MÉMOIRES DE LA S. M. F.

JACQUES VÉLU

Les points rationnels de $X_0(37)$

Mémoires de la S. M. F., tome 37 (1974), p. 169-179

<http://www.numdam.org/item?id=MSMF_1974__37__169_0>

© Mémoires de la S. M. F., 1974, tous droits réservés.

L'accès aux archives de la revue « Mémoires de la S. M. F. » (http://smf.emath.fr/Publications/Memoires/Presentation.html) 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/

Journées arithmétiques [1973, Grenoble]
Bull. Soc. math. France
Mémoire 37, 1974, p. 169-179

LES POINTS RATIONNELS DE $X_0(37)$

par

Jacques VELU

-:-:-:-

Table des matières

§1 - Courbes elliptiques et isogénies

Courbes elliptiques sur $\mathbb{C}$.

Par définition, une courbe elliptique E sur $\mathbb{C}$ est une variété abélienne de dimension 1 , ou, ce qui est équivalent, une courbe complète non singulière connexe de genre 1 munie d'une origine, ou encore un groupe de Lie complexe, compact, connexe, de dimension 1. L'espace tangent $T(E)$ est un espace vectoriel de dimension 1 sur $\mathbb{C}$. On a la suite exacte

$$0 \longrightarrow \Lambda \longrightarrow T(E) \xrightarrow{\exp} E(\mathbb{C}) \longrightarrow 0$$

Λ étant un sous-groupe discret de $T(E)$, noyau de l'exponentielle. Le choix d'une base de $T(E)$, ou, ce qui revient au même, le choix d'une différentielle holomorphe $\omega \neq 0$ sur E permet d'identifier $T(E)$ à $\mathbb{C}$ et Λ à un réseau de $\mathbb{C}$. On définit ainsi une bijection entre l'ensemble des couples (E,ω) et l'ensemble des réseaux de $\mathbb{C}$, et une bijection entre l'ensemble des courbes elliptiques sur $\mathbb{C}$ et l'ensemble des classes à homothétie près de réseaux de $\mathbb{C}$. Or ce dernier ensemble est en bijection avec $\mathfrak{H}/\Gamma$, quotient du demi-plan de Poincaré $\mathfrak{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$ par le groupe $\Gamma = SL(2,\mathbb{Z})$, au moyen de l'application qui associe à $\tau \in \mathfrak{H}$ le réseau de base $(1,\tau)$. La variété analytique complexe $\mathfrak{H}/\Gamma$ est isomorphe à $\mathbb{C}$, son complété $\overline{\mathfrak{H}/\Gamma} = \mathfrak{H}/\Gamma \cup \{\infty\}$ à $\mathbb{P}_1(\mathbb{C})$ et le corps des fonctions méromorphes sur $\overline{\mathfrak{H}/\Gamma}$ est $\mathbb{C}(j)$, où j

est l'"invariant modulaire", fonction définie de façon unique par les trois conditions :

(i) j a un seul pôle, en $\{\infty\}$, et ce pôle est simple ;

(ii) $j(e^{2\pi i/3}) = 0$;

(iii) $j(i) = 1728 = 2^6.3^3$.

On a donc :

THEOREME 1. - Une courbe elliptique sur $\mathbb{C}$ est déterminée à isomorphisme près par son invariant modulaire.

Si E est définie sur un sous-corps K de $\mathbb{C}$, on sait qu'elle peut être plongée comme cubique non singulière dans $\mathbb{P}_2(K)$ avec une équation de la forme $y^2 = x^3 - \frac{C_4}{48}x + \frac{C_6}{864}$, où $C_4^3 - C_6^2 \neq 0$, et que l'invariant modulaire de E est $j = \frac{1728C_4^3}{C_4^3 - C_6^2}$. Un K-isomorphisme entre deux telles courbes E et E' est de la forme $x' = \lambda^2 x$, $y' = \lambda^3 y$ où $\lambda \in K - \{0\}$, et on a $C'_4 = \lambda^4 C_4$ et $C'_6 = \lambda^6 C_6$. En particulier :

