SÉMINAIRE N. BOURBAKI

BARRY MAZUR
JEAN-PIERRE SERRE

Points rationnels des courbes modulaires $X_0(N)$

Séminaire N. Bourbaki, 1976, exp. n° 469, p. 238-255
<http://www.numdam.org/item?id=SB_1974-1975__17__238_0>

© Association des collaborateurs de Nicolas Bourbaki, 1976, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (http://www.bourbaki.ens.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI 469-01
27e année, 1974/75, n° 469 Juin 1975

POINTS RATIONNELS DES COURBES MODULAIRES $X_0(N)$

[d'après [7] , [9]]

par Barry MAZUR et Jean-Pierre SERRE

§ 1. Rappels sur les courbes $X_0(N)$

On se borne à de brèves indications. Pour plus de détails voir [1], [13], [14].

1.1 Définitions

Soient N un entier ≥ 1 , et $\Gamma_0(N)$ le sous-groupe de $SL_2(\mathbf{Z})$ formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que $c \equiv 0 \pmod{N}$. Soit $H = \{z \mid \mathrm{Im}(z) > 0\}$ le demi-plan de Poincaré. Le quotient $H/\Gamma_0(N)$ est une courbe algébrique affine $Y_0(N)_{/\mathbf{C}}$ sur $\mathbf{C}$; on la compactifie en lui adjoignant l'ensemble de ses "pointes", i.e. le quotient $P_1(\mathbf{Q})/\Gamma_0(N)$; la courbe projective ainsi obtenue est notée $X_0(N)_{/\mathbf{C}}$. Son corps de fonctions est $\mathbf{C}(j, j_N)$, où $j = j(z)$ est l'invariant modulaire usuel, et $j_N(z) = j(Nz)$. Les courbes $Y_0(N)_{/\mathbf{C}}$ et $X_0(N)_{/\mathbf{C}}$ se déduisent par extension des scalaires de courbes algébriques sur $\mathbf{Q}$, notées $Y_0(N)$ et $X_0(N)$, caractérisées par le fait que leur corps de fonctions est $\mathbf{Q}(j, j_N)$; on trouvera dans [1], p. 221-227, une définition plus naturelle (sinon plus simple) de $Y_0(N)$ et $X_0(N)$, qui a notamment l'avantage de s'appliquer en toute caractéristique ne divisant pas N .

On renvoie à Hecke [3], p. 810 (resp. Ogg [9a]) pour la détermination des pointes (resp. de leur corps de rationalité), et du genre de $X_0(N)$. Bornons-nous à signaler que :

a) si N est premier, il n'y a que deux pointes, 0 et ∞ ; elles sont rationnelles sur $\mathbf{Q}$;

b) l'application $f \longmapsto f\,dq/q$ (où $q = e^{2\pi iz}$) définit une bijection entre

formes modulaires paraboliques de poids 2 sur $\Gamma_0(N)$

et

formes différentielles de première espèce sur $X_0(N)_{/\mathbb{C}}$.

L'importance de $X_0(N)$ et $Y_0(N)$ provient de ce que $Y_0(N)$ classifie les couples (E,A) , où E est une courbe elliptique et A un sous-groupe cyclique d'ordre N de E . De façon plus précise (cf. [1], p. 274), si (E,A) est défini sur un corps k , il lui correspond un point $j(E,A)$ de $Y_0(N)(k)$, et tout point de $Y_0(N)(k)$ est obtenu ainsi ; on a $j(E,A) = j(E',A')$ si et seulement si (E,A) et (E',A') deviennent isomorphes sur une extension de k .

1.2 L'involution w

C'est un automorphisme de $X_0(N)$ de carré 1 , caractérisé par le fait qu'il échange j et j_N ; il laisse stable les pointes (en particulier, il échange 0 et ∞), et opère donc sur $Y_0(N)$. Son action sur $X_0(N)_{/\mathbb{C}}$ s'obtient par passage au quotient à partir de $z \mapsto -1/Nz$.

Du point de vue modulaire, w transforme (E,A) en $(E/A\,,\, E_N/A)$, où E_N désigne le noyau de la multiplication par N dans E .

Remarque.- Plus généralement, toute décomposition $N = N_1N_2$ de N en facteurs N_1 , N_2 premiers entre eux définit une involution $w(N_1,N_2)$ de $X_0(N)$, caractérisée par :

$$(E,A) \mapsto (E/A_1\,,\,(A + E_{N_1})/A_1) ,$$

où A_1 désigne l'unique sous-groupe d'ordre N_1 de A .

1.3 Les opérateurs de Hecke T_ℓ

Soit ℓ un nombre premier ne divisant pas N . L'opérateur de Hecke T_ℓ est une correspondance sur $X_0(N)$ de degré $\ell+1$: le transformé $T_\ell(x)$ d'un point x est une somme de $\ell+1$ points. Du point de vue modulaire, T_ℓ est défini par

$$(E,A) \mapsto \sum_B (E/B\,,\,(A+B)/B) ,$$

où B parcourt l'ensemble des $\ell+1$ sous-groupes d'ordre ℓ de E .

Les T_ℓ commutent entre eux et à w ; ils laissent stables les pointes ; ils multiplient par $\ell+1$ les pointes 0 et ∞ . Leur action sur les différen-

tielles de première espèce (identifiées aux formes paraboliques de poids 2) est :

$$\Sigma a_n q^n \longmapsto \Sigma a_{\ell n} q^n + \ell \Sigma a_n q^{\ell n} .$$

§ 2. Idéal d'Eisenstein et théorèmes de finitude

2.1 Hypothèses et notations

Dans tout ce qui suit, on suppose que N est **premier**, et que le genre g de la courbe $X_0(N)$ est ≥ 1 , autrement dit que $N \neq 2, 3, 5, 7, 13$ (lorsque $g = 0$, la courbe $X_0(N)$ est isomorphe à la droite projective, et a donc une infinité de points rationnels).

