans le cas où $c_1 c_2 - 2c_2 + 1 \equiv 0 \mod (N)$, on obtient $c_2 \equiv 1 \mod (N)$ et $c_1 \equiv 0 \mod (N)$ donc $1 \equiv 0 \mod (N)$, dans les deux cas on obtient donc une contradiction. Ainsi c_1 est congru à c_2 modulo N et puisque $0 < c_1, c_2 \leq N$, $c_1 = c_2$. □

Proposition 5.3.4. *Le nombre μ_3 de points $\Gamma_0(N)$-elliptiques, inéquivalents et de multiplicité 3 est donné par*

$$\mu_3 = \begin{cases} 0 & si\, N \equiv 0 \mod (9) \\ \displaystyle\prod_{p|N} \eta_p & sinon \end{cases}$$

Démonstration. De même que pour la démonstration de la proposition 5.3.3 on suppose en premier que $N = p^r$. Montrons que l'on a
$E_3(N) = \left\{\gamma_{(c,1)}\rho^2, 0 < c \leq N, c^2 - c + 1 \equiv 0 \mod (N)\right\}$, si on se donne $z \in E_3(N)$ alors il existe $\gamma_0 \in \Gamma_0(N)$ tel que $z = \gamma_0 z$ et, puisque z est en particulier $\Gamma(1)$-elliptique de multiplicité 3, $z = \gamma_1 \rho^2$ avec $\gamma_1 \in \Gamma(1)$, d'où $\gamma_1^{-1}\gamma_0\gamma_1 \in \mathrm{Stab}_{\Gamma(1)}(\rho^2)$ donc $\gamma_1^{-1}\gamma_0\gamma_1 \in \{\pm ST, \pm (ST)^2\}$. On a $\gamma_1^{-1}\gamma_0\gamma_1 \neq \pm(ST)^2$ car sinon $|\mathrm{Tr}(\gamma_0)| = |\mathrm{Tr}(\pm(ST)^2)| = 2 \geq 2$. Il existe $(c,d) \in A_N$ tel que $\gamma_1 \in \Gamma_0(N)\gamma_{(c,d)}$ donc $\gamma_{(c,d)} S T \gamma_{(c,d)}^{-1} \in \Gamma_0(N)$ c'est-à-dire

$$\begin{pmatrix} ac + b(d-c) & ad + b(d-b) \\ c^2 + d^2 - cd & cd + d(d-b) \end{pmatrix} \in \Gamma_0(N) \text{ d'où } c^2 + d^2 - cd \equiv 0 \mod (N)$$

Montrons que $d = 1$: Pour cela supposons qu'il existe un nombre premier p qui divise d alors $c^2 \equiv 0 \mod (p)$ donc $p|c$ impossible car $c \wedge d = 1$. On a donc $c^2 - c + 1 \equiv 0 \mod (N)$, $0 < c \leq N$ et $\gamma_{(c,d)} = \gamma_{(c,1)}$ donc $z \in \Gamma_0(N)\gamma_{(c,1)}\rho^2$ et z est $\Gamma_0(N)$-équivalent à $\gamma_{(c,1)}\rho^2$.
Inversement si $c^2 - c + 1 \equiv 0 \mod (N)$ alors

$$\gamma_{(c,1)} S T \gamma_{(c,1)}^{-1} \in \Gamma_0(N) \text{ et } \gamma_{(c,1)} S T \gamma_{(c,1)}^{-1} \gamma_{(c,1)} \rho^2 = \gamma_{(c,1)}\rho^2$$

D'aprés la proposition 3.3.8 $\gamma_{(c,1)}\rho^2$ est de multiplicité 3 pour $\pi_{\Gamma(1)}$ donc d'après la proposition 4.3.3 $\gamma_{(c,1)}\rho^2$ est de multiplicité 1 ou 3 pour $\pi_{\Gamma_0(N)}$ mais $\gamma_{(c,1)}\rho^2$ est $\Gamma_0(N)$-elliptique donc d'après la proposition 3.3.9 sa multiplicité est différente de 1. Maintenant

si $\gamma_{(c_1,1)}\rho^2 = \gamma_0\gamma_{(c_2,1)}\rho^2$ avec $0 < c_1, c_2 \leq N$ tels que $c_1^2 - c_1 + 1 \equiv 0 \mod (N)$ et $c_2^2 - c_2 + 1 \equiv 0 \mod (N)$ alors $\gamma_{(c,1)}^{-1}\gamma_0\gamma_{(c_2,1)} \in \mathrm{Stab}_{\Gamma(1)}(\rho^2)$ et donc $c_1 \equiv c_2 \mod (N)$ ou $c_1c_2 - c_1 + 1 \equiv 0 \mod (N)$ ou $c_1c_2 - 2c_1 + 1 \equiv 0 \mod (N)$. D'après le lemme 5.3.3 on a $c_1 = c_2$ et ainsi les points $\gamma_{(c,1)}\rho^2$ sont inéquivalents sous $\Gamma_0(N)$.
Ainsi d'après la proposition 5.3.2 on a :

$$\mu_3 = |E_3(N)| = |\left\{c \in \mathbb{N}^\star, c \leq N, c^2 - c + 1 \equiv 0 \mod (N)\right\}| = \begin{cases} 0 & \text{si } p^r \equiv 0 \mod (9) \\ \eta_p & \text{sinon} \end{cases}$$