THEOREME 2. - Soit E une courbe elliptique définie sur $\mathbb{C}$, d'invariant j ; alors :

i) $\mathrm{Aut}_{\mathbb{C}}(E) \simeq \mu_4$ si $j = 1728$;

ii) $\mathrm{Aut}_{\mathbb{C}}(E) \simeq \mu_6$ si $j = 0$;

iii) $\mathrm{Aut}_{\mathbb{C}}(E) \simeq \mu_2$ si $j \neq 0$, 1728

(μ_n désigne le groupe des racines $n^{\text{ièmes}}$ de 1) .

THEOREME 3. -

1) Si E est une courbe elliptique définie sur K , son invariant appartient à K .

2) Soit $j \in K$; l'ensemble des courbes elliptiques à K-isomorphisme près, définies sur K , d'invariant j est en bijection avec :

a) $K^\times/K^{\times 4}$ si $j = 1728$;

b) $K^\times/K^{\times 6}$ si $j = 0$;

c) $K^\times/K^{\times 2}$ si $j \neq 0$, 1728 .

N-isogénies.

Soient E une courbe elliptique, C un sous-groupe cyclique d'ordre N de E. Par définition, l'homomorphisme $\varphi : E \to E' = E/C$ est une isogénie de degré N. (Nous nous restreignons aux isogénies à noyau cyclique). Les espaces $T(E)$ et $T(E')$ s'identifient par $T(\varphi)$ et on a $\Lambda' \supset \Lambda$ et $\Lambda'/\Lambda \simeq \mathbb{Z}/N\mathbb{Z}$. De plus, le choix d'une base de $T(E)$ permet d'identifier $T(E)$ à $\mathbb{C}$, Λ et Λ' à deux réseaux de $\mathbb{C}$. Il y a donc bijection entre les couples (E,C) et les classes à homothétie près de couples de réseaux (Λ,Λ') tels que $\Lambda' \supset \Lambda$ et $\Lambda'/\Lambda \simeq \mathbb{Z}/N\mathbb{Z}$. Or on vérifie que cet ensemble est lui-même en bijection avec $\mathfrak{H}/\Gamma_o(N)$, quotient du demi-plan de Poincaré par le groupe

$$\Gamma_o(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c \equiv 0 \ (N)\}$$

au moyen de l'application qui associe à $\tau \in \mathfrak{H}$ les couples de réseaux de base $(1,N\tau)$ et $(1,\tau)$. Ceci nous permet d'énoncer :

THEOREME 4. - *Les couples (E,C) formés d'une courbe elliptique et d'un sous-groupe cyclique d'ordre N de E sont en bijection avec $\mathfrak{H}/\Gamma_o(N)$.*

COROLLAIRE. - *Soient E et E' des courbes elliptiques sur $\mathbb{C}$ d'invariants modulaires j et j'. Pour qu'il existe une isogénie $\varphi : E \to E'$, définie sur $\mathbb{C}$, à noyau cyclique d'ordre N, il faut et il suffit qu'il existe $\tau \in \mathfrak{H}$ tel que $j = j(\tau)$ et $j' = j(N\tau)$.*

La courbe $X_o(N)$

L'ensemble $\mathfrak{H}/\Gamma_o(N)$ n'est pas compact, son compactifié $\overline{\mathfrak{H}/\Gamma_o(N)}$ est obtenu en lui ajoutant l'ensemble fini $\mathbb{P}_1(\mathbb{Q})/\Gamma_o(N)$ des "pointes"; et le corps des fonctions méromorphes sur $\overline{\mathfrak{H}/\Gamma_o(N)}$ est $\mathbb{C}(j,j_N)$ où j_N est la fonction $\tau \mapsto j(N\tau)$. On démontre ([11]) :

THEOREME 5. - *Il existe un polynôme irréductible $F_N \in \mathbb{Z}[X,Y]$ tel que $F_N(j,j_N) = 0$.*

Il en résulte qu'il existe une courbe algébrique projective non singulière notée $X_o(N)$, définie sur $\mathbb{Q}$, dont le corps des fonctions est $\mathbb{Q}(j,j_N)$, et

telle que les variétés analytiques complexes $\overline{\mathcal{H}/\Gamma_o(N)}$ et $X_o(N)(\mathbb{C})$ soient isomorphes. Un modèle plan (à singularités) de cette courbe est donné par l'équation $F_N(X,Y) = 0$.

