

Corps engendré par les points de 13-torsion des courbes elliptiques

par

MARUSIA REBOLLEDO HOCHART (Paris)

Soit E une courbe elliptique sur un corps de nombres. Les propriétés des accouplements de Weil montrent que le corps $K_n(E)$ engendré par les points de n -torsion de E est une extension du corps $\mathbb{Q}(\mu_n)$ engendré par les racines n -ièmes de l'unité dans une clôture algébrique $\overline{\mathbb{Q}}$ de \mathbb{Q} .

Soit \mathcal{S} l'ensemble des nombres premiers p pour lesquels il existe une courbe elliptique E telle que $K_p(E) = \mathbb{Q}(\mu_p)$. Il est connu que l'ensemble \mathcal{S} contient les nombres 2, 3, 5 et Halberstadt a prouvé que 7 n'est pas dans \mathcal{S} . Merel a étudié plus avant cet ensemble. En particulier, il a montré avec Stein ([7], [9]) qu'aucun nombre premier $p \neq 13$, $7 < p < 1000$, n'appartient à \mathcal{S} . L'objet de ce papier est de traiter le cas $p = 13$, pour lequel les techniques de Merel ne s'appliquent pas.

Nous démontrons le théorème suivant :

THÉORÈME 1. *Aucune courbe elliptique sur un corps de nombres n'a tous ses points d'ordre 13 définis sur $\mathbb{Q}(\mu_{13})$ (autrement dit, $13 \notin \mathcal{S}$).*

Notons $Y(13)$ (resp. $Y_1(13)$) la courbe affine sur \mathbb{Q} classifiant les classes d'isomorphismes de paires (E, π) (resp. (E, P)) où E est une courbe elliptique et $\pi : (\mathbb{Z}/13\mathbb{Z})^2 \hookrightarrow E[13]$ un plongement (resp. P un point d'ordre 13 de E). Soit $X(13)$ (resp. $X_1(13)$) la courbe complète obtenue en adjoignant les pointes à $Y(13)$ (resp. $Y_1(13)$).

Montrer le théorème revient à montrer que $Y(13)$ n'a pas de point $\mathbb{Q}(\mu_{13})$ -rationnel. Pour ce faire, nous étudions la courbe $Y_1(13)$: l'examen détaillé d'un plongement de $X_1(13)$ dans sa jacobienne $J_1(13)$ et la description complète du groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$ permettent de borner le cardinal de $Y_1(13)(\mathbb{Q}(\mu_{13}))$. On raisonne alors par l'absurde : l'image d'un point de $Y(13)(\mathbb{Q}(\mu_{13}))$ par le revêtement $X(13) \rightarrow X_1(13)$ fournirait "trop" de points de $Y_1(13)(\mathbb{Q}(\mu_{13}))$.

2000 *Mathematics Subject Classification*: Primary 11G05, 11F67; Secondary 11G18, 11G40.

Nous noterons par la suite \bar{n} l'image dans $\mathbb{Z}/13\mathbb{Z}$ d'un entier n , et \tilde{a} un relevé dans \mathbb{Z} d'un entier a modulo 13. Soient $\Gamma_0(13)$, $\Gamma = \Gamma_1(13)$ les sous-groupes de $\mathrm{SL}_2(\mathbb{Z})$ formés des éléments congrus respectivement à $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ et $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ modulo 13. Nous noterons $S = S_2(\Gamma_1(13))$ l'espace des formes modulaires paraboliques de poids 2 pour $\Gamma_1(13)$. Pour $\phi : (\mathbb{Z}/13\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ un caractère, $S_2(13, \phi)$ désignera l'ensemble des formes f de S telles que, pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\Gamma_0(13)$, $f | \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \phi(\bar{d}).f$. Nous noterons enfin W_{13} l'opérateur d'Atkin–Lehner, c'est-à-dire l'involution de $X_1(13)$ déduite de l'involution $z \mapsto -\frac{1}{13z}$ sur $\overline{\mathcal{H}}$, où $\overline{\mathcal{H}} = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$, \mathcal{H} étant le demi-plan de Poincaré.

1. Étude du groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$. Rappelons que deux pointes

$$\alpha_i = p_i/q_i, \quad i = 1, 2, \quad \mathrm{pgcd}(p_i, q_i) = 1,$$

sont équivalentes modulo $\Gamma = \Gamma_1(13)$ si et seulement si

$$q_2 = \lambda q_1 \pmod{13}, \quad p_2 = \lambda p_1 \pmod{\mathrm{pgcd}(q_1, 13)}, \quad \lambda = \pm 1$$

(voir [2]). De plus les pointes de $X_1(13)$ sont toutes $\mathbb{Q}(\mu_{13})$ -rationnelles et $\sigma \in (\mathbb{Z}/13\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_{13})/\mathbb{Q})$ opère sur une pointe par $\begin{pmatrix} \sigma & 0 \\ 0 & 1 \end{pmatrix}$. Ainsi la courbe $X_1(13)$ possède six pointes \mathbb{Q} -rationnelles : $P_i = \Gamma.\frac{13}{i}$, $1 \leq i \leq 6$, et six autres pointes : $Q_j = \Gamma.\frac{j}{13}$, $1 \leq j \leq 6$. L'opérateur d'Atkin–Lehner W_{13} échange P_i et Q_i pour $1 \leq i \leq 6$.