On note J la jacobienne de $X_0(N)$; on plonge $X_0(N)$ dans J par l'application $x \longmapsto \mathrm{cl}((x) - (\infty))$.

Les correspondances T_ℓ (ℓ premier $\neq N$) et w du § 1 définissent des endomorphismes de J , que nous noterons encore T_ℓ et w ; on a $w^2 = 1$.

Remarque.- Toutes ces constructions se font "sur $\mathbb{Q}$ " ; en particulier J est définie sur $\mathbb{Q}$ et les T_ℓ , ainsi que w , opèrent sur le groupe $J(\mathbb{Q})$ des points rationnels de J .

2.2 Le groupe C

Soit $c = \mathrm{cl}((0) - (\infty))$ l'image dans J de la pointe 0 de $X_0(N)$; on a $c \in J(\mathbb{Q})$; notons C le sous-groupe de $J(\mathbb{Q})$ engendré par c .

THÉORÈME 1 (Ogg [9a]).- Le groupe C est un groupe cyclique fini d'ordre égal au numérateur n de $\frac{N-1}{12}$.

Soit h le pgcd de $N-1$ et de 12 ; on a $n = (N-1)/h$. Considérons la fonction f sur le demi-plan de Poincaré définie par

$$f(z) = \left(\frac{\Delta(Nz)}{\Delta(z)} \right)^{1/h} = q^n \prod_{m=1}^{\infty} (1 - q^{mN})^{24/h} (1 - q^m)^{-24/h} ,$$

où $q = e^{2\pi i z}$. On peut montrer que f est invariante par le groupe $\Gamma_0(N)$; elle s'identifie donc à une fonction rationnelle sur $X_0(N)$. Son diviseur est $n((\infty) - (0))$, ce qui prouve que $nc = 0$ dans $J(\mathbb{Q})$. Il reste à montrer que, si n' divise strictement n , on a $n'c \neq 0$; Ogg le fait en prouvant que

$f^{n'/n}$ n'est pas invariante par $\Gamma_0(N)$; cela peut aussi se déduire du th. 4 du n° 3.1 ci-après.

Remarques.- 1) On a $n > 1$ puisque $N-1$ n'est pas un diviseur de 12 ; d'ailleurs il est clair que $c \neq 0$ puisque $x \mapsto cl((x)-(\infty))$ est un plongement de $X_0(N)$ dans J.

2) On verra plus loin (n° 3.2, th. 5) que C est le sous-groupe de torsion de $J(\mathbb{Q})$.

3) Il est facile de voir que $T_\ell c = (1+\ell)c$ et $wc = -c$; en particulier, C est stable par les T_ℓ et w.

2.3 Algèbre de Hecke

C'est le sous-anneau $\underline{T}$ de $\mathrm{End}(J)$ engendré par les T_ℓ (ℓ premier $\nmid N$) et w ; il est commutatif, et libre de rang g sur $\mathbb{Z}$. La $\mathbb{Q}$-algèbre $\mathbb{Q} \otimes \underline{T}$ est un produit de corps de nombres algébriques totalement réels K_α ; les noyaux $\mathfrak{p}_\alpha$ des homomorphismes $\underline{T} \to K_\alpha$ sont les idéaux premiers minimaux de $\underline{T}$. La décomposition $\mathbb{Q} \otimes \underline{T} = \prod_\alpha K_\alpha$ correspond à une décomposition de J (à isogénie près)

$$J \sim \prod_\alpha J_\alpha \qquad \text{avec} \quad \dim(J_\alpha) = g_\alpha = [K_\alpha : \mathbb{Q}] ,$$

les J_α étant des variétés abéliennes absolument simples, deux à deux non isomorphes, telles que

$$\mathbb{Q} \otimes \mathrm{End}(J_\alpha) = \mathbb{Q} \otimes \mathrm{End}_{\mathbb{C}}(J_\alpha) = K_\alpha , \qquad \text{cf. [12].}$$

Exemples

$N = 11, 17, 19$: $g = 1$, $\mathbb{Q} \otimes \underline{T} = \mathbb{Q}$, $\underline{T} = \mathbb{Z}$, $w = -1$;

$N = 23, 31$: $g = 2$, $\mathbb{Q} \otimes \underline{T} = \mathbb{Q}(\sqrt{5})$, $\underline{T} = \mathbb{Z}[(1+\sqrt{5})/2]$, $w = -1$;

$N = 37$: $g = 2$, $\mathbb{Q} \otimes \underline{T} = \mathbb{Q} \times \mathbb{Q}$, $\underline{T}$ est le sous-anneau de $\mathbb{Z} \times \mathbb{Z}$ formé des (a,b) tels que $a \equiv b \pmod 2$, $w = (1,-1)$.

2.4 Idéal d'Eisenstein

C'est l'idéal I de $\underline{T}$ engendré par $1+w$ et par les $1+\ell-T_\ell$, avec ℓ premier $\nmid N$. Le quotient $\underline{T}/I$ est cyclique fini.

Avec les notations de 2.2, on a $I.C = 0$. Comme C est cyclique d'ordre

$n = \mathrm{Num}\left(\frac{N-1}{12}\right)$, on en déduit une surjection $\underline{T}/I \to \mathbb{Z}/n\mathbb{Z}$. En particulier, on a $I \neq \underline{T}$.

Soit maintenant p un nombre premier. Faisons l'hypothèse

(i) p *divise* n .

