Bornes pour la torsion des courbes elliptiques sur les corps de nombres

Loïc Merel

Introduction

Ce texte fournit la preuve de l'assertion suivante.

Théorème. — *Soit* E *une courbe elliptique, définie sur un corps de nombres* K *de degré* $d > 1$ *sur* $\mathbf{Q}$. *Si* E(K) *possède un point d'ordre premier* p, *on a* $p < d^{3d^2}$.

Mentionnons un corollaire de ce théorème (voir [3] ou [9]), reposant sur des résultats de Faltings et Frey ([4] , [5]).

Corollaire. — *Soit* d *un entier* ≥ 1. *Il existe un nombre réel* $\mathrm{B}(d)$ *tel que pour toute courbe elliptique* E, *définie sur un corps de nombres* K *de degré* d *sur* $\mathbf{Q}$, *tout point de torsion de* E(K) *soit d'ordre* $\leq \mathrm{B}(d)$. *Ou de façon équivalente, il n'existe qu'un nombre fini, à isomorphisme près, de groupes qui sont la partie de torsion du groupe de Mordell-Weil d'une courbe elliptique définie sur une extension de* $\mathbf{Q}$ *de degré* d.

Une borne explicite est fournie dans le théorème uniquement pour assurer du caractère concret de notre résultat. Oesterlé semble être en mesure de remplacer l'expression d^{3d^2} par $(1 + 3^{d/2})^2$ dans l'énoncé du théorème. La borne $B(d)$ ne semble pas pouvoir être calculée par la méthode de Kamienny, Mazur et Frey.

Le principe de la démonstration devrait apparaître clairement dans le texte. Soulignons seulement que nous reprenons la méthode inventée par Mazur et généralisée par Kamienny [7] en remplaçant le"quotient d'Eisenstein" par le "quotient d'enroulement" (voir §1), qui est une variété abélienne définie sur $\mathbf{Q}$ quotient de la jacobienne de la courbe modulaire $\mathrm{X}_0(p)$ et de groupe de Mordell-Weil fini. Ce dernier point est suggéré par la conjecture de Birch et Swinnerton-Dyer et confirmé par un théorème de Kolyvagin et Logachev.

Ajoutons que les lemmes 1, 2, 3 et 4 sont présents dans ma thèse mais j'ai préféré donner toutes les démonstrations nécessaires plutôt que faire appel à des résultats non publiés.

§0. Préliminaires

Soit p un nombre premier. Notons $\Gamma_0(p)$ le sous-groupe de $\mathrm{SL}_2(\mathbf{Z})$ formé des matrices $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ telles que p divise γ. Ce groupe opère sur le demi-plan de Poincaré $\mathcal{H}$. Notons $\mathrm{Y}_0(p)$ la surface de Riemann quotient $\Gamma_0(p)\backslash\mathcal{H}$. Elle est munie d'une structure de courbe algébrique sur $\mathbf{Q}$ dont les points K-rationnels, pour K extension de $\mathbf{Q}$, classifient à $\bar{\mathrm{K}}$-isomorphisme près les couples (E, C), où E est une courbe elliptique définie sur K et C est un sous groupe cyclique d'ordre p de E défini sur K. Notons $\mathrm{X}_0(p)$ la courbe complète obtenue en adjoignant l'ensemble des pointes $\Gamma_0(p)\backslash\mathbf{P}^1(\mathbf{Q}) = \{\Gamma_0(p)0, \Gamma_0(p)\infty\}$ à $\mathrm{Y}_0(p)$. Notons $\mathrm{J}_0(p)$ la variété jacobienne de $\mathrm{X}_0(p)$. Notons $\mathbf{S}$ l'espace des formes modulaires paraboliques de poids 2 pour $\Gamma_0(p)$. Notons $\mathbf{H} = \mathrm{H}_1(\mathrm{X}_0(p); \mathbf{Z})$, $\tilde{\mathbf{H}} = \mathrm{H}_1(\mathrm{X}_0(p), \mathrm{X}_0(p) - \mathrm{Y}_0(p); \mathbf{Z})$, $\tilde{\mathbf{H}}' = \mathrm{H}_1(\mathrm{Y}_0(p); \mathbf{Z})$ et $\mathbf{H}^+$ la partie invariante de $\mathbf{H}$ par l'action de la conjugaison complexe. Pour r nombre entier positif et premier à p, notons T_r la correspondance analytique sur $\mathrm{X}_0(p)$ qui à $\Gamma_0(p)z$ associe $\sum \Gamma_0(p)\frac{(r/\delta)z-\beta}{\delta}$, où δ parcourt les diviseurs > 0 de r, et β parcourt les entiers $0, 1, \ldots, \delta - 1$. Notons W_p l'automorphisme analytique de $\mathrm{X}_0(p)$ qui à $\Gamma_0(p)z$ associe $\Gamma_0(p)\frac{-1}{pz}$. Ces correspondances sont définies sur $\mathbf{Q}$ et définissent des endomorphismes encore notés T_r et W_p de $\mathrm{J}_0(p)$. Notons $\mathbf{T}$ le sous-anneau commutatif de $\mathrm{End}(\mathrm{J}_0(\mathrm{p}))$ engendré par les opérateurs de Hecke et l'involution d'Atkin-Lehner. C'est l'*algèbre de Hecke*, elle opère fidèlement sur $\mathrm{J}_0(p)$, $\mathbf{H}$ et $\mathbf{S}$. De plus $\mathbf{S}$ est un $\mathbf{T} \otimes \mathbf{C}$-module libre de rang 1 et $\mathbf{H}^+ \otimes \mathbf{Q}$ est $\mathbf{T} \otimes \mathbf{Q}$-module libre de rang 1. Un élément f de $\mathbf{S}$ sera appelé *forme primitive* si on a $\mathbf{T}f \subset \mathbf{C}f$ et si le premier coefficient du développement de Fourier de f en l'infini est égal à 1. Ajoutons que les correspondances de Hecke et l'involution d'Atkin-Lehner définissent des endomorphismes de $\tilde{\mathbf{H}}$ qui étendent l'action des opérateurs de Hecke sur $\mathbf{H}$ lorsqu'on identifie $\mathbf{H}$ à un sous-groupe de $\tilde{\mathbf{H}}$, ce que nous ferons par la suite. Elles définissent également des endomorphismes de $\tilde{\mathbf{H}}'$ compatibles à la surjection canonique $\tilde{\mathbf{H}}' \to \mathbf{H}$.

Pour $(\alpha, \beta) \in \mathbf{P}^1(\mathbf{Q})^2$ la classe dans $\tilde{\mathbf{H}}$ de l'image dans $\mathrm{X}_0(p)$ du chemin géodésique de $\mathbf{H}$ reliant α à β dans $\mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$ sera appelé *symbole modulaire* et noté $\{\alpha, \beta\}$. Lorsque $\Gamma_0(p)\alpha = \Gamma_0(p)\beta$, on a $\{\alpha, \beta\} \in \mathbf{H}$.

On a des accouplements bilinéaires unimodulaires $\mathbf{H} \times \mathbf{H} \to \mathbf{Z}$ et $\tilde{\mathbf{H}} \times \tilde{\mathbf{H}}' \to \mathbf{Z}$, notés $\bullet$, fournis par les produits d'intersection. Les opérateurs de Hecke et l'involution d'Atkin-Lehner sont auto-adjoints pour ces accouplements.

