SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

B. MORLAYE

Points rationnels sur Q de certaines courbes modulaires

Séminaire de théorie des nombres de Grenoble, tome 5 (1975-1977), exp. n° 6, p. 1-10

<http://www.numdam.org/item?id=STNG_1975-1977__5__A6_0>

Séminaire de Théorie des Nombres
21 octobre 1976
Grenoble

POINTS RATIONNELS SUR $\mathbb{Q}$ DE CERTAINES COURBES MODULAIRES.

par

B. MORLAYE

INTRODUCTION.

Soit N un entier. Désignons par $\Gamma_o(N)$ le sous-groupe de $SL_2(\mathbb{Z})$ formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ vérifiant $c \equiv 0 \pmod{N}$. Ce groupe opère sur le demi-plan de Poincaré $H = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ par : $\begin{pmatrix} a & b \\ c & d \end{pmatrix} . z = \dfrac{az+b}{cz+d}$.

Le quotient $\Gamma_o(N)\backslash H$ est une courbe algébrique affine, non compacte $Y_o(N)_{\mathbb{C}}$. On la compactifie en une courbe projective $X_o(N)_{\mathbb{C}}$ en lui ajoutant l'ensemble (fini) de ses pointes : $\Gamma_o(N)\backslash \mathbb{P}^1(\mathbb{Q})$. On montre que $Y_o(N)_{\mathbb{C}}$ et $X_o(N)_{\mathbb{C}}$ s'obtiennent par extension des scalaires de courbes algébriques sur $\mathbb{Q}$, notées $Y_o(N)$ et $X_o(N)$. Ces courbes sont susceptibles d'une interprétation en terme modulaire, qui explique leur intérêt.

Mis à part le nombre (fini) des cas où $X_o(N)$ est de genre 0 , auquel cas l'ensemble $X_o(N)_{\mathbb{Q}}$ des points rationnels sur $\mathbb{Q}$ de $X_o(N)$ est infini, on conjecture que $X_o(N)_{\mathbb{Q}}$ est un ensemble fini.

Cette conjecture a été vérifiée lorsque le genre est 1 (cf. [2]). Elle a été également vérifiée par Ogg et Mazur, lorsque le genre est ≥ 2 et que N est un nombre <u>premier</u> < 250 , à un petit nombre d'exceptions près (cf. [4] et aussi la table à la fin de [3]). L'exposé qui suit est consacré à étudier trois des cas exceptionnels en question. Plus précisément, on va montrer ([6]) :

THEOREME. - Pour $N = 53, 113, 137$ les seuls points rationnels de $X_o(N)$ sur $\mathbb{Q}$ sont les pointes.

La démonstration utilise notamment des résultats encore non publiés de Mazur (cf. toutefois [3]), et un théorème récent d'Atkin, que nous commencerons par rappeler.

I. RAPPELS.

1) L'interprétation modulaire de $X_o(N)$.

On montre que la courbe $X_o(N)$ paramètre les classes d'isomorphisme de paires (E,C) où E est une courbe elliptique et $C \subset E$ est un sous-groupe cyclique d'ordre N . En fait à un tel couple est associé un point $j(E,A)$ de $Y_o(N)_k$ si le couple est défini sur le corps k , et tout point de $Y_o(N)_k$ peut être obtenu ainsi.

On peut aussi dire que la courbe $X_o(N)$ paramètre les classes d'isomorphisme d'isogénies rationnelles cycliques de degré N .

2) L'involution d'Atkin-Lehner.

Nous supposerons désormais, dans toute la suite, que N est premier. Dans ces conditions, la courbe $X_o(N)$ a deux pointes : P_o et P_∞ correspondant respectivement à 0 et ∞ , et ces deux pointes sont rationnelles sur $\mathbb{Q}$.

La courbe $X_o(N)$ a alors une involution W , qui échange les deux pointes, et qui, lorsqu'elle agit sur $X_o(N)_{\mathbb{C}}$, est associée à la matrice $W_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$, c'est-à-dire à la transformation $z \mapsto -\frac{1}{Nz}$ de H . Il est bon de remarquer que la matrice W_N normalise $\Gamma_o(N)$.

