N° d'ordre : / 2005 – M / MT.

Université des Sciences et de la Technologie

Houari Boumediene

جامعة هواري بومدين
للعلوم والتكنولوجيا
U S T H B

Faculté de Mathématiques

Laboratoire d'Algèbre et Théorie des Nombres

Thèse de Magister ***présentée pour***

l'obtention du grade de : *Magister en Mathématiques*

Par M^{elle} *ALOUACHE Leila*

Spécialité : Algèbre et Théorie des Nombres

Sujet:
Courbes Modulaires - Formes Modulaires

Soutenue publiquement le :

Devant le jury composé de :

Mr R. BEBBOUCHI	Professeur à l'U.S.T.H.B	Président.
Mr M. ZITOUNI	Professeur à l'U.S.T.H.B	Directeur de thèse.
Mr M. HERNANE	Maître de conférence l'U.S.T.H.B	Examinateur.
Mr M. S. HACHAICHI	Maître de conférence à l'U.S.T.H.B	Examinateur.

Remerciements

Tout d'abord, j'aimerais exprimer toute ma gratitude et mon admiration à mon directeur de thèse, monsieur ***ZITOUNI Mohamed****, professeur à l'U.ST.H.B : la qualité de son enseignement, sa gentillesse et sa disponibilité ont été d'un apport inestimable dans l'élaboration de ce manuscrit.*

Je souhaite remercier chaleureusement monsieur ***BEBOUCHI Rachid****, professeur à l'U.S.T.H.B d'avoir accepté de présider le jury ainsi que monsieur* ***HACHAICHI Mohamed Salah*** *et monsieur* ***HARNANE Mohand****, maîtres de conférence à l'U.S.T.H.B qui me font l'honneur d'être membres de mon jury.*

Cette thèse est dédiée avec toute mon affection à toute ma famille et en particulier mes parents et mes sœurs Fatma, Samia, Nora, Dalila et Latifa, ma nièce Sarah et mon neveu Yahia.

Sommaire

Page

Chapitre IV *Les Courbes Modulaires*

Références:

Introduction

Dans cette thèse de magister sur les "Courbes Modulaires et formes Modulaires" il y a 4 chapitres

Dans le chapitre I nous avons commencé par la théorie algébrique et arithmétique des Courbes Elliptiques. Nous avons utilisé la théorie du résultant de 2 polynômes pour classifier les Courbes Elliptiques avec leurs discriminant $\Delta(A)$ et leurs invariants modulaires $c_4(A)$.

Dans le chapitre II, nous avons étudié la structure de groupe abélien $A(K)$. Selon Mordell – Weil ce groupe est de type fini; dans une partie de la preuve de ce théorème, il figure les hauteurs sur un groupe abélien et la descente infinie.

Dans le chapitre III, nous avons décrit la structure du groupe modulaire $SL(2,\mathbb{Z})$ et ses sous groupes de congruence $\Gamma_0(N)$, $\Gamma_1(N)$, $\Gamma(N)$, de niveau N.
En nous inspirons d'ouvrages d'Apostol [1], de Shimura [16], de Silverman [17], nous avons étudié les formes modulaires.

Dans le 4ième et dernier chapitre. Selon Silverman [17], il existe pour tout entier $N \geq 1$ une courbe projective lisse $X_0(N)/\mathbb{Q}$ et un isomorphisme analytique complexe d'espace quotient:

$$j : \mathbb{H}^*/\Gamma_0(N) \longrightarrow X_0(N)(\mathbb{C});$$

Et à chaque nombre z de l'espace $\mathbb{H}^*/\Gamma_0(N)$, on fait correspondre une classe de Courbes Elliptiques ayant un point d'ordre N.
Nous avons suivie la méthode de Ligozat pour obtenir les 12 Courbes Modulaires Elliptiques. Les autres qui sont de genre $g(N) = 0$ et $g(N) \geq 2$ ne sont pas Elliptiques; leurs jacobiennes $J_0(N)$ sont des produits de Courbes Elliptiques.

CHAPITRE I – Arithmétique des Courbes Elliptiques

1. Introduction :

Une Courbe Modulaire $X_0(N)$ de niveau N diffère d'une courbe algébrique par plusieurs éléments, dont les formules de leurs genres.

Les courbes algébriques affines sont classifiées par leur genre. Le genre d'une courbe algébrique C de degré n, admettant s points singuliers est égal à l'entier non négatif :

$$g(C) = \frac{(n-1)(n-2)}{2} - s \ ;$$

Cette formule n'est pas valable pour les Courbes Modulaires.

Le genre d'une courbe modulaire $X_0(N)$ est déterminé par la formule de Hurwitz.

La classe des Courbes Modulaires de genre un est isomorphe à une classe de Courbes Elliptiques.

C'est pourquoi nous commençons par l'étude de l'Arithmétique des Courbes Elliptiques.

2. Equations de Weierstrass d'une Courbe Elliptique :

Une Courbe Elliptique a une structure de variété abélienne de dimension un. Elle est déterminée par une équation particulière : l'équation de Weierstrass.

Définition 1

Une Courbe Elliptique a une structure de variété abélienne de dimension un. Elle est déterminée par une équation particulière : l'équation de Weierstrass.

$$A : y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in K[x,y] \ ; \qquad (1)$$

dans le plan affine $IA^2(K)$ ***et :***

$$A : y^2 z + a_1 x y z + a_3 y z^2 = x^3 + a_2 x^2 z + a_4 x z^2 + a_6 z^3 \in K[x,y,z] \ ; \qquad (1\text{-}1)$$

dans le plan projectif $IP^2(K)$***.***

Les 5 coefficients a_1, a_2, a_3, a_4, a_6 sont des éléments d'un corps commutatif K global ou local ou fini.

Les 2 variables x et y sont racines de l'équation algébrique (1), donc ce sont des éléments d'une clôture algébrique K_{alg} de K.

Les propriétés d'une Courbe Elliptique dépendent de son corps de base K :

Lorsque K est un corps de nombres algébriques nous étudions la Courbe Elliptique au moyen de la Théorie des Nombres (entiers algébriques, discriminants, idéaux, équations diophantiennes, nombres premiers, fonctions arithmétiques, valuations….).

Lorsque K est le corps de nombres complexes, nous étudions la Courbe Elliptique au moyen de l'Analyse Complexe (réseaux, tores complexes, fonctions elliptiques, formes modulaires, groupe modulaire …) et la Géométrie Algébrique (diviseurs, variétés, schémas …).

Lorsque K est un corps fini IF_q, à $q = p^n$ éléments, p premier, nous étudions la Courbe Elliptique au moyen de la Théorie des Corps Finis.

3. Transformations linéaires de l'équation de Weierstrass :

L'objet d'une transformation est d'éliminer certains monômes.

Nous éliminons les monômes en $x\,y$ et en y avec le changement linéaire de variables :

$$(x,y)\rightarrow\left(X,\frac{Y-a_1X-a_3}{2}\right), \text{ pour carac } (K)\neq 2\ . \qquad (2)$$

Nous obtenons l'équation de Weierstrass :

$$A_1 : Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6\ ; \qquad (2\text{-}1)$$

Les coefficients b_{2i} sont des polynômes « homogènes » de degré $2i$ de l'anneau $\mathbb{Z}[a_1,a_2,a_3,a_4,a_6]$

$$\begin{aligned} b_2 &= a_1^2 + 4\,a_2\ ; \\ b_4 &= 2\,a_4 + a_1\,a_3\ ; \\ b_6 &= 4\,a_6 + a_3^2\ ; \end{aligned} \qquad (2\text{-}2)$$

Nous éliminons le coefficient 4 et le monôme en x^2 avec la transformation linéaire :

$$(X,Y)\rightarrow\left(\frac{x-3b_2}{36},\frac{y}{108}\right), \text{ pour carac } (K)\neq 2,\ 3\ . \qquad (3)$$

Nous obtenons l'équation de Weierstrass :

$$A_2 : y^2 = x^3 - 27c_4x - 54c_6\ ; \qquad (3\text{-}1)$$

Les *2* coefficients c_{2i} sont des polynômes « homogènes » de degré $2i$ de l'anneau $\mathbb{Z}[b_2, b_4, b_6]$

$$c_4 = b_2^2 - 24\, b_4 ;$$
$$c_6 = -b_2^3 + 36\, b_2\, b_4 - 216\, b_6 ; \qquad (3\text{-}2)$$

Il existe d'autres modèles d'équations de Weierstrass :

1) Modèle de Legendre :

$$A_3 : y^2 = x(x-1)(x-d) \text{ ; pour } d \neq 0,1. \qquad (4)$$

2) Modèle de Cassels : avec les trois coefficients nuls $a_1=a_2=a_3=0$.

$$A_4 : y^2 = x^3 + Ax + B \in \mathbb{Z}[x,y] \text{ et } 4A^3+27B^2 \neq 0 ; \qquad (4\text{-}1)$$

3) Modèle de Tate :

$$A_5 : y^2 + xy = x^3 + ax + b \in \mathbb{C}[x,y] ; \qquad (4\text{-}2)$$

les coefficients *a* et *b* admettent des développements en séries :

$$a = -5 \sum_{n \geq 1} n^3 q^n (1 - q^n)^{-1} ;$$
$$b = -\frac{1}{12} \sum_{n \geq 1} q^n (7n^5 + 5n^3)(1 - q^n)^{-1} ; \qquad (4\text{-}3)$$

Avec $q=exp(2i\pi z)$ et z dans le demi-plan supérieur $\mathbb{H} = \{z \in \mathbb{C},\ Im\ z \succ 0\}$.

4) Modèle de Deuring :

$A_6 : y^2 + axy + y = x^3$; Avec a non cube.

4. Invariants d'une Courbe Elliptique :

Les coefficients b_{2i} et c_{2i} permettent de définir plusieurs invariants arithmétiques, algébriques, géométriques, différentiels : le discriminant, l'invariant modulaire, l'invariant différentiel, l'invariant de Hasse, le conducteur, le régulateur, le rang, la série *L* de Dirichlet, la fonction Zêta …

Définition 2 :

a)Le discriminant d'une Courbe Elliptique A est le polynôme « homogène » de degré 12 de l'anneau $\mathbb{Z}[b_2,b_4,b_6,b_8]$ égal à :

$$\Delta(A)= 9\, b_2\, b_4\, b_6 - 8\, b_4^3 - 27\, b_6^2 - b_2^2\, b_8 \; ; \qquad (5)$$

lorsque la caractéristique de K est différente de 2 et 3.

Où on a posé:

$$4\, b_8 = b_2\, b_6 - b_4^2 \; ; \qquad (5\text{-}1)$$

b) L'invariant modulaire d'une Courbe Elliptique A est l'élément du corps K égal à :

$$j(A) = \frac{c_4^3}{\Delta(A)} \; ; \qquad (5\text{-}2)$$

c) L'invariant différentiel d'une Courbe Elliptique A est l'élément différentiel

$$\omega(A) = \frac{dx}{2y + a_1 x + a_3} = \frac{-\,dy}{3x^2 + 2a_2 x + a_4 - a_1 y} \; ; \qquad (5\text{-}3)$$

Les dénominateurs sont les dérivées partielles dans l'équation différentielle :

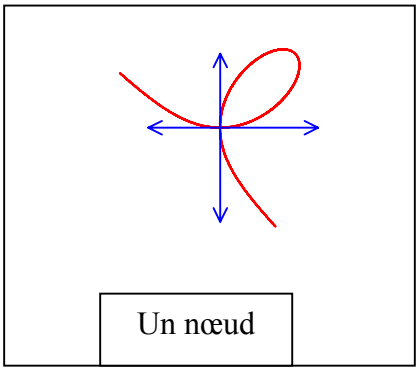
$$dF = F_x' dx + F_y' dy = 0 \; ; \qquad (5\text{-}4)$$

où $F(x,y) = y^2 + a_1 x\, y + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0$ est l'équation de Weierstrass de la Courbe Elliptique A.

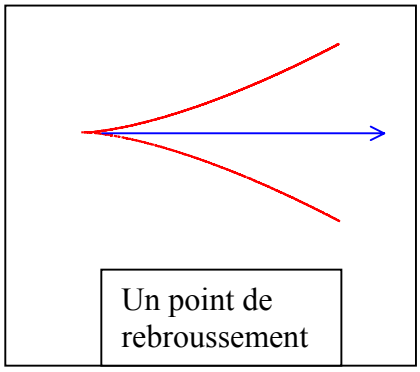
5. Classification des cubiques planes avec le discriminant $\Delta(A)$ et l'invariant $c_4(A)$:

D'après la théorie des singularités d'une courbe algébrique, une cubique plane admet 0 ou 1 point singulier.

Le point singulier est soit un nœud soit un point de rebroussement.



Un nœud



Un point de rebroussement

La cubique A admet 2 tangentes distinctes au nœud

Elle admet 2 tangentes confondues au point de rebroussement.

L'équation projective d'une cubique A dans le plan projectif $IP^2(K)$ est :

$$f(x,y,z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 = 0; \quad (6)$$

Le point $0_A = (0,1,0)$ joue un rôle important dans l'étude de la cubique. Ce point 0_A est donc un représentant de la classe des demi-droites parallèles à l'axe Oy.

Dans le plan affine $IA^2(K)$, ce point $0_A = (\infty,\infty)$ est le point à l'infini de la cubique A.

Proposition 1

Le point à l'infini 0_A d'une cubique A est un point non singulier de la cubique.

Preuve :

Prenons l'équation projective $f(x,y,z)=0$, formule (6).

Au point $0_A = (0,1,0)$, la fonction f prend la valeur :

$f(0,1,0) = 0$;

Cela implique que le point 0_A est sur la cubique A.

Pour savoir si ce point 0_A est singulier, calculons les dérivées partielles de f :

$f_x' = a_1 y z - 3x^2 - 2a_2 x z$;

$f_y' = 2yz + a_1 x z + a_3 z^2$;

$f_z' = y^2 + a_1 x y + 2a_3 y z - a_2 x^2 - 2a_4 x z - 3a_6 z^2$;

Au point à l'infini $0_A = (0,1,0)$, la dérivée f_z' prend la valeur :

$f'(0,1,0) = 1 \neq 0$;

Il en résulte que le point à l'infini 0_A est un point non singulier de la cubique A

□

5.1 Résultant de deux polynômes :

Pour classifier les cubiques planes il est utile d'utiliser la théorie du résultant de deux polynômes de l'anneau $K[x]$. Cette théorie se trouve dans plusieurs ouvrages («Algebra» de, S. Lang, par exemple).

Soit deux polynômes :

$f(t) = a_0 t^n + a_1 t^{n-1} + a_2 t^{n-2} + \ldots\ldots\ldots + a_n$ .De degré n, $a_0 \neq 0$;

$g(t) = b_0 t^m + b_1 t^{m-1} + b_2 t^{m-2} + \ldots\ldots\ldots + b_m$ .De degré m, $b_0 \neq 0$;

Définition 3

Le résultant de 2 polynômes f et g de l'anneau K[x] est le déterminant d'ordre n+m

$$\begin{vmatrix}
a_0 & a_1 & . & . & . & . & a_n & 0 & . & . & . & 0 \\
0 & a_0 & a_1 & . & . & . & a_{n-1} & a_n & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . \\
0 & . & . & . & . & . & a_0 & a_1 & . & . & . & a_n \\
b_0 & b_1 & . & . & . & . & . & b_m & 0 & . & . & 0 \\
. & b_0 & b_1 & . & . & . & . & b_{m-1} & b_m & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . \\
0 & . & . & . & . & . & 0 & b_0 & b_1 & . & . & b_m
\end{vmatrix}$$

avec n lignes de $(a_0,a_1,\ldots a_n)$ et m lignes $(b_0,b_1,\ldots b_m)$; les termes manquants sont remplacés par des zéros.

