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

Marusia Rebolledo Hochart

September 30, 2002

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 $\bar{\mathbb{Q}}$ 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 $J_1(13)(\mathbb{Q}(\mu_{13}))$, permet de borner le cardinal de

*2000 Mathematics Subject Classification. Primary 11F, 11G, 14G.

$Y_1(13)(\mathbb{Q}(\mu_{13}))$. On raisonne alors par l'absurde : l'image d'un point de $Y(13)(\mathbb{Q}(\mu_{13}))$ par le revêtement $X(13) \longrightarrow X_1(13)$ fournirait "trop" de points de $Y_1(13)(\mathbb{Q}(\mu_{13}))$.

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 $\begin{pmatrix} \star & \star \\ 0 & \star \end{pmatrix}$ et $\begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix}$ modulo 13. Nous noterons $S = S_2(\Gamma_1(13))$ l'espace des formes modulaires paraboliques de poids 2 pour $\Gamma_1(13)$. Pour $\phi : (\mathbb{Z}/13\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ 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 $\bar{\mathcal{H}}$, où $\bar{\mathcal{H}} = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$, $\mathcal{H}$ étant le demi-plan de Poincaré.

J1(Q(mu13))

1 Etude du groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$

Rappelons que deux pointes $\alpha_i = \frac{p_i}{q_i}$, $i = 1, 2$, $\mathrm{pgcd}(p_i, q_i) = 1$, sont équivalentes modulo $\Gamma = \Gamma_1(13)$ si et seulement si $q_2 = \lambda q_1 \pmod{13}$, $p_2 = \lambda p_1 \pmod{\mathrm{pgcd}(q_1, 13)}$ où $\lambda = \pm 1$ (voir [2]). De plus les pointes 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 comme $\begin{pmatrix} \sigma & 0 \\ 0 & 1 \end{pmatrix}$. 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 :

$$\iota : \begin{cases} X_1(13) \longrightarrow J_1(13) \\ P \mapsto [(P) - (P_6)] \end{cases}$$

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 : $C_1 = \langle u_1, ..u_6 \rangle$, où $u_i = \iota(P_i)$, $1 \leq i \leq 6$, est cyclique d'ordre 19. Par conséquent, le sous-groupe $C_2 = W_{13}.C_1 = \langle v_1, ..v_6 \rangle$, où $v_j = [(Q_j) - (Q_6)]$, $1 \leq j \leq 6$, l'est également. Ces deux groupes d'ordre 19, distincts pour des raisons de rationnalité, 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 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 $\epsilon, \bar{\epsilon}$ 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 $\epsilon(2) = \zeta^2$, $\bar{\epsilon}(2) = \zeta^{-2}$. On a $S = S_2(13, \epsilon) \oplus S_2(13, \bar{\epsilon})$, et les $\mathbb{C}$-espaces vectoriels $S_2(13, \epsilon)$ et $S_2(13, \bar{\epsilon})$ sont de dimension 1 engendrés chacun par une forme primitive f_ϵ et $f_{\bar{\epsilon}}$ 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 :

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

Pour prouver la finitude du groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$, il suffit alors de prouver que la condition (C_1) suivante est satisfaite :

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

Pour $\chi:(\mathbb{Z}/13\mathbb{Z})^\times\longrightarrow\mathbb{C}^\times$, notons $\tau(\chi)=\sum_{b \bmod 13}\chi(b)e^{-\frac{2i\pi\tilde b}{13}}$. La formule :

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

nous conduit à utiliser les symboles modulaires. Nous allons énoncer une condition (C_2) sur certains symboles modulaires, qui entraîne (C_1) 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 $\Gamma\backslash\bar{\mathcal{H}}$, où $\bar{\mathcal{H}}=\mathcal{H}\cup\mathbb{P}^1(\mathbb{Q})$, $\mathcal{H}$ 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. $H_1(X,ptes;\mathbb{Z})$) l'homologie singulière absolue (resp. relative à l'ensemble $\{ptes\}$ 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 $H_1(X,ptes;\mathbb{Z})$ de l'image d'une géodésique reliant α à β.

