ANNALES DE L'INSTITUT FOURIER

JEAN-FRANÇOIS MESTRE

Points rationnels de la courbe modulaire $X_0(169)$

Annales de l'institut Fourier, tome 30, n° 2 (1980), p. 17-27

<http://www.numdam.org/item?id=AIF_1980__30_2_17_0>

Ann. Inst. Fourier, Grenoble
30, 2 (1980), 17-27.

POINTS RATIONNELS DE LA COURBE MODULAIRE $X_0(169)$

par Jean-François MESTRE (*)

INTRODUCTION

Soit N un entier naturel. Le groupe

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) / c \equiv 0(N) \right\}$$

agit sur le demi-plan de Poincaré. Par passage au quotient, on obtient une courbe algébrique affine, définie sur $\mathbf{Q}$, que nous notons ici $Y_0(N)_{/\mathbf{Q}}$. Si K est un sous-corps de $\mathbf{C}$, de clôture algébrique $\bar{K}$, l'ensemble $Y_0(N)(K)$ des points de $Y_0(N)_{/\mathbf{Q}}$ à valeurs dans K est en bijection avec les classes d'isomorphisme (sur $\bar{K}$) des couples formés d'une courbe elliptique définie sur K et d'un sous-groupe cyclique d'ordre N du groupe de torsion de la courbe, stable sous l'action de $Gal(\bar{K}/K)$, cf. [2], VI, 3.2.

Dans [6], Mazur montre que, si N est premier et n'appartient pas à l'ensemble $\{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$, $Y_0(N)(\mathbf{Q})$ est vide, i.e. il n'existe pas de courbe elliptique définie sur $\mathbf{Q}$ possédant un groupe d'ordre N stable sous l'action de $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$, ou, si l'on préfère, il n'existe pas de N-isogénie, définie sur $\mathbf{Q}$, entre deux courbes elliptiques définies sur $\mathbf{Q}$.

Pour N quelconque, le problème de l'existence ou de la non-existence de telles N-isogénies, à noyau cyclique, définies sur $\mathbf{Q}$, serait complètement résolu si l'on montrait que $Y_0(N)(\mathbf{Q})$ est vide pour $N = 3.13, 5.13, 7.13, 13^2, 5^3$.

(*) Laboratoire Associé au C.N.R.S. n° 226.

Kenku a montré que $Y_0(N)(\mathbf{Q})$ est vide pour $N = 3.13, 5.13, 7.13$; ([4] et d'autres articles à paraître). Nous montrons ici le résultat suivant :

THÉORÈME. — $Y_0(13^2)(\mathbf{Q})$ *est vide.*

1. RAPPELS

1.1. Les pointes dans la théorie transcendante.

Soit $\bar{H}$ la réunion du demi-plan de Poincaré H et de la droite projective rationnelle $P^1(\mathbf{Q})$. L'action de $\Gamma_0(N)$ sur $\bar{H}$ permet d'obtenir, par passage au quotient, la courbe algébrique complète $X_0(N)_{/\mathbf{Q}}$, définie sur $\mathbf{Q}$. La courbe $Y_0(N)_{/\mathbf{Q}}$ est le complémentaire, dans $X_0(N)_{/\mathbf{Q}}$, d'un ensemble fini de points, rationnels sur le corps des racines N-ièmes de l'unité : les *pointes* de $X_0(N)_{/\mathbf{Q}}$. Les pointes sont en bijection avec les classes d'équivalence de $P^1(\mathbf{Q})$ modulo $\Gamma_0(N)$. Pour $N > 1$, $X_0(N)_{/\mathbf{Q}}$ a toujours au moins deux pointes distinctes, correspondant aux classes de (0) et (∞) ; ces deux pointes sont rationnelles sur $\mathbf{Q}$.

En particulier, si N est premier, ce sont les deux seules pointes de $X_0(N)_{/\mathbf{Q}}$; si $N = p^2$, p premier, on obtient $p - 1$ autres pointes P_i, $i = 1, \ldots, p - 1$, correspondant aux classes des rationnels $\frac{i}{p}$. Ces pointes sont rationnelles sur le corps des racines p-ièmes de l'unité, et sont conjuguées entre elles sous l'action de $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$.