Nous allons donner l'interprétation modulaire de W (cf. [4] et [5]).

PROPOSITION. -

i) Du point de vue modulaire, W transforme le couple (E,C) en le couple $(E/C\,,\,E_N/C)$ où $E_N = \{x \in E \mid N.x = 0\}$.

ii) En termes d'isogénies, W transforme l'isogénie $E \xrightarrow{\lambda} E'$, cyclique de degré N , en l'isogénie $E' \xrightarrow{\hat{\lambda}} E$ avec $\hat{\lambda} \circ \lambda = N : E \to E$ et $\lambda \circ \hat{\lambda} = N : E' \to E'$.

Remarque : on a des interprétations modulaires analogues, même lorsque N est non premier.

On peut en particulier caractériser les points fixes de W . Supposons que le couple (E,C) corresponde à un point fixe de W . Les paires (E,C) et $(E/C\,,\,E_N/C)$ sont alors isomorphes : il existe un isomorphisme $E/C \to E$ transformant E_N/C en C . Il en résulte que E admet une multiplication complexe λ de noyau C qui vérifie $\lambda^2 = N.\varphi$, $\varphi \in \mathrm{Aut}(E)$. Si l'on suppose $N > 3$, on a alors $\varphi = -1$ et $\lambda^2 = -N$: la courbe $X_o(N)$ admet une multiplication complexe par $\sqrt{-N}$. On a obtenu :

PROPOSITION. - Si $N > 3$, les points fixes de W sur $X_o(N)$ correspondent aux courbes elliptiques qui admettent une multiplication complexe par $\sqrt{-N}$.

Rappelons enfin que si l'on pose $X_o(N)^+ = \{1,W\}\backslash X_o(N)$, la courbe $X_o(N)^+$ a un genre g^+ donné par :

$$g^+ = \frac{g+1}{2} - \frac{n(W)}{4} \quad .$$

Dans cette formule :

- $g = \dfrac{N-a}{12}$ est le genre de $X_o(N)$, où l'on suppose

$$\begin{cases} N \equiv a \pmod{12} \\ a = -1,5,7,13 \end{cases}$$

- $n(W)$ est le nombre des points fixes de W . Il se calcule à l'aide de la formule de Fricke :

$$n(W) = \begin{cases} h(-N) + h(-4N) & \text{si } N \equiv 3 \pmod 4 \\ h(-4N) & \text{sinon} \end{cases}$$

où $h(-D)$ est le nombre de classes de formes quadratiques binaires de discriminant $-D$.

Il faut aussi rappeler que W est définie sur $\mathbb{Q}$, et qu'il en est donc de même de $X_0^+(N)$.

3) La jacobienne de $X_0(N)$. Résultats de Mazur.

Soit C une courbe algébrique, de genre $g \geq 1$. On lui associe une variété abélienne $J(C)$, de dimension g : sa jacobienne. Cette dernière est obtenue comme ensemble des classes des diviseurs de C , modulo l'équivalence linéaire, i.e., deux diviseurs D , D' de C sont équivalents si $D - D' = (f)$ diviseur de la fonction (méromorphe) f .

Si P est un point fixé de C , on a un plongement $C \xrightarrow{\varphi} J(C)$ en posant $\varphi(Q)$ = classe de $Q - P$; en outre φ est rationnelle si le point fixé P est rationnel (disons qu'ici toutes les questions de rationnalité sont relatives à $\mathbb{Q}$).

En particulier la courbe $X_0(N)$ se plonge rationnellement dans sa jacobienne $J_0(N)$ par $P \to P - P_\infty$ (la classe...). En particulier, soit $c = c\ell(P_0 - P_\infty)$ l'image de P_0 dans ce plongement. C'est un point rationnel de $J_0(N)$: $c \in J_0(N)_{\mathbb{Q}}$.