§1. Le quotient d'enroulement $\mathrm{J}_{\mathbf{e}}$ de $\mathrm{J}_0(p)$

La forme linéaire $\omega \mapsto -\int_{\{0,\infty\}} \omega$ de $\mathrm{Hom}_{\mathbf{C}}(\mathrm{H}^0(X_0(p),\Omega^1),\mathbf{C})$ est l'image par l'isomorphisme canonique d'espaces vectoriels réels $\mathbf{H}\otimes\mathbf{R} \to \mathrm{Hom}_{\mathbf{C}}(\mathrm{H}^0(X_0(p),\Omega^1),\mathbf{C})$, qui à $c\otimes 1$ associe $\omega \mapsto \int_c \omega$, d'un élément $\mathbf{e}$ de $\mathbf{H}\otimes\mathbf{R}$, que nous appellerons *élément d'enroulement* (*winding element* dans [12]). En fait on a $(p-1)\mathbf{e} \in \mathbf{H}^+\otimes 1$ ([12]).

Notons $\mathcal{I}_{\mathbf{e}}$ le noyau de l'endomorphisme de $\mathbf{T}$-modules $\mathbf{T} \to \mathbf{H}\otimes\mathbf{Q}$ qui à t associe $t\mathbf{e}$. Notons $\mathcal{I}_{\mathbf{e}}\mathrm{J}_0(p)$ la sous-variété abélienne de $\mathrm{J}_0(p)$ engendrée par l'image de l'application $\mathcal{I}_{\mathbf{e}} \times \mathrm{J}_0(p) \to \mathrm{J}_0(p)$ qui à (t,x) associe tx. On définit alors le *quotient d'enroulement* $\mathrm{J}_{\mathbf{e}}$ de $\mathrm{J}_0(p)$ comme la variété abélienne quotient $\mathrm{J}_0(p)/\mathcal{I}_{\mathbf{e}}\mathrm{J}_0(p)$. C'est une variété abélienne définie sur $\mathbf{Q}$.

Proposition 1. — *Le groupe de Mordell-Weil de* $\mathrm{J}_{\mathbf{e}}$ *est fini.*

Démonstration. — Les $\mathbf{T}\otimes\mathbf{Q}$-modules suivants sont semi-simples et libres de rang 1 : $\mathbf{T}\otimes\mathbf{Q}$, $\mathbf{H}^+\otimes\mathbf{Q}$ et $\mathbf{S}_{\mathbf{Q}}$ (espace des formes modulaires paraboliques de coefficients de Fourier à l'infini rationnels, $\mathbf{S}_{\mathbf{Q}}\otimes\mathbf{C}$ s'identifie canoniquement à $\mathbf{S}$). Soit I un idéal de $\mathbf{T}\otimes\mathbf{Q}$. Notons I_0 l'unique idéal de $\mathbf{T}$ tel que $(\mathrm{I}_0\otimes\mathbf{Q})\oplus\mathrm{I} = \mathbf{T}\otimes\mathbf{Q}$ et qui soit maximal pour cette propriété. Notons J_{I} la variété abélienne (définie sur $\mathbf{Q}$) $\mathrm{J}_0(p)/\mathrm{I}_0\mathrm{J}_0(p)$. On a une isogénie définie sur $\mathbf{Q}$: $\mathrm{J}_{\mathrm{I}} \to \prod_{\mathrm{I}'} \mathrm{J}_{\mathrm{I}'}$, où I' parcourt les sous-$\mathbf{T}\otimes\mathbf{Q}$-modules irréductibles de I. Le groupe $\mathrm{J}_{\mathrm{I}}(\mathbf{Q})$ est fini si chacun des $\mathrm{J}_{\mathrm{I}'}(\mathbf{Q})$ est fini.

Soit I' un sous-$\mathbf{T}\otimes\mathbf{Q}$-module irréductible de I. Alors le groupe $\mathrm{Aut}\mathbf{C}$ opère (via son action sur les coefficients de Fourier) transitivement sur les formes primitives de $\mathrm{I}'\mathbf{S}$. On a, par un théorème de Shimura [17] complété par Carayol [2], $\mathrm{L}(\mathrm{J}_{\mathrm{I}'},s) = \prod \mathrm{L}(f,s)$ où f parcourt les formes primitives de $\mathrm{I}'\mathbf{S}$ et où $\mathrm{L}(f,s) = (2\pi)^s\Gamma(s)^{-1}\int_0^\infty f(iy)y^{s-1}\,dy$. D'après un théorème de Kolyvagin et Logachev [10] (reposant sur les travaux de Gross et Zagier [6] et complété indépendamment par Bump, Friedberg et Hoffstein [1] d'une part et par M.R. Murty et V.K. Murty [14] d'autre part), si on a $\mathrm{L}(\mathrm{J}_{\mathrm{I}'},1) \neq 0$ alors le groupe $\mathrm{J}_{\mathrm{I}'}(\mathbf{Q})$ est fini.

Par conséquent $\mathrm{J}_{\mathrm{I}}(\mathbf{Q})$ est fini si les fonctions L de toutes les formes primitives de $\oplus_{\mathrm{I}'}\mathrm{I}'\mathbf{S} = \mathrm{I}\mathbf{S}$ (où I' parcourt les sous-$\mathbf{T}\otimes\mathbf{Q}$-modules irréductibles de I) ne s'annulent pas en 1. Jusqu'à la fin de cet démonstration on supposera que I est le sous-$\mathbf{T}\otimes\mathbf{Q}$-module supplémentaire de $\mathcal{I}_{\mathbf{e}}\otimes\mathbf{Q}$ dans $\mathbf{T}\otimes\mathbf{Q}$. On a alors une isogénie canonique $\mathrm{J}_{\mathrm{I}} \to \mathrm{J}_{\mathbf{e}}$. Par

conséquent $\mathrm{J_I}(\mathbf{Q})$ est fini si et seulement si $\mathrm{J_e}(\mathbf{Q})$ est fini. Il nous faut donc prouver que $\mathrm{L}(f,1)$ est non nul pour toute forme primitive de $\mathbf{IS}$.

On a un accouplement bilinéaire non dégénéré $\mathbf{H}^+ \otimes \mathbf{Q} \times \mathbf{S} \to \mathbf{C}$ qui à $(c \otimes 1, f)$ associe $< c, f >= \int_{\tilde{c}} f(z)\, dz = \int_c \omega_f$, où $\tilde{c}$ est une combinaison linéaire de chemins de $\mathcal{H}$ d'image c dans $\mathbf{H}^+ \otimes \mathbf{Q}$ et où ω_f est la forme différentielle sur $\mathrm{X}_0(p)$ déduite de $f(z)\, dz$ grâce à la surjection canonique $\mathcal{H} \cup \mathbf{P}^1(\mathbf{Q}) \to \mathrm{X}_0(p)$. Les opérateurs de Hecke sur $\mathbf{H} \otimes \mathbf{Q}$ et $\mathbf{S}$ sont adjoints pour cet accouplement. Par conséquent les formes primitives de $\mathbf{IS}$ sont les formes primitives orthogonales à $\mathcal{I}_\mathbf{e}\mathbf{H}^+ \otimes \mathbf{Q}$ pour l'accouplement bilinéaire $< ., . >$. Soit f une telle forme primitive. Comme $\mathbf{H}^+ \otimes \mathbf{Q}$ est un $\mathbf{T} \otimes \mathbf{Q}$-module libre semi-simple de rang 1, on a une décomposition de $\mathbf{H}^+ \otimes \mathbf{Q}$ en somme directe $(\mathbf{T} \otimes \mathbf{Q}\mathbf{e}) \oplus (\mathcal{I}_\mathbf{e}\mathbf{H}^+ \otimes \mathbf{Q})$. La forme f est orthogonale à la deuxième composante de cette somme directe pour l'accouplement non dégénéré $< ., . >$. Il donc existe $t \in \mathbf{T}$ tel que $< t\mathbf{e}, f > \neq 0$. Par conséquent, on a $< \mathbf{e}, tf > \neq 0$. Or on a $tf \in \mathbf{C}f$ puisque f est primitive. On a donc $< \mathbf{e}, f > \neq 0$ et par suite, en raison de la définition de $\mathbf{e}$,

$$\mathrm{L}(f,1) = 2\pi \int_0^\infty f(iy)\, dy = 2\pi i < \mathbf{e}, f > \neq 0.$$