Dans une clôture algébrique du corps K les deux polynômes *f et g* se factorisent sous la forme :

$f(t) = a_0 (t - \alpha_1) \ldots \ldots \ldots (t - \alpha_n)$;

$g(t) = b_0 (t - \beta_1) \ldots \ldots \ldots (t - \beta_m)$;

Où les racines α_s *et* β_t sont simples ou multiples.

Ces 2 polynômes *f* et *g* sont liés par un invariant : leur résultant qui est une fonction des zéros de *f* et *g*.

Proposition 2

Le résultant des 2 polynômes f(x) et g(x) est une fonction polynomiale homogène des zéros, $\alpha_1, \alpha_2, \ldots \alpha_n$ de f(x) et $\beta_1, \beta_2, \ldots \beta_m$ de g(x) :

$$\textbf{Res (f,g)} = a_0^m b_0^n \prod_{1 \le i \le n;\ 1 \le j \le m} (\alpha_i - \beta_j) \text{ ;} \qquad \textbf{(1)}$$

Preuve :

Dans «Algebra» de S. Lang.

La formule (1) implique le:

Corollaire :

Soit la proposition 2. Alors :

a) ***le résultant Res(f,g) = 0 si et seulement si les 2 polynômes ont une racine commune*** $\alpha_s = \beta_t$, $1 \le s \le n$, $1 \le t \le m$.

b) ***lorsque le polynôme f est le produit de 2 polynômes*** $f(x) = f_1(x) f_2(x)$, ***le résultant Res(f,g) prend la valeur***

$Res(f_1 f_2, g) = Res(f_1, g)\, Res(f_2, g)$.

Dans le cas d'un polynôme $f(x)$ et de sa dérivée $f'(x)$ le résultant $Res(f, f')$ est déterminé par la :

Proposition 3 :

Le résultant d'un polynôme f de degré n

$f(t) = a_0 (t - \alpha_1) \dots \dots \dots (t - \alpha_n)$, $a_0 \neq 0$.

et de sa dérivée $f'(t)$ ***est égal à :***

$$Res(f, f') = a_0^{n-1} \prod_{1 \le i \le n} f'(\alpha_i).$$

Preuve:

Soit un polynôme f de degré n de l'anneau $K[t]$

$f(t) = a_0 (t - \alpha_1) \dots \dots \dots (t - \alpha_n)$, $a_0 \neq 0$; (1-1)

et le polynôme dérivé

$f'(t) = n\, a_0 (t - \sigma_1) \dots \dots \dots (t - \sigma_{n-1})$; (1-2)

où les α_i sont les racines du polynôme f et les σ_j sont les racines de la dérivée f'

La proposition 2 implique la valeur du résultant :

$$Res(f, f') = a_0^{n-1} (n\, a_0)^n \prod_{1 \le i \le n, 1 \le j \le m} (\alpha_i - \sigma_j) ; \quad (1\text{-}3)$$

La formule (1-3) implique le résultant :

$$Res(f, f') = a_0^{n-1} \prod_{1 \le i \le n} f'(\alpha_i);$$

□

Par définition, le discriminant d'un polynôme f est égal à :

$$dis\,(f) = a_0^{2n-2} \prod_{1 \le i < j \le n} \left(\alpha_i - \beta_j\right)^2 \; ; \qquad (2)$$

Ce discriminant de f est lié au résultant par la relation :

$$Res\,(f, f') = (-1)^{\frac{n(n-1)}{2}} a_0\, dis\,(f) \; ; \qquad (2\text{-}1)$$

Exemples :

1) discriminant d'un polynôme f de degré 2

$f(x) = ax^2+bx+c$;

En appliquant la définition 3 et la formule (2-1), nous obtenons :

$$dis\,(f) = b^2-4ac \; ; \qquad (2\text{-}2)$$

2) discriminant d'un polynôme f de degré 3

$f(x) = a_0 x^3 + a_1 x^2 + a_2 x + a_3$;

En appliquant la formule (2) et les fonctions symétriques des racines, nous obtenons

$$dis(f) = 18\, a_0 a_1 a_2 a_3 + a_1^2 a_2^2 - 4a_0 a_2^3 - 4a_1^3 a_3 - 27 a_0^2 a_3^2 \; ; \qquad (2\text{-}3)$$

5.2 Relation entre le discriminant d'un polynôme f et le discriminant d'une cubique E d'équation de Weierstrass $y^2 = f(x)$:

Soit une Courbe Elliptique E d'équation de Weierstrass :

$E : y^2 = 4x^3+b_2x^2+2b_4x+b_6 = f(x) \in K[x,y]$;

Avec le calcul nous obtenons le discriminant du polynôme $f(x)$:

$$dis\,(f) = 16(\, 9b_2b_4b_6 - b_2^2 b_8 - 8b_4^3 - 27b_6^2 \,); \qquad (2\text{-}4)$$

Avec la formule (5) du discriminant $\Delta(E)$ et (2-4) nous obtenons la relation :

$$dis(f) = 16\, \Delta(E);$$

Proposition 4 :

Soit une Courbe Elliptique E d'équation de Weierstrass :

$$y^2 = f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$$

Alors les discriminants dis (f) du polynôme f (x) et Δ(E) de la Courbe Elliptique E sont liés par la relation :

$$dis(f) = 16\, \Delta(E).$$

Application aux polynômes:

$f_1(x) = x^3 + a_2x^2 + a_4x + a_6;$

$f_2(x) = x^3 + A\,x + B;$

$f_3(x) = (x-e_1)\,(x-e_2)\,(x-e_3);$

Soient les 3 Courbes Elliptiques d'équations de Weierstrass:

$E_1: y^2 = f_1(x);$ (1)

$E_2: y^2 = f_2(x);$ (2)

$E_3: y^2 = f_3(x);$ (3)

Avec la proposition 3 nous obtenons les discriminants des 3 polynômes:

$$dis(f_1) = 18a_2a_4a_6 + a_2^2a_4^2 - 4a_4^3 - 4a_2^2a_6 - 27a_6^2.$$

$$dis(f_2) = -\left(4A^3 + 27B^2\right).$$

$$dis(f_3) = (e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2.$$

Avec la formule du discriminant $\Delta(E)$ d'une Courbe Elliptique E, nous obtenons les discriminant:

$$\Delta(E_1) = \frac{1}{16}\left(18a_2a_4a_6 + a_2^2a_4^2 - 4a_4^3 - 4a_2^2a_6 - 27a_6^2\right).$$

$$\Delta(E_2) = -\frac{1}{16}\left(4A^3 + 27B^2\right).$$

$$\Delta(E_3) = \frac{1}{16}\,(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2.$$

Nous en déduisons les relations entre $dis(f_i)$ et $\Delta(E_i)$.

Par la théorie des singularités des courbes algébriques d'équation $g(x,y) = 0$
Les points singuliers de E ont pour coordonnées les solutions du système de 3 équations :

$$g(x,y) = 0, \qquad \frac{\partial g}{\partial x}(x, y) = 0, \qquad \frac{\partial g}{\partial y}(x, y) = 0.$$

Pour une cubique d'équation $y^2=f(x)$, un point singulier est un point multiple d'ordre $d = 2$.La relation $dis\,(f) = 16\,\Delta(E)$ permet de trouver un critère dépendant du discriminant $\Delta(E)$.

Proposition 5 :

Soit une cubique E de discriminant $\Delta(E)$. Alors cette cubique est une Courbe Elliptique si et seulement si $\Delta(E) \neq 0$.

Preuve de «la Courbe *E* est Elliptique» implique «$\Delta(E) \neq 0$» :

Prenons une Courbe Elliptique *E* d'équation de Weierstrass

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = f(x) \in \mathbb{R}[x] \quad (1)$$

Par définition d'une Courbe Elliptique, la Courbe *E* n'a pas de point singulier, il en résulte que les trois racines du polynôme $f(x)$ sont simples.

$$f(x) = 4(x-e_1)(x-e_2)(x-e_3), \quad e_i \neq e_j \in \mathbb{R} \quad (2)$$

Par définition le discriminant du polynôme cubique (2) est calculé avec la formule :

$$dis(f) = 4^4 \prod_{1 \leq i < j \leq 3} (e_i - e_j)^2 \; ; \quad (3)$$

Les trois racines étant distinctes, les carrés $(e_i - e_j)^2$ ne sont pas nuls.

Il en résulte:

$$dis(f) \neq 0 \; ; \quad (4)$$

La relation entre discriminant de *f* et discriminant de *E* et la formule (4) impliquent la valeur :

$$\Delta(E) \neq 0 \; ;$$

□

Preuve de «$\Delta(E) \neq 0$» implique «la courbe *E* est une Courbe Elliptique» :

Prenons une cubique *E* d'équation de Weierstrass :

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = f(x) \; ; \quad (5)$$

La relation $dis(f) = 16\Delta(E)$ et l'hypothèse $\Delta(E) \neq 0$ impliquent la valeur :

$$dis(f) \neq 0 \; ; \quad (6)$$

La définition du discriminant d'un polynôme, l'équation (5) et la formule (6) impliquent que $f(x)$ admet 3 racines simples e_i

$$f(x) = 4(x-e_1)(x-e_2)(x-e_3), \quad e_i \neq e_j;$$

Donc la cubique *E* n'a pas de point singulier. C'est une Courbe Elliptique.

□

Il en résulte qu'une cubique *E* de discriminant $\Delta(E) = 0$ est singulière. Elle admet un point singulier.

Corollaire:

Soit une cubique plane E de discriminant $\Delta(E)$ et d'invariant usuel $c_4(E) = b_2^2 - 24\, b_4$;

Alors :

1) La cubique admet un nœud si et seulement $\Delta(E) = 0$ et $c_4(E) \neq 0$.

2) La cubique E admet un point de rebroussement si et seulement si $\Delta(E) = c_4(E) = 0$.

Preuve de « la cubique *E* admet un nœud » implique «$\Delta(E) = 0$ et $c_4(E) \neq 0$» :

Soit une cubique *E* qui admet un nœud ; donc *E* est singulière, son discriminant est nul :

$$\Delta(E) = 0 \ ;$$

L'hypothèse «*E* admet un nœud » implique qu'elle admet 2 tangentes distinctes en ce nœud.

Nous prenons une cubique d'équation de Weierstrass :

$$E : y^2 = 4x^3 + b_2 x^2 + 2\, b_4 x + b_6 = f(x); \qquad (1)$$

Les tangentes à la cubique *E* ont une pente égale à la dérivée y' de *y*.

Avec la dérivation de l'équation (1) nous obtenons la dérivée :

$$y' = \frac{6x^2 + b_2 x + b_4}{y} = \frac{N(x)}{y} \ ; \qquad (2)$$

Le polynôme $N(x)$ est du $2^{\text{iéme}}$ degré, son discriminant est égal à :

$$dis\,(N(x)) = b_2^2 - 24\, b_4 \neq 0 \ ; \qquad (3)$$

Alors l'hypothèse $b_2^2 - 24\, b_4 = c_4(E)$ et (3) impliquent $c_4(E) \neq 0$. □

Preuve de «la cubique *E* admet un point de rebroussement» implique «$\Delta(E) = c_4(E) = 0$» :

Nous gardons l'équation (1) précédente de la cubique *E*.

L'hypothèse « point de rebroussement sur *E* » implique que la cubique *E* est singulière, donc son discriminant :

$$\Delta(E) = 0 \ ;$$

En un point de rebroussement, la cubique admet 2 tangentes confondues.

Les pentes de ces deux tangentes sont les dérivées y', formule (2) précédente.

Le polynôme $N(x)$ admet une racine double, cela implique son discriminant :

$dis\ (N(x)) = 0$;

Il en résulte :

$b_2^2 - 24\ b_4 = c_4(E) = 0;$

□

L'allure d'une Courbe Elliptique E est déterminée par le signe de son discriminant $\Delta(E)$.

Proposition 6 :

Soit une Courbe Elliptique E, de discriminant $\Delta(E)$ et d'équation de Weierstrass

E :$y^2 = f(x) \in IR\ [x,y]$

Alors :

1) ***Elle coupe l'axe Ox en 3 points simples si et seulement $\Delta(E) > 0$.***
2) ***Elle coupe l'axe Ox en un seul point, simple si et seulement si $\Delta(E) < 0$.***

Preuve de « *E* coupe l'axe *Ox* en trois points » implique «$\Delta(E) > 0$ » :

L'hypothèse «*E* coupe l'axe *Ox* en trois points » implique que l'équation de *E* se met sous la forme :

$y^2 = (x-e_1)\ (x-e_2)\ (x-e_3) = f(x)$;

Les 3 points $P_i = (e_i, 0)$ sont les trois points d'intersection.

Par définition, le discriminant de $f(x)$ est égal à :

$$dis\ (f) = \prod_{1 \le i < j \le 3} \left(e_i - e_j\right)^2 \ ;$$

Les trois racines sont des nombres réels ; cela implique :

$(e_i - e_j)^2 > 0$ et $dis(f) > 0$;

La relation entre les discriminants de $f(x)$ et de E implique le signe :

$\Delta(E) > 0$.

□

Preuve de « *E* coupe l'axe *Ox* en un point » implique « $\Delta(E) < 0$ » :

L'hypothèse *E* coupe l'axe *Ox* en un seul point (e , 0) implique une équation de *E* de la forme :

$E : \ y^2 = (x-e)\,(x^2+sx+t) = f(x)$;

Avec $s^2-4t < 0$

Le polynôme x^2+sx+t de degré 2 admet 2 racines conjuguées complexes :

$$e_1 = \frac{1}{2}\left(-s - \sqrt{s^2-4t}\right), \quad e_2 = \frac{1}{2}\left(-s + \sqrt{s^2-4t}\right) ;$$

$$\sqrt{s^2-4t} = i\sqrt{4t-s^2}\ ,\ 4t-s^2 > 0.$$

Par définition le discriminant de *f* égal :

$dis(f) = (e_1-e_2)^2\,(e-e_1)^2\,(e-e_2)^2;$

Il en résulte :

$$dis(f) = -[(e+\frac{s}{2}) + 4t-s^2\,]^2\,[(4t-s^2)] < 0;$$

□

Les résultats précédents impliquent une classification des cubiques planes *E* en 4 classes selon leurs discriminants $\Delta(E)$ et leurs invariants $c_4(E)$.

Proposition 7 :

Les cubiques E d'équation de Weierstrass :

$\boldsymbol{y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6}$ ***;***

de discriminant $\boldsymbol{\Delta(E)}$ ***et de coefficient usuel***

$\boldsymbol{c_4(E) = b_2^2 - 24\,b_4}$ ***;***

sont réparties dans 4 classes :

1) ***Classe (cl 1) des cubiques planes qui ont un nœud***

   $\boldsymbol{\Delta(E) = 0}$ ***et*** $\boldsymbol{c_4(E) \neq 0}$.

2) ***Classe (cl 2) des cubiques planes qui ont un point de rebroussement***

   $\boldsymbol{\Delta(E) = 0 = c_4(E) = 0}$.

3) ***Classe (cl 3) des Courbes Elliptiques qui coupent l'axe Ox en un seul point simple***

   $\boldsymbol{\Delta(E) < 0}$.

4) ***Classe (cl 4) des Courbes Elliptiques qui coupent l'axe Ox en 3 points simples***

   $\boldsymbol{\Delta(E) > 0}$.