Choisissons le plongement de $X_1(13)$ dans $J_1(13)$ donné par la pointe P_6 :

$$\iota : X_1(13) \rightarrow J_1(13), \quad P \mapsto [(P) - (P_6)].$$

Ogg ([10]) montre que le sous-groupe de $J_1(13)(\mathbb{Q}(\mu_{13}))$ engendré par les images sous ι des pointes \mathbb{Q} -rationnelles :

$$C_1 = \langle u_1, \dots, u_6 \rangle, \quad u_i = \iota(P_i), \quad 1 \leq i \leq 6,$$

est cyclique d'ordre 19. Par conséquent, le sous-groupe

$$C_2 = W_{13}.C_1 = \langle v_1, \dots, v_6 \rangle, \quad v_j = [(Q_j) - (Q_6)], \quad 1 \leq j \leq 6,$$

l'est également. Ces deux groupes d'ordre 19, distincts pour des raisons de rationalité, sont donc en somme directe et on a

$$(\mathbb{Z}/19\mathbb{Z})^2 \cong C_1 \oplus C_2 \subset J_1(13)(\mathbb{Q}(\mu_{13})).$$

On va en fait montrer l'égalité :

PROPOSITION 1. *On a $J_1(13)(\mathbb{Q}(\mu_{13})) = C_1 \oplus C_2$.*

L'essentiel de la démonstration repose sur le lemme suivant :

LEMME 1. *Le groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$ est fini.*

D'après ce qui précède, le lemme suivant suffira alors à prouver la proposition :

LEMME 2. Pour tout premier l distinct de 19, on a

$$J_1(13)(\mathbb{Q}(\mu_{13}))[l] = \{0\},$$

et pour tout $n \in \mathbb{N}$,

$$J_1(13)(\mathbb{Q}(\mu_{13}))[19^n] = J_1(13)(\mathbb{Q}(\mu_{13}))[19] \cong (\mathbb{Z}/19\mathbb{Z})^2.$$

1.1. Finitude de $J_1(13)(\mathbb{Q}(\mu_{13}))$. Rappelons que la courbe $X_1(13)$ est de genre $g = 2$. Le groupe $\Gamma_0(13)/\Gamma_1(13) \cong (\mathbb{Z}/13\mathbb{Z})^\times$ agissant sur S , on a $S = \bigoplus_\phi S_2(13, \phi)$, où ϕ décrit l'ensemble des caractères pairs de $(\mathbb{Z}/13\mathbb{Z})^\times$ (voir [3]).

La formule de Riemann–Hurwitz montre que $S_2(13, \phi) = 0$ pour ϕ d'ordre distinct de l'ordre maximal 6. En effet, si $\Gamma_1(13) \subset \ker \phi \subset \Gamma_0(13)$ sont des inclusions strictes, la courbe modulaire associée à $\ker \phi$ est de genre nul. Notons $\varepsilon, \bar{\varepsilon}$ les deux caractères d'ordre 6 de $(\mathbb{Z}/13\mathbb{Z})^\times$, et ζ une racine primitive douzième de l'unité. Ces deux caractères sont définis par $\varepsilon(2) = \zeta^2$, $\bar{\varepsilon}(2) = \zeta^{-2}$. On a $S = S_2(13, \varepsilon) \oplus S_2(13, \bar{\varepsilon})$, et les \mathbb{C} -espaces vectoriels $S_2(13, \varepsilon)$ et $S_2(13, \bar{\varepsilon})$ sont de dimension 1 engendrés chacun par une forme primitive f_ε et $f_{\bar{\varepsilon}}$ respectivement.

Les résultats de Kato ([4, corollaire 14.3]) en direction de la conjecture de Birch et Swinnerton-Dyer montrent que si $L(J_1(13), \mathbb{Q}(\mu_{13}), 1) \neq 0$ alors $J_1(13)(\mathbb{Q}(\mu_{13}))$ est fini. De plus, d'après un théorème de Shimura complété par Carayol,

$$L(J_1(13), \mathbb{Q}(\mu_{13}), s) = \prod_{\chi, f} L(f, \chi, s),$$

où χ décrit l'ensemble des caractères de Dirichlet modulo 13 et f l'ensemble des formes primitives de poids 2 de niveau 13. D'après ce qui précède, on a donc

$$L(J_1(13), \mathbb{Q}(\mu_{13}), 1) = \prod_{\chi : (\mathbb{Z}/13\mathbb{Z})^\times \rightarrow \mathbb{C}^\times} L(f_\varepsilon, \chi, 1) \cdot L(f_{\bar{\varepsilon}}, \chi, 1).$$

Pour prouver la finitude du groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$, il suffit alors de prouver que la condition (C₁) suivante est satisfaite :

$$(C_1) \quad \forall \chi : (\mathbb{Z}/13\mathbb{Z})^\times \rightarrow \mathbb{C}^\times, \quad L(f_\varepsilon, \chi, 1) \neq 0, \quad L(f_{\bar{\varepsilon}}, \chi, 1) \neq 0.$$

Pour $\chi : (\mathbb{Z}/13\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$, notons $\tau(\chi) = \sum_{b \bmod 13} \chi(b) e^{-2i\pi\tilde{b}/13}$ la somme de Gauss. La formule ([6, théorèmes 3.9 et 4.2])

$$L(f, \chi, 1) = \frac{-2i\pi\tau(\chi)}{13} \sum_{a \bmod 13} \bar{\chi}(a) \int_{\tilde{a}/13}^{\infty} f(u) du \quad (f \in S)$$

nous conduit à utiliser les symboles modulaires. Nous allons énoncer une condition (C₂) sur certains symboles modulaires, qui entraîne (C₁) et donc la finitude de $J_1(13)(\mathbb{Q}(\mu_{13}))$.

1.1.1. *Symboles modulaires et condition suffisante à la finitude de $J_1(13)(\mathbb{Q}(\mu_{13}))$.* Dans cette section, nous verrons $X = X_1(13)(\mathbb{C})$ comme la surface de Riemann compacte connexe $\Gamma \backslash \overline{\mathcal{H}}$, où $\overline{\mathcal{H}} = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$, \mathcal{H} étant le demi-plan de Poincaré. Pour ce qui concerne la théorie des symboles modulaires nous renvoyons à [2], [6], [8].

Soient $H_1(X; \mathbb{Z})$ (resp. $H_1(X, \text{ptes}; \mathbb{Z})$) l’homologie singulière absolue (resp. relative à l’ensemble $\{\text{ptes}\}$ des pointes) de X . Pour $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$, on note $\{\alpha, \beta\}$, appelé *symbole modulaire*, la classe d’homologie dans $H_1(X, \text{ptes}; \mathbb{Z})$ de l’image d’une géodésique reliant α à β .

