UNIVERSITÉ PARIS XI
U.E.R. MATHÉMATIQUE
91405 ORSAY FRANCE

# COURBES MODULAIRES DE GENRE 1

par M. LIGOZAT

n° 75 7411

# COURBES MODULAIRES DE GENRE 1

Résumé d'auteur.

On désigne par $\Gamma_0(N)$ le sous-groupe du groupe modulaire $SL(2,\mathbb{Z})$ formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que $c \equiv 0 \pmod{N}$. Au groupe $\Gamma_0(N)$ est associée de façon canonique une courbe algébrique $X_N$ projective et lisse sur le corps $\mathbb{Q}$ des nombres rationnels, et que l'on appelle la "courbe modulaire de niveau N". Ce travail traite essentiellement des douze courbes modulaires qui sont des courbes de genre 1. Ces dernières, munies d'une structure de courbe elliptique canonique, sont appelées "courbes modulaires elliptiques".

On établit tout d'abord le résultat suivant: le conducteur de la courbe modulaire elliptique $X_N$ est égal à son niveau $N$, et on explique de quelle façon ce résultat peut être généralisé.

On montre d'autre part que la fonction L d'une courbe modulaire elliptique coïncide avec la série de Dirichlet canoniquement associée aux formes paraboliques de poids 2 sur le groupe $\Gamma_0(N)$. Cela permet de calculer la valeur de la fonction $L(s)$ au point $s = 1$. On vérifie alors que les résultats obtenus sont compatibles avec la conjecture de Birch et Swinnerton-Dyer. Enfin, on obtient des résultats analogues pour certaines courbes elliptiques isogènes sur $\mathbb{Q}$ aux courbes modulaires elliptiques.

## 0. Introduction

Le but de ce travail est l'étude de certaines courbes algébriques, associées aux sous-groupes $\Gamma_0(N)$ du groupe modulaire $SL(2,\mathbb{Z})$, que nous appellerons les courbes modulaires, et particulièrement de celles d'entre elles, les courbes modulaires elliptiques, qui sont des courbes de genre 1. Ces dernières sont canoniquement munies d'une structure de courbe elliptique (c'est-à-dire de variété abélienne de dimension 1) définie sur le corps $\mathbb{Q}$ des nombres rationnels. Nous nous proposons d'en faire une description aussi complète que possible: conducteur, fonction L, points rationnels, et d'examiner la compatibilité des résultats obtenus avec la conjecture de Birch et Swinnerton-Dyer.

0.1. Soit $N$ un entier positif. On désigne par $\Gamma_0(N)$ le sous-groupe du groupe modulaire $SL(2,\mathbb{Z})$ formé des matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{telles que} \quad c \equiv 0 \pmod{N}.$$

Le groupe $\Gamma_0(N)$ opère sur le demi-plan de Poincaré $\mathcal{H}$. On désigne par $\mathcal{H}^*$ la réunion de $\mathcal{H}$ et des pointes de $\Gamma_0(N)$. Le quotient de $\mathcal{H}^*$ par l'action de $\Gamma_0(N)$ est alors une surface de Riemann compacte $X_{N,\mathbb{C}}$. On constate que la courbe algébrique sur le corps $\mathbb{C}$ des complexes que l'on obtient de cette façon provient par extension des scalaires d'une courbe algébrique définie sur $\mathbb{Q}$, dont le corps des fonctions est $\mathbb{Q}(j,j_N)$. Ici $j(z)$ est la fonction invariant modulaire de la variable complexe $z$, et $j_N(z) = j(Nz)$.

On désigne par $X_N$, et on appelle courbe modulaire de niveau N, un modèle de $\mathbb{Q}(j,j_N)$ projectif et lisse sur $\mathbb{Q}$.

Les courbes modulaires nous intéressent à deux titres:

0.2. D'une part, il résulte d'une conjecture de Weil que toute courbe elliptique définie sur $\mathbb{Q}$, de conducteur $N$, est isomorphe sur $\mathbb{Q}$ à un quotient de $J_N$, variété jacobienne de la courbe modulaire $X_N$.

0.3. D'autre part, la fonction L de la courbe $X_N$ s'exprime essentiellement (à savoir à un nombre fini de facteurs près) comme un produit eulérien ne dépendant que des valeurs propres de l'action des opérateurs de Hecke sur l'espace des formes paraboliques de poids 2 attaché à $\Gamma_0(N)$.

0.4. La courbe modulaire $X_N$ est de genre 1 pour douze valeurs de N :

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

On la munit alors canoniquement d'une structure de variété abélienne définie sur $\mathbb{Q}$, et on appelle courbe modulaire elliptique de niveau N la courbe elliptique ainsi obtenue. La fonction L d'une courbe elliptique est définie sans ambiguité, et nous montrons que celle de la courbe modulaire elliptique $X_N$ coïncide avec la série de Dirichlet canoniquement associée à l'action des opérateurs de Hecke. Cela nous permet de calculer la valeur de la fonction L(s) au point $s = 1$, en employant une méthode due à Swinnerton-Dyer.

On peut rapprocher ces résultats de ceux obtenus pour une courbe elliptique admettant une multiplication complexe. La fonction L d'une telle courbe s'obtient comme série L associée à un certain "Grössencharakter" et l'on peut faire dans certains cas le calcul explicite de L(1)(cf. [35]).

0.5. Le paragraphe 1 est essentiellement consacré aux propriétés de réduction des courbes modulaires. Le résultat suivant est obtenu pour les courbes modulaires elliptiques:

THÉORÈME A (1.4.2). Le conducteur de la courbe modulaire elliptique $X_N$ est égal à N.

Pour une courbe modulaire de genre non-nécessairement égal à 1, on indique comment certains résultats de Deligne permettent de déterminer le conducteur de la jacobienne $J_N$ de $X_N$, du moins lorsque N est un entier sans facteurs carrés(1).

0.6. On étudie dans le paragraphe 2 la fonction L d'une courbe modulaire. Cette fonction est définie par un produit eulérien dont les facteurs locaux $L_p$ sont définis pour presque tout nombre premier p. Dans le cas particulier d'une courbe elliptique, on sait définir $L_p$ pour tout p, et la fonction L de la courbe elliptique est le produit de tous les $L_p$.

THÉORÈME B (2.2.3). La fonction L de la courbe modulaire elliptique $X_N$ coïncide avec la série de Dirichlet canoniquement associée au groupe $\Gamma_0(N)$.

La démonstration de ce théorème utilise les résultats des calculs explicites des paragraphes 3 et 4. Elle est achevée en (4.3.4).

Le théorème B entraîne en particulier:

THÉORÈME C (2.3.2). Soit L(N,s) la fonction L de la courbe modulaire elliptique $X_N$, et soit $\Xi(N,s) = (2\pi)^{-s}.N^{s/2}.\Gamma(s).L(N,s)$.

Alors $\Xi(N,s)$ est une fonction entière, bornée dans toute bande verticale, et vérifie l'équation fonctionnelle

$$\Xi(N,s) = \Xi(N,2-s).$$

Les résultats précédents apparaissent comme des conséquences, dans le cas particulier des courbes modulaires elliptiques, d'une conjecture de Weil. On montre comment les résultats du paragraphe 1 concernant le conducteur de la jacobienne $J_N$ d'une courbe modulaire se généralisent

(1) Cf. note au bas de la p.26.

de façon conjecturale pour un niveau N quelconque.

0.7. Le paragraphe 3 est consacré à la construction explicite de formes modulaires sur le groupe $\Gamma_0(N)$. A coté de la détermination effective de la série de Dirichlet canoniquement associée aux courbes modulaires de genre 1, on établit de façon élémentaire le

THÉORÈME D (3.2.16). Désignons par $P_1$ , $P_N$ les points de la courbe modulaire $X_N$ images des points z=0, z=i de $\mathfrak{h}$ par l'application canonique. Alors le diviseur $P_1 - P_N$ a une image d'ordre fini dans le groupe des classes de diviseurs modulo l'équivalence linéaire.

De plus, on peut donner une détermination explicite de cet ordre.

0.8. A partir du paragraphe 4 , on s'occupe exclusivement des douze courbes modulaires elliptiques. On utilise tout d'abord les calculs faits par Fricke pour écrire une équation explicite de $X_N$ . On peut alors calculer le conducteur de $X_N$ en utilisant un théorème de Ogg, et vérifier ainsi le théorème A. On détermine également les facteurs locaux $L_p$ de la fonction L de $X_N$ pour les valeurs de p telles que $X_N$ ait mauvaise réduction en p. On termine ainsi la démonstration du théorème B.

0.9. On démontre dans le paragraphe 5 le

THÉORÈME E. Le groupe $X_N(\mathbb{Q})$ des points de la courbe modulaire elliptique $X_N$ rationnels sur $\mathbb{Q}$ est un groupe fini, et engendré par les pointes de $\Gamma_0(N)$ qui sont rationnelles sur $\mathbb{Q}$. (théorèmes (5.5.1) et (5.2.5)).

0.10. Le paragraphe 6 est consacré à la conjecture de Birch et Swinnerton-Dyer, et au calcul de la valeur au point s = 1 de la fonction L "normalisée" $L^*(s)$. On obtient:

THÉORÈME F (6.3.3). Soit $L^*(N,s)$ la fonction L normalisée de la courbe modulaire elliptique $X_N$, et soit $\eta_0(N)$ l'ordre du groupe $X_N(\mathbb{Q})$. Alors

$$L^*(N,1) = (\eta_0(N))^{-2}.$$

Ce résultat est en accord avec la conjecture de Birch et Swinnerton-Dyer, et il entraine, si l'on admet cette dernière, que le groupe de Tate-Šafarevič des courbes modulaires elliptiques est trivial.

0.11. Enfin, on montre au paragraphe 7 comment le calcul de $L^*(1)$ peut être étendu à toutes les courbes elliptiques de conducteur $N \in \mathfrak{M}_1$ que l'on connaît explicitement (on désigne par $\mathfrak{M}_1$ l'ensemble des entiers N tels que $X_N$ soit de genre 1). On utilise une liste des courbes elliptiques de petit conducteur dressée par Swinnerton-Dyer. Comme on l'indique en 7.5.1, il est probable que cette liste contient toutes les courbes elliptiques de conducteur $N \in \mathfrak{M}_1$.

Pour chacune des courbes de la liste, on trouve comme plus haut:

$$L^*(1) = \eta_0^{-2}$$

et la conclusion concernant le groupe de Tate-Šafarevič est la même.

Ce travail n'aurait pas été mené à bien sans les conseils et les encouragements d'A. Néron. Je tiens à lui exprimer ici ma vive reconnaissance, ainsi qu'à G. Poitou et M. Raynaud. Enfin, J.P. Serre a bien voulu lire mon manuscrit. Il m'est agréable de lui exprimer ma gratitude pour ses remarques stimulantes.

7. Application à certaines courbes isogènes.

7.1. Fonction L normalisée et isogénies.

7.2. Parasites.

7.3. Paramétrisation de Weierstrass.

7.4. Isogénies de noyau cyclique.

7.5. Application aux courbes de la liste de Swinnerton-Dyer de conducteur $N \in \mathcal{M}_1$.

# 1. LES COURBES MODULAIRES $X_N$.

## 1.1. Groupes fuchsiens de première espèce.

Dans ce qui suit, on s'intéresse à certains sous-groupes G de $\underset{\sim}{SL}(2,\underset{\sim}{R})$, commensurables à $\underset{\sim}{SL}(2,\underset{\sim}{Z})$, et contenant $-1$. En particulier, G est un groupe fuchsien de première espèce au sens de [32].

On désigne par $\mathfrak{h}$ le demi-plan de Poincaré, et par $\mathfrak{h}^*$ la réunion de $\mathfrak{h}$ et des pointes de G. Le quotient $G\backslash\mathfrak{h}^*$ de $\mathfrak{h}^*$ par l'action de G est une surface de Riemann compacte $X_{G,\underset{\sim}{C}}$.

Si G et G' sont deux tels groupes, et si G' est un sous-groupe de G d'indice n dans G, l'homomorphisme d'inclusion $G' \longrightarrow G$ induit un revêtement de degré n des surfaces de Riemann. L'indice de ramification $e_{P'}$ en un point P' de $X_{G',\underset{\sim}{C}}$ est alors donné par

$$e_{P'} = \left(\mathrm{Stab}_G(z) : \mathrm{Stab}_{G'}(z)\right) \quad \text{où } z \in \mathfrak{h} \text{ a pour image } P'$$

et $\mathrm{Stab}_G(z)$ désigne le stabilisateur de z dans G.

Si $p_G$, $p_{G'}$ désignent les genres de $X_{G,\underset{\sim}{C}}$, $X_{G',\underset{\sim}{C}}$, la formule de Riemann-Hurwitz s'écrit

$$2p_{G'} - 2 = n(2p_G - 2) + \sum_{P \in X_{G',\underset{\sim}{C}}} (e_P - 1).$$

On se reportera à [32] pour plus de détails.

1.2. La courbe modulaire de niveau N

On désigne par $\Gamma_0(N)$ le sous-groupe du groupe $SL(2,\mathbb{Z})$ formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que $c \equiv 0 \pmod{N}$, et par $X_{N,\mathbb{C}}$ la surface de Riemann correspondante. Le corps des fonctions de $X_{N,\mathbb{C}}$ est $\mathbb{C}(j,j_N)$, où $j(z)$ est la fonction invariant modulaire, et $j_N(z) = j(Nz)$.

On sait que $j$ et $j_N$ sont liées par l'équation modulaire de niveau N :

$$\Phi_N(j,j_N) = 0 \qquad (1.2.1)$$

où $\Phi_N \in \mathbb{Z}[X,Y]$ est un polynôme absolument irréductible [13]. La courbe $X_{N,\mathbb{C}}$ projective et lisse sur $\mathbb{C}$ s'obtient donc par extension des scalaires à partir de la normalisée projective sur $\mathbb{Q}$ de la courbe plane définie par

$$\Phi_N(X,Y) = 0.$$

On désigne par $X_N$, et on appelle courbe modulaire de niveau N cette normalisée; c'est l'unique courbe projective et lisse sur $\mathbb{Q}$ dont le corps des fonctions est $\mathbb{Q}(j,j_N)$.

On dira qu'un $\mathbb{Z}$-schéma $\mathcal{X}_N$, plat et surjectif sur $\mathbb{Z}$, est un $\mathbb{Z}$-modèle de $X_N$, si la fibre générique de $\mathcal{X}_N$ est isomorphe à $X_N$.

Les images des points $z = 0$, $z = i\infty$ de $\mathfrak{h}^*$ dans $X_N$ sont des points $P_1$ et $P_N$ rationnels sur $\mathbb{Q}$ ([15,2.1.]). On convient de choisir comme morphisme canonique de $X_N$ dans sa jacobienne $J_N$ celui qui envoie $P_N$ sur l'origine de $J_N$. Lorsque $X_N$ est une courbe de genre 1, on dira que $X_N$, munie de la structure de courbe elliptique (c'est à dire de variété abélienne de dimension 1) d'élément neutre $P_N$, est la courbe modulaire elliptique de niveau N.

1.3. Genre de $X_N$.

Désignons par $p_0(N)$ le genre de $X_N$. La considération du revêtement associé à l'inclusion canonique de $\Gamma_0(N)$ dans $SL(2,\mathbb{Z})$ permet de calculer $p_0(N)$ en fonction de N [32, 27, 12]. On obtient

$$p_0(N) = 1 + \frac{\mu_0}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

où

$$\mu_0 = N \cdot \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

$$\nu_2 = \begin{cases} 0 & \text{si } N \equiv 0 \pmod 4 \\ \prod_{p|N} \left(1 + \left(\frac{-1}{p}\right)\right) & \text{sinon} \end{cases}$$

$$\nu_3 = \begin{cases} 0 & \text{si } N \equiv 0 \pmod 9 \\ \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{sinon} \end{cases}$$

$$\nu_\infty = \sum_{\substack{d|N \\ d>0}} \varphi((d, N/d)) .$$

Dans ces formules $\left(\frac{\cdot}{p}\right)$ désigne le symbole de Legendre, $(d,N/d)$ le pgcd de d et N/d, et $\varphi$ la fonction d'Euler.

En particulier, $p_0(N)$ tend vers l'infini avec N.

On désigne par $\mathcal{M}_k$ l'ensemble des entiers N tels que $p_0(N) = k$. Par exemple:

$$\mathcal{M}_0 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\},$$
$$\mathcal{M}_1 = \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\},$$
$$\mathcal{M}_2 = \{22, 23, 26, 28, 29, 31, 37, 50\}.$$

1.4. Propriétés de réduction.

Igusa [12] a démontré le résultat suivant:

PROPOSITION 1.4.1. *Il existe un $\underset{\sim}{Z}$-modèle normal de $X_N$ projectif sur $\underset{\sim}{Z}$ et lisse sur $\underset{\sim}{Z}[\frac{1}{N}]$.*

Lorsque $N \in \mathfrak{M}_1$, on obtient un résultat beaucoup plus précis. Avant de l'énoncer, on rappelle qu'à toute variété abélienne A définie sur $\underset{\sim}{Q}$ est associé un entier qu'on appelle le conducteur de A. On renvoie à [30], [10] pour la définition et les propriétés du conducteur de A, qu'on note $\chi(A)$. On a

$$\chi(A) = \prod p^{e_p(A)}$$

où $e_p(A)$, exposant en p du conducteur de A, est nul si et seulement si A a bonne réduction en p.

Soit $N \in \mathfrak{M}_1$:

THÉORÈME 1.4.2. *Le conducteur de la courbe modulaire elliptique $X_N$ est égal à N.*

Démonstration. On déterminera explicitement, en (4.2.4), une équation de chacune des courbes modulaires elliptiques. Le tableau (6.3.4) indique le type des fibres singulières du modèle de Néron (les notations sont celles de Néron [20]). La vérification de (1.4.2) se fait alors au moyen du théorème de Ogg (4.3.2) et (4.3.3).

1.4.3. Soit N un entier sans facteurs carrés. Alors, d'après Deligne et Rapoport [6], il existe un $\underset{\sim}{Z}$-modèle de $X_N$, soit $\mathcal{X}_N$, lisse sur $\underset{\sim}{Z}[\frac{1}{N}]$, régulier, dont la fibre en p, pour p divisant N, de genre arithmétique $p_0(N)$, s'obtient en recollant transversalement en $s_N(p)$ points deux exemplaires de la fibre en p de $\mathcal{X}_{N/p}$. Ici $s_N(p)$ désigne le nombre des classes de courbes supersingulières en caractéristique p, munies d'un sous-groupe cyclique d'ordre N/p.

On a donc, écrivant que le genre arithmétique de la fibre en p est $p_0(N)$:

(1.4.3.1) $$p_0(N) = 2p_0(N/p) + s_N(p) - 1 \ .$$

Désignant par $J_N$ la jacobienne de $X_N$, il en résulte que le modèle de Néron (au sens faible) de $J_N$ a une fibre en p sans partie unipotente, et dont la partie torique est de dimension $s_N(p) - 1$. L'exposant en p du conducteur de $J_N$ est donc

$s_N(p) - 1 = p_0(N) - 2p_0(N/p)$, d'où le conducteur $\chi(J_N)$ de $J_N$ :

(1.4.3.2) $$\chi(J_N) = \prod_{p \mid N} p^{p_0(N) - 2p_0(N/p)}$$

Lorsque $N \in \mathcal{M}_1$ est sans facteurs carrés, on retrouve le résultat du théorème 1.4.2. On verra en (2.6.3) comment on peut formuler une conjecture généralisant ce résultat pour N quelconque(2).

(2) Cf. note au bas de la p. 26.

# 2. FONCTION L DES COURBES MODULAIRES.

## 2.1. Rappels et notations.

On se contente dans ce paragraphe de préciser les notations, et l'on renvoie pour plus de détails au livre de Shimura [32] et à l'article d'Atkin-Lehner [1].

Soit G un sous-groupe (fuchsien de première espèce) de $SL(2,\mathbb{R})$. Si f(z) est une fonction holomorphe dans $\mathfrak{h}$, et si $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, on désigne par $f\left|\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right.$ la fonction

$$z \longmapsto (az+b)^{-2} \cdot f\left(\frac{az+b}{cz+d}\right).$$

On désigne par $\langle G,2 \rangle$ (resp. $\langle G,2 \rangle_0$) l'espace des formes modulaires (resp. des formes paraboliques) de poids 2 sur G, c'est à dire des fonctions f telles que:

(i) $f\left|\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right. = f$ pour tout élément $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de G,

(ii) f est holomorphe aux pointes de G (resp. f est nulle aux pointes de G).

Soit $f \in \langle G,2 \rangle$. Alors f est développable en série de Fourier au voisinage de la pointe à l'infini $i\infty$ de G:

$$f(z) = \sum_{n=0}^{\infty} a_n \cdot \exp(2\pi i n z) \quad . \tag{2.1.0}$$

DÉFINITION 2.1.1. La série de Fourier (2.1.0) est appelée série de Fourier de f. On appelle série de Dirichlet de f la série

$$D(s) = \sum_{n=1}^{\infty} a_n \cdot n^{-s} \quad .$$

On dit que la série de Fourier, ou la série de Dirichlet de f est normalisée si $a_1 = 1$.

On rappelle que l'application $f \longmapsto f(z)dz$ est un isomorphisme de $\mathbb{C}$-espaces vectoriels de $\langle G,2 \rangle_0$ avec l'espace des formes différentielles de première espèce sur la surface de Riemann associée à G.

On suppose maintenant que $G = \Gamma_0(N)$.

On renvoie à Ogg[27] pour la définition des opérateurs de Hecke $T(n)$ $(n \geq 1)$ et leurs propriétés. $T(n)$ est un opérateur sur l'espace vectoriel $\langle \Gamma_0(N), 2 \rangle$. On utilisera la

PROPOSITION 2.1.2. Les opérateurs de Hecke vérifient l'identité formelle:

$$\sum_{n=1}^{\infty} T(n).n^{-s} = \prod_{p \text{ premier}} (1-T(p).p^{-s}+\varepsilon'(p).p^{1-2s})^{-1}$$

où $\varepsilon'(p) = 0$ si $p$ divise $N$, $\varepsilon'(p) = 1$ sinon.

En particulier, si $f$ est normalisée et vecteur propre de $T(n)$ pour tout $n$, soit

$$f \mid T(n) = \lambda(n).f$$

on a, désignant par $D(s)$ la série de Dirichlet de $f$:

$$D(s) = \sum_{n=1}^{\infty} a_n.n^{-s} = \prod_{p \text{ premier}} (1-a_p.p^{-s}+\varepsilon'(p).p^{1-2s})^{-1} \quad \text{où } a_p=\lambda(p).$$

On définit dans $\langle \Gamma_0(N), 2 \rangle_0$ un produit scalaire, le produit scalaire de Petersson, qui fait de $\langle \Gamma_0(N), 2 \rangle_0$ un espace hermitien. Les opérateurs de Hecke sont alors des opérateurs hermitiens, d'où la possibilité de trouver une base orthogonale de $\langle \Gamma_0(N), 2 \rangle_0$ formée de vecteurs propres des opérateurs $T(n)$, pour tout $n$ premier à $N$.

Lorsque $N \in \mathcal{M}_1$, l'espace vectoriel $\langle \Gamma_0(N), 2 \rangle_0$ est de dimension 1 sur $\mathbb{C}$, et toute forme parabolique $f$ non-nulle est vecteur propre de $T(n)$ pour tout $n$. D'autre part, il résultera de (2.4) que $f$ peut être choisie normalisée. On peut donc énoncer:

PROPOSITION 2.1.3. Soit $N \in \mathcal{M}_1$, et soit $f \in \langle \Gamma_0(N), 2 \rangle_0$ la forme parabolique normalisée associée. Alors la série de Dirichlet de $f$ admet un produit eulérien

$$(2.1.3.1) \qquad D(s) = \prod_{p \text{ premier}} (1-\lambda(p).p^{-s}+\varepsilon'(p).p^{1-2s})^{-1}$$

où $\varepsilon'(p) = 0$ si p divise N , $\varepsilon'(p) = 1$ sinon, et où $\lambda(p)$ est la valeur propre de l'action de $T(p)$ sur f : $f|T(p) = \lambda(p).f$.

2.2. Résultat fondamental.

Soit X une courbe projective et lisse définie sur $\mathbb{Q}$. S'il existe un $\mathbb{Z}$-modèle $\mathcal{X}$ de X dont la fibre en p est lisse, la fonction zêta de la fibre en p s'écrit $Z(\mathcal{X}_p,u) = P(u).(1-u)^{-1}.(1-pu)^{-1}$. On pose alors

$$L_p(X,s) = P(p^{-s}),$$

et $L(X,s) = \prod L_p(X,s)$ , le produit portant sur tous les p vérifiant les conditions précédentes.