Proposition 2. — *Soient d un entier > 1 et p un nombre premier. Si $\mathrm{T}_1\mathbf{e}$,..., $\mathrm{T}_d\mathbf{e}$ sont linéairement indépendants dans $\mathbf{H} \otimes \mathbf{Q}$ et s'il existe une courbe elliptique E définie sur un corps de nombres K de degré d sur $\mathbf{Q}$ possédant un point de torsion d'ordre p défini sur K alors on a $p \leq 2^{d+1}(d!)^{5d/2}$, et donc $p \leq d^{3d^2}$.*

Démonstration. — Soit $\mathcal{I}$ un idéal de $\mathbf{T}$ définissant une variété abélienne quotient $\mathrm{J}_0(p)/\mathcal{I}\mathrm{J}_0(p)$ de $\mathrm{J}_0(p)$ définie sur $\mathbf{Q}$. Dans [7], Kamienny prouve l'assertion suivante lorsque $\mathcal{I}$ est le noyau de l'homomorphisme canonique de $\mathbf{T}$ dans son complété en l'idéal d'Eisenstein : *Soient d un entier ≥ 1 et p un nombre premier. Si T_1,..., T_d sont linéairement indépendants dans $\mathbf{T}/\mathcal{I}$ et s'il existe une courbe elliptique E définie sur un corps de nombres K de degré d sur $\mathbf{Q}$ possédant un point de torsion d'ordre p défini sur K alors on a $p \leq 2^{d+1}(d!)^{5d/2}$.* En réalité la méthode de Kamienny s'applique sans difficulté pour prouver cette proposition pour n'importe quel idéal $\mathcal{I}$ de $\mathbf{T}$ pourvu que le groupe de Mordell-Weil de $\mathrm{J}_0(p)/\mathcal{I}\mathrm{J}_0(p)$ soit fini (Voir le texte de Edixhoven au séminaire Bourbaki qui donne la borne $2^{d+1}(d!)^{5d/2}$ [3]). L'assertion ci-dessus est donc encore valable si on considère pour $\mathcal{I}$ l'idéal $\mathcal{I}_\mathbf{e}$. Cela nous donne la preuve de la proposition 2.

§2. Indépendance linéaire des opérateurs de Hecke dans $\mathbf{Te}$

Dans ce qui suit on identifie $\mathbf{H}$ et $\tilde{\mathbf{H}}$ à des sous-groupes de $\tilde{\mathbf{H}} \otimes \mathbf{Q}$. On a donc $(p-1)\mathbf{e} \in \mathbf{H}$. Pour prouver le théorème il suffit de prouver la proposition suivante (Le cas $d = 2$ dans le théorème résulte des travaux de Kamienny [8]).

Proposition 3. — *Soient d un nombre entier ≥ 1 et p un nombre premier vérifiant $\frac{p}{\log^4 p} > \mathrm{Sup}(400d^4, d^8)$. C'est le cas lorsqu'on a $p > 2^{d+1}(d!)^{5d/2}$ et $d \geq 4$, ou encore lorsque $p > d^{3d^2}$ et $d \geq 3$. Alors $\mathrm{T}_1\mathbf{e}$,..., $\mathrm{T}_d\mathbf{e}$ sont linéairement indépendants dans $\mathbf{H} \otimes \mathbf{Q}$.*

Démonstration. — Il suffit de prouver que $\mathbf{e} = \mathrm{T}_1\mathbf{e}$, $(\mathrm{T}_2 - 3)\mathbf{e}$,... , $(\mathrm{T}_d - \sigma_1(d))\mathbf{e}$ sont linéairement indépendants dans $\mathbf{H} \otimes \mathbf{Q}$ (On a noté $\sigma_1(r)$ la somme des diviseurs positifs de r). Exposons la démarche suivie lors de cette démonstration. Soit $(\lambda_1, ..., \lambda_d) \in \mathbf{Z}^d$ tel que $\lambda_1\mathbf{e} + \sum_{r=2}^{d} \lambda_r(\mathrm{T}_r - \sigma_1(r))\mathbf{e} = 0$. Nous allons montrer $\lambda_1 = \lambda_2 = ... = \lambda_d = 0$. Soit $c \in \{2, ..., d\}$ tel que pour tout entier c' vérifiant $c < c' \leq d$ on ait $\lambda_{c'} = 0$ (il en existe). Utilisons les produits d'intersection : pour tout $x \in \mathbf{H}$ on a $(\lambda_1\mathbf{e} + \sum_{r=2}^{d} \lambda_r(\mathrm{T}_r - \sigma_1(r))\mathbf{e}) \bullet x = 0$. Nous allons d'abord prouver l'existence d'un symbole modulaire $x_1 \in \mathbf{H}$ orthogonal pour $\bullet$ à $\sum_{r=2}^{d} \lambda_r(\mathrm{T}_r - \sigma_1(r))\mathbf{e}$ mais pas à $\mathbf{e}$; cela prouvera $\lambda_1 = 0$. Nous prouverons ensuite l'existence d'un symbole modulaire $x_c \in \mathbf{H}$ orthogonal à $(\mathrm{T}_r - \sigma_1(r))\mathbf{e}$ pour tout entier $r < c$ mais pas orthogonal à $(\mathrm{T}_c - \sigma_1(c))\mathbf{e}$; cela prouvera $\lambda_c = 0$.

Pour $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$, le symbole modulaire $\{g0, g\infty\}$ ne dépend que de $\Gamma_0(p)g$ dans $\Gamma_0(p)\backslash\mathrm{SL}_2(\mathbf{Z})$, *i.e.* que de l'image de $\frac{\gamma}{\delta}$ dans $\mathbf{Z}/p\mathbf{Z} \cup \{\infty\}$. Notons $\xi(\frac{\gamma}{\delta})$ ce symbole modulaire. Lorsque k est un entier non divisible par p, on a, en considérant la matrice $\begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}$, $\xi(k) = \{0, \frac{1}{k}\} \in \mathbf{H}$. On a de plus $\xi(0) = \{0, \infty\} \in \tilde{\mathbf{H}}$.

Pour $k \in \{1, ..., p-1\}$ notons k_* l'unique élément de $\{1, ..., p-1\}$ tel que $p|(kk_* + 1)$.

L'élément d'Eisenstein $\mathcal{E}$ de $\tilde{\mathbf{H}}$

Pour r entier positif premier à p l'opérateur $\mathrm{T}_r - \sigma_1(r)$ est inversible sur $\mathbf{H} \otimes \mathbf{Q}$ et $\mathbf{S}$ (cela résulte par exemple des majorations de type Ramanujan-Petersson). La correspondance $\mathrm{T}_r - \sigma_1(r)$ est nulle sur l'ensemble ptes des pointes de $\mathrm{X}_0(p)$. Comme $\tilde{\mathbf{H}}/\mathbf{H}$ est un $\mathbf{Z}$-module libre de rang 1, et comme l'application bord $\tilde{\mathbf{H}} \to \mathbf{Z}[\mathrm{ptes}]$ est de rang 1 et de noyau $\mathbf{H}$, l'opérateur $\mathrm{T}_r - \sigma_1(r)$ est nul sur $\tilde{\mathbf{H}}/\mathbf{H}$ et il existe un unique

élément $\mathcal{E}$ de $\tilde{\mathbf{H}} \otimes \mathbf{Q}$ vérifiant $\mathrm{T}_r\mathcal{E} = \sigma_1(r)\mathcal{E}$ et de bord $(p-1)((\Gamma_0(p)\infty) - (\Gamma_0(p)0))$ dans $\mathbf{Z}[\mathrm{ptes}]$. Appelons-le *élément d'Eisenstein.*

Lemme 1. — *On a* $(p-1)\mathbf{e} = \mathcal{E} - (p-1)\{0,\infty\}$, *et donc* $\mathcal{E} \in \tilde{\mathbf{H}}$.