Notons $H = H_1(X; \mathbb{C})$ et $H' = H_1(X, \text{ptes}; \mathbb{C})$. Le \mathbb{C} -espace vectoriel H est de dimension $2g = 4$, et vérifie la suite exacte longue d’homologie :

$$(*) \quad 0 \rightarrow H \rightarrow H' \xrightarrow{\delta} \mathbb{C}[\text{ptes}] \xrightarrow{\text{deg}} \mathbb{C} \rightarrow 0,$$

où δ est l’application “bord” : $\{\alpha, \beta\} \mapsto (\Gamma\beta) - (\Gamma\alpha)$, et deg l’application “degré” usuelle sur les diviseurs. L’espace vectoriel H' est donc de dimension 15 sur \mathbb{C} .

On dispose également de l’homomorphisme de groupes de Manin :

$$\xi : \begin{cases} \mathbb{C}[\Gamma \backslash \text{SL}_2(\mathbb{Z})] \rightarrow H', \\ [\Gamma.g] \mapsto \{g0, g\infty\} = \{b/d, a/c\}, \end{cases} \quad \text{avec} \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}).$$

Rappelons que ξ est surjectif, de noyau engendré par les *relations de Manin*, c’est-à-dire par les éléments de la forme $[x] + [x\sigma]$, $[x] + [x\tau] + [x\tau^2]$, où $x \in \Gamma \backslash \text{SL}_2(\mathbb{Z})$, et σ, τ des éléments de $\text{SL}_2(\mathbb{Z})$ d’ordre respectif 4 et 3 :

$$\sigma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \tau = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Notons $\mathcal{A} = [(\mathbb{Z}/13\mathbb{Z})^2 - (0, 0)]$. Remarquons que l’application

$$\Gamma. \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (\bar{c}, \bar{d})$$

est une bijection de $\Gamma \backslash \text{SL}_2(\mathbb{Z})$ sur \mathcal{A} . Le morphisme de Manin fournit donc une application encore notée ξ sur $\mathbb{C}[\mathcal{A}]$. On note $[c, d]$, appelé *symbole de Manin*, l’image par ξ dans H' de l’élément (c, d) de \mathcal{A} . Le groupe $\text{SL}_2(\mathbb{Z})$ agit sur les symboles de Manin par multiplication à droite.

Les correspondances de Hecke T_n , $n \in \mathbb{N}$, et les opérateurs diamants $\langle m \rangle$, $(m, 13) = 1$, sur $X_1(13)$, induisent des endomorphismes de H' que nous noterons respectivement T'_n et $\langle m \rangle'$: on pose $t'.\{\alpha, \beta\} = \{t.\alpha, t.\beta\}$, où $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$, $t = T_n$ ou $\langle m \rangle$. Soit \mathbb{T}' la sous-algèbre de $\text{End}(H')$ engendrée par les endomorphismes T'_p , et $\langle q \rangle'$ pour p, q premiers, $q \neq 13$. L’espace H vu comme sous-espace de H' est stable sous l’action de \mathbb{T}' . L’action des opérateurs diamants est donnée par

$$\langle m \rangle'[c, d] = [\bar{m}c, \bar{m}d].$$

Pour χ caractère de Dirichlet modulo 13 et x dans H' , notons H'^χ (resp. H^χ) la composante χ -isotypique de H' (resp. H), et x^χ la projection de x sur H'^χ . Posons également

$$\theta_\chi = t_\chi \cdot \sum_{a \bmod 13} \chi(a) \cdot [1, a] \quad \text{avec} \quad t_\chi = \begin{cases} 1 & \text{si } \chi \text{ est impair,} \\ (T_2' - 2\langle 2 \rangle' - 1) & \text{si } \chi \text{ est pair.} \end{cases}$$

LEMME 3. *La condition (C₂) suivante entraîne la condition (C₁) et donc la finitude du groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$:*

$$(C_2) \quad \forall \chi : (\mathbb{Z}/13\mathbb{Z})^\times \rightarrow \mathbb{C}^\times, \quad \theta_\chi^\varepsilon \neq 0, \quad \theta_\chi^{\bar{\varepsilon}} \neq 0.$$

Preuve. Montrons tout d'abord que l'élément θ_χ de H' est en réalité dans H . On a

$$\delta(\theta_\chi) = \delta\left(t_\chi \cdot \sum_{a \bmod 13} \chi(a) \cdot \left\{ \frac{-1}{\bar{a}}, 0 \right\}\right) = - \sum_{a \bmod 13} \chi(a) \left(t_\chi \left(\Gamma \cdot \frac{-1}{\bar{a}} \right) \right).$$

Or

$$\Gamma \cdot \left(\frac{-1}{\bar{a}} \right) = \Gamma \cdot \frac{1}{\bar{a}} = \Gamma \cdot \left(\frac{-1}{-\bar{a}} \right),$$

donc pour χ impair,

$$\delta(\theta_\chi) = - \sum_{k=1}^6 (\chi(\bar{k}) + \chi(-\bar{k})) \left(\Gamma \cdot \frac{1}{\bar{k}} \right) = 0.$$

Pour χ pair, un calcul montre que $t_\chi \left(\Gamma \cdot \frac{1}{\bar{a}} \right) = 0$ ([11, 2.4]).

La conjugaison complexe sur X , déduite de l'involution $z \mapsto -\bar{z}$ sur \mathcal{H} , induit sur H' l'involution $i : [c, d] \mapsto [-c, d]$. Le sous-espace H est stable sous i . Notons H^+ (resp. H^-) la partie invariante (resp. antiinvariante) de H sous i . On a $H = H^+ \oplus H^-$, et H^+ , H^- sont des \mathbb{C} -espaces vectoriels de dimension 2. On vérifie que $\theta_\chi \in H^+$ pour χ pair, et $\theta_\chi \in H^-$ pour χ impair.