Il résulte de ce qui précède que :

(ii) *L'idéal* $P = I + p\underline{T}$ *est un idéal maximal de* $\underline{T}$ *contenant* I , *et* $\underline{T}/P = \mathbb{Z}/p\mathbb{Z}$.

(En effet, P annule le sous-groupe d'ordre p de C , donc est distinct de $\underline{T}$, et il est clair que $\underline{T}/P = \mathbb{Z}/p\mathbb{Z}$.)

(iii) *Le groupe* $J(\mathbb{Q})$ *contient un élément d'ordre* p .

Si $\bar{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$, notons $J(\bar{\mathbb{Q}})[p]$ le noyau de la multiplication par p dans $J(\bar{\mathbb{Q}})$; c'est un module sur la $\mathbb{F}_p$-algèbre du groupe $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, et (iii) entraîne évidemment :

(iv) *Le module galoisien* $J(\bar{\mathbb{Q}})[p]$ *possède un quotient de Jordan-Hölder isomorphe à* $\mathbb{Z}/p\mathbb{Z}$ (ainsi qu'un quotient isomorphe au groupe μ_p des racines p-ièmes de l'unité, cela en résulte par dualité).

De plus :

(v) Il existe une *forme modulaire parabolique* f *de poids* 2 (mod.p) *sur* $\Gamma_0(N)$ (cf. Katz [4]) *dont le développement à l'infini est*

$$f = \sum_{m=1}^{\infty} \sigma_1'(m)\, q^m \qquad \text{avec} \quad \sigma_1'(m) = \sum_{\substack{d \mid m \\ (d,N)=1}} d \ .$$

En effet, si $p \neq 2$ (ou si $p = 2$ et $N \equiv 1$ (mod.16)) , on peut prendre pour f la réduction (mod. p) $\tilde{G}_2(N)$ de la série d'Eisenstein

$$G_2(N) = \frac{N-1}{24} + \sum_{m=1}^{\infty} \sigma_1'(m)\, q^m \ , \qquad \text{cf. [3], p. 817.}$$

Si $p = 2$ et $N \not\equiv 1$ (mod. 16) , on prend $f = \tilde{G}_2(N) + 1$, ce qui est loisible car la constante 1 est une forme modulaire (mod. 2) de n'importe quel poids ≥ 0 .

En fait :

PROPOSITION 1 ([7]).- Les propriétés (i), (ii), (iii), (iv) et (v) sont équivalentes.

L'équivalence de (i) et (v) se déduit des propriétés des formes modulaires (mod.p), cf. [7] ainsi que Koike [5] (noter que, pour $p = N$, (v) doit être convenablement interprété ...).

Supposons (ii) satisfaite. Un argument élémentaire d'algèbre commutative montre qu'il existe un sous-module galoisien simple W de $J(\bar{\mathbb{Q}})[p]$ qui est annulé par I. Utilisant la relation d'Eichler-Shimura, on constate que, pour presque tout ℓ, les valeurs propres de Frob_ℓ dans W sont congrues à 1 ou ℓ modulo p ; on en déduit facilement que W est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ ou μ_p ; d'où (ii) $\Rightarrow$ (iv). Un argument analogue montre l'existence d'une forme parabolique $F = \Sigma\, a_n q^n$ de poids 2 sur $\Gamma_0(N)$, à coefficients p-entiers, telle que $F \not\equiv 0 \pmod{p}$ et $I.F \equiv 0 \pmod{p}$; il en résulte que $a_1 \not\equiv 0 \pmod{p}$, et, si l'on normalise F en prenant $a_1 = 1$, la réduction $f = \tilde{F}$ de $F \pmod{p}$ satisfait à (v) ; d'où (ii) $\Rightarrow$ (v).

Pour les démonstrations des autres implications, on se borne à renvoyer à [7] ([1]).

COROLLAIRE.- Les idéaux maximaux de $\underline{T}$ contenant I sont les idéaux $P = I + p\underline{T}$, où p parcourt l'ensemble des facteurs premiers de n.

Cela résulte de l'équivalence (i) $\Leftrightarrow$ (ii).

2.5 Quotient d'Eisenstein et théorèmes de finitude

Soit $\underline{T}_I$ le complété de $\underline{T}$ pour la topologie I-adique ; c'est un anneau semi-local dont les composantes correspondent aux idéaux maximaux P de $\underline{T}$ contenant I. Le noyau $\mathfrak{a}$ de l'homomorphisme $\underline{T} \to \underline{T}_I$ est l'intersection des idéaux premiers minimaux $\mathfrak{p}_\alpha$ tels que $\mathfrak{p}_\alpha + I \neq \underline{T}$, i.e. tels qu'il existe un idéal maximal P contenant à la fois $\mathfrak{p}_\alpha$ et I. Comme $I \neq \underline{T}$, il existe au moins un tel $\mathfrak{p}_\alpha$, et l'on a $\mathfrak{a} \neq \underline{T}$.

Soit $\mathfrak{a}J$ la sous-variété abélienne de J engendrée par les images des endomorphismes appartenant à $\mathfrak{a}$. La variété abélienne quotient $\tilde{J} = J/\mathfrak{a}J$ est appelée (par Mazur) le quotient d'Eisenstein de J ; avec les notations de 2.3,

([1]) Le cas $p = 2$ présente des difficultés particulières que l'auteur de [7] espère avoir surmontées.

$\tilde{J}$ est isogène au produit des J_α relatifs aux $\mathfrak{p}_\alpha$ tels que $\mathfrak{p}_\alpha + I \neq \underline{T}$.

Remarques.- 1) Le fait qu'il existe au moins un tel $\mathfrak{p}_\alpha$ entraîne que $\tilde{J} \neq 0$.