Démonstration. — Les deux membres de l'égalité ci-dessus sont de bord nul et appartiennent donc à $\mathbf{H} \otimes \mathbf{Q}$. Considérons l'accouplement $\mathbf{H} \otimes \mathbf{Q} \times \mathbf{S} \to \mathbf{C}$ introduit dans la démonstration de la proposition 1. Puisque cet accouplement est non dégénéré, il suffit de prouver que les deux membres définissent la même forme linéaire sur les formes modulaires par l'intégration. L'intégration des formes modulaires sur le demi-plan de Poincaré définit un accouplement $\tilde{\mathbf{H}} \otimes \mathbf{Q} \times \mathbf{S} \to \mathbf{C}$ prolongeant l'accouplement $< .,. >$ considéré ci-dessus et encore noté $< .,. >$. Compte-tenu de la définition de $\mathbf{e}$, il nous suffit de prouver que $\mathcal{E}$ est orthogonal à $\mathbf{S}$ pour cet accouplement. Cela résulte d'une propriété d'adjonction des opérateurs de Hecke. En effet, on a pour tout forme modulaire parabolique f :

$$0 =< (\mathrm{T}_r - \sigma_1(r))\mathcal{E}, f >=< \mathcal{E}, (\mathrm{T}_r - \sigma_1(r))f > .$$

Or l'opérateur $\mathrm{T}_r - \sigma_1(r)$ est surjectif sur $\mathbf{S}$. On a donc prouvé le lemme.

Un analogue d'une formule de Manin

L'énoncé suivant est très voisin du théorème 7.9 de [11].

Lemme 2. — *Soit* r *un entier positif* $< p$. *On a dans* $\mathbf{H} \otimes \mathbf{Q}$

$$(\mathrm{T}_r - \sigma_1(r))\mathbf{e} = -\sum_{u>v\geq 0, t>w>0, ut-vw=r} \xi(\frac{w}{t})$$

où u, v, w *et* t *sont des nombres entiers (cette somme est finie).*

Démonstration. — D'après le lemme 1 on a dans $\tilde{\mathbf{H}}$

$$(p-1)(\mathrm{T}_r - \sigma_1(r))\mathbf{e} = (\mathrm{T}_r - \sigma_1(r))(\mathcal{E} - (p-1)\{0,\infty\}).$$

En utilisant la relation $\mathrm{T}_r\mathcal{E} = \sigma_1(r)\mathcal{E}$, on obtient $(\mathrm{T}_r - \sigma_1(r))\mathbf{e} = -(\mathrm{T}_r - \sigma_1(r))\{0,\infty\}$, et donc

$$(\mathrm{T}_r - \sigma_1(r))\mathbf{e} = -\mathrm{T}_r\{0,\infty\} + \sum_{u>v\geq 0, t>w\geq 0, ut-vw=r} \xi(\frac{w}{t}) - \sum_{u>v\geq 0, t>w>0, ut-vw=r} \xi(\frac{w}{t}).$$

En effet le nombre de quadruplets $(u,v,w,t) \in \mathbf{Z}^4$ vérifiant $u > v \geq 0$, $t > w \geq 0$, $ut - vw = r$ avec $w = 0$ est égal à $\sigma_1(r)$ et pour $w = 0$ on a $\xi(\frac{w}{t}) = \xi(0) = \{0,\infty\}$.

Il reste donc à prouver qu'on a $\mathrm{T}_r\{0,\infty\} = \sum_{u>v\geq 0, t>w\geq 0, ut-vw=r} \xi(\frac{w}{t})$. Rappelons qu'on a, par fonctorialité des correspondances de Hecke,

$$\mathrm{T}_r\{0,\infty\} = \sum_{\delta,\beta} \{ \begin{pmatrix} \frac{r}{\delta} & -\beta \\ 0 & \delta \end{pmatrix} 0, \begin{pmatrix} \frac{r}{\delta} & -\beta \\ 0 & \delta \end{pmatrix} \infty \},$$

où les couples d'entiers (δ,β) satisfont $0 \leq \beta < \delta$ et δ divise r. Notons $\mathrm{M}_2(\mathbf{Z})_r$ l'ensemble des matrices de $\mathrm{M}_2(\mathbf{Z})$ de déterminant r. Notons $\mathcal{X}_r$ l'ensemble des matrices $\begin{pmatrix} u & v \\ w & t \end{pmatrix}$ de $\mathrm{M}_2(\mathbf{Z})_r$ vérifiant $u > v \geq 0$ et $t > w \geq 0$. Cet ensemble est fini.

L'ensemble des matrices $m(\delta,\beta) = \begin{pmatrix} \delta & \beta \\ 0 & \frac{r}{\delta} \end{pmatrix}$ (resp. $\begin{pmatrix} \frac{r}{\delta} & 0 \\ \beta & \delta \end{pmatrix}$) de $\mathrm{M}_2(\mathbf{Z})_r$ avec $0 \leq \beta < \delta$ est un système de représentants de $\mathrm{M}_2(\mathbf{Z})_r/\mathrm{SL}_2(\mathbf{Z})$. Ces matrices sont les seuls éléments $M = \begin{pmatrix} u & v \\ w & t \end{pmatrix}$ de $\mathcal{X}_r$ tels que $w = 0$, *i.e.* $M\infty = \infty$ (resp. $v = 0$, *i.e.* $M0 = 0$).

Dans ces conditions, posons $C(\delta,\beta) = m(\delta,\beta)\mathrm{SL}_2(\mathbf{Z})$. Pour $M = \begin{pmatrix} u & v \\ w & t \end{pmatrix} \in C(\delta,\beta)$, on a $m(\delta,\beta)^{-1}M \in \mathrm{SL}_2(\mathbf{Z})$ et $\xi(\frac{w}{t}) = \{m(\delta,\beta)^{-1}M0, m(\delta,\beta)^{-1}M\infty\}$. On a donc

$$\sum_{u>v\geq 0, t>w\geq 0, ut-vw=r} \xi(\frac{w}{t}) = \sum_{\delta,\beta} \sum_{M\in\mathcal{X}_r\cap C(\delta,\beta)} \{m(\delta,\beta)^{-1}M0, m(\delta,\beta)^{-1}M\infty\},$$

où les couples d'entiers (δ,β) satisfont $0 \leq \beta < \delta$ et δ divise r (on adopte la même convention pour toutes les sommes qui suivent faisant intervenir les couples (δ,β)).

Si $M = \begin{pmatrix} u & v \\ w & t \end{pmatrix}$ est un élément de $\mathcal{X}_r$ avec $M\infty \neq \infty$, *i.e.* $w \neq 0$ (resp. $M0 \neq 0$, *i.e.* $v \neq 0$), il existe un unique élément M' de $\mathcal{X}_r \cap M\mathrm{SL}_2(\mathbf{Z})$ tel que $M\infty = M'0$ (resp. $M0 = M'\infty$). En effet M' doit être de la forme $M\begin{pmatrix} m & 1 \\ -1 & 0 \end{pmatrix}$ (resp. $M\begin{pmatrix} 0 & -1 \\ 1 & m \end{pmatrix}$) ; les conditions définissant $\mathcal{X}_r$ imposent qu'il existe un unique entier m convenable : le plus petit entier $\geq t/w$ (resp. u/v).