On dispose d'autre part de l'application \mathbb{C} -linéaire

$$H \rightarrow \text{Hom}_{\mathbb{C}}(H^0(X, \Omega_X^1), \mathbb{C}), \quad c \mapsto \left(\omega \mapsto \int_c \omega \right).$$

Pour $f \in S = S_2(\Gamma_1(13))$, notons ω_f la différentielle holomorphe sur $X_1(13)$ induite par $2i\pi f(z)dz$. L'application $f \mapsto \omega_f$ est un isomorphisme de S sur $H^0(X, \Omega_X^1)$. Le morphisme qui s'en déduit,

$$F : H \rightarrow \text{Hom}_{\mathbb{C}}(S, \mathbb{C}), \quad c \mapsto \left(f \mapsto \int_c \omega_f \right),$$

induit un isomorphisme F^+ sur H^+ , resp. F^- sur H^- .

Soit \mathbb{T} l'algèbre engendrée par les correspondances de Hecke T_p et les diamants $\langle q \rangle$ sur $X_1(13)$, pour p, q premiers, $q \neq 13$. L'algèbre \mathbb{T} agit à droite sur les formes modulaires et donc sur $\text{Hom}_{\mathbb{C}}(S, \mathbb{C})$. Cette action munit H^+ ,

resp. H^- , d'une structure de \mathbb{T} -module : pour $t \in \mathbb{T}$, $c \in H^\pm$, $t.c$ est défini par $\int_{t.c} \omega_f = \int_c \omega_{t.f}$. Les actions de \mathbb{T} et \mathbb{T}' sur H coïncident. En particulier l'action des diamants fournit des isomorphismes sur chaque composante : $F^{\pm, \phi} : H^{\pm, \phi} \xrightarrow{\sim} \text{Hom}_{\mathbb{C}}(S_2(13, \phi), \mathbb{C})$, pour ϕ caractère modulo 13. On en déduit $H^\phi = 0$ pour $\phi \neq \varepsilon, \bar{\varepsilon}$, et $H = H^\varepsilon \oplus H^{\bar{\varepsilon}}$.

Soient

$$c_\chi = \sum_{a \bmod 13} \bar{\chi}(a) \left\{ \frac{\tilde{a}}{13}, \infty \right\} \in H', \quad f \in S, \quad \chi : (\mathbb{Z}/13\mathbb{Z})^\times \rightarrow \mathbb{C}^\times.$$

On a

$$L(f, \chi, 1) = -\frac{\tau(\chi)}{13} \int_{c_\chi} \omega_f.$$

On remarque que $\theta_\chi = t_\chi W_{13} c_{\bar{\chi}}$. Notons t_χ^* l'élément de \mathbb{T} tel que l'on a $t_\chi W_{13} = W_{13} t_\chi^*$.

Supposons à présent que la condition (C_2) est vérifiée. En particulier $\theta_\chi^\varepsilon \neq 0$. Les isomorphismes $F^{\pm, \varepsilon}$ montrent qu'il existe f dans $S_2(13, \varepsilon)$ telle que $\int_{\theta_\chi^\varepsilon} \omega_f \neq 0$. L'espace $S_2(13, \varepsilon)$ étant engendré par f_ε , il s'ensuit que $\int_{\theta_\chi} \omega_{f_\varepsilon} = \int_{\theta_{\bar{\chi}}^\varepsilon} \omega_{f_\varepsilon} \neq 0$. Or

$$\int_{\theta_\chi} \omega_{f_\varepsilon} = \int_{t_\chi \cdot W_{13} c_{\bar{\chi}}} \omega_{f_\varepsilon} = \int_{t_\chi^* \cdot c_{\bar{\chi}}} \omega_{f_{\bar{\varepsilon}}} = \lambda_\chi \cdot \int_{c_{\bar{\chi}}} \omega_{f_{\bar{\varepsilon}}} = -\frac{13\lambda_\chi}{\tau(\bar{\chi})} L(f_{\bar{\varepsilon}}, \bar{\chi}, 1),$$

où $t_\chi^* \cdot f_{\bar{\varepsilon}} = \lambda_\chi \cdot f_{\bar{\varepsilon}}$, $\lambda_\chi \in \mathbb{C}$. Ceci prouve que si $\theta_\chi^\varepsilon \neq 0$ alors $L(f_{\bar{\varepsilon}}, \bar{\chi}, 1) \neq 0$. De même, si $\theta_\chi^{\bar{\varepsilon}} \neq 0$ alors $L(f_\varepsilon, \bar{\chi}, 1) \neq 0$. ■

1.1.2. Vérification de la condition (C_2) . Nous allons faire les calculs dans les composantes H'^ε , $H'^{\bar{\varepsilon}}$ de H' , espace pour lequel nous disposons de la présentation de Manin. Pour cela nous allons déterminer une base de H'^ε (resp. $H'^{\bar{\varepsilon}}$) et exprimer θ_χ^ε (resp. $\theta_\chi^{\bar{\varepsilon}}$) dans cette base. La dimension de ces composantes se déduit de la suite exacte $(*)$ de la section 1.1.1 :

LEMME 4. *On a $\dim H' = 15$, et $\dim H'^\phi$ vaut 0 si ϕ est impair, 1 si ϕ est trivial, 4 si $\phi = \varepsilon$ ou $\bar{\varepsilon}$, et 2 sinon.*

Soit ϕ désignant indifféremment ε ou $\bar{\varepsilon}$. On peut voir H'^ϕ comme le quotient de H' par les relations

$$[nu, nv] = \phi(n) \cdot [u, v] \quad (n \in (\mathbb{Z}/13\mathbb{Z})^\times, (u, v) \in \mathcal{A}).$$

Notons $[u, v]^\phi$ l'image de $[u, v]$ dans H'^ϕ . Pour tout $u \neq 0$ dans $\mathbb{Z}/13\mathbb{Z}$, on a $[u, v]^\phi = \phi(u) \cdot [1, vu^{-1}]^\phi$, et $[0, v]^\phi = \phi(v) \cdot [0, 1]^\phi$. On en déduit que $\{[0, 1]^\phi, [1, w]^\phi : w \in \mathbb{Z}/13\mathbb{Z}\}$ forme un système de générateurs de H'^ϕ . En écrivant les relations de Manin pour ces générateurs, on obtient la proposition suivante :