2) On peut montrer ([1]) que $1 + w$ appartient à $\mathfrak{a}$, autrement dit que $\tilde{J}$ est un quotient de la variété abélienne $J^- = J/J_+$, où $J_+ = (1 + w)J$. Lorsque $N < 250$, on a $\tilde{J} = J^-$ sauf pour $N = 67, 109, 139, 151, 179, 227$, cf. § 4.

THÉORÈME 2 ([7]).- Le groupe $\tilde{J}(\mathbb{Q})$ est fini.

Voir n° 2.6.

Remarque.- Le comportement de J_+ est très différent de celui de $\tilde{J}$. En effet $J_+(\mathbb{Q})$ est infini (cf. [7]) dès que $\dim(J_+) \geq 1$, ce qui se produit pour tout $N \geq 73$, ainsi que pour $N = 37, 43, 53, 61, 67$, cf. § 4.

THÉORÈME 3 ([7]).- $X_0(N)(\mathbb{Q})$ est fini.

(On rappelle que N est supposé premier $\neq 2, 3, 5, 7, 13$.)

En effet, soit $\tilde{X}$ l'image de $X_0(N)$ dans $\tilde{J}$ par la projection canonique $X_0(N) \to J \to \tilde{J}$. Le th. 2 entraîne que $\tilde{X}(\mathbb{Q})$ est fini. D'autre part, on a $\dim(\tilde{J}) \geq 1$, et $\tilde{X}$ engendre $\tilde{J}$; il s'ensuit que $\tilde{X}$ est une courbe, et les fibres de $X_0(N) \to \tilde{X}$ sont finies. La finitude de $X_0(N)(\mathbb{Q})$ résulte alors de celle de $\tilde{X}(\mathbb{Q})$.

Remarque.- On savait déjà, d'après Manin (cf. [13], th. 2') que, pour tout nombre premier N , il existe un entier $m(N) \geq 1$ tel que $X_0(N^m)(\mathbb{Q})$ soit fini pour $m \geq m(N)$ (ou pour $m = m(N)$, cela revient au même). Le th. 3 équivaut à dire que l'on peut prendre $m(N)$ égal à 1 si $N \neq 2, 3, 5, 7, 13$.

2.6 Démonstration du théorème 2

2.6.1 p-groupes admissibles

Soit p un nombre premier $\neq N$. Par un p-groupe admissible on entendra un schéma en groupes G sur $S = \mathrm{Spec}(\mathbb{Z})$ jouissant des propriétés suivantes :

(i) G est quasi-fini, plat et séparé ;

(ii) G est annulé par une puissance de p ;

(iii) au-dessus de $S' = \mathrm{Spec}(\mathbb{Z}[\frac{1}{N}])$, le groupe $G_{/S'}$ est fini et plat, et admet une filtration (dite admissible) par des sous-groupes finis et plats dont

les quotients successifs sont S'-isomorphes à l'un des schémas en groupes $\mathbb{Z}/p\mathbb{Z}$ et μ_p (racines p-ièmes de l'unité).

A un tel groupe on attache les invariants numériques suivants :

$\ell(G) = \log_p(\text{ordre de } G_{/S'})$

$\delta(G) = \log_p(\text{ordre de } G_{/S'}) - \log_p(\text{ordre de } G_{/\mathbb{F}_N})$

$\alpha(G) =$ nombre de $\mathbb{Z}/p\mathbb{Z}$ intervenant dans les quotients successifs d'une filtration admissible de $G_{/S'}$

$h^i(G) = \log_p(\mathrm{Card}(H^i(S,G)))$, la cohomologie étant prise pour la topologie fppf.

En raisonnant par récurrence sur $\ell(G)$, on démontre l'inégalité

(*) $\qquad h^1(G) - h^0(G) \leq \delta(G) - \alpha(G)$.

2.6.2 Finitude en p

On prend maintenant pour p un facteur premier de n , et l'on pose $P = I + p\underline{T}$, cf. n° 2.4. On note $\underline{T}_p$ le complété de T pour la topologie P-adique ; il est facile de voir que $\underline{T}_p$ est facteur direct de l'anneau semi-local $\underline{T}_p = \mathbb{Z}_p \otimes \underline{T}$, complété de $\underline{T}$ en p ; on note ε_p l'idempotent correspondant de $\underline{T}_p$.

Soit maintenant $J_{\mathbb{Z}}$ le modèle de Néron [8] de J sur $\mathbb{Z}$, et $J^o_{\mathbb{Z}}$ sa composante neutre (elle ne diffère d'ailleurs de $J_{\mathbb{Z}}$ qu'au-dessus du nombre premier N , cf. n° 3.1). Si $m \geq 1$, on note $J^o[p^m]$ le sous-schéma en groupes de $J^o_{\mathbb{Z}}$ noyau de p^m ; l'anneau $\underline{T}/p^m\underline{T}$ (donc aussi l'anneau $\underline{T}_p$) opère de façon naturelle sur $J^o[p^m]$, ce qui permet de définir la P-composante

$$J^o[p^m]_p = \varepsilon_p . J^o[p^m]$$

de $J^o[p^m]$.

Les schémas en groupes $J^o[p^m]$ et $J^o[p^m]_p$ jouissent des propriétés (i) et (ii) de 2.6.1. De plus :

(a) $J^o[p^m]_p$ jouit de la propriété (iii), i.e. est un p-groupe admissible.

Cela se démontre par un argument analogue à celui utilisé au n° 2.4, cf. [7].

(b) Quand m varie, l'ordre de $H^1(S, J^o[p^m]_p)$ reste borné.