Le symbole modulaire $\{\alpha,\beta\}$ ne dépend que de $[\alpha]-[\beta]$ dans $\mathbf{Z}[\mathbf{P}^1(\mathbf{Q})]$. Par conséquent le symbole modulaire $\sum_{u>v\geq 0, t>w\geq 0, ut-vw=r} \xi(\frac{w}{t})$ ne dépend que de

$$\sum_{\delta,\beta} \sum_{M\in\mathcal{X}_r\cap C(\delta,\beta)} [m(\delta,\beta)^{-1}M0] - [m(\delta,\beta)^{-1}M\infty]$$

dans $\mathbf{Z}[\mathbf{P}^1(\mathbf{Q})]$. En utilisant les propriétés de $\mathcal{X}_r$ établies ci-dessus on trouve que cet élément de $\mathbf{Z}[\mathbf{P}^1(\mathbf{Q})]$ est égal à

$$\sum_{\delta,\beta} (\sum_{M\in\mathcal{X}_r\cap C(\delta,\beta), M0=0} [m(\delta,\beta)^{-1}M0] - \sum_{M\in\mathcal{X}_r\cap C(\delta,\beta), M\infty=\infty} [m(\delta,\beta)^{-1}M\infty]),$$

c'est-à-dire, puisqu'il n'y a qu'un seul élément $M \in \mathcal{X}_r \cap C(\delta,\beta)$ tel que $M0 = 0$ (resp. $M\infty = \infty$) (cf. ci-dessus),

$$\sum_{\delta,\beta} [m(\delta,\beta)^{-1}0] - [m(\delta,\beta)^{-1}\infty].$$

On a donc

$$\sum_{u>v\geq 0, t>w\geq 0, ut-vw=r} \xi(\frac{w}{t}) = \sum_{\delta,\beta} \{m(\delta,\beta)^{-1}\infty, m(\delta,\beta)^{-1}0\} = \mathrm{T}_r\{0,\infty\}.$$

Cela achève de prouver le lemme 2.

Remarquons que lorsque un quadruplet $(u,v,w,t) \in \mathbf{Z}^4$ vérifie $u > v \geq 0, t > w \geq 0, ut - vw = r$, les quatre entiers u, v, w et t sont inférieurs ou égaux à r. Notons $E_c = \{\frac{u}{v} \in \mathbf{Q}, 0 < u < v \leq c\}$ et $E_c^* = \{-\frac{v}{u} \in \mathbf{Q}, 0 < u < v \leq c\}$. Observons alors que $\lambda_1 \mathbf{e} + \sum_{r=2}^{d} \lambda_r(\mathrm{T}_r - \sigma_1(r))\mathbf{e}$ se récrit en utilisant le lemme 2 de la façon suivante $\lambda_1\mathbf{e} + \sum_{q\in E_d} \mu_q \xi(q)$, avec μ_q entier pour tout $q \in E_d$. Cette somme est en fait à support dans E_c. Remarquons que le coefficient $\mu_{\frac{1}{c}}$ est égal à $-\lambda_c$. Nous ferons usage de ces remarques lors des démonstrations des lemmes 6 et 7.

L'homomorphisme de Rademacher

Pour u et v nombre entiers premiers entre eux, $v > 0$, la somme de Dedekind $S(u,v)$ est donnée par la formule

$$S(u,v) = \sum_{h=0}^{v-1} \bar{\mathrm{B}}_1(\frac{h}{v})\bar{\mathrm{B}}_1(\frac{uh}{v})$$

($\bar{\mathrm{B}}_1$ est le premier polynôme de Bernoulli rendu périodique : on a $\bar{\mathrm{B}}_1(x) = x - \frac{1}{2}$ si $x \in]0,1[$, $\bar{\mathrm{B}}_1(0) = 0$ et $\bar{\mathrm{B}}_1$ est une fonction périodique de période 1).

Rappelons que, pour $k \in \{1,...,p-1\}$, k_* est l'unique élément de $\{1,...,p-1\}$ tel que $p|(1+kk_*)$.

Lemme 3. — *Soit* $k \in \{1,...,p-1\}$. *On a*

$$(p-1)\mathbf{e} \bullet \xi(k) = \frac{(k-k_*)}{p}(1-p) - 12S(k,p).$$

Démonstration. — Pour $g \in \Gamma_0(p)$, notons c_g la classe dans $\tilde{\mathbf{H}}'$ de l'image dans $\mathrm{Y}_0(p)$ d'un chemin de $\mathcal{H}$ reliant z à gz pour $z \in \mathcal{H}$. Cette classe ne dépend pas du choix de z. L'application qui à g associe c_g est un homomorphisme surjectif de groupes.

Posons dans $\Gamma_0(p)$, $W_k = \begin{pmatrix} k_* & -1 \\ 1+kk_* & -k \end{pmatrix}$. L'image de c_{W_k} dans $\mathbf{H}$ par la surjection canonique $\tilde{\mathbf{H}}' \to \mathbf{H}$ est égale à la classe de l'image dans $\mathrm{X}_0(p)$ du chemin géodésique reliant 0 à $W_k 0 = \frac{1}{k}$ dans $\mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$, *i.e.* égale à $\xi(k)$. En utilisant le lemme 1 on obtient :

$$(p-1)\mathbf{e} \bullet \xi(k) = (\mathcal{E} - (p-1)\{0,\infty\}) \bullet c_{W_k}.$$

Nous allons calculer séparément $\mathcal{E} \bullet c_{W_k}$ et $\{0,\infty\} \bullet c_{W_k}$. Commençons par le premier de ces termes.

L'application R qui à une matrice $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ de $\Gamma_0(p)$ associe $(p-1)\frac{\beta}{\delta}$ si $\gamma = 0$ et $\frac{\alpha+\delta}{\gamma}(p-1) + 12\frac{\gamma}{|\gamma|}(S(\delta,|\gamma|) - S(\delta,|\frac{\gamma}{p}|))$ sinon est un homomorphisme de groupe que nous appellerons *homomorphisme de Rademacher* (voir [15]). Elle est à valeur dans $\mathbf{Z}$ et se factorise par un homomorphisme de groupe $\phi_{\mathrm{R}} : \tilde{\mathbf{H}}' \to \mathbf{Z}$ via l'homomorphisme qui à g associe c_g ([13], II.2). Nous allons prouver qu'on a $\mathrm{R}(g) = -\mathcal{E} \bullet c_g$ pour tout $g \in \Gamma_0(p)$. Il suffit de prouver qu'on a $\phi_{\mathrm{R}}(y) = -\mathcal{E} \bullet y$ pour tout $y \in \tilde{\mathbf{H}}'$. Comme l'accouplement $\tilde{\mathbf{H}} \times \tilde{\mathbf{H}}' \to \mathbf{Z}$ est unimodulaire, il existe un unique élément $\mathcal{E}' \in \tilde{\mathbf{H}}$ tel que $\phi_{\mathrm{R}}(y) = -\mathcal{E}' \bullet y$ pour tout $y \in \tilde{\mathbf{H}}'$. D'après [13], proposition 1, ϕ_{R} est fonction propre pour l'opérateur de Hecke T_l, l nombre premier différent de p, avec la valeur propre $1+l$. On en déduit qu'il en est de même pour $\mathcal{E}'$. Les éléments $\mathcal{E}$ et $\mathcal{E}'$ sont donc proportionnels, d'après la définition de $\mathcal{E}$. Pour prouver qu'ils sont opposés considérons la matrice de $\Gamma_0(p)$ suivante $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. On a $\phi_{\mathrm{R}}(c_T) = \mathrm{R}(T) = p-1$. Par ailleurs le chemin c_T est la classe d'un petit lacet tournant dans le sens trigonométrique autour de la pointe $\Gamma_0(p)\infty$. Comme $\mathcal{E}$ a pour bord $(p-1)(\Gamma_0(p)\infty) - (\Gamma_0(p)0)$, $\mathcal{E}$ est la classe d'un chemin de $\mathrm{X}_0(p)$ d'extrémité $\Gamma_0(p)\infty$ et d'origine $\Gamma_0(p)0$; on a donc $\mathcal{E} \bullet c_T = 1-p$. Cela prouve qu'on a $\mathrm{R}(g) = -\mathcal{E} \bullet c_g$ pour tout $g \in \Gamma_0(p)$. D'après [13], propositions 2 et 3, on a $\mathrm{R}(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}) = \mathrm{R}(\begin{pmatrix} \alpha & \frac{\gamma}{p} \\ p\beta & \delta \end{pmatrix})$. En utilisant cette formule pour calculer $\mathrm{R}(W_k)$ on obtient