Rationalité.

On démontre (*) :

THEOREME 6. - Soit K un sous-corps de $\mathbb{C}$. Si (E,C) est défini sur K ; le point correspondant de $X_o(N)$ est rationnel sur K ; inversement, tout point de $X_o(N)$ rationnel sur K , qui n'est pas une pointe est obtenu ainsi.

((E,C) est défini sur K signifie que E est définie sur K et que C est stable par $Gal(\overline{K}/K)$).

Propriétés de la courbe $X_o(N)$.

On a de nombreux renseignements sur $X_o(N)$ ([3]) . Ainsi, on connaît son genre, on sait que les pointes $\{\infty\}$ et $\{0\}$ sont rationnelles sur $\mathbb{Q}$, que le diviseur $\{\infty\}-\{0\}$ est d'ordre fini sur la jacobienne de $X_o(N)$, et on peut calculer son ordre. De plus, $\overline{\mathcal{H}/\Gamma_o(N)}$ possède l'involution W_N déduite de l'involution $\tau \mapsto -\frac{1}{N\tau}$ dans $\mathcal{H}$. Cette involution agit sur le corps des fonctions par $(j,j_N) \xleftrightarrow{W_N} (j_N,j)$ elle est donc rationnelle sur $\mathbb{Q}$. Sur $X_o(N)$, elle s'interprète de la façon suivante : (E,C) étant un point de $X_o(n)$ $E_n \supset C$ étant le sous-groupe des points d'ordre N de E , on a :

$$(E,C) \xleftrightarrow{W_N} (E/C, E_N/C) \quad .$$

§2 - Résultats numériques

Le genre de $X_o(N)$ est

0 pour $N = 2,3,4,5,6,7,8,9,10\ 12\ 13\ 16,18,25$;

1 pour $N = 11\ 14\ 15,17,19,20\ 21,24,27,32,36,49$;

2 pour $N = 22\ 23\ 26\ 28,29,31,37,50$.

(*) A l'heure actuelle, il est pratiquement impossible de trouver dans la littérature une démonstration de ce théorème non trivial.

On connaît les expressions de F_1 , F_2 , $F_3^{(3,10)}$ qui sont :

$$F_1(X,Y) = X - Y$$

$$F_2(X,Y) = X^3 + Y^3 - X^2Y^2 + 2^4\cdot 3\cdot 31XY(X+Y) - 2^4\cdot 3^4\cdot 5^3(X^2+Y^2) + 3^4\cdot 5^3\cdot 4027XY + 2^8\cdot 3^7\cdot 5^6(X+Y) - 2^{12}\cdot 3^9\cdot 5^9$$

$$F_3(X,Y) = X(X+2^{15}\cdot 3\cdot 5^3)^3 + Y(Y+2^{15}\cdot 3\cdot 5^3)^3 - X^3Y^3 + 2^3\cdot 3^2\cdot 31X^2Y^2(X+Y) - 2^2\cdot 3^3\cdot 9907XY(X^2+Y^2) + 2\cdot 3^4\cdot 13\cdot 193\cdot 6367X^2Y^2 + 2^{16}\cdot 3^5\cdot 5^3\cdot 17.263XY(X+Y) - 2^{31}\cdot 5^6\cdot 22973XY \quad .$$

La complication de ces expressions explique qu'on ne connaît pas F_N pour d'autres valeurs de N . On sait pourtant ([11]) que pour N premier on peut écrire F_N sous la forme :

$$F_N(X,Y) = (X^N-Y)(Y^N-X) - N \sum_{\substack{0\le h\le N \\ 0\le k\le N}} a_{h,k}X^hY^k$$

où les $a_{h,k} \in \mathbb{Z}$, $a_{h,k} = a_{k,h}$ et $a_{N,N} = 0$.