Lorsque X est une courbe elliptique définie sur $\mathbb{Q}$ , on définit également des facteurs locaux en p lorsque X a mauvaise réduction en p. Pour cela, soit $\mathcal{X}$ le modèle de Néron (au sens faible [20]) de X. Si X a mauvaise réduction en p, la fibre de $\mathcal{X}$ en p est:

Soit isomorphe sur $\mathbb{F}_p$ à une extension du groupe multiplicatif par un groupe fini, et on pose

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

soit isomorphe sur $\mathbb{F}_{p^2}$, et non sur $\mathbb{F}_p$, à une telle extension et on pose

$$L_p(X,s) = (1+p^{-s})^{-1} ;$$

soit enfin isomorphe à une extension du groupe additif par un groupe fini et on pose

$$L_p(X,s) = 1 .$$

La fonction L de X est le produit des facteurs locaux $L_p$ pour tout p premier.

En particulier, lorsqu'on parlera de la fonction L d'une courbe modulaire elliptique, il s'agira toujours de la fonction de la courbe considérée comme courbe elliptique.

Soit N un entier $\geqslant 1$, et soit p un nombre premier tel que la courbe modulaire $X_N$ possède un $\mathbb{Z}$-modèle lisse en p. Le résultat suivant est dû

à Eichler [8] et a été généralisé par Shimura [31, 32]:

PROPOSITION 2.2.1. Le facteur local de la fonction L de la courbe modulaire $X_N$ en p premier de bonne réduction est donné par

(2.2.1.1) $$L_p(X_N,s) = (\det(1-T(p).p^{-s}+p^{1-2s}))^{-1}.$$

Il résulte de (1.4.1) que cette proposition s'applique pour tout p ne divisant pas N. Lorsque $N \in \mathfrak{M}_1$, les nombres premiers p de mauvaise réduction sont exactement les diviseurs premiers de N, d'après (1.4.2). Comparant dans ce dernier cas (2.2.1.1) et (2.1.3.1), on obtient:

PROPOSITION 2.2.2. Soit $N \in \mathfrak{M}_1$, et soit p un nombre premier ne divisant pas N. Alors le facteur local en p de la fonction L de la courbe modulaire elliptique $X_N$ coïncide avec celui de la série de Dirichlet normalisée associée à $\Gamma_0(N)$.

On peut maintenant énoncer le résultat fondamental:

THÉORÈME 2.2.3. Soit $N \in \mathfrak{M}_1$. La fonction L de la courbe modulaire elliptique $X_N$ coïncide avec la série de Dirichlet normalisée associée à $\Gamma_0(N)$.

La proposition (2.2.2) montre qu'il suffit de vérifier que les facteurs locaux des deux séries en question coïncident en p, pour p divisant N. Cette vérification sera faite en (4.3.4), en utilisant les résultats de (4.2.4) et de (3.1.3).

## 2.3. Conséquences.

Le résultat du théorème (2.2.3) va permettre:

(i) De calculer la valeur au point $s = 1$ de la fonction L des courbes modulaires elliptiques. Cela sera fait au paragraphe 6.

(ii) De déterminer explicitement l'équation fonctionnelle à laquelle satisfait la fonction L des courbes modulaires elliptiques, ce qui constitue dans ce cas particulier une vérification des conjectu-

res classiques [29, 35]. En effet, rappelons la

PROPOSITION 2.3.1. Soit N un entier positif, et soit $f \in \langle \Gamma_0(N), 2 \rangle_0$ une forme parabolique de poids 2. Désignons par D(s) la série de Dirichlet de f, et posons

$$\Lambda(s) = (2\pi)^{-s} \cdot \Gamma(s) \cdot D(s).$$

Alors, si $f = -C \cdot f \left| \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \right.$

on a:

(i) $\Lambda(s) + N^{s/2} \cdot \left( \frac{a_0}{s} + C \cdot \frac{a_0}{2-s} \right)$ est une fonction entière bornée dans toute bande verticale.

(ii) $\Lambda(s) = C \cdot N^{1-s} \cdot \Lambda(2-s)$. (cf. [27, V-10, th.1.6]).

Soit maintenant $N \in \mathfrak{M}_1$, et $f \in \langle \Gamma_0(N), 2 \rangle_0$ la forme parabolique normalisée.

D'après le théorème (2.2.3), la série de Dirichlet de f est la fonction L de la courbe modulaire elliptique $X_N$. D'autre part, d'après le théorème (1.4.2), N est le conducteur de $X_N$. Enfin, d'après (2.5.4), on a $f \left| \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \right. = -f$. On peut donc appliquer (2.3.1), avec C = 1:

THÉORÈME 2.3.2. Soit $N \in \mathfrak{M}_1$, et désignons par L(N,s) la fonction L de la courbe modulaire elliptique $X_N$. Soit

$$\Xi(N,s) = (2\pi)^{-s} \cdot N^{s/2} \cdot \Gamma(s) \cdot L(N,s).$$

Alors $\Xi(N,s)$ est une fonction entière, bornée dans toute bande verticale, et satisfait à l'équation fonctionnelle:

$$\Xi(N,s) = \Xi(N,2-s).$$

2.4. Formes primitives.

Soient N' un diviseur positif de N, et t un diviseur positif de N/N'. Alors, pour tout élément g de $\langle \Gamma_0(N'),2 \rangle_0$ , les formes modulaires $g_t(z) = g(tz)$ sont des éléments de $\langle \Gamma_0(N),2 \rangle_0$ .

DÉFINITION 2.4.1. On appelle espace des formes non primitives ("old forms" dans [1]) le sous-espace de $\langle \Gamma_0(N),2 \rangle_0$ engendré par les formes $g_t(z)$, où $g \in \langle \Gamma_0(N'),2 \rangle_0$ , t parcourant les diviseurs positifs de N/N', et N' les diviseurs positifs de N distincts de N.

On appelle forme primitive("new form") tout élément non nul de $\langle \Gamma_0(N),2$ qui est orthogonal à l'espace des formes non primitives pour le produit scalaire de Petersson, et vecteur propre de T(n) pour tout n premier à N.

On démontre ([1, lemme 9 p. 45]) que le premier terme $a_1$ de la série de Fourier d'une forme primitive est non nul. On peut donc toujours la normaliser (2.1.1).

Les formes primitives normalisées forment une base canonique de l'espace orthogonal à l'espace des formes non primitives. Les formes primitives sont alors les multiples non nuls des vecteurs de base.

Notations. Soit p un diviseur premier de N. On suppose que $N \equiv 0 \pmod{p^r}$, $N \not\equiv 0 \pmod{p^{r+1}}$. Choisissant des entiers $u,v \in \underset{\sim}{Z}$ tels que $p^{2r} v - N u = p^r$ , on pose

$$W_p = p^{-\frac{r}{2}} \begin{pmatrix} p^r & u \\ N & p^r v \end{pmatrix} .$$

On pose également

$$W_N = N^{-\frac{r}{2}} \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} .$$

Soit $f \in \langle \Gamma_0(N),2 \rangle_0$ . Les applications $f \mapsto f|W_p$ , $f \mapsto f|W_N$ sont des endomorphismes linéaires de $\langle \Gamma_0(N),2 \rangle_0$ , le premier ne dépendant pas du choix de u et v.

On désigne encore par $W_p$ , $W_N$ les involutions de $\langle \Gamma_0(N),2 \rangle_0$ obtenues de cette façon.

On démontre qu'une forme primitive est vecteur propre de $T(n)$ pour tout $n$, et vecteur propre de $W_p$ ( $p$ divise $N$). De plus

$$f|T(p) = 0 \quad \text{si } p^2|N ,$$
$$f|T(p) * f|W_p = 0 \quad \text{si } p|N,\ p^2\not|N. \quad \text{(cf. [1, th.3 p.149])}.$$

On peut donc énoncer:

PROPOSITION 2.4.3. *Soit* $f = \sum_{n=1}^{\infty} \lambda(n).\exp(2\pi i n z)$ *une forme primitive normalisée. Alors* $f$ *est vecteur propre de* $T(n)$ *pour tout* $n$, *avec la valeur propre* $\lambda(n)$. *La série de Dirichlet associée à* $f$ *s'écrit:*

$$D(s) = \sum_{n=1}^{\infty} \lambda(n).n^{-s} = \prod_{(p,N)=1} (1 - \lambda(p).p^{-s} + p^{1-2s})^{-1} . \prod_{\substack{p|N \\ p^2\not|N}} (1 + w_p.p^{-s})^{-1}$$

*où* $w_p = \pm 1$ *est défini par*

$$f|W_p = w_p.f .$$

REMARQUE 2.4.4. *Lorsque* $N \in \mathcal{N}_1$ , *tout élément non-nul de* $\langle \Gamma_0(N), 2 \rangle_0$ *est une forme primitive.*

## 2.5. Morphismes canoniques.

Reprenant les notations de (2.4), on désigne par $N'$ un diviseur positif de $N$, et par $t$ un diviseur positif de $N/N'$. On désigne par $M(t)$ la matrice $\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}$. Dans ces conditions

$$M(t).\Gamma_0(N).M(t)^{-1} \hookrightarrow \Gamma_0(N').$$

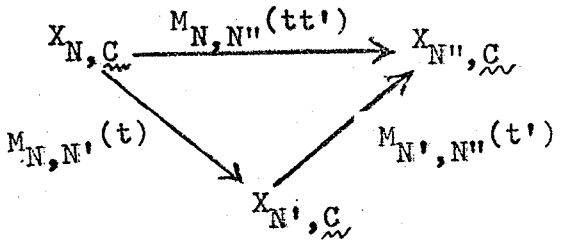
Il en résulte que $M(t)$ définit un morphisme canonique

$$M_{N,N'}(t) : X_{N,\underset{\sim}{C}} \longrightarrow X_{N',\underset{\sim}{C}}$$

décrit par le diagramme commutatif

$$\begin{array}{ccc} \mathcal{H}_0^* & \xrightarrow{z \longmapsto tz} & \mathcal{H}_0^* \\ \downarrow & & \downarrow \\ X_{N,\underset{\sim}{C}} & \xrightarrow{M_{N,N'}(t)} & X_{N',\underset{\sim}{C}} \end{array} \qquad \text{(cf [32, 6.7])}$$

où les flèches verticales sont les morphismes canoniques d'espaces analytiques complexes. Si $N''$ divise $N'$, et $d'$ divise $N'/N''$, le diagramme suivant est commutatif




Il résulte de [32, 6.7] que $M_{N,N'}(t)$ provient d'un morphisme défini sur $\underset{\sim}{Q}$, que l'on note de la même façon

$$M_{N,N'}(t) : X_N \longrightarrow X_{N'} .$$

Soit $\omega = f(z)dz$ une forme différentielle de première espèce sur $X_{N'}$. Alors $(M_{N,N'}(t))^*(\omega) = f(tz)dz$. On obtient donc une forme non primitive sur $\Gamma_0(N)$, si $N' \neq N$.

Soit $J_N$ la jacobienne de $X_N$. Avec les conventions faites en (1.2), $M_{N,N'}(t)$ induit un morphisme de $\underset{\sim}{Q}$-variétés abéliennes

$$M_{N,N'}(t) : J_N \longrightarrow J_{N'} ,$$

d'où un morphisme

$$M_N : J_N \longrightarrow \prod_{\substack{N' \mid N \\ N' \neq N}} (J_{N'})^{\sigma_0(N/N')}$$

induit par les $M_{N,N'}(t)$ pour $N'$ parcourant les diviseurs positifs de $N$ distincts de $N$, et $t$ les diviseurs positifs de $N/N'$. Ici $\sigma_0(n)$ désigne le nombre de diviseurs positifs de $n$.

On définit par récurrence sur $N$ une sous-variété abélienne de $J_N$:

NOTATION 2.5.1 <u>On note $J_N^0$ la composante connexe du noyau de $M_N$</u>.

Il est clair par construction qu'une base des formes différentielles invariantes sur $J_N^0$ est de la forme $\{f_i(z)dz\}$ où $\{f_i\}$ est une base de l'espace des formes primitives associées à $\Gamma_0(N)$. On en conclut que $M_N$ se factorise à travers le produit

$$\prod_{\substack{N' \mid N \\ N' \neq N}} (J_{N'}^0)^{\sigma_0(N/N')}$$

de sorte qu'on obtient une isogénie sur $\underset{\sim}{Q}$

$$(2.5.2) \qquad M_N^0 = J_N \xrightarrow{\sim} \prod_{N'|N} (J_{N'}^0)^{\sigma_0(N/N')} \quad .$$

Désignons par $\Gamma_0^*(N)$ (resp. $\Gamma_{0,p}(N)$) le sous-groupe de $\underset{\sim}{SL}(2,\underset{\sim}{R})$ engendré par $\Gamma_0(N)$ et $W_N$ (resp. $W_p$), avec les notations de (2.4). Il est immédiat que

(i) $W_N^2 = 1$ , $W_p^2 \equiv 1$ (modulo $\Gamma_0(N)$),

(ii) $\prod_{p|N} W_p \equiv W_N$ (modulo $\Gamma_0(N)$),

(iii) $W_N$, et $W_p$ sont contenus dans le normalisateur de $\Gamma_0(N)$ dans $\underset{\sim}{SL}(2,\underset{\sim}{R})$.

Le groupe $\Gamma_0(N)$ est donc d'indice 2 dans $\Gamma_0^*(N)$ (resp. $\Gamma_{0,p}(N)$). $W_N$, $W_p$ définissent des automorphismes de la surface de Riemann $X_{N,\underset{\sim}{C}}$ (et même de la courbe algébrique sur $\underset{\sim}{Q}$ d'après [32, 6.7]). On désigne encore par $W_N$, $W_p$ ces involutions.

Le revêtement canoniquement associé à l'inclusion de $\Gamma_0(N)$ dans $\Gamma_0^*(N)$ (resp. $\Gamma_{0,p}(N)$) correspond au quotient de $X_N$ par le groupe d'automorphismes d'ordre 2 $\{1, W_N\}$ (resp. $\{1, W_p\}$).

Supposons maintenant que $N \in \mathcal{M}_1$. Soit $f: X \to Y$ un revêtement de degré 2, où X est de genre 1. Alors, ou bien f est non-ramifié, et Y est de genre 1, ou bien f est ramifié en quatre points, et Y est de genre 0. On se trouve dans le second cas si et seulement si l'involution de X associée admet des points fixes.

D'autre part, les automorphismes involutifs d'une surface de Riemann de genre 1 sont de deux sortes: Si l'on choisit une origine, on obtient une involution de la courbe elliptique obtenue, donc , ou

bien une translation par un point d'ordre 2, ou bien une translation suivie d'une symétrie par rapport à l'origine.

On conclut des remarques précédentes:

CONSÉQUENCE.(2.5.3) Soit $N \in \mathfrak{M}_1$. Alors la surface de Riemann associée à $\Gamma_0^*(N)$ est de genre 0.

En effet, $z_0 = -i.N^{-1/2} \in \mathcal{H}$ est un point fixe de $W_N$.

CONSÉQUENCE.(2.5.4) Soit $N \in \mathfrak{M}_1$, et $f \in \langle \Gamma_0(N), 2 \rangle_0$. Alors $f|W_N = -f$.

En effet, $f|W_N = f$ entraîne $f \in \langle \Gamma_0^*(N), 2 \rangle_0$, donc f=0 d'après (2.5.3)

CONSÉQUENCE.(2.5.5) Soit $N \in \mathfrak{M}_1$, N premier (donc N = 11, 17, ou 19). Alors $f|T(N) = f$. (cf. [11, Satz 1 p.776])

Cela résulte de ce qui précède et de (2.4.3). Plus généralement:

PROPOSITION 2.5.6. Soit $N \in \mathfrak{M}_1$, et p un diviseur premier de N. Alors $f|W_p = -f$ si et seulement si $W_p$ admet des points fixes. Sinon $f|W_p = f$.

(2.5.7) Applications. Examinons le cas de deux valeurs particulières de $N \in \mathfrak{M}_1$.

**N = 14.** On peut représenter $W_7$ par la matrice

$$W_7 = \begin{pmatrix} -21 & 8 \\ -56 & 21 \end{pmatrix}.7^{-1/2}.$$

Le point $z_0 = (21+i\sqrt{7})/56$ est un point de $\mathcal{H}$ fixe sous $W_7$. On a donc, tenant compte de ce que $W_2.W_7 = W_{14}$ (modulo $\Gamma_0(14)$):

$$\begin{cases} f|W_2 = f \\ f|W_7 = -f \end{cases} \quad \text{donc} \quad \begin{cases} f|T(2) = -f \\ f|T(7) = f \end{cases}$$

pour $f \in \langle \Gamma_0(14), 2 \rangle_0$.

En particulier, $W_2$ correspond à une involution de la courbe modulaire elliptique $X_{14}$ qui est une translation par un point d'ordre

2 rationnel sur $\mathbb{Q}$.

**N = 21** On peut représenter $W_3$ par la matrice

$$W_3 = \begin{pmatrix} 3 & -1 \\ -21 & -6 \end{pmatrix} .3^{-1/2} .$$

Le point $z_0 = (-21+i\sqrt{3})/42$ est un point fixe sous $W_3$. Donc

$$\begin{cases} f|W_3 = -f \\ f|W_7 = f \end{cases} \quad \text{et} \quad \begin{cases} f|T(3) = f \\ f|T(7) = -f \end{cases}$$

pour $f \in \langle \Gamma_0(21), 2 \rangle_0$.

On pourrait procéder de la même façon pour calculer les valeurs propres $\lambda(p)$ des opérateurs de Hecke $T(p)$, pour $p$ divisant $N$, $N \in \mathfrak{M}_1$. Cependant, il sera plus simple d'utiliser la détermination explicite de la forme parabolique normalisée qui est faite en (3.1.3).

## 2.6. Conjecture de Weil.

Nous allons voir comment les résultats de (1.4.2) et (1.4.3) s'interprètent comme des conséquences immédiates d'une conjecture de Weil. Les notations sont celles de (2.5).

CONJECTURE 2.6.1. *Toute courbe elliptique définie sur $\mathbb{Q}$, de conducteur $N$, est isomorphe sur $\mathbb{Q}$ à un quotient de $J_N$.*

CONSÉQUENCE 1. *Il n'existe pas de courbe elliptique définie sur $\mathbb{Q}$, de conducteur $N \in \mathfrak{M}_0$.*

CONSÉQUENCE 2. *Soit $X$ une courbe elliptique définie sur $\mathbb{Q}$, de conducteur $N \in \mathfrak{M}_1$. Alors $X$ est isogène sur $\mathbb{Q}$ à la courbe modulaire elliptique $X_N$.*

S'il existe pour chaque $N \in \mathfrak{M}_1$ au moins une courbe elliptique de conducteur $N$ (on peut par exemple en exhiber une explicitement), on en déduit:

CONSÉQUENCE 3. (= théorème (1.4.2)) Le conducteur de la courbe modulaire elliptique $X_N$ est égal à N.

La conséquence 1 a été vérifié pour certaines valeurs de $N \in \mathcal{M}_0$ ; il en est de même pour la conséquence 2, pour $N = 2^\alpha$ et $N = 2.3^\beta$, $2^2.3^\beta$ (cf. Ogg[25],[26]).

Considérons la décomposition (2.5.2) de $J_N$, que nous écrivons

$$(2.6.1.1) \qquad J_N \approx J_N^0 \times \prod_{\substack{N' \mid N \\ N' \neq N}} (J_{N'}^0)^{\sigma_0(N/N')} = J_N^0 \times J_N^1 .$$

On démontre que T(p), considéré comme un endomorphisme de $J_N$, conserve cette décomposition. Si $f \in \langle \Gamma_0(N), 2 \rangle_0$ est une forme primitive, à valeurs propres $\lambda(p)$ entières, on lui associe la composante connexe de l'intersection des noyaux des endomorphismes $T(p) - \lambda(p)$ de $J_N^0$. On montre que cette composante connexe est une courbe elliptique $E_f$, définie sur $\underset{\sim}{Q}$, et que les facteurs locaux $L_p$ de sa fonction L sont ceux de la série de Dirichlet de f, pour p ne divisant pas N (cf. [32, 7.5]). Lorsque N est sans facteurs carrés, on peut montrer, en utilisant les résultats de Deligne (cf. (1.4.3)), que le conducteur de $E_f$ est égal à N. On ne sait pas le faire dans le cas général.

CONJECTURE 2.6.2. ( Conjecture de Weil) Toute courbe elliptique définie sur $\underset{\sim}{Q}$, de conducteur N, est isogène sur $\underset{\sim}{Q}$ à une courbe $E_f$ et une seule, où $f \in \langle \Gamma_0(N), 2 \rangle_0$ est une forme primitive à valeurs propres entières. La série L de la courbe coïncide avec la série de Dirichlet de f. ( cf. [40] ).

Le résultat du théorème (1.4.2) se généralise de la façon suivante:

CONJECTURE 2.6.3. Soit $\pi(N)$ la dimension de $J_N^0$ (= la dimension de l'espace des formes primitives sur $\Gamma_0(N)$). Alors le conducteur de $J_N^0$ est égal à $N^{\pi(N)}$.

Il est facile de calculer $\pi(N)$ en fonction de N. D'après (2.5.2)

$$p_0(N) = \sum_{d|N} \pi(d) \cdot \sigma_0(N/d) ,$$

ce qui s'écrit $p_0 = \pi * \sigma_0$ , en notant par $*$ le produit de convolution de deux fonctions arithmétiques. On en déduit

$$\pi = p_0 * \mu * \mu$$

où $\mu$ est la fonction de Möbius, définie par

(i) $\mu$ est multiplicative

(ii) $\mu(p^\alpha) = (-1)^\alpha$ si $\alpha \leq 1$,

$\mu(p^\alpha) = 0$ si $\alpha \geqslant 2$.

PROPOSITION 2.6.4. Soit N un entier sans facteurs carrés. Alors la conjecture (2.6.3) est vraie. (3).

En effet, supposons d'abord que $J_N^0 = J_N$ . D'après (1.4.3.2), l'exposant du conducteur en p , pour p diviseur de N , est égal à $p_0(N)$, ce qui est bien ce qu'affirme la conjecture.

Lorsque N est un entier sans facteurs carrés arbitraire, on se ramène au cas précédent en utilisant les isogénies (2.6.1.1)et à nouveau la formule (1.4.3.2).

(3) Des résultats récents de Deligne permettent de démontrer ce qui suit:

Soit N un entier positif arbitraire. Soit p un nombre premier, $p \neq 2$. Alors $e_p(J_N^0)$, exposant en p du conducteur de $J_N^0$ (cf.(1.4)) a la valeur prévue par la conjecture (2.6.3).

2.6.5. Exemples.

Passons en revue les valeurs de $N \in \mathcal{M}_2$.

(i) $\boxed{N = 23, 29, 31}$ Doi et Matsui (cf [7], [16]) ont démontré que les jacobiennes $J_{23}$, $J_{29}$, $J_{31}$, sont des variétés abéliennes simples. La conjecture (2.6.1) entraîne qu'il n'existe pas de courbes elliptiques de conducteurs 23, 29, ou 31.

Dans les trois cas $\pi(N) = 2$, et le conducteur vaut $23^2$, $29^2$, $31^2$, respectivement.

(ii) $\boxed{N = 22, 28}$ Ici, $\pi(N) = 0$. D'après la conjecture (2.6.1), il n'existe pas de courbe elliptique de conducteur 22 ou 28. D'après (2.5.2), $J_{22}$ est isogène sur $\underset{\sim}{Q}$ à $X_{11} \times X_{11}$, et $J_{28}$ à $X_{14} \times X_{14}$. Du reste, on constate que, dans les deux cas la courbe correspondant au quotient de $X_N$ par le groupe d'automorphismes $\{1, W_N\}$ est de genre 1. C'est une autre façon de voir que $J_N$ est isogène sur $\underset{\sim}{Q}$ au produit de deux courbes elliptiques. Une troisième est de remarquer que les courbes $X_{22}$, $X_{28}$, de genre 2, possèdent deux involutions distinctes (par exemple $W_N$ et $W_2$).

(iii) $\boxed{N = 26, 37, 50}$ Dans ces trois cas $\pi(N) = 2$.

$J_{37}$ est isogène au produit de deux courbes elliptiques parce que, ici encore, le quotient de $X_{37}$ par le groupe d'automorphismes $\{1, W_{37}\}$ est une courbe de genre 1. D'après la conjecture (2.6.2), $J_{37}$ est isogène sur $\underset{\sim}{Q}$ au produit de deux courbes elliptiques de conducteur 37. On connaît effectivement deux classes d'isogénies de courbes elliptiques définies sur $\underset{\sim}{Q}$, de conducteur 37.

Un modèle singulier de $X_{26}$ est la courbe plane d'équation

$$y^2 = x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1 \qquad (\text{cf. [9], p.458}).$$

Cette équation met en évidence le fait que $X_{26}$ admet, outre l'involution $\begin{cases} x \longmapsto x \\ y \longmapsto -y \end{cases}$,

l'involution $\begin{cases} x \longmapsto 1/x \\ y \longmapsto y/x^3 \end{cases}$,

et leur produit $\begin{cases} x \longmapsto 1/x \\ y \longmapsto -y/x^3 \end{cases}$.

on voit sans peine que ces trois involutions sont $W_{26}$, $W_2$, $W_{13}$. (cf. [19]). On en déduit là encore que $J_{26}$ est isogène au produit de deux courbes elliptiques. La conjecture de Weil entraîne que ces dernières sont de conducteur 26, ce qu'on vérifie, et que toute courbe elliptique de conducteur 26 est isogène sur $\underset{\sim}{Q}$ à l'une des deux.

