

# SUR LA NATURE NON-CYCLOTOMIQUE DES POINTS D’ORDRE FINI DES COURBES ELLIPTIQUES

---

LOÏC MEREL

Appendice de E. Kowalski et P. Michel

## Résumé

*Nous étudions le corps  $K_p$  engendré par les points d’ordre premier  $p$  d’une courbe elliptique sur un corps de nombres. Avec l’aide de Kowalski et Michel, nous démontrons que pour presque tout nombre premier  $p$ , toute courbe elliptique sur le corps cyclotomique  $\mathbf{Q}(\mu_p)$  possédant un sous-groupe cyclique  $\mathbf{Q}(\mu_p)$ -rationnel d’ordre  $p$  a potentiellement bonne réduction en caractéristique  $p$ . Nos méthodes s’appliquent aussi pour étudier, nombre premier par nombre premier, les courbes elliptiques n’ayant pas potentiellement bonne réduction en  $p$ . En particulier, nous démontrons qu’on a  $K_p \neq \mathbf{Q}(\mu_p)$  pour  $5 < p < 1000$  et  $p \equiv 1 \pmod{4}$ . Nous faisons un usage crucial des travaux de Kato sur la conjecture de Birch et Swinnerton-Dyer.*

## 0. Introduction

Lorsque  $E$  est une courbe elliptique sur un corps de nombres, le corps  $K_p(E)$  engendré par les points de  $p$ -division de  $E$  contient un corps cyclotomique  $\mathbf{Q}(\mu_p)$  engendré par les racines  $p$ -ièmes de l’unité — Cela est une conséquence évidente de la structure fournie par les accouplements de Weil. Cet article vise à établir que  $K_p(E)$  ne peut guère être aussi petit que  $\mathbf{Q}(\mu_p)$ .

Notons  $S$  l’ensemble des nombres premiers  $p$  tels qu’il existe une telle courbe elliptique avec  $\mathbf{Q}(\mu_p) = K_p(E)$ . Il est connu que l’ensemble  $S$  contient les nombres 2, 3 et 5 (puisque la courbe modulaire paramétrant le problème de module correspondant est de genre nul et possède au moins un point  $\mathbf{Q}(\mu_p)$ -rationnel). E. Halberstadt semble avoir établi récemment que  $S$  ne contient pas 7 (voir [6]). Nous sommes incapable d’établir la finitude de  $S$  (les techniques de [21] sont de peu de secours). Pour aborder cette dernière question, il semble naturel de séparer le problème en trois classes de courbes elliptiques sur  $\mathbf{Q}(\mu_p)$ , selon la géométrie de la fibre en l’idéal  $\mathcal{P}$  au dessus

DUKE MATHEMATICAL JOURNAL

Vol. 110, No. 1, © 2001

Received 19 May 2000. Revision received 18 September 2000.

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

de  $p$  du modèle de Néron sur  $\mathbf{Z}[\mu_p]$  :

- Le cas  $p$ -cuspidal, c’est-à-dire le cas des courbes elliptiques n’ayant pas potentiellement bonne réduction en  $\mathcal{P}$ . Nous obtenons beaucoup d’informations dans ce cas.
- Le cas  $p$ -ordinaire, c’est-à-dire le cas des courbes elliptiques ayant potentiellement bonne réduction ordinaire en  $\mathcal{P}$ . Dans le cas ordinaire on peut distinguer le cas (non déterminé par la géométrie) des *anomalies*, c’est-à-dire le cas où la réduction modulo  $\mathcal{P}$  de la courbe elliptique possède un point d’ordre  $p$ . Une étude facile montre que les courbes elliptiques ordinaires donnant lieu aux éléments de  $S$  présentent des anomalies.
- Le cas  $p$ -supersingulier, qui concerne, comme on s’en doute, les courbes elliptiques ayant réduction potentiellement supersingulière en caractéristique  $p$ . J. Oesterlé m’a convaincu que ces courbes ne donnent naissance à aucun élément  $p > 3$  de  $S$ .

Faute de pouvoir montrer la finitude de  $S$ , nous nous proposons d’aller dans la direction générale suivante : étudier les ensembles  $S_{0,c}$ ,  $S_{0,o}$  et  $S_{0,s}$  de nombres premiers pour lesquels il existe une courbe elliptique sur  $\mathbf{Q}(\mu_p)$   $p$ -cuspidale,  $p$ -ordinaire ou  $p$ -supersingulière respectivement munie d’un sous-groupe  $C$  d’ordre  $p$  qui est  $\mathbf{Q}(\mu_p)$ -rationnel. Ajoutons que notre méthode semble indiquer que l’énumération des trois cas dénote une difficulté croissante.

Dans le cas cuspidal, nous obtenons le résultat suivant (conséquence de la proposition 5, du corollaire 3 de la proposition 6 et de l’appendice).

#### THÉORÈME

*L’ensemble  $S_{0,c}$  est fini.*

Les techniques utilisées dans notre preuve font appel de façon centrale aux idées vieilles de vingt ans de B. Mazur [17] et aux résultats récents de K. Kato (heureusement rédigés pour l’essentiel par A. Scholl [26]) en direction de la conjecture de Birch et Swinnerton-Dyer.

Nous procédons en deux étapes : d’abord nous nous efforçons de montrer que les points  $\mathbf{Q}(\mu_p)$ -rationnels  $p$ -cuspidaux (en le sens ci-dessus, mais notre méthode s’applique aussi parfois aux points  $p$ -ordinaires) de la courbe modulaire  $X_0(p)$  sont quadratiques réels. Nous concluons en appliquant les méthodes de S. Kamienny d’étude des points quadratiques de  $X_0(p)$ .

Soient  $p$  un nombre premier et  $\chi$  un caractère de Dirichlet  $(\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \mathbf{C}^*$ . On résumera par  $H_p(\chi)$  l’assertion suivante : *il existe une forme modulaire parabolique  $f = \sum_n a_n q^n$  de poids 2 pour  $\Gamma_0(p)$  telle que la fonction entière  $L(f, \chi, s)$  qui prolonge la série de Dirichlet  $\sum_{n=1}^{\infty} a_n \chi(n) n^{-s}$  ne s’annule pas en  $s = 1$ .* Nous

démontrons que les nombres premiers appartenant à  $S_{0,c}$  ne vérifient pas  $H_p(\chi)$  pour au moins un caractère  $\chi : (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \mathbf{C}^*$  non quadratique pair. L'étude de  $H_p(\chi)$  est donc essentielle à notre démonstration.