Klein et Fricke ([3]) ont donné d'autres modèles plans des courbes $X_o(N)$ pour les petites valeurs de N ; ce sont ces équations plus simples qu'on utilise pour rechercher leurs points rationnels sur $\mathbb{Q}$. On obtient les résultats suivants :

a) Lorsque la courbe $X_o(N)$ est de genre 0 , l'ensemble de ses points rationnels sur $\mathbb{Q}$ est infini, ce qui provient du fait que cet ensemble n'est pas vide, puisqu'il contient la pointe $\{\infty\}$.

b) Les courbes $X_o(N)$ de genre 1 , ont été étudiées par Billing-Mahler ([1]) , Birch, Swinnerton-Dyer, Ligozat ([4]) , Mazur ([5]) etc... Ils ont montré que ces courbes elliptiques n'ont qu'un nombre fini de points. Ces points ne sont pas singuliers pour l'équation $F_N(X,Y) = 0$: par conséquent, les valeurs (j,j_N) correspondantes, données par le tableau suivant, déterminent bien des couples (E,C) .

N	# $X_o(N)(\mathbb{Q})$	# {Pointes rationnelles}	(j, j_N)
11	5	2	$(-2^{15}, -2^{15})$ $(-11^2, -11.131^3)$ $(-11.131^3, -11^2)$
14	6	4	$(-3^3.5^3, 3^3.5^3.17^3)$ $(3^3.5^3.17^3, -3^3.5^3)$
15	8	4	$(-\frac{5^2}{2}, \frac{5.211^3}{2^{15}})$ $(\frac{5.211^3}{2^{15}}, -\frac{5^2}{2})$ $(-\frac{5.29^3}{2^5}, -\frac{5^2.241^3}{2^3})$ $(-\frac{5^2.241^3}{2^3}, -\frac{5.29^3}{2^5})$
17	4	2	$(-\frac{17^2.101^3}{2}, -\frac{17.373^3}{2^{17}})$ $(-\frac{17.373^3}{2^{17}}, -\frac{17^2.101^3}{2})$
19	3	2	$(-2^{15}.3^3, -2^{15}.3^3)$
20	6	6	———
21	8	4	$(\frac{3^3.5^3}{2}, -\frac{3^2.5^3.101^3}{2^{21}})$ $(-\frac{3^2.5^3.101^3}{2^{21}}, \frac{3^3.5^3}{2})$ $(-\frac{3^2.5^6}{2^3}, -\frac{3^3.5^3.383^3}{2^7})$ $(-\frac{3^3.5^3.383^3}{2^7}, -\frac{3^2.5^6}{2^3})$
24	8	8	———
27	3	2	$(-2^{15}.3.5^3, -2^{15}.3.5^3)$
32	4	4	———
36	6	6	———
49	2	2	———

c) Si la conjecture de Mordell est vraie, les courbes $X_o(N)$ de genre ≥ 2 n'ont qu'un nombre fini de points rationnels sur $\mathbb{Q}$. Pour le genre 2, on montre que les points rationnels de $X_o(22)$, $X_o(26)$ ([8]), $X_o(50)$ sont des pointes, tandis que $X_o(37)$ possède en plus de ses deux pointes deux points rationnels sur $\mathbb{Q}$. C'est ce dernier résultat dû à Mazur et Swinnerton-Dyer ([7]) que nous allons exposer maintenant.

§3 - Etude de $X_o(37)$

Méthode classique.