Pour N = 50, l'existence des involutions $W_{50}$, $W_2$, $W_5$ entraîne encore que $J_{50}$ est isogène au produit de deux courbes elliptiques. On connaît effectivement deux classes d'isogénies de courbes elliptiques de conducteur 50.

# 3. CONSTRUCTION DE FORMES MODULAIRES ET APPLICATIONS.

## 3.1. Construction de formes modulaires.

Dans ce paragraphe, on désigne par $\eta(z)$ la forme modulaire de Dedekind

$$\eta(z) = q^{1/24}.\prod_{n=1}^{\infty}(1-q^n) = \Delta(z)^{1/24} \quad \text{où}$$

$$q = \exp(2\pi i z) .$$

On utilise $\eta(z)$ pour construire certaines formes modulaires sur $\Gamma_0(N)$.

Rappelons les résultats suivants (cf. [22]):

(i) Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de $SL(2,\mathbb{Z})$, avec $c > 0$.

Alors $\eta\left(\frac{az+b}{cz+d}\right) = \varepsilon\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right).(-i(cz+d))^{1/2}.\eta(z)$

avec $\varepsilon\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \exp(-i\pi\,\alpha\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)$ ,et $\alpha\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \in \mathbb{Z}$.

(ii) Lorsque $(a,6) = 1$, l'entier $\alpha\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)$ défini par (i) vérifie la congruence suivante:

$$\alpha\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \equiv \frac{1}{12}\, a(c-b-3) - \frac{1}{2}\left\{1-\left(\frac{c}{a}\right)\right\} \pmod 2 .$$

(iii) Le groupe $\Gamma_0(N)$ est engendré par les éléments

$$\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \in \Gamma_0(N) \quad \text{tels que} \quad (a,6) = 1 \ , \ a \gg 0, \ c \gg 0.$$

On désigne par $\delta$ un diviseur positif de N, et par $\delta'$ l'entier défini par $\delta\delta' = N$. On note $\underline{r} = (r_\delta)$ une famille d'entiers positifs ou nuls, indexés par l'ensemble des diviseurs positifs de N, et on considère la forme modulaire

$$g_{\underline{r}}(z) = \prod_{\delta|N} \eta(\delta z)^{r_\delta}.$$

PROPOSITION 3.1.1. Supposons vérifiées les hypothèses suivantes:

(A) $\sum_{\delta|N} r_\delta \cdot \delta \equiv 0 \pmod{24}$ ,

(B) $\sum_{\delta|N} r_\delta \cdot \delta \equiv 0 \pmod{24}$ ,

(C) $\sum_{\delta|N} r_\delta = 4$ ,

(D) $\prod_{\delta|N} (\delta')^{r_\delta} \in \mathbb{Z}^2$.

Alors $g_{\underline{r}}(z)$ est une forme parabolique de poids 2 sur $\Gamma_0(N)$.

Remarque. Cette méthode ne permet pas d'obtenir toutes les formes paraboliques de poids 2, même si l'on se limite à $N \in \mathcal{M}_1$ (cf.(3.1.2)).

Démonstration. Soit $U = \begin{pmatrix} a & b \\ Nc & d \end{pmatrix}$ un élément de $\Gamma_0(N)$. Alors

$$\eta(\delta \cdot Uz) = \eta(U_\delta \cdot \delta z) \quad \text{où} \quad U_\delta = \begin{pmatrix} a & b\delta \\ c\delta' & d \end{pmatrix},$$

par conséquent

$$g_{\underline{r}}(Uz) = (-i(Ncz+d))^{\sum_{\delta|N} \frac{r_\delta}{2}} \cdot g_{\underline{r}}(z) \cdot \prod_{\delta|N} \varepsilon(U_\delta)^{r_\delta}.$$

Calculons le troisième facteur de cette expression. Tenant compte de ce qu'on peut supposer d'après (iii) que $(a,6) = 1$, et que $c > 0$, on voit que

$$\prod_{\delta|N} \epsilon(U_\delta)^{r_\delta} = \exp(-i\pi\lambda) \quad \text{où} \quad \lambda = \sum_{\delta|N} r_\delta \cdot \alpha(U_\delta).$$

Utilisant d'autre part (iii) en même temps que (ii):

$$\alpha(U_\delta) \equiv \frac{1}{12} a(c\delta' - b\delta - 3) - \frac{1}{2}\left\{1 - \left(\frac{c\delta'}{a}\right)\right\} \pmod 2,$$

d'où

$$\lambda \equiv \frac{1}{12} ac\left(\sum_{\delta|N} r_\delta \cdot \delta'\right) - \frac{1}{12} ab\left(\sum_{\delta|N} r_\delta \cdot \delta\right) - \frac{a}{4}\sum_{\delta|N} r_\delta - \frac{1}{2}\sum_{\delta|N}\left\{1 - \left(\frac{c\delta'}{a}\right)\right\} \cdot r_\delta \pmod 2.$$

Utilisant maintenant (A), (B), et (C), on en déduit:

$$1+\lambda \equiv \frac{1}{2}\sum_{\delta|N} r_\delta \cdot \left\{1 - \left(\frac{\delta' c}{a}\right)\right\} \pmod 2,$$

et par conséquent

$$\exp(-i\pi\lambda) = -\prod_{\delta|N}\left(\frac{\delta' c}{a}\right)^{r_\delta} = -\prod_{\delta|N}\left(\frac{\delta'}{a}\right)^{r_\delta} \quad \text{d'après (C)},$$

qui vaut $-1$ d'après (D). Revenant à la fonction $g_{\underline{r}}$, et utilisant à nouveau (C), on obtient:

$$g_{\underline{r}}(Uz) = -i^2 \cdot (Ncz+d)^2 \cdot g_{\underline{r}}(z).$$

D'autre part, il est clair que $g_{\underline{r}}$ s'annule en chaque pointe de $\Gamma_0(N)$. D'où la conclusion.

Utilisons la proposition (3.1.1) dans chacun des cas suivants:

| N | $\underline{r} = (r_\delta)$ |
|---|---|
| 11 | $r_1 = r_{11} = 2$ |
| 14 | $r_1 = r_2 = r_7 = r_{14} = 1$ |
| 15 | $r_1 = r_3 = r_5 = r_{15} = 1$ |
| 20 | $r_2 = r_{10} = 2$ |
| 24 | $r_2 = r_4 = r_6 = r_{12} = 1$ |
| 27 | $r_3 = r_9 = 2$ |
| 32 | $r_4 = r_8 = 2$ |
| 36 | $r_6 = 4$ |

On en déduit:

COROLLAIRE. Les formes paraboliques normalisées associées à $\Gamma_0(N)$, pour $N = 11, 14, 15, 20, 24, 27, 32, 36$ sont données par le tableau (3.1.2)

| N | |
|---|---|
| 11 | $\eta(z)^2\eta(11z)^2$ |
| 14 | $\eta(z)\eta(2z)\eta(7z)\eta(14z)$ |
| 15 | $\eta(z)\eta(3z)\eta(5z)\eta(15z)$ |
| 20 | $\eta(2z)^2\eta(10z)^2$ |
| 24 | $\eta(2z)\eta(4z)\eta(6z)\eta(12z)$ |
| 27 | $\eta(3z)^2\eta(9z)^2$ |
| 32 | $\eta(4z)^2\eta(8z)^2$ |
| 36 | $\eta(6z)^4$ |

On en déduit les développements suivants de la forme parabolique normalisée:

| N | |
|---|---|
| 11 | $q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} + O(q^{12})$ |
| 14 | $q - q^2 - 2q^3 + q^4 + 2q^6 + q^7 - q^8 + q^9 + O(q^{10})$ |
| 15 | $q - q^2 - q^3 - q^4 + q^5 + q^6 + 3q^8 + q^9 + O(q^{10})$ |
| 20 | $q - 2q^3 - q^5 + 2q^7 + q^9 + O(q^{12})$ |
| 24 | $q - q^3 - 2q^5 + q^9 + 4q^{11} - 2q^{13} + O(q^{14})$ |
| 27 | $q - 2q^4 - q^7 + 5q^{13} + O(q^{14})$ |
| 32 | $q - 2q^5 - 3q^9 + 6q^{13} + O(q^{16})$ |
| 36 | $q - 4q^7 + 2q^{13} + 8q^{19} + O(q^{24})$ |

On en déduit enfin, pour chacune de ces huit valeurs de N, les valeurs propres des opérateurs de Hecke T(p), pour p divisant N. Ce sont les coefficients $a_p$ de la série de Fourier de la forme parabolique normalisée, d'après (2.1.2). Regroupant ces résultats avec ceux

de (2.5.5) pour N = 17, 19 , de (2.4.3) pour N = 49, et ceux de (2.5.7) pour N = 21, on obtient les valeurs données par le tableau suivant, où l'on pose $N = p_1^{n_1} \cdot p_2^{n_2}$ , $p_1 < p_2$ , $n_1 > 0$ :

(3.1.3)

| N | $\lambda(p_1)$ | $\lambda(p_2)$ |
|---|---|---|
| 11 | 1 | — |
| 14 | -1 | 1 |
| 15 | -1 | 1 |
| 17 | 1 | — |
| 19 | 1 | — |
| 20 | 0 | -1 |
| 21 | 1 | -1 |
| 24 | 0 | -1 |
| 27 | 0 | — |
| 32 | 0 | — |
| 36 | 0 | 0 |
| 49 | 0 | — |

On a ainsi entièrement déterminé les facteurs locaux de la série de Dirichlet associée à $\Gamma_0(N)$, pour p divisant N, $N \in \mathcal{M}_1$ (cf. (2.1.3). Il suffira de vérifier en (4.3.4) que ces facteurs locaux coïncident avec ceux de la série L de la courbe modulaire elliptique $X_N$ pour terminer la démonstration du théorème (2.2.3).

## 3.2. Pointes de $\Gamma_0(N)$.

On conserve les notations de (3.1). On désigne par $d, \delta$ des diviseurs positifs de N, et on pose $d' = N/d$, $\delta' = N/\delta$. On suppose maintenant que $\underline{r} = (r_\delta)$ est une famille d'entiers $r_\delta \in \mathbb{Z}$ indexée par les $\delta$.

PROPOSITION 3.2.1. La forme modulaire $g_{\underline{r}}$ définit une fonction sur la courbe modulaire $X_N$ si et seulement si les conditions suivantes sont vérifiées:

$$(A)\quad \sum_{\delta|N} r_\delta \cdot \delta' \equiv 0 \pmod{24},$$

$$(B)\quad \sum_{\delta|N} r_\delta \cdot \delta \equiv 0 \pmod{24},$$

$$(C')\quad \sum_{\delta|N} r_\delta = 0,$$

$$(D')\quad \prod_{\delta|N} (\delta')^{r_\delta} \in \underset{\sim}{Q}^2.$$

Démonstration. La suffisance se démontre facilement en reprenant la démonstration de (3.1.1). Démontrons la nécessité.

Celle de (C') est évidente. Ecrivant que $g_{\underline{r}}$ est invariante sous $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, on obtient (B). De même, l'invariance sous $\begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}$ entraîne (A). Par conséquent, $\prod_{\delta|N} \left(\frac{\delta'}{a}\right)^{r_\delta} = 1$ pour tout $a > 0$, premier à 6N. On est ramené à démontrer:

LEMME. Soient m,n des entiers premiers entre eux. On suppose que $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$ pour presque tout p. Alors $m/n \in \underset{\sim}{Q}^2$.

En effet, cela entraîne que mn est un résidu quadratique modulo p pour presque tout p, donc un carré d'après le théorème de Dirichlet.

Remarque. Il est clair que la série de Fourier de $g_{\underline{r}}$ est à coefficients rationnels. Par conséquent, si $\underline{r}$ vérifie les conditions de (3.2.1), $g_{\underline{r}}$ est dans le corps des fonctions $\underset{\sim}{Q}(X_N)$.

L'ensemble des pointes de $\Gamma_0(N)$ est $\underset{\sim}{Q} \cup \{i\infty\} = \mathfrak{h}^* - \mathfrak{h}$. Les orbites de l'action de $\Gamma_0(N)$ sur l'ensemble des pointes de $\Gamma_0(N)$ sont en nombre fini. On obtient donc une bijection de l'ensemble de ces orbites avec un ensemble fini de points de la surface de Riemann $X_{N,\underset{\sim}{C}}$, qu'on appelle les pointes de $X_{N,\underset{\sim}{C}}$.

PROPOSITION 3.2.2. Soit P une pointe de $X_{N,\underset{\sim}{C}}$. Il existe un unique diviseur positif d de N tel que l'orbite correspondante contienne $b/d$, où b est un entier premier à d. On dira que P est une pointe de niveau d.

Si d est un diviseur positif de N, il existe $\varphi((d,d'))$ pointes de $X_{N,C}$ de niveau d, où $\varphi$ désigne la fonction d'Euler.

Cela résulte par exemple de [32, dém. prop.(1.4.3)].

En particulier, pour $d = 1$, N, il n'existe qu'une seule pointe de niveau d, correspondant à l'orbite de 0, $i\infty$ respectivement.

NOTATION 3.2.3. On note $(P_d)$ le diviseur de $X_{N,\underset{\sim}{C}}$ somme des pointes $P_{d,i}$ de niveau d:

$$(P_d) = P_{d,1} + \cdots + P_{d,\varphi((d,d'))} .$$

Nous allons voir que, $N>1$ et $d' \mid N$ étant donnés, on peut trouver une famille $\underset{\sim}{r}$ d'entiers, vérifiant les conditions de (3.2.1), et telle que le diviseur de $g_{\underset{\sim}{r}}$ soit un multiple du diviseur de degré zéro

$$\varphi((d,d')).P_1 - (P_d).$$

Il en résultera que ce dernier est d'ordre fini dans le groupe des classes de diviseurs modulo l'équivalence linéaire, et que $(P_d)$ est un diviseur rationnel sur $\underset{\sim}{Q}$.

Pour ce faire, nous commençons par déterminer l'ordre de $g_{\underset{\sim}{r}}$ en une pointe.

LEMME 3.2.4. Soit P une pointe de $X_{N,\mathbb{C}}$, de niveau d. Alors un paramètre local de $X_{N,\mathbb{C}}$ en P est

$$\exp(2\pi i\, \rho(z)/h) \quad \text{où} \quad h = d'/(d,d') ,$$

et où $\rho \in SL(2,\mathbb{R})$ envoie P sur la pointe à l'infini $P_N$.

En effet [32, (2.1)], h est défini par le fait que

$$\rho \circ \mathrm{Stab}_{\Gamma_0(N)}(s) \circ \rho^{-1} = \left\{ \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m \;\middle|\; m \in \mathbb{Z} \right\}$$ (s est un point de l'orbite associée à P, et $\mathrm{Stab}_{\Gamma_0(N)}(s)$ désigne son stabilisateur dans $\Gamma_0(N)$).

Soit $s = b/d$, avec $(b,d) = 1$. On peut prendre $\rho$ de la forme

$$\begin{pmatrix} * & * \\ d & -b \end{pmatrix}, \quad \text{donc} \quad \rho^{-1} \cdot \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \cdot \rho = \begin{pmatrix} * & * \\ -hd^2 & * \end{pmatrix},$$

et $\begin{pmatrix} * & * \\ -hd^2 & * \end{pmatrix} \in SL(2,\mathbb{Z})$ est un élément de $\Gamma_0(N)$ si et seulement si N divise $hd^2$, donc si h est multiple de $d'/(d,d')$.

LEMME 3.2.5. Soit $s = b/d$ une pointe de $\Gamma_0(N)$, de niveau d, et soit $\Delta_\delta(z) = \Delta(\delta z)$, où $\delta$ est un diviseur positif de N. Soit $\rho$ un élément de $SL(2,\mathbb{Z})$ tel que $\rho(s) = i\infty$. Alors

$$\Delta_\delta(\rho^{-1}(z)) = \left(\frac{d}{\delta}(d,\delta)\cdot z + \beta\right)^{12} \cdot \Delta\left(\frac{(d,\delta)^2}{\delta}\cdot z + \gamma\right),$$

où $\beta, \gamma$, sont des entiers.

En effet, soit $\rho = \begin{pmatrix} c & -a \\ d & -b \end{pmatrix}$.

$$\Delta_\delta(\rho^{-1}(z)) = \Delta\left(\begin{pmatrix} -b\delta & a \\ -d & c \end{pmatrix}\cdot z\right) = \Delta\left(\begin{pmatrix} -b\delta_1 & a \\ -d_1 & c \end{pmatrix}\cdot uz\right),$$

où on a posé $u = (d,\delta)$, $\delta = \delta_1 u$, $d = d_1 u$.

De $(d_1,\delta_1) = 1$ résulte $(d_1,\delta_1 b)) = 1$. Il existe donc $\begin{pmatrix} -b\delta_1 & * \\ -d_1 & * \end{pmatrix} \in \underline{SL}(2,\underline{Z})$ telle que $\begin{pmatrix} -b\delta_1 & a \\ -d_1 & c \end{pmatrix} = \begin{pmatrix} -b\delta_1 & * \\ -d_1 & * \end{pmatrix} \cdot \begin{pmatrix} 1 & * \\ 0 & \delta_1 \end{pmatrix}$,

d'où

$$\Delta_\delta(\rho^{-1}(z)) = \left(\frac{d}{\delta}(d,\delta).z + \beta\right)^{12} \cdot \Delta\left(\frac{(d,\delta)^2}{\delta} z + \gamma\right),$$

en utilisant le fait que $\Delta$ est une forme modulaire de poids 12 sur $\underline{SL}(2,\underline{Z})$.

NOTATION 3.2.6. On pose $\boxed{a_N(d,\delta) = \frac{N}{(d,d')} \cdot \frac{(d,\delta)^2}{d\delta}}$.

LEMME 3.2.7. On a $a_N(d,\delta) = a_N(d',\delta')$.

Revenant à la fonction $g_{\underline{r}}$, et utilisant les lemmes (3.2.4) et (3.25), on obtient en définitive:

PROPOSITION 3.2.8. Soit $\underline{r}$ une famille vérifiant les conditions de (3.2.1). Alors la valuation de $g_{\underline{r}}$ en une pointe de niveau d est donnée par

$$b_{\underline{r}}(d) = \frac{1}{24} \sum_{\delta | N} a_N(d,\delta).r_\delta ,$$

donc le diviseur de $g_{\underline{r}}$ est

$$(g_{\underline{r}}) = \sum_{\delta | N} b_{\underline{r}}(d).(P_d) .$$

COROLLAIRE. Sous les hypothèses de (3.2.8), on a

$$\deg((g_{\underline{r}})) = \sum_{d | N} b_{\underline{r}}(d).\varphi((d,d')) = 0.$$

LEMME 3.2.9. Soit v l'application $\underset{\sim}{Q}$-linéaire de $\underset{\sim}{Q}$-espaces vectoriels définie par:

$$v(r_1,\dots,r_n) = (b_{\underline{r}}(1),\dots,b_{\underline{r}}(n), y=\sum_{i=1}^{i=n} r_i ),$$

(où $n = \sigma_0(N)$ = nombre de diviseurs positifs de N ). Alors v est injective, et l'intersection de son image avec l'hyperplan $\{ y = 0 \}$ est donnée par

$$\sum_{d|N} \varphi((d,d')).b_{\underline{r}}(d) = 0 \quad , y = 0 .$$

L'injectivité résulte de ce que $g_{\underline{r}}$ ne peut être une constante que pour $\underline{r} = 0$.

On déduit de (3.2.1), (3.2.8) et (3.2.9):

PROPOSITION 3.2.10. Soit D un diviseur de la forme

$$D = \sum_{d|N} m_d.(P_d) \text{ , où } (P_d) \text{ est le diviseur somme des}$$

pointes de niveau d (3.2.3), de degré 0, c'est à dire tel que

$$\sum_{d|N} \varphi((d,d')).m_d = 0.$$

Alors il existe une famille d'entiers $\underline{r}$ telle que le diviseur de $g_{\underline{r}}$ soit un multiple de D.

En particulier, D est rationnel sur $\underset{\sim}{Q}$ et d'ordre fini dans le groupe des classes de diviseurs pour l'équivalence linéaire.

COROLLAIRE. Pour tout diviseur positif d de N, le diviseur

$(P_d) - \varphi((d,d')).P_1$ est rationnel sur $\underset{\sim}{Q}$ et d'ordre fini dans le groupe des classes de diviseurs pour l'équivalence linéaire.

Les pointes $P_1$ et $P_N$ sont rationnelles sur $\underset{\sim}{\mathbb{Q}}$ (cf. (1.2)). Par conséquent le diviseur $(P_d)$ est rationnel sur $\underset{\sim}{\mathbb{Q}}$. En particulier, si $\varphi((d,d')) = 1$, donc si $(d,d') = 1$ ou 2, la pointe $P_d$ est rationnelle sur $\underset{\sim}{\mathbb{Q}}$.

De façon plus précise, on peut montrer que le plus petit corps de rationalité des pointes $P_{d,i}$ de niveau d est le corps $\underset{\sim}{\mathbb{Q}}(\zeta)$, où $\zeta$ est une racine primitive $\varphi((d,d'))$-ième de l'unité.

D'autre part, il résulte de la théorie des symboles modulaires de Manin ([14, 15]) que $P_1 - P$ est un diviseur d'ordre fini dans le groupe des classes de diviseurs pour l'équivalence linéaire, pour toute pointe P de $X_{N,\underset{\sim}{\mathbb{C}}}$.

Dans le cas particulier du diviseur $P_1 - P_N$, la proposition (3.2.1) permet de déterminer explicitement cet ordre. En effet:

NOTATION 3.2.11. On pose $\quad \tilde{N} = \prod_{p|N} p \ , \quad k(N) = N \prod_{p|N} (p - \frac{1}{p})$.

Soit $\delta$ un diviseur positif de N. On pose

$$s_\delta = \frac{\tilde{N}}{\delta} \mu(\delta) \ , \ r_\delta = s_\delta - s_{\delta'} \ , \text{ où } \mu$$

désigne la fonction de Möbius, et $\delta' = N/\delta$ (cf. (2.6.3)).

LEMME 3.2.12. On a

$$\sum_{\delta|N} a_N(d,\delta) \cdot r_\delta = \begin{cases} k(N) & \text{si } d = 1 \\ 0 & \text{si } d \neq 1, N \\ -k(N) & \text{si } d = N \end{cases} ,$$

où $a_N(d,\delta)$ est défini par (3.2.6).

LEMME 3.2.13. Soit $N = p_1^{n_1} p_2^{n_2} \ldots p_g^{n_g}$ la décomposition de N en facteurs premiers.

Alors on a

$$w = \prod_{\delta|N} (\delta')^{r_\delta} = p_1^{w_1} p_2^{w_2} \ldots p_g^{w_g} \ , \text{ avec}$$

$$w_j = (n_j p_j - n_j + 2) \prod_{l \neq j} (p_l - 1) \ .$$

Démonstration du lemme (3.2.1.2).

Notons $g_k(n)$ la fonction $g_k(n) = n^k$.

$\sum_{\delta|N} a_N(d,\delta).s_\delta = \sum_{\delta|N} \frac{N}{(d,d')} \cdot \frac{(d,\delta)^2}{d\delta^2} \cdot \tilde{N}\mu(\delta)$, et il suffit de se borner aux diviseurs $\delta$ sans facteurs carrés.

Si $d = 1$, on trouve:

$$\sum_{\delta|N} \frac{N\tilde{N}}{\delta^2}\mu(\delta) = \frac{N}{\tilde{N}}(g_2 * \mu)(N) = k(N).$$

Si $d \neq 1$, soit p un diviseur premier de d. Comme $\delta$ est sans facteurs carrés, la multiplication par p envoie bijectivement les diviseurs $\delta$ premiers à p sur ceux qui sont des multiples de p. Si $\delta$ est premier à p, on a:

$$\mu(p\delta) = -\mu(\delta) \quad \text{et} \quad (d,\delta) = (d/p,\delta).$$

Donc:

$$\sum_{\delta|N} a_N(d,\delta).s_\delta = \frac{N\tilde{N}}{(d,d')}\left\{\sum_{\substack{\delta|N \\ (\delta,p)=1}} \frac{(d,\delta)^2}{d\delta^2}\mu(\delta) + \sum_{\substack{\delta|N \\ p|\delta}} \frac{(d,\delta)^2}{d\delta^2}\mu(\delta)\right\}.$$

D'après les remarques précédentes, le terme entre les accolades s'écrit:

$$\sum_{\substack{\delta|N \\ (\delta,p)=1}} \frac{(d,\delta)^2}{d\delta^2}\mu(\delta) + \sum_{\substack{(\delta/p)|N \\ ((\delta/p),p)=1}} \frac{(d/p,\delta/p)^2}{d(\delta/p)^2}\mu(\delta/p) = 0.$$

D'autre part:

$\sum_{\delta|N} a_N(d,\delta).s_{\delta'} = \sum_{\delta'|N} a_N(d',\delta').s_{\delta'} = \sum_{\delta|N} a_N(d',\delta).s_\delta$: le calcul qu'on vient de faire montre que cette expression est égale à $k(N)$ si $d' = 1$, et à 0 sinon. Le lemme est donc démontré.