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

$$(*)\qquad 0\to H\to H'\xrightarrow{\delta}\mathbb{C}[ptes]\xrightarrow{\deg}\mathbb{C}\to 0,$$

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 :

$$\xi : \begin{cases} \mathbb{C}[\Gamma\backslash SL_2(\mathbb{Z})] \longrightarrow H' \\ [\Gamma.g] \mapsto \{g0, g\infty\} = \{b/d, a/c\} \end{cases}, \text{ avec } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

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 $x \in \Gamma\backslash SL_2(\mathbb{Z})$, et $\sigma,\ \tau$ des éléments de $SL_2(\mathbb{Z})$ d'ordre respectif 4 et 3 :

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

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 $\Gamma\backslash SL_2(\mathbb{Z})$ 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 $SL_2(\mathbb{Z})$ 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 $\langle m\rangle' : t'.\{\alpha, \beta\} = \{t.\alpha, t.\beta\}$, où $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$, $t = T_n$ ou $\langle m\rangle$. Soit $\mathbb{T}'$ la sous-algèbre de 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 :

$$\theta_\chi = t_\chi . \sum_{a \bmod 13} \chi(a).[1, a] \qquad \text{avec } t_\chi = \begin{cases} 1 & \text{si } \chi \text{ est impair,} \\ (T'_2 - 2\langle 2\rangle' - 1) & \text{si } \chi \text{ est pair.} \end{cases}$$

Lemme 3 *La condition (C_2) suivante entraîne la condition (C_1) et donc la finitude du groupe $J_1(13)(\mathbb{Q}(\mu_{13}))$:*

$$(C_2) \qquad \forall \chi : (\mathbb{Z}/13\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times,\ \theta_\chi^\epsilon \neq 0,\ \theta_\chi^{\bar{\epsilon}} \neq 0.$$

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

On a $\delta(\theta_\chi) = \delta(t_\chi . \sum_{a \bmod 13} \chi(a).\{\frac{-1}{\tilde{a}}, 0\}) = -\sum_{a \bmod 13} \chi(a)(t_\chi(\Gamma.\frac{-1}{\tilde{a}}))$. Or $\Gamma.(\frac{-1}{\tilde{a}}) = \Gamma.\frac{1}{\tilde{a}} = \Gamma.(\frac{-1}{-\tilde{a}})$, donc pour χ impair, $\delta(\theta_\chi) = -\sum_{k=1}^{6}(\chi(\bar{k}) + \chi(-\bar{k}))(\Gamma.\frac{1}{k}) = 0$. Pour χ pair, un calcul montre que $t_\chi(\Gamma.\frac{1}{\tilde{a}}) = 0$ ([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 : :

$$\begin{cases} H \longrightarrow \mathrm{Hom}_{\mathbb{C}}(H^0(X, \Omega^1_X), \mathbb{C}) \\ c \mapsto (\omega \mapsto \int_c \omega) \end{cases}$$

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 $H^0(X, \Omega^1_X)$. Le morphisme qui s'en déduit :

$$F : \begin{cases} H \longrightarrow \mathrm{Hom}_{\mathbb{C}}(S, \mathbb{C}) \\ c \mapsto (f \mapsto \int_c \omega_f) \end{cases}$$

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 $\mathrm{Hom}_{\mathbb{C}}(S, \mathbb{C})$. 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 : $F^{\pm,\phi} : H^{\pm,\phi} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}}(S_2(13, \phi), \mathbb{C})$, pour ϕ caractère modulo 13. D'où $H^\phi = 0$ pour $\phi \neq \epsilon$, $\bar{\epsilon}$, et $H = H^\epsilon \oplus H^{\bar{\epsilon}}$.

Soient $c_\chi = \sum_{a \bmod 13} \bar{\chi}(a)\{\frac{\tilde{a}}{13}, \infty\} \in H'$, $f \in S$, et $\chi : (\mathbb{Z}/13\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$. On a :

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

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

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

Or

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

où $t_\chi^* . f_{\bar\epsilon} = \lambda_\chi . f_{\bar\epsilon},\ \lambda_\chi \in \mathbb{C}$.

Ceci prouve que si $\theta_\chi^\epsilon \neq 0$ alors $L(f_{\bar\epsilon}, \bar\chi, 1) \neq 0$. De même, si $\theta_\chi^{\bar\epsilon} \neq 0$ alors $L(f_\epsilon, \bar\chi, 1) \neq 0$.