Par des méthodes à la Fricke, Swinnerton-Dyer a trouvé une équation de $X = X_o(37)$ qui est :

$$y^2 = -x^6 - 9x^4 - 11x^2 + 37 .$$

Cette courbe de genre 2, possède l'involution hyperelliptique :
$S : (x,y) \mapsto (x,-y)$, qui a 6 points fixes, ainsi que les involutions
$W : (x,y) \mapsto (-x,y)$ qui a 2 points fixes réels α_1 et α_2 , et $T : (x,y) \mapsto (-x,-y)$ qui a 2 points fixes imaginaires β_1 et β_2 . Les quotients sont X/S de genre 0 $E = X/W$ de genre 1 , $F = X/T$ de genre 1 . Nous allons les décrire :

▪ E est une courbe elliptique dont on obtient un modèle minimal ([12]) en posant $\alpha = \frac{-x^2-3}{4}$, $\beta = \frac{y-4}{8}$, ce qui donne $\beta^2+\beta = \alpha^3-\alpha$. Cette courbe a pour conducteur 37 ; $E(\mathbb{Q})$ est sans torsion, mais possède des points d'ordre infini, par exemple le point $(0,0)$.

▪ F est une courbe elliptique dont on obtient un modèle minimal en posant : $u = \frac{1}{4}(\frac{37}{x^2}-5)$, $v = \frac{1}{8}(\frac{37y}{x^3}-4)$, ce qui donne :

$$v^2 + v = u^3 + u^2 - 23u - 50 .$$

Cette courbe a pour conducteur 37, et $F(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, comme on peut le voir en faisant une descente sur les points d'ordre 3 ou en utilisant un théorème de Mazur ([5]) . Les points de $F(\mathbb{Q})$ de coordonnées $(8,18)$ et $(8,-19)$ nous donnent les points rationnels de X qui sont $(1,4)$, $(-1,4)$, $(1,-4)$ et $(-1,-4)$ et parmi ceux-ci, seuls les deux derniers ne sont pas des pointes.

THEOREME 7. -

1) Il existe deux courbes elliptiques E et E' et une isogénie $\varphi : E \to E'$ de degré 37 définis sur $\mathbb{Q}$.

2) Toute telle isogénie est isomorphe soit à $\varphi : E \to E'$ soit à sa transposée $\varphi' : E' \to E$.

En d'autres termes, $X_o(37)$ n'a que deux points rationnels sur $\mathbb{Q}$ en plus des pointes $\{\infty\}$ et $\{0\}$, et ces points sont permutés par W_{37} .

En utilisant une méthode suggérée par Swinnerton-Dyer on trouve les modèles minimaux de E et E' :

$$E : y^2 + xy + y = x^3 + x^2 - 8x + 6 \ , \quad j = -7.11^3 \ ;$$

$$E' : y^2 + xy + y = x^3 + x^2 - 208083x - 36621194 \ , \quad j = -7.137^3.2083^3 .$$

Méthodes "sans calculs" (Mazur-Swinnerton-Dyer ([7])) .

La méthode précédente a le défaut de nécessiter des calculs pénibles qui diffèrent d'une valeur de N à une autre, c'est pourquoi il est préférable de raisonner directement sur $X_o(N)$.

1) On sait que $X = X_o(37)$ est de genre 2, et possède deux pointes $\{\infty\}$ et $\{0\}$ qui sont rationnelles sur $\mathbb{Q}$.

2) Il en résulte que X possède une involution hyperelliptique unique S qui a 6 points fixes.

3) X possède aussi l'involution $W : \tau \to \frac{-1}{37\tau}$. On calcule les points fixes de cette involution à l'aide des classes de formes quadratiques de discriminant -4.37 . On trouve deux points fixes α_1 , α_2 , représentés par $\tau_1 = \frac{1}{\sqrt{-37}}$ et $\tau_2 = \frac{1+1\sqrt{-37}}{2}$. Comme $W \neq S$, $E = X/W$ est de genre 1 .

4) L'involution hyperelliptique étant unique, on a $WSW = S$. Par conséquent, $WS = SW = T$ est une autre involution de X qui a deux points fixes β_1 et β_2 et telle que $F = X/T$ soit de genre 1 .