Démonstration du lemme (3.2.13).

Tout d'abord, $w = \prod_{\delta|N} (\delta')^{r_\delta} = \prod_{\delta|N} \left(\frac{N}{\delta^2}\right)^{s_\delta} = \frac{N^{\sum_\delta s_\delta}}{\left(\prod \delta^{s_\delta}\right)^2}$ .

Or $\sum_{\delta|N} s_\delta = \sum_{\delta|N} \left(\frac{\tilde{N}}{\delta}\right)\mu(\delta) = \prod_{p|N}(p-1) = (p_1-1)(p_2-1)\ldots(p_g-1)$.

D'autre part, il est clair que l'exposant de $p_j$ dans $\prod \delta^{s_\delta}$ est:

$$-\frac{\tilde{N}}{p_j} + \sum_{k\neq j} \frac{\tilde{N}}{p_j p_k} - \sum_{\substack{j\neq k \\ j\neq \ell \\ k\neq \ell}} \frac{\tilde{N}}{p_j p_k p_\ell} + \ldots + (-1)^g =$$

$$= -\prod_{k\neq j}(p_k - 1).$$

Par conséquent, l'exposant $w_j$ de $p_j$ dans $w$ est:

$$w_j = n_j \cdot (p_j - 1)\prod_{j\neq k}(p_k - 1) + 2\prod_{j\neq k}(p_k - 1),$$

ce qui est bien le résultat annoncé.

On considère toujours la famille $\underline{r}$ définie en (3.2.11).

LEMME 3.2.14. Il existe un unique entier positif $m$ satisfaisant aux conditions suivantes:

(i) La famille $\frac{24}{m}\underline{r}$ satisfait aux conditions de la proposition (3.2.1).

(ii) Si $m'$ est un entier positif tel que (i) soit satisfaite, alors $m'$ divise $m$.

Plus précisément, avec les notations de (3.2.13):

$$m = \operatorname{pgcd}_{\substack{1\leq\delta\leq g \\ \delta|N}}\left(k(N),\ 12w_j,\ 24r_\delta\right).$$

Démonstration du lemme (3.2.14).

Considérons les conditions (A),(B),(C'),(D') de la proposition (3.2.1). La condition (C') est trivialement vérifiée par tout multiple rationnel de $\underline{r}$. D'autre part, il est clair que la famille $24\underline{r}$ vérifie les trois autres conditions. Du reste, tenant compte de ce que $a_N(1,\delta) = \delta'$, et $a_N(N,\delta) = \delta$, le lemme (3.2.12) montre que

$$\sum r_\delta . \delta' = - \sum r_\delta . \delta = k(N).$$

L'existence et l'unicité de $m$ sont maintenant claires: $m$ est le plus grand entier positif tel que l'on ait simultanément

$$\begin{cases} \frac{24}{m} . k(N) \equiv 0 \pmod{24}, \\ \frac{24}{m} . w_j \equiv 0 \pmod{2} \quad \text{( notations de (3.2.13))}. \\ \frac{24}{m} r_\delta \in \mathbb{Z}. \end{cases}$$

Il est clair que la solution est

$$m = \operatorname*{pgcd}_{\substack{1 \leq j \leq g \\ \delta | N}} ( k(N), 12 w_j , 24 r_\delta ).$$

Conservons les notations des lemmes précédents.

LEMME 3.2.15. (i) *Le diviseur de la fonction* $g_{\frac{24}{m}\underline{r}}$ *est*

$$\frac{k(N)}{m} . ( P_1 - P_N ).$$

(ii) *Le diviseur* $P_1 - P_N$ *sur la courbe modulaire* $X_N$ *est d'ordre* $\frac{k(N)}{m}$ *dans le groupe des classes de diviseurs pour l'équivalence linéaire.*

D'après la proposition (3.2.8), la fonction considérée est régulière et non nulle en dehors des pointes. Le lemme (3.2.12) montre que $b_{\underline{r}}(d) = 0$ pour $d|N$, $d \neq 1, N$, et que $b_{\underline{r}}(1) = - b_{\underline{r}}(N) = k(N)/24$, avec les notations de (3.2.8). D'où (i).

D'autre part, si $m$ est l'entier dont le lemme 3.2.14 affirme l'existence, l'ordre de $P_1 - P_N$ divise $\frac{k(N)}{m}$. Soit $\frac{k(N)}{m_1}$ cet ordre, où $m_1$ est un multiple de $m$. Si la famille $\frac{24}{m}.\underline{r}$ est une famille d'entiers, la proposition (3.2.1) s'applique, et par conséquent les conditions (A),(B),(C'),(D') sont vérifiées. Le lemme (3.2.14) entraîne alors $m_1 = m$, cqfd.

Il reste à voir que $\frac{24}{m}.\underline{r}$ est nécessairement une famille d'entiers. Posons $\frac{24}{m}.\underline{r} = \underline{t}$, et montrons que les hypothèses:

(i) $g_{\underline{t}} = \prod_{\delta | N} \eta_\delta^{t_\delta}$ définit une fonction méromorphe sur $X_N$,

(ii) la fonction ainsi définie possède un pôle en $P_1$, un zéro en $P_N$, et est régulière et non nulle partout ailleurs,

entraînent que $\underline{t}$ est une famille d'entiers. En effet, il résulte de [6] que le développement de $g_{\underline{t}}(z)$ au voisinage de $P_N$ est un élément de $\underset{\sim}{Z}[[q]]$, où $q = \exp(2\pi i z)$.

Posons $n = \sum_{\delta | N} t_\delta . \delta$. Alors

$$g_{\underline{t}}(z) = q^n \prod_{k=1}^{\infty} \prod_{\delta | N} (1 - q^{k\delta_i})^{t_{\delta_i}} \quad ;$$

supposons les diviseurs $\delta_i$ rangés dans l'ordre croissant. On a donc

$$g_{\underline{t}} \equiv q^n (1 - q^{\delta_1})^{t_{\delta_1}} \equiv q^n (1 - t_{\delta_1} q^{\delta_1}) \pmod{q^{\delta_1}},$$

et par conséquent

$$t_{\delta_1} \in \underset{\sim}{Z}.$$

On peut alors diviser $g_{\underline{t}}$ par la série

$\prod_{k=1}^{\infty} (1 - q^{k\delta_1})^{t_{\delta_1}}$, qui est un élément inversible de $\underset{\sim}{Z}[[q]]$, et le même raisonnement montre que $t_{\delta_2} \in \underset{\sim}{Z}$. En définitive, on obtient le résultat voulu: La famille $\underline{t}$ est une famille d'entiers.

Regroupons les résultats de cette partie dans le

THÉORÈME 3.2.16. *Soit* $N$ *un entier positif distinct de* 1. *Alors le diviseur* $P_1 - P_N$ *sur la courbe modulaire* $X_N$ *est rationnel sur* $\mathbb{Q}$, *et d'ordre fini dans le groupe des classes de diviseurs pour l'équivalence linéaire.*

*Plus précisément,* $P_1 - P_N$ *est d'ordre* $k(N)/m$ , *où l'on a posé:*

$$N = p_1^{n_1} p_2^{n_2} \dots p_g^{n_g} \ ,$$

$$k(N) = N.(p_1 - \frac{1}{p_1})(p_2 - \frac{1}{p_2}) \dots (p_g - \frac{1}{p_g}) \ ,$$

$$m = \text{pgcd}\ (\ k(N),\ 12w_j\ ,\ 24r_\delta\ ),$$

$$r_\delta = s_\delta - s_{\delta'} \ , \quad s_\delta = \frac{\widetilde{N}}{\delta}\mu(\delta) \quad (\text{cf. } 3.2.11),$$

$$w_j = (n_j p_j - n_j + 2) \prod_{l \neq j} (p_l - 1) \ , \quad j = 1, \dots, g.$$

Lorsque $N$ est premier, ou carré d'un nombre premier, on retrouve les expressions données par Ogg:

(i) $\boxed{N = p}$. Ici $k(p) = p^2 - 1$, et $w = p+1$, donc $m = (p+1).(p-1, 12)$. L'ordre de $P_1 - P_p$ est

$$\frac{p-1}{(p-1,12)} .$$

(ii) $\boxed{N = p^2}$. Cette fois $k(p^2) = p(p^2-1)$, et $w = 2p$ ; $m = p.(p^2-1, 24)$. D'où l'ordre cherché, qui est

$$\frac{p^2-1}{(p^2-1,24)} .$$

3.3. Applications.

(i) Soit $N \in \mathcal{M}_0 - \{1\}$. Alors $P_1$ , $P_N$ sont des points distincts de $X_N$, et le calcul explicite de l'ordre de $P_1 - P_N$ grâce à (3.2) donne: $P_1 - P_N$ est le diviseur d'une fonction; on retrouve ainsi le fait que $X_N$ est de genre 0.

(ii) L'ordre de $P_1 - P_N$, pour $N \in \mathcal{M}_1 \cup \mathcal{M}_2$ , est donné par le tableau suivant (3.3.1):

| N | 11 | 14 | 15 | 17 | 19 | 20 | 21 | 24 | 27 | 32 | 36 | 49 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ordre de $P_1 - P_N$ | 5 | 6 | 4 | 4 | 3 | 6 | 4 | 4 | 3 | 4 | 6 | 2 |
| N | 22 | 23 | 26 | 28 | 29 | 31 | 37 | 50 | | | | |
| ordre de $P_1 - P_N$ | 5 | 11 | 21 | 6 | 7 | 5 | 3 | 15 | | | | |

# 4. EQUATIONS EXPLICITES.

## 4.1. Résultats de Fricke.

On suppose maintenant que $N \in \mathcal{M}_1$. La surface de Riemann $Y_{N,\mathbb{C}}$ ( resp. $X_{N',\mathbb{C}}$ ) associée à $\Gamma_0^*(N)$ (cf. (2.5)) ( resp. associée à $\Gamma_0(N')$, où $N'$ divise proprement $N$ ) est alors de genre 0 ( cf.(2.5.3) et (1.3) ).

Pour $N = 11, 14, 15, 17, 19, 21, 49$ ( resp. 20, 24, 27, 32, 36 ) Fricke construit dans [9] une fonction méromorphe $\tau(z)$ de la variable $z \in \mathfrak{h}^*$, qui induit une fonction méromorphe sur la courbe $Y_{N,\mathbb{C}}$, ( resp. sur la courbe $X_{N',\mathbb{C}}$, pour $N' = 10, 12, 9, 16$ respectivement ), et dont la restriction au demi-axe imaginaire $\{ z \in \mathbb{C} \mid \mathrm{Re}(z) = 0 , \mathrm{Im}(z) > 0 \}$ est une fonction à valeurs réelles.

Plus précisément, soit $z_0 = i.N^{-1/2}$ le point fixe de $W_N$ situé dans $\mathfrak{h}^*$ ( cf. (2.4) ). La restriction de $\tau$ au demi-axe imaginaire est une fonction analytique de $\mathrm{Im}(z)$. Cette dernière vérifie $\tau(z) = \tau(-1/Nz)$, est croissante pour $\mathrm{Im}(z) > \mathrm{Im}(z_0)$, et tend vers $+\infty$ lorsque $\mathrm{Im}(z)$ tend vers $+\infty$ ( resp. : cette dernière est une fonction décroissante de $\mathrm{Im}(z)$, à valeurs positives, tendant vers $0^+$ lorsque $\mathrm{Im}(z)$ tend vers $+\infty$ et vers $+\infty$ lorsque $\mathrm{Im}(z)$ tend vers $0^+$ ).

Fricke construit également une fonction méromorphe $\sigma(z)$ de la variable $z$, qui induit une fonction méromorphe sur $X_{N,\mathbb{C}}$. La restriction de $\sigma$ au demi-axe imaginaire est à valeurs réelles. C'est une fonction croissante de $\mathrm{Im}(z)$, vérifiant $\sigma(z) = -\sigma(-1/Nz)$, positive pour $\mathrm{Im}(z) > \mathrm{Im}(z_0)$, et tendant vers $+\infty$ lorsque $\mathrm{Im}(z)$ tend

vers $+\infty$ ( resp.: c'est une fonction décroissante de $Im(z)$, tendant vers $+\infty$ lorsque $Im(z)$ tend vers $0^+$, et vers une limite finie lorsque $Im(z)$ tend vers $+\infty$ ).

Posons de nouveau $q = \exp(2\pi i z)$. On aura besoin plus loin du premier terme non-nul du développement en série de $\tau(z)$, $\sigma(z)$ au voisinage de $i\infty$ ( cf. (4.2.7.1)). Utilisant [9], on trouve aisément les résultats suivants, lorsque $q \to 0$:

(i) $N = 11, 14, 15, 17, 19, 21, 49$:

$$\sigma(z) = q^{-2} + O(q^{-1}), \qquad \tau(z) = q^{-1} + O(1).$$

(ii) $N = 20$: $\sigma(z) = 5 + O(q)$, $\tau(z) = 10q + O(q^2)$.

$N = 24$: $\sigma(z) = 6 + O(q)$, $\tau(z) = 12q + O(q^2)$.

$N = 27$: $\sigma(z) = 3 + 9q + O(q^2)$, $\tau(z) = 9q + O(q^2)$.

$N = 32$: $\sigma(z) = 4 + O(q)$, $\tau(z) = 8q + O(q^2)$.

$N = 36$: $\sigma(z) = 3 + O(q)$, $\tau(z) = 6q + O(q^2)$.

Les fonctions $\sigma$ et $\tau$ sont liées par:

$(F_N)$ $\qquad \sigma^2 = F_N(\tau)$, où $F_N \in \underset{\sim}{Z}[T]$ est un polynôme de degré 4 ( resp. de degré 3), à racines distinctes.

On désigne également par $F_N$ la courbe algébrique irréductible définie sur $\underset{\sim}{Q}$ par $Y^2 = F_N(X)$.

Il résulte de la description des fonctions $\sigma, \tau$ que l'application

$$z \longmapsto (\tau(z), \sigma(z))$$

du demi-axe imaginaire dans $F_N(\underset{\sim}{R}) \subset \underset{\sim}{R}^2$ définit une bijection $C^\infty$ du demi-axe sur la branche connexe de $F_N(\underset{\sim}{R})$ qui contient des points d'abscisse arbitrairement grande ( resp. sur $(\sigma, \tau) \in F_N(\underset{\sim}{R})$ tels que $\sigma, \tau > 0$ ).

Nous allons voir que $F_N$ est un modèle de $X_N$ sur $\underset{\sim}{Q}$, et pas seulement sur $\underset{\sim}{C}$.

En effet, les fonctions $j(z)$ et $j(Nz)$ s'expriment comme des fonctions rationnelles de $\sigma$ et $\tau$, à coefficients dans $\underset{\sim}{Q}$, d'après [9]:

(4.1.0) $\qquad j = J(\sigma,\tau) \quad j_N = J'(\sigma,\tau) \quad$ où $J, J' \in \underset{\sim}{Q}(X,Y)$.

Désignons par $\Theta_N : F_N \longrightarrow X_N$ l'application rationnelle définie par (4.1.0).

LEMME 4.1.1. $\Theta_N$ est une application birationnelle.

En effet, la donnée de $j(z)$, $j(Nz)$ détermine $z$ à un élément de $\Gamma_0(N)$ près, sauf pour un nombre fini de points de $F_N$, donc détermine un unique couple $(\sigma,\tau)$, ce qui montre que $\Theta_N$ est de degré 1.

COROLLAIRE. La normalisée de $F_N$ est isomorphe sur $\underset{\sim}{Q}$ à $X_N$.

4.2. Equation de Weierstrass.

Soit X une courbe elliptique, définie sur $\underset{\sim}{Q}$ par une équation de la forme:

(4.2.0) $\qquad y^2z + \lambda xyz + \mu yz^2 = x^3 + \alpha x^2z + \beta xz^2 + \gamma z^3$ ,

où $\lambda, \mu, \alpha, \beta, \gamma \in \underset{\sim}{Z}$, l'élément neutre de la loi de groupe étant le point $(0,1,0)$.

Considérons l'ensemble des équations (4.2.0), à coefficients entiers, et qui définissent sur $\underset{\sim}{Q}$ une courbe isomorphe sur $\underset{\sim}{Q}$ à la courbe X. On définit une relation de préordre sur cet ensemble en associant à chaque équation la valeur absolue de son discriminant ( [20], p.95 ), et en prenant l'image réciproque de la relation d'ordre naturelle sur $\underset{\sim}{N}$.

DÉFINITION 4.2.1. Une équation de la forme (4.2.0), à coefficients entiers, et définissant sur $\underset{\sim}{Q}$ une courbe isomorphe à X est dite minimale si elle est minimale pour la relation de préordre ainsi définie.

Toute courbe elliptique définie sur $\mathbb{Q}$ admet une équation de la forme (4.2.0), donc une équation minimale.

On a le résultat d'unicité suivant:

PROPOSITION 4.2.2. L'équation minimale d'une courbe elliptique X définie sur $\mathbb{Q}$ est unique à un automorphisme

$$(x,y,z) \longmapsto (x+qz,\ \pm y + sx + rz,\ z)$$

près, où $q, r, s \in \mathbb{Z}$.

On trouve dans [36] ou [20 , 23] un algorithme permettant d'écrire une équation minimale en partant d'une équation (4.2.0) quelconque.

DEFINITION 4.2.3. Si (4.2.0) est une équation minimale de la courbe elliptique X définie sur $\mathbb{Q}$, on dit que la forme différentielle

$$\omega = \frac{dx}{2y + \lambda x + \mu}$$

est une forme différentielle minimale de X.

COROLLAIRE. La forme différentielle minimale d'une courbe elliptique définie sur $\mathbb{Q}$ est déterminée au signe près.

Partant des équations données par Fricke dans [9] pour la courbe $F_N$ (cf.(4.1)), on a calculé pour chacune des douze courbes modulaires elliptiques une équation minimale. Les coefficients de cette dernière, sous la forme (4.2.0), sont donnés par le tableau (4.2.6).

Soit $\sigma^2 = a\tau^4 + b\tau^3 + c\tau^2 + d\tau + e$ l'équation de $F_N$ obtenue par Fricke. Le tableau (4.2.4) donne les coefficients a,b,c,d,e et la page de [9] où on les trouve.

(4.2.4) Equation de $F_N$ :

$$\sigma^2 = a\tau^4 + b\tau^3 + c\tau^2 + d\tau + e .$$

| N | a | b | c | d | e | page |
|---|---|---|---|---|---|---|
| 11 | 1 | -20 | 56 | -44 | 0 | 406 |
| 14 | 1 | -14 | 19 | -14 | 1 | 453 |
| 15 | 1 | -10 | -13 | 10 | 1 | 439 |
| 17 | 1 | -6 | -27 | -28 | -16 | 431 |
| 19 | 1 | -16 | 64 | -76 | 0 | 411 |
| 20 | 0 | 2 | 13 | 30 | 25 | 455 |
| 21 | 1 | -6 | -17 | -6 | 1 | 442 |
| 24 | 0 | 1 | 11 | 36 | 36 | 455 |
| 27 | 0 | 1 | 0 | 0 | -432 | 388 |
| 32 | 0 | 1 | 6 | 16 | 16 | 378 |
| 36 | 0 | 1 | 6 | 12 | 9 | 455 |
| 49 | 1 | -14 | 63 | -98 | 21 | 403 |

(4.2.5) Passage à une équation minimale.

**N = 11** $\quad \sigma = \dfrac{-11.(2y + 1.)}{(x - 5)^2}$ , $\quad \tau = \dfrac{-11}{(x - 5)}$ ,

**N = 14** $\quad \sigma = \dfrac{(2y + x + 57)^2}{4(x - 9)^2} - 2(x - 9) - \dfrac{109}{4}$ ,

$$\tau = \frac{(2y + x + 57)}{2(x - 9)} + \frac{7}{2} ,$$

**N = 15**

$$\sigma = \frac{(2y + x + 46)^2}{4(x - 8)^2} - 2(x - 8) - \frac{101}{4},$$

$$\tau = \frac{(2y + x + 46)}{2(x - 8)} + \frac{5}{2},$$

**N = 17**

$$\sigma = \frac{(2y + x + 35)^2}{4(x - 7)^2} - 2(x - 7) - \frac{81}{4},$$

$$\tau = \frac{(2y + x + 35)}{2(x - 7)} + \frac{3}{2},$$

**N = 19**

$$\sigma = \frac{-19(2y + 1)}{(x - 5)^2}, \qquad \tau = \frac{-19}{(x - 5)},$$

**N = 20**

$$\sigma = \frac{y}{2}, \qquad \tau = \frac{(x - 4)}{2},$$

**N = 21**

$$\sigma = \frac{(2y + x + 21)^2}{4(x - 5)^2} - 2(x - 5) - \frac{61}{4},$$

$$\tau = \frac{(2y + x + 21)}{2(x - 5)} + \frac{3}{2},$$

**N = 24**

$$\sigma = y, \qquad \tau = x - 4,$$

**N = 27**

$$\sigma = x, \qquad \tau = \frac{1}{3}\left(y + \frac{1}{2}\right) - \frac{3}{2},$$

**N = 32**

$$\sigma = y, \qquad \tau = x - 2,$$

**N = 36**

$$\sigma = y, \qquad \tau = x - 2,$$

**N = 49**

$$\sigma = \frac{(2y + x)^2}{4(x - 2)^2} - 2(x - 2) - \frac{21}{4},$$

$$\tau = \frac{2y + x}{2(x - 2)} + \frac{7}{2}.$$

(4.2.6) Équation minimale.

(4.2.0) $$y^2z + \lambda xyz + \mu yz^2 = x^3 + \alpha x^2z + \beta xz^2 + \gamma z^3 .$$

| N | 11 | 14 | 15 | 17 | 19 | 20 | 21 | 24 | 27 | 32 | 36 | 49 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\lambda$ | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| $\mu$ | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| $\alpha$ | -1 | 0 | 1 | -1 | 1 | 1 | 0 | -1 | 0 | 0 | 0 | -1 |
| $\beta$ | -10 | 4 | -10 | -1 | -9 | 4 | -4 | -4 | 0 | 4 | 0 | -2 |
| $\gamma$ | -20 | -6 | -10 | -14 | -15 | 4 | -1 | 4 | -7 | 0 | 1 | -1 |

(4.2.7) On désigne par $\psi_N$ l'application définie sur $\mathfrak{h}_0^*$ par

$$\begin{array}{ccc} \mathfrak{h}^* & \xrightarrow{\psi_N} & X_N(\underset{\sim}{C}) \subset \underset{\sim}{P}_2(\underset{\sim}{C}) \\ z & \longmapsto & (x(z),y(z)) \end{array}$$

(cf. (4.2.5) et (4.1.))

La différentielle minimale (4.2.3) s'écrit en fonction de $\sigma$ et $\tau$ :

(i) $N = 11, 14, 15, 17, 19, 21, 49$ :

$$\omega = -d\tau / \sigma .$$

(ii) $N = 20, 24, 32, 36$:

$$\omega = d\tau / 2\sigma .$$

(iii) $N = 27$:

$$\omega = d\sigma / (6\tau + 9).$$

D'autre part (cf.(2.1)):

$\omega = f_\omega(z)\, dz$, où $f_\omega$ est un élément non-nul de l'espace vectoriel $\langle \Gamma_0(N), 2 \rangle_0$ ( de dimension 1 sur $\underset{\sim}{C}$ ).

LEMME 4.2.7.1. Soit $f \in \langle \Gamma_0(N), 2 \rangle_0$ la forme parabolique normalisée. Alors

$$f_\omega = (2\pi i) \cdot f .$$

Il suffit pour vérifier ce résultat d'utiliser les expressions qu'on vient d'obtenir pour $\omega$ et les développements en série obtenus en (4.1) pour $\sigma$ et $\tau$.

4.3. Démonstration des théorèmes (1.4.2) et (2.2.3).

(4.3.1) Notations. Soit X une courbe elliptique définie sur $\mathbb{Q}$. On désigne par $\mathcal{X}$ (resp. par $\mathcal{X}^*$) son modèle de Néron au sens faible (resp. au sens fort) (cf. [20], [21]). On note:

$\ell_p(X)$ le nombre de composantes irréductibles de la fibre géométrique de $\mathcal{X}^*$ en p,

$c_p(X)$ le nombre de composantes connexes rationnelles sur le corps $\mathbb{F}_p$ de la fibre de $\mathcal{X}$ en p,

$\mathrm{ord}_p(X)$ la valuation en p du discriminant d'une équation minimale de X.

Pour calculer le conducteur de la courbe modulaire elliptique $X_N$, on utilise le théorème suivant:

THÉORÈME 4.3.2. (Ogg [23]) Soit X une courbe elliptique définie sur $\mathbb{Q}$. L'exposant en p du conducteur de X est donné par

$$e_p(X) = \mathrm{ord}_p(X) - \ell_p(X) + 1 .$$

Le tableau (6.3.4) indique le type de la fibre du modèle de Néron (au sens fort) des courbes modulaires elliptiques $X_N$, ainsi que les valeurs de $c_p(X_N)$. (cf. (4.3.5.)). Les notations employées sont celles de Néron. La valeur de $\ell_p(X_N)$ se déduit facilement de l'examen du tableau de [20], pp. 124, 125.