□

1.1.2 Vérification de la condition (C_2)

Nous allons faire les calculs dans les composantes H'^{ϵ}, $H'^{\bar\epsilon}$ de H', espace pour lequel nous disposons de la présentation de Manin. Pour cela nous allons déterminer une base de H'^{ϵ} (resp. $H'^{\bar\epsilon}$) et exprimer θ_χ^ϵ (resp. $\theta_\chi^{\bar\epsilon}$) 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* $\phi = \epsilon$ *ou* $\bar\epsilon$*, et* 2 *sinon.*

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

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

Notons $[u, v]^\phi$ l'image de $[u, v]$ dans H'^{ϕ}. Pour $u \neq 0$ dans $\mathbb{Z}/13\mathbb{Z}$, $[u, v]^\phi = \phi(u).[1, vu^{-1}]^\phi$, et $[0, v]^\phi = \phi(v).[0, 1]^\phi$. 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* $\phi = \epsilon$ *ou* $\bar\epsilon$*. Dans cette base, les générateurs* $[0, 1]^\phi,\ [1, w]^\phi,\ w \in \mathbb{Z}/13\mathbb{Z}$ *s'écrivent respectivement:*

$[0, 1]^\phi = -[1, 0]^\phi$ $\quad$ $[1, 1]^\phi = [1, -1]^\phi = 0$

$[1, -2]^\phi = [1, 2]^\phi$ $\quad$ $[1, 6]^\phi = [1, -6]^\phi = -\phi(6).[1, 2]^\phi$

$[1, 4]^\phi = -\phi(4).[1, 3]^\phi$ $\quad$ $[1, -4]^\phi = -\phi(4).[1, -3]^\phi$

$[1, 5]^\phi = \phi(6).[1, 3]^\phi - \phi(6).[1, 2]^\phi$ $\quad$ $[1, -5]^\phi = \phi(4).[1, 2]^\phi - \phi(4).[1, -3]^\phi$

Pour χ impair, on a alors :

$$\theta_\chi^\epsilon = (\chi(3)-\chi(4)\epsilon(4)+\chi(5)\epsilon(6)).[1,3]^\epsilon+(-\chi(3)+\chi(4)\epsilon(4)+\chi(5)\epsilon(4)).[1,-3]^\epsilon.$$

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 : $-\chi(3)+\chi(4)\epsilon(4)-\chi(5)\epsilon(6) = -\zeta^{4k}+\zeta^{2k+4}-\zeta^{9k+10}$. Ce terme est non nul pour $k=1,3,5,7,9,11$, donc θ_χ^ϵ et $\theta_\chi^{\bar\epsilon} = \theta_{\bar\chi}^\epsilon$ sont non nuls pour χ impair.

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

$\theta_\chi^\epsilon = \sum_{a=1}^{12}\chi(a).([2,a]^\epsilon+[2,1+a]^\epsilon+[1+a,2a]^\epsilon+[1,2a]^\epsilon-2[2,2a]^\epsilon-[1,a]^\epsilon)$
$\theta_\chi^\epsilon = A.[1,2]^\epsilon+B.[1,3]^\epsilon+C.[1,-3]^\epsilon$
où
$B = [-2\chi(2)\epsilon(4)-\chi(3)\epsilon(2)-\chi(4)+\chi(5)(\epsilon(2)+\epsilon(4))+\chi(6)(1+\epsilon(2)+\epsilon(4))]$
$C = [\chi(2)(1-\epsilon(4)-\epsilon(2))-\chi(3)\epsilon(2)+\chi(4)\epsilon(5)+\chi(5)(\epsilon(2)+\epsilon(4))+2\chi(6)\epsilon(2)]$

Lorsque $\chi(2)=\zeta^k$, on a $C = \zeta^k(1-\zeta^4-\zeta^2)-\zeta^{4k+2}-\zeta^{2k+3}+\zeta^{9k}(\zeta^4+\zeta^2)+2\zeta^{5k+2}$. Ce terme étant non nul pour $k=2,4,6,8,12$, θ_χ^ϵ et $\theta_\chi^{\bar\epsilon}$ sont non nuls 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 I.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 $\underline{k_p}$ (resp. $f_p = [k_p : \mathbb{F}_p]$) le corps (resp. le degré) résiduel en $\mathfrak{p}$ de $\mathbb{Z}[\mu_{13}]$, $\overline{k_p}$ une clôture algébrique de k_p et $\phi_p \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ 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 stucture 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 $\mathrm{End}_{\mathbb{T}}(J_1(13)(\overline{k_p})[l])$ (voir par exemple [12], théorème 2) :

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

permet de trouver un polynôme $P_p \in \mathbb{T}/l\mathbb{T}[X]$ annulant $\phi_p^{f_p}$. 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 $\mathbb{T} \cong \mathbb{Z}[Y]/\Phi_6(Y)$ ([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 $l \neq 2, 3, 19$, $J_1(13)(\mathbb{Q}(\mu_{13}))[l] = \{0\}$.
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 $l \neq 2, 3, 5, 11, 19$, $J_1(13)(\mathbb{Q}(\mu_{13}))[l] = \{0\}$.
Les choix de p qui précèdent montrent que pour $l \neq 2, 3, 19$, $J_1(13)(\mathbb{Q}(\mu_{13}))[l] = \{0\}$. 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 $\mathbb{T}/3\mathbb{T} \cong \mathbb{F}_3[Y]/\overline{\Phi_6}(Y)$, $T_{79} = 4$, $\langle 79\rangle = 1$, donc $P_{79}(1) = 76$. Or $76 \not\equiv 0 \bmod 3$, 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 $(i,j) \in \{1,\ldots,6\}^2$. 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 : $\Gamma_2(13) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(13),\ a^2 \equiv \pm 1 \pmod{13}\}$. Cette courbe est de genre nul et induit les revêtements :