$$\mathcal{E} \bullet c_{W_k} = -\mathrm{R}(\begin{pmatrix} k_* & \frac{1+kk_*}{p} \\ -p & -k \end{pmatrix}) = \frac{(k-k_*)}{p}(1-p) - 12S(k,p),$$

car $S(-k,p) = -S(k,p)$ et $S(k,1) = 0$. Il reste à prouver qu'on a $\{0,\infty\} \bullet c_{W_k} = 0$. Considérons le quadrilatère hyperbolique Q ouvert de sommets 0, ∞, $\frac{1+\sqrt{-3}}{2}$ et $\frac{-1+\sqrt{-3}}{2}$. C'est la réunion du domaine fondamental D habituel de $\mathrm{SL}_2(\mathbf{Z})$, de $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} D$ et du support de l'arc géodésique reliant $\frac{1+\sqrt{-3}}{2}$ à $\frac{-1+\sqrt{-3}}{2}$. Pour $g \in \mathrm{SL}_2(\mathbf{Z})$ notons $\overline{gQ}$ le projeté dans $\mathrm{X}_0(p)$ de gQ. Le symbole modulaire $\{0,\infty\}$ est la classe de l'image c_0

dans $\mathrm{X}_0(p)$ du chemin géodésique de $\mathcal{H}\cup\mathbf{P}^1(\mathbf{Q})$ reliant 0 à ∞. Ce chemin privé de ses extrémités est à support dans Q. Il suffit de prouver que c_{W_k} est égal à la classe d'un chemin de $\mathrm{Y}_0(p)$ ne rencontrant pas c_0. Pour $g\in\mathrm{SL}_2(\mathbf{Z})$, notons $[g]$ l'image dans $\mathrm{X}_0(p)$ du chemin géodésique de $\mathbf{H}$ reliant $g\frac{1+\sqrt{-3}}{2}$ à $g\frac{-1+\sqrt{-3}}{2}$. Il ne dépend que de $\Gamma_0(p)g$ et est à support dans $\overline{gQ}$. Par un raisonnement sur les domaines fondamentaux de $\mathrm{SL}_2(\mathbf{Z})$, il rencontre c_0 si et seulement si $g\in\Gamma_0(p)$ ou $g\in\Gamma_0(p)S$ (avec $S=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$). Remarquons que le chemin $[gS]$ est l'inverse du chemin $[g]$. De plus l'origine du chemin $[g]$ est égale à l'extrémité du chemin $[gT]$ ($T=\begin{pmatrix}1&1\\0&1\end{pmatrix}$). Il en résulte que le chemin $\Gamma=[ST^{-1}]\circ[ST^{-2}]\circ...\circ[ST^{1-k}]\circ[ST^{-k}S]^{-1}\circ[ST^{-k}ST]^{-1}\circ[ST^{-k}ST^2]^{-1}\circ...\circ[ST^{-k}ST^{k_*}]^{-1}$, où $\circ$ désigne la composition des chemins, est continu. Son origine est égale à $ST^{-1}\frac{1+\sqrt{-3}}{2}=\frac{1+\sqrt{-3}}{2}$. Son extrémité est égale à $ST^{-k}ST^{k_*}\frac{-1+\sqrt{-3}}{2}=ST^{-k}ST^{k_*}S\frac{1+\sqrt{-3}}{2}=W_k\frac{1+\sqrt{-3}}{2}$. Par conséquent Γ est un chemin fermé de $\mathrm{Y}_0(p)$ de classe c_{W_k} dans $\tilde{\mathbf{H}}'$. Par ailleurs Γ ne rencontre pas c_0 car il est composé de chemin ne rencontrant pas c_0. En effet, on a $\Gamma_0(p)ST^{-i}\neq\Gamma_0(p)$, $\Gamma_0(p)ST^{-i}\neq\Gamma_0(p)S$, $\Gamma_0(p)ST^{-k}S\neq\Gamma_0(p)$, $\Gamma_0(p)ST^{-k}S\neq\Gamma_0(p)S$, $\Gamma_0(p)ST^{-k}ST^j\neq\Gamma_0(p)$ et $\Gamma_0(p)ST^{-k}ST^j\neq\Gamma_0(p)S$, pour $i=1,...,k-1$ et $j=1,...,k_*-1$. On a donc $\{0,\infty\}\bullet c_{W_k}=0$. Cela achève de prouver le lemme.

Le lemme des cordes

Pour $k\in\{1,...,p-1\}$ notons C_k la corde (*i.e.* le chemin géodésique de $\mathbf{C}$) reliant $e^{\frac{2\pi ik_*}{p}}$ à $e^{\frac{2\pi ik}{p}}$.

Lemme 4. — *Soient k et k' deux éléments de $\{1,...,p-1\}$ tels que $k\neq k'$, $k\neq k'_*$. Le produit d'intersection $\xi(k)\bullet\xi(k')$ est égal au nombre d'intersection (égal à -1, 0 ou 1) des cordes $C_{k'}$ et C_k.*

Démonstration. — Conservons les notations introduites dans la démonstration du lemme précédent. Pour $l\in\{1,...,p-1\}$, notons c_l le projeté dans $\mathrm{X}_0(p)$ du chemin géodésique de $\mathcal{H}\cup\mathbf{P}^1(\mathbf{Q})$ reliant 0 à $\frac{1}{l}$, *i.e.* la classe de c_l dans $\mathbf{H}$ est égale à $\xi(l)$. Le chemin c_l est, excepté les extrémités, à support dans $\overline{\begin{pmatrix}1&0\\l&1\end{pmatrix}Q}$. De plus le chemin c_{l_*} est le chemin inverse de c_l. En effet c_l est l'image dans $\mathrm{X}_0(p)$ de $\begin{pmatrix}1&0\\l&1\end{pmatrix}c_0$ et ne dépend que de $\Gamma_0(p)\begin{pmatrix}1&0\\l&1\end{pmatrix}$; or on a $\Gamma_0(p)\begin{pmatrix}1&0\\l&1\end{pmatrix}=\Gamma_0(p)\begin{pmatrix}1&0\\l_*&1\end{pmatrix}S$ et Sc_0 est le chemin inverse de c_0. Pour g et g' deux éléments de $\mathrm{SL}_2(\mathbf{Z})$ on a $\overline{gQ}\cap\overline{g'Q}=\emptyset$ sauf si $\Gamma_0(p)g=\Gamma_0(p)g'$ ou $\Gamma_0(p)g=\Gamma_0(p)g'S$. Cela entraîne que les chemins c_k et $c_{k'}$ ne se rencontrent pas dans