Cela se voit de la manière suivante (cf. [7]) : on commence par prouver que

$$\delta(J^o[p^m]_p) = mg_p + O(1) \quad \text{pour} \quad m \to \infty$$

$$\alpha(J^o[p^m]_p) = mg_p + O(1) \quad \text{pour} \quad m \to \infty ,$$

où g_p est le rang de $\underline{T}_p$ sur Z_p (i.e. la somme des g_α relatifs aux $\mathfrak{p}_\alpha$ contenus dans P). Vu l'inégalité (*), on en conclut que $h^1(J^o[p^m]_p) - h^o(J^o[p^m]_p)$ reste borné. Mais $H^o(S, J[p^m]_p)$ est un sous-groupe du groupe de torsion de $H^o(S, J_{\mathbf{Z}}) = J(\mathbf{Q})$, donc est d'ordre borné ; il en résulte que $h^o(J^o[p^m]_p)$ est borné, et il en est par suite de même de $h^1(J^o[p^m]_p)$.

Posons maintenant

$$M = H^o(S, J_{\mathbf{Z}}) = J(\mathbf{Q}) \quad \text{et} \quad M^o = H^o(S, J^o_{\mathbf{Z}}) .$$

Le quotient M/M^o est fini. La suite exacte de cohomologie associée à la suite exacte de faisceaux fppf

$$0 \to J^o[p^m] \to J^o_{\mathbf{Z}} \xrightarrow{p^m} J^o_{\mathbf{Z}} \to 0$$

donne une injection de $M^o/p^m M^o$ dans $H^1(S, J^o[p^m])$, d'où par passage à la limite un homomorphisme injectif de $\underline{T}_p$-modules

$$\mathbf{Q}_p/\mathbf{Z}_p \otimes M^o = \varinjlim . \; M^o/p^m M^o \to \varinjlim . \; H^1(S, J^o[p^m]) .$$

En passant aux P-composantes, on en déduit une injection

$$\underline{T}_P \otimes_{\underline{T}_p} (\mathbf{Q}_p/\mathbf{Z}_p \otimes M^o) \to \varinjlim . \; H^1(S, J^o[p^m]_p) .$$

Comme, d'après (b), le groupe $\varinjlim . \; H^1(S, J^o[p^m]_p)$ est fini, on en conclut que $\underline{T}_P \otimes_{\underline{T}_p} (\mathbf{Q}_p/\mathbf{Z}_p \otimes M^o)$ est fini, ce qui entraîne la finitude de $\underline{T}_P \otimes_{\underline{T}} M^o$, donc aussi celle de $\underline{T}_P \otimes_{\underline{T}} M$.

Remarque.- La méthode de "descente infinie" utilisée ci-dessus fournit en même temps la finitude de la composante P-primaire $Ш_P$ du groupe de Šafarevič-Tate de J sur $\mathbf{Q}$. En fait, on a $Ш_P = 0$ si $p \neq 2$; cela se voit par une descente simple ("first descent") utilisant l'existence (cf. [7]) d'un élément π_P de $\underline{T}$

tel que $I.\underline{T}_P = \pi_P.\underline{T}_P$.

2.6.3 Fin de la démonstration du th. 2

Soient (P_i) les idéaux maximaux de $\underline{T}$ contenant I . L'anneau $\underline{T}_I$ est produit des anneaux locaux $\underline{T}_{P_i}$. D'après 2.6.2, le groupe $\underline{T}_I \otimes_{\underline{T}} M$ est fini (car produit des $\underline{T}_{P_i} \otimes_{\underline{T}} M$), et il est facile de voir que cela équivaut à la finitude de $J(\mathbf{Q})$.

§ 3. Modèle de Néron et applications

3.1 Fibre en N du modèle de Néron $J_{\mathbf{Z}}$

Notons $J_{/\mathbf{F}_N}$ (resp. $J^0_{/\mathbf{F}_N}$) la fibre en N de $J_{\mathbf{Z}}$ (resp. de sa composante neutre $J^0_{\mathbf{Z}}$). Tout élément x de $M = J(\mathbf{Q})$ définit par spécialisation un point rationnel $\bar{x}$ de $J_{/\mathbf{F}_N}$; le point $\bar{x}$ appartient à $J^0_{/\mathbf{F}_N}$ si et seulement si x appartient au sous-groupe M^0 de M , cf. 2.6.2. En particulier, le groupe C du n° 2.2 se spécialise en un sous-groupe $\bar{C}$ de $J_{/\mathbf{F}_N}$ formé de points rationnels sur $\mathbf{F}_N$.

THÉORÈME 4.- On a $J_{/\mathbf{F}_N} = \bar{C} \times J^0_{/\mathbf{F}_N}$, et $\bar{C}$ est d'ordre n .

(Ce résultat est essentiellement dû à Deligne-Rapoport [1], cf. l'Appendice de [7], écrit en collaboration avec Rapoport.)

Voir n° 3.4.

3.2 Rétraction de $J(\mathbf{Q})$ sur C et torsion de $J(\mathbf{Q})$

Le th. 4 montre en particulier que, pour tout $x \in J(\mathbf{Q})$, il existe un unique $y \in C$ tel que l'image de $\bar{x}$ par la projection de $J_{/\mathbf{F}_N}$ sur $\bar{C}$ soit $\bar{y}$. L'application $x \mapsto y$ est une rétraction ρ de $J(\mathbf{Q})$ sur C ; en particulier C est facteur direct dans $J(\mathbf{Q})$.

THÉORÈME 5 ([7]).- Le sous-groupe de torsion de $J(\mathbf{Q})$ est réduit à C .

(Ce résultat avait été conjecturé par Ogg [9b].)