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

Notons $f : X_1(13) \longrightarrow X_2(13)$, 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 $\bar{5}^2 \equiv -1 \pmod{13}$, $\sigma_5 \in \Gamma_2(13)$. D'autre part, σ_5 agit sur les pointes de $X_1(13)$ par :

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

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 $P_i + Q_j$, $(i,j) \in \{1,..6\}^2$, 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 $C_1 = \langle u_1, ..u_6 \rangle \subset J_1(13)(\mathbb{Q})$, $C_2 = W_{13}.C_1 = \langle v_1, ..v_6 \rangle$, $u_i = \iota(P_i)$, $v_j = [(Q_j) - (Q_6)]$, $1 \leq i,\ j \leq 6$ (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 $(\mu,\nu) \in (\mathbb{Z}/19\mathbb{Z})^2$ 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 maintenant qu'il existe i,j,k dans $\{1,..6\}$ 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 $\{1,..6\}$, 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 les valeurs de (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 un plongement : $\pi : (\mathbb{Z}/13\mathbb{Z})^2 \longrightarrow E[13]$. Un tel point donne lieu à $\frac{13^2-1}{2} = 84$ 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 $\mathcal{P}_{(E,\pi)}$. Le sous-ensemble $\mathcal{P}_{(E,\pi)} \cup W_{13}.\mathcal{P}_{(E,\pi)}$ de $Y_1(13)(\mathbb{Q}(\mu_{13}))$ est alors 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 $e_{13}(P',P) = e^{2i\pi/13}$, $e_{13} : E[13] \times E[13] \longrightarrow \mu_{13}$ 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 End E de E sur $\mathbb{C}$ est isomorphe à un ordre R d'un corps quadratique imaginaire. Soit $[.] : R \longrightarrow$ 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, $13 = \deg[\alpha] = \mid N_{\mathbb{Q}}^K(\alpha) \mid$ 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 les résultats de Coleman :

Théorème 2 (Coleman - 1985, [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.

References

[1] R. F. Coleman. Effective chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[2] J. E. Cremona. Modular symbols for $\gamma_1(n)$ and elliptic curves with everywhere good reduction. *Math. Proc. Camb. Phil. Soc.*, III(2):199–218, 1992.

[3] F. Diamond and J. Im. Modular forms and modular curves. In CMS Conf. Proc, editor, *Seminar on Fermat's last theorem*, volume 17, pages 39–133. Toronto, ON, 1993-1994.

[4] Kato. p-adic hodge theory and values of zeta functions of modular forms.

[5] J.-C. Lario and J. Quer. Table of some hecke operator's eigenvalues. Non publiée.

[6] Y. Manin. Parabolic points and zeta function of modular curves. *Math. USSR Isv.*, 6:19–64, 1972.

[7] L. Merel. Sur la nature non cyclotomique des points d'ordre fini des courbes elliptiques. A paraître dans Duke Math. Journal.

[8] L. Merel. Universal fourier expansions of modular forms. In Lectures Notes in Math, editor, *On Artin's conjecture for odd 2-dimensional representations*, volume 1585, pages 59–94. Springer, 1994.

[9] L. Merel and W. Stein. The field generated by the points of small prime order on an elliptic curve. A paraître dans IRMN.

[10] A. P. Ogg. Rational points on certain elliptic modular curves. Mimeographed notes, Berkeley, St. Louis, 1972. AMS.

[11] P. Parent. Torsion des courbes elliptiques sur les corps cubiques. *Ann. Inst. Fourier Grenoble*, 50(3):723–749, 2000.

[12] D. E. Rohrlich. Modular curves, hecke correspondences, and l-functions. In Cornell, Silverman, and Stevens, editors, *Modular forms and Fermat's last theorem*, pages 41–100. Springer, 1997.

[13] J. Tilouine. Hecke algebras and the gorenstein property. In Cornell, Silverman, and Stevens, editors, *Modular forms and Fermat's last theorem*, pages 327–342. Springer, 1997.