D'autre part, si le genre de $X_0(N)_{/\mathbf{Q}}$ est strictement positif, considérons le morphisme f de $X_0(N)_{/\mathbf{Q}}$ dans sa jacobienne $J_0(N)_{/\mathbf{Q}}$ qui à un point x associe le diviseur $(x) - (\infty)$. D'après [5], le groupe engendré par l'image des pointes par f est un groupe fini. En particulier, si $N = p^2$, p premier, $f((0))$ est d'ordre $\frac{p^2 - 1}{24}$ ([7]).

LEMME 1.1. — *Supposons que* $X_0(p)_{/\mathbf{Q}}$, *avec p premier, soit de genre* 0, *et que* $X_0(p^2)_{/\mathbf{Q}}$ *soit de genre strictement positif; si f désigne le morphisme défini ci-dessus de* $X_0(p^2)_{/\mathbf{Q}}$ *dans sa jacobienne, et si* $P_1, \ldots, P_{p-1}$ *sont les pointes non rationnelles de* $X_0(p^2)_{/\mathbf{Q}}$, *on a :* $f(P_1) + \cdots + f(P_{p-1}) = f((0))$.

En effet, le revêtement de degré $p : X_0(p^2)_{/\mathbf{Q}} \to X_0(p)_{/\mathbf{Q}}$ est totalement ramifié en la pointe (0) de $X_0(p^2)_{/\mathbf{Q}}$, alors que la pointe (∞) et les pointes P_i

de $X_0(p^2)_{/\mathbf{Q}}$ s'envoient sur la pointe (∞) de $X_0(p)_{/\mathbf{Q}}$. Sur $X_0(p)_{/\mathbf{Q}}$, le diviseur $(0) - (\infty)$ est linéairement équivalent à 0; par suite, sur $X_0(p^2)_{/\mathbf{Q}}$, il en est de même du diviseur $(\infty) + (P_1) + \cdots + (P_{p-1}) - p(0)$, d'où le lemme.

1.2. Le schéma $X_0(N)_{/\mathbf{Z}}$ et l'interprétation modulaire des pointes.

1.2.1. — Soit $F_N(X, Y) \in \mathbf{Z}[X, Y]$ le polynôme modulaire ([2]); ce polynôme est irréductible et a la propriété suivante : soit E (resp. E') une courbe elliptique d'invariant j (resp. j'), définie sur un corps k de caractéristique ne divisant pas N. S'il existe une N-isogénie à noyau cyclique entre E et E', définie sur k, on a $F_N(j,j') = 0$.

Soit donc $Y_0(N)_{/\mathbf{Z}}$ le spectre du normalisé de $\mathbf{Z}[X,Y]/(F_N(X,Y))$. Alors, pour tout corps k de caractéristique ne divisant pas N, l'ensemble $Y_0(N)(k)$ des points de $Y_0(N)_{/\mathbf{Z}}$ à valeur dans k est en bijection avec les classes d'isomorphisme (sur $\bar{k}$) des courbes elliptiques définies sur k, munies d'un sous-groupe cyclique d'ordre N de leur groupe de torsion, stable sous l'action de $\mathrm{Gal}(\bar{k}/k)$ ($\bar{k}$ est ici la clôture algébrique de k).

Si k est un corps de caractéristique p divisant N, avec p^2 ne divisant pas N, $Y_0(N)(k)$ classifie des objets analogues. Par contre, dès que p^2 divise N, la situation est beaucoup plus complexe.

D'après [2], $Y_0(N)_{/\mathbf{Z}}$ se plonge dans un schéma $X_0(N)_{/\mathbf{Z}}$, défini sur $\mathbf{Z}$, propre et lisse sur $\mathrm{Spec}\left(\mathbf{Z}\left[\frac{1}{N}\right]\right)$. De même que

on a
$$Y_0(N)_{/\mathbf{Q}} = Y_0(N)_{/\mathbf{Z}} \times \mathrm{Spec}(\mathbf{Q}),$$
$$X_0(N)_{/\mathbf{Q}} = X_0(N)_{/\mathbf{Z}} \times \mathrm{Spec}(\mathbf{Q});$$

$Y_0(N)_{/\mathbf{Z}}$ est le complémentaire dans $X_0(N)_{/\mathbf{Z}}$ d'un ensemble fini de points à valeurs dans $\mathrm{Spec}(\mathbf{Z}[\zeta_N])$, les *pointes de* $X_0(N)_{/\mathbf{Z}}$.