De la même manière que dans la démonstration de la proposition 5.3.3 on a

$$|E_3(N)| = \prod_{i=1}^{n} |E_3(p_i^{r_i})|$$

d'où le résultat. □

Lemme 5.3.4. *Soit $N = \prod_i p_i^{r_i}$, on a*

$$\sum_{d|N, d>0} \varphi(d \wedge (N/d)) = \prod_{p|N} \sum_{s=0}^{r_i} \varphi(p_i^{min(s, r_i - s)})$$

Démonstration. On pose $\nu(N) = \sum_{d|N,d>0} \varphi(d \wedge (N/d))$. Montrons que ν est multiplicative, soit n et m deux entiers premier entre eux alors si $d_1|n$ et $d_2|m$ on a $(d_1 \wedge (n/d_1)) \wedge (d_2 \wedge (m/d_2)) = 1$ et $(d_1 \wedge (n/d_1)) \times (d_2 \wedge (m/d_2)) = d_1d_2 \wedge (nm/d_1d_2)$ donc, puisque φ est multiplicative, on a $\varphi(d_1 \wedge (n/d_1))\varphi(d_2 \wedge (m/d_2)) = \varphi(d_1d_2 \wedge (nm/d_1d_2))$. De plus $\{d|nm\} = \{d_1|n\}.\{d_2|m\}$ donc $\nu(n)\nu(m) = \nu(nm)$. De plus $\nu(p^r) = \sum_{s=0}^{r} \varphi(p^{min(s,r-s)})$ donc $\nu(N) = \prod_{p|N} \nu(p^r) = \prod_{p|N} \sum_{s=0}^{r} \varphi(p^{min(s,r-s)})$. □

Proposition 5.3.5. *Le nombre μ_∞ de cusps $\Gamma_0(N)$-inéquivalents est donné par*

$$\mu_\infty = \sum_{d|N, d>0} \varphi(d \wedge (N/d))$$

Démonstration. On pose $E_\infty = \{\text{cusps } \Gamma_0(N)\text{-inéquivalent}\}$, $\Gamma_\infty = \mathrm{Stab}_{\Gamma(1)}(\infty)$ et $\Gamma_0(N)\backslash\Gamma(1)/\Gamma_\infty = \{\Gamma_0(N)\gamma\Gamma_\infty, \gamma \in \Gamma(1)\}$ l'ensemble des classes doubles. On considère l'application

$$\begin{aligned} f : \Gamma_0(N)\backslash\Gamma(1)/\Gamma_\infty &\longrightarrow \pi_{\Gamma_0(N)}(\{cusps\}) \\ \Gamma_0(N)\gamma\Gamma_\infty &\longmapsto \pi_{\Gamma_0(N)}(\gamma\infty) \end{aligned}$$

f est bien définie car si $\gamma_1 \in \Gamma_0(N)\gamma_2\Gamma_\infty$ alors $\pi_{\Gamma_0(N)}(\gamma_1\infty) = \pi_{\Gamma_0(N)}(\gamma_2\infty)$. De plus f est surjective car $\Gamma(1)$ agit transitivement sur les cusps et f est injective car si $\gamma_0\gamma_1\infty = \gamma_2\infty$ alors $\gamma_2^{-1}\gamma_0\gamma_1 \in \Gamma_\infty$ et donc $\gamma_2 \in \Gamma_0(N)\gamma_1\Gamma_\infty$. Ainsi

$$\mu_\infty = \mathrm{Card}(\Gamma_0(N)\backslash\Gamma(1)/\Gamma_\infty)$$

On considère maintenant l'ensemble

$$M_N = \{(\bar{m}, \bar{n}), \mathrm{PGCD}(m, n, N) = 1\} \subset \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$$

et on définit de la manière suivante une relation d'équivalence sur cet ensemble :

$$(\bar{a},\bar{c}) \sim (\bar{a}',\bar{c}') \Leftrightarrow (\bar{a}',\bar{c}') = \pm(\bar{m}\bar{a}+\bar{n}\bar{c},\bar{m}^{-1}\bar{c}),\ \bar{m} \in (\mathbb{Z}/N\mathbb{Z})^{\times},\ \bar{n} \in \mathbb{Z}/N\mathbb{Z}$$