Preuve :

Cette proposition rassemble les résultats de la proposition 6 et du corollaire de la proposition 5.

□

6. Exemples :

1) Cubique avec un nœud :

Soit la cubique E_1 d'équation de Weierstrass :

$E_1 : y^2 = x^3 - 6x + 4\sqrt{2}$;

Calcul d'invariants de E_1 :

$b_2 = 0$; $b_4 = -12$; $b_6 = 16\sqrt{2}$; $c_4 = 288$; $\Delta(E_1) = 0$;

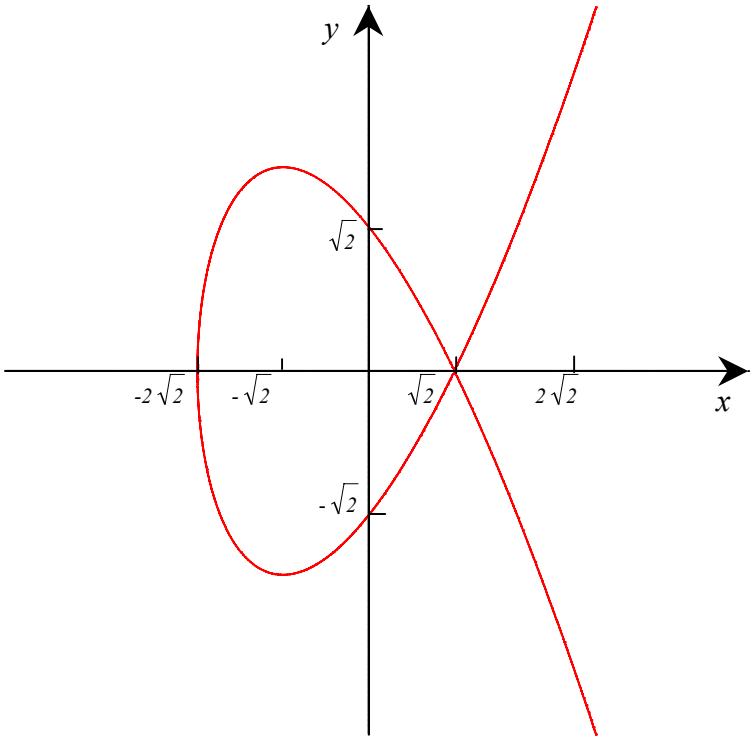
Les valeurs :

$\Delta(E_1) = 0$ et $c_4(E_1) \neq 0$ impliquent que cette cubique admet un nœud.

Tableau des coordonnées de quelques points de la cubique E_1 :

x	-3	$-2\sqrt{2}$	-2	-1	0	1	$\sqrt{2}$	2
y	*pas de solution réelle*	0	$\pm 2\sqrt{1+\sqrt{2}}$	$\pm\sqrt{5+4\sqrt{2}}$	$\pm 2\sqrt{2}$	$\pm\sqrt{-5+4\sqrt{2}}$	0	$\pm 2\sqrt{-1+\sqrt{2}}$

Le point $(\sqrt{2}, 0)$ est le nœud de la cubique E_1.



2) Cubique avec un point de rebroussement :

Soit la cubique E_2 d'équation de Weierstrass :

$E_2 : y^2+4xy+2y = x^3-4x^2-4x-1$;

Calcul d'invariants de E_2 :

$b_2 = b_4 = b_6 = 0;\ \ c_4 = 0$; $\Delta(E_2) = 0;$

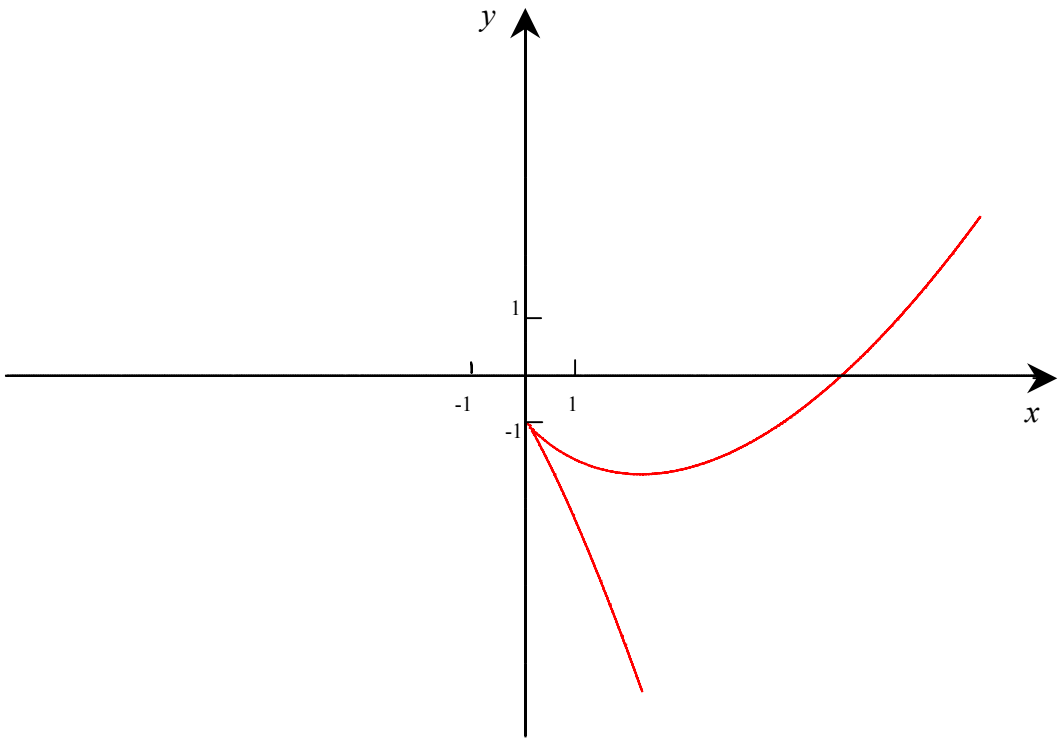
Les valeurs :

$\Delta\ (E_2) = 0$ et $c_4\ (E_2) = 0$ impliquent que cette cubique admet un point de rebroussement.

Tableau des coordonnées de quelques points de la cubique E_2 :

x	*-1*	*0*	*1*	*2*
y	*Pas de solution réelle*	*-1 racine double*	*-4 et -2*	$-2\sqrt{2}-5$ et $2\sqrt{2}-5$

Le point $(0,-1)$ est le point de rebroussement de la cubique E_2.



3) Courbe Elliptique qui coupe l'axe Ox en un seul point :

Soit la cubique E_3 d'équation de Weierstrass :

$$E_3 : y^2 + xy + y = (x+4)(x^2 + x + \frac{3}{2}) ;$$

Calcul d'invariants de E_3 :

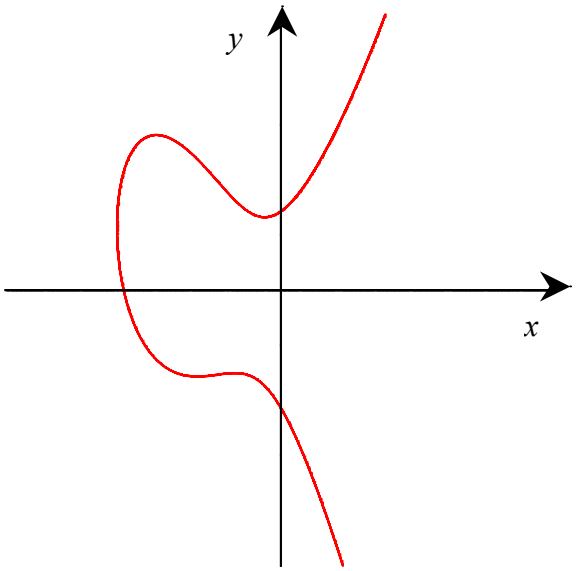
$$b_2 = 21;\ \ b_4 = 12;\ \ b_6 = 25;\ b_8 = \frac{381}{4};\ \ c_4 = 153\ \ ;\ \Delta(E_3) = \frac{-64017}{4};$$

Le discriminant $\Delta\,(E_3) < 0$ implique que la cubique E_3 est une Courbe Elliptique qui coupe l'axe Ox en un seul point.

Tableau des coordonnées de quelques points de la cubique E_3 :

x	-4	-3	-2	-1	0	1	$\frac{75}{4}$
y	0 et 3	$\frac{1}{2}\sqrt{34}+1$ et $-\frac{1}{2}\sqrt{34}+1$	$\frac{1}{2}\sqrt{29}+\frac{1}{2}$ et $-\frac{1}{2}\sqrt{29}+\frac{1}{2}$	$\frac{1}{2}\sqrt{62}$ et $-\frac{1}{2}\sqrt{62}$	-3 et 2	$\frac{1}{2}\sqrt{74}-1$ et $-\frac{1}{2}\sqrt{74}-1$	$\frac{661}{8}$ et $\frac{-819}{8}$

Donc la Courbe Elliptique E_3 coupe l'axe Ox au point $P = (-4,0)$.



4) Courbe Elliptique qui coupe l'axe Ox en trois points :

Soit la cubique E_4 d'équation de Weierstrass :

$E_4 : y^2+2\,xy\,+4\,y = (x+1)\,(x+5)\,(x-2)\,;$

Calcul d'invariants de E_4 :

$b_2 = 20;\ \ b_4 = -6;\ \ b_6 = -24;\ b_8 = -129 c_4 = 544\ ;\ \Delta(E_4) = 63696;$

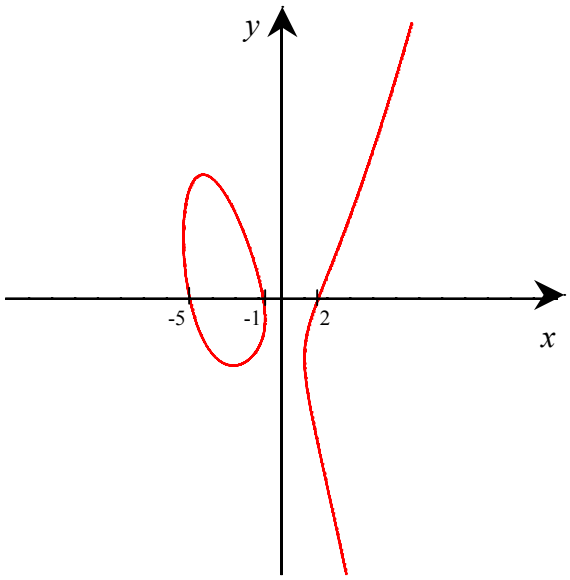
Le discriminant $\Delta(E_4) > 0$ implique que la cubique E_4 est une Courbe Elliptique qui coupe l'axe Ox en trois points.

Tableau des coordonnées de quelques points de la cubique E_4 :

x	-5	-4	-3	-2	-1	0	1	2	22
y	0 et 6	$5\sqrt{6}+2$ et $-5\sqrt{6}+2$	$\sqrt{39}+1$ et $-\sqrt{39}+1$	$2\sqrt{3}$ et $-2\sqrt{3}$	0 et -2	Pas de solution	Pas de solution	0 et -8	-138 et 90

Donc la Courbe Elliptique E_4 coupe l'axe Ox en trois points :

$P_1 = (-5,0),\ P_2 = (-1,0),\ P_3 = (2,0).$


y
x
-5
-1
2

CHAPITRE II *– Groupe de Mordell-Weil d'une Courbe Elliptique*

1. Introduction:

D'après Lang [Elliptic Curves Diophantine Analysis], Poincaré a conjecturé que l'ensemble $E(K)$ des points K - rationnels d'une Courbe Elliptique E est un groupe abélien de type fini. Plus tard en 1922 Mordell a prouvé cette conjecture [Diophantine Equation-Academic Press] ; Weil a étendu ce résultat aux variétés abéliennes [Sur un théorème de Mordell-Weil, Bull-Sci.Math-54(1930) p181-191].

Munissons l'ensemble $E(K)$ d'une loi de groupe abélien :

2. Ensemble E (K) des points K-rationnels d'une Courbe Elliptique :

Considérons l'application :

$$\lambda : E(K) \times E(K) \longrightarrow E(K);$$

De valeur :

$$\lambda (P_1, P_2) = P_1 + P_2 ;$$

Le point $P_1 + P_2$ est construit avec la règle géométrique :

«3 points P_i, colinéaires de la courbe E ont une somme nulle».

$$P_1 + P_2 + P_3 = 0_E ;$$

Le point à l'infini $0_E = (\infty,\infty) = (0,1,0)$ est considéré comme élément neutre

Cette construction du point $P_1 + P_2$ est représentée dans la figure 1.

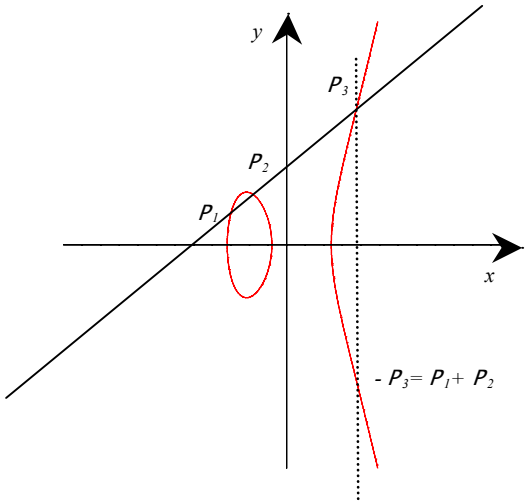


figure 1

Le point à l'infini O_E est déterminé par la direction Oy.

La $P_1 + P_2 + P_3 = O_E$ implique la somme $P_1 + P_2 = -P_3$.

Ce point $-P_3$ est donc le 2ième point d'intersection de la Courbe Elliptique par la parallèle à l'axe Oy passant par P_3.

Vérifions les 4 axiomes d'un groupe abélien :

Axiome de l'élément neutre :

Le point $P+O_E$ est représenté par la parallèle à Oy passant par le point P

Donc $P+O_E = P = O_E + P$.

Axiome du symétrique :

Soit un point P sur le groupe E (K) ;

La parallèle à l'axe Oy passant par le point P coupe la courbe E en trois points P, R, O_E. Ces 3 points satisfont la relation :

$$P + R + O_E = O_E ;$$

Il en résulte que le symétrique du point P est le point $R = - P$.

Cette construction du symétrique d'un point P de la courbe E est représentée dans la figure 2 :

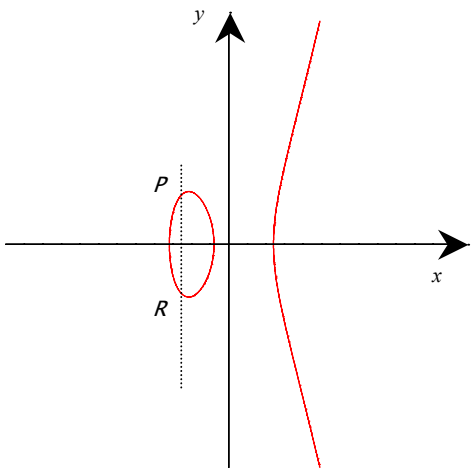


figure 2

Axiome de commutativité :

Les sécantes P_1 P_2 et P_2 P_1 sont confondues ; il en résulte la relation :

$$P_1 + P_2 + P_3 = P_2 + P_1 + P_3 = O_E ;$$

Cela implique:

$P_1 + P_2 = P_2 + P_1 = - P_3$;

Axiome d'associativité:

Soient 3 points A, B, C non colinéaires de la Courbe Elliptique E.

Posons $A + B = L$, $L + C = M$, $B + C = R$ et $A + R = S$.