LEMME 5. Les éléments $[1, 0]^\phi$, $[1, 2]^\phi$, $[1, 3]^\phi$, $[1, -3]^\phi$ forment une base de H'^ϕ , où $\phi = \varepsilon$ ou $\bar{\varepsilon}$. Dans cette base, les générateurs $[0, 1]^\phi$, $[1, w]^\phi$, pour $w \in \mathbb{Z}/13\mathbb{Z}$, s'écrivent respectivement :

$$\begin{aligned} [0, 1]^\phi &= -[1, 0]^\phi, & [1, 1]^\phi &= [1, -1]^\phi = 0, \\ [1, -2]^\phi &= [1, 2]^\phi, & [1, 6]^\phi &= [1, -6]^\phi = -\phi(6) \cdot [1, 2]^\phi, \\ [1, 4]^\phi &= -\phi(4) \cdot [1, 3]^\phi, & [1, -4]^\phi &= -\phi(4) \cdot [1, -3]^\phi, \\ [1, 5]^\phi &= \phi(6) \cdot [1, 3]^\phi - \phi(6) \cdot [1, 2]^\phi, & [1, -5]^\phi &= \phi(4) \cdot [1, 2]^\phi - \phi(4) \cdot [1, -3]^\phi. \end{aligned}$$

Pour χ impair, on a alors :

$$\begin{aligned} \theta_\chi^\phi &= (\chi(3) - \chi(4)\phi(4) + \chi(5)\phi(6)) \cdot [1, 3]^\phi \\ &\quad + (-\chi(3) + \chi(4)\phi(4) + \chi(5)\phi(4)) \cdot [1, -3]^\phi. \end{aligned}$$

Or, χ est défini par $\chi(2) = \zeta^k$, ζ une racine primitive douzième de l'unité, $k = 1, 3, 5, 7, 9, 11$. Donc $\chi(3) - \chi(4)\varepsilon(4) + \chi(5)\varepsilon(6) = \zeta^{4k} - \zeta^{2k+4} + \zeta^{9k+10}$. Ce terme est non nul pour $k = 1, 3, 5, 7, 9, 11$, donc θ_χ^ε est non nul pour χ impair. De même, on montre que $\theta_\chi^{\bar{\varepsilon}} \neq 0$ pour χ impair.

D'après [8], on a $T_2' \cdot [c, d] = [2c, d] + [2c, c + d] + [c + d, 2d] + [c, 2d]$. Donc, pour χ pair,

$$\begin{aligned} \theta_\chi^\phi &= \sum_{a=1}^{12} \chi(a) \cdot ([2, a]^\phi + [2, 1 + a]^\phi + [1 + a, 2a]^\phi + [1, 2a]^\phi \\ &\quad - 2[2, 2a]^\phi - [1, a]^\phi), \end{aligned}$$

où $\theta_\chi^\phi = A_\phi \cdot [1, 2]^\phi + B_\phi \cdot [1, 3]^\phi + C_\phi \cdot [1, -3]^\phi$,

$$\begin{aligned} C_\phi &= [\chi(2)(1 - \phi(4) - \phi(2)) - \chi(3)\phi(2) + \chi(4)\phi(5) \\ &\quad + \chi(5)(\phi(2) + \phi(4)) + 2\chi(6)\phi(2)]. \end{aligned}$$

Si χ est défini par $\chi(2) = \zeta^k$, on a

$$C_\varepsilon = \zeta^k(1 - \zeta^4 - \zeta^2) - \zeta^{4k+2} - \zeta^{2k+3} + \zeta^{9k}(\zeta^4 + \zeta^2) + 2\zeta^{5k+2}.$$

Ce terme étant non nul pour $k = 2, 4, 6, 8, 12$, $\theta_\chi^\varepsilon \neq 0$ pour χ pair. De même $C_{\bar{\varepsilon}} \neq 0$ montre que $\theta_\chi^{\bar{\varepsilon}} \neq 0$ pour χ pair.

Ceci termine la preuve de la finitude de $J_1(13)(\mathbb{Q}(\mu_{13}))$ (c'est-à-dire du lemme 1). ■

1.2. Fin de la preuve de la proposition 1. Comme nous l'avons signalé au début de cette section, le groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$ étant fini et contenant $C_1 \oplus C_2$ (voir 1.1), il suffit maintenant de montrer le lemme 2 pour achever la preuve de la proposition 1.

Preuve du lemme 2. Soient p un nombre premier distinct de 13 et \mathfrak{p} un idéal de $\mathbb{Z}[\mu_{13}]$ au-dessus de p . Notons k_p (resp. $f_p = [k_p : \mathbb{F}_p]$) le corps (resp. le degré) résiduel en \mathfrak{p} de $\mathbb{Z}[\mu_{13}]$, \bar{k}_p une clôture algébrique de k_p , et

$\phi_p \in \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ un endomorphisme de Frobenius en p . Le modèle de Néron $\mathcal{J}_1(13)$ sur \mathbb{Z} de $J_1(13)$ a bonne réduction modulo p . Par conséquent, pour tout nombre premier l distinct de p , on a

$$J_1(13)(\mathbb{Q}(\mu_{13}))[l] \hookrightarrow J_1(13)(k_p)[l].$$

Or $J_1(13)(k_p)[l]$ est l'ensemble des invariants sous $\phi_p^{f_p}$ de $J_1(13)(\overline{k}_p)[l]$ muni de sa structure de module galoisien. Montrons que pour $l \neq 19$ cet ensemble se réduit à $\{0\}$.