Ogg et Mazur ont démontré le résultat suivant :

THEOREME. -

i) le sous-groupe cyclique C de $J_0(N)_{\mathbb{Q}}$ engendré par c est fini, d'ordre $\operatorname{num} \frac{N-1}{12}$.

ii) C est le sous-groupe de torsion de $J_0(N)_{\mathbb{Q}}$.

iii) Si x n'est pas une pointe de $X_0(N)$ et est rationnel sur $\mathbb{Q}$

et si $N = 53, 113, 137$, l'image du diviseur $x - w(x)$ dans $J_o(N)_{\mathbb{Q}}$ est égale à $\pm 1/3\, c$.

4) Points de Weierstrass. Théorème d'Atkin.

Rappelons d'abord qu'un point P est dit point de Weierstrass de la courbe algébrique C , de genre g s'il existe une fonction définie sur C , ayant en P un pôle d'ordre $\leq g$ et partout ailleurs régulière sur C .

Atkin a montré récemment le :

THEOREME. - Si N est un entier premier, la pointe P_∞ n'est jamais point de Weierstrass de la courbe $X_o(N)$. (cf. [1]).

II. DEMONSTRATION DU THEOREME DE PARRY.

Nous supposerons désormais que $N = 53, 113$ ou 137. Dans ces conditions P_o et P_∞ sont les seules pointes de $X_o(N)$. Elles sont rationnelles et s'échangent par W . L'étude des points rationnels de $X_o(N)$ revient donc à l'étude de $Y_o(N)_{\mathbb{Q}}$. En utilisant ses méthodes, Mazur a prouvé que $Y_o(N)_{\mathbb{Q}}$ contenait 0 ou deux points. Nous allons prouver que :

THEOREME. - $Y_o(N)_{\mathbb{Q}}$ est vide.

Il est clair que ce résultat est équivalent au théorème énoncé dans l'introduction.

1) Construction des fonctions f_1 , f_2 .

Remarquons que la formule donnée au I, permet de calculer le genre $g(N)$ des trois courbes modulaires qui nous intéressent. On trouve :

a) $g(53) = 4$

b) $g(113) = 9$

c) $g(137) = 11$.

Observons par ailleurs que, dans chacun de ces cas, le numérateur de $\frac{N-1}{12}$ est :

a) $n = 13$; b) $n = 28$ et c) $n = 34$.

On vérifie ainsi le :

LEMME. - <u>On a toujours</u> $n = 3g + 1$.

Il en résulte que le sous-groupe d'Ogg de $J_0(N)_{\mathbb{Q}}$, engendré par $c = P_0 - P_\infty$ est d'ordre $3g + 1$. Donc $(3g+1)c = 0$ et ainsi $\frac{1}{3}c = -gc$ [remarquons que $1/3$ a un sens ici (dans $\mathbb{Z}/n\mathbb{Z}$)].

Soit maintenant $x \in Y_0(N)_{\mathbb{Q}}$. L'involution w est définie sur $\mathbb{Q}$, donc $w(x) \in Y_0(N)_{\mathbb{Q}}$. Considérons l'image dans $J_0(N)_{\mathbb{Q}}$ du diviseur $x - w(x)$. D'après le théorème d'Ogg-Mazur, cette image est $\pm\frac{1}{3}c$, et la remarque précédente permet de supposer que c'est $\frac{1}{3}c$ (sinon on échange x et $w(x)$). Or, puisque $\frac{1}{3}c = -gc$, il en résulte que $x - w(x)$ et $-g(P_0 - P_\infty)$ d'une part et $x - w(x)$ et $-\frac{1}{3}(P_0 - P_\infty)$ d'autre part sont linéairement équivalents. Ainsi, <u>il existe deux fonctions</u> f_1 <u>et</u> f_2 <u>méromorphes sur</u> $X_0(N)$ <u>et telles que</u> :

$$(f_1) = P_0 - P_\infty - 3x + 3w(x)$$

$$(f_2) = gP_0 - gP_\infty + x - w(x)$$

L'involution w opérant linéairement sur les diviseurs, il résulte de ce qui précède que $(f_1 \circ w) = -(f_1)$ et $(f_2 \circ w) = -(f_2)$. Ainsi, quitte à multiplier f_1 et f_2 par un nombre complexe $\neq 0$ convenable, on peut supposer :

$$f_1 \circ w = \frac{1}{f_1} \qquad f_2 \circ w = \frac{1}{f_2} \ .$$

Il en résulte tout de suite que si x est fixe par w , $f_1(x) = \pm 1$ et $f_2(x) = \pm 1$.