5) On vérifie ([7]) que les 6 points fixes de S , α_1 , α_2 , β_1 , β_2 , $\{\infty\}$, $\{0\}$ sont distincts ; on pose $\gamma_o = T(\{0\})$ et $\gamma_\infty = T(\{\infty\})$ de sorte qu'on a :

$$\begin{array}{ccc} \{\infty\} & \overset{W}{\longleftrightarrow} & \{0\} \\ \updownarrow T & & \updownarrow T \\ \gamma_\infty & \overset{W}{\longleftrightarrow} & \gamma_0 \end{array}$$

6) Le lieu réel $X(\mathbb{R})$ est connexe, car pour tout nombre premier p , $X_o(p)(\mathbb{R})$ est connexe. En effet, dans "le domaine fondamental" de $\Gamma_o(p)$, les points réels de $X_o(p)$ sont représentés par les deux demi-droites $Re(\tau) = 0$ et $Re(\tau) = -\frac{1}{2}$.

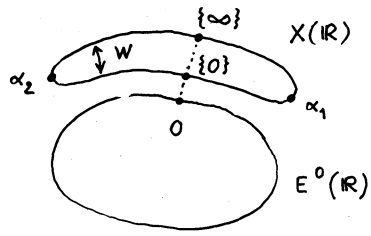
Après ces préliminaires, on peut décrire les deux revêtements $X(\mathbb{R}) \overset{\varphi}{\to} E^0(\mathbb{R})$ et $X(\mathbb{R}) \overset{\psi}{\to} F^0(\mathbb{R})$, où $E^0(\mathbb{R})$ et $F^0(\mathbb{R})$ sont les composantes neutres de $E(\mathbb{R})$ et $F(\mathbb{R})$. On choisit les lois de groupe sur E et F pour que $\varphi(\{\infty\})$ et $\psi(\{\infty\})$ soient éléments neutres de E et F.

Revêtement.

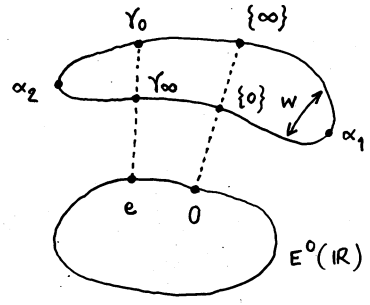
$$X(\mathbb{R}) \overset{\varphi}{\to} E^0(\mathbb{R}) .$$

$E = X/W$, φ est un revêtement d'ordre 2.

1) Les points fixes α_1 et α_2 de W sont réels. En effet, $\tau_1 = 1/\sqrt{-37}$, $\tau_2 = \frac{1+1/\sqrt{-37}}{2}$, et par conséquent, $q_i = e^{2\pi i \tau_i} \in \mathbb{R}$. Comme les fonctions sur X admettent des développements en q à coefficients réels, α_1 et α_2 sont réels. Il en résulte que le revêtement est ramifié aux deux points α_1 et α_2. On a :



2) Il reste à placer γ_0 et γ_∞. Sur $X(\mathbb{R})$, W renverse l'orientation, ainsi que S qui est une involution hyperelliptique, donc du type $(x,y) \to (x,-y)$. Il en résulte que T conserve l'orientation sur $X(\mathbb{R})$, donc que β_1 et β_2 ne sont pas réels. Comme $T\alpha_1 = \alpha_2$ la seule possibilité est :

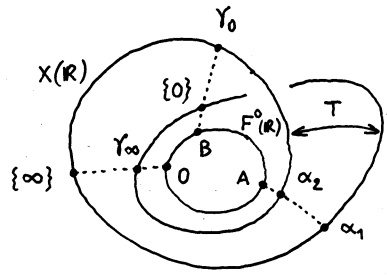


T induit sur E une involution qui a des points fixes sur $\mathbb{C}$; par conséquent, cette involution est $P \to e-P$, où e est l'image de γ_0 et γ_∞ dans E .