Puisque $\mathbb{Z}/N\mathbb{Z} \cong \prod_{i=1}^{n} \mathbb{Z}/p_i^{r_i}\mathbb{Z}$ on a $|M_N| = \prod_{p|N} |M_{p^r}|$ et comme

$$m \wedge N = 1 \Leftrightarrow \forall p|N,\ m \wedge p^r = 1$$

on a

$$|M_N/\sim| = \prod_{p|N} |M_{p^r}/\sim|$$

Calculons maintenant $|M_{p^r}/\sim|$. Montrons que si $(\bar{a},\bar{c}) \in M_{p^r}$ alors il existe un unique $0 \leq s \leq r$ tel que $(\bar{a},\bar{c}) \sim (\star,\bar{p^s})$. Si $a \wedge p^r \neq 1$ alors $c \wedge p^r = 1$ et en prenant $n = 0$ et $\bar{m} = \bar{c}^{-1}$ on a $(\bar{a},\bar{c}) \sim (\bar{c}\bar{a},\bar{1})$. Si $a \wedge p^r = 1$ et $c \wedge p^r \neq 1$ alors $(\bar{a},\bar{c}) \sim (\overline{\frac{ac}{c\wedge p^r}}, \overline{c \wedge p^r})$. L'unicité vient du fait que si $p^{s_1} = p^{s_2}m + kp^r$ avec $m \wedge p^r = 1$ et $s_1 \geq s_2$ alors $p^{s_1-s_2}|m$ donc $s_1 - s_2 = 0$. Ainsi il suffit de regarder les classes des éléments $(\bar{a},\bar{p^s})$ avec $0 \leq s \leq r$. Supposons $s > 0$ alors $\bar{a} \wedge p^r = 1$ et montrons que

$$(\bar{a},\bar{p^s}) \sim (\bar{a}',\bar{p^s}) \Leftrightarrow a \equiv a' \mod (p^{min(s,r-s)})$$

Si $\pm p^s = mp^s + kp^r$ et $\pm a' = am + np^s + jp^r$ alors en divisant la première égalité par p^s on a $a' = a(1-kp^{r-s}) + np^s + jp^r$ ce qui implique que $a \equiv a' \mod (p^{min(s,r-s)})$. Inversement si $a \equiv a' \mod (p^{min(s,r-s)})$ en prenant $(\bar{m},\bar{n}) = (\bar{a}'\bar{a}^{-1},0)$ si $s > r-s$ et $(m,n) = (1,\frac{a-a'}{p^s})$ si $s \leq r-s$ on a $(\bar{a},\bar{p^s}) \sim (\bar{a}',\bar{p^s})$. Puisque si $s = 0$ les éléments $(\bar{a},1)$ sont tous dans la même classe on a $|M_{p^r}/\sim| = \sum_{s=0}^{r} \varphi(p^{min(s,r-s)})$. Ainsi

$$|M_N/\sim| = \prod_{p|N} \sum_{s=0}^{r} \varphi(p^{min(s,r-s)})$$

et donc d'après le lemme précédent

$$|M_N/\sim| = \sum_{d|N,d>0} \varphi(d \wedge (N/d))$$

Dans la démonstration de la proposition 5.1.2 on a pu voir que si $\mathrm{PGCD}(a,c,N) = 1$ alors il existe $n \in \mathbb{Z}$ tel que $a \wedge (c+nN) = 1$ donc l'application

$$\begin{aligned} g : \Gamma(1) &\longrightarrow M_N \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\longmapsto (\bar{a},\bar{c}) \end{aligned}$$

est surjective. Supposons maintenant que $\gamma_1 = \gamma_0\gamma_2\gamma_\infty$ avec

$$\gamma_1 = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma_1,\ \gamma_2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1,\ \gamma_0 = \begin{pmatrix} \alpha & \beta \\ kN & \delta \end{pmatrix} \in \Gamma_0,\ \gamma_\infty = \pm \begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix} \in \Gamma_\infty$$

Puisque $\alpha\delta \equiv 1 \mod (N)$, on a

$$(a',c') = \pm(\bar{\alpha}\bar{a} + \bar{\beta}\bar{c}, \bar{\delta}\bar{c}) = \pm(\bar{\alpha}\bar{a} + \bar{\beta}\bar{c}, \bar{\alpha}^{-1}\bar{c})$$