(4.3.3) En utilisant le tableau (6.3.4), on vérifie cas par cas que le conducteur de la courbe modulaire elliptique $X_N$ est N, ce qui démontre le théorème (1.4.2).

(4.3.4) On vérifie de même, à l'aide des équations (4.2.6), que les facteurs locaux de la fonction L de la courbe modulaire elliptique $X_N$, aux nombres premiers p divisant N (cf. (2.2)), coïncident avec les facteurs locaux correspondants de la série de Dirichlet associée à $\Gamma_0(N)$ tels qu'ils ont été déterminés en (3.1.3). On termine ainsi la démonstration du théorème (2.2.3).

(4.3.5) Calcul de $c_p(X)$. Donnons ici quelques indications sur la façon dont on calcule les entiers $c_p(X_N)$.

Soit X une courbe elliptique définie sur $\underset{\sim}{\mathbb{Q}}$ par une équation de la forme (4.2.0) qui est de plus une équation p-standard de X au sens de [20].

On désigne par $\mathcal{X}$ le modèle de Néron au sens faible de X, et on pose

$$\mu_i = \mu/p^i, \text{etc.}$$

LEMME 4.3.5.1. $c_p(X)$ est donné par le tableau suivant (notations de [20]).

| Type de réduction en p | Valeur de $c_p$ |
|---|---|
| $(b_m)$ | $c_p(X) = m$ si $(\mathcal{X} \otimes \underset{\sim}{F}_p)^0$ est déployé sur $\underset{\sim}{F}_p$ ; $c_p(X) = \begin{cases} 1 & \text{pour m impair} \\ 2 & \text{pour m pair} \end{cases}$ dans le cas contraire. |

(suite):

| | |
|---|---|
| (c 1) | $c_p(X) = 1$ . |
| (c 2) | $c_p(X) = 2$ . |
| (c 3) | $c_p(X) = 1$ ou 3 selon que l'équation : $y^2 + \mu_1 y - \gamma_2 = 0$ a ou n'a pas des racines dans $\underset{\sim}{F}_p$ . |
| (c 4) | $c_p(X) = 1$, 2 ou 4 selon que l'équation : $x^3 + \alpha_1 x^2 + \beta_2 x + \gamma_3 = 0$ a 0, 1 ou 2 racines dans $\underset{\sim}{F}_p$ . |
| ($c\ 5_m$) | $m = 2n-1$ : $c_p(X) = 2$ ou 4 selon que l'équation : $y^2 + \mu_{n+1} y + \gamma_{2n+2} = 0$ a ou n'a pas des racines dans $\underset{\sim}{F}_p$ .<br><br>$m = 2n$ : $c_p(X) = 2$ ou 4 selon que l'équation : $\alpha_1 x^2 + \beta_{n+2} x + \gamma_{2n+3} = 0$ a ou n'a pas des racines dans $\underset{\sim}{F}_p$ . |
| (c 6) | $c_p(X) = 1$ ou 3 selon que l'équation : $y^2 + \mu_2 y - \gamma_4 = 0$ a ou n'a pas des racines dans $\underset{\sim}{F}_p$ . |
| (c 7) | $c_p(X) = 2$ . |
| (c 8) | $c_p(X) = 1$ . |

Démonstration. On peut se reporter à [20], pp. 103-122 .

Exemples.

(i) $\boxed{N = 14}$ . Les fibres du modèle de Néron en $p = 2$, $p = 7$ sont de type $(b_6)$ et $(b_3)$ respectivement, non-déployé en 2, déployé en 7. Donc $c_2(X_{14}) = 2$, et $c_7(X_{14}) = 3$.

(ii) $\boxed{N = 15}$ . Les fibres en $p = 3$, $p = 5$ sont ici de type $(b_4)$, déployé en 3, non déployé en 5. Donc $c_3(X_{15}) = 2$, et $c_5(X_{15}) = 4$.

# 5. POINTS RATIONNELS DES COURBES MODULAIRES ELLIPTIQUES.

## 5.1. Finitude de $X_N(\mathbb{Q})$.

THÉORÈME 5.1.1. *Le groupe $X_N(\mathbb{Q})$ des points de la courbe modulaire elliptique $X_N$ rationnels sur $\mathbb{Q}$ est un groupe fini.*

(5.1.2) Nous allons démontrer ce résultat en premier lieu pour les courbes modulaires elliptiques $X_N$ qui possèdent un point d'ordre 2 rationnel sur $\mathbb{Q}$, c'est à dire pour $N \in \mathcal{M}_1 - \{11, 19, 27\}$. Pour ce faire, on utilise le procédé classique de "2-descente" (cf. [5]) sous la forme donnée par Tate dans [37]. Nous renvoyons à ce dernier pour la justification des affirmations qui suivent.

*Notations.* Soit X une courbe elliptique définie sur $\mathbb{Q}$. D'après le théorème de Mordell-Weil, le groupe $X(\mathbb{Q})$ est un groupe de type fini. On appelle *rang de* X le rang du groupe libre quotient de $X(\mathbb{Q})$ par sa partie de torsion $X(\mathbb{Q})_{\text{tors}}$.

Lorsque X possède un point rationnel d'ordre 2, on peut trouver une équation de X de la forme

$$y^2 = x(x^2 + ax + b) \qquad a, b \in \mathbb{Z},$$

le point d'ordre 2 étant l'origine (0,0).

On considère alors la courbe $\bar{X}$ quotient de X par le sous-groupe d'ordre 2 engendré par (0,0):

$$y^2 = x(x^2 + \bar{a}x + \bar{b}) \qquad \text{où} \quad \bar{a} = -2a, \ \bar{b} = a^2 - 4b .$$

Soit $\alpha : X(\underset{\sim}{Q}) \longrightarrow \underset{\sim}{Q}^*/\underset{\sim}{Q}^{*2}$ l'application définie par la condition de prendre la valeur 1 sur l'élément neutre de $X(\underset{\sim}{Q})$, et par

$$\alpha(0,0) = b \pmod{\underset{\sim}{Q}^{*2}},$$

$$\alpha(x,y) = x \pmod{\underset{\sim}{Q}^{*2}} \text{ si } x \neq 0.$$

Alors $\alpha$ est un morphisme de groupes dont l'image $\alpha(X(\underset{\sim}{Q}))$ est finie. On désigne par $|X|$ l'ordre du groupe $\alpha(X(\underset{\sim}{Q}))$. Définissant de façon analogue $\overline{\alpha}$ et $|\overline{X}|$ pour la courbe $\overline{X}$, on a

$$|X|\,|\overline{X}| = 2^{r+2} \quad , \text{ r désignant le rang de X.}$$

Nous allons voir que $|X|\,|\overline{X}| = 4$ pour chacune des courbes $X_N$ où $N \in \mathcal{M}_1 - \{11, 19, 27, 32, 36\}$. Ce qui précède montre qu'il revient au même de le voir pour des courbes isogènes sur $\underset{\sim}{Q}$ aux courbes en question. Nous ne traitons pas les cas de $X_{32}$ et $X_{36}$: Le fait que ces deux courbes n'ont qu'un nombre fini de points rationnels sur $\underset{\sim}{Q}$ est bien connu (cf. par exemple [33] ).

Soit $(x,y)$ un point de X: $y^2 = x(x^2 + ax + b)$ rationnel sur $\underset{\sim}{Q}$, avec $y \neq 0$. Un tel point s'écrit:

$$(5.1.2.0) \qquad x = b_1 M^2/e^2 \ , \quad y = b_1 MR/e^3$$

où e, M, R, $b_1$ sont des éléments de $\underset{\sim}{Z}$, et où $b_1$ est un diviseur de b. Posant $b_2 = b/b_1$ , on peut supposer de plus que les conditions suivantes sont vérifiées:

$$(M,e) = (R,e) = (b_1,e) = 1$$

$$(b_2,M) = (M,R) = 1. \qquad \text{(cf. [37], p.5-5 ).}$$

L'image $\alpha(X(\underset{\sim}{Q}))$ est le sous-groupe de $\underset{\sim}{Q}^*/\underset{\sim}{Q}^{*2}$ formé des classes modulo $\mathbb{Q}^{*2}$ de 1, b et des $b_1$ tels que l'équation

$$(5.1.2.1) \qquad R^2 = b_1 M^4 + aM^2e^2 + b_2 e^4$$

ait une solution entière (M,R) non-triviale.

(5.1.3) Démonstration du théorème (5.1.1) pour N = 14, 15, 17, 20, 21, 24 et 49.

On utilise les notations et les résultats de (5.1.2).

**N = 14** On prend pour X la courbe $C_{14}$ (cf.(7.5.5)).

$$X: \quad y^2 = x^3 - 11x^2 + 32x$$
$$\overline{X}: \quad y^2 = x^3 + 22x^2 - 7x$$

(i) X possède les points rationnels (8,8) et (4,-4) qui donnent $b_1 = 2$, $b_1 = 1$ respectivement.

D'autre part, $b = 32$, donc $b_1 \in \{\pm 1, \pm 2 \ (\text{mod. } \mathbb{Q}^{*2})\}$.

On doit donc examiner si

$$(1) \qquad R^2 = -M^4 - 11\, M^2e^2 - 32\, e^4 \ ,$$
$$(11) \qquad R^2 = -2\, M^4 - 11\, M^2e^2 - 16\, e^4 ,$$

ont ou n'ont pas de solutions entières non-triviales.

Or il est clair que (1) et (11) n'ont pas de solutions non-nulles dans $\mathbb{R}$.

Donc $\alpha(X(\mathbb{Q})) = \{1, 2 \ (\text{mod. } \mathbb{Q}^{*2})\}$.

(ii) Le point (0,0) de $\overline{X}$ donne $\overline{b}_1 = -7$. D'autre part, $\overline{b}_1 \in \{\pm 1, \pm 7 \ (\text{mod. } \mathbb{Q}^{*2})\}$.

On doit donc examiner l'équation

$$(111) \qquad R^2 = -M^4 + 22\, M^2e^2 + 7\, e^4 .$$

Cette dernière entraîne modulo 8:

$$R^2 \equiv -(M^2 + e^2)^2 \ ,$$

ce qui entraîne

$$\text{soit} \quad R^2 \equiv 0 \ (\text{mod. } 8) \quad M^2 + e^2 \equiv 0 \ (\text{mod. } 8),$$
$$\text{soit} \quad R^2 \equiv 4 \ (\text{mod. } 8) \quad M^2 + e^2 \equiv 4 \ (\text{mod. } 8),$$

en tous cas

$$M^2 \equiv -e^2 \ (\text{mod. } 4) \quad \text{donc} \quad M^2 \equiv e^2 \equiv 0 \ (\text{mod. } 4).$$

Or $(M,e) = 1$.

Par conséquent $\alpha(\overline{X}(\underset{\sim}{Q})) = \{+1, -7 \pmod{\underset{\sim}{Q}^{*2}}\}$.

Donc $|X|\,|\overline{X}| = 4$.

**N = 15** On prend pour X la courbe $C_{15}$ (cf. (7.5.5)).

$$X: \quad y^2 = x^3 - 7x^2 + 16x$$

$$\overline{X}: \quad y^2 = x^3 + 14x - 15x$$

(i) On a pour la courbe X: $b_1 \in \{\pm 1, \pm 2 \pmod{\underset{\sim}{Q}^{*2}}\}$.

L'équation (5.1.2.1) s'écrit

$$R^2 = b_1 M^4 - 7M^2e^2 + b_2 e^4, \text{ avec } b_1 b_2 = +16.$$

Elle n'a donc pas de solutions réelles non-nulles lorsque $b_1 < 0$.

D'autre part

$$(1) \quad R^2 = 2M^4 - 7M^2e^2 + 8e^4$$

entraîne <u>modulo</u> 4:

$$R^2 \equiv M^2(2M^2 + e^2)$$

d'où: soit $M^2 \equiv 0 \pmod 4$ $R^2 \equiv 0 \pmod 4$, or $(M,R) = 1$,

soit $M^2 \equiv 1 \pmod 4$ et $R^2 \equiv e^2 + 2 \pmod 4$,

donc $R^2 \equiv 2$ ou $-1 \pmod 4$, ce qui est impossible.

Par conséquent

$$\alpha(X(\underset{\sim}{Q})) = \{1 \pmod{\underset{\sim}{Q}^{*2}}\}.$$

(ii) Les points $(1,0)$, $(5,20)$, $(-3,12)$, $(15,0)$ de $\overline{X}$ donnent respectivement

$$b_1 \equiv 1, 5, -3, -15 \pmod{\underset{\sim}{Q}^{*2}}.$$

On est ramené à étudier:

$$(1) \qquad R^2 = -M^4 + 14\,M^2e^2 + 15\,e^4$$

$$(11) \qquad R^2 = 3\,M^4 + 14\,M^2e^2 - 5\,e^4.$$

(1) entraîne modulo 8 :

$R^2 \equiv -(M^2 + e^2)^2 \pmod 8$, qui n'a pas de solutions vérifiant les conditions voulues, comme on l'a déja vu.

(11) s'écrit modulo 16

$$R^2 \equiv 3\,(M^2 - 3e^2)^2 \pmod{16},$$

ce qui entraîne

$$R^2 \equiv 0 \pmod{16} \quad \text{et} \quad (M^2 - 3e^2)^2 \equiv 0 \pmod{16},$$

d'où $M^2 + e^2 \equiv 0 \pmod 4$, donc $M^2 \equiv e^2 \equiv 0 \pmod 4$. Or $(M,e) = 1$.

On en déduit

$$\alpha(\overline{X}(\mathbb{Q})) = \{1, 5, -3, -15 \pmod{\mathbb{Q}^{*2}}\}.$$

Donc $|X||\overline{X}| = 4$.

**N = 17** On prend pour X la courbe $A_{17}$ (cf. (7.5.5)).

$$X: \quad y^2 = x^3 + 9x^2 + 16x$$

$$\overline{X}: \quad y^2 = x^3 - 18x^2 + 17x$$

(i) Le point $(-4,4)$ de X donne $b_1 \equiv -1 \pmod{\mathbb{Q}^{*2}}$.

D'autre part $b_1 \in \{\pm 1, \pm 2 \pmod{\mathbb{Q}^{*2}}\}$. On doit donc examiner:

$$(1) \qquad R^2 \equiv \pm 2\,M^4 + 9\,M^2e^2 \pm 8\,e^4,$$

qui entraîne modulo 4:

$R^2 \equiv M^2\,(2M^2 + e^2)$, équation qu'on a déja rencontrée, et qui n'a pas de solutions non-triviales modulo 4 vérifiant les conditions voulues.

On en conclut

$$\alpha(X(\mathbb{Q})) = \{\pm 1 \pmod{\mathbb{Q}^{*2}}\}.$$

(ii) On a pour $\overline{X}$: $b_1 \in \{\pm 1, \pm 17 \pmod{\mathbb{Q}^{*2}}\}$.

L'équation (5.1.2.1) n'a pas de solutions réelles non-nulles lorsque $b_1 < 0$. Donc

$$\alpha(\overline{X}(\mathbb{Q})) = \{+1, +17 \pmod{\mathbb{Q}^{*2}}\}, \text{ et } |X||\overline{X}| = 4.$$

**N = 20** On prend pour X la courbe $X_{20}$.

$$X: \quad y^2 = x^3 - 2x^2 + 5x \ .$$
$$\overline{X}: \quad y^2 = x^3 + 4x^2 - 16x \ .$$

(i) On a pour X: $b_1 \in \{\pm 1, \pm 5 \pmod{\mathbb{Q}^{*2}}\}$,
et l'équation (5.1.2.1) n'a pas de solutions réelles non-nulles lorsque $b_1 < 0$.

Donc $$\alpha(X(\mathbb{Q})) = \{+1, +5 \pmod{\mathbb{Q}^{*2}}\}.$$

(ii) Pour $\overline{X}$: $b_1 \in \{\pm 1, \pm 2 \pmod{\mathbb{Q}^{*2}}\}$, et le point (0,0) donne $b_1 = -1$.

On doit donc examiner:

$$(1) \quad R^2 = 2M^4 + 4M^2e^2 - 8e^4 \ ,$$
$$(11) \quad R^2 = -2M^4 + 4M^2e^2 + 8e^4 \ ,$$

qui entraînent <u>modulo</u> 4:

$$R^2 \equiv 2M^4 \ . \text{ Or } (M,R) = 1.$$

Donc $$\alpha(\overline{X}(\mathbb{Q})) = \{\pm 1 \pmod{\mathbb{Q}^{*2}}\},$$
et $|X||\overline{X}| = 4$.

**N = 21**

On prend pour X la courbe $C_{21}$ (cf. (7.5.5)):

$$X: \quad y^2 = x^3 + x^2 + 16\,x \ .$$
$$\overline{X}: \quad y^2 = x^3 - 2\,x^2 - 63\,x \ .$$

(i) Pour la courbe X: $b_1 \in \{\pm 1 \ (\text{mod.} \ \mathbb{Q}^{*2})\}$.

On doit donc examiner

$$(I) \quad R^2 = \pm 2\,M^4 + M^2e^2 \pm 8\,e^4 \ ,$$
$$(II) \quad R^2 = -M^4 + M^2e^2 - 16\,e^4 \ ,$$
$$(III) \quad R^2 = -4\,M^4 + M^2e^2 - 4\,e^4 \ .$$

(I) entraîne <u>modulo</u> 4:

$R^2 \equiv M^2\,(2\,M^2 + e^2)$, équation déja rencontrée.

Le second membre de (II, III) est défini négatif, donc (II, III) n'ont pas de solutions réelles non-triviales.

Donc $\alpha(X(\mathbb{Q})) = \{1 \ (\text{mod.} \ \mathbb{Q}^{*2})\}$.

(ii) Les points (0,0), (-3,-12) et (21,84) de $\overline{X}$ donnent $b_1 = -7, -3$ et 21 respectivement.

On doit examiner:

$$(I) \quad R^2 = -M^4 - 2\,M^2e^2 + 63\,e^4 \ ,$$
$$(II) \quad R^2 = -9\,M^4 - 2\,M^2e^2 + 7\,e^4 \ ,$$
$$(III) \quad R^2 = 3\,M^4 - 2\,M^2e^2 - 21\,e^4 \ .$$

(I) entraîne <u>modulo</u> 16:

$$R^2 \equiv -(M^2 + e^2)^2 \quad (\text{mod.}16),$$

donc $R^2 \equiv 0 \quad (\text{mod.}16)$ et $(M^2 + e^2)^2 \equiv 0 \ (\text{mod.}16)$,

soit $M^2 + e^2 \equiv 0 \ (\text{mod.}4)$, donc $M^2 \equiv e^2 \equiv 0 \ (\text{mod.}4)$. Or $(M,e)=1$

(II) entraîne modulo 16 :

$$R^2 \equiv 7\,(M^2 + e^2)^2 \pmod{16},$$

ce qui entraîne là encore

$$R^2 \equiv 0 \pmod{16} \quad \text{et} \quad (M^2 + e^2)^2 \equiv 0 \pmod{16}.$$

(III) entraîne modulo 16 :

$$R^2 \equiv 3\,(M^2 - 3e^2)^2 \pmod{16}$$

donc $R^2 \equiv 0 \pmod{16}$ et $(M^2 - 3e^2)^2 \equiv 0 \pmod{16}$,

d'où $M^2 + e^2 \equiv 0 \pmod{4}$, soit $M^2 \equiv e^2 \equiv 0 \pmod{4}$,

or $(M,e) = 1$.

Donc $\alpha(\overline{X}(\underset{\sim}{Q})) = \left\{1, -3, -7, 21 \pmod{\underset{\sim}{Q}^{*2}}\right\}$,

et $|X|\cdot|\overline{X}| = 4$.

**N = 24** On prend pour X la courbe $X_{24}$.

$$X : \quad y^2 = x^3 + 5x^2 + 4x .$$

$$\overline{X} : \quad y^2 = x^3 - 10\,x^2 + 9x .$$

(i) Les points $(-4,0)$, $(-1,0)$, $(2,6)$ et $(-2,2)$ de X donnent $b_1 = 1, -1, 2, -2 \pmod{\underset{\sim}{Q}^{*2}}$ respectivement. D'où :

$$\alpha(X(\underset{\sim}{Q})) = \left\{\pm 1, \pm 2 \pmod{\underset{\sim}{Q}^{*2}}\right\}.$$

(ii) L'équation (5.1.2.1) associée à $\overline{X}$ n'a pas de solutions réelles non-nulles lorsque $b_1 < 0$.

On est ramené à examiner

$$(1) \qquad R^2 = 3M^4 - 10\,M^2e^2 + 3e^4,$$

qui entraîne modulo 3 :

$$R^2 \equiv -M^2e^2,$$

d'où $R^2 \equiv M^2e^2 \equiv 0 \pmod{3}$. Or $(R,e) = (R,M) = 1$.

Donc $\alpha(\overline{X}(\underset{\sim}{Q})) = \left\{1 \pmod{\underset{\sim}{Q}^{*2}}\right\}$, et $|X|\cdot|\overline{X}| = 4$.

**N = 49** On prend pour X la courbe $A_{49}$ (cf. (7.5.5)).

$$X: \quad y^2 = x^3 + 2x^2 + 11.2\,x$$
$$\bar{X}: \quad y^2 = x^3 - 42x^2 - 7x.$$

(i) On a pour la courbe X :

$b_1 \in \{\pm 1, \pm 2, \pm 7, \pm 14 \pmod{\mathbb{Q}^{*2}}\}$, et le point (0,0) donne $b_1 = 7$.

Il reste donc à examiner:

$$(I) \quad R^2 = -M^4 + 21\,M^2e^2 - 11.2\,e^4 ,$$
$$(II) \quad R^2 = 2M^4 + 21\,M^2e^2 + 56\,e^4 ,$$
$$(III) \quad R^2 = -2M^4 + 21\,M^2e^2 - 56\,e^4 ,$$
$$(IV) \quad R^2 = -4M^4 + 21\,M^2e^2 - 28\,e^4 ,$$
$$(V) \quad R^2 = 8M^4 + 21\,M^2e^2 + 14\,e^4 ,$$
$$(VI) \quad R^2 = -8M^4 + 21\,M^2e^2 - 14\,e^4 ,$$
$$(VII) \quad R^2 = -16\,M^4 + 21\,M^2e^2 - 7\,e^4 .$$

<u>modulo 7</u>

(I) et (VI) entraînent:

$R^2 \equiv -M^4 \pmod 7$, donc $R^2 \equiv M^4 = 0 \pmod 7$.

Or $(M,R) = 1$.

(III) et (VII) entraînent:

$R^2 \equiv -2M^4 \pmod 7$, donc $R^2 \equiv M^4 \equiv 0 \pmod 7$.

(IV) entraîne:

$R^2 \equiv 3M^4 \pmod 7$, donc $R^2 \equiv M^4 \equiv 0 \pmod 7$.

<u>modulo 4</u>

(II) et (V) entraînent respectivement

$R^2 \equiv M^2(2M^2 + e^2)$ et $R^2 \equiv e^2(2e^2 + M^2)$,

déja rencontrées.

Par conséquent

$$\alpha(X(\underset{\sim}{Q})) = \{1, 7 \pmod{\underset{\sim}{Q}^{*2}}\}.$$

(ii) Pour la courbe $\overline{X}$, $b_1 \in \{\pm 1, \pm 7 \pmod{\underset{\sim}{Q}^{2}}\}$, et le point $(0,0)$ donne $b_1 = -7$.

On doit donc examiner l'équation :

$$R^2 = -M^4 - 42\, M^2 e^2 + 7\, e^4,$$

qui entraîne modulo 7 :

$$R^2 = -M^4 \pmod{7},$$

équation déja rencontrée plus haut.

D'où $\alpha(\overline{X}(\underset{\sim}{Q})) = \{1, 7 \pmod{\underset{\sim}{Q}^{*2}}\}$, et $|X|\cdot|\overline{X}| = 4$.

(5.1.4) Pour terminer la démonstration du théorème (5.1.1), il reste à examiner le cas des trois courbes modulaires elliptiques $X_{11}$, $X_{19}$ et $X_{27}$.

Le résultat est connu pour $X_{11}$ (cf. [35]).

La courbe $X_{27}$ est isogène sur $\underset{\sim}{Q}$ à la courbe $y^2 = x^3 - 11x + 6$, dont le rang est nul d'après les tables de Birch et Swinnerton-Dyer (cf. [2], [3]).

Le fait que $X_{19}$ a un nombre fini de points rationnels sur $\underset{\sim}{Q}$ est démontré par Mazur dans [17] (table 1 p.258, ou prop. 10.2). Nous allons en donner une démonstration plus élémentaire. Pour cela, il nous suffira de modifier quelque peu la démonstration de Sansone et Cassels [41].

(5.1.5) Démonstration du théorème (5.1.1.) pour $N = 19$.

La courbe $X_{19}$ est la courbe elliptique d'équation:

$$Y^2Z + YZ^2 = X^3 + X^2Z - 9\,XZ^2 - 15\,Z^3$$

( cf. (4.2.0) ).