Ces pointes se spécialisent en caractéristique 0 en les pointes définies en 1.1. En caractéristique p, p^2 ne divisant pas N, elles restent toutes distinctes entre elles. Ceci n'est plus vrai dès que p^2 divise N.

1.2.2. — Toujours d'après [2], on a une interprétation modulaire des pointes de $X_0(N)_{/k} = X_0(N)_{/\mathbf{Z}} \times \mathrm{Spec}\, k$ pour tout corps k dont le carré de la caractéristique ne divise pas N : les pointes classifient alors les polygones de Néron ([2], p. 31) sur $\bar{k}$ munis d'un sous-schéma en groupes cycliques d'ordre N, qui rencontre chaque composante irréductible du polygone.

En particulier, la pointe (∞) correspond au polygone à 1 côté (dont le lieu lisse est isomorphe à $\mathbf{G}_m$), muni de μ_N ; la pointe (0) correspond au polygone à N côtés (dont le lieu lisse est isomorphe à $\mathbf{G}_m \times \mathbf{Z}/N\mathbf{Z}$), muni du groupe $\{e\} \times \mathbf{Z}/N\mathbf{Z}$. Enfin, si $N = p^2$, p premier, les $p-1$ pointes qui se spécialisent en caractéristique nulle en les pointes P_i de 1.1 correspondent, en caractéristique différente de p, aux polygones à p côtés (dont le lieu lisse est $\mathbf{G}_m \times \mathbf{Z}/p\mathbf{Z}$), munis des groupes engendrés par (ζ_{p^2}, i), $i = 1, \ldots, p-1$, ζ_{p^2} racine p^2-ième de l'unité.

2. POINTS RATIONNELS DE $X_0(169)_{/\mathbf{Q}}$.

2.1. La paramétrisation de Fricke de $X_0(13)_{/\mathbf{Z}}$.

Fricke (F) donne l'équation non homogène suivante de $X_0(13)_{/\mathbf{Z}}$:

$$xx' = 13$$

– Le morphisme « oubli » de $X_0(13)_{/\mathbf{Z}}$ dans $\mathbf{P}^1$ (correspondant à l'application qui à tout couple (E,C) associe l'invariant modulaire j de E) est donné par :

$$j(x,x') = (x+5+x')(x^4+7x^3+20x^2+19x+1)^3$$

– L'involution d'Atkin-Lehner w_{13} de $X_0(13)_{/\mathbf{Z}}$ est donnée par :

$$w_{13}(x,x') = (x',x)$$

– La section (∞) (resp. (0)) correspond au point $(0,\infty)$ (resp. $(\infty,0)$).

Pour le voir, on remarque que le morphisme d'oubli j est non ramifié (resp. totalement ramifié) le long de la section (∞) (resp. (0)) ; la formule explicite de Fricke citée plus haut permet de conclure.

– Modulo 13, on retrouve les résultats classiques concernant la réduction de $X_0(p)_{/\mathbf{Z}}$ modulo p : la courbe $X_0(13)_{/\mathbf{F}_{13}}$ a deux composantes irréductibles de multiplicité 1, isomorphes à $\mathbf{P}^1$, se coupant transversalement en le point supersingulier. Sur $\mathbf{F}_{13}$, j est donné par la formule :

$$j(x,x') = x^{13} + x' + 5$$

– La seule courbe supersingulière en caractéristique 13 est la courbe d'invariant $j = 5$. Par suite, $X_0(13)_{/\mathbf{Z}}$ est le modèle minimal de $X_0(13)_{/\mathbf{Q}}$,

d'après la théorie générale ([2], p. 148). C'est d'ailleurs clair sur l'équation $xx' = 13$: l'idéal $(x,x',13)$ est égal à l'idéal (x,x'), et l'anneau local correspondant est donc régulier.

LEMME 2.1. — *Soit* E *une courbe elliptique définie sur* $\mathbf{Q}$, *munie d'un groupe cyclique* C *d'ordre* 13, *stable par* $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$; *le couple* (E,C) *correspond à un point* (x,x') *de* $Y_0(13)_{/\mathbf{Q}}$. *Soit* p *un nombre premier,* v_p *la valuation associée.*

i) E *a bonne réduction potentielle en* p *si et seulement si :*

— $v_p(x) = 0$ *si* $p \neq 13$.