E. Kowalski et P. Michel démontrent que tout nombre premier  $p > 10^{25}$  vérifie  $H_p(\chi)$  pour  $\chi$  non quadratique pair (voir [13]). L'une de leurs démonstrations, qui est élémentaire, est donnée en appendice. On est tenté de ne pas se satisfaire de leur borne. C'est pourquoi nous faisons quelques efforts, indépendamment de Kowalski et Michel, visant à établir  $H_p(\chi)$  dans la deuxième partie. Nos résultats sont partiels, mais nous espérons qu'ils jettent une lumière intéressante sur l'hypothèse  $H_p(\chi)$ . En particulier, nous démontrons que  $H_p(\chi)$  est vérifiée dans les trois cas suivants : lorsque  $p$  est un nombre premier congru à 11 ou 19 modulo 20 et  $\chi$  est impair, lorsque  $\chi$  est injectif et  $p \notin \{2, 3, 5, 7, 13, 1487\}$  et lorsque  $\chi$  est un caractère d'ordre une puissance d'un nombre premier  $\ell > 3$ . L'étude du dernier cas fait intervenir l'idéal d'Eisenstein de l'algèbre de Hecke de  $J_0(p)$ . Cela retiendra peut-être l'attention du lecteur familier avec [16].

Ajoutons que l'hypothèse  $H_p(\chi)$  est fausse lorsque  $p \in \{2, 3, 5, 7, 13\}$ , et lorsque  $\chi$  est quadratique pair. W. Stein a vérifié qu'elle n'est fausse dans aucun autre cas pour  $p < 1000$ . En se fondant sur une variante de la proposition 16, et avec l'aide de Stein, nous avons démontré qu'aucun nombre premier  $p$  vérifiant  $7 < p < 1000$  n'appartient à  $S$ , sauf, peut-être, 13. Les détails relatifs à ces calculs seront publiés séparément.

## 1. Géométrie et arithmétique de $X_0(p)$ et $J_0(p)$

### 1.1. Un lemme élémentaire de géométrie arithmétique

Soit  $p$  un nombre premier. Conformément à l'usage, notons  $X_0(p)$  la courbe sur  $\mathbf{Q}$  qui classe grossièrement les courbes elliptiques généralisées munies d'un sous-groupe cyclique d'ordre  $p$  (voir [1]). Notons  $\mathcal{X}_0(p)$  le modèle régulier minimal de  $X_0(p)$  sur  $\mathbf{Z}$ . Notons  $J_0(p)$  la variété jacobienne de  $X_0(p)$ . Notons  $\mathbf{T}$  le sous-anneau (commutatif) de  $\text{End}_{\mathbf{Q}} J_0(p)$  engendré par les opérateurs de Hecke et l'involution  $W_p$ . (Nos notations coïncident notamment avec celles de [16].) Notons  $\mathcal{J}_0(p)$  le modèle de Néron sur  $\mathbf{Z}$  de  $J_0(p)$  (dont la composante neutre n'est autre que  $\text{Pic}^0(\mathcal{X}_0(p))$ .) Notons  $\mathcal{X}_0(p)_\ell$  la partie lisse de  $\mathcal{X}_0(p)$  : elle est obtenue en ôtant les sections qui sont supersingulières dans la fibre en  $p$  (voir [1]).

Pour étudier l'existence de points  $\mathbf{Q}(\mu_p)$ -rationnels sur  $X_0(p)$  nous ferons usage du résultat suivant. Lorsque  $\chi$  est un caractère à valeurs complexes, on notera  $\mathbf{Z}[\chi]$  le sous-anneau de  $\mathbf{C}$  engendré par les valeurs de  $\chi$ .

PROPOSITION 1

Soit  $p$  un nombre premier. Soient  $K$  et  $L$  deux extensions finies de  $\mathbf{Q}_p$  vérifiant les inclusions  $\mathbf{Q}_p \subset K \subset L \subset \mathbf{Q}_p(\mu_p)$  et d’anneaux des entiers  $\mathcal{O}_K$  et  $\mathcal{O}_L$  respectivement. Posons  $S_0 = \operatorname{spec} \mathcal{O}_K$  et  $S = \operatorname{spec} \mathcal{O}_L$ . Soit  $\mathcal{X}$  un schéma séparé et noethérien sur  $S_0$  de fibre spéciale  $\tilde{\mathcal{X}}$ . Soient  $s_1$  et  $s_2$  des sections du morphisme canonique  $\mathcal{X} \times_{S_0} S \longrightarrow S$  dont les restrictions à la fibre générique (les “points”  $L$ -rationnels) sont notées  $P_1$  et  $P_2$ . Supposons que les restrictions de ces sections à la fibre spéciale de  $S$  coïncident avec une section  $\bar{s} : \operatorname{spec} \mathbf{F}_p \longrightarrow \tilde{\mathcal{X}}$ .

Supposons que pour tout caractère  $\chi : \operatorname{Gal}(L/K) \longrightarrow \mathbf{C}^*$  il existe un morphisme de  $S_0$ -schémas  $\phi_\chi : \mathcal{X} \longrightarrow \mathcal{A}$ , où  $\mathcal{A}$  est le modèle de Néron sur  $S_0$  d’une variété abélienne  $A$  sur  $\mathbf{Q}_p$  et  $t_\chi \in \operatorname{End}_K A \otimes \mathbf{Z}[\chi]$  vérifiant les deux conditions suivantes :

- (i) L’homomorphisme de  $\mathbf{Z}[\chi]$ -modules  $\phi_\chi^* \circ t_\chi^*$  (dédié des morphismes  $\phi_\chi$  et  $t_\chi$  par passage aux espaces cotangents et extension des scalaires) :  $\operatorname{Cotg}_{\phi_\chi(\bar{s})} \mathcal{A} \otimes \mathbf{Z}[\chi] \longrightarrow \operatorname{Cotg}_{\bar{s}} \mathcal{X} \otimes \mathbf{Z}[\chi]$  est surjectif (on dira alors que le couple  $(t_\chi, \phi_\chi)$  constitue une pseudo-immersion formelle au point  $\bar{s}$ ).
- (ii) On a dans  $A(L) \otimes \mathbf{Z}[\chi]$  :

$$\sum_{\sigma \in \operatorname{Gal}(L/K)} \chi(\sigma) t_\chi \sigma(\phi_\chi(P_1)) = \sum_{\sigma \in \operatorname{Gal}(L/K)} \chi(\sigma) t_\chi \sigma(\phi_\chi(P_2)).$$

Alors les sections  $s_1$  et  $s_2$  (et donc  $P_1$  et  $P_2$ ) coïncident.

Démonstration

Notons  $\mathcal{P}$  l’idéal de  $\mathbf{Z}_p[\mu_p]$  au-dessus de  $p\mathbf{Z}_p$ . Notons  $\mathcal{P}_{\mathcal{X}}$  (resp.  $\mathcal{P}_{\mathcal{A}}$ ) l’idéal maximal du complété formel de  $\mathcal{X}$  (resp.  $\mathcal{A}$ ) le long de  $\bar{s}$  (resp.  $\phi_\chi(\bar{s})$ ).