Posons:

$$\begin{cases} X = 4(x + y) + 9\,z\,, \\ Y = -8\,x + 11\,y + z\,, \\ Z = -3(x + y) - 2\,z\,. \end{cases}$$

On obtient l'équation:

$$x^3 + y^3 + z^3 = 2\,xyz\,. \tag{1}$$

Il s'agit de voir que l'équation (1) n'a pas de solutions entières non-triviales, c'est à dire autres que celles définies par $xyz = 0$.

Supposons qu'il n'en soit pas ainsi, et choisissons parmi les solutions non-triviales une solution $(x,y,z)$ telle que $|xyz|$ soit minimal. On peut supposer par exemple que $3$ ne divise pas $z$.

Posons:

$$\begin{cases} x_1 = 3\,x + 3\,y + 2\,z\,, \\ y_1 = 3\zeta\,x + 3\zeta^2\,y + 2\,z\,, \\ \bar{y}_1 = 3\zeta^2\,x + 3\zeta\,y + 2\,z\,, \end{cases} \tag{2}$$

où $\zeta$ est une racine primitive 3-ième de l'unité. On obtient:

$$19\,(x_1 + y_1 + \bar{y}_1)^3 = -6^3 \cdot x_1 y_1 \bar{y}_1\,. \tag{3}$$

Soit $K = \mathbb{Q}(\zeta)$ le 3-corps cyclotomique. L'anneau des entiers $O_K = \mathbb{Z}[\zeta]$ de $K$ est principal. Le seul idéal premier ramifié est $3$:

$$3.O_K = \mathfrak{q}^2.O_K \qquad \mathfrak{q} = (\zeta - \zeta^2).O_K\,.$$

L'idéal $19$ se décompose en produit d'idéaux premiers:

$$19.O_K = (5+3\zeta)(5+3\zeta^2).O_K\,.$$

L'équation (3) s'écrit:

$$(4) \qquad (5+3\zeta)(5+3\zeta^2)(x_1 + y_1 + \bar{y}_1)^3 = (\zeta-\zeta^2)^6\, 2^3\, xy\bar{y}_1 \,.$$

On voit comme dans [41] que le pgcd de $x_1$, $y_1$, $\bar{y}_1$ est un entier rationnel $\ell$. On pose:

$$(5) \qquad x_1 = \ell x_2 \,,\; y_1 = \ell y_2 \,.$$

On obtient l'équation (6) analogue à (4), où $x_1$, $y_1$, $\bar{y}_1$ sont remplacés par $x_2$, $y_2$, $\bar{y}_2$. La factorisation de (6) amène à distinguer trois cas:

Cas 1. Supposons que $(5+3\zeta)$ divise $x_2$. L'équation (6) s'écrit:

$$(7) \qquad (x_2 + y_2 + \bar{y}_2)^3 = -2^3 \cdot 3^3 \cdot \frac{x_2}{19}\, y_2\bar{y}_2 \,.$$

On peut donc trouver $x_3 \in \underset{\sim}{Z}$, $y_3 \in O_K$ tels que:

$$(8) \qquad \begin{cases} x_2 = 19\, x_3^3 \,, \\ y_2 = -\zeta^j \cdot y_3^3 \,, \\ \bar{y}_2 = -\zeta^{2j} \cdot \bar{y}_3^3 \,, \end{cases} \qquad j = 0,\ 1,\ \text{ou}\ 2,$$

vérifiant:

$$(9) \qquad 19\, x_3^3 - \zeta^j \cdot y_3^3 - \zeta^{2j} \cdot \bar{y}_3^3 = -6\, x_3 y_3 \bar{y}_3 \,.$$

Cas 2. Supposons que $(5+3\zeta)$ divise $y_2$. On obtient:

$$(10) \qquad \begin{cases} x_2 = x_3^3 \,, \\ y_2 = -\zeta^j (5+3\zeta)\, y_3^3 \,, \\ \bar{y}_2 = -\zeta^{2j}(5+3\zeta^2)\, \bar{y}_3^3 \,, \end{cases}$$

$$(11) \qquad x_3^3 - \zeta^j(5+3\zeta)\, y_3^3 - \zeta^{2j}(5+3\zeta^2)\, \bar{y}_3^3 = -6\, x_3 y_3 \bar{y}_3 \,.$$

Cas 3. Supposons enfin que $(5+3\zeta)$ divise $\bar{y}_2$. On obtient l'analogue du cas 2, où on a permuté $(5+3\zeta)$ et $(5+3\zeta^2)$.

Dans tous les cas:

(12) $\qquad (\zeta - \zeta^2)$ ne divise pas $x_3\, y_3\, \bar{y}_3$ .

3 étant totalement ramifié, on a :

$$\mathbb{F}_3 = \mathbb{Z} / 3\mathbb{Z} \cong O_K / \mathfrak{q} ,$$

et par conséquent:

$$\begin{cases} x_3 \equiv \pm 1 \pmod{\mathfrak{q}} , \\ y_3 \equiv \pm 1 \pmod{\mathfrak{q}} , \end{cases}$$

d'où

$$(13) \qquad \begin{cases} x_3^3 \equiv \pm 1 \pmod{9}, \\ y_3^3 \equiv \bar{y}_3^3 \equiv \pm 1 \pmod{9}, \\ -6\, x_3\, y_3\, \bar{y}_3 \not\equiv 0 \pmod{9}. \end{cases}$$

Cas 1. (9) entraîne modulo 3:

$$x_3^3 - (\zeta^j + \zeta^{2j})\, y_3^3 \equiv 0 \pmod{3}$$

soit

$$x_3^3 + y_3^3 \equiv 0 \pmod{3},$$

soit, à cause de (13):

$$x_3^3 \equiv - y_3^3 \pmod{9},$$

et (9) entraîne modulo 9:

$$-y_3^3 - (\zeta^j + \zeta^{2j})\, y_3^3 \equiv -6\, x_3\, y_3\, \bar{y}_3$$

ce qui entraîne d'après (13)

$$j = 0 .$$

On pose alors:

$$(15) \qquad \begin{cases} 6\, x_3 = x_4 + y_4 + z_4 , \\ 3\, y_3 = x_4 + \zeta\, y_4 + \zeta^2 z_4 , \\ 3\, \bar{y}_3 = x_4 + \zeta^2 y_4 + \zeta z_4 , \end{cases}$$

où $x_4 , y_4 , z_4 \in \mathbb{Z}$. Alors (9) s'écrit:

(16) $$(x_4 + y_4 + z_4)^3 = 8\, x_4\, y_4\, z_4 \ .$$

On peut donc trouver des entiers rationnels $m, x_5, y_5, z_5$, vérifiant:

$$\begin{cases} x_4 = m\, x_5^3 \ , \\ y_4 = m\, y_5^3 \ , \\ z_4 = m\, z_5^3 \ , \end{cases}$$

et

$$x_5^3 + y_5^3 + z_5^3 = 2\, x_5\, y_5\, z_5 \ .$$

Raisonnant comme dans [41], on arrive à une contradiction.

Cas 2. Le même type de raisonnement que dans le cas 1 montre qu'on a nécessairement $j = 0$ dans (11).

Posant cette fois:

(17) $$\begin{cases} 3\, x_3 = x_4 + y_4 + z_4 \ , \\ 3\, y_3 = x_4 + \zeta y_4 + \zeta^2 z_4 \ , \\ 3\, \bar{y}_3 = x_4 + \zeta^2 y_4 + \zeta\, z_4 \ , \end{cases}$$

on obtient:

(18) $$x_4^2 y_4 + y_4^2 z_4 + z_4^2 x_4 = 2\, x_4\, y_4\, z_4 \ ,$$

donc

$$\begin{cases} x_4 = m\, y_5\, z_5^2 \ , \\ y_4 = m\, z_5\, x_5^2 \ , \\ z_4 = m\, x_5\, y_5^2 \ , \end{cases}$$

avec $m, x_5, y_5, z_5 \in \underset{\sim}{Z}$, et

$$x_5^3 + y_5^3 + z_5^3 = 2\, x_5\, y_5\, z_5 \ .$$

On conclut comme dans [41]. De même pour le cas 3.

5.2. Points d'ordre fini.

D'après le théorème (5.1.1), la détermination des points rationnels de la courbe modulaire elliptique $X_N$ se réduit à la détermination des points rationnels d'ordre fini.

On connaît d'autre part un point rationnel d'ordre fini, à savoir la pointe $P_1$ ( on rappelle que la pointe $P_N$ est choisie comme élément neutre de la loi de groupe). L'ordre de la pointe $P_1$ a été déterminé en (3.3).

Enfin, il est facile d'obtenir une borne de l'ordre $\eta_0(X_N)$ du groupe $X_N(\underset{\sim}{Q}) = X_N(\underset{\sim}{Q})_{tors}$ en utilisant la

PROPOSITION 5.2.1. *Soit* $X$ *une courbe elliptique définie sur* $\underset{\sim}{Q}$, *et soit* $\mathcal{X}$ *son modèle de Néron* ( au sens faible). *L'application de réduction modulo* $p$

$$X(\underset{\sim}{Q})_{tors} \longrightarrow (\mathcal{X} \otimes_{\underset{\sim}{Z}} \underset{\sim}{F}_p)(\underset{\sim}{F}_p)$$

*est injective sur la partie de* $X(\underset{\sim}{Q})_{tors}$ *d'ordre premier à* $p$.

Cette proposition est une conséquence du fait que le noyau ${}_n\mathcal{X}$ de la multiplication par $n$ dans $\mathcal{X}$ est étale au-dessus d'un ouvert de $\mathrm{Spec}(\underset{\sim}{Z})$ contenant $p$, lorsque $(n,p)=$ ( SGA 7, IX ), et de ce qu'une section d'un morphisme étale au-dessus d'un ouvert connexe est déterminée par sa valeur en un point ( SGA 1, I.5.3).

*Remarque* (5.2.2). Soit $X$ une courbe elliptique ayant bonne réduction en $p$. Le nombre $m_p(X)$ des points de $\mathcal{X} \otimes \underset{\sim}{F}_p$ rationnels sur $\underset{\sim}{F}_p$ est donné par

$$m_p(X) = 1 - \mathrm{Tr}(\pi_p) + p \ ,$$

où $Tr(\mathcal{T}_p)$ est la trace de l'endomorphisme de Frobenius de $\mathcal{X} \otimes \underset{\sim}{F}_p$.

D'autre part, d'après (2.2), lorsque X est une courbe modulaire elliptique,

$$Tr(\mathcal{T}_p) = \lambda(p) ,$$

$\lambda(p)$ désignant la valeur propre de l'opérateur de Hecke T(p).

On peut donc dans ce cas, pour les petites valeurs de p ne divisant pas N, calculer $m_p(X_N)$ en utilisant les développements en série obtenus en (3.1.2), donc sans avoir à utiliser une équation de $X_N$.

On obtient ainsi les résultats rassemblés dans le tableau (5.2.2.1).

(5.2.2.1) Tableau.

Dans ce tableau, on désigne par $\eta_0$ l'ordre de $X_N(\underset{\sim}{Q})$, et par $m_p$ l'ordre de $(\mathcal{X}_N \otimes \underset{\sim}{F}_p)(\underset{\sim}{F}_p)$, groupe des points de la fibre en p du modèle de Néron qui sont rationnels sur $\underset{\sim}{F}_p$.

| N | $m_2$ | $m_3$ | $m_5$ | $m_7$ | $m_{11}$ | $m_{13}$ | $m_{17}$ | $m_{19}$ | Majoration de $\eta_0$ |
|---|---|---|---|---|---|---|---|---|---|
| 11 | 5 | 5 | 5 | 10 | — | 10 | 20 | 20 | 5 |
| 14 | — | 6 | 6 | — | 12 | 18 | 12 | 18 | 6 |
| 15 | 4 | — | — | 8 | 16 | 16 | 16 | 16 | 8 |
| 17 | 4 | 4 | 8 | 4 | 12 | 16 | — | 24 | 4 |
| 19 | 3 | 6 | 3 | 9 | 9 | 18 | 21 | — | 3 |
| 20 | — | 6 | — | 6 | 12 | 12 | 24 | 24 | 6 |
| 2 | 4 | — | 8 | — | 16 | 16 | 24 | 16 | 8 |
| 24 | — | — | 8 | 8 | 8 | 16 | 16 | 24 | 8 |
| 27 | 3 | — | 6 | 9 | 12 | 9 | 18 | 27 | 3 |
| 32 | — | 4 | 8 | 8 | 12 | 8 | 16 | 20 | 4 |
| 36 | — | — | 6 | 12 | 12 | 12 | 18 | 12 | 6 |
| 49 | 2 | 2 | 6 | — | 8 | 14 | 18 | 22 | 2 |

La comparaison des tableaux (5.2.2.1) et (3.3.1) montre immédiatement que la pointe $P_1$ engendre le groupe $X_N(\underset{\sim}{Q})$ tout entier lorsque $N \in \mathcal{M}_1 - \{15, 21, 24\}$, et un sous-groupe de $X_N(\underset{\sim}{Q})$ d'indice au plus 2 pour les trois niveaux $N = 15, 21,$ et $24$. D'autre part, on remarque que le groupe de Lie réel $X_N(\underset{\sim}{R})$ est connexe pour $N \in \mathcal{M}_1 - \{15,21,24\}$ et qu'il a deux composantes connexes lorsque $N = 15, 21, 24$.

Nous allons voir que pour ces trois valeurs de $N$, la pointe $P_1$ engendre le sous-groupe $X_N(\underset{\sim}{Q}) \cap X_N(\underset{\sim}{R})^0$ des points de la composante neutre $X_N(\underset{\sim}{R})^0$ de $X_N(\underset{\sim}{R})$ qui sont rationnels sur $\underset{\sim}{Q}$, que $X_N(\underset{\sim}{Q}) \cap X_N(\underset{\sim}{R})^0$ est d'indice 2 dans $X_N(\underset{\sim}{Q})$, et que $X_N(\underset{\sim}{Q})$ est engendré par l'ensemble des pointes de $X_N$ rationnelles sur $\underset{\sim}{Q}$.

Reprenons les notations de (4.2.7). L'image de $z = i\infty$ par $\psi_N$ est un point rationnel sur la courbe $X_N \subset \underset{\sim}{P}_2$ d'équation (4.2.0). Faisant suivre $\psi_N$ de la translation par $-\psi_N(i\infty)$, on obtient:

$$\psi_N : \mathcal{H}^* \longrightarrow X_N(\underset{\sim}{C}) \subset \underset{\sim}{P}_2(\underset{\sim}{C}) \tag{5.2.2.2}$$

qui envoie $i\infty$ sur l'élément neutre $(0,1,0)$ de $X_N$.

(5.2.3) Points rationnels.

(i) Points rationnels de $X_{15}$.

On a pris pour équation minimale de $X_{15}$ (cf. (4.2.6)):

$$y^2 + xy + y = x^3 + x^2 - 10x - 10 .$$

La pointe $P_1$ est un point d'ordre 4. Utilisant (4.1) et (4.2.5), on voit que ses coordonnées sont $(8,-27)$.

Les involutions $W_{15}$, $W_3$, $W_5$ s'écrivent, dans les coordonnées $(\sigma, \tau)$:

$$W_{I5}(\sigma,\tau) = (-\sigma, \tau),$$

$$W_3(\sigma,\tau) = (\sigma/\tau^2, -1/\tau),$$

$$W_5(\sigma,\tau) = (-\sigma/\tau^2, -1/\tau),$$

comme on le voit facilement en remarquant que $W_{15}$ échange les pointes $P_1$ et $P_{15}$, et que $W_3$ n'a pas de points fixes ( puisque $\lambda(3) = 1$, d'après (3.1.3)).

La définition de $W_3$ en termes de matrices montre que $W_3(P_{15}) = P_5$. Il en résulte que $P_5$ est un point rationnel d'ordre 2, et que $W_3$ est la translation par $P_5$. L'expression obtenue pour $W_3$ permet de calculer les coordonnées de $P_5$, qui sont $(-1,0)$.

De même, $W_3(P_1) = P_3$, soit $P_1 + P_5 = P_3$, ce qui montre que $P_3$ est un point d'ordre 4.

On peut donc donner la liste des points rationnels de $X_{15}$ :

$P_{15}$ ; $P_3 = (-2,-2)$ ,

$P_1 = (8,-27)$ , $P_5 = (-1,0)$ ,

$2P_1 = (3,-2)$ , $P_5+3P_1 = (-2,3)$ ,

$3P_1 = (8,18)$ , $P_5+2P_1 = (-13/4,9/8)$,

et l'expression des involutions $W_3$ , $W_5$ , $W_{15}$ :

$W_3(P) = P + P_5$ , $W_5(P) = P_3 - P$ , $W_{15}(P) = P_1 - P$ .

On vérifie bien les résultats annoncés. Le tableau (5.2.4) indique la structure de $X_{15}(\underset{\sim}{R})$ et $X_{15}(\underset{\sim}{Q})$.

(ii) Points rationnels de $X_{21}$ .

On a pris pour équation minimale de $X_{21}$ :

$$y^2 + xy = x^3 - 4x - 1. \qquad \text{(cf. (4.2.6))}.$$

Procédant de la même façon que pour $X_{15}$, on établit ce qui suit:

Les involutions $W_{21}$, $W_3$, $W_7$ s'écrivent

$$W_{21}(\sigma, \tau) = (-\sigma, \tau),$$

$$W_3(\sigma, \tau) = (\sigma/\tau^2, 1/\tau),$$

$$W_7(\sigma, \tau) = (-\sigma/\tau^2, 1/\tau).$$

ou, en termes de la loi de groupe :

$W_3(P) = P_7 - P$ , où $P_7$ est d'ordre 4,

$W_7(P) = P + P_3$ , et $P_3$ est d'ordre 2,

$W_{21}(P) = P_1 - P$ .

Le groupe $X_{21}(\mathbb{Q})$ est d'ordre 8 , et engendré par les pointes:

$P_{21}$ , $\qquad P_3 = (-2,1)$ ,

$P_1 = (5,-3)$ , $\qquad P_7 = (-1,2)$ ,

$2P_1 = (2,-1)$ , $\qquad 3P + P_3 = (-1,-1)$ ,

$3P_1 = (5,8)$ , $\qquad 2P_1 + P_3 = (-1/4, 1/8)$ .

(iii) Points rationnels de $X_{24}$ .

On a pris pour équation minimale de $X_{24}$ (cf. (4.2.6)

$$y^2 = x^3 - x^2 - 4x + 4^{\circ}.$$

Pour chaque diviseur positif d de 24, il existe une pointe $P_d$ et une seule de niveau d. On obtient ainsi tous les points rationnels de $X_{24}$.

Le fait que $\lambda(3) = -1$ (cf. (3.3)) montre que $W_3$ est une translation par un point d'ordre 2, à savoir $P_8$. D'autre part, d'après Fricke [9], on a :

$$\tau(1/2) = -2, \quad \tau(1/3) = -3, \quad \tau(1/4) = -4, \quad \tau(1/6) = 6.$$

Utilisant les équations (4.2.5), on obtient les coordonnées des pointes.

$P_{24}$ ,  $P_8 = (1,0)$ ,

$P_2 = (4,6)$ ,  $P_3 = (0,-2)$ ,

$P_1 = (4,-6)$ ,  $P_6 = (0,2)$ ,

$P_{12} = (2,0)$ ,  $P_4 = (-2,0)$.

Remarque.

Les courbes $X_{20}$, $X_{36}$ possèdent six pointes rationnelles sur $\mathbb{Q}$. Là encore, les groupes $X_{20}(\mathbb{Q})$, $X_{36}(\mathbb{Q})$ sont formés des pointes.

(iv) Liste des points rationnels.

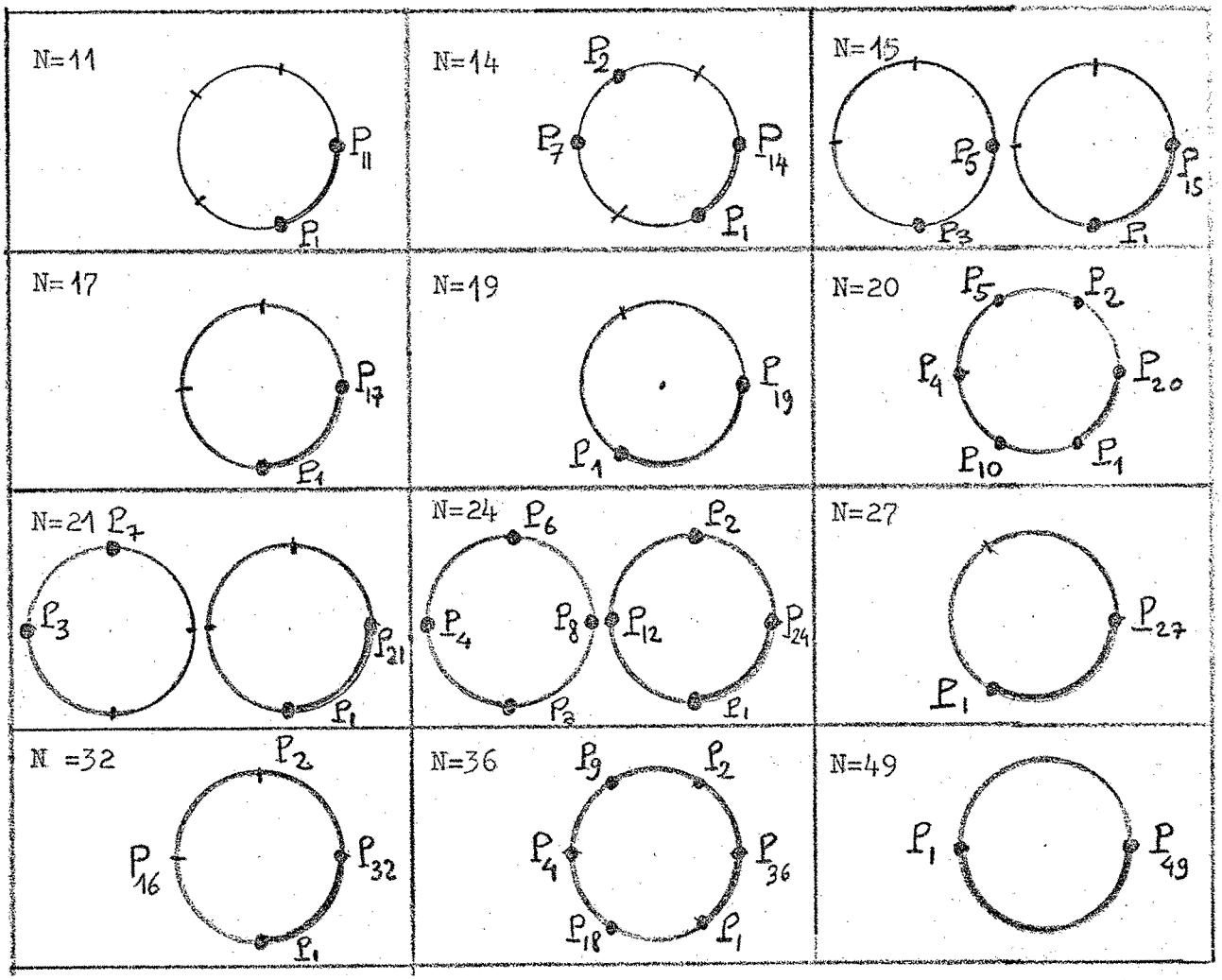
Le tableau suivant donne la liste des points rationnels des courbes modulaires elliptiques. Les coordonnées des points sont relatives à l'équation minimale donnée par le tableau (4.2.6). On omet de noter le point à l'infini. Lorsque $X_N(\mathbb{R})$ possède deux composantes connexes, ce qui a lieu pour $N = 15, 21, 24$, on a séparé par un point virgule les points situés sur deux composantes connexes distinctes.

(5.2.3.1). Coordonnées des points rationnels.

| | |
|---|---|
| $X_{11}$ | (5,5), (5,-6), (16,60), (16,-61). |
| $X_{14}$ | (1,-1), (2,2), (2,-5), (9,23), (9,-33). |
| $X_{15}$ | (-13/4,9/8), (-2,3), (-2,-2), (-1,0); (3,-2), (8,18), (8,-27). |
| $X_{17}$ | (11/4,-15/8), (7,13), (7,-21). |
| $X_{19}$ | (5,9), (5,-10). |
| $X_{20}$ | (-1,0), (0,±2), (4,±10). |
| $X_{21}$ | (-2,1), (-1,2), (-1,-1), (-1/4,1/8); (2,-1), (5,8), (5,-3). |
| $X_{24}$ | (-2,0), (0,±2), (1,0); (2,0), (4,±6). |
| $X_{27}$ | (3,4),(3,-5). |
| $X_{32}$ | (0,0), (2,±4). |
| $X_{36}$ | (-1,0), (0,±1), (2,±3). |
| $X_{49}$ | (2,-1). |

(5.2.4 ) Tableau: Structure de $X_N(\underset{\sim}{Q}) \subset X_N(\underset{\sim}{R})$.

Le tableau suivant représente le groupe de Lie réel $X_N(\underset{\sim}{R})$, les points marqués étant les points de $X_N(\underset{\sim}{Q})$, parmi lesquels figurent les pointes rationnelles . On utilise le plongement de $X_N(\underset{\sim}{R})$ dans $P_2(\underset{\sim}{R})$ défini par (5.2.2.2).