— $v_p(x) = 0$ *ou* 1 *si* $p = 13$.

ii) (E,C) *se réduit modulo* p *sur la pointe* (∞) *si et seulement si* $v_p(x') < 0$.

iii) (E,C) *se réduit modulo* p *sur la pointe* (0) *si et seulement si* $v_p(x) < 0$.

C'est clair sur l'équation $xx' = 13$, les pointes (∞) et (0) étant déterminées par les points $(0,\infty)$ et $(\infty,0)$.

2.2. La courbe $X_0(169)_{/\mathbf{Q}}$ et son modèle minimal $X'_0(169)_{/\mathbf{Z}}$.

Soit k un corps de caractéristique différente de 13 ; $X_0(13)_{/k}$ est alors isomorphe à $\mathbf{P}^1_{/k}$, et le morphisme d'oubli $j : \mathbf{P}^1 \to \mathbf{P}^1$ s'écrit :

$$x \longmapsto j(x) = \frac{(x^2+5x+13)\,(X^4+7x^3+20x^2+19x+1)^3}{x}.$$

C'est d'ailleurs l'équation que donne Fricke dans [3], mais elle ne convient pas en caractéristique 13.

Soit à présent (E,C) un couple formé d'une courbe elliptique E, définie sur k, munie d'un groupe cyclique C d'ordre 169, stable par $\mathrm{Gal}(\bar{k}/k)$. On peut associer à (E,C) un triplet (E_1,C_1,C'_1) formé d'une courbe elliptique E_1 définie sur k, munie de deux sous-groupes cycliques C_1 et C'_1 d'ordre 13, stables par $\mathrm{Gal}(\bar{k}/k)$: (E_1,C_1) est le transformé de (E,13C) par l'involution d'Atkin-Lehner w_{13} ; C'_1 est l'image de C par l'isogénie correspondante de E dans E_1. Si (E',C') est le transformé de (E,C) par l'involution d'Atkin-Lehner w_{169}, (E_1,C'_1) est aussi le transformé de (E',13C') par l'involution w_{13}.

Par suite, à (E,C) correspond un couple de points (x,y) tels que x (resp. y) corresponde à (E_1,C_1) (resp. (E_1,C_1')); on a évidemment $j(x) = j(y)$, et l'équation (1) : $\dfrac{j(x) - j(y)}{x - y} = 0$ donne une courbe $X_0''(169)_{/k}$ birationnellement équivalente à $X_0(169)_{/k}$, de normalisée $X_0(169)_{/k}$, et qui est la spécialisation sur k d'un schéma $X_0''(169)_{/\mathbf{Z}}$, d'équation non homogène l'équation (1).

L'équation (1), rendue homogène par le changement de variables $x = \dfrac{X}{T}$, $y = \dfrac{Y}{T}$, devient :

$$(1')\quad XY\left(\frac{X^{13} - Y^{13}}{X - Y}\right) + 13(TQ_{13}(X,Y) + T^2Q_{12}(X,Y) + \cdots - T^{12}XY - T^{14}) = 0,$$

où les Q_i sont des polynômes homogènes de degré i de $\mathbf{Z}[X,Y]$. Les points à l'infini de $X_0''(169)_{/\mathbf{Z}}$ sont donc les points $(\infty)''_{/\mathbf{Z}} = (1,0,0)$, $(0)''_{/\mathbf{Z}} = (0,1,0)$ et $(P_i)''_{/\mathbf{Z}} = (1,\zeta_{13}^i,0)$, $i = 1, \ldots, p-1$.

– En caractéristique 13, l'équation de $X_0''(169)_{/\mathbf{F}_{13}}$ est :

$$XY(X-Y)^{12} = 0.$$

Par suite, les points $(\infty)''_{/\mathbf{F}_{13}}$ et $(0)''_{/\mathbf{F}_{13}}$ sont dans le lieu lisse de $X_0''(169)_{/\mathbf{F}_{13}}$. En fait, le lemme suivant est clair, d'après (1') :

LEMME 2.2.1. – *Les sections* $(\infty)''_{/\mathbf{Z}}$ *et* $(0)''_{/\mathbf{Z}}$ *s'envoient dans* $X_0''(169)^{\text{lisse}}{}_{/\mathbf{Z}}$, *le lieu lisse de* $X_0''(169)_{/\mathbf{Z}}$. *Soit* $S' = \operatorname{Spec}\left(\mathbf{Z}\left[\dfrac{1}{13}\right]\right)$; *les spécialisations des* $(P_i)_{/\mathbf{Z}}$ *à* S' *sont des points de* $X_0''(169)^{\text{lisse}}{}_{/S'}$ *à valeurs dans* $\mathbf{Z}\left[\zeta_{13}, \dfrac{1}{13}\right]$.