Vu ce qui précède, on a $J(\mathbf{Q}) = M^0 \oplus C$ et il suffit de montrer que M^0 est sans torsion. Sinon, M^0 contiendrait un sous-groupe isomorphe à $\mathbf{Z}/p\mathbf{Z}$,

avec p premier. D'après la prop. 1 du n° 2.4, p diviserait l'ordre n de C , et $J(\mathbb{Q})$ contiendrait donc un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$; si $p \neq 2$ (resp. si $p = 2$) un argument facile (resp. pas si facile, cf. note ([1]), n° 2.4) sur les formes modulaires (mod.p) montre que c'est impossible (voir [7] pour plus de détails).

3.3 Image de $X_0(N)(\mathbb{Q})$ dans C

Si l'on restreint la rétraction ρ à $X_0(N)(\mathbb{Q})$ on obtient une application

$$\rho : X_0(N)(\mathbb{Q}) \to C = \mathbb{Z}/n\mathbb{Z} .$$

THÉORÈME 6 ([7]).- Si $x \in X_0(N)(\mathbb{Q})$, l'élément $\rho(x)$ de $\mathbb{Z}/n\mathbb{Z}$ est égal à l'une des valeurs suivantes :

0 ou 1 ,

1/2 (possible seulement si $N \equiv -1 \pmod 4$) ,

1/3 ou 2/3 (possible seulement si $N \equiv -1 \pmod 3$) .

Voir n° 3.4.

Remarques.- 1) Si $N \equiv -1 \pmod 3$, l'entier n n'est pas divisible par 3 , et 1/3 a un sens dans $\mathbb{Z}/n\mathbb{Z}$; de même 1/2 a un sens dans $\mathbb{Z}/n\mathbb{Z}$ lorsque n est impair, ce qui est le cas si $N \equiv -1 \pmod 4$.

2) On a $\rho(0) = 1$ et $\rho(\infty) = 0$.

Posons maintenant $J_- = (1 - w)J \subset J$; si $x \in X_0(N)$, on vérifie facilement que l'élément $r(x) = cl((x) - (wx))$ appartient à J_- , d'où un morphisme

$$r : X_0(N) \to J_- .$$

Si $x \in X_0(N)(\mathbb{Q})$, posons $\lambda(x) = \rho(r(x)) \in \mathbb{Z}/n\mathbb{Z}$.

COROLLAIRE 1.- On a $\lambda(x) = \pm 1 , 0 ,$ ou $\pm\frac{1}{3}$.

Cela résulte du th. 6 et du fait que $\lambda(x) = 2\rho(x) - 1$.

COROLLAIRE 2.- Supposons $J_-(\mathbb{Q})$ fini. Alors :

a) On a $J_-(\mathbb{Q}) = C$.

b) Pour tout $x \in X_0(N)(\mathbb{Q})$, on a $r(x) = \lambda(x).c$, avec $\lambda(x) = \pm 1 , 0$ ou $\pm\frac{1}{3}$.

L'assertion a) résulte de ce que C est contenu dans $J_-(\mathbb{Q})$, et que c'est le sous-groupe de torsion de $J(\mathbb{Q})$, cf. th. 5. L'assertion b) résulte du cor. 1 et du fait que ρ est l'identité sur C .

Remarque.- Un cas particulier important où $J_-(\mathbb{Q})$ est fini est celui où $\widetilde{J} = J^-$ (cf. n° 2.5) puisqu'alors J_- est isogène à $\widetilde{J}$ et l'on peut appliquer le th. 2.

THÉORÈME 7.- a) Si $N \neq 11, 17, 19, 37$, le morphisme $r : X_0(N) \to J_-$ est injectif en dehors des points fixes de w.

b) Si $J_-(\mathbb{Q})$ est fini, et $x \in X_0(N)(\mathbb{Q})$, on a :

$\lambda(x) = \pm\frac{1}{3} \Rightarrow N = 11$ ou 17,

$\lambda(x) = 0 \Rightarrow N = 11, 19, 43, 67,$ ou 163.

L'assertion a) est facile ; l'assertion b) est due à Ogg, Parry et Brumer.

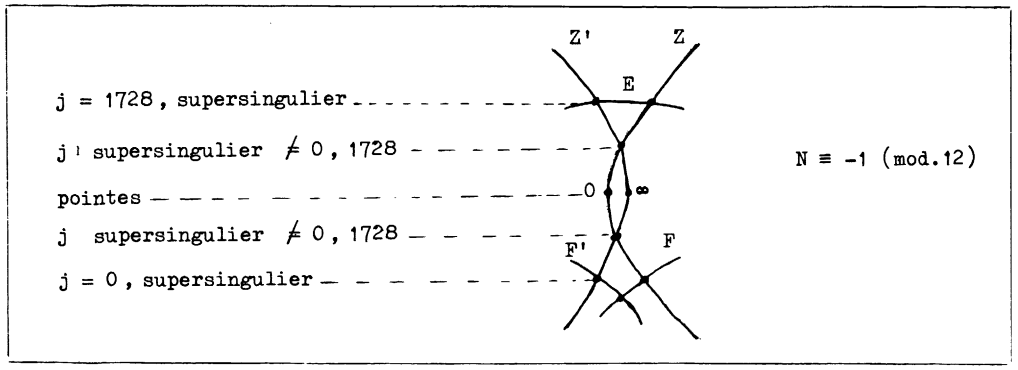
Remarques.- 1) Pour $N = 11, 17$, il existe $x \in X_0(N)(\mathbb{Q})$ tel que $\lambda(x) = \pm\frac{1}{3}$.

2) Pour $N = 11, 19, 43, 67, 163$, les courbes elliptiques à multiplication complexe par $\mathbb{Z}[(1 + \sqrt{-N})/2]$ fournissent des exemples de points rationnels x tels que $\lambda(x) = 0$.