Il faut calculer les coordonnées des points L, M, R, S.

En comparant les coordonnées x_M et x_S, y_M et y_S, nous obtenons l'égalité :

$(A + B) + C = A + (B + C)$ prouvant l'associativité de la loi.

Nous avons montré la :

Proposition 1 :

L'ensemble E (K) des points K- rationnels d'une Courbe Elliptique E est un groupe abélien d'élément neutre le point à l'infini O_E avec la règle géométrique

«3 points colinéaires L, M et N de la Courbe Elliptique E ont une somme nulle»

$L + M + N = O_E$.

□

Calculons les coordonnées du symétrique $-P$ d'un point P :

Coordonnées du symétrique $-P$ d'un point $P = (x_P, y_P)$ de la courbe, E (figure 2):

Nous prenons un point P de la Courbe Elliptique E

La parallèle à l'axe Oy passant par P, coupe la courbe en un 2ième point qui est le symétrique $-P$.

Equation de cette parallèle :

$x = x_P$;

Donc le symétrique $-P$ a la même abscisse que le point P et une ordonnée y_{-p} solution de l'équation en y du 2ième degré :

$y^2 + y(a_1 x_P + a_3) = x_P^3 + a_2 x_P^2 + a_4 x_P + a_6$;

La somme des deux racines est une fonction symétrique élémentaire de ces racines

$y_P + y_{-p} = - (a_1 x_P + a_3)$;

Nous déduisons les coordonnées du symétrique :

$$- P = (x_P\ ,\ - y_P - a_1 x_P\ - a_3) \qquad (1)$$

Calculons les coordonnées d'une somme $P_1 + P_2$ de 2 points $P_1 \neq \pm P_2$:

Coordonnées du point somme $T = P_1 + P_2$ de deux points :

$P_1=(x_1,y_1) \neq \pm P_2=(x_2,y_2)$ de la courbe E, (figure 1) :

La sécante $P_1\ P_2$ coupe la courbe E en un 3ième point P_3.

La règle géométrique de trois points colinéaires implique la relation :

$$P_1 + P_2 + P_3 = O_E\ ;$$

Il en résulte la somme T de 2 points :

$$T = P_1 + P_2 = - P_3\ ;$$

L'équation de la droite $P_1\ P_2$ est égale à :

$$y=y_1+\lambda(x-x_1),\ \lambda = \frac{y_1 - y_2}{x_1 - x_2}\ ;$$

Les abscisses $x_1,\ x_2,\ x_3$ sont solutions de l'équation cubique en x :

$$[y_1+\lambda(x-x_1)]^2 + (a_1x+a_3)\ [\lambda(x-x_1) + y_1] = x^3+a_2x^2+a_4\ x+a_6\ ;$$

La fonction symétrique somme des racines vaut :

$$x_1+x_2+x_3 =\lambda^2+a_1\lambda-a_2\ ; \qquad (1\text{-}1)$$

La formule (1-1) implique les coordonnées du point P_3 :

$$P_3=(x_3 = \lambda^2+a_1\lambda-a_2-x_1-x_2,\ y_3=y_1+\lambda(x_3-x_1))\ ;$$

Avec le calcul nous obtenons les coordonnées du symétrique $-P_3 = P_1 + P_2$.

$$-P_3 = P_1 + P_2 = \begin{cases} x_{P_1+P_2} = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_{P_1+P_2} = -\lambda^3 - 2a_1\lambda^2 + \lambda\left(a_2 + 2x_1 + x_2 - a_1^2\right) + a_1a_2 - a_3 - y_1 + a_1\left(x_1 + x_2\right) \end{cases}$$

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2},\ x_1 \neq x_2.$$

Nous avons démontré la

Proposition 2 :

Soit une Courbe Elliptique E d'équation de Weierstrass

$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in K\,[x,y]$.

La somme $P_1 + P_2 = T$ de 2 points $P_1 \neq \pm P_2$ de la courbe E est un point de coordonnées

$$P_1 + P_2 = T = \begin{cases} x_T = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_T = -\lambda^3 - 2a_1\lambda^2 + \lambda\left(a_2 + 2x_1 + x_2 - a_1^2\right) + a_1 a_2 - a_3 - y_1 + a_1\left(x_1 + x_2\right) \end{cases}$$

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2},\ x_1 \neq x_2.$$

□

Les coordonnées du point $2P$ sont déterminées par la proposition 3:

Proposition 3 :

Pour tout point $P = (x_P, y_P)$ du groupe de Mordell-Weil E (K) d'une Courbe Elliptique E le point $P + P = 2P$ a pour coordonnées

$$2P = \begin{cases} x_{2P} = t^2 + a_1 t - a_2 - 2x_P \ ; \\ y_{2P} = -t^3 + a_1 t^2 + t\,(a_2 - a_1^2 + 3x_P) + a_1 a_2 - a_3 + 2a_1 x_P - y_P \ ; \end{cases}$$

$$t = \frac{3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P}{2y_P + a_1 x_P + a_3}.$$

□

Preuve : (figure 3)

Soit un point $P = (x_P, y_P)$;

La tangente à la Courbe Elliptique E au point P a pour équation :

$y = t\,(x - x_P) + y_P$,

où t est la pente de la tangente à la Courbe Elliptique E au point $P = (x_P, y_P)$:

$$y' = t = \frac{3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P}{2y_P + a_1 x_P + a_3}.$$

Cette tangente coupe la courbe E en un point double $P = (x_P, y_P)$ et un point simple $M = (x_M, y_M)$

La règle de trois points colinéaires implique la relation :

$2P + M = 0_E$ et $2P = -M$; (1-3)

Les abscisses de ces trois points sont les racines de l'équation cubique en x :

$$[y_P + t(x - x_P)]^2 + a_1 x\,[t(x - x_P) + y_P] = x^3 + a_2 x^2 + a_4 x + a_6 \; ; \quad (1\text{-}4)$$

La fonction symétrique élémentaire des racines de l'équation (1-4) implique la relation :

$$2x_P + x_M = t^2 + a_1 t - a_2 \; ; \quad (1\text{-}5)$$

(1-5) implique l'abscisse du point M :

$$x_M = t^2 + a_1 t - a_2 - 2x_P \; ; \quad (1\text{-}6)$$

(1-3) (1-6) et la formule (1) du symétrique d'un point impliquent les coordonnées du point $2P$

$$2P = \begin{cases} x_{2P} = t^2 + a_1 t - a_2 - 2x_P \; ; \\ y_{2P} = -t^3 + a_1 t^2 + t(a_2 - a_1^2 + 3x_P) + a_1 a_2 - a_3 + 2a_1 x_P - y_P \; ; \end{cases}$$

$$t = \frac{3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P}{2y_P + a_1 x_P + a_3} \; .$$

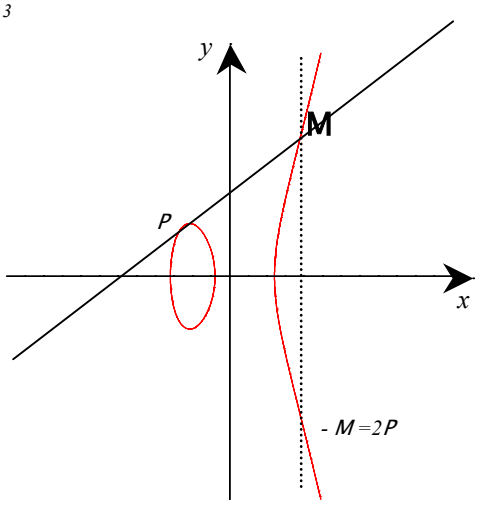


figure 3

Exemple : (*figure 4*)

Soit la Courbe Elliptique E d'équation de Weierstrass :

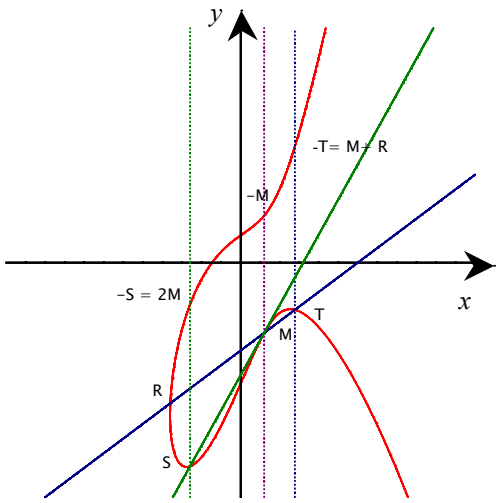
$$E : y^2 - 3xy + 4y = x^3 - 2x^2 + x + 6 \; ;$$

Le groupe de Mordell-Weil $E(\mathbb{Q})$ contient les deux points $M = (1,-3)$ et $R = (-3,-6)$

Calcul des coordonnées des points $M + R$, $-M$, $2M$, $2R$.

Nous obtenons les résultats :

$$M + R = \left(\frac{37}{16}, \frac{317}{64}\right),\ -M = (1,2),\ 2M = \left(\frac{-54}{25}, \frac{-224}{125}\right),\ 2R = (426,-8158)$$



(*figure 4*)

3. Hauteur et descente infinie :

Pour montrer que le groupe de Mordell-Weil est de type fini, il faut utiliser des fonctions particulières sur un groupe abélien et la descente infinie.

Le terme de hauteur est utilisé pour les polynômes, les idéaux, dans un sens différent d'une hauteur sur un groupe abélien.

Définition 1 :

Une hauteur sur un groupe abélien A est une fonction réelle :

$$h : A \longrightarrow \mathbb{R}$$

qui satisfait les 3 axiomes :

(h1) à tout point P_1 de A, on peut associer une constante $C_1(P_1, A) = C_1$ telle que:

$$h(P, P_1) \leq 2h(P) + C_1 \text{ ; pour tout point } P \text{ de } A.$$

(h2) il existe un entier $m \geq 2$ et une constante C_2 tels que :

$$h(mP) \geq m^2 h(P) - C_2 \text{ ; pour tout point } P \text{ de } A.$$

(h3) pour toute constante C_3, l'ensemble des points P de hauteur bornée, $\{ P \in A ; \ h(P) \leq_3 \}$ est fini.

Chaque valeur $h(P)$ définit une hauteur, il y a donc plusieurs types de hauteurs.

Proposition 4 :

Le groupe E (K) / 2 E (K), quotient du groupe de Mordell-Weil d'une Courbe Elliptique E par le sous groupe 2 E (K) est fini.

Preuve :

On utilise la suite exacte pour une extension galoisienne L de E

$$0 \longrightarrow [E(K) \cap 2E(L)] / 2E(K) \longrightarrow E(K) / 2E(K) \longrightarrow E(L) / 2E(L)$$

et l'application bilinéaire de Kummer :

$$u : E(K) \times G(K_{alg} / K) \longrightarrow E[m]$$

K_{alg} = clôture algébrique de K , $G(K_{alg} / K)$ = groupe de Galois, $E[m]$ = sous groupe de m-torsion

(Définition Silverman [17]).

□

Alors, une fonction hauteur est utilisée pour démontrer qu'un groupe abélien A est de type fini lorsque le groupe quotient A / mA est fini.

Proposition 5 :

Soit un groupe abélien A et un entier $m \geq 2$ tel que le groupe quotient A/mA est de type fini. Alors le groupe A est de type fini.

□

Preuve :

Considérons un groupe fini A/mA et des représentants de ses classes :

$$S_1, S_2, \ldots S_p; \tag{1}$$

Construisons une suite infinie de points P_i, sur le groupe A avec l'algorithme de descente infinie :

$$P = m P_1 + S_{1,i}; P_1 = m P_2 + S_{2,i}, \ldots P_n = m P_{n+1} + S_{n+1,i}, \ldots \tag{2}$$

où les points $S_{t,i}$ sont pris dans le système (1).

Introduisons une hauteur h sur sur le groupe A ;

$$h : A \longrightarrow \mathbb{R}; \tag{3}$$

Dans la suite de points (2), prenons une combinaison

$$m P_N = P_{N-1} - S_{N,1} ; \tag{4}$$

Appliquons à l'égalité (4), l'axiome (h2) à gauche et l'axiome (h1) à droite ; nous obtenons l'inégalité:

$$m^2 h(P_N) - C_2 \leq 2 h(P_{N-1}) + C_1 ; \tag{5}$$

Faisons la somme membre à membre des inégalités (5) pour $N = 1, 2, \ldots$

Nous obtenons l'inégalité :

$$h(P_N) \leq \left(\frac{2}{m^2}\right)^N h(P) + (m^{-2} + 2 m^{-4} + \ldots + 2^{N-1} m^{-2N}) C_4, \quad C_4 = C_1 + C_2 ; \tag{6}$$

Pour $m \geq 2$, l'inégalité (6) est transformée :

$$h(P_N) \le u(N)\, h(P) + \frac{C_4}{m^2 - 2},\ \lim_{N \to \infty} u(N) = 0\ ; \qquad (7)$$

Donc à la limite, (7) implique que le 1er membre $h(P_N)$ est borné par un certain nombre B.

$$h(P_N) \le B\ ; \qquad (8)$$

Par l'axiome (h3) l'inégalité (8) implique que l'ensemble

$\{P_t \le B\}$ est fini ; soit $P_1, \ldots P_d$ ces points (9)

Les relations (1) et (9) impliquent que le système de points

$$\{S_1,\ S_2, \ldots\ S_p, P_1, \ldots P_d\ \}\ ; \qquad (10)$$

engendre le groupe abélien A

Il en résulte que tout point P du groupe abélien A est une combinaison linéaire :

$$P = a_1 S_1 + \ldots + a_p S_p + b_1 P_1 + \ldots + b_d P_d,\quad a_i, b_d \in \mathbb{Z}.$$

□

Proposition 6:

Le groupe de Mordell-Weil d'une Courbe Elliptique est de type fini.

□

Preuve :

Le groupe de torsion $T(E)$ d'une Courbe Elliptique est fini. C'est le groupe des points d'ordre fini de la Courbe Elliptique E. Il est engendré par un système $T_1, \ldots, T_s$ de points d'ordre fini.

Le groupe quotient $E(K) / T(E)$ est de type fini ; il est engendré par un système $D_1, \ldots, D_r$ de points d'ordre infini.

Alors tout point $P \in E(K)$ est une combinaison linéaire

$$P = \alpha_1 T_1 + \ldots + \alpha_s T_s + \beta_1 D_1 + \ldots + \beta_r D_r.$$

Le nombre r de points $D_1, \ldots, D_r$, d'ordre infini, linéairement indépendants est un invariant de la Courbe Elliptique E

C'est un entier non négatif

Définition 2 :

Le rang d'une Courbe Elliptique E est le nombre r = r (E) ≥ 0 de générateurs indépendants de la partie infinie du groupe E(K) de Mordell-Weil.

Cet invariant r (E) intervient dans le:

Corollaire :

Le groupe de Mordell-Weil E(K) d'une Courbe Elliptique E est isomorphe à un produit de groupes abéliens

$$E(K) \approx T(E) \times \mathbb{Z}^r .$$

$T(E)$ est le groupe de torsion de E

$\mathbb{Z}^r = r$ copies du groupe abélien $\mathbb{Z}$

Exemples :

1) La Courbe Elliptique d'équation de Weierstrass :

$E : y^2 = 4x^3 - 28x + 25 \in \mathbb{Q}[x,y]$.

a un rang $r(E) = 3$, d'après Buhler, Gross, Zagier.

2) La Courbe Elliptique d'équation de Weierstrass :

$E : y^2 = x^3 + ax^2 + bx \in \mathbb{Q}[x,y]$, $a=1692602$ et $b=530052723915$

a un rang $r(E) \geq 7$, d'après Pemey et Pomerance.