Supposons que  $s_1$  et  $s_2$  ne coïncident pas. Par passage aux espaces cotangents, ces sections définissent des homomorphismes  $s_1^*$  et  $s_2^* : \mathcal{P}_{\mathcal{X}} / \mathcal{P}_{\mathcal{X}}^2 \longrightarrow \mathcal{P} / \mathcal{P}^2$  qui ne coïncident pas par le lemme de Nakayama. Pour  $\chi$  caractère de  $\operatorname{Gal}(L/K)$  notons  $e_\chi = (1/[L : K]) \sum_{\sigma \in \operatorname{Gal}(L/K)} \bar{\chi}(\sigma) \sigma$  l’idempotent de  $\mathbf{Z}[\chi, 1/(p-1)][\operatorname{Gal}(L/K)]$  qui projette sur la composante  $\chi$ -isotypique. Le nombre  $p$  étant premier à  $[L : K]$ , ces idempotents définissent une décomposition en somme directe du  $\mathbf{F}_p$ -espace vectoriel  $\mathcal{P} / \mathcal{P}^2$ . Il existe donc un caractère  $\chi : \operatorname{Gal}(L/K) \longrightarrow \mathbf{Z}[\chi]^*$  tel que  $e_\chi \circ s_1^*$  et  $e_\chi \circ s_2^*$  soient distincts. Comme l’application cotangente  $\phi_\chi^* \circ t_\chi^*$  est surjective, les applications  $e_\chi \circ s_1^* \circ \phi_\chi^* \circ t_\chi^*$  et  $e_\chi \circ s_2^* \circ \phi_\chi^* \circ t_\chi^*$  sont distinctes. Or cela contredit la formule dans  $\mathcal{A}(\mathcal{O}_L) \otimes \mathbf{Z}[\chi]$  déduite de l’hypothèse (ii) par extension au modèle de Néron et application à l’espace cotangent.  $\square$

*Remarque.* L’hypothèse (i) est vérifiée lorsque  $t_\chi \in \operatorname{End}_K A$  et  $t_\chi \circ \phi_\chi$  est une immersion formelle (au sens habituel) au point  $\bar{s}$ , d’où notre terminologie. L’hypothèse (ii) est vérifiée par exemple lorsque  $t_\chi = 1$  et lorsque  $A$ ,  $t_\chi$ ,  $P_1$  et  $P_2$  sont  $M$ -rationnels

pour un sous-corps  $M$  de  $L$  tel que  $t_\chi A(M) = 0$ . Mais ces hypothèses plus faibles ne nous suffisent pas.

### 1.2. Points d'ordre $p$ de $J_0(p)$

L'assertion suivante est une conséquence facile des travaux de Mazur [16].

#### PROPOSITION 2

*La variété abélienne  $J_0(p)$  ne possède pas de point  $\mathbf{Q}(\mu_p)$ -rationnel d'ordre  $p$ .*

#### Démonstration

L'énoncé est évident et sans intérêt si  $p = 2$ . Supposons donc que  $p > 2$ .

Soit  $P \in J_0(p)(\mathbf{Q}(\mu_p))[p]$ . Si  $P$  est non nul, quitte à multiplier par un élément de  $\mathbf{T}$  approprié on peut supposer que l'annulateur de  $P$  dans  $\mathbf{T}$  est un idéal maximal  $\mathfrak{M}$  qui est nécessairement de caractéristique résiduelle  $p$ .

Considérons le sous-schéma  $N$  en  $\mathbf{T}/\mathfrak{M}$ -vectoriel engendré par  $P$ . C'est un sous-schéma  $\mathbf{T}/\mathfrak{M}$ -vectoriel de  $J_0(p)[\mathfrak{M}]$ . Notons  $i$  la dimension de l'espace vectoriel sur  $\mathbf{T}/\mathfrak{M}$  sous-jacent. Comme  $J_0(p)(\mathbf{Q})[\mathfrak{M}]$  est un espace vectoriel de dimension 2 sur  $\mathbf{T}/\mathfrak{M}$  (voir [16, proposition II.14.2] qui s'applique car  $p > 2$ ), on a  $i = 1$  ou 2.

Supposons qu'on ait  $i = 1$ . D'après [16, proposition II.14.1], l'idéal  $\mathfrak{M}$  est un idéal premier d'Eisenstein. Cela n'est possible que lorsque  $p$  divise le numérateur de  $(p-1)/12$ , c'est-à-dire jamais. Cela exclut le cas  $i = 1$ .

Étudions maintenant le cas  $i = 2$ . On obtient alors un homomorphisme de groupes

$$\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q}) \simeq (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \mathrm{Aut} J_0(p)(\bar{\mathbf{Q}})[\mathfrak{M}] \simeq \mathrm{GL}_2(\mathbf{T}/\mathfrak{M}).$$

Comme  $\mathbf{T}/\mathfrak{M}$  est un corps fini de caractéristique  $p > 2$ , une étude facile nous indique que l'image de cet homomorphisme est conjuguée (dans  $\mathrm{GL}_2(\mathbf{T}/\mathfrak{M})$ ) à un sous-groupe diagonal. On obtient donc l'existence d'un sous  $\mathbf{T}/\mathfrak{M}[\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})]$ -module de dimension 1 sur  $\mathbf{T}/\mathfrak{M}$ . L'étude du cas  $i = 1$  exclut précisément cette situation.

On a donc  $P = 0$ . □

#### COROLLAIRE

*Soit  $P$  un point d'ordre fini  $n$  de  $J_0(p)(\mathbf{Q}(\mu_p))$ . L'extension de  $P$  au modèle de Néron de  $J_0(p)$  est d'ordre  $n$  dans la fibre en  $p$ .*

#### Démonstration

On sait que  $n$  est premier à  $p$  d'après la proposition précédente. Un lemme de spécialisation bien connu (voir par exemple [17]) permet de conclure : dans un schéma

en groupe fini et plat sur l’anneau des entiers  $\mathcal{O}$  d’une extension finie de  $\mathbf{Q}_p$ , l’ordre d’un point d’ordre premier à  $p$  est déterminé dans la fibre spéciale. Or la variété abélienne  $J_0(p)$  possède bonne réduction en dehors de  $p$ , si bien que  $J_0(p)[n]$  s’étend en un schéma en groupe fini et plat sur  $\text{Spec } \mathbf{Z}[1/p]$ .  $\square$

*Remarque.* Ce dernier corollaire pourrait se déduire simplement du fait que le modèle de Néron sur  $\mathbf{Z}$  de  $J_0(p)$  est une variété abélienne semi-stable et ne possède pas de sous-schéma en groupe de type  $\mu$  d’ordre  $p$  d’après [16, théorème 2].