COROLLAIRE.- Si $N \neq 11, 17, 19, 37, 43, 67, 163$, et si $J_-(\mathbb{Q})$ est fini, les seuls points rationnels de $X_0(N)$ sont les pointes 0 et ∞.

3.4 Démonstrations des ths. 4 et 6

Elles utilisent le modèle minimal régulier $X_0(N)_{/\mathbb{Z}}$ sur $\mathrm{Spec}(\mathbb{Z})$ de la courbe $X_0(N)$. Rappelons (cf. [1], p. 290) que ce schéma est obtenu en faisant éclater certains points (super)singuliers du schéma modulaire attaché à $X_0(N)$. La fibre en N de $X_0(N)_{/\mathbb{Z}}$ a la structure indiquée ci-dessous (dans le cas particulier $N \equiv -1 \pmod{12}$, qui est le plus compliqué) :



Elle est formée de deux droites projectives Z et Z' (correspondant à j(z) et j(Nz) , si l'on ose dire...) se coupant transversalement aux valeurs supersingulières de j distinctes de 0 , 1728 ; lorsque N+1 est divisible par 4 (resp. par 3), on ajoute à Z et Z' une droite E (resp. deux droites F et F') correspondant à l'éclatement de la valeur supersingulière j = 1728 (resp. j = 0).

Cette description explicite de $X_0(N)_{/\mathbb{Z}}$, jointe à un résultat de Raynaud [11], permet de démontrer le th. 4. En ce qui concerne le th. 6, on remarque qu'un point rationnel de $X_0(N)$ se spécialise en un point lisse de la fibre en N , c'est-à-dire en un point de l'une des courbes $\tilde{Z}$, $\tilde{Z}'$, $\tilde{E}$, $\tilde{F}$, $\tilde{F}'$ obtenues en retirant de Z ,..., F' ses points d'intersection avec les autres. Tout revient alors à prouver que

$$\rho(\tilde{Z}) = 1 \ , \quad \rho(\tilde{Z}') = 0 \ , \quad \rho(\tilde{E}) = \tfrac{1}{2} \ , \quad \rho(\tilde{F}) = \tfrac{2}{3} \ , \quad \rho(\tilde{F}') = \tfrac{1}{3} \ ;$$

le calcul se trouve dans l'Appendice de [7].

§ 4. Compléments

4.1 Résultats numériques

La TABLE des pages 16-17 résume l'essentiel des résultats connus pour $N < 250$. On y trouvera :

la valeur de $n = \mathrm{Num}\left(\frac{N-1}{12}\right)$;

la dimension g_+ (resp. g_-) de J_+ (resp. J_-), décomposée en somme des g_α correspondant aux différents facteurs simples J_α (cf. n° 2.3) ; les g_α correspondant aux facteurs de $\tilde{J}$ sont soulignés ;

le nombre ν de points rationnels de $X_0(N)$ distincts des pointes 0 et ∞ ;

les valeurs des invariants $\lambda(x)$ du n° 3.3.

Remarques.- 1) Les valeurs de g_+ , g_- et des g_α sont tirées de tables de Wada et d'Atkin.

2) On constate que, pour $N < 250$ et $N \neq 151 , 227$, on a $\dim(J_-) = \dim(\tilde{J})$ ou $\dim(J_-) = \dim(\tilde{J}) + 1$. Dans le second cas, J_- est isogène au produit de

$\tilde{J}$ par une courbe elliptique E de conducteur N n'ayant qu'un nombre fini de points rationnels (cela a été démontré par Brumer et Kramer au moyen d'une " 2-descente "). Vu le th. 2, il en résulte que $J_-(\mathbb{Q})$ est fini, et le th. 7 du n° 3.3 est applicable ; cela explique que, pour ces valeurs de N , on puisse déterminer presque complètement les points rationnels de $X_0(N)$.

4.2 Points d'ordre fini des courbes elliptiques

Si M est un entier ≥ 1 , rappelons que l'on note $Y_1(M)$ la courbe modulaire dont les points correspondent aux couples (E,P) , où E est une courbe elliptique et P un point d'ordre M sur E . La courbe projective obtenue en adjoignant à $Y_1(M)$ ses "pointes" est notée $X_1(M)$; c'est un revêtement (en général ramifié) de $X_0(M)$, le groupe de Galois du revêtement étant $(\mathbb{Z}/M\mathbb{Z})^*/\{\pm 1\}$.

Lorsque $M = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$, la courbe $X_1(M)$ est de genre 0 , et $Y_1(M)$ a une infinité de points rationnels. En dehors de ces cas (i.e. pour $M \geq 13$ et $M = 11$), on ne connaît aucun point rationnel de $Y_1(M)$ et il paraît raisonnable de conjecturer avec Ogg qu'il n'en existe pas. On a à ce sujet le résultat suivant :

THÉORÈME 8.- Supposons $M \geq 13$ ou $M = 11$. Alors :

a) La courbe $Y_1(M)$ n'a qu'un nombre fini de points rationnels.

b) Si $M < 250$, et $M \neq 151, 227$, la courbe $Y_1(M)$ n'a aucun point rationnel.

D'après Kubert [6], a) et b) sont vrais si tous les facteurs premiers de M sont < 23 . Si d'autre part M possède un facteur premier $N \geq 23$, la courbe $X_1(M)$ se projette sur la courbe $X_0(N)$; comme $X_0(N)(\mathbb{Q})$ est fini (th. 3), il en est de même de $X_1(M)(\mathbb{Q})$, ce qui démontre a) ; l'assertion b) se démontre par un argument analogue, basé sur les déterminations explicites du n° 4.1.