3) La Courbe Elliptique d'équation de Weierstrass :

$E : y^2 = x^3 - D^2x \in \mathbb{Q}[x,y]$, $D = 1.2.3 \bmod 8$

a un rang $r(E) = 0$, d'après Ono.

4) La Courbe Elliptique d'équation de Weierstrass :

$E : y^2 = x^3 - n^2 x \in \mathbb{Q}[x,y]$, $n = 1513$

a un rang $r(E) = 2$, d'après Wada.

4. Points d'ordre fini d'une Courbe Elliptique :

Pour tout entier rationnel m, et pour tout point P de la courbe E la relation :

$m\ P = 0_E$ signifie :

$$m\ P = \begin{cases} P + P + \ldots + P, \ m \text{ fois } P \text{ lorsque } m>0 \\ (-P) + (-P) + \ldots + (-P), (-m) \text{ fois } P \text{ lorsque } m<0 \\ 0_E \text{ lorsque } m=0 \end{cases} \quad (1)$$

Dans la publication «Diophantine Equation With Special References To Elliptic Curves» Cassels à établi des formules de récurrence pour le calcul des coordonnées de points $m\ P$

Ces formules sont appliquées aux Courbes Elliptiques d'équation de Weierstrass :

$A : y^2 = x^3 + Ax + B \in \mathbb{Z}[x,y]$, $4A^3 + 27B^2 \neq 0$

Les coordonnées des points $m\ P$ sont déterminées avec la formule :

$$m\ P = \left(\frac{\varphi_m(P)}{\psi_m^2(P)}, \frac{\omega_m(P)}{\psi_m^3(P)} \right); \quad (2)$$

Valeurs particulières des polynômes Ψ_m :

$$\Psi_{-1} = -1, \quad \Psi_0 = 0, \quad \Psi_1 = 1, \quad \Psi_2 = 2y, \quad \Psi_3 = 3x^4 + 6Ax^2 + 12Bx - B,$$

$$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) ; \quad (3)$$

Pour $m \geq 2$, les polynômes Ψ_m satisfont les relations de récurrence :

$$\Psi_m = 2\Psi_m(\Psi_{m+2}\ \Psi_{m-1} - \Psi_{m-2}^2\ \Psi_{m+1}^2) ;$$

$$\Psi_{2m+1} = \Psi_{m+1}\ \Psi_m^3 - \Psi_{m-1}^3 ; \quad (4)$$

Les polynômes ϕ_m et ω_m sont égaux à :

$$\phi_m = x\Psi_m^2 - (\Psi_{m+1}\ \Psi_{m-1}) ;$$

$$4y\omega_m = \Psi_{m+2}\ \Psi_{m-1}^2 - \Psi_{m-2}\ \Psi_{m+1}^2 ; \quad (5)$$

Exemples :(figure 5)

Soit la Courbe Elliptique E d'équation de Weierstrass:

$E : y^2 = x^3 - x + 1$;

Calcul de discriminant :

$\Delta(E) = -16 \times 23 < 0$;

Donc la Courbe Elliptique coupe l'axe Ox en 1 seul point

La condition $4A^3 + 27B^2 = 23 \neq 0$ est satisfaite.

Le groupe de Mordell-Weil $E(\mathbb{Q})$ contient le point $P = (1,1)$

La proposition 2 implique les coordonnées du point $2P$:

$2P = (-1,1)$

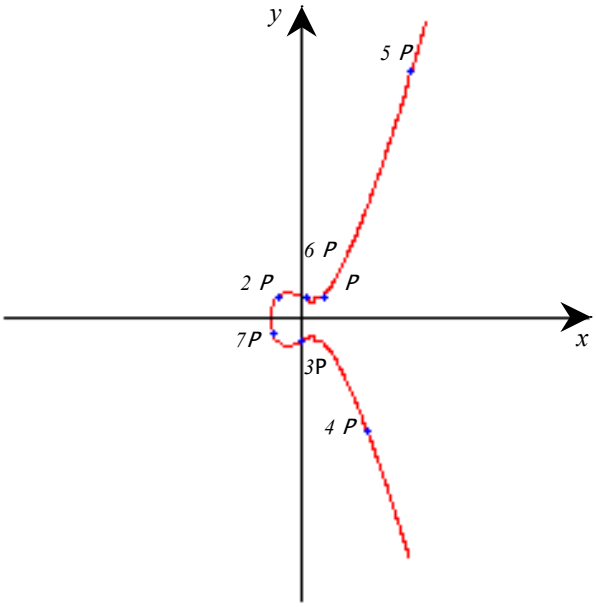
Les formules (2), (3), (4) et (5) impliquent les coordonnées des points :

$$3P = (0,-1),\ 4P = (3,-5),\ 5P = (5,11),\ 6P = \left(\frac{1}{4}, \frac{7}{8}\right),\ 7P = \left(\frac{-11}{9}, \frac{-17}{27}\right),$$

$$8P = \left(\frac{19}{25}, \frac{-103}{125}\right),\ 9P = (56,-419),\ 10P = \left(\frac{159}{121}, \frac{1861}{1331}\right).$$

Nous vérifions la forme des dénominateurs: Ψ_m^2 et Ψ_m^3

$\Psi_6 = 2,\ \Psi_7 = 3,\ \Psi_8 = 5,\ \Psi_{10} = 11.$



Le sous $E(K)$ de Mordell-Weil d'une Courbe Elliptique admet des sous groupes $E(K)[m]$ de m torsion et un sous groupe de torsion $T(E)$

Définition :

1) ***le sous groupe de m – torsion d'une Courbe Elliptique E, pour tout entier m > 1, est l'ensemble des points $P \in E(K)$ d'ordre m :***

   $E(K)[m] = \{ P \in E(K); m P = 0_E \}$

Ces sous groupes sont cycliques où abéliens d'ordre m

2) ***le groupe de torsion d'une Courbe Elliptique est l'ensemble des points P d'ordre fini ; c'est la réunion infinie des sous groupes de m – torsion de E***

   $T(E) = \{ P \in E(K); \ m P = 0_E, m \in \mathbb{Z} \}$

   $= \bigcup_m E(K)[m]$.

Chapitre III –Groupe modulaire- Formes modulaires

1. Introduction:

Dans l'ensemble des matrices, nous trouvons plusieurs structures algébriques : espaces vectoriels de matrices, groupes de matrices, anneaux de matrices, algèbre de matrices.

Dans l'ensemble des groupes multiplicatifs de matrices, nous trouvons les groupes linéaires $GL(n,\mathbb{Q})$, $GL(n,\mathbb{C})$, $GL(n,\mathbb{R})$, formés de matrices de déterminant non nul et des groupes linéaires spéciaux formés de matrices de déterminant 1

Nous nous sommes inspirés pour décrire le groupe modulaire et les formes modulaires des ouvrages:

a) «Modular Functions and Dirichlet Series in Number Theory» de T.Apostol.
b) «Introduction to the Arithmetic Theory of Automorphic Functions» de G.Shimura.
c) «The Arithmetic of Elliptic Curve» de J.H.Silverman
d) «Modular forms and Dirichlet Series» de Andrew.Ogg.

2. Le groupe modulaire $SL(2,\mathbb{Z})$:

Définition 1 :

Le groupe modulaire est le groupe spécial linéaire $SL(2,\mathbb{Z})$ des 2×2 matrices à coefficients entiers rationnels et de déterminant égal à 1

C'est donc un sous groupe discret du groupe spécial linéaire $\mathrm{SL}(2,\mathbb{R})$ des 2×2 matrices à coefficients réels et de déterminant égal à 1.

La 2×2 matrice I_2 et la matrice $-I_2$ forment un sous groupe fini du groupe $\mathrm{SL}(2,\mathbb{Z})$

Définition 2 :

Le groupe projectif spécial linéaire $PSL(2,\mathbb{Z})$ est égal au groupe quotient $SL(2,\mathbb{Z})/\{\pm I_2\}$.

Le groupe modulaire contient les matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *et* $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

Par le calcul nous obtenons leurs ordres:

$S^2 = -I_2$, $S^4 = I_2$, $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ pour $n \geq 1$, $TS = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$, $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$

$(ST)^3 = -I_2$, $(ST)^6 = I_2$.

Donc la matrice S est d'ordre 6et la matrice T est d'ordre infini.

Proposition1:

Le groupe modulaire $SL(2,\mathbb{Z})$ est un groupe non commutatif, infini, engendré par les 2 matrices :

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ et } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Preuve:

Par définition, un groupe engendré par 2 éléments A et B contient leurs inverses A^{-1} et B^{-1} et tous les composés $A^{n_1} B^{n_2} A^{n_3} B^{n_4} \ldots$ avec $n_i \in \mathbb{Z}$.

L'inverse de la matrice S est égale à:

$$S^3 = S^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix};$$

L'inverse de la matrice T est égale à:

$$T^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix};$$

Il en résulte que toute matrice A du groupe modulaire $SL(2,\mathbb{Z})$ est de la forme:

$A = S^{n_1} T^{n_2} S^{n_3} T^{n_4} \ldots S^{n_k} T^{n_{k+1}}$, avec $n_1, n_2, \ldots, n_{k+1} \in \mathbb{Z}$.

□

Corollaire:

Toute matrice A du groupe modulaire est un produit de la forme :

$$A = ST^{n_1}ST^{n_2}S...ST^{n_k},\ n_i \in \mathbb{Z}.$$

Cette représentation n'est pas unique.

□

Exemple:

La matrice $A = \begin{pmatrix} 10 & 7 \\ 7 & 5 \end{pmatrix}$ a un déterminant det A = 1.

Pour trouver une décomposition de la forme:

$$A = ST^{n_1}ST^{n_2}...ST^{n_k}$$

Nous utilisons l'algorithme de multiplication des matrices à droite:

AT^{n_1}, puis $AT^{n_1}S$, $AT^{n_1}ST^{n_2}$, …

jusqu'à l'obtention d'une relation de la forme:

$AT^{n_1}ST^{n_2}ST^{n_3}\ldots = I_2$

avec cet algorithme nous avons obtenue les 2 décomposition:

$$A = T^2\ ST^2\ ST^4ST = TS\ T^{-2}\ ST^3\ ST.$$

Les matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ du groupe linéaire $GL(n,\mathbb{R})$, peuvent être classifiées par leurs traces:

tr (A) = a + d

Définition 3:

Une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ***est parabolique si tr (A) = a + d = ± 2.***

Une matrice A est elliptique si tr (A) est réelle et $|tr(A)| < 2$ **.**

Exemples de matrices A_i de $SL(2,\mathbb{Z})$ des deux types elliptiques et paraboliques:

$A_1 = \begin{pmatrix} 5 & 4 \\ -4 & -3 \end{pmatrix}$ a une trace égale à +2; donc la matrice A_1 est parabolique.

$A_2 = \begin{pmatrix} 11 & -12 \\ 12 & -13 \end{pmatrix}$ a une trace égale à -2; donc la matrice A_2 est parabolique.

$A_3 = \begin{pmatrix} 7 & -19 \\ 3 & -8 \end{pmatrix}$ a une trace égale à -1; donc la matrice A_3 est elliptique.

$A_4 = \begin{pmatrix} 6 & -1 \\ 37 & -6 \end{pmatrix}$ a une trace nulle; donc la matrice A_4 est elliptique.

Les matrices elliptiques sont conjuguées de l'une des matrices:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}.$$

Définition 4:

Pour tout entier $N \geq 1$, les sous groupes modulaires de congruence de niveau $N \geq 1$ sont:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z});\ c \equiv 0 \bmod N \right\}.$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z});\ c \equiv 0 \bmod N,\ a \equiv d \equiv 1 \bmod N \right\}.$$

Les sous groupes de congruence principaux de niveau N sont:

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z});\ a \equiv d \equiv 1 \bmod N,\ b \equiv c \equiv 0 \bmod N \right\}.$$

Le sous groupe $\Gamma(N)$ est un sous groupe normal du groupe modulaire $SL(2,\mathbb{Z})$

Tout sous groupe G du groupe modulaire $SL(2,\mathbb{Z})$ qui contient $\Gamma(N)$ est un sous groupe de congruence de $SL(2,\mathbb{Z})$

Ces sous groupes forment une suite:

$$\{\pm I_2\} \subset \Gamma_0(N) \subset \Gamma_1(N) \subset G \subset SL(2,\mathbb{Z})\ ;$$

et une suite exacte:

$$I_2 \longrightarrow \Gamma(N) \longrightarrow SL(2,\mathbb{Z}) \longrightarrow SL(2, \mathbb{Z}/N\mathbb{Z}) \longrightarrow I_2$$

Proposition2:

1) Pour les entiers $N > 1$, le sous groupe de congruence principal $\Gamma(N)$ n'a pas de matrice elliptique.

2) L'ordre du groupe quotient $\Gamma(1) / \Gamma(N)$ est égal à :

$(N^3/2) \prod_{p/N}(1 - p^{-2})$, ***pour*** $N > 2$ ***et à 6 pour*** $N = 2$.

Preuve:

Proposition 1-39 de Shimura**.**

□

Exemple:

Le groupe $\Gamma(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}),\ a \equiv d \equiv 1 \bmod 2, b \equiv c \equiv 0 \bmod 2 \right\}$.

le groupe $\Gamma(2)$ est formé des 6 matrices:

$$B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ B_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ B_3 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix},\ B_4 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix},$$

$$B_5 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},\ B_6 = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}.$$

cela implique que le groupe quotient $\Gamma(1) / \Gamma(2)$ est formé de 6 classes de matrices modulo le sous groupe $\Gamma(2)$.

3. Action du groupe modulaire sur le demi-plan supérieur $\mathcal{H}$:

Le groupe modulaire opère sur certains ensembles.

Définition 5:

Le demi plan supérieur est la partie du plan complexe formée des nombres complexe de partie imaginaire positive:

$\mathcal{H} = \{z = x+iy \in \mathbb{C},\ Im\ z = y > 0\}$.

Toute matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ du groupe modulaire $SL(2, \mathbb{Z})$ opère sur le demi-plan supérieur $\mathcal{H}$ par la transformation homographique :

$$A\,z = \frac{az + b}{cz + d}$$

L'action des générateurs S et T du groupe modulaire est égale à:

$$S\,z = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} z = \frac{-1}{z}$$, c'est une inversion.

$$T\,z = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} z = z+1$$, c'est une translation.

Nous nous intéressons aux matrices qui laissent fixes 1 ou 2 points z du demi plan supérieur $\mathbb{H}$.

Définition 6:

1) ***Une pointe pour un sous groupe G du groupe modulaire SL(2,ℤ) est un point réel s ∈ ℚ ∪ ∞ fixé par une matrice parabolique de G.***
2) ***Un point elliptique pour G est un point z du demi plan supérieur ℍ fixé par une matrice elliptique de G.***

L'ensemble des matrices $A \in G$ *de point elliptique* z *a une structure particulière.*

Proposition3:

Soit un point z elliptique pour un sous groupe G du groupe modulaire SL(2,ℤ)

Alors l'ensemble des matrices { A ∈ G; A z = z } est un groupe cyclique fini.

Preuve:

Soit un point elliptique z pour un sous groupe G du groupe modulaire $SL(2,\mathbb{Z})$

$A^2\,z = A\,(A\,z) = A\,z = z$ et $A\,B\,z = A\,(B\,z) = A\,z = z$.

Cela implique $A^n\,z = z$.

Par définition, une matrice elliptique A a une trace réelle tr A, $-2 < tr\,A < 2$

Cela implique les valeurs possibles tr A = -1, 0 ou 1

C'est la proposition 1.16 de Shimura.