### 1.3. Rappels sur la géométrie de la section cuspidale

Considérons les pointes  $\infty$  et  $0$  de  $\mathcal{X}_0(p)$  qui sont des sections  $\text{Spec } \mathbf{Z} \rightarrow \mathcal{X}_0(p)$ . Ces notations désignent encore, par abus, toutes les sections qui s’en déduisent par changement de base (comme dans [16, II.1]). Considérons le morphisme (sur  $\mathbf{Q}$ )  $\phi : X_0(p) \rightarrow J_0(p)$  qui à  $P$  associe la classe du diviseur  $(P) - (\infty)$ . Il s’étend en un morphisme sur  $\text{Spec } \mathbf{Z}$  encore noté  $\phi : \mathcal{X}_0(p)_\ell \rightarrow \mathcal{J}_0(p)$ . Soit  $t \in \mathbf{T}$ . L’action de  $t$  s’étend en un endomorphisme sur  $\text{Spec } \mathbf{Z}$  de  $\mathcal{J}_0(p)$ . Notons  $\phi_t$  le morphisme de  $\mathbf{Z}$ -schémas obtenu en composant  $\phi$  avec  $t$ . Étudions la géométrie de  $\phi_t$  dans la fibre en  $p$ , en reprenant la méthode de [17].

#### PROPOSITION 3

*Supposons qu’on ait  $t \notin p\mathbf{T}$ . Le morphisme  $\phi_t$  est une immersion formelle le long de la fibre spéciale en  $p$  de la pointe  $\infty$ .*

#### Démonstration

Pour démontrer cela il suffit de vérifier d’une part que l’application déduite de  $\phi_t$  sur les corps résiduels des complétés formels est bijective (ce qui est évident) et d’autre part que l’application  $\phi_t^*$  déduite de  $\phi_t$  sur les espaces cotangents en  $\infty$  et  $0$  est surjective. L’étude de ces espaces cotangents est menée à bien dans [17] à l’aide de la structure fournie par la courbe de Tate. D’une part, le complété formel de  $\mathcal{X}_0(p)_{/\mathbf{F}_p}$  en  $\infty$  s’identifie à  $\mathbf{F}_p[[q]]$  (voir [1]), d’où l’isomorphisme de  $\mathbf{F}_p$ -espaces vectoriels  $\text{Cot}_\infty(\mathcal{X}_0(p)_{/\mathbf{F}_p}) \simeq \mathbf{F}_p$ . D’autre part,  $\text{Cot}_0 \mathcal{J}_0(p)_{/\mathbf{F}_p}$  s’identifie, par application de la dualité de Grothendieck, à  $H^0(\mathcal{X}_0(p)_{/\mathbf{F}_p}, \Omega)$ , lequel s’identifie à son tour à  $\text{Hom}(\mathbf{T}, \mathbf{F}_p)$ , par la théorie des  $q$ -développements (voir [17, 2.e])). En utilisant ces identifications dans le diagramme commutatif suivant, l’application  $\phi^*$  est décrite

ainsi (voir [17, démonstration de la proposition 3.1]) :

$$\begin{array}{ccc} \mathrm{Cot}_0(\mathcal{J}_0(p)/\mathbf{F}_p) & \longrightarrow & \mathrm{Cot}_\infty(\mathcal{X}_0(p)/\mathbf{F}_p) \\ \downarrow & & \downarrow \\ \mathrm{Hom}(\mathbf{T}, \mathbf{F}_p) & \longrightarrow & \mathbf{F}_p \\ \psi & \mapsto & \psi(T_1). \end{array}$$

L'application cotangente déduite de l'action de  $t$  sur  $\mathcal{J}_0(p)$  est l'endomorphisme dual de  $t$  dans  $\mathrm{Cot}_0(\mathcal{J}_0(p)/\mathbf{F}_p)$ . En composant les applications cotangentes, et en utilisant la compatibilité fournie par [17, lemme 2.1], on obtient que l'application cotangente  $\phi_t^*$  :

$$\mathrm{Hom}(\mathbf{T}, \mathbf{F}_p) \simeq \mathrm{Cot}_0(\mathcal{J}_0(p)/\mathbf{F}_p) \longrightarrow \mathrm{Cot}_\infty(\mathcal{X}_0(p)/\mathbf{F}_p) \simeq \mathbf{F}_p$$

déduite de  $\phi_t$  est donnée par  $\psi \mapsto \psi(t)$ . Cette application cotangente est évidemment surjective si et seulement si  $t \notin p\mathbf{T}$ .  $\square$

*Remarque.* Contrairement à [17], nous travaillons ici avec des sous-variétés abéliennes de  $J_0(p)$  et non des variétés abéliennes quotient. Cela nous dispense d'étudier les problèmes techniques posés par le comportement des suites exactes courtes de variétés abéliennes après passage aux espaces cotangents. Il serait plus délicat de prouver que  $\phi_t$  en tant que morphisme à valeurs dans la variété abélienne  $tJ_0(p)$  est une immersion formelle en caractéristique  $p$ .

Ce point de vue a également été adopté par Parent dans sa thèse.

Soit  $\chi$  un caractère de Dirichlet  $(\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \mathbf{C}^*$ . Posons  $\mathbf{T}[\chi] = \mathbf{T} \otimes \mathbf{Z}[\chi]$  et  $\mathbf{F}_p[\chi] = \mathbf{F}_p \otimes \mathbf{Z}[\chi]$ .

#### COROLLAIRE

Soit  $t_\chi \in \mathbf{T}[\chi]$  dont l'image dans  $\mathbf{T}[\chi]/p\mathbf{T}[\chi]$  engendre un  $\mathbf{F}_p[\chi]$ -module libre. Le couple  $(t_\chi, \phi)$  constitue une pseudo-immersion formelle au point  $\infty/\mathbf{F}_p$ .

#### Démonstration

Cela se déduit du diagramme figurant dans la démonstration de la proposition 3 en étendant les scalaires à  $\mathbf{Z}[\chi]$ .  $\square$

#### 1.4. La géométrie des sections ordinaires

Notons  $J_S$  l'ensemble des invariants modulaires des courbes elliptiques supersingulières en caractéristique  $p$ . C'est un sous-ensemble de  $\mathbf{P}^1(\mathbf{F}_{p^2})$  déduit du sous- $\mathrm{Spec} \mathbf{F}_p$ -schéma fini de  $\mathbf{P}^1$  défini par le polynôme supersingulier.