– Soit à présent $X_0'(169)_{/\mathbf{Z}}$ le modèle minimal de $X_0(169)_{/\mathbf{Q}}$. Soit $(\infty)'_{/\mathbf{Z}}$ (resp. $(0)'_{/\mathbf{Z}}$) le prolongement à $X_0'{}^{\text{lisse}}(169)_{/\mathbf{Z}}$ de la pointe (∞) (resp. (0)) de $X_0(169)_{/\mathbf{Q}}$; de même, soient $(P_i)_{/S'}$ les prolongements à $X_0'{}^{\text{lisse}}(169)_{/S'} = X_0'(169)/S' = X_0(169)_{/S'}$ des pointes (P_i) de $X_0(169)_{/\mathbf{Q}}$.

– Soit E une courbe elliptique définie sur $\mathbf{Q}$, munie d'un groupe cyclique C d'ordre 169, stable par $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$; le couple (E,C) correspond sur $X_0''(169)_{/\mathbf{Z}}$ à un point $(x,y) = z''$ de $\mathbf{Q}^2$; d'autre part, il correspond à un

point $z_{/\mathbf{Q}}$ de $X_0(169)_{/\mathbf{Q}}$ qui se prolonge en un point $z'_{/\mathbf{Z}}$ de $X_0'^{\text{lisse}}(169)_{/\mathbf{Z}}$. D'après le lemme 2.2.1, l'assertion suivante est vraie :

LEMME 2.2.2. — *Soit p un nombre premier.*

i) $z''_{/\mathbf{F}_p} = (\infty)''_{/\mathbf{F}_p}$ (resp. $(0)''_{/\mathbf{F}_p}$) $\Leftrightarrow z'_{/\mathbf{F}_p} = (\infty)'_{/\mathbf{F}_p}$ (resp. $(0)'_{/\mathbf{F}_p}$).

ii) *Soit p premier différent de* 13.

$$z''/\mathbf{F}_p = (P_i)''_{/\mathbf{F}_p} \Leftrightarrow z'_{/\mathbf{F}_p} = (P_i)'_{/\mathbf{F}_p}.$$

Montrons à présent qu'il n'est pas possible que $z''_{/\mathbf{F}_{13}} = (P_i)''_{/\mathbf{F}_{13}}$, i.e. que l'on ait $v_{13}(x) < 0$ et $v_{13}(y) < 0$.

En effet, dans ce cas, l'invariant modulaire de E n'est pas entier en 13 : par suite, en reprenant les notations du début de 2.2, la courbe E_1, après torsion éventuelle par un ou deux corps quadratiques, est isomorphe sur $\mathbf{Q}_{13}$ à sa courbe de Tate $\mathbf{G}_m/q^{\mathbf{Z}}$; le groupe des points d'ordre 13 de E_1 est alors isomorphe au groupe engendré par ζ_{13} et $q^{1/13}$. L'hypothèse $z''_{/\mathbf{F}_{13}} = (P_i)''_{/\mathbf{F}_{13}}$ équivaut à dire que (E_1,C_1) et (E_1,C_1') se réduisent modulo 13 sur la pointe (0), i.e. qu'il existe i, i' distincts et non nuls modulo 13 tels que (E_1,C_1) (resp. (E_1,C_1')) soit isomorphe à $\zeta_{13}q^{i/13}$ (resp. $\zeta_{13}q^{i/13}$). Il est clair que deux tels groupes ne peuvent être simultanément stables par $\mathrm{Gal}(\bar{\mathbf{Q}}_{13}/\mathbf{Q}_{13})$.