Pour $l \neq 2$, le $\mathbb{T}/l\mathbb{T}$ -module $J_1(13)(\overline{k}_p)[l]$ est libre de rang 2 (se reporter à [13, théorème 3.4, corollaire 2]), et la relation d'Eichler–Shimura dans $\text{End}_{\mathbb{T}}(J_1(13)(\overline{k}_p)[l])$ (voir par exemple [12, théorème 2])

$$\phi_p^2 - T_p\phi_p + p\langle p \rangle = 0$$

permet de trouver un polynôme $P_p \in \mathbb{T}/l\mathbb{T}[X]$ annihilant $\phi_p^{f_p}$. Si le $\mathbb{T}/l\mathbb{T}$ -module $J_1(13)(\overline{k}_p)[l]$ admettait des invariants sous $\phi_p^{f_p}$ alors 1 serait racine de P_p . Un choix judicieux de p permet de conclure. Nous utiliserons également le fait que $\mathbb{T} \cong \mathbb{Z}[Y]/\Phi_6(Y)$ en niveau 13 ([5]).

Choisissons d'abord $p = 3$. Soit l premier, $l \neq 2, 3$. On a $f_3 = 3$, et un calcul montre que le polynôme suivant annule ϕ_3^3 :

$$P_3 = X^2 + (9\langle 3 \rangle T_3 - T_3^3)X + 27\langle 3 \rangle^3.$$

Dans $\mathbb{T}/l\mathbb{T} \cong \mathbb{F}_l[Y]/\overline{\Phi}_6(Y)$, T_3 s'écrit $2Y - 2$ et $\langle 3 \rangle = Y$ ([5]), donc

$$P_3(1) = 1 + 9Y(2Y - 2) + 27Y^3 = 2 \times 19.$$

On en déduit que, pour $l \neq 2, 3, 19$, on a $J_1(13)(\mathbb{Q}(\mu_{13}))[l] = \{0\}$.

Soit maintenant $p = 5$ et $l \neq 2, 5$. On a $f_5 = 4$ et ϕ_5^4 est annulé par

$$P_5 = X^2 + (20\langle 5 \rangle T_5^2 - T_5^4 - 50\langle 5 \rangle^2)X + 625\langle 5 \rangle^4.$$

Dans $\mathbb{T}/l\mathbb{T} \cong \mathbb{F}_l[Y]/\overline{\Phi}_6(Y)$, $T_5 = -2Y + 1$ et $\langle 5 \rangle = -1$, donc

$$P_5(1) = 627 = 3 \times 11 \times 19,$$

et pour $l \neq 2, 3, 5, 11, 19$, on a $J_1(13)(\mathbb{Q}(\mu_{13}))[l] = \{0\}$.

Les choix de p qui précèdent montrent que, pour $l \neq 2, 3, 19$, on a $J_1(13)(\mathbb{Q}(\mu_{13}))[l] = \{0\}$. Pour le cas $l = 3$, choisissons $p = 79$. On a $f_{79} = 1$ car $79 \equiv 1 \pmod{13}$. Le polynôme $P_{79} = X^2 - T_{79}X + 79\langle 79 \rangle$ annule ϕ_{79} . Dans $\mathbb{T}/3\mathbb{T} \cong \mathbb{F}_3[Y]/\overline{\Phi}_6(Y)$, on a $T_{79} = 4$, $\langle 79 \rangle = 1$, donc $P_{79}(1) = 76$. Or $76 \not\equiv 0 \pmod{3}$, donc $J_1(13)(\mathbb{Q}(\mu_{13}))[3] = \{0\}$.

Examinons le cas de la 2-torsion. Considérons ϕ_5^4 sur le \mathbb{F}_2 -espace vectoriel $J_1(13)(\overline{\mathbb{F}}_5)[2]$ de dimension 4. Le polynôme

$$P_5 = X^2 + X + 1 \in \mathbb{F}_2[X] \subset \mathbb{T}/2\mathbb{T}[X] \cong \mathbb{F}_4[X]$$

annule ϕ_5^4 et n'admet pas 1 pour racine. Donc $J_1(13)(\mathbb{Q}(\mu_{13}))[2] = \{0\}$.

Terminons par le cas de la 19-torsion. On a

$$(\mathbb{Z}/19\mathbb{Z})^2 \cong C_1 \oplus C_2 \subset J_1(13)(\mathbb{Q}(\mu_{13}))[19].$$

D'autre part, le calcul de la borne de Weil pour $J_1(13)(\mathbb{F}_{3^3})$ donne

$$|J_1(13)(\mathbb{F}_{3^3})| \leq 1587.$$

Or $19^3 > 1587$, donc $|J_1(13)(\mathbb{F}_{3^3})[19^\infty]| = 19^k$ avec $k \leq 2$. On en déduit que $|J_1(13)(\mathbb{Q}(\mu_{13}))[19]| = |J_1(13)(\mathbb{Q}(\mu_{13}))[19^\infty]| = 19^2$. ■

2. Borne pour le cardinal de $Y_1(13)(\mathbb{Q}(\mu_{13}))$

2.1. Revêtement de degré 2 de $X_1(13)$ et conséquences

LEMME 6. Soit $(i, j) \in \{1, \dots, 6\}^2$. Aucune fonction rationnelle sur $X_1(13)$ n'a pour diviseur des pôles $P_i + Q_j$.

Preuve. Considérons la courbe modulaire $X_2(13)$ associée au sous-groupe d'indice 3 de $\Gamma_0(13)$ suivant :

$$\Gamma_2(13) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(13) : a^2 \equiv \pm 1 \pmod{13} \right\}.$$

Cette courbe est de genre nul et induit les revêtements

$$X_1(13) \xrightarrow{2} X_2(13) \xrightarrow{3} X_0(13).$$

Notons $f : X_1(13) \rightarrow X_2(13)$, et σ_5 l'élément de $\Gamma_0(13)$ congru à $\begin{pmatrix} \bar{5}^{-1} & 0 \\ 0 & \bar{5} \end{pmatrix}$ modulo 13. Comme $\bar{5}^2 \equiv -1 \pmod{13}$, on a $\sigma_5 \in \Gamma_2(13)$. D'autre part, σ_5 agit sur les pointes de $X_1(13)$ par

$$\sigma_5.P_i = \Gamma.\frac{13}{5i}, \quad \sigma_5.Q_j = \Gamma.\frac{5j}{13}.$$

Donc $f(P_1) = f(P_5)$, $f(P_2) = f(P_3)$, $f(P_4) = f(P_6)$, $f(Q_1) = f(Q_5)$, $f(Q_2) = f(Q_3)$, $f(Q_4) = f(Q_6)$ sont des pointes de $X_2(13)$.