Rappelons quelle est la structure de la fibre spéciale en  $p$  de  $\mathcal{X}_0(p)$  (voir [1, V.1]) : elle possède deux composantes irréductibles isomorphes à  $\mathcal{X}_0(1)$  (qui, via

l’invariant modulaire  $j$ , est canoniquement isomorphe à  $\mathbf{P}^1$ ) qui se croisent transversalement en les points supersinguliers. L’involution  $W_p$  échange ces composantes et change un point supersingulier en son conjugué par  $\text{Gal}(\mathbf{F}_{p^2}/\mathbf{F}_p)$ . Considérons la partie lisse  $\mathcal{X}_0(p)_{\ell/\mathbf{F}_p}$  de  $\mathcal{X}_0(p)/\mathbf{F}_p$ . Tout point de  $\mathcal{X}_0(p)_{\ell/\mathbf{F}_p}$  est dans l’image de l’une des deux immersions ouvertes  $\alpha_1$  et  $\alpha_p : \mathbf{P}^1 - J_S \simeq \mathcal{X}_0(1) - j^{-1}(J_S) \longrightarrow \mathcal{X}_0(p)_{\ell/\mathbf{F}_p}$ .

Notons  $\Delta_S$  le groupe des diviseurs de degré zéro à support dans les courbes elliptiques supersingulières en caractéristique  $p$  à isomorphisme près. Rappelons que la composante neutre de la fibre en  $p$  du modèle de Néron de  $J_0(p)$  est un tore sur  $\mathbf{F}_p$  dont le groupe des caractères  $\bar{\mathbf{F}}_p$ -rationnels s’identifie à  $\Delta_S$  (voir [23]). Voici comment est obtenue cette identification. Soit  $\sum_E n_E [E] \in \Delta_S$ . Soit  $\mathcal{F}$  un faisceau inversible sur  $\mathcal{X}_0(p)/\mathbf{F}_p$ . Sa restriction aux composantes irréductibles de  $\mathcal{X}_0(p)/\mathbf{F}_p$ , qui sont isomorphes à  $\mathbf{P}_{\mathbf{F}_p}^1$ , est trivialisable. Notons  $s_0$  et  $s_\infty$  des sections jamais nulles de ces restrictions aux composantes contenant les pointes 0 et  $\infty$  respectivement. Le caractère  $\lambda$  de  $\mathcal{J}_0(p)_{\mathbf{F}_p}^0$  correspondant à  $\sum_E [E] \in \Delta_S$  est donné par la formule

$$\lambda(\tilde{\mathcal{F}}) = \prod_E (s_\infty(P_E)/s_0(P_E))^{n_E},$$

où  $P_E$  désigne le point de  $\mathcal{X}_0(p)/\mathbf{F}_p(\bar{\mathbf{F}}_p)$  correspondant à la courbe elliptique supersingulière  $E$  et où  $\tilde{\mathcal{F}}$  désigne la classe de  $\mathcal{F}$  dans le groupe de Picard. Cette identification munit  $\Delta_S$  d’une structure de  $\mathbf{T}$ -module qui a été étudiée en détail, d’un point de vue théorique et d’un point de vue expérimental, par J.-F. Mestre et Oesterlé [22], [23], par B. Gross et S. Kudla [5] et par Gross [4]. Ajoutons que le groupe des composantes connexes de  $\mathcal{J}_0(p)/\mathbf{F}_p$  est d’ordre égal au numérateur de  $(p-1)/12$  d’après [16, appendice].

Considérons une situation plus générale que celle étudiée dans la section 1.3. Soit  $d$  un entier plus que ou égal à 1 (nous n’utilisons dans le reste de cet article que les cas  $d=1$  et  $d=2$ ; mais il nous semble que le cas général sera utile tôt ou tard). Notons par l’indice supérieur  $(d)$  le passage à la puissance symétrique  $d$ -ième. Considérons le morphisme

$$\phi^{(d)} : X_0(p)^{(d)} \longrightarrow J_0(p),$$

normalisé par le fait que la puissance symétrique  $d$ -ième de la pointe  $\infty$  est envoyée sur zéro. Par propriété universelle des modèles de Néron, il s’étend en un morphisme sur  $\mathbf{Z}$  encore noté  $\phi^{(d)} : \mathcal{X}_0(p)_\ell^{(d)} \longrightarrow \mathcal{J}_0(p)$ .

Pour  $t \in \mathbf{T}$ , la composition de  $\phi^{(d)}$  avec la multiplication par  $t$  dans  $\mathcal{J}_0(p)$ , donne un morphisme sur  $\mathbf{Z}$

$$\phi_t^{(d)} : \mathcal{X}_0(p)_\ell^{(d)} \longrightarrow \mathcal{J}_0(p).$$

Bien entendu, on a  $\phi_t^{(1)} = \phi_t$ .



Quitte à composer  $\phi^{(d)}$  avec la multiplication par  $p - 1$ , ce qui est sans conséquence pour les propriétés de finitude de points rationnels et d'immersion formelle en caractéristique  $p$ , on peut supposer, compte-tenu de ce qui vient d'être dit sur la nature du groupe des composantes, que  $\phi_t^{(d)}(\mathcal{X}_0(p)_{/\mathbf{F}_p}^{(d)} \ell)$  est contenu dans  $\mathcal{J}_0(p)_{/\mathbf{F}_p}^0$ . Soit un caractère  $\lambda$  du tore  $\mathcal{J}_0(p)_{/\mathbf{F}_p}^0$  correspondant au diviseur  $\sum_E n_E[E] \in \Delta_S$ , où  $E$  parcourt les courbes elliptiques supersingulières. Soit  $(j_1, j_2, \dots, j_d) \in (\mathbf{P}^1(\bar{\mathbf{F}}_p) - J_S)^d$ . Posons  $P_d = \alpha_1^{(d)}(j_1, j_2, \dots, j_d)$ . On a

$$\lambda \circ \phi^{(d)}(P_d) = \prod_{i=1}^d \prod_E (j_i - j(E))^{n_E}.$$

Cette formule a été obtenue pour  $d = 1$  par Mestre et Oesterlé [23]; la formule générale s'en déduit en remarquant que  $\phi^{(d)}(P_1, \dots, P_d) = \phi(P_1) + \dots + \phi(P_d)$ .

Pour  $u \in \{1, 2, \dots, d\}$ , notons  $\iota_u$  l'homomorphisme de groupes  $\Delta_S \rightarrow \bar{\mathbf{F}}_p$  donné par la formule

$$\iota_u \left( \sum_E n_E[E] \right) = \sum_E \frac{n_E}{(j - j(E))^u}.$$

Soit  $j \in \mathbf{P}^1(\bar{\mathbf{F}}_p) - J_S$ . Posons  $P = \alpha_1(j) \in \mathcal{X}_0(p)_{\ell/\mathbf{F}_p}(\bar{\mathbf{F}}_p)$ . Notons  $P^{(d)}$  la puissance symétrique  $d$ -ième de  $P$ .