Remarque. — On peut démontrer ce résultat à partir de l'équation (1) :

$$xy(x^{12}+x^{11}y+\cdots+y^{12}) + 13(Q_{13}(x,y)+\cdots-1) = 0.$$

En effet, l'hypothèse faite sur (E,C) équivaut à $v_{13}(x) = v_{13}(y) = -k$, avec $k > 0$. Posons $u = \dfrac{y}{x}$. L'équation devient :

$$ux^{14}(1+u+\cdots+u^{12}) = -13(x^{13}q_{12}(u)+\cdots-1),$$

les q_i étant des polynômes en u de degré i. La valuation du membre de droite est supérieure ou égale à $-13k+1$, alors que celle du membre de gauche est égale à $-14k + v_{13}(1+u+\cdots+u^{12})$, d'où une impossibilité en vertu du lemme suivant :

LEMME 2.2.3. — *Soit $u \in \mathbf{Z}_p$, p premier $\neq 2$; la valuation de $1+u+\cdots+u^{p-1}$ est égale à 0 ou 1.*

Il est clair que, si cette valuation n'est pas nulle, on a $u \equiv 1(p)$. Or, si $u = 1 + vp$, $v \in \mathbf{Z}_p$, la somme

$$1 + u + \cdots + u^{p-1} = (1+pv)^{p-1} + \cdots + (1+pv) + 1$$

est congrue à $p \bmod p^2$.

Les résultats précédents entraînent le lemme suivant :

LEMME 2.2.4. — *Soit* E *une courbe elliptique définie sur* $\mathbf{Q}$, *munie d'un groupe cyclique* C *d'ordre* 169 *stable par* $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$; (E,C) *correspond à un point* $z'_{/\mathbf{Z}}$ (*resp.* $z''_{/\mathbf{Z}} = (x,y)$, x *et* y *dans* $\mathbf{Q}$) *de* $X'_0(169)_{/\mathbf{Z}}$ (*resp.* $X''_0(169)_{/\mathbf{Z}}$). *Soit* p *un nombre premier.*

i) E *a bonne réduction potentielle en* $p \Leftrightarrow \begin{cases} v_p(x) = 0 \text{ si } p \neq 13 \\ v_p(x) = 0 \text{ ou } 1 \text{ si } p = 13. \end{cases}$

ii) $z'_{/\mathbf{F}_p} = (\infty)'_{/\mathbf{F}_p}$ (*resp.* $(0)'_{/\mathbf{F}_p} \Leftrightarrow v_p(x) < 0$ *et*

$$v_p(y) > 0 \text{ (resp. } v_p(y) < 0 \text{ et } v_p(x) > 0).$$

Dans ce cas, si $v_p(x)$ (*resp.* $v_p(y)$) $= -k$, $k > 0$, *on a*

$$v_p(y) \text{ (resp. } v_p(x)) = 13k + m_p,$$

avec $m_p = 1$ *si* $p = 13$ *et* 0 *sinon.*

iii) $\begin{cases} z'_{/\mathbf{F}_p} = (\mathrm{P}_i)'_{/\mathbf{F}_p} \Leftrightarrow v_p(x) < 0 \text{ et } v_p(y) < 0 \\ p \neq 13. \end{cases}$

Dans ce cas,

$$v_p(x) = v_p(y) = -k, \qquad k > 0.$$

Admettons provisoirement le résultat suivant, qui sera démontré plus loin (§ 3) :

LEMME 3. — *On conserve les notations du lemme* 2.2.4.

Supposons qu'il existe un nombre premier p *tel que* $z'_{/\mathbf{F}_p} = (\infty)'_{/\mathbf{F}_p}$ (*resp.* $(0)'_{/\mathbf{F}_p}$, *resp.* $(\mathrm{P}_i)'_{/\mathbf{F}_p}$). *Alors, pour tout* ℓ *premier tel que* E *n'ait pas bonne réduction potentielle en* ℓ, *on a* $z'_{/\mathbf{F}_\ell} = (\infty)'_{/\mathbf{F}_\ell}$ (*resp.* $(0)'_{/\mathbf{F}_\ell}$, *resp.* $(\mathrm{P}_i)'_{/\mathbf{F}_\ell}$).

On peut alors aborder la démonstration du théorème. Supposons d'abord que la courbe E ait bonne réduction potentielle partout. Dans ce cas, le couple (x,y) est tel que $x = \pm 1$ ou ± 13, $y = \pm 1$ ou ± 13. En reportant dans l'équation (1), on voit que l'on n'obtient pas de solution.