Exemples:

1) les pointes du groupe modulaire $SL(2,\mathbb{Z})$ forment l'ensemble $\mathbb{Q} \cup \infty$**.**

2) la relation $S\,i = \frac{0i+1}{-i+0} = i$, implique que i est fixé par la matrice

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

donc z = i est un point elliptique pour le groupe modulaire $SL(2,\mathbb{Z})$.

4. Domaine fondamental du groupe modulaire:

Dans la théorie des groupes opérant sur un ensemble, il y a la notion de points équivalents par ce groupe.

Définition 7 :

Soit un sous groupe modulaire G de congruence; 2 points z et z' du demi-plan supérieur IH sont G-équivalents s'il existe une matrice A de G qui satisfait la relation :

$$A\,z = z'.$$

Cette relation est une relation d'équivalence dans le demi-plan supérieur IH. Elle détermine des classes d'équivalence IH/G.

La classe d'un nombre z du demi-plan supérieur IH est l'ensemble :

$$G\,z = \{A\,z;\ A \in G\}$$

Dans le langage de la théorie des groupes, cet ensemble $G\,z$ est l'orbite de z par le groupe G.
Cette relation d'équivalence détermine un sous ensemble particulier dans le demi-plan supérieur IH.

Définition 8 :

Le domaine fondamental d'un sous groupe G du groupe modulaire est le sous ensemble ouvert $D(G)$ du demi-plan supérieur IH qui satisfait les 2 conditions :

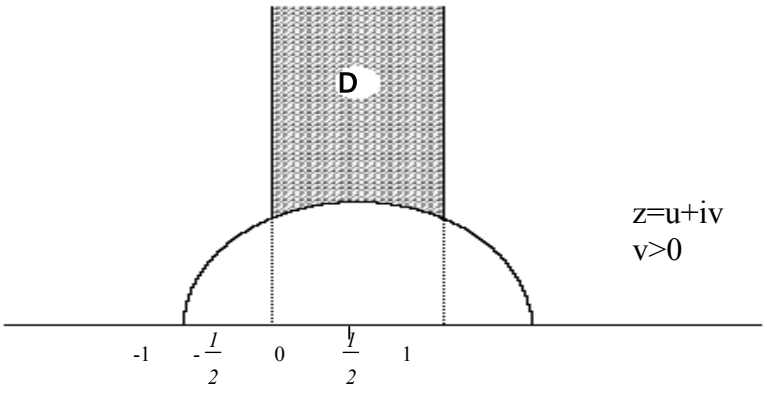
1) ***Il n'y a pas 2 points distincts de $D(G)$ qui soient G–équivalents***
2) ***Pour tout point $z \in IH$, il y a un point z' dans la clôture du domaine $D(G)$ qui est équivalent à G.***

Exemple :

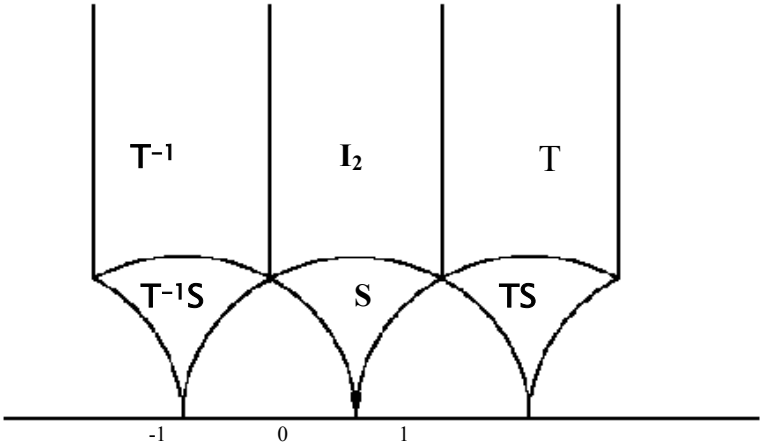
Domaine fondamental du groupe modulaire $SL(2,\mathbb{Z})$

Il est formé des points $z \in IH$ tels que

$|z| > 1$ $\quad\quad$ $|z+\bar{z}| < 1$



Images du domaine fondamental par les matrices S, T (Apostol)



5. Formes automorphes de poids k pour $SL(2,\mathbb{Z})$:

Nous nous intéressons à des fonctions particulières liées au groupe modulaire $SL(2,\mathbb{Z})$ sur le demi plan supérieur $\mathbb{H} = \{z = x+iy \in \mathbb{C},\ Im\ z = y > 0\}$: formes automorphes, fonctions modulaires et formes modulaires.

Définition 9:

Une forme automorphe de poids un entier k, par rapport au groupe modulaire $SL(2,\mathbb{Z})$ est une fonction méromorphe $f: \mathbb{H} \longrightarrow \mathbb{C}$ qui satisfait les 2 conditions:

1) $f(Az) = (cz+d)^k f(z)$ pour toute matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ du groupe modulaire $SL(2,\mathbb{Z})$

2) f est méromorphe en tout point parabolique du groupe modulaire $SL(2,\mathbb{Z})$.

C'est la définition 2-1 de Shimura.
Selon Apostol, une forme automorphe *f* admet un développement de Fourier de la forme:

$$f(z) = \sum_{-m \le n < +\infty} a_n\, q^n, \quad q = exp(2\pi i z). \tag{1}$$

Proposition 4:

Les fonctions automorphes pour un sous groupe modulaire $\Gamma_0(p)$ bornées dans le demi plan supérieur $\mathbb{H}$ sont constantes.

□

Exemple de fonction automorphe pour le sous groupe $\Gamma_0(k)$:
La fonction elliptique de Weierstrass attachée à un réseau complexe *L* est la série infinie:

$$\mathrm{P}(z,L) = \frac{1}{z^2} + \sum_{\omega \in L-\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right); \tag{1-1}$$

Soit le polynôme cubique $4x^3 - g_2(L)\, x - g_3(L)$, associée à la fonction elliptique $\mathrm{P}(z,L)$ de Weierstrass.
Son discriminant Δ admet un développement de Fourier:

$$\Delta(z) = (2\pi)^{12} \sum_{n\geq 1} \tau(n) q^n, \quad q = exp(2\pi i z), \quad z \in IH \qquad (1\text{-}2)$$

Alors les coefficients $\tau(n)$ sont des entiers, $\tau(1) = 1$, $\tau(2) = -24$, $\tau(3) = 252$, …

La fonction $\tau(n)$ est la fonction TAU de Ramanujan.

Proposition 5: (Apostol)

La fonction $f(z) = \Delta(kz) / \Delta(z)$, $z \in IH$ est une fonction automorphe pour le sous groupe $\Gamma_0(k)$

□

6. Formes modulaires:

Définition 10:

Une fonction modulaire de poids un entier k, par rapport au groupe modulaire $SL(2,\mathbb{Z})$ est une fonction méromorphe $f: IH \longrightarrow \mathbb{C}$ qui satisfait les 2 conditions:

1) $f(Az) = (cz+d)^k f(z)$ pour toute matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ du groupe modulaire $SL(2,\mathbb{Z})$.

2) f admet un développement de Fourier de la forme:

$$f(z) = \sum_{n=-m}^{\infty} c(n) q^n, \quad q = exp\,(2i\pi z).$$

Une forme modulaire est une fonction modulaire holomorphe même aux pôles.

Définition 11:

Une forme modulaire de poids k pour le groupe modulaire $SL(2,\mathbb{Z})$ est une fonction holomorphe $f: IH \longrightarrow \mathbb{C}$ qui satisfait les deux conditions:

1) $f(A z) = (cz + d)^k f(z)$, pour toute matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ du groupe modulaire $SL(2,\mathbb{Z})$.

2) f admet un développement de Fourier de la forme:

$$f(z) = \sum_{n \geq 0} c(n) q^n , \quad q = exp\ (2i\pi z), \text{ avec } f(\infty) = c(0).$$

Lorsque $c(0) = 0$, la forme modulaire est parabolique;

alors: $$f(z) = \sum_{n_f \leq n} c(n) q^n = c(n_f) q^{n_f} + ..., \quad n_f \succ 0. \qquad (1\text{-}3)$$

L'ensemble des formes modulaires f est classifié par le poids k:

Proposition 6:

1) ***les seules formes modulaires de poids k=0 sont les fonctions constantes.***
2) ***Lorsque k est impair et lorsque k = 0, les formes modulaires de poids k sont les fonctions nulles.***
3) ***Toute forme modulaire non nulle et non constante a un poids pair k ≥ 4.***
4) ***Les formes modulaires parabolique de poids k < 12 sont nulles.***

Preuve:

On utilise la formule du poids k d'une forme modulaire:

$$k = 12N + 6\ N(i) + 4\ N(\rho) + 12\ N(i\infty).$$

où N = nombre de zéros de f dans la clôture de la région fondamentale.

$N(x)$ = nombre de zéros de f aux points $x = i, \rho, i\infty$, $i^4 = 1$, $\rho^3 = 1$.

C'est le théorème 6-1, Apostol.

□

La représentation d'une forme modulaire de poids k dépend des séries d'Eisenstein:

$$G_k(z) = \sum_{(m,n) \neq (0,0)} \frac{1}{(m + nz)^k} \ . \qquad (1\text{-}4)$$

Proposition 7:

***Toute forme modulaire f de poids k est un polynôme*:**

$$f = \sum_{a,b} c(a,b)\ G_4^a\ G_6^b \in \mathbb{C}[G_4, G_6]$$

avec *a et b ≥0 et 4a + 6b = k*

□

Les formes modulaires de poids k forment un espace vectoriel complexe M_k

Sa dimension est précisée par les formules:

$$dim\ (M_k) = \begin{cases} \left[\frac{k}{12}\right] & \text{si } k \equiv 2 \bmod 12 \\ 1 + \left[\frac{k}{12}\right] & \text{si non} \end{cases} \qquad (1\text{-}5)$$

où $[x]$ = partie entière du nombre réel x.

L'ensemble des formes modulaires paraboliques de poids k est un sous espace $M_{k,0}$ de l'espace vectoriel complexe M_k des formes modulaires de poids k.

On en déduit la formule de la dimension

$$dim\ M_{k,0} = dim\ M_k - 1.$$

Exemples:

$dim\ M_k = 1$ lorsque $k = 4,6,8,10$ *et* 14;

$dim\ M_{k,0} = 1$ lorsque k = $12,16,18,20,22$et 26.

7. Opérateurs de Hecke T_n:

Les opérateurs T_n opèrent sur les espaces vectoriels M_k de formes modulaires.

Définition 12:

L'opérateur T_n de Hecke, n = 1,2,3,..., opère sur les formes modulaires f de poids k par la formule:

$$(T_n f)(z) = n^{k-1} \sum_{d/N} d^{-k} \sum_{b=0}^{d-1} f\left(\frac{nz + bd}{d^2}\right) \qquad \textbf{(2)}$$

Pour les nombres premiers p, cette formule devient :

$$(T_p f)(z) = p^{k-1} f(pz) + \frac{1}{p} \sum_{b=0}^{p-1} f\left(\frac{z + b}{p}\right) \qquad \textbf{(2-1)}$$

Proposition 8:

1) ***la transformée de Hecke $T_n f$ d'une forme modulaire de poids k, est une forme modulaire de poids k.***
2) ***la transformée de Hecke $T_n f$ d'une forme modulaire parabolique de poids k est une forme modulaire parabolique de poids k***

□

D'après Apostol, théorème 6. 12
La composée de 2 opérateurs de Hecke est déterminée par la:

Proposition 9:

Soient les opérateurs T_n de Hecke, n = 1,2,...Alors:

1) $T_m\ T_n = T_{m\,n}$ ***lorsque m et n sont premiers entre eux***
2) ***Lorsque m et n ne sont pas premiers entre eux, alors:***

$T_m\ T_n = \sum_{d/R} d^{k-1} T_{mn/d^2}$, ***où R = pgcd(m,n)***

Preuve:

Il faut faire les calculs avec les formules $(T_n f)(z)$.

□

8. Exemples de formes modulaires:

Il y a des formes classiques: discriminant, invariant modulaire, fonction Eta de Dedekind

Proposition 10:

Soit une courbe elliptique E/$\mathbb{C}$ de discriminant $\Delta(E)$ et d'invariant modulaire j(E) Alors:

1) ***L'invariant modulaire j(E) est une fonction modulaire de poids 0, holomorphe sur le demi plan supérieur $\mathbb{H}$. Sa série de Fourier est de la forme:***

$$j(z) = \frac{1}{q} + 744 + \sum_{n\geq 1} c(n) q^n, \quad c(n) \in \mathbb{Z} \text{ et } q = \exp(2\pi i t) \qquad \textbf{(2-2)}$$

2) ***le discriminant $\Delta(E)$ est une forme modulaire parabolique de poids 12. Sa série de Fourier est de la forme:***

$$\Delta(z) = (2\pi)^{12} q \sum_{n\geq 1} \left(1 - q^n\right)^{24} \qquad \textbf{(2-3)}$$

3) ***les séries d'Eisenstein $G_{2k}(z)$ sont des formes modulaires de poids 2k, leurs séries de Fourier sont de la forme:***

$$G_{2k}(z) = 2\xi(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n\geq 1}\sigma_{2k-1}(n)q^n \qquad (2\text{-}4)$$

avec $\xi(s)$= fonction Zêta de Riemann

$$\xi(2k) = (-1)^{k+1}\frac{(2\pi)^{2k}}{2(2k)!}B_{2k}. \qquad (2\text{-}5)$$

B_k = k ^{ième} nombre de Bernoulli

$\sigma_d(n)$ = somme des puissances d'ordre d des diviseurs de n ***(2-6)***

Preuve:

Les formules sont obtenues avec le calcul.

□

Définition 13:

La fonction Eta de Dedekind est la série infinie

$$\eta(z) = q^{\frac{1}{24}}\prod_{n\geq 1}(1-q^n), \quad q^{\frac{1}{24}} = exp\left(\frac{\pi it}{12}\right) \qquad (3)$$

Elle satisfait les relations:

$$\eta(z+1) = \eta(z)\ exp\left(\frac{\pi i}{12}\right) \text{ et } \eta\left(\frac{-1}{z}\right) = (-iz)^{1/2}\ \eta(z). \qquad (3\text{-}1)$$

La fonction Eta de Dedekind est une forme modulaire de poids $k = \frac{1}{2}$

la fonction $f(z) = \eta(z)^2\ \eta(11z)^2$ est une forme parabolique de poids *2* pour le sous groupe de congruence modulaire $\Gamma_0(11)$

Formes modulaires et discriminant Δ(z):

Soient les fonctions:

$$h^{24}(z) = -\Delta\left(\frac{z+1}{2}\right)\Big/\ \Delta(z);$$

$$h_1^{24} = -\Delta(z/2)/\Delta(z);$$

$$h_2^{24}(z) = 2^{12}\Delta(2z)/\Delta(z);$$

Selon Monsky, les 3 fonction *h, h_1,* et h_2 sont modulaires et holomorphes sur le demi plan supérieur *IH*. Il les a utilisées pour déterminer des points rationnels sur les courbes elliptiques d'équation de Weierstrass: $y^2 = x^3 + N\,x$.