Soit ψ un isomorphisme de $X_2(13)$ sur \mathbb{P}^1 qui envoie la pointe $f(P_1)$ sur $\infty \in \mathbb{P}^1$. La fonction $\tilde{f} = \psi \circ f$ est un revêtement de degré 2 de $X_1(13)$ sur \mathbb{P}^1 . Ce qui précède montre que la fonction rationnelle sur $X_1(13)$ induite par \tilde{f} admet pour diviseur des pôles

$$P_1 + P_5 \sim P_2 + P_3 \sim P_4 + P_6 \sim Q_1 + Q_5 \sim Q_2 + Q_3 \sim Q_4 + Q_6.$$

Une fonction rationnelle de diviseur des pôles $P_i + Q_j$, $(i, j) \in \{1, \dots, 6\}^2$, induirait un revêtement de degré 2 de $X_1(13)$ sur \mathbb{P}^1 distinct de \tilde{f} , ses fibres au-dessus de ∞ étant distinctes. L'unicité d'un tel revêtement pour les courbes de genre 2 interdit cette éventualité. ■

2.2. Borne

PROPOSITION 2. Le cardinal de $Y_1(13)(\mathbb{Q}(\mu_{13}))$ est inférieur ou égal à 12^2 .

Preuve. Rappelons que $J_1(13)(\mathbb{Q}(\mu_{13})) = C_1 \oplus C_2$, avec $C_1 = \langle u_1, \dots, u_6 \rangle \subset J_1(13)(\mathbb{Q})$, $C_2 = W_{13}.C_1 = \langle v_1, \dots, v_6 \rangle$, $u_i = \iota(P_i)$, $v_j = [(Q_j) - (Q_6)]$ pour $1 \leq i, j \leq 6$ (proposition 1). Les résultats de Ogg ([10]) montrent que C_1, C_2 sont des groupes cycliques d'ordre 19, et on a $u_i = a_i u_4$, $v_i = a_i v_4$, $a_i \in \mathbb{Z}/19\mathbb{Z}$, avec $a_1 = 4$, $a_2 = -5$, $a_3 = 6$, $a_4 = 1$, $a_5 = -3$, $a_6 = 0$, où on note encore n la classe d'un entier n dans $\mathbb{Z}/19\mathbb{Z}$.

En particulier, il existe $(a, b) \in (\mathbb{Z}/19\mathbb{Z})^2$ tels que

$$\iota(Q_6) = [(Q_6) - (P_6)] = au_4 + bv_4.$$

Or $W_{13}.\iota(Q_6) = -\iota(Q_6) = bu_4 + av_4$, donc $b = -a$ dans $\mathbb{Z}/19\mathbb{Z}$. De plus, d'après 2.1, on a $P_4 + P_6 \sim Q_4 + Q_6$, donc $2\iota(Q_6) = u_4 - v_4 = 2au_4 - 2av_4$. On en déduit que $a = -9$ et $\iota(Q_6) = -9u_4 + 9v_4$.

Soit maintenant P dans $Y_1(13)(\mathbb{Q}(\mu_{13}))$. Notons $u = \iota(P)$ et soient $(\mu, \nu) \in (\mathbb{Z}/19\mathbb{Z})^2$ tels que $u = \mu u_4 + \nu v_4$. Ogg montre que $C_1 \cap \iota(Y_1(13)) = \emptyset$. On en déduit que $\nu \neq 0$. D'autre part, si $\mu = -9$, on a $u = \iota(Q_6) + (\nu - 9)v_4$, donc $[(P) - (Q_6)] \in C_2$, c'est-à-dire $\iota(W_{13}.P) \in C_1 \cap \iota(Y_1(13))$. Ceci étant impossible, $\mu \neq -9$.

Supposons qu'il existe i, j, k dans $\{1, \dots, 6\}$ tels que $u = u_i + v_j - v_k$. On aurait alors $P + Q_k \sim P_i + Q_j$, ce qui est impossible d'après 2.1. La différence $a_j - a_k$ décrivant $\mathbb{Z}/19\mathbb{Z}$ lorsque j, k décrivent $\{1, \dots, 6\}$, ceci impose $\mu \neq 0, 1, 4, 6, -3, -5$. De même, on montre que $u \neq u_i - u_k + v_j + \iota(Q_6)$, ce qui impose $\nu \neq 9, -9, 6, -6, 4, -4$.

Les contraintes précédentes sur (μ, ν) montrent la proposition. ■

3. Preuve du théorème. Il s'agit de montrer que $Y_1(13)(\mathbb{Q}(\mu_{13}))$ est vide. Procédons par l'absurde : soit (E, π) un point de $Y(13)(\mathbb{Q}(\mu_{13}))$, où E est une courbe elliptique définie sur $\mathbb{Q}(\mu_{13})$ et π est un plongement $(\mathbb{Z}/13\mathbb{Z})^2 \rightarrow E[13]$. Un tel point donne lieu à $(13^2 - 1)/2 = 84$ points de $Y_1(13)(\mathbb{Q}(\mu_{13}))$. Notons $\mathcal{P}_{(E, \pi)}$ cet ensemble de points. Supposons que pour tout x de $\mathcal{P}_{(E, \pi)}$, $W_{13}.x$ n'est pas dans $\mathcal{P}_{(E, \pi)}$. Alors le sous-ensemble $\mathcal{P}_{(E, \pi)} \cup W_{13}.\mathcal{P}_{(E, \pi)}$ de $Y_1(13)(\mathbb{Q}(\mu_{13}))$ est de cardinal $2 \times 84 = 168 > 12^2$, ce qui est impossible d'après la proposition 2.