Soit $C_N \subset X_N(\underset{\sim}{Q})$ le sous-groupe engendré par la pointe $P_1$. D'après ce que l'on vient de voir, $C_N$ est d'indice 2 dans $X_N(\underset{\sim}{Q})$ pour $N = 15, 21, 24$, et $C_N = X_N(\underset{\sim}{Q})$ pour $N \in \mathfrak{M}_1 - \{15, 21, 24\}$. Dans les trois premiers cas, on peut trouver une pointe rationnelle sur $\underset{\sim}{Q}$, non contenue dans $C_N$. On a donc le résultat annoncé:

THÉORÈME 5.2.5. *Le groupe $X_N(\underset{\sim}{Q})$ des points de la courbe modulaire elliptique $X_N$ rationnels sur $\underset{\sim}{Q}$ est fini et engendré par les pointes de $X_N$ qui sont rationnelles sur $\underset{\sim}{Q}$.*

On désignera par $\eta_1(N)$ l'ordre du groupe $C_N$.

(5.2.6) Chemin fondamental.

Soit $t \in ]0,1]$, et posons $z(t) = -i.\mathrm{Log}(t)$. L'application ainsi définie se prolonge en une application continue de $[0,1]$ dans la sphère de Riemann, et dont l'image est contenue dans $\mathcal{H}^*$. Composant avec le l'application canonique

$$\mathcal{H}^* \longrightarrow \mathcal{H}^*/\Gamma_0(N) ,$$

on obtient un chemin $I_N$ dans la surface de Riemann $X_{N,\underset{\sim}{C}}$:

$$I_N : [0,1] \longrightarrow X_{N,\underset{\sim}{C}} .$$

Le chemin $I_N$ s'appelle le chemin fondamental de $X_{N,\underset{\sim}{C}}$.

Considérons l'application $\psi_N$ ( cf.(4.2.7) ), qui induit un plongement de $X_{N,\underset{\sim}{C}}$ dans $\underset{\sim}{P}_2(\underset{\sim}{C})$:

$$\psi_N : \mathcal{H}^* \longrightarrow X_N(\underset{\sim}{C}) \subset \underset{\sim}{P}_2(\underset{\sim}{C}) .$$

La restriction de $\psi_N$ au demi-axe imaginaire $\mathrm{Re}(z)=0$, $\mathrm{Im}(z)>0$, considérée comme fonction de la variable réelle $\mathrm{Im}(z)$, est injective, analytique, et à valeurs dans $X_N(\underset{\sim}{R})^0$. L'injectivité résulte de ce que le demi-axe imaginaire est contenu dans un domaine fondamental de $\Gamma_0(N)$, l'analyticité de celle des fonctions $\sigma(z)$ et $\tau(z)$ ( cf.(4.1)). Enfin, $\sigma(z)$ et $\tau(z)$, donc $x(z)$ et $y(z)$ sont à valeurs réelles pour $z$ imaginaire pur.

De la sorte, par composition avec $\psi_N$, la restriction à $]0,1[$ du chemin fondamental s'identifie à un chemin sans fin dans $X_N(\underset{\sim}{R})^0 \subset \underset{\sim}{R}^2$, soit $I'_N$ :

$$I'_N(t) = ( x(z(t)), y(z(t))) \in \underset{\sim}{R}^2 .$$

LEMME 5.2.6.1.

(i) a) Soit $N = 20, 24, 32, 36$ resp.. L'image de $I'_N$ est contenue dans l'ouvert

$$\left\{(x,y)\in \underset{\sim}{R}^2 \;\middle|\; \begin{matrix} x>4 \\ y>0 \end{matrix} \quad (\text{resp. } x>4,\ x>2,\ x>2)\right\}.$$

b) Soit $N = 27$. L'image de $I'_N$ est contenue dans l'ouvert

$$\left\{(x,y)\in \underset{\sim}{R}^2 \;\middle|\; y>4\right\}.$$

(ii) a) Soit $N = 11, 19$. L'image de $I'_N$ est contenue dans l'ouvert

$$\left\{(x,y)\in \underset{\sim}{R}^2 \;\middle|\; x<5\right\}.$$

b) Soit $N = 14, 15, 17, 21, 49$ resp.. L'image de $I'_N$ est contenue dans l'ouvert

$$\left\{(x,y)\in \underset{\sim}{R}^2 \;\middle|\; \begin{matrix} x>9 \\ y>0 \end{matrix} \quad (\text{resp. } x>8,\ x>7,\ x>5,\ x>2)\right\}.$$

Démonstration. (i) Comme on l'a rappelé en (4.1), les fonctions $\sigma(z)$ et $\tau(z)$ sont dans ce cas des fonctions analytiques de $Im(z)$ sur le demi-axe imaginaire, strictement décroissantes, tendant vers $+\infty$ lorsque $Im(z)$ tend vers $0^+$ ; $\tau(z)$ tend vers 0 lorsque $Im(z)$ tend vers $+\infty$, et $\sigma(z)$ tend vers une limite finie. Utilisant alors l'expression (4.2.5) de x,y en fonction de $\sigma$ et $\tau$, on obtient facilement le résultat du lemme.

(ii) Cette fois, $\sigma(z)$ est une fonction strictement croissante de $Im(z)$, qui s'annule pour $Im(z) = N^{-1/2}$, et qui tend vers $-\infty$, $+\infty$ resp. lorsque $Im(z)$ tend vers $0^+$, $+\infty$ resp. La fonction $\tau$ est décroissante pour $Im(z)\in ]0, N^{-1/2}[$, croissante pour $Im(z)> N^{-1/2}$, et tend vers $+\infty$ aux deux extrémités. Là encore, on utilise les équations (4.2.5) pour conclure.

De plus, dans tous les cas, la deuxième coordonnée $y(t)$ de $I'_N(t)$ est une fonction strictement croissante de $t\in ]0,1[$.

La comparaison des résultats du lemme (5.2.6) avec la liste des points rationnels de $X_N$ donnée par le tableau (5.2.3.1) montre immédiatement:

CONSÉQUENCE. <u>L'image de $I'_N$ dans $X_N(\underset{\sim}{R})$ ne contient aucun point de $X_N(\underset{\sim}{Q})$ ( et a fortiori aucun point de $C_N$ )</u>.

L'application $I'_N : ]0,+\infty[ \longrightarrow \underset{\sim}{R}^2$ étant de classe $C^\infty$ et injective permet d'orienter $X_N(\underset{\sim}{R})^0$ dans le sens des t croissants. D'autre part, la sphère $S^1$ est munie de son orientation canonique. Dans ces conditions, il existe un unique isomorphisme de groupes de Lie réels orientés, soit

$$\vartheta : X_N(\underset{\sim}{R})^0 \longrightarrow S^1 = \underset{\sim}{R}/\underset{\sim}{Z}.$$

Par composition avec $\vartheta$, le chemin sans fin $I'_N$, de classe $C^\infty$, donne un chemin sans fin $\vartheta \circ I'_N$, de classe $C^\infty$, injectif, et qui se prolonge en un chemin continu $\vartheta \circ I_N$, d'extrémités $I_N(0)$, $I_N(1)$ vérifiant:

$\vartheta \circ I_N(0) = \vartheta(P_N) = 0$ ( élément neutre de $S^1$),

$\vartheta \circ I_N(1)$ engendre le sous-groupe de $S^1$ noyau de la multiplication par $\eta_1$.

Enfin, l'image de $I'_N$ ne contient aucun point de ce noyau, à cause de la conséquence du lemme (5.2.6).

Le chemin $\vartheta \circ I_N$ se relève de façon unique en un chemin $\widetilde{\vartheta \circ I_N}$ dans le revêtement universel $\underset{\sim}{R}$ de $S^1$:

$$\widetilde{\vartheta \circ I_N} : [0,1] \longrightarrow \underset{\sim}{R}.$$

L'application $\widetilde{\vartheta \circ I_N}$ possède les propriétés suivantes:

(i) $\widetilde{\vartheta \circ I_N}$ est continue, injective, croissante;

(ii) $\widetilde{\vartheta \circ I_N}(0) = 0$ ;

$\widetilde{\vartheta \circ I_N}(1) \in \frac{1}{\eta_1} \underset{\sim}{Z}$ ;

(iii) la restriction de $\widetilde{\vartheta \circ I_N}$ à $]0,1[$ est de classe $C^\infty$, et son image ne contient aucun point de $\frac{1}{\eta_1} \underset{\sim}{Z}$.

Par conséquent, $\widetilde{\vartheta \circ I_N}$ est une bijection continue croissante de $[0,1]$ sur $[0, \frac{1}{\eta_1}]$, dont la restriction à $]0,1[$ est de classe $C^\infty$. En particulier:

PROPOSITION 5.2.6.2. Le chemin $\vartheta \circ I_N : [0,1] \longrightarrow \underset{\sim}{R/Z}$ est équivalent au chemin

$$t \longmapsto \frac{t}{\eta_1(N)} \quad .$$

L'image de $I_N$ est représentée en trait gras dans le tableau (5.2.4).

# 6. LA CONJECTURE DE BIRCH ET SWINNERTON-DYER.

## 6.1. Fonction $L^*$ normalisée.

Soit $X$ une courbe elliptique définie sur $\mathbb{Q}$. Rappelons ici la définition de la fonction $L^*$ de $X$ (cf. [35]).

(6.1.1) Désignons par $\omega$ une forme différentielle minimale de $X$ (cf.(4.2.3)).

A toute place $v$ de $\mathbb{Q}$ est associé le groupe de Lie $X(\mathbb{Q}_v)$, où $\mathbb{Q}_v$ désigne le complété de $\mathbb{Q}$ en $v$. On désigne par $\mu_v$ la mesure de Haar normalisée de $\mathbb{Q}_v$, c'est à dire la mesure de Lebesgue si $\mathbb{Q}_v = \mathbb{R}$, et la mesure de Haar telle que $\mu_v(\mathbb{Z}_p) = 1$ si $v = p$.

Dans ces conditions, au couple $(\omega, \mu_v)$ est canoniquement associée une mesure sur $X(\mathbb{Q}_v)$ (cf.[4],p.38, 10.1.4). On note $(\omega)_v$ cette mesure.

DÉFINITION 6.1.2. On appelle longueur de $X$ relative à $v$, et on note $M_v(X)$ le nombre

$$M_v(X) = \int_{X(\mathbb{Q}_v)} (\omega)_v .$$

(6.1.3) On désigne par $S$ un ensemble fini de places de $\mathbb{Q}$, contenant les places de mauvaise réduction de $X$ et la place à l'infini.

On associe à $S$ le produit eulérien:

$$(6.1.3.1) \qquad L_S^*(X,s) = \prod_{v \in S} (M_v(X))^{-1} \cdot \prod_{v \notin S} L_p(X,s),$$

où $L_p(X,s)$ est le facteur local en $p$ de la fonction $L$ de $X$ (cf.(2.2)).

On constate facilement [35] que, pour deux tels ensembles $S_1$, $S_2$,

le quotient $L^*_{S_1}(X,s)/L^*_{S_2}(X,s)$ est une fonction de s qui tend vers 1 lorsque s tend vers 1.

Par conséquent, si la fonction $L(X,s)$ est définie au point $s = 1$, la valeur $L^*_S(X,1)$ de $L^*_S(X,s)$ au point $s = 1$ ne dépend pas de S.

DÉFINITION 6.1.4. On appelle fonction $L^*$ de la courbe elliptique X, et on désigne par $L^*(X,s)$, tout produit eulérien ne différant de (6.1.3.1) que par un nombre fini de facteurs, et tel que $L^*(X,s)/L^*_S(X,s)$ tende vers 1 lorsque s tend vers 1.

PROPOSITION 6.1.5. Avec les notations de (4.3.1) et (6.1.2), on a:

$$M_p(X) = c_p(X)/L_p(X,1)$$

pour tout nombre premier p.

Ce résultat est démontré dans les notes de Tate [36].

COROLLAIRE. Le produit eulérien

$$(6.1.5.1) \qquad L^*(X,s) = \Big( M_\infty(X) \cdot \prod_{p \text{ premier}} c_p(X) \Big)^{-1} \cdot L(X,s)$$

est une fonction $L^*$ de la courbe X.

C'est cette fonction $L^*$ normalisée que nous utiliserons par la suite.

## 6.2. Énoncé de la conjecture.

Nous pouvons maintenant énoncer la conjecture de Birch et Swinnerton-Dyer (on se reportera à [34], [35], [38] pour plus de détails).

CONJECTURE 6.2.1. (Conjecture de Birch et Swinnerton-Dyer).

Soient X une courbe elliptique définie sur $\mathbb{Q}$, L(X,s) sa fonction L, et $L^*(X,s)$ une fonction $L^*$ de X.

(i) La fonction L(X,s) est non-nulle au point $s = 1$ si le rang r de X est nul, et admet un zéro d'ordre r en ce point si $r > 0$.

(ii) Supposons que $r = 0$, et soit $\eta_0$ l'ordre du groupe $X(\mathbb{Q})$. Alors:

$$L^*(X,1) = \frac{Sh}{\eta_0^2},$$

où Sh est l'ordre du groupe de Tate-Šafarevič (cf. [5], [38]).

Remarque. On a un énoncé analogue à (ii) dans le cas où le rang de X est non-nul. On se reportera à [35], [33], [38].

Exemples. La majorité des exemples numériques explicites à l'appui de la conjecture de Birch et Swinnerton-Dyer concernent des courbes elliptiques admettant une multiplication complexe (cf. [2], [3], [33]).

Le premier exemple de calcul explicite de $L^*(X,1)$ pour une courbe elliptique sans multiplication complexe est donné par Swinnerton-Dyer dans [35]: Il s'agit de la courbe modulaire elliptique de niveau 11.

6.3. Calcul de $L^*(N,1)$.

Nous sommes maintenant en mesure de calculer $L^*(X_N,1) = L^*(N,1)$ pour chacune des courbes modulaires elliptiques $X_N$, $N \in \mathcal{M}_1$.

(6.3.1) Soit $\omega = dx/(2y + \lambda x + \mu)$ la forme différentielle minimale de $X_N$ déja considérée en (4.2.7). On a vu (cf.(4.2.7.1)) que

$$\omega = f_\omega(z)\, dz ,$$

et que la fonction

$$f(z) = (2\pi i)^{-1} \cdot f_\omega(z)$$

a pour série de Dirichlet associée la fonction $L(N,s)$ de la courbe $X_N$ (cf. (2.2.3)).

La technique utilisée par Swinnerton-Dyer consiste à passer de $L$ à $f$ grâce à la formule de Mellin. En effet, d'après cette dernière:

$$L(N,1) = \int_0^{i\infty} -2\pi i\, f(z)\, dz ,$$

l'intégrale étant prise sur le demi-axe imaginaire, orienté comme en (5.2).

Utilisant $\varphi_N$ (cf.(5.2)), et le fait que ce dernier conserve les orientations:

$$L(N,1) = \int_{P_1}^{P_N} -\omega \ ;$$

l'intégrale figurant au second membre est celle d'une 1-forme différentielle calculée le long d'un chemin différentiable dans une variété de dimension orientée.

Utilisant maintenant l'isomorphisme $\vartheta$ de (5.2), le fait que $-\omega$ est une différentielle invariante sur le groupe de Lie $X_N(\mathbb{R})^0$ ( donc est transformée par $\vartheta$ en un multiple de $dt$ sur $S^1$ ), et la proposi-

tion (5.2.6.2)on obtient:

$$L(N,1) = \eta_1(N)^{-1} \cdot \int_{X_N(\mathbb{R})^0} (-\omega) ;$$

enfin, se reportant à (6.1), dans le cas particulier où v est la place à l'infini, et utilisant une coordonnée locale pour calculer l'intégrale de la forme différentielle $-\omega$ sur la variété orientée $X_N(\mathbb{R})^0$, on vérifie sans peine:

$$(\omega)_\infty = -\omega \qquad \text{( notations de (6.1)).}$$

D'où en définitive:

$$L(N,1) = \eta_1(N)^{-1} \cdot \left( \left( X_N(\mathbb{R}) : X_N(\mathbb{R})^0 \right) \right)^{-1} \cdot M_\infty (X_N).$$

D'après ( 5.2.4) , on a pour toutes les courbes modulaires elliptiques $X_N$:

$$\eta_1(N)\left( X_N(\mathbb{R}) : X_N(\mathbb{R})^0 \right) = \eta_0(X_N) ,$$

où $\eta_0(X_N)$ désigne l'ordre du groupe $X_N(\mathbb{Q})$ ( cf. (5.2.3.1)). Donc:

(6.3.1.1) $$L(N,1) = \eta_0^{-1} \cdot M_\infty (X_N).$$

(6.3.2) Notons $L^*(N,1)$ la valeur au point $s = 1$ d'une fonction $L^*$ de la courbe $X_N$. Utilisant la fonction $L^*$ normalisée (6.1.5.1), on obtient:

$$L^*(N,1) = \left( \prod_{p|N} c_p(X_N) \right)^{-1} \cdot \eta_0^{-1} .$$

On est donc ramené au calcul des entiers $c_p(X_N)$. Ce calcul a déja été fait ( cf. (4.3.5), et le tableau (6.3.4)). On trouve dans tous les cas considérés:

$$\prod_{p \text{ premier}} c_p(X_N) = \eta_o(X_N).$$

On a donc démontré:

THÉORÈME 6.3.3. *Soit* $L^*(N,s)$ *une fonction* $L^*$ *de la courbe modulaire elliptique* $X_N$, *et* $\eta_o(N)$ *l'ordre du groupe* $X_N(\mathbb{Q})$. *Alors*

$$L^*(N,1) = (\eta_o(N))^{-2}.$$

On constate que les courbes modulaires elliptiques vérifient la partie (i) de la conjecture de Birch et Swinnerton-Dyer (6.2.1). Si l'on admet la partie (ii) de cette dernière, le théorème précédent entraîne:

Le groupe de Tate-Šafarevič des courbes modulaires elliptiques est trivial.

Tableau (6.3.4) Courbes modulaires elliptiques $X_N$.

Notations. On a posé $N = p_1^{n_1} \cdot p_2^{n_2}$, $p_1 < p_2$, $n_1 > 0$. On note

$\Delta$ le discriminant d'une équation minimale de $X_N$ (cf. (4.2.1)),

$j$ l'invariant de la courbe elliptique $X_N$,

$\eta_0$ l'ordre du groupe $X_N(\mathbb{Q})$ (cf. (5.1)),

$c_p$ l'entier défini en (4.3.1) (cf.(4.3.5.1) pour le calcul de $c_p$),

$L^*(1) = L^*(N,1)$ la valeur en 1 de la fonction $L^*$ normalisée (cf.(6.3.2)).

| N | $\Delta$ | j | type de réd. en $p_1$ | type de réd. en $p_2$ | $c_{p_1}$ | $c_{p_2}$ | $\eta_0$ | $L^*(1)$ |
|---|---|---|---|---|---|---|---|---|
| 11 | $11^5$ | $-2^{12}31^3 11^{-5}$ | $(b_5)$ | — | 5 | — | 5 | 1/25 |
| 14 | $2^6 7^3$ | $5^3 43^3 2^{-6} 7^{-3}$ | $(b_6)$ | $(b_3)$ | 2 | 3 | 6 | 1/36 |
| 15 | $-3^4 5^4$ | $13^3 37^3 3^{-4} 5^{-4}$ | $(b_4)$ | $(b_4)$ | 2 | 4 | 8 | 1/64 |
| 17 | $17^4$ | $-3^3 11^3 7^{-4}$ | $(b_4)$ | — | 4 | — | 4 | 1/16 |
| 19 | $19^3$ | $-2^{18} 7^3 19^{-3}$ | $(b_3)$ | — | 3 | — | 3 | 1/9 |
| 20 | $2^8 5^2$ | $2^4 11^3 5^{-2}$ | (c 6) | $(b_2)$ | 3 | 2 | 6 | 1/36 |
| 21 | $-3^4 7^2$ | $193^3 3^{-4} 7^{-2}$ | $(b_4)$ | $(b_2)$ | 4 | 2 | 8 | 1/64 |
| 24 | $2^8 3^2$ | $2^4 13^3 3^{-2}$ | $(c\ 5_1)$ | $(b_2)$ | 4 | 2 | 8 | 1/64 |
| 27 | $3^9$ | 0 | (c 6) | — | 3 | — | 3 | 1/9 |
| 32 | $2^{12}$ | $2^6 3^3$ | $(c\ 5_3)$ | — | 4 | — | 4 | 1/16 |
| 36 | $2^4 3^3$ | 0 | (c 3) | (c 2) | 3 | 2 | 6 | 1/36 |
| 49 | $7^3$ | $-3^2 5^3$ | (c 2) | — | 2 | — | 2 | 1/4 |

# 7. APPLICATION A CERTAINES COURBES ISOGÈNES.

## 7.1. Fonction L normalisée et isogénies.

Soient $X$, $X'$ deux courbes elliptiques définies sur $\underset{\sim}{Q}$. On rappelle qu'une isogénie $X \longrightarrow X'$ définie sur $\underset{\sim}{Q}$ est dite admissible si elle induit un morphisme séparable des composantes connexes des fibres fermées du modèle de Néron (faible).

PROPOSITION 7.1.1. *Soient $X$, $X'$ deux courbes elliptiques définies sur $\underset{\sim}{Q}$, telles qu'il existe une isogénie admissible de $X$ sur $X'$. Alors $X$ et $X'$ ont même conducteur et même fonction L.*

On se reportera à [15], 6.11.

Désignons par $L^*(X,s)$, $L^*(X',s)$ les fonctions L normalisées (cf. (6.1.5.1)) de $X$ et $X'$.

COROLLAIRE. *Sous les hypothèses de* (7.1.1):

$$\frac{L^*(X,s)}{L^*(X',s)} = \frac{M_\infty(X') \cdot \prod c_p(X')}{M_\infty(X) \cdot \prod c_p(X)}$$

*où $M_\infty(X)$ est la longueur de $X$ relative à la place à l'infini* (6.1.2), *et $c_p(X)$ l'entier défini en* (4.3.1).

Il nous suffira donc, connaissant $L^*(X,1)$, de calculer $M_\infty(X')$ et $\prod c_p(X')$ pour en déduire $L^*(X',1)$.

7.2. Parasites.

Nous dirons qu'une équation de la forme (4.2.0), à coefficients dans $\underset{\sim}{Q}$, et définissant sur $\underset{\sim}{Q}$ une courbe elliptique X, contient le parasite $\rho$, $\rho > 0$ si son discriminant vaut $\rho^{12}.\Delta$, où $\Delta$ désigne le discriminant minimal (c'est à dire le discriminant d'une équation minimale) de la courbe X.

Etant donnée une équation (4.2.0) de X, contenant le parasite $\rho$, soit $\omega' = dx/(2y + \lambda x + \mu)$. Alors $\rho.\omega'$ est une forme différentielle minimale de la courbe X.

7.3. Paramétrisation de Weierstrass.

Supposons que la courbe elliptique X d'équation

(7.3.1) $$y^2 = x^3 + ax + b \quad ,$$

soit paramétrée par la fonction de Weierstrass $\wp(u)$, de périodes $\omega_1$, $\omega_2$, où l'on suppose $\omega_1$ réel positif:

$$\begin{cases} x = \wp(u) \\ y = (1/2).\wp'(u). \end{cases}$$

Supposons que l'image du segment $[0, \omega_1[$ soit la composante neutre $X(\underset{\sim}{R})^0$ du groupe de Lie réel $X(\underset{\sim}{R})$. Alors:

$$\int_{X(\underset{\sim}{R})} |dx/2y| = \left(X(\underset{\sim}{R}) : X(\underset{\sim}{R})^0\right).\int_0^{\omega_1} du = \left(X(\underset{\sim}{R}) : X(\underset{\sim}{R})^0\right).\omega_1 .$$

Supposons enfin que l'équation (7.3.1) contienne le parasite $\rho$. Alors la longueur de X relative à la place à l'infini (6.1.2) est donnée par:

$$M_\infty(X) = \rho.\left(X(\underset{\sim}{R}) : X(\underset{\sim}{R})^0\right).\omega_1 .$$

7.4. Isogénies de noyau cyclique .

On conserve les notations de (7.3). Soit P un point de $X_{tors}$ rationnel sur $\underset{\sim}{Q}$. Alors

(i) ou bien $P \in X(\underset{\sim}{R})^0$, et son paramètre est alors

$$u = \frac{k}{n}\omega_1 \quad , \quad \text{avec} \quad (k,n) = 1 \quad .$$

Désignant par X' le quotient de X par le sous-groupe cyclique d'ordre n engendré par P, et par $\rho'$ le parasite contenu dans l'équation (7.3.1) associée aux périodes $\frac{\omega_1}{n}$, $\omega_2$, on a:

$$M_\infty(X') = \rho' \cdot \left(X'(\underset{\sim}{R}) : X'(\underset{\sim}{R})^0\right) \cdot \frac{\omega_1}{n} \quad ,$$

(ii) ou bien $P \notin X(R)^0$. On a alors:

$$M_\infty(X') = \rho' \cdot \left(X'(\underset{\sim}{R}) : X'(\underset{\sim}{R})^0\right) \cdot \omega_1 \quad .$$

On se reportera à la note [39] pour les équations explicites des isogénies de noyau cyclique.