Construction de formes modulaires par Ligozat:

Toute forme modulaire parabolique *f* de poids *2* sur le sous groupe modulaire $\Gamma_0(11)$ se développe en série de Fourier de la forme:

$$f(z) = \sum_{n \geq 1} a(n)\, q^n, \quad q = exp\ (2\pi iz)$$

La forme modulaire Eta de Dedekind implique plusieurs combinaisons (Ligozat):

$$f_1(z) = \eta(z)^2\ \eta(11z)^2 = q \prod_{n \geq 1} (1-q^n)^2 (1-q^{11n})^2$$

$$f_2(z) = f_1(z) - 11 f(11z);$$

$$g_1(z) = \eta(z)\ \eta(11z)^2\ \eta(121z) = q^6 \prod (1-q^n)(1-q^{11n})^2 (1-q^{121n}) \text{ (Ligozat)}$$

Avec les opérateurs T_n *de* Hecke, Ligozat a construit les formes modulaires:

$$f_3 = -(2 + 3T_2 + 2T_4 + T_8)(g_1) = q + 2q^2 - q^3 + 2q^4 + q^5 - 2q^6 + 2q^7 - 2q^9 + \ldots$$

$$f_4 = (2 - T_4 - T_8)(g_1) = q + q^2 + 2q^3 - q^4 + q^5 + 2q^6 - 2q^7 - 3q^8 + q^9 + \ldots$$

$$f_5 = -(2 - T_4 + T_8)(g_1) = q - q^2 + 2q^3 - q^4 + q^5 - 2q^6 + 2q^7 + 3q^8 + q^9 + \ldots$$

Ligozat a obtenu la Courbe Elliptique *E* d'équation de Weierstrass:

$$E : y^2 + xy + y = x^3 + x^2 - 305x + 7888\ .$$

en utilisant l'action des opérateurs de Hecke sur Γ_0(N) (dans ATKIN et LEHMER 1970) et les tables numériques de Courbes Elliptiques (dans Modular Functions of One Variable, IV, LNM, 476, BIRCH et KUYK, 1975.

Construction de formes modulaires avec les séries d'Eisenstein G_4 et G_6:

$$\boldsymbol{f} = \sum_{\boldsymbol{a,b}} \boldsymbol{c(a,b)}\ \boldsymbol{G_4^a}\ \boldsymbol{G_6^b} \in \mathbb{C}[\boldsymbol{G_4, G_6}] \qquad (1)$$

avec *a≥0 et b ≥0 et 4a + 6b = k*.

Nous avons résumé les résultats obtenus dans le tableau:

k	*f*	*série de Fourier de f*
12	$G_4^3 + G_6^2$	$1488375\,\pi^{12}(\ 23 + 5040z + 4399920z^2 + 387051840z^3 + 9147363120z^4 + 106500108960z^5 + 791575606080z^6 + 4312184123520z^7 + 18742660599600z^8 + \ldots)$

14	$G_4^2 G_6$	$1913625\,\pi^{14}\,(2 - 48z - 393264z^2 - 76527552z^3 - 3221618736z^4 - 58593750048z^5 - 626990233536z^6 - 4650672499584z^7 - 26391500685360z^8 + \ldots)$
16	$G_4 G_6^2$	$40186125\,\pi^{16}\,(4 - 3072z - 76032z^2 + 269316096z^3 + 19336683264z^4 + 550623467520z^5 + 8488442704896z^6 + 85675772633088z^7 + 635043263880960z^8 + \ldots)$
18	$G_4^3 G_6$	$86113125\,\pi^{18}\,(2 + 432z - 400464z^2 - 171001152z^3 - 22437968976z^4 - 999725273568z^5 - 22169343180096z^6 - 304692764310144z^7 - 2949382547061840z^8 + \ldots)$
20	$G_4^2 G_6^2$	$1808375625\,\pi^{20}\,(4 - 2112z - 804672z^2 + 244459776z^3 + 83787743424z^4 + 5772585582720z^5 + 184213690189056z^6 + 3446907156515328z^7 + 43579372598182080z^8 + \ldots)$
22	$G_4 G_6^3 + G_4^4 G_6$	$63293146875\,\pi^{22}\,(46 - 2064z - 91152z^2 - 3153251136z^3 - 1433419768848z^4 - 155906935005024z^5 - 7170542654683968z^6 - 182568560023519872z^7 - 3014818740990239760z^8 + \ldots)$

les calculs sont faits avec le logiciel Magma.

Construction de formes modulaires avec la fonction Eta de Dedekind:

Ligozat a utilisé des résultats de Newman concernant la fonction Eta de Dedekind (dans "construction and application of a class of modular functions", Proc.London Math. Soc.(3) 7 (1957).) pour obtenir certaines formes modulaires paraboliques de poids 2 sur $\Gamma_0(N)$ de la forme:

$$g_r(z) = \prod_{\delta / N} \eta(\delta z)^{r\delta};$$

r_δ entier positif indexé par les diviseurs δ de N.

δ' l'entier défini par $\delta\,\delta' = N$.

Les formes paraboliques associées aux niveaux N = 11, 14, 15, 20, 24, 27, 32, 36 sont rassemblées par le tableau:

N	$g(z)$	*série de Fourier de g*
11	$\eta(z)^2\eta(11z)^2$	$q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} + \ldots$

14	$\eta(z)\,\eta(2z)\,\eta(7z)\eta\,(14z)$	$q-q^2-2q^3+q^4+2q^6+q^7-q^8+q^9+\ldots$
15	$\eta(z)\,\eta(3z)\,\eta(5z)\eta\,(15z)$	$q-q^2-q^3-q^4+q^5+q^6+3q^8+q^9+\ldots$
20	$\eta(2z)^2\,\eta(10z)^2$	$q-2q^3-q^5+2q^7+q^9+\ldots$
24	$\eta(2z)\,\eta(4z)\,\eta(6z)\eta\,(12z)$	$q-q^3-2q^5+q^9+4q^{11}-2q^{13}+\ldots$
27	$\eta(3z)^2\,\eta(9z)^2$	$q-2q^4-q^7+5q^{13}+\ldots$
32	$\eta(4z)^2\,\eta(8z)^2$	$q-2q^5-3q^9+6q^{13}+\ldots$
36	$\eta(6z)^4$	$q-4q^7+2q^{13}+8q^{19}+\ldots$

CHAPITRE IV – *Courbes Modulaires*

1. Introduction:

Dans les chapitres précédents nous avons étudié la structure du groupe modulaire $\Gamma = SL(2,\mathbb{Z})$ et ses sous groupes modulaires de congruence principaux de niveau $N \geq 1$.

$\Gamma_0(N)$, $\Gamma_1(N)$, $\Gamma(N)$.

ces groupes opèrent sur le demi plan supérieur:

$\mathbb{H} = \{ z \in \mathbb{C}, Im\, z \succ 0 \}$.

par une transformation homographique.

L'ensemble des points fixes d'un groupe modulaire de congruence est formé des points elliptiques d'ordre 2 et 3 et de pointes.

le demi plan $\mathbb{H}$ est complété par l'ensemble $\mathbb{Q} \cup \{\infty\}$.

$\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$.

2. Espaces quotients $\mathbb{H}^*/G$, $G = \Gamma_0(N)$, $\Gamma_1(N)$, $\Gamma(N)$:

Une étude approfondie de ces espaces se trouve dans plusieurs publications et ouvrages comme:

(1)*" Introduction to the Arithmetic Theory of Automorphic Functions"* Princeton University Press-(1971), par G. SHIMURA.

1.5 The quotient $\Gamma / \mathbb{H}^*$ as a Riemann surface. 1.6 Congruence subgroups of $SL(2,\mathbb{Z})$.

2.5 The measure of $\Gamma / \mathbb{H}$.

Définition 1:

Une surface de Riemann est une surface analytique complexe de dimension 1.

Définition 2:

Une surface de Riemann est un espace de Hausdorff $\mathfrak{B}$ ***muni de la " structure complexe S " satisfaisant les propriétés:***

a) S est une collection de paires (U_α, p_α), α ***dans un ensemble d'indices avec un recouvrement ouvert*** $\{U_\alpha\}$ ***de la surface*** $\mathfrak{B}$ ***et un homéomorphisme:***

$p_\alpha : U_\alpha \longrightarrow E$, *E est un sous ensemble ouvert de l'espace* $\mathbb{C}$.

b) Soient 2 ouverts U_α *et* U_β *d'intersection* $U_\alpha \cap U_\beta$ *non vide. Alors l'application:*

$p_\beta \circ p_\alpha^{-1} : p_\alpha(U_\alpha \cap U_\beta) \longrightarrow p_\beta(U_\alpha \cap U_\beta)$ *est holomorphe.*

c) Cette collection S de paires (U_α, p_α) *est maximale sous les 2 conditions précédentes.*

(2) ***" Rational points on the jacobians of modular curves "*** Math-Sbornik-USSR 30 (1976) 478-500.

(3) ***"Rational points and Eiseinstein ideal "*** Publi. IHES 47-Paris (1977). Par MAZUR.

(4) ***" Rational isogenies of prime degree "*** Inv Math 44 (1978) 129-162 par MAZUR.

(5) ***" Modular Curves and Diophantine Equations "*** Math. Jap.25-(1980) 245 – 250 par ISHI classification AMS; 10D05 et 10B10.

(6) ***"The Arithmetic of Elliptic Curve "*** GTM 106 (1986), par J.H.SILVERMAN.

D'après ces références, les quotients du demi plan $\mathcal{H}$ par les sous groupes modulaires de congruence de niveau N sont les "courbes" :

$Y_0(N)$, $Y_1(N)$ et $Y(N)$.

Ces courbes sont compactifieés dans le demi plan $\mathcal{H} \cup \mathbb{Q} \cup \{\infty\} = \mathcal{H}^*$ et deviennent des courbes compactes:

$X_0(N)$, $X_1(N)$ et $X(N)$ de niveau N.

Nous nous intéressons aux courbes modulaires $X_0(N)$.

Le corps de fonctions d'une telle courbe modulaire $X_0(N)$ est le corps K engendré par la fonction modulaire $j(z)$.

$K = \mathbb{Q}(j(z), j_N(z))$, $z \in \mathcal{H}$, $j_N(z) = j(Nz)$.

A chaque nombre z de l'éspace $\mathcal{H}^*/\Gamma_0(N)$ il correspond une classe de courbes elliptiques ayant un point d'ordre N .

La fonction modulaire j induit un isomorphisme analytique complexe d'espace quotient:

$j : \mathbb{H} / SL(2,\mathbb{Z}) \longrightarrow A$, A = variété sur $\mathbb{Q}$.

Selon Silverman, il existe pour tout entier $N \geq 1$ une courbe projective lisse $X_0(N) / \mathbb{Q}$ et un isomorphisme analytique complexe d'espace quotient:

$$j : \mathbb{H}^* / \Gamma_0(N) \longrightarrow X_0(N)(\mathbb{C});$$

qui satisfait les propriétés:

a) à tout nombre $z \in \mathbb{H} / \Gamma_0(N)$ il correspond un corps $K = \mathbb{Q}(j(z))$ et une classe d'équivalence de courbes elliptiques E ayant un sous groupe cyclique C de points d'ordre N.

b) cette classe contient une courbe elliptique E / K et le sous groupe cyclique C d'ordre N est invariant par le groupe de Galois $G(K_{alg} / K)$.

c) La fonction invariant modulaire est égale à:

$$j(z) = \frac{1}{q} + 744 + \sum_{n \geq 1} c(n) q^n \ , \ c(n) \in \mathbb{Z} \ \text{ et } q = exp(2\pi iz).$$

3. Construction de courbes modulaires:

Pour la construction de courbes modulaires il y a plusieurs méthodes qui ont été utilisées:

1) Méthode de Fricke:

La méthode basée sur des équations explicites a permis à Fricke d'obtenir l'équation:

$$F_N : u^2 = av^4 + bv^3 + cv^2 + dv + 2 \ ;$$

Ces résultat se trouvent dans:
" Die elliptischer Funktionen und ihre Ansvend ungen, II, Teubner, Leipzig – Berlin, (1922), par Fricke.

L'équation $F_N(u,v)$ est transformée en équation en x, y par des changements dépendant du niveau N de $\Gamma_0(N)$.

Pour $N = 11$, les résultats sont:

$$a = 1,\ b = -20,\ c = 56,\ d = -44,\ e = 0,\ u = \frac{-11(2y+1)}{(x-5)^2} \ et \ v = \frac{-11}{x-5}.$$

Pour $N = 14$, les résultats sont:

$a = 1,\ b = -14,\ c = 19,\ d = -14,\ e = 1,\ u = \dfrac{(2y + x + 57)^2}{4(x - 9)^2} - 2(x - 9) - \dfrac{109}{4}$ *et*

$v = \dfrac{2y + x + 57}{2(x - 9)} + \dfrac{7}{2}.$

Pour $N = 19$, les résultats sont:

$a = 1,\ b = -16,\ c = 64,\ d = -76,\ e = 0,\ u = \dfrac{-19(2y + 1)}{(x - 5)^2}$ et $v = \dfrac{-19}{x - 5}.$

Pour $N = 20$, les résultats sont:

$a = 0,\ b = 2,\ c = 13,\ d = 30,\ e = 25,\ u = \dfrac{y}{2},$ et $v = \dfrac{x - 4}{2}.$

Pour $N = 21$, les résultats sont:

$a = 1,\ b = -6,\ c = -17,\ d = -6,\ e = 1,\ u = \dfrac{(2y + x + 21)^2}{4(x - 5)^2} - 2(x - 5) - \dfrac{61}{4}$ et

$v = \dfrac{(2y + x + 21)}{2(x - 5)} + \dfrac{3}{2}.$

Pour $N = 36$, les résultats sont:

$a = 0,\ b = 1,\ c = 6,\ d = 12,\ e = 9,\ u = y,\ v = x - 2.$

Pour $N = 49$, les résultats sont:

$a = 1,\ b = -14,\ c = 63,\ d = -98,\ e = 21,\ u = \dfrac{(2y + x)^2}{4(x - 2)^2} - 2(x - 2) - \dfrac{21}{4}$ *et*

$v = \dfrac{2y + x}{2(x - 2)} + \dfrac{7}{2}.$

2) Méthode de Ligozat:

La méthode utilisée par Ligozat est basée sur la théorie des groupes fuchsiens de première espèce et sur l'équation modulaire de niveau N liant les fonctions j et j_N.

$\Phi_N(j, j_N) = 0.$

cette équation est un polynôme de l'anneau $\mathbb{Z}[X, Y]$; elle définit une courbe algébrique plane irréductible non singulière.

La courbe modulaire $X_0(N)$ est obtenue par extension des scalaires sur le corps $K = \mathbb{Q}(j, j_N)$.

où $j_N(N) = j(Nz)$ et $j(z)$ = invariant modulaire.

Le genre de cette courbe $X_0(N)$ est égal au nombre:

$$p_0(N) = 1 + \frac{\mu_0}{12} - \frac{\mu_2}{4} - \frac{\mu_3}{3} - \frac{\mu_\infty}{2}.$$

où $\mu_0 = N\prod_p\left(1+\frac{1}{p}\right)$ pour les diviseurs premiers p de N.

$\mu_2 = 0$ si $N \equiv 0 \bmod 4$ et $\mu_2 = \prod_p\left(1+\left(\frac{-1}{p}\right)\right)$ si $N \not\equiv 0 \bmod 4$.

$\mu_3 = 0$ si $N \equiv 0 \bmod 9$ et $\mu_3 = \prod_p\left(1+\left(\frac{-3}{p}\right)\right)$ si $N \not\equiv 0 \bmod 9$.

$\mu_\infty = \sum_d \varphi(d, N/d)$, $d =$ diviseurs de N.

les symboles de Legendre $\left(\frac{-1}{p}\right)$ et $\left(\frac{-3}{p}\right)$.