$\mathrm{Y}_0(p)$, sauf peut-être si $k = k'$ ou $k = k'_*$, ce qui est exclu par hypothèse. L'involution W_p est un automorphisme analytique de $\mathrm{X}_0(p)$ laissant stable $\mathrm{Y}_0(p)$. Les chemins $W_p c_k$ et $W_p c_{k'}$ ne se rencontrent pas non plus en dehors de leurs extrémités, qui sont égales à la pointe $\Gamma_0(p)\infty$ de $\mathrm{X}_0(p)$. Comme l'involution d'Atkin-Lehner est un automorphisme analytique de $\mathrm{X}_0(p)$, le résultat cherché est égal au résultat de l'intersection de $W_p c_k$ et $W_p c_{k'}$ en la pointe $\Gamma_0(p)\infty$. Le chemin $W_p c_l$ est l'image dans $\mathrm{X}_0(p)$ du chemin géodésique de $\mathcal{H}\cup\mathbf{P}^1(\mathbf{Q})$ reliant ∞ à $-\frac{l}{p}$. L'application $z \mapsto e^{2\pi i z}$ sur $\mathcal{H}\cup\mathbf{P}^1(\mathbf{Q})$ définit par passage aux quotients une uniformisante locale q sur $\mathrm{X}_0(p)$ au voisinage de $\Gamma_0(p)\infty$. L'image par q de l'inverse de $W_p c_{l_*}$ composée avec $W_p c_l$ est égale au chemin γ_l du disque unité de $\mathbf{C}$ reliant $e^{\frac{-2\pi i l_*}{p}}$ à 0 puis à $e^{\frac{-2\pi i l}{p}}$. Remarquons que l'intersection en $\Gamma_0(p)\infty$ de $W_p c_k$ et $W_p c_{k'}$ est transportée par q en l'intersection en 0 des chemins γ_k et $\gamma_{k'}$. On change deux fois le signe de cette intersection en inversant k et k' puis en transformant ces chemins par leurs conjugués complexes. On déduit enfin le lemme en utilisant l'invariance par homotopie des produits d'intersection.

Lemme de théorie analytique des nombres

Le principe de la démonstration du lemme suivant m'a été indiqué par Fouvry.

Lemme 5. — *Soient p un nombre premier, a et b deux nombres réels ≥ 1. Soient A et B deux intervalles de l'ensemble $\{1, 2, ..., p-1\}$ de cardinaux $\frac{p}{a}$ et $\frac{p}{b}$ respectivement. Si on a l'inégalité $p > a^2 b^2 \log^4 p$ alors il existe $k \in A$ tel que $k_* \in B$.*

Démonstration. — L'inégalité $p > a^2 b^2 \log^4 p$ impose $p > 1000$. Notons χ_A et χ_B les fonctions caractéristiques de A et B. Posons $\Lambda(A, B) = \sum_{n=1}^{p-1} \chi_A(n)\chi_B(n_*)$. Il nous faut prouver que cette quantité est strictement positive. Développons en série de Fourier les fonctions χ_A et χ_B. On a

$$\chi_A(n) = \frac{1}{p}\sum_{h=0}^{p-1}\sum_{m\in A} e^{\frac{2\pi i h(m-n)}{p}}.$$

On a donc

$$\Lambda(A,B) = \frac{1}{p^2}\Big(\sum_{h=0}^{p-1}\sum_{h'=0}^{p-1}\Big(\sum_{m\in A} e^{\frac{2\pi i h m}{p}}\Big)\Big(\sum_{m'\in B} e^{\frac{2\pi i h' m'}{p}}\Big)\Big(\sum_{n=1}^{p-1} e^{\frac{-2\pi i(hn+h' n_*)}{p}}\Big)\Big).$$

Comme A est un intervalle, l'expression $\sum_{m\in A} e^{\frac{2\pi i h m}{p}}$ est somme des termes d'une suite géométrique finie de raison $e^{\frac{2\pi i h}{p}}$. Elle est donc majorée en module par $1/\sin\frac{\pi i h}{p}$ si $h \neq 0$.

La fonction $x \mapsto 1/\sin x$ est convexe sur l'intervalle $]0,\pi[$. On a donc $1/\sin\frac{\pi h}{p} \leq \int_{h-\frac{1}{2}}^{h+\frac{1}{2}} \frac{dt}{\sin\frac{\pi t}{p}}$ et donc $\sum_{h=1}^{p-1} 1/\sin\frac{\pi h}{p} \leq \int_{\frac{1}{2}}^{p-\frac{1}{2}} \frac{dt}{\sin\frac{\pi t}{p}} \leq \frac{2p}{\pi}\log\frac{4p}{\pi}$. De plus on a $\frac{p}{a} = |\sum_{h=1}^{p-1}\sum_{m\in A} e^{\frac{2\pi i h m}{p}}|$ et l'égalité analogue relative à B. L'expression $(\sum_{n=1}^{p-1} e^{\frac{-2\pi i(hn+h'n_*)}{p}})$ est une somme de Kloosterman majorée en module par $2\sqrt{p}$ si p ne divise pas hh' (majoration due à Weil [18]), égale à $p-1$ si p divise h et h' et égale à -1 sinon.

Isolons les termes correspondant à $h = 0$ ou $h' = 0$ dans l'expression se $\Lambda(A,B)$ ci-dessus. Utilisons les majorations et les identités mentionnés plus haut. On obtient alors la minoration suivante

$$\Lambda(A,B) \geq \frac{p-1}{ab} + \frac{1}{ab} + \frac{1}{ab} - \frac{8p^{1/2}}{\pi^2}\log^2\frac{4p}{\pi} = \frac{p+1}{ab} - \frac{8p^{1/2}}{\pi^2}\log^2\frac{4p}{\pi}.$$

Le membre de droite de la dernière égalité est strictement positif dès lors que $p > a^2b^2\log^4 p$, car $p > 1000$, comme le montre un calcul élémentaire.

La nullité de λ_1

Lemme 6. — *Supposons qu'on ait* $\frac{p}{\log^4 p} > 400d^4$. *Alors on a* $\lambda_1 = 0$.

Démonstration. — Appliquons le lemme 5 à $A = \mathbf{Z}\cap]\frac{p}{10d}, \frac{p}{5d}+1[$ et $B = \mathbf{Z}\cap]\frac{p}{2d}-1-\frac{1}{d}, \frac{p-1}{d}[$ et donc $a \leq 10d$ et $b \leq 2d$. Avec l'hypothèse donnée sur p, par application du lemme 5, il existe $k \in A$ tel que $k_* \in B$. Soit $\frac{u}{v} \in E_d$ (resp. $-\frac{v}{u} \in E_d^*$). Tout représentant positif q de la réduction modulo p de $\frac{u}{v}$ est $\geq \frac{p-1}{d}$. En effet on a $p|(vq-u)$ et $vq-u > 0$ (resp. $p|(uq+v)$ et $uq+v > 0$) vu les conditions sur u et v et donc $q \geq \frac{p+u}{v} \geq \frac{p-1}{d}$ (resp. $q \geq \frac{p-v}{u} \geq \frac{p-d}{d-1} \geq \frac{p-1}{d}$, vu les hypothèses sur p et d). Par conséquent la corde C_q ne rencontre pas la corde C_k. On en déduit $\xi(q) \bullet \xi(k) = 0$ pour tout $q \in E_d$ d'après le lemme 4. On a donc $(\mathrm{T}_r - \sigma_1(r))\mathbf{e} \bullet \xi(k) = 0$ pour tout entier r compris entre 2 et d d'après le lemme 2. On a donc $\lambda_1 \mathbf{e} \bullet \xi(k) = 0$. En utilisant la formule $12(S(k,p)+S(p,k)) = -3 + \frac{p}{k} + \frac{k}{p} + \frac{1}{pk}$ (voir [16]) et le lemme 3, on obtient :

$$(p-1)\mathbf{e} \bullet \xi(k) = k_* - k + \frac{k-k_*}{p} + 12S(p,k) + 3 - \frac{k}{p} - \frac{p}{k} - \frac{1}{pk}.$$

En utilisant les encadrements imposés à k et k_* et l'inégalité $|12S(p,k)| \leq k$, on obtient

$$\mathbf{e} \bullet \xi(k) \geq \frac{p}{10d} - 10d - 2.$$

Le membre de droite de la dernière égalité est strictement positif lorsque $\frac{p}{\log^4 p} > 400d^4$. On en déduit $\mathbf{e} \bullet \xi(k) \neq 0$ et donc $\lambda_1 = 0$.