Ainsi g induit une application surjective $\tilde{g} : \Gamma_0(N)\backslash\Gamma(1)/\Gamma_\infty \longrightarrow M_N/\sim$. Montrons que $\tilde{g}$ est injective, on garde les mêmes notations et on suppose que $(a,c) \sim (a',c')$ dans M_N. Montrons pour cela que le polynôme $P(X) = cc'X + c'd - cd'$ admet une racine $\bar{x}$ dans $\mathbb{Z}/N\mathbb{Z}$ car en prenant

$$\gamma_0 = \begin{pmatrix} -ad' + c'(ax+b) & -a'(ax+b) + ab' \\ P(x) & -a'(cx+d) + cb' \end{pmatrix},\ \gamma_\infty = -\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}$$

on aura alors que $\gamma_0\gamma_1\gamma_\infty = \gamma_2$. Si $c \wedge N = 1$ alors $c' \wedge N = 1$ et P a une racine dans $\mathbb{Z}/N\mathbb{Z}$. Maintenant si $c \wedge N \neq 1$, en écrivant $N = \prod_{p|N} p^r$ on a $(a,c) \sim (a',c')$ dans M_{p^r}. Si $c \wedge p^r \neq 1$ on pose $c' = p^s K'$ avec $K' \wedge p^r = 1$ alors $c = p^s K$ et $1 = ad - bc = ad - bKp^s = a'd' - b'K'p^s$ donc $p^s | ad - a'd'$ et puisque $a' = ma + cn$ mod (p^r) on a $p^s | a(d - md')$. Ainsi puisque $p^s \wedge a = 1$ on peut écrire $d - md' = \lambda p^s$ d'où $P(X) = K'p^{2s}(mK'X + \lambda)$ et puisque m et K' sont premiers avec p^r, P a au moins une racine dans $\mathbb{Z}/p^r\mathbb{Z}$ et donc P a au moins une racine dans $\mathbb{Z}/N\mathbb{Z}$.

Ainsi :

$$\mu_\infty = \mathrm{Card}(\Gamma_0(N)\backslash\Gamma(1)/\Gamma_\infty) = |M_N/\sim| = \sum_{d|N, d>0} \varphi(d \wedge (N/d))$$

□

Proposition 5.3.6. *Le genre de $X_0(1)$ est nul et pour $N \geq 2$ le genre de $X_0(N)$ est*

$$g(X_0(N)) = \begin{cases} 1 + \frac{1}{12}N\prod_{p|N}\frac{p+1}{p} - \frac{1}{3}\prod_{p|N}\eta_p - \frac{1}{2}\sum_{d|N,d>0}\varphi(d\wedge(N/d)) & \text{si } 4|N \\ 1 + \frac{1}{12}N\prod_{p|N}\frac{p+1}{p} - \frac{1}{4}\prod_{p|N}\epsilon_p - \frac{1}{2}\sum_{d|N,d>0}\varphi(d\wedge(N/d)) & \text{si } 9|N \\ 1 + \frac{1}{12}N\prod_{p|N}\frac{p+1}{p} - \frac{1}{2}\sum_{d|N,d>0}\varphi(d\wedge(N/d)) & \text{si } 36|N \\ 1 + \frac{1}{12}N\prod_{p|N}\frac{p+1}{p} - \frac{1}{4}\prod_{p|N}\epsilon_p - \frac{1}{3}\prod_{p|N}\eta_p - \frac{1}{2}\sum_{d|N,d>0}\varphi(d\wedge(N/d)) & \text{sinon} \end{cases}$$

Démonstration. Il suffit d'appliquer le théorème 4.3.1 en utilisant les propositions 5.1.3, 5.3.3, 5.3.4 et 5.3.5. □

Exemple 5.3.1. *On peut calculer quelques valeurs de $g(X(N))$ et $g(X_0(N))$:*

N	$g(X(N))$	$g(X_0(N))$
1,...,5	0	0
6	1	0
7	3	0
8	5	0
9	10	0
10	13	0
11	26	1
12	25	0
13	50	0
14	49	1
15	73	1
16	81	0
17	133	1
18	109	0
19	196	1
20	169	1
21	241	1
22	241	2
23	375	2
24	289	2
25	476	1
26	421	2
27	568	1
28	529	2
29	806	2
30	577	3
31	1001	2

TABLE 1 – Valeurs du genre de $g(X(N))$ et $g(X_0(N))$ pour $1 \leq N \leq 31$

Références

[1] Maurice MIGNOTTE. *Algèbre Concrète*. Ellipses.

[2] James S. MILNE. Modular functions and modular forms (v1.30), 2012.

[3] J.S. MILNE. *Elliptic Curves*. BookSurge Publishers, 2006.

[4] Rick MIRANDA. *Algebraic Curves and Riemann Surfaces*. Graduate Studies in Mathematics.

[5] Toshitsune MIYAKE. *Modular Forms*. Springer.

[6] Daniel PERRIN. *Cours d'Algèbre*. Ellipses.

[7] Walter RUDIN. *Analyse Réelle et Complexe troisième édition*. Dunod.

[8] Gôro SHIMURA. *Introduction to arithmetic theory of automorphic functions*. Princeton University Press, 1971.