#### PROPOSITION 4

Soit  $t \in \mathbf{T}$ . S'il existe  $\delta_1, \delta_2, \dots, \delta_d \in \Delta_S$  tels que le déterminant de la matrice  $(\iota_u(t\delta_i))_{u,i \in \{1,2,\dots,d\}}$  soit non nul dans  $\mathbf{F}_p$ , la restriction à la fibre spéciale en  $p$  du morphisme  $\phi_t^{(d)}$  est une immersion formelle au point  $P^{(d)}$ .

#### Démonstration

Posons  $t\delta_i = \sum_E m_{E,i}[E]$ . Notons  $\lambda_i$  le caractère du tore  $\mathcal{J}_0(p)_{/\mathbf{F}_p}^0$  correspondant à  $t\delta_i$  par l'identification mentionnée ci-dessus. Notons  $\lambda$  le morphisme de groupes algébriques  $(\lambda_1, \dots, \lambda_d) : \mathcal{J}_0(p)_{/\mathbf{F}_p}^0 \rightarrow \mathbf{G}_m^d/\bar{\mathbf{F}}_p$ .

Il faut donc établir que l'homomorphisme d'anneaux locaux  $\phi_t^{(d)*}$  sur les complétés formels déduit de  $\phi_t^{(d)}$  est surjectif. Il suffit pour cela de prouver que l'homomorphisme d'anneaux  $\phi^{(d)*} \circ \lambda^*$  est surjectif, c'est-à-dire que le morphisme  $\lambda \circ \phi^{(d)} : \mathcal{X}_0(p)_{\ell/\mathbf{F}_p}^{(d)} \rightarrow \mathbf{G}_m^d/\mathbf{F}_p$  est une immersion formelle au point  $P^{(d)}$ .

Composons encore par l'immersion ouverte  $\alpha_1^{(d)}$ . Il suffit de démontrer que le morphisme  $\lambda \circ \phi^{(d)} \circ \alpha_1^{(d)} : (\mathbf{P}^1 - \mathcal{J})^{(d)} \rightarrow \mathbf{G}_m^d$  est une immersion formelle en  $j^{(d)}$ . Notons  $\sigma_u$  le  $u$ -ième polynôme symétrique élémentaire en  $j_1, \dots, j_d$ . La  $i$ -ième

coordonnée du morphisme  $\lambda \circ \phi \circ \alpha_1^{(d)}$  est donnée par la fraction rationnelle  $F_i$  :

$$\begin{aligned} (j_1, \dots, j_d) \mapsto F_i(j_1, \dots, j_d) &= \prod_{k=1}^d \prod_E (j_k - j(E))^{m_{E,i}} \\ &= \prod_E \left( \sum_{u=0}^d (-1)^u \sigma_{d-u} j(E)^u \right)^{m_{E,i}}. \end{aligned}$$

L'espace cotangent en  $j^{(d)}$  de  $(\mathbf{P}^1 - \mathcal{S})^{(d)}$  a pour base la famille  $d\sigma_1, \dots, d\sigma_d$ . Un calcul évident de différentielle logarithmique donne

$$\frac{dF_i}{F_i} = \sum_E \frac{m_{E,i}}{\prod_{k=1}^d (j_k - j(E))} \sum_{u=0}^{d-1} (-1)^u j(E)^u d\sigma_{d-u}.$$

Le morphisme  $\lambda \circ \phi \circ \alpha_1^{(d)}$  est une immersion formelle en  $(j_1, \dots, j_d)$  si et seulement la famille  $(dF_i)$  est linéairement indépendante dans l'espace cotangent en  $(j_1, \dots, j_d)$  de  $(\mathbf{P}^1 - \mathcal{S})^{(d)}$ .

Comme on examine la situation en  $(j_1, \dots, j_d) = (j, \dots, j)$ , cela revient à vérifier que la matrice carrée d'ordre  $d$  de terme  $(i, u)$  égal à  $(\sum_E m_{E,i} j(E)^{u-1} / (j - j(E))^d)$  est inversible. Une manipulation élémentaire montre que cette matrice est de déterminant égal à celui de la matrice  $(\iota_u(t\delta_i))_{u,i \in \{1,2,\dots,d\}}$ . Cela achève notre démonstration.  $\square$

*Remarque.* Cette condition d'indépendance linéaire est à comparer à celle obtenue par Kamienny dans [9], pour  $P = \infty$ ; néanmoins nous ne faisons pas intervenir la suite des opérateurs de Hecke  $T_1, T_2, \dots$ .

Comme nous le verrons dans la troisième partie, la proposition 4 est utile à l'étude au cas par cas de la non-existence de points  $p$ -ordinaires de  $X_0(p)$ . Pour étudier de façon uniforme ces points, il faudrait savoir comparer les  $\mathbf{T}$ -modules  $\Delta_S$  et  $H_1(X_0(p)(\mathbf{C}), \mathbf{Z})$  de façon à comprendre la relation entre les valeurs de fonctions  $L$  et la structure de  $\mathbf{T}$ -module de  $\Delta_S$ . Les meilleures informations dont on dispose dans cette direction semblent être contenues dans [5] et [4].

Notons encore  $\iota_u$  l'homomorphisme de  $\mathbf{Z}[\chi]$ -modules :  $\Delta_S \otimes \mathbf{Z}[\chi] \longrightarrow \mathbf{F}_p[\chi]$  obtenu à partir de  $\iota_u$  par extension des scalaires par  $\mathbf{Z}[\chi]$ .

#### COROLLAIRE

Soit  $t_\chi \in \mathbf{T} \otimes \mathbf{Z}[\chi]$ . S'il existe  $\delta_1, \delta_2, \dots, \delta_d \in \Delta_S \otimes \mathbf{Z}[\chi]$  tels que le déterminant de la matrice  $(\iota_u(t_\chi \delta_i))_{u,i \in \{1,2,\dots,d\}}$  soit inversible dans  $\mathbf{F}_p[\chi]$ , le couple  $(t_\chi, \phi^{(d)})$  est une pseudo-immersion formelle au point  $P^{(d)}$ .

*Démonstration*

Cela se déduit de la proposition 4 par extension des scalaires par  $\mathbf{Z}[\chi]$ .  $\square$

*1.5. Discussion de la littérature sur les travaux de Kato*

Soit  $\chi$  un caractère de Dirichlet  $(\mathbf{Z}/p\mathbf{Z})^* \rightarrow \mathbf{C}^*$ , identifié par la théorie du corps de classes à un caractère de  $\text{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ . Soit  $t_\chi$  un élément de  $\mathbf{T}[\chi]$  engendrant un sous-anneau intègre de  $\mathbf{T}[\chi]$  et tel que  $t_\chi g = 0$  dès lors que  $g \in S_2(\Gamma_0(p))$  vérifie  $L(g, \chi, 1) = 0$ . Posons  $K = t_\chi \mathbf{T}[\chi] \otimes \mathbf{Q}$ ; c'est un sous-corps de nombres de  $\mathbf{T}[\chi] \otimes \mathbf{Q}$ .