Par conséquent, il existe $x \in \mathcal{P}_{(E, \pi)}$ tel que $y = W_{13}.x \in \mathcal{P}_{(E, \pi)}$. Autrement dit, il existe P, Q deux points d'ordre 13 de E définis sur $\mathbb{Q}(\mu_{13})$ et un isomorphisme défini sur $\mathbb{Q}(\mu_{13})$ envoyant (E, Q) sur

$$W_{13}.(E, P) = (E/\langle P \rangle, P' + \langle P \rangle),$$

où P' est le point d'ordre 13 de E tel que $e_{13}(P', P) = e^{2i\pi/13}$, l'application $e_{13} : E[13] \times E[13] \rightarrow \mu_{13}$ étant l'accouplement de Weil.

En particulier, on dispose d'une isogénie ψ de E dans E de degré 13 définie sur $\mathbb{Q}(\mu_{13})$. La courbe elliptique E est donc à multiplication complexe. L'ensemble des endomorphismes $\text{End } E$ de E sur \mathbb{C} est isomorphe

à un ordre R d'un corps quadratique imaginaire. Soit $[\cdot] : R \rightarrow \text{End } E$ l'isomorphisme normalisé, et $\alpha \in R$ tel que $\psi = [\alpha]$. L'isogénie $[\alpha]$ étant définie sur $\mathbb{Q}(\mu_{13})$ ainsi que la courbe elliptique E , on a $\alpha \in \mathbb{Q}(\mu_{13})$. Or $13 \equiv 1 \pmod{4}$, donc $\mathbb{Q}(\mu_{13})$ ne contient aucun corps quadratique imaginaire, et donc $\alpha \in \mathbb{Q}$. C'est impossible car sinon, $13 = \deg[\alpha] = |N_{\mathbb{Q}}^K(\alpha)|$ serait un carré. Ceci achève la preuve. ■

4. Remarque. Lorsque j'ai exposé cette démonstration pendant les vingt-deuxièmes Journées Arithmétiques (juin 2001), B. Poonen m'a signalé un résultat de R. F. Coleman qui, en utilisant la finitude du groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$, fournit une borne plus petite du cardinal de $Y_1(13)(\mathbb{Q}(\mu_{13}))$, et simplifie alors la démonstration du théorème.

Rappelons le résultat de Coleman :

THÉORÈME 2 (Coleman, [1]). *Soient C une courbe de genre g définie sur un corps de nombres K , et J sa jacobienne. Supposons que le rang de $J(K)$ soit au plus $g - 1$. Soit \mathcal{P} un idéal non ramifié de K en lequel C a bonne réduction et de caractéristique résiduelle supérieure à $2g$. Notons $f_{\mathcal{P}}$ le degré résiduel en \mathcal{P} . Alors*

$$|C(K)| \leq f_{\mathcal{P}} + 2g(\sqrt{f_{\mathcal{P}}} + 1) - 1.$$

Appliquons ce théorème à $C = X_1(13)$, $K = \mathbb{Q}(\mu_{13})$, $\mathcal{P} | 53$, pour lesquels les hypothèses sont vérifiées, en particulier grâce au lemme 1 qui assure que le rang de $J_1(13)(\mathbb{Q}(\mu_{13}))$ est inférieur à $g - 1 = 1$. On obtient $|X_1(13)(\mathbb{Q}(\mu_{13}))| \leq 85$, donc $|Y_1(13)(\mathbb{Q}(\mu_{13}))| \leq 73$. On raisonne alors par l'absurde comme dans la section 3 : un point de $Y(13)(\mathbb{Q}(\mu_{13}))$ donnerait lieu à 84 points de $Y_1(13)(\mathbb{Q}(\mu_{13}))$, ce qui est impossible d'après ce qui précède.

Références

- [1] R. F. Coleman, *Effective Chabauty*, Duke Math. J. 52 (1985), 765–770.
- [2] J. E. Cremona, *Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction*, Math. Proc. Cambridge Philos. Soc. 111 (1992), 199–218.
- [3] F. Diamond and J. Im, *Modular forms and modular curves*, dans : Seminar on Fermat's Last Theorem, vol. 17, Toronto, ON, 1993-1994, 39–133.
- [4] K. Kato, *p -adic Hodge theory and values of zeta functions of modular forms*, à paraître.
- [5] J.-C. Lario and J. Quer, *Table of some Hecke operator's eigenvalues*, non publiée.
- [6] Yu. Manin, *Parabolic points and zeta function of modular curves*, Math. USSR-Izv. 6 (1972), 19–64.
- [7] L. Merel, *Sur la nature non cyclotomique des points d'ordre fini des courbes elliptiques*, Duke Math. J. 110 (2001), 81–119.
- [8] —, *Universal Fourier expansions of modular forms*, dans : On Artin's Conjecture for Odd 2-Dimensional Representations, Lecture Notes in Math. 1585, Springer, 1994, 59–94.

- [9] L. Merel and W. Stein, *The field generated by the points of small prime order on an elliptic curve*, Internat. Math. Res. Notices 2001, no. 20, 1075–1082.
- [10] A. P. Ogg, *Rational points on certain elliptic modular curves*, mimeographed notes, Berkeley, St. Louis, 1972.
- [11] P. Parent, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier (Grenoble) 50 (2000), 723–749.
- [12] D. E. Rohrlich, *Modular curves, Hecke correspondences, and L-functions*, dans : Modular Forms and Fermat's Last Theorem, G. Cornell, J. H. Silverman and G. Stevens (eds.), Springer, 1997, 41–100.
- [13] J. Tilouine, *Hecke algebras and the Gorenstein property*, *ibid.*, 327–342.

Université Paris VI
175 rue du Chevaleret
75013 Paris, France
E-mail: rebolledo@math.jussieu.fr

Reçu le 3.12.2001

(4165)