La nullité de λ_c

Rappelons que c est un entier appartenant $\{2,...,d\}$ tel que pour tout nombre entier c' vérifiant $c < c' \leq d$ on ait $\lambda_{c'} = 0$.

Lemme 7. — *Supposons qu'on ait* $\frac{p}{\log^4 p} > \mathrm{Sup}(d^8, 400d^4)$. *Alors on a* $\lambda_c = 0$.

Démonstration. — Posons $q = p - c_*$. Appliquons le lemme 5 à $A = \mathbf{Z} \cap]q, q + \frac{p-d^2}{d(d-1)}[$ et $B = \mathbf{Z} \cap]q - \frac{p-d^2}{d(d-1)}, q[$. On a $a \leq d^2$ et $b \leq d^2$, car $\frac{p-d^2}{d(d-1)} - 1 \geq \frac{p}{d^2}$. Il existe k dans $\{1,...,p-1\}$ tel que $k \in A$ et $k_* \in B$. La différence r entre q et un représentant de la réduction modulo p d'un élément $\frac{u}{v} \in E_c - \{\frac{1}{c}\}$ (resp. $-\frac{v}{u} \in E_c^*$) vérifie $|r| \geq \frac{p-d^2}{d(d-1)}$. En effet cela se vérifie facilement si $v = d$; si $v \neq d$ on a $p|(vcr + cu - v)$ (resp. $p|(urc - cv - u)$) ; comme on a $0 < u < v \leq c \leq d$ et $u/v \neq 1/c$, on a $vcr + cu - v \neq 0$ (resp. $urc - cv - u \neq 0$ car c ne divise pas u) et donc $|r| \geq \frac{p-|v-cu|}{vc} \geq \frac{p-d^2}{d(d-1)}$ (resp. $|r| \geq \frac{p-|cv+u|}{uv} \geq \frac{p-d^2}{d(d-1)}$ car $v < d$). On en déduit que les ensembles A et B ne rencontrent pas les réductions modulo p des ensembles E_c et E_c^*. Soit $q' \in E_c - \{\frac{1}{c}\}$. La corde $C_{q'}$ ne rencontre donc pas la corde C_k. On a donc $\xi(q') \bullet \xi(k) = 0$ par application du lemme 4. On en déduit $(\mathrm{T}_r - \sigma_1(r))\mathbf{e} \bullet \xi(k) = 0$ pour tout entier r compris entre 2 et d d'après le lemme 2. Par ailleurs $\lambda_1 = 0$ d'après le lemme 6. On a donc $\lambda_c \xi(q) \bullet \xi(k) = 0$. On constate que q_* n'est pas un élément de $A \cup B \cup \{q\}$ en raison des conditions imposées sur p et d. Par conséquent la corde C_q rencontre la corde C_k. On en déduit $\xi(\frac{1}{c}) \bullet \xi(k) \neq 0$ d'après le lemme 4 et donc $(\mathrm{T}_c - \sigma_1(c))\mathbf{e} \bullet \xi(k) \neq 0$ d'après le lemme 2. On a donc $\lambda_c = 0$.

On obtient la proposition 3 par applications répétées du lemme 7.

Remarques. — 1) Comme le remarque le rapporteur, les arguments de cet articles permettent de démontrer que les vecteurs $\mathbf{e}$, $\xi(2)$, $\xi(3)$,..., $\xi(d)$ sont linéairement indépendants dès lors que $\frac{p}{\log^4 p} > \mathrm{Sup}(400d^4, d^8)$.

2) Le rapporteur remarque également que la formule démontrée dans le lemme 2 n'est pas indispensable car on peut utiliser l'algorithme de fractions continues de Birch-Manin.

3) Un argument utilisé par Oesterlé pour améliorer la borne indiquée dans l'énoncé du théorème permet de simplifier cet article, en particulier de se passer des lemmes 3 et 6. Voir son article à paraître.

4) Il n'a pas été fait usage dans cette démonstration de la présentation par générateurs et relations de l'homologie donnée par Manin ([11]). On aimerait utiliser cet ingrédient pour donner une démonstration de la proposition 3 qui ne fasse pas intervenir les produits d'intersection.

Remerciements : Je tiens à remercier E. Ullmo et S. David, pour les conversations qui sont à l'origine de ce travail, E. Fouvry pour le lemme 5, le rapporteur pour des commentaires précis et J. Oesterlé pour la grande attention qu'il a porté à ce travail.

Bibliographie

[1] D. Bump, S. Friedberg et J. Hoffstein, *Nonvanishing theorems for* L*-functions of modular forms and their derivatives*, Invent. Math. **102**, 543–618, 1990.

[2] H. Carayol, *Sur les représentations* l*-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. de l'ENS **19**, 409–468, 1986.

[3] B. Edixhoven, *Rational torsion points on elliptic curves over number fields*, A paraître dans Astérisque, Séminaire Bourbaki **782**, 46ème année, 1993–94.

[4] G. Faltings, *The general case of S. Lang's conjecture*, à paraître dans "The Barsotti symposium in algebraic geometry".

[5] G. Frey, *Curves with manitely many points of fixed degree*, prépublication, Institut für experimentelle Mathematik.

[6] B. Gross et D. Zagier, *Heegner points and derivatives of* L*-series*, Invent. Math. **84**, 225–320, 1986.

[7] S. Kamienny, *Torsion points on elliptic curves over fields of higher degree*, International Mathematics Research Notices **6**, 1992.

[8] S. Kamienny, *Torsion points on elliptic curves and* q*-coefficients of modular forms*, Invent. Math. **109**, 221–229, 1992.

[9] S. Kamienny et B. Mazur, *Rational torsion of prime order in elliptic curves over number fields*, à paraître dans Astérisque.

[10] V.A. Kolyvagin et D.Yu. Logachev, *Finiteness of the group of rational points for some abelian modular varieties*, Leningrad Math. J. **1**, n^0 5, 1229–1253, 1990.

[11] Yu. Manin, *Parabolic points and zeta function of modular curves*, Math. USSR Izvestija **6**, n^0 1, 19–64, 1972.

[12] B. Mazur, *Modular curves and the Eisenstein ideal*, Pub. math. de l'IHES **47**, 33–186, 1977.

[13] B. Mazur, *On the arithmetic of special values of* L*-functions*, Invent. Math. **55**, 207–240, 1979.

[14] M. R. Murty et V. K. Murty, *Mean values of derivatives of modular* L*-series*, Ann. Math. **133**, 447–475, 1991.

[15] H. Rademacher, *Zur Theorie der Modulfunktionen*, Journal für die reine und angewandte Mathematik **167**, 312–336, 1931.

[16] H. Rademacher et E. Grosswald, *Dedekind sums*, n^0 16 in Carus mathematical monographs, Math. association of America, 1972.

[17] G. Shimura, *Introduction to the arithmetic theory of automorphic forms*, Iwanami Shoten et Princeton University Press, 1971.

[18] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. USA **34**, 204–207, 1948.

Loïc Merel, Problèmes Diophantiens, Institut de Mathématiques, Université Pierre et Marie Curie, 4 Place Jussieu, 75252 Paris Cedex 05, France, merel@moka.ccr.jussieu.fr

Mis à jour le 12 décembre 1994