$\varphi(n) =$ fonction arithmétique d'Euler.

Ligozat a déterminé les courbes modulaires $X_0(N)$ pour les genres $p_0(N) = 0, 1$ et 2:

15 courbes $X_0(N)$ de genre *0* pour les entiers N:

N = *1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18* et *25*;

12 courbes $X_0(N)$ de genre *1* pour les entiers N:

N = *11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36* et *49*.

8 courbes $X_0(N)$ de genre *2* pour les entiers N :

N = *22, 23, 26, 28, 29, 31, 37* et *50*;

Proposition 1:

Les courbes modulaires $X_0(N)$ de genre $p_0(N) = 1$ sont des courbes modulaires elliptiques.

Le conducteur de ces courbes $X_0(N)$ est égal à N.

□

La courbe elliptique $X_0(11)$ a été étudiée par Velu.

Swinnerton – Dyer a établi une liste de courbes elliptiques de petit conducteur.
Ishi a utilisé l'équation diophantienne $x^3 - 27y^2 = 1$ pour obtenir une courbe modulaire elliptique de même équation.
Mestre (1980) a utilisé les propriétés des pointes pour le sous groupe $\Gamma_0(N)$ de niveau N pour la courbe modulaire $X_0(169)$.

4. Courbes modulaires et leurs jacobiennes:

Soit une courbe modulaire $X_0(N) = X$ et le groupe $Div(X)$ des classes de diviseurs de la courbe X. Alors la jacobienne de la courbe X est la courbe isomorphe au groupe $Pic^0(X)$ des diviseurs de degré *0*.

$J(X) \approx Pic^0(X)$;

Exemples:

1) ***Silverman*** (Homogeneous spaces)

Soit la courbe hyperelliptique:

$$C : dw^2 = d^2 - 2\,a\,d\,z^2 + \left(a^2 - 4b\right)z^4 ;$$

transformée de la courbe elliptique:

$$E : y^2 = x^3 + ax^2 + bx ;$$

par le changement :

$$\phi : E \longrightarrow C$$

$$(x, y) \longrightarrow (z, w)$$

$$d \in \mathbb{N},\ z = \frac{x\sqrt{d}}{y},\ w = \sqrt{d}\left(x - \frac{b}{x}\right)\left(\frac{x}{y}\right)^2 .$$

Alors, le groupe $Pic^0(C)$ des diviseurs de degré *0* de a courbe *C* est isomorphe à la jacobienne de la courbe elliptique *E*.

2) ***Mestre*** (Points rationnels de la courbe modulaire $X_0(169)$. Grenoble. Ann. Inst. Fourier (1980/ 17 – 27).

Soit une Courbe modulaire $X_0(N)$ et les pointes de sous groupe $\Gamma_0(N)$.

Alors, le morphisme:

$X_0(N)(\mathbb{Q}) \longrightarrow Div(X_0(N))$ = groupe des diviseurs de la courbe $X_0(N)$

$x \longrightarrow (x) - (\infty)$, où (x) = diviseur de x

applique l'ensemble des pointes sur un groupe fini.

3) Ligozat a déterminé un modèle singulier de la courbe modulaire $X(26)$:

$$y^2 = x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1.$$

La jacobienne $J(26)$ de $X(26)$ est isogène au produit de 2 courbes elliptiques de conducteur $N = 26$.

Proposition 2:

Il existe 12 courbes elliptiques définies sur $\mathbb{Q}$ qui sont quotients de la jacobienne $J_0(121)$ de la courbe modulaire $X_0(121)$ de niveau $N = 121$.

trois d'entre elle ont pour conducteur N = 11 et sont liées par des isogénies de degré 5.
les neuf autres courbes elliptiques ont pour conducteur 121 et sont liées par des isogénies de degré 5 ou 11.

4) ***Mazur et Tate*** (Points of order 13 on Elliptique Curves – Inv – Math, 22 (1973), 41 - 49).

La courbe modulaire $X_1(13)$ de niveau 13 est de genre $g = 2$

Elle est isomorphe au produit de 2 courbes elliptiques isogènes

Sa jacobienne $J_1(13)$ a une structure de variété abelienne de dimension 2 sur le corps $\mathbb{Q}$ des rationnels; elle admet une mauvaise réduction au seul nombre premier 13.
L'étude des points rationnels de la jacobienne $J_1(13)$ a montré les résultats de la:

Proposition 3:

1) ***La jacobienne $J_1(13)$ de la courbe modulaire $X_1(13)$ possède exactement 19 points rationnels.***
2) ***Les 6 pointes $\mathbb{Q}$- rationnelles de $X_1(13)$ sont les seuls points $\mathbb{Q}$- rationnels de cette courbe.***
3) ***Il n'y a pas de courbe elliptique sur le corps $\mathbb{Q}$ qui possède un point rationnel d'ordre 13.***

5. Fonction L de Dirichlet de courbes modulaires:

Selon SHIMURA [16], ATKIN –LEHMER [2] et LIGOZAT [9]:

Soit un sous groupe fuschien de première espèce du groupe $SL(2,\mathbb{R})$ et une fonction holomorphe:

$$f: \mathbb{H}^* \longrightarrow \mathbb{H}^*$$

qui satisfait:

$$f(z) = (az+b)^{-k} \; f\left(\frac{az+b}{cz+d}\right), A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \subset \; SL(2,\mathbb{R}).$$

Lorsque f est modulaire de poids 2, elle satisfait:

$f(Az) = (az+b)^2 \; f$ et f holomorphe aux pointes de G.

Lorsque f est parabolique de poids 2, elle satisfait:

$f(Az) = (az+b)^2 \; f$ et f est nulle aux pointes aux pointes de G.

Chaque forme modulaire f admet un développement en série de Fourier en $z = i\infty$:

$$f(z) = \sum_{n \geq 0} a(n) q^n, \; q = exp(2\pi i z).$$

Elle admet une série de Dirichlet de la forme:

$$D(s) = \sum_{n \geq 1} a(n) n^{-s}.$$

la série est normalisée lorsque $a(1) = 1$.

Les opérateurs de Hecke T_n admettent un développement en produit lorsque $G = \Gamma_0(N)$.

Proposition 4:

Les opérateurs T_n de Hecke opèrent sur les formes modulaires paraboliques de poids 2 pour le sous groupe $\Gamma_0(N)$.

Ils admettent une série de Dirichlet:

$$\sum_{n\geq 1} \tau(n) n^{-s} = \prod_{p} \left(1 - \tau(p) p^{-s} + u(p) p^{1-2s}\right)^{-1}$$

où p = diviseurs premiers de n

$u(p) = 0$ si p divise N et $u(p) = 1$ si p ne divise pas N.

□

En particulier, lorsque la forme parabolique f est normalisée et vecteur propre de $T(n)$ pour $n \geq 1$, alors elle satisfait:

$T_n(f) = \lambda(n) f$.

Sa série de Dirichlet est égale à:

$$D(s) = \sum_{n\geq 1} a(n) n^{-s} = \prod_{p} \left(1 - \lambda(p) p^{-s} + u(p) p^{1-2s}\right)^{-1}$$

où p = diviseurs premiers de n, $u(p) = 0$ si p divise N, $u(p) = 1$ si p ne divise pas N.

La fonction L de Dirichlet d'une courbe modulaire elliptique $X = X_0(N)$ associée à un sous groupe modulaire $\Gamma_0(N)$ est un produit de facteurs locaux $L_p(X,s)$:

$$L(X,s) = \prod_{p} L_p(X,s);$$

Ce produit est obtenu avec un modèle de Néron en X dont la fibre est lisse.

Lorsque X a une mauvaise réduction en p. alors la fibre Y de Néron est isomorphe:

soit à une extension du groupe multiplicatif sur IF_p, alors :

$$L_p(X,s) = \left(1 - p^{-s}\right)^{-1};$$

soit à une telle extension sur $IF_p{}^2$, alors :

$$L_p(\chi,s) = \left(1 + p^{-s}\right)^{-1};$$

soit à une extension du groupe additif , alors:

$$L_p(\chi,s) = 1;$$

Le facteur local $L_p(\chi_0(N),s)$ est lié aux opérateurs de Hecke:

Proposition 5:

Soit une courbe modulaire $\chi_0(N)$ elliptique qui a une bonne réduction en un nombre premier p. Alors le facteur local L_p est égal à:

$$L_p(\chi_0(N),s) = \left(\det\left(1 - T_p p^{-s} + p^{1-2s}\right)\right)^{-1}$$

□

(D'après Eichler et Shimura).

La fonction $L(N, s)$ d'une courbe modulaire elliptique $\chi_0(N)$ satisfait à l'équation fonctionnelle:

$$Z(N, s) = Z(N, 2- s);$$

où $Z(N, s) = (2\pi)^{-s} N^{\frac{s}{2}} \Gamma(s) L(N, s)$, $\Gamma(s) = \int_0^\infty t^{s-1} exp(-t)\, dt$.

6. Formes modulaires paraboliques primitives:

Les formes paraboliques f de poids 2 pour $\Gamma_0(N)$ forment un $\mathbb{C}$-espace vectoriel $M(N, 2)$ de dimension 1.

Soit un diviseur d de N et un diviseur t de N/d.

Alors pour toute forme g de l'espace $M\left(\frac{N}{d}, 2\right)$, les formes modulaires $g_t(z) = g(tz)$ sont des formes modulaires de l'espace $M(N, 2)$.

Définition 3:

1) ***les formes $g_t(z)$ ci-dessus sont des formes non primitives (" old forms " de Atkin et Lehner)***
2) ***les formes primitives sont les formes $h(z) \in M(N, 2)$ orthogonales aux formes non primitives $g_t(z)$ pour le produit scalaire de Peterson, et vecteurs propres de $T(n)$ pour tout entier n premier à N.***

A ces formes sont associées des matrices particulières :

B_p et B_N.

Soit un diviseur premier p de N tel que:

$$N \equiv 0 \bmod p^r \text{ et } N \not\equiv 0 \bmod p^{r+1}$$

et des entiers u et v tels que:

$$v p^{2r} - u N = p^r;$$

Soit les 2 matrices:

$$B_p = p^{\frac{-r}{2}} \begin{pmatrix} p^r & u \\ N & vp^r \end{pmatrix} \text{ et } B_N = N^{\frac{-r}{2}} \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix};$$

Alors les endomorphismes de l'éspace vectoriel $M(N, 2)$:

$$M(N, 2) \longrightarrow M(N, 2)$$

$$f \longrightarrow B_p f$$

et:

$$M(N, 2) \longrightarrow M(N, 2)$$

$$f \longrightarrow B_N f$$

sont les involutions $W_p(f)$ et $W_N(f)$ de l'espace $M(N, 2)$:

$$W_p(f) = B_p f \text{ et } W_N(f) = B_N f$$

Alors une forme primitive f est un vecteur propre de l'opérateur $T(n)$ de Hecke pour $n \geq 1$ et vecteur propre de l'involution W_p

Les involutions W_p et W_N possèdent des propriétés:

Proposition 6:

***Soient les involutions W_p et W_N ci-dessus. Alors*:**

1) $W_N^2 \equiv 1$, $W_p^2 \equiv 1 \mod \Gamma_0(N)$.

2) $\prod_p W_p \equiv W_N \mod \Gamma_0(N)$, p **divise** N.

3) W_p ***et*** W_N ***sont contenus dans le normalisateur du sous groupe*** $\Gamma_0(N)$.

□

Exemples:

Pour $N = 14$, la matrice $B_7 = \begin{pmatrix} -21 & 8 \\ -56 & 21 \end{pmatrix} 7^{\frac{-1}{2}}$

et $B_2\ B_7 \equiv B_{14} \mod \Gamma_0(14)$

Pour $N = 21$, la matrice $B_3 = 3^{\frac{-1}{2}} \begin{pmatrix} 3 & -1 \\ -21 & -6 \end{pmatrix}$

Ces résultats permettent de calculer la valeur au point $s = 1$ des courbes modulaires elliptiques.

7. Courbes modulaires $X_0(N)$, $X_1(N)$ et $X(N)$:

Ogg a construit les courbes modulaires elliptiques:

$X_0(24)$ et $X_0(36)$.

Hadans a construit les courbes modulaires $X_0(N)$ pour :

$N = 14,20$ et 36.

Miyaki a construit les courbes modulaires $X_0(N)$ pour :

$N = 11,17$ et 19 et 27.

Nous avons étudié les courbes modulaires $X_0(N)$ au moyen des espaces quotients $IH^*/\Gamma_0(N)$.

les sous groupes de congruences modulaires $\Gamma_1(N)$ et $\Gamma(N)$ sont en correspondance avec les espaces quotients correspondants.

Proposition 7:

1) ***A tout sous groupe de congruences $\Gamma_1(N)$ il correspond une courbe projective lisse $X_1(N)(\mathbb{Q})$ et un isomorphisme analytique complexe:***

$$h_1 : /H^*/\Gamma_1(N) \longrightarrow X_1(N)(\mathbb{C})$$

qui satisfait les propriétés:

à tout nombre $z \in /H/\Gamma_1(N)$ il correspond une paire (E,T) de classes d'équivalence formées d'une courbe elliptique E et d'un point $T \in E(\mathbb{Q})$ d'ordre N.

cette classe contient une courbe elliptique $E/K = \mathbb{Q}(h_1(z))$ et un point d'ordre N sur le groupe E(K).

2) ***A tout sous groupe de congruence modulaire $\Gamma(N)$ il correspond une courbe projective lisse $X(N)$ et un isomorphisme analytique complexe:***

$$h : /H^*/\Gamma(N) \longrightarrow X(N)(\mathbb{C})$$

qui satisfait les propriétés:

a tout nombre $z \in /H/\Gamma(N)$ il correspond des classes d'équivalence (E, T_1, T_2) formées d'une courbe elliptique E et deux points T_1 et T_2 qui engendrent le sous groupe $E[N]$ de $N-$torsion de $E(\mathbb{Q})$.

ces deux générateurs satisfont $e_N(T_1, T_2) = z_N$ = racine primitive $N-$éme de 1(e_N est l'application bilinéaire de Weil)

la classe d'équivalence (E, T_1, T_2) contient une courbe elliptique E sur le corps $K = \mathbb{Q}(z_N, h(z))$, les points T_1 et T_2 sont sur le groupe E(K).

(d'après J. H. Silverman, théorème 13.1)

□

Dans le vocabulaire des courbes modulaires, une courbe modulaire $X_0(N)$ est une courbe de Weil. Ces courbes sont donc paramétrisées par les fonctions modulaires .

Conjecture:

Toute courbe elliptique E / $\mathbb{Q}$ est une courbe modulaire elliptique.

Il y a un $\mathbb{Q}$ - morphisme surjectif f : $X_0(N) \longrightarrow$ E pour toute courbe elliptique de conducteur N.

C'est la conjecture de Taniyama – Weil. Elle a été vérifié pour quelques valeurs de N par Birch swinnerton – Dyer, Katz, Mazur .

Dans une thèse ultérieure, nous pensons à étudier de façon approfondie les courbes modulaires du point de vue isogénie, isomorphisme et multiplication complexe.
Nous suivons la méthode de Cremona exposée dans l'ouvrage " Algorithms for Modular Elliptic Curves "(1997), l'auteur a calculé les coefficients $a_1,\ldots a_6$, le rang $r(E(\mathbb{Q}))$, l'ordre du groupe de torsion $T(E(\mathbb{Q}))$ pour les courbes elliptiques E de conducteur $N(E)$ de *11 à 999,* sauf pour certaines valeurs $N = 12, 13, 16, 18, 25,\ldots 991, 992, 993, 998.$