Nous avons besoin de l'énoncé suivant, que nous comprenons comme une conséquence des résultats annoncés par Kato (série d'exposés à l'IAS (Institute for Advanced Study), Princeton, automne 1995), qui résulte de la conjecture de Birch et Swinnerton-Dyer pour les variétés abéliennes sur  $\mathbf{Q}$  et qui ne dépend que de  $p$ ,  $\chi$  et  $K$ .

*La composante  $\chi$ -isotypique du  $\text{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ -module  
 $t_\chi J_0(p)(\mathbf{Q}(\mu_p)) \otimes \mathbf{Z}[\chi]$  est finie.*

Signalons que cela ne semble pas résulter de [12]. En attendant que Kato publie ses travaux, sans prétendre donner une démonstration, essayons d'orienter le lecteur dans la lecture des textes de Scholl [26] et K. Rubin [25] pour obtenir le résultat dont nous avons besoin.

Soit  $f \in S_0(\Gamma_0(p))$  une forme primitive telle que  $t_\chi f \neq 0$ ; on a donc  $L(f, \chi, 1) \neq 0$ . Considérons la forme modulaire  $f_\chi$  obtenue en tordant la forme  $f$  par le caractère  $\chi$ . C'est une forme primitive pour  $\Gamma_1(p^2)$  lorsque  $\chi \neq 1$ . La théorie de G. Shimura lui associe une variété abélienne  $A_\chi$  simple sur  $\mathbf{Q}$  qui est un quotient de  $J_1(p^2)$ . Rappelons quels sont les liens entre  $A_\chi$  et la variété abélienne  $A$  associée à  $f$  par la théorie de Shimura [27] :  $A_\chi$  est un facteur de la décomposition à isogénie près de la variété abélienne obtenue à partir de  $A/\mathbf{Q}(\mu_p)$  par restriction des scalaires de  $\mathbf{Q}(\mu_p)$  à  $\mathbf{Q}$ . De plus la série  $L$  de  $A_\chi$  est donnée par la formule :

$$L(A_\chi, s) = \prod_{f'} L(f', s),$$

où  $f'$  parcourt les formes primitives conjuguées de la forme modulaire  $f_\chi$ . Il s'ensuit que la non nullité de  $L(f, \chi, 1)$  équivaut à la non nullité de  $L(A_\chi, 1)$  et donc à la non nullité de  $L(f_\chi, 1)$ . Par ailleurs la finitude de  $A_\chi(\mathbf{Q})$  équivaut à la finitude de la composante  $\chi$ -isotypique de  $t_\chi J_0(p)(\mathbf{Q}(\mu_p)) \otimes \mathbf{Z}[\chi]$ . On se ramène ainsi à démontrer que  $A_\chi(\mathbf{Q})$  est un groupe fini.

La variété abélienne  $A_\chi$  possède des multiplications par un ordre  $\mathcal{O}$  du corps de nombres  $K$ . Soit  $\lambda$  un idéal maximal de  $\mathcal{O}$ . Notons  $l$  la caractéristique résiduelle

correspondante. Pour rester dans un cadre aussi proche que possible de celui de [25], nous imposons à  $l$  d’être distinct de  $p$  et totalement décomposé dans  $K$  (cela est loisible sans être nécessaire). On a donc  $K_\lambda = \mathbf{Q}_l$ . Le module de Tate  $\lambda$ -adique  $T_\lambda$  de  $A_\chi$  fournit une représentation  $l$ -adique  $V$  de dimension 2 et continue :

$$\rho : \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \text{GL}(T_\lambda \otimes \mathbf{Q}_l) \simeq \text{GL}_2(K_\lambda) \simeq \text{GL}_2(\mathbf{Q}_l) \simeq \text{GL}(V).$$

Cette représentation  $l$ -adique entre dans le cadre de l’étude de [25, section 1]. Pour prouver la finitude de  $A_\chi(\mathbf{Q})$ , il suffit de prouver la finitude du groupe de Selmer associé (voir [25]). Pour cela on applique le formalisme des systèmes d’Euler comme dans [25, sections 2 et 3] (les preuves détaillées figurent dans les références indiquées dans [25]). Pour appliquer ce formalisme on vérifie que  $V$  est bien muni d’un système d’Euler, en adaptant [26, section 5.2] au cas où  $A_\chi$  n’est pas nécessairement une courbe elliptique. Plus précisément, on utilise que  $J_1(p^2)$  et donc  $A_\chi$  est un quotient de  $J(p^2)$ ; or dans [26] est établi l’existence d’un système d’Euler, noté  $(\xi_r \in H^1(\mathbf{Q}(\mu_r), T_l(J(N))))_{r \in \mathcal{R}}$  (où  $\mathcal{R}$  est l’ensemble des entiers sans facteur carré premiers à  $p$ ), relatif au module de Tate  $T_l(J(N))$   $l$ -adique de  $J(p^2)$  qui par projection sur la variété abélienne  $A_\chi$  donne lieu à un système d’Euler  $(\xi_r(A_\chi))_{r \in \mathcal{R}}$  relatif à  $V$ , que l’on peut utiliser pour appliquer les théorèmes de [25]. La non nullité de  $\xi_1(A_\chi)$  résulte de la non nullité de  $L(f_\chi, 1)$  (nous n’avons pas vérifié ce point essentiel, qui est démontré dans [25, théorème 5.2.7], lorsque  $A_\chi$  est un quotient elliptique).

Pour appliquer [25, théorème 3.1], et conclure à la finitude du groupe de Selmer il faut encore vérifier que l’hypothèse  $\text{Hyp}(\mathbf{Q}_\infty, V)$  de [25, section 3] est satisfaite. C’est-à-dire l’existence de  $\tau \in \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$  agissant trivialement sur les racines de l’unité d’ordre une puissance de  $l$  et tel que l’endomorphisme  $\rho(\tau)$  soit non-scalaire et possède 1 comme valeur propre.

Comme  $J_0(p)$  (et donc aussi  $A$ ) a réduction purement multiplicative en  $p$ , il existe  $\tau_0 \in \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$  (plus précisément dans un groupe de décomposition en  $p$ ) agissant de façon unipotente et non triviale sur le module de Tate  $l$ -adique de  $A$ . En raison des accouplements de Weil, il en résulte que  $\tau_0$  agit trivialement sur les racines d’ordre une puissance de  $l$ . Posons  $\tau = \tau_0^{p-1} \in \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ . Cet élément opère de façon unipotente et non triviale sur le module de Tate  $l$ -adique de  $A$  et trivialement sur les racines d’ordre une puissance  $l$ . Puisque  $A_\chi$  est obtenue par restriction des scalaires de  $\mathbf{Q}(\mu_p)$  à  $\mathbf{Q}$ , et que  $\tau$  opère trivialement sur  $\mathbf{Q}(\mu_p)$ ,  $\rho(\tau)$  est unipotent et non trivial. Il satisfait donc les conditions cherchées. Cela prouve l’hypothèse  $\text{Hyp}(\mathbf{Q}_\infty, V)$ .