D'après la formule de Hurwitz donnant le nombre des points fixes de w , et compte-tenu du fait que dans chacun des trois cas étudiés le discriminant de $\mathbb{Q}(\sqrt{-N})$ est $-4N$, on a dans tous ces cas : $n(W) = h$ (= nombre de classes de $\mathbb{Q}(\sqrt{-N})$.

On en conclut que pour $N = 53$ (resp. 113, 137), $n(w) = 6$ (resp. $n(w) = 8$).

Considérons alors l'application f_1. Elle est de degré $4 = (f_1)_\infty$, et d'après l'interprétation de ce degré en termes de diviseurs l'application f_1 prend au plus en quatre points la même valeur. Puisqu'on a toujours $n(w) > 4$, c'est que f_1 prend effectivement les valeurs $+1$ et -1 en certains points fixes de w.

2) Le cas $N = 53$.

Soit donc, dans ce cas, $y \in X_o(N)$ fixe par w tel que $f_1(y) = 1$. On peut supposer que l'on a également $f_2(y) = 1$ (sinon on considère $-f_2$).

LEMME. - Il existe un automorphisme σ de $\mathbb{C}$ qui, agissant sur $X_o(N)$ permute circulairement les points fixes de w.

En effet, dans les cas envisagés le groupe des classes de $\mathbb{Q}(\sqrt{-N})$ est cyclique. Le lemme résulte alors des propriétés connues des courbes avec multiplication complexe et de l'interprétation en termes de telles courbes des points fixes de w.

Soit alors f_1^σ et f_2^σ les transformées de f_1 et f_2 par σ. Les diviseurs de f_1 et f_2 étant rationnels sur $\mathbb{Q}$, f_1^σ et f_2^σ sont nécessairement des multiples constants de f_1 et f_2. Mais aussi $f_1^\sigma(\sigma(y)) = \sigma(f_1(y)) = \sigma(1) = 1$. Or $\sigma(y)$ est aussi un point fixe de f_1. C'est donc que $f_1(\sigma(y)) = \pm 1$. Il en résulte aussitôt que $f_1^\sigma = \pm f_1$. Or, nous savons que f_1 prend effectivement la valeur -1, et aussi, en posant $f_1^\sigma = \varepsilon f_1$, $\varepsilon = \pm 1$, on a $f_1 \circ \sigma = 2f_1^\sigma \circ \sigma = \varepsilon . \sigma \circ f_1$ et par récurrence $f_1 \circ \sigma^\nu = \varepsilon^\nu \sigma^\nu \circ f_1$. D'où si $\varepsilon = +1$, tous les éléments fixes par w étant de la forme $\sigma^\nu(y)$, le fait que f_1 ne prendrait que la valeur 1. Donc $\varepsilon = -1$.

Par conséquent $f_1^\sigma = -f_1$, et alors par récurrence : $f_1(\sigma^m(y)) = (-1)^m$.

Nous énonçons :

LEMME. - Soit $y \in X_o(N)$ fixe par W tel que $y = 1$. Il existe un automorphisme σ de $\mathbb{C}$ permutant circulairement les points fixes de W qui est tel que $f_1(\sigma^m(y)) = (-1)^m$.

Le théorème en découle puisque le lemme prouve que $f_1 - 1$ s'annule en y , $\sigma^2(y)$ et $\sigma^4(y)$. En effet, σ étant un automorphisme, ces zéros doivent avoir le même ordre, mais on a vu que f_1 était de degré 4 , et donc prenait au plus 4 fois la même valeur. On en déduit que y , $\sigma^2(y)$ et $\sigma^4(y)$ ne peuvent être que des zéros simples de $f_1 - 1$, qui a nécessairement un autre zéro ξ . Ainsi :

$$(f_1 - 1)_o = y + \sigma^2(y) + \sigma^4(y) + \xi$$

ξ ne peut être fixe par W puisque les points fixes de W sont les $\sigma^\nu(y)$ et que si ν est impair $\sigma^\nu(y)$ n'annule pas $f_1 - 1$.