Supposons donc qu'il existe p premier tel que E a une réduction potentiellement multiplicative en p. Trois cas peuvent se présenter :

i) $v_p(x) = -k_p$, $v_p(y) = 13k_p + m_p$. Alors $z'_{/\mathbf{F}_p} = (\infty)'_{/\mathbf{F}_p}$ d'après le lemme 2.2.4, et, si ℓ est un nombre premier distinct de 13, $v_\ell(x) = -k_\ell$, $v_\ell(y) = 13k_\ell$, avec $k_\ell = 0$ si E a bonne réduction potentielle en ℓ; pour $\ell = 13$, $v_{13}(x) = 0$ ou 1 et $v_{13}(y) = 0$ ou 1 si E a bonne réduction

potentielle en 13 ; sinon,

$$v_{13}(x) = -k_{13}, \qquad v_{13}(y) = 13k_{13} + 1.$$

Par suite, il existe un entier n tel que le couple (x,y) est de l'un des types suivants :

$$\left(\pm\frac{1}{n}, \pm n^{13}\right), \qquad \left(\pm\frac{1}{n}, \pm 13n^{13}\right),$$
$$\left(\pm\frac{13}{n}, \pm n^{13}\right), \qquad \left(\pm\frac{13}{n}, \pm 13n^{13}\right).$$

A vrai dire, le dernier couple est à rejeter immédiatement : il est clair sur l'équation (1) que x et y ne peuvent avoir simultanément une valuation en 13 strictement positive. Les autres couples sont plus délicats à éliminer : il faut montrer que l'équation en n obtenue en remplaçant x et y par leur valeur en fonction de n dans l'équation (1) n'a pas de solution entière. C'est une vérification un peu pénible, mais sans difficulté.

ii) $z'_{/\mathbf{F}_p} = (0)'_{/\mathbf{F}_p}$. On se ramène au cas précédent en faisant agir l'involution d'Atkin-Lehner w_{169} sur (E,C).

iii) $v_p(x) = -k_p$, $v_p(y) = -k_p$. Par un raisonnement analogue à i), on voit que (x,y) est de l'un des types suivants :

$$\left(\pm\frac{1}{n}, \pm\frac{1}{n}\right), \qquad \left(\pm\frac{1}{n}, \pm\frac{13}{n}\right).$$

On obtient à nouveau des équations polynomiales à une inconnue en remplaçant x et y par leur valeur en fonction de n dans l'équation (1), et on vérifie qu'elles n'ont pas de solution dans $\mathbf{Z}$. D'où le théorème.

3. DÉMONSTRATION DU LEMME 3

Soit f le morphisme de $X_0(169)_{/\mathbf{Q}}$ dans sa jacobienne $J_0(169)_{/\mathbf{Q}}$ défini en 1.1. Berkovič ([1]) a montré l'existence d'un quotient $\mathrm{Eis}_{/\mathbf{Q}}$ de $J_0(169)_{/\mathbf{Q}}$, dit quotient d'Eisenstein de $J_0(169)_{/\mathbf{Q}}$, et qui possède les deux propriétés suivantes :

i) $\mathrm{Eis}_{/\mathbf{Q}(\mathbf{Q})}$ est fini.

ii) Si h désigne le morphisme composé de f et de la projection de $J_0(169)_{/\mathbf{Q}}$ sur $\mathrm{Eis}_{/\mathbf{Q}}$, l'image de la pointe (0) par h est non triviale.

Or ((1.1)), $f((0))$ est d'ordre $\dfrac{169-1}{24} = 7$, donc $h((0))$ est aussi d'ordre 7.

D'autre part, d'après le lemme 1.1, $f(P_1) + \cdots + f(P_{12}) = f((0))$. Donc

$$h(P_1) + \cdots + h(P_{12}) = h((0));$$

les points P_i étant tous conjugués entre eux par $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, les points $f(P_i)$, et donc $h(P_i)$ ont tous le même ordre, qui n'est donc pas premier à 7.

Soit $J_0(169)_{/\mathbf{Z}}$ (resp. $\mathrm{Eis}_{/\mathbf{Z}}$) le modèle de Néron, sur $\mathbf{Z}$, de $J_0(169)_{/\mathbf{Q}}$ (resp. $\mathrm{Eis}_{/\mathbf{Q}}$). On sait que $X_0'(169)^{\mathrm{lisse}}{}_{/\mathbf{Z}}$ s'envoie dans $J_0(169)_{/\mathbf{Z}}$ par une application qui prolonge f; si h désigne le morphisme de $X_0'(169)^{\mathrm{lisse}}{}_{/\mathbf{Z}}$ dans $\mathrm{Eis}_{/\mathbf{Z}}$ qui prolonge h, il est clair d'après Oort-Tate ([8]) que la spécialisation en tout p (y compris $p = 7$) de $h((0)'_{/\mathbf{Z}})$ donne un point d'ordre 7 de $\mathrm{Eis}(\mathbf{F}_p)$.