7.5. Application aux courbes de la liste de Swinnerton-Dyer de conducteur $N \in \mathcal{M}_1$ .

On utilise dans cette partie une liste de courbes elliptiques de petit conducteur établie par Swinnerton-Dyer. Pour N = 11, on a rajouté à la liste originale la courbe notée $C_{11}$, qui n'y figurait pas, et dont le calcul est dû à Vélu [39].

Pour chacune des valeurs de $N \in \mathcal{M}_1$, la liste contient un nombre fini de courbes elliptiques, toutes isogènes entre elles (conformément à ce que prédit la conjecture de Weil (2.6)). Pour chaque $N \in \mathcal{M}_1$, on désigne par $A_N$, $B_N$, etc. les courbes de la liste de conducteur N, exception faite pour la courbe modulaire elliptique $X_N$, que l'on continue de

noter de cette façon.

Remarque (7.5.1). La question se pose de savoir si la liste de Swinnerton-Dyer (complétée par $C_{11}$) comprend toutes les courbes de conducteur $N \in \mathcal{M}_1$.

On peut répondre affirmativement à cette question pour $N = 24, 32, 36$, où cela résulte des travaux de Ogg [25], [26]. Baker et Coates ont montré que la détermination de toutes les courbes de conducteur donné est possible en théorie, le seul obstacle étant la longueur des calculs que cela implique.

Si l'on admet que deux courbes de conducteur $N \in \mathcal{M}_1$ sont isogènes sur $\underset{\sim}{\mathbb{Q}}$, on est ramené à déterminer toutes les courbes isogènes sur $\underset{\sim}{\mathbb{Q}}$ à une courbe donnée, à savoir la courbe $X_N$. Ce dernier problème est plus facile, et on peut le résoudre dans certains cas, par exemple pour $N = 11$. En effet:

(i) Il résulte des travaux de Serre [28] que le groupe de Galois des points d'ordre $l$ de $A_{11}$ est $\underset{\sim}{GL}(2, \underset{\sim}{\mathbb{Z}}/l\underset{\sim}{\mathbb{Z}})$ pour tout nombre premier $l$ autre que 5. Cela entraîne que les seules isogénies de $A_{11}$ définies sur $\underset{\sim}{\mathbb{Q}}$ et de degré premier sont de degré 5.

(ii) La théorie de Tate montre que du point de vue rigide-analytique $A_{11}$ est isomorphe à $\underset{\sim}{\mathbb{Q}}_{11}^{\times}/(q^{\underset{\sim}{\mathbb{Z}}})$ avec $v_{11}(q) = 1$. Or il existe une isogénie de degré 5, à savoir celle qui donne la courbe $\underset{\sim}{\mathbb{Q}}_{11}^{\times}/(q^{5\underset{\sim}{\mathbb{Z}}}) = X_{11}$ qui augmente la valuation en 11. Toutes les autres ne peuvent que la diminuer: Il n'y en a donc pas. Le même raisonnement vaut pour $B_{11}$. Il en résulte que les seules courbes isogènes sur $\underset{\sim}{\mathbb{Q}}$ à $X_{11}$ sont $A_{11}$ et $B_{11}$.

(7.5.2) On a calculé pour chacune des courbes $X$ figurant dans la liste et de conducteur $N \in \mathcal{N}_1$ :

(i) La longueur $M_\infty(X)$ relative à la place à l'infini. Pour simplifier l'écriture, et tenant compte de ce que seul intervient le rapport de deux telles longueurs, on convient de prendre pour unité, pour chaque $N \in \mathcal{N}_1$, le nombre $\omega_1$ défini en (7.3) qui est tel que l'équation (7.3.1) correspondante contienne le parasite 1.

En d'autres termes, avec cette unité:

$$M_\infty(X_N) = \left( X_N(\underset{\sim}{R}) : X_N(\underset{\sim}{R})^\circ \right).$$

(ii) Les coefficients $c_p(X)$ définis en (4.3.1) (cf.(4.3.5) pour le calcul de $c_p$ ).

(iii) L'ordre $\eta_0(X)$ du groupe $X(\underset{\sim}{Q})$.

Pour ce dernier calcul, il est commode d'utiliser (7.3.1).

Remarque (7.5.3).

(i) Lorsque la fibre en p du modèle de Néron de X est de type multiplicatif non-déployé, elle ne devient isomorphe à une extension de $\underset{\sim}{G}_m$ par un groupe fini que sur $\underset{\sim}{F}_{p^2}$. On doit en tenir compte si l'on veut utiliser la proposition (5.2.1) dans ce cas: On peut examiner le cas de $X_{24}$, $p = 3$, pour s'en convaincre.

(ii) La proposition (5.2.1) est classique lorsqu'on suppose que X a bonne réduction en p. Elle donne alors une majoration de $\eta_0(X)$ invariante par isogénie sur $\underset{\sim}{Q}$ ( c'est la majoration obtenue en (5.2.2.1). Par contre, l'utilisation du modèle de Néron permet une majoration plus fine.

Exemple. Considérons dans la liste de Swinnerton-Dyer les courbes de conducteur 21 : $A_{21}$, $B_{21}$, etc.

Comme l'indique (5.2.2.1), toutes ces courbes ont un groupe de points rationnels d'ordre divisant 8.

D'autre part, la fibre en p = 3 est déployée sur $\underset{\sim}{F}_3$, de type

$(b_8)$, $(b_4)$, $(b_2)$, $(b_1)$, $(b_1)$ respectivement.

On en conclu que l'ordre de $X(\underset{\sim}{Q})$ divise

8, 8, 4, 4, 2, 2, respectivement.

(7.5.4) On pose dans le tableau (7.5.6):

$$\gamma_0(X) = M_\infty(X).\prod c_p(X)$$

(avec les conventions faites en (7.5.2)), ce qui fait que le corollaire de (7.1.1) s'écrit:

$$\frac{L^*(X,s)}{L^*(X',s)} = \frac{\gamma_0(X')}{\gamma_0(X)}.$$

On constate que pour toutes les courbes étudiées on a:

$$L^*(1) = \eta_0^{-2} .$$

Si l'on admet la conjecture de Birch et Swinnerton-Dyer, on peut donc conclure:

Le groupe de Tate-Šafarevič des courbes de la liste de Swinnerton-Dyer de conducteur $N \in \mathcal{M}_1$ est trivial.

(7.5.5) Tableau. (Extrait de la liste de Swinnerton-Dyer).

Ce tableau donne les coefficients $\lambda, \mu, \alpha, \beta, \gamma$ d'une équation minimale (4.2.0) de chacune des courbes $A_N$, $B_N$, etc., $N \in \mathcal{M}_1$. (cf. les notations du début de (7.5)).

| | $\lambda$ | $\mu$ | $\alpha$ | $\beta$ | $\gamma$ |
|---|---|---|---|---|---|
| $A_{11}$ | 0 | 1 | -1 | 0 | 0 |
| $X_{11}$ | 0 | 1 | -1 | -10 | -20 |
| $C_{11}$ | 0 | 1 | -1 | -7820 | -263580 |
| $X_{14}$ | 1 | 1 | 0 | 4 | -6 |
| $B_{14}$ | 1 | 1 | 0 | -36 | -70 |
| $C_{14}$ | 1 | 1 | 0 | -1 | 0 |
| $D_{14}$ | 1 | 1 | 0 | -171 | -874 |
| $E_{14}$ | 1 | 1 | 0 | -11 | 12 |
| $F_{14}$ | 1 | 1 | 0 | -2731 | -55146 |
| $A_{15}$ | 1 | 1 | 1 | -80 | 242 |
| $B_{15}$ | 1 | 1 | 1 | -5 | 2 |
| $C_{15}$ | 1 | 1 | 1 | 0 | 0 |
| $X_{15}$ | 1 | 1 | 1 | -10 | -10 |
| $E_{15}$ | 1 | 1 | 1 | -135 | -660 |
| $F_{15}$ | 1 | 1 | 1 | 35 | -28 |
| $G_{15}$ | 1 | 1 | 1 | -2160 | -39540 |
| $H_{15}$ | 1 | 1 | 1 | -110 | -880 |
| $A_{17}$ | 1 | 1 | -1 | -1 | 0 |
| $B_{17}$ | 1 | 1 | -1 | -6 | -4 |
| $C_{17}$ | 1 | 1 | -1 | -91 | -310 |
| $X_{17}$ | 1 | 1 | -1 | -1 | -14 |
| $A_{19}$ | 0 | 1 | 1 | 1 | 0 |
| $X_{19}$ | 0 | 1 | 1 | -9 | -15 |
| $C_{19}$ | 0 | 1 | 1 | -769 | -8470 |
| $A_{20}$ | 0 | 0 | 1 | -41 | -116 |
| $B_{20}$ | 0 | 0 | 1 | -36 | -140 |
| $C_{20}$ | 0 | 0 | 1 | -1 | 0 |
| $X_{20}$ | 0 | 0 | 1 | 4 | 4 |

| | $\lambda$ | $\mu$ | $\alpha$ | $\beta$ | $\gamma$ |
|---|---|---|---|---|---|
| $A_{21}$ | 1 | 0 | 0 | -39 | 90 |
| $X_{21}$ | 1 | 0 | 0 | -4 | -1 |
| $C_{21}$ | 1 | 0 | 0 | 1 | 0 |
| $D_{21}$ | 1 | 0 | 0 | -49 | -136 |
| $E_{21}$ | 1 | 0 | 0 | -784 | -8515 |
| $F_{21}$ | 1 | 0 | 0 | -34 | -217 |
| $A_{24}$ | 0 | 0 | -1 | -24 | -36 |
| $B_{24}$ | 0 | 0 | -1 | -384 | -2772 |
| $X_{24}$ | 0 | 0 | -1 | -4 | 4 |
| $D_{24}$ | 0 | 0 | -1 | 16 | -180 |
| $E_{24}$ | 0 | 0 | -1 | -64 | 220 |
| $F_{24}$ | 0 | 0 | -1 | 1 | 0 |
| $X_{27}$ | 0 | 1 | 0 | 0 | -7 |
| $B_{27}$ | 0 | 1 | 0 | 0 | 0 |
| $C_{27}$ | 0 | 1 | 0 | -270 | -1708 |
| $D_{27}$ | 0 | 1 | 0 | -30 | 63 |
| $X_{32}$ | 0 | 0 | 0 | 4 | 0 |
| $B_{32}$ | 0 | 0 | 0 | -1 | 0 |
| $C_{32}$ | 0 | 0 | 0 | -11 | -14 |
| $D_{32}$ | 0 | 0 | 0 | -11 | 14 |
| $X_{36}$ | 0 | 0 | 0 | 0 | 1 |
| $B_{36}$ | 0 | 0 | 0 | -15 | 22 |
| $C_{36}$ | 0 | 0 | 0 | 0 | -27 |
| $D_{36}$ | 0 | 0 | 0 | -135 | -594 |
| $X_{49}$ | 1 | 0 | -1 | -2 | 1 |
| $B_{49}$ | 1 | 0 | -1 | -37 | -78 |

(7.5.6) Tableau.

Les notations utilisées sont celles précisées en (7.5.2) et (7.5.4).
Pour $N \in \mathcal{M}_1$ on pose $N = p_1^{n_1} p_2^{n_2}$, avec $p_1 < p_2$ et $n_1 > 0$.

| | $M_\infty$ | $c_{p_1}$ | $c_{p_2}$ | type de réd. en $p_1$ | type de réd. en $p_2$ | $\gamma_0$ | $\eta_0$ | $L^*$ (1) |
|---|---|---|---|---|---|---|---|---|
| $A_{11}$ | 5 | 1 | | $(b_1)$ | | 5 | 5 | 1/25 |
| $X_{11}$ | 1 | 5 | — | $(b_5)$ | — | 5 | 5 | 1/25 |
| $C_{11}$ | 1/5 | 1 | | $(b_1)$ | | 1/5 | 1 | 1 |
| $X_{14}$ | 1 | 2 | 3 | $(b_6)$ | $(b_3)$ | 6 | 6 | 1/36 |
| $B_{14}$ | 1 | 1 | 6 | $(b_3)$ | $(b_6)$ | 6 | 6 | 1/36 |
| $C_{14}$ | 3 | 2 | 1 | $(b_2)$ | $(b_1)$ | 6 | 6 | 1/36 |
| $D_{14}$ | 1/3 | 2 | 1 | $(b_{18})$ | $(b_1)$ | 2/3 | 2 | 1/4 |
| $E_{14}$ | 3 | 1 | 2 | $(b_1)$ | $(b_2)$ | 6 | 6 | 1/36 |
| $F_{14}$ | 1/3 | 1 | 2 | $(b_9)$ | $(b_2)$ | 2/3 | 2 | 1/4 |
| $A_{15}$ | 4 | 1 | 1 | $(b_1)$ | $(b_1)$ | 4 | 4 | 1/16 |
| $B_{15}$ | 4 | 2 | 2 | $(b_2)$ | $(b_2)$ | 16 | 8 | 1/64 |
| $C_{15}$ | 4 | 1 | 1 | $(b_1)$ | $(b_1)$ | 4 | 4 | 1/16 |
| $X_{15}$ | 2 | 2 | 4 | $(b_4)$ | $(b_4)$ | 16 | 8 | 1/64 |
| $E_{15}$ | 1 | 2 | 2 | $(b_8)$ | $(b_2)$ | 4 | 4 | 1/16 |
| $F_{15}$ | 1 | 2 | 8 | $(b_2)$ | $(b_8)$ | 16 | 8 | 1/64 |
| $G_{15}$ | 1/2 | 2 | 1 | $(b_4)$ | $(b_1)$ | 1 | 2 | 1/4 |
| $H_{15}$ | 1/2 | 2 | 1 | $(b_{16})$ | $(b_1)$ | 1 | 2 | 1/4 |
| $A_{17}$ | 4 | 1 | | $(b_1)$ | | 4 | 4 | 1/16 |
| $B_{17}$ | 2 | 2 | — | $(b_2)$ | — | 4 | 4 | 1/16 |
| $C_{17}$ | 1 | 1 | | $(b_1)$ | | 1 | 2 | 1/4 |
| $X_{17}$ | 1 | 4 | | $(b_4)$ | | 4 | 4 | 1/16 |
| $A_{19}$ | 6 | 1 | | $(b_1)$ | | 6 | 3 | 1/9 |
| $X_{19}$ | 2 | 3 | — | $(b_3)$ | — | 6 | 3 | 1/9 |
| $C_{19}$ | 2/3 | 1 | | $(b_1)$ | | 2/3 | 1 | 1 |
| $A_{20}$ | 2/3 | 1 | 1 | (c 3) | $(b_3)$ | 2/3 | 2 | 1/4 |
| $B_{20}$ | 1/3 | 1 | 2 | (c 6) | $(b_6)$ | 2/3 | 2 | 1/4 |
| $C_{20}$ | 2 | 3 | 1 | (c 3) | $(b_1)$ | 6 | 6 | 1/36 |
| $X_{20}$ | 1 | 3 | 2 | (c 6) | $(b_2)$ | 6 | 6 | 1/36 |

(7.5.6) (suite).

| | $M_\infty$ | $c_{p_1}$ | $c_{p_2}$ | type de réd. en $p_1$ | type de réd. en $p_2$ | $\gamma_0$ | $\eta_0$ | $L^*$ (1) |
|---|---|---|---|---|---|---|---|---|
| $A_{21}$ | 2 | 8 | 1 | $(b_8)$ | $(b_1)$ | 16 | 8 | 1/64 |
| $X_{21}$ | 2 | 4 | 2 | $(b_4)$ | $(b_2)$ | 16 | 8 | 1/64 |
| $C_{21}$ | 2 | 2 | 1 | $(b_2)$ | $(b_1)$ | 4 | 4 | 1/16 |
| $D_{21}$ | 1 | 2 | 2 | $(b_2)$ | $(b_4)$ | 4 | 4 | 1/16 |
| $E_{21}$ | 1/2 | 1 | 2 | $(b_1)$ | $(b_2)$ | 1 | 2 | 1/4 |
| $F_{21}$ | 1/2 | 1 | 2 | $(b_1)$ | $(b_8)$ | 1 | 2 | 1/4 |
| $A_{24}$ | 1 | 2 | 2 | (c 7) | $(b_4)$ | 4 | 4 | 1/16 |
| $B_{24}$ | 1/2 | 1 | 2 | (c 8) | $(b_2)$ | 1 | 2 | 1/4 |
| $X_{24}$ | 2 | 4 | 2 | (c $5_1$) | $(b_2)$ | 16 | 8 | 1/64 |
| $D_{24}$ | 1/2 | 1 | 2 | (c 8) | $(b_8)$ | 1 | 2 | 1/4 |
| $E_{24}$ | 2 | 2 | 1 | (c 7) | $(b_1)$ | 4 | 4 | 1/16 |
| $F_{24}$ | 2 | 2 | 1 | (c 2) | $(b_1)$ | 4 | 4 | 1/16 |
| $X_{27}$ | 1 | 3 | | (c 6) | | 3 | 3 | 1/9 |
| $B_{27}$ | 3 | 1 | | (c 1) | | 3 | 3 | 1/9 |
| $C_{27}$ | 1/3 | 1 | — | (c 8) | — | 1/3 | 1 | 1 |
| $D_{27}$ | 3 | 1 | | (c 3) | | 3 | 3 | 1/9 |
| $X_{32}$ | 1 | 4 | | (c $5_1$) | | 4 | 4 | 1/16 |
| $B_{32}$ | 2 | 2 | | (c 2) | | 4 | 4 | 1/16 |
| $C_{32}$ | 1 | 1 | — | (c 4) | — | 1 | 2 | 1/4 |
| $D_{32}$ | 2 | 2 | | (c 4) | | 4 | 4 | 1/16 |
| $X_{36}$ | 1 | 3 | 2 | (c 3) | (c 2) | 6 | 6 | 1/36 |
| $B_{36}$ | 1 | 3 | 2 | (c 6) | (c 2) | 6 | 6 | 1/36 |
| $C_{36}$ | 1/3 | 1 | 2 | (c 3) | (c 7) | 2/3 | 2 | 1/4 |
| $D_{36}$ | 1/3 | 1 | 2 | (c 6) | (c 7) | 2/3 | 2 | 1/4 |
| $X_{49}$ | 1 | 2 | | (c 2) | | 2 | 2 | 1/4 |
| $B_{49}$ | 1 | 2 | — | (c 2) | — | 2 | 2 | 1/4 |

BIBLIOGRAPHIE

[1] A. ATKIN et J. LEHNER - Hecke operators on $\Gamma_0(m)$, Math. Ann., 185, 1970, p. 134-160.

[2] B.J. BIRCH et H.P.F. SWINNERTON-DYER - Notes on elliptic curves. I, Journ. reine u. angewandte Math., 212, 1963, p. 7-25.

[3] B.J. BIRCH et H.P.F. SWINNERTON-DYER - Notes on elliptic curves. II, Journ. reine u. angewandte Math., 218, 1965, p. 79-108.

[4] N. BOURBAKI - Variétés différentielles et analytiques, fascicule de résultats, § 10, Hermann, Paris 1971.

[5] J. CASSELS - Diophantine equations with special reference to elliptic curves, J. London Math. Soc., 41, 1966, p. 193-291.

[6] P. DELIGNE et M. RAPOPORT - Les schémas de modules de courbes elliptiques, Modular Functions of One Variable II , Lecture Notes in Math. 349, p. 143-316, Berlin-Heidelberg-New York, Springer 1973.

[7] K. DOI - On the jacobian varieties of the fields of elliptic modular functions, Osaka Math. J., 15, 1963, p. 249-256.

[8] M. EICHLER - Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion, Arch. Math., 5, 1954, p. 355-366.

[9] R. FRICKE - Die elliptischen Funktionen und ihre Anwendungen, II, Teubner, Leipzig-Berlin 1922.

[10] A. GROTHENDIECK - Modèles de Néron et monodromie, Groupes de monodromie en Géométrie Algébrique ( SGA 7 I), Exposé IX, Lecture Notes in Math. 288, p. 313-523, Berlin-Heidelberg-New York, Springer 1972.

[11] E. HECKE - Mathematische Werke, Göttingen, Vandenhoeck und Ruprecht 1959.

[12] J. IGUSA - Fibre systems of Jacobian varieties, III, Amer. J. of Math., 81, 1959, p.453-476.

[13] J. IGUSA - Kroneckerian model of fields of elliptic modular functions Amer. J. of Math., 81, 1959, p. 561-577.

[14] Y. MANIN - Corps cyclotomiques et courbes modulaires (en russe), Uspekhi Mat. Nauk. Tom XXVI 6 (162), 1971, p. 7-71 [trad. anglaise: Russian Math. Surveys, vol. 26, nº 6, 1971, p. 7-78].

[15] Y. MANIN - Points paraboliques et fonctions zêta des courbes modulaires (en russe), Izv. Akad. N. C.C.C.P., 36, 1972, p.19-66 [trad. anglaise: Math. USSR-Izvestja, 6, 1972, p. 19-64].

[16] T. MATSUI - On the endomorphism algebra of jacobian varieties attached to the fields of elliptic modular functions, Osaka J. Math., 1, 1964, p. 25-31.

[17] B. MAZUR - Rational Points of Abelian Varieties with Values in Towers of Number Fields, Invent. Math., 18, 1972, p. 183-266.

[18] B. MAZUR - Courbes elliptiques et symboles modulaires, Sém. Bourbaki, 24e année, 1971/72, exposé nº 414, Lecture Notes in Math. 317, Berlin-Heidelberg-New York, Springer 1973.

[19] B. MAZUR et J. VÉLU - Courbes de Weil de conducteur 26, C. R. Acad. Sci. Paris, 275, 1972, p. 743-745.

[20] A. NÉRON - Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, Publ. Math. I.H.E.S., 21, 1964.

[21] A. NÉRON - Modèles minimaux et différentielles, C.I.M.E., 1969.

[22] M. NEWMAN - Construction and application of a class of modular functions, Proc. London Math. Soc., (3) 7 , 1957, p. 334-350; Construction and application of a class of modular functions II, ibid., (3) 9 , 1959, p. 373-387.

[23] A. OGG - Elliptic curves and wild ramification, Amer. J. of Math., 89, 1967, p. 1-21.

[24] A. OGG - Survey of Modular Functions of One Variable, Modular Functions of One Variable I, Lecture Notes in Math. 320, p. 1-35, Berlin-Heidelberg-New York, Springer 1973.

[25] A. OGG - Abelian curves of 2-power conductor, Proc. Camb. Phil. Soc., 62, 1966, p. 143-148.

[26] A. OGG - Abelian curves of small conductor, Journ. reine u. angewandte Math., 226, 1968, p. 204-215.

[27] A. OGG - Dirichlet series and modular functions, Benjamin 1968.

[28] J.-P. SERRE - Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math., 15, 1972, p. 259-331.

[29] J.-P. SERRE - Facteurs locaux des fonctions zêta des variétés algébriques ( définitions et conjectures), Sém. Delange-Pisot-Poitou, 1969/70, nº 19.

[30] J.-P. SERRE et J. TATE - Good reduction of abelian varieties, Ann. of Math., 88, 1968, p. 492-517.

[31] G. SHIMURA - Correspondances modulaires et les fonctions $\zeta$ de courbes algébriques, J. Math. Soc. Japan, 10, nº 1, 1958, p. 1-28.

[32] G. SHIMURA - Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan, nº 11, Tokyo-Princeton, 1971.

[33] N. M. STEPHENS - The diophantine equation $X^3+Y^3=DZ^3$ and the conjectures of Birch and Swinnerton-Dyer, Journ. reine u. angewandte Math., 231, 1968, p. 121-162.

[34] P. SWINNERTON-DYER - An Application of Computing to Class Field Theory, dans: J. CASSELS et A. FRÖHLICH (ed.): Algebraic Number Theory, p. 280-291, London-New York, Academic Press 1967.

[35] P. SWINNERTON-DYER - The Conjectures of Birch and Swinnerton-Dyer, and of Tate, Proceedings of a Conference on Local Fields, NUFFIC Summer School held at Driebergen, p. 132-157, 1966, Berlin-Heidelberg New York, Springer 1967.

[36] J. TATE - Algorithm for determining the type of a singular fibre in an elliptic pencil (notes diffusées par l' I.H.E.S.).

[37] J. TATE - Rational points on elliptic curves, course given at Haverford (May, April 1961), re-edited, 1970, without the author's permission by "Faculté des Sciences de Poitiers".

[38] J. TATE - On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, Sém. Bourbaki, exposé n° 306, 1965/66, New York-Amsterdam, Benjamin 1966.

[39] J. VÉLU - Courbes elliptiques sur $\mathbb{Q}$ ayant bonne réduction en dehors de $\{11\}$, C. R. Acad. Sci. Paris, 273, 1971, p. 73-75; Isogénies entre courbes elliptiques, ibid., 273, 1971, p. 238-241.

[40] A. WEIL - Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, Math. Ann., 168, 1967, p. 149-156.

[41] G. SANSONE et J. CASSELS - Sur le problème de M. Werner Mnich, Acta Arithmetica, 7, 1961/62, p. 187-190.