Mais si u est un zéro de $f_1 - 1$: $f_1(u) = 1$, $w(u)$ en est aussi un puisque $f_1(w(u)) = (f_1 \circ w)(u) = \frac{1}{f_1(u)} = 1$. Donc $(f_1 - 1)_o$ est fixe par w , ce qui implique que ξ est fixe par w . Contradiction.

On a prouvé :

THEOREME. - $Y_o(N)_{\mathbb{Q}} = \phi$ si $N = 53$.

3) Les cas $N = 113, 137$.

Nous distinguerons deux sous-cas.

a) $f_2(u) = 1$ quel que soit u fixe par w .

Alors la première partie du 2), qui reste valable sans changement, montre que l'on a $f_2^\sigma = f_2$ et que, par suite $f_2 - 1$ s'annule en tous les points fixes de w . Mais, également, on prouve que $(f_2 - 1)_o$ est fixe par w (en chaque point fixe de w , $f_2 - 1$ a un zéro simple).

D'autre part, on a le :

LEMME. -

i) il existe une forme différentielle $\neq 0$, ω , fixe par w , telle que la forme $\omega' = \frac{\omega}{f_2 - 1}$ n'ait pas de pôle en dehors des points fixes de w .

ii) Toute forme différentielle fixe par w doit s'annuler en chacun des points fixes de w .

Admettons pour l'instant le lemme. On peut alors construire la forme ω' , et il résulte de ii) et des propriétés des zéros de $f_2 - 1$ que ω' est une forme holomorphe.

Si v_∞ est la valuation à l'infini, on a ensuite :

$$v_\infty(f_2 - 1) \geq \mathrm{Inf}(v_\infty(f_2), v_\infty(1)) = -g$$

par construction même de f_2 . Donc $v_\infty(\frac{1}{f_2 - 1}) \geq g$. Puisque ω' est holomorphe, elle n'a pas de pôle, et on a ainsi prouvé : P_∞ est zéro de ω' d'ordre $\geq g$. En d'autres termes, P_∞ est point de Weierstrass de $X_o(N)$. Cela contredit le théorème de Atkin. Contradiction.

b) Cas où f_2 prend la valeur -1 en au moins un point fixe de α .

Par des méthodes analogues, on prouve ici que $f_2^\sigma = -f_2$, et donc que $f_2(\sigma^m(y)) = (-1)^m$ quel que soit m . On raisonne alors comme dans le cas a) en remplaçant f_2 par $f_1 f_2$.

Dans tous les cas, la contradiction est établie : $Y_o(N)_{\mathbb{Q}}$ ne peut avoir de point rationnel : $Y_o(N)_{\mathbb{Q}} = \emptyset$. Le théorème est démontré.

Il reste à prouver le lemme.

L'existence de ω résulte des observations suivantes :

- g^+ est la dimension de l'espace Ω^+ des différentielles fixes par w
- si $\omega \in \Omega^+$, (ω) est fixe par w
- $(f_2 - 1)_o$ est fixe par w , et des valeurs respectives de g , g^+ et $h = n(w)$ qui ont été rappelées au début.

BIBLIOGRAPHIE

[1] ATKIN - "Exposé au Congrès, Ann Arbor, 23-27 juin 1975".

[2] LIGOZAT - "Courbes modulaires de genre 1 ". Mémoire n° 43 S.M.F.

[3] MAZUR-SERRE - "Points rationnels des courbes modulaires $X_o(N)$ ". Séminaire Bourbaki, 1974-1975, n° 469.

[4] OGG - "Diophantine equations and Modular forms". Bull. A.M.S. 81, 1975, pp. 14-27.

[5] OGG - "Hyperelliptic Modular Curves". Bull. S.M.F. 102, 1974, pp. 449-462.

[6] PARRY - à paraître au Journal of Number Theory.

-:-:-:-

Laboratoire de Mathématiques Pures - Institut Fourier
dépendant de l'Université Scientifique et Médicale de Grenoble
associé au C.N.R.S.
B.P. 116
38402 ST MARTIN D'HERES (France)