Avec la terminologie de Mazur ([6]) , le nombre d'enroulement est 0 et par conséquent la fonction L de la courbe E a un zéro en s = 1 ; ce qui est en accord avec les conjectures de Birch et Swinnerton-Dyer, puisqu'on a déjà vu que la courbe E possède des points d'ordre infini.

Revêtement $X(\mathbb{R}) \downarrow F^0(\mathbb{R})$.

F = X/T , ψ est un revêtement d'ordre 2 qui n'est pas ramifié puisque T n'a pas de points fixes réels. On a :



B est un point d'ordre 3 sur F car sur X la fonction $[\frac{\Delta(37\tau)}{\Delta(\tau)}]^{1/12}$ a pour diviseur $3\{\infty\} - 3\{0\}$. Ayant des points fixes, W induit sur F l'involution $P \to A-P$, et comme $W(0) = B$, on a $A = -B$ ce qui montre que A est aussi un point d'ordre 3 sur F .

Il reste à voir que 0,A et B sont les seuls points rationnels de $F^0(\mathbb{R})$ et que par conséquent, $\{\infty\}$, $\{0\}$, γ_∞ et γ_0 sont les seuls points rationnels de X .

D'après Deligne ([2]) , une courbe elliptique provenant de $X_0(p)$ a pour conducteur p (pour p premier). D'après Mazur ([5]) , si $\mathcal{E}$ a pour conducteur p , ou $\#\mathcal{E}(\mathbb{Q}) = 6$, ou $\mathcal{E}(\mathbb{Q})$ est sans torsion. Appliqué à F , ceci prouve que $F(\mathbb{Q})$ est, soit $\mathbb{Z}/6\mathbb{Z}$, soit $\mathbb{Z}/3\mathbb{Z}$. Enfin, Miyawaki ([9]) a déterminé toutes les courbes elliptiques sur $\mathbb{Q}$, de conducteur premier, ayant des points d'ordre fini non triviaux ; il trouve deux courbes de conducteur 37 et aucune n'a de point rationnel d'ordre 2. Par conséquent, $F(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$ et le théorème 7 est redémontré.

Le nombre d'enroulement de ψ est $2/3$ ce qui montre que la fonction L de F ne s'annule pas en $s = 1$ et que l'ordre conjectural du groupe $Ш(F)$ est 1 .

-:-:-:-

BIBLIOGRAPHIE

([1]) BILLING-MAHLER. - On exceptional points on cubic curves. J. London Math. Soc., 15 (1940).

([2]) DELIGNE. - Formes modulaires et représentations ℓ-adiques. Séminaire Bourbaki, n°355, fév. 69.

([3]) FRICKE. - Algebra III. Leipzig, Teubner, 1928.

([4]) LIGOZAT. - Fonction L des courbes modulaires. Séminaire Delange-Pisot-Poitou, 1969-70, n°9.

([5]) MAZUR. - Rational points of abelian varieties with values in towers of number fields. Inventiones Math., 18, 1972.

([6]) MAZUR. - Courbes elliptiques et symboles modulaires. Séminaire Bourbaki, n°414, juin 72.

([7]) MAZUR-SWINNERTON-DYER. - Curves of analytic conductor 37, (non publié).

([8]) MAZUR-VELU. - Courbes de Weil de conducteur 26. Note aux C.R.A.S. (16 oct. 72).

([9]) MIYAWAKI. - Elliptic curves of prime power conductor with $\mathbb{Q}$-rational points of finite order. Osaka J. Math, 10 (1973).

([10]) SMITH. - Note on a modular equation of the transformation of the third ordre. Collected mathematical papers, III, pp.274-278, Chelsea.

([11]) WEBER. - Lehrbuch der Algebra, III, Chelsea.

([12]) Pour tout ce qui concerne les modèles de Néron voir NERON : Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. I.H.E.S. Publ. n°21. Pour la définition du conducteur d'une courbe elliptique, voir OGG : Elliptic curves and wild ramification. American J. Math., janvier 67.

-:-:-:-

C.N.R.S. Orsay
Mathématiques
Bâtiment 425
91405 ORSAY