De même, soit $S' = \mathrm{Spec}\,\mathbf{Z}\left[\dfrac{1}{13}\right]$. Les points (P_i) de $X_0(169)_{/\mathbf{Q}}$, à valeurs dans $\mathbf{Q}(\zeta_{13})$, se prolongent en des points $(P_i)'_{/S'}$ de $X_0'(169)^{\mathrm{lisse}}{}_{/S'}$ à valeurs dans $\mathbf{Z}\left[\zeta_{13}, \dfrac{1}{13}\right]$. Toujours d'après Oort-Tate, la spécialisation en tout $p \neq 13$ de $h_{/S'}((P_i)'_{/S'})$ est d'ordre divisible par 7, pour tout i de $\{1, \ldots, 12\}$.

Soit maintenant un couple (E,C) formé d'une courbe elliptique définie sur $\mathbf{Q}$ et d'un groupe cyclique C d'ordre 169 stable par $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Soit $z'_{/\mathbf{Z}}$ le point correspondant de $X_0'(169)^{\mathrm{lisse}}{}_{/\mathbf{Z}}$. Supposons qu'il existe p, tel que $z'_{/\mathbf{F}_p} = (\infty)'_{/\mathbf{F}_p}$. Alors $h(z')_{/\mathbf{F}_p} = 0$; donc, toujours d'après Oort-Tate, le point $h(z')_{/\mathbf{Q}}$ est d'ordre premier à 7, et ne peut donc s'envoyer, pour $\ell \neq p$, sur $h((0)')_{/\mathbf{F}_\ell}$ ou sur $h((P_i)')_{/\mathbf{F}_\ell}$. Par suite, si E n'a pas bonne réduction potentielle en ℓ, on a : $z'_{/\mathbf{F}_\ell} = (\infty)'_{/\mathbf{F}_\ell}$.

Le cas où $z'_{/\mathbf{F}_p} = (0)'_{/\mathbf{F}_p}$ se ramène au précédent en faisant agir l'involution w_{169} sur z'. Le cas où $z'_{/\mathbf{F}_p} = (P_i)'_{/\mathbf{F}_p}$ se résoud en raisonnant par l'absurde, à partir des deux cas précédents, d'où le lemme.

BIBLIOGRAPHIE

[1] V. G. Berkovič, The rational points on the Jacobian of modular curves, *Mat. Sbornik*, 101 (143) (1976); traduction anglaise, *Math. U.S.S.R. Sbornik*, 30, 4 (1976), 478-500.

[2] P. DELIGNE, M. RAPOPORT, Schémas de modules des courbes elliptiques, vol. II of the Proceedings of the International Summer School on modular functions, Antwerp (1972), *Lecture Notes in Mathematics* 349, Berlin-Heidelberg-New York, Springer, 1973.
[3] R. FRICKE, Die elliptischen Funktionen und ihre Anwendungen, II, Leipzig-Berlin, Teubner, 1922.
[4] M. A. KENKU, The modular curve $X_0(39)$ and rational isogeny, *Math. Proc. Cambridge Philo. Soc.*, 85, (1979), 21-23.
[5] Y. MANIN, Parabolic points and zeta functions of modular forms (Russian), *Isv. Acad. Nauk.*, (1972), 19-66.
[6] B. MAZUR, Rational isogenies of prime degree, *Inventiones Mathematicae*, 44 (1978), 129-163.
[7] A. OGG, Rational points on certain elliptic modular curves, *Proc. Symp. Pure Math.*, A.M.S., Providence, 24 (1973), 221-231.
[8] F. OORT, J. TATE, Group schemes of prime order, *Ann. Scient. Ec. Norm. Sup.*, série 4,3 (1970), 1-21.

Manuscrit reçu le 14 octobre 1979.

Jean-François MESTRE,
Laboratoire de Mathématiques
351, cours de la Libération
33405 Talence Cedex (France).