Remarque.- Demjanenko a publié [2] une démonstration de l'assertion suivante :

(?) Pour tout corps de nombres algébriques k fini sur $\mathbb{Q}$, il existe un entier $m(k)$ tel que $Y_1(M)$ n'ait pas de point rationnel sur k pour $M \geq m(k)$.

Malheureusement, sa démonstration ne semble pas complète.

4.3 Autres courbes modulaires

Les résultats de cet exposé sont relatifs aux courbes modulaires définies par le sous-groupe de Borel $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ du groupe $GL_2(\mathbf{Z}/N\mathbf{Z})$. On aimerait pouvoir traiter aussi les courbes modulaires liées aux autres sous-groupes de $GL_2(\mathbf{Z}/N\mathbf{Z})$, notamment :

a) au sous-groupe "exceptionnel" formé des éléments dont l'image dans $PGL_2(\mathbf{Z}/N\mathbf{Z})$ appartient au sous-groupe $\mathfrak{S}_4$ $(N \not\equiv \pm 1 \pmod 8)$;

b) aux normalisateurs de sous-groupes de Cartan, tant déployés que non déployés.

La multiplication complexe permet de construire des points rationnels sur les courbes de type b). Ces points sont-ils les seuls points rationnels de ces courbes (à part les pointes) pour N assez grand, par exemple $N \geq 13$? Il serait intéressant de le savoir.

TABLE

N	n	g_+	g_-	ν	valeurs de $\lambda(x)$
11	5	0	$\underline{1}$	3	$0, \pm 1/3$
17	4	0	$\underline{1}$	2	$\pm 1/3$
19	3	0	$\underline{1}$	1	0
23	11	0	$\underline{2}$	0	
29	7	0	$\underline{2}$	0	
31	5	0	$\underline{2}$	0	
37	3	1	$\underline{1}$	2	± 1
41	10	0	$\underline{3}$	0	
43	7	1	$\underline{2}$	1	0
47	23	0	$\underline{4}$	0	
53	13	1	$\underline{3}$	0	
59	29	0	$\underline{5}$	0	
61	5	1	$\underline{3}$	0	
67	11	2	$1+\underline{2}$	1	0
71	35	0	$\underline{3}+\underline{3}$	0	
73	6	2	$\underline{1}+\underline{2}$	0	
79	13	1	$\underline{5}$	0	
83	41	1	$\underline{6}$	0	
89	22	1	$\underline{1}+\underline{5}$	0	
97	8	3	$\underline{4}$	0	
101	25	1	$\underline{7}$	0	
103	17	2	$\underline{6}$	0	
107	53	2	$\underline{7}$	0	
109	9	3	$1+\underline{4}$	0	
113	28	3	$\underline{1}+\underline{2}+\underline{3}$	0	
127	21	3	$\underline{7}$	0	
131	65	1	$\underline{10}$	0	
137	34	4	$\underline{7}$	0	
139	23	3	$1+\underline{7}$	0	
149	37	3	$\underline{9}$	0	

TABLE (suite)

N	n	g_+	g_-	ν	valeurs de $\lambda(x)$
151	25	3	3 + 6	??	??
157	13	5	7	0	
163	27	1 + 5	7	1	0
167	83	2	12	0	
173	43	4	10	0	
179	89	3	1 + 11	0	
181	15	5	9	0	
191	95	2	14	0	
193	16	2 + 5	8	0	
197	49	1 + 5	10	0	
199	33	4	2 + 10	0	
211	35	3 + 3	2 + 9	0	
223	37	2 + 4	12	0	
227	113	2 + 3	2 + 2 + 10	??	??
229	19	1 + 6	11	0	
233	58	7	1 + 11	0	
239	119	3	17	0	
241	20	7	12	0	

BIBLIOGRAPHIE

[1] P. DELIGNE et M. RAPOPORT - Les schémas de modules de courbes elliptiques, Lecture Notes in Math. n° 349, p. 143-316, Springer, 1973.

[2] V.A. DEMJANENKO - Sur la torsion des courbes elliptiques [en russe], Izv. Akad. N. CCCP, 35 (1971), p. 280-307 [MR 44, 2755].

[3] E. HECKE - Mathematische Werke, 2ème édition, Göttingen, 1970.

[4] N. KATZ - p-adic properties of modular schemes and modular forms, Lecture Notes in Math. n° 350, p. 69-190, Springer, 1973.

[5] M. KOIKE - On the congruences between Eisenstein series and cusp forms, à paraître.

[6] D. KUBERT - Universal bounds on the torsion of elliptic curves, à paraître.

[7] B. MAZUR - Modular curves and the Eisenstein ideal, en préparation.

[8] A. NÉRON - Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, Publ. Math. I.H.E.S., 21 (1964), p. 361-483 [MR 31, 3424].

[9] A. OGG - a) Rational points on certain elliptic modular curves, Proc. Symp. Pure Math., 24 (1973), AMS, Providence, p. 221-231.

b) Diophantine equations and modular forms, Bull. AMS, 81 (1975), p. 14-27.

[10] A. OGG - Hyperelliptic modular curves, Bull. Soc. math. France, 102 (1974), p. 449-462.

[11] M. RAYNAUD - Spécialisation du foncteur de Picard, Publ. Math. I.H.E.S., 38 (1970), p. 27-76.

[12] K. RIBET - Endomorphisms of semi-stable abelian varieties over number fields, Annals of Math., 101 (1975), p. 555-562.

[13] J.-P. SERRE - p-torsion des courbes elliptiques (d'après Y. MANIN), Séminaire Bourbaki, 22e année, 1969/70, exposé 380, Lecture Notes in Math. n° 180, Springer, 1971.

[14] G. SHIMURA - Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan, n° 11, Tokyo-Princeton, 1971.