### 1.6. Points quadratiques $p$ -cuspidaux

La question des points quadratiques se traite grâce aux méthodes de Kamienny et Mazur [11]. À noter que la question des points  $\mathbf{Q}(\sqrt{\pm p})$ -rationnels de  $X_1(p)$  a été

étudiée dans [8] et [7]. Par un *point  $p$ -cuspidal*  $\mathbf{Q}(\mu_p)$ -rationnel de  $Y_0(p)$ , nous entendons un point  $\mathbf{Q}(\mu_p)$ -rationnel de  $X_0(p)$  distinct d'une pointe et d'invariant modulaire qui est de valuation  $p$ -adique strictement négative (de façon équivalente c'est un point dont l'extension en une  $\text{spec } \mathbf{Z}[\mu_p]$ -section coïncide avec une pointe dans la fibre en  $p$  mais pas dans la fibre générique).

PROPOSITION 5

*La courbe modulaire  $Y_0(p)$  ne possède pas de points quadratiques  $\mathbf{Q}(\mu_p)$ -rationnels qui sont  $p$ -cuspidaux lorsque  $p > 19$  et  $p \neq 37$ .*

*Démonstration*

Supposons que la courbe modulaire  $X_0(p)$  possède un tel point  $P$  (qui serait bien entendu  $\mathbf{Q}(\sqrt{p})$  ou  $\mathbf{Q}(\sqrt{-p})$  rationnel). Il en résulterait l'existence d'un point  $\mathbf{Q}$ -rationnel du carré symétrique  $X_0(p)^{(2)}$  de  $X_0(p)$ . Un tel point s'étend en un point sur  $\mathbf{Z}$  de  $\mathcal{X}_0(p)^{(2)}$ . Comme ce point est déduit d'un point cuspidal  $\mathbf{Q}(\mu_p)$ -rationnel et de son conjugué, sa réduction modulo  $p$  coïncide avec le carré symétrique de l'une des deux pointes de la fibre en  $p$  de  $\mathcal{X}_0(p)$ . Quitte à appliquer l'involution  $W_p$ , on peut supposer que cette pointe est  $\infty$ .

Considérons maintenant le morphisme  $\phi^{(2)} : \mathcal{X}_0(p)_\ell^{(2)} \longrightarrow \mathcal{J}_0(p)$  (voir section 1.4). Composons-le avec le morphisme canonique de schémas en groupes sur  $\mathbf{Z}$ ,

$$\mathcal{J}_0(p) \longrightarrow \tilde{\mathcal{J}},$$

où  $\tilde{\mathcal{J}}$  est le modèle de Néron sur  $\mathbf{Z}$  du quotient d'Eisenstein  $\tilde{J}$  de  $J_0(p)$  (voir [16]).

Le fait que  $\tilde{\mathcal{J}}$  ne possède qu'un nombre fini de points  $\mathbf{Q}$ -rationnels (voir [16]) permet d'utiliser le critère d'immersion formelle de Kamienny [10] : si les opérateurs  $T_1$  et  $T_2$  sont  $\mathbf{F}_p$ -linéairement indépendants dans  $\mathbf{T}/(p\mathbf{T} + \cap_{k=1}^\infty \mathcal{I}^k)$  (où  $\mathcal{I}$  désigne l'idéal d'Eisenstein de  $\mathbf{T}$ , et où  $T_1$  et  $T_2$  sont les éléments de  $\mathbf{T}$  déduits des correspondances de Hecke  $T_1$  et  $T_2$ ) alors  $P$  coïncide avec la pointe  $\infty$ . Prenons note que Kamienny n'a utilisé son critère d'immersion formelle qu'en caractéristiques distinctes de 2 et  $p$  ; en réalité l'argument fonctionne de façon identique en caractéristique  $p$  si on tient compte du fait que  $J_0(p)$  ne possède pas de point  $\mathbf{Q}$ -rationnel d'ordre  $p$ , ce qui est prouvé dans [16].

Supposons que les opérateurs  $T_1$  et  $T_2$  soient linéairement dépendants. On a alors  $T_2 \in p\mathbf{T} + \mathbf{Z}$ . L'inégalité de Ramanujan-Petersson impose qu'on a  $T_2 \in \mathbf{Z}$  ; en effet, si  $\alpha$  et  $\beta$  sont deux valeurs propres distinctes de  $T_2$ , le nombre  $(\alpha - \beta)/p$  est un entier algébrique non nul dont toutes les valeurs absolues archimédiennes sont bornées par  $4\sqrt{2}/p$ , et on a  $4\sqrt{2}/p < 1$  lorsque  $p > 7$ .

Kamienny [9], a démontré que  $T_2$  n'est pas un scalaire dans le quotient d'Eisenstein lorsque  $p > 61$ . Un examen des tables de formes modulaires montre que cela est encore le cas lorsque  $p > 19$  et  $p \neq 37$ .  $\square$

*Remarque.* Au vu de la section 1.7, seuls nous intéressent les cas où  $p \equiv 1 \pmod{4}$ . Y a-t-il des points  $p$ -cuspidaux et  $\mathbf{Q}(\sqrt{p})$ -rationnels de  $Y_0(p)$  pour  $p = 17$  et  $p = 37$  ?

### 1.7. Preuve du théorème principal

Par point  $p$ -supersingulier  $\mathbf{Q}(\mu_p)$ -rationnel de  $X_0(p)$  on entendra un point  $\mathbf{Q}(\mu_p)$ -rationnel dont l’extension en une  $\text{spec } \mathbf{Z}[\mu_p]$ -section est supersingulière dans la fibre en  $p$ .

#### PROPOSITION 6

Soient  $P_1$  et  $P_2$  deux points  $\mathbf{Q}(\mu_p)$ -rationnels de  $X_0(p)$  dont les extensions  $s_1$  et  $s_2$  à  $\mathcal{X}_0(p)_\ell$  coïncident sans être supersingulières dans la fibre en  $p$ . Supposons que pour tout caractère de Dirichlet  $\chi$  de  $\text{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ , il existe  $t_\chi \in \mathbf{T} \otimes \mathbf{Z}[\chi]$  tel que la classe du diviseur  $t_\chi((P_1) - (P_2))$  soit d’ordre fini dans la composante  $\chi$ -isotypique de  $J_0(p)(\mathbf{Q}(\mu_p)) \otimes \mathbf{Z}[\chi]$  et tel que le couple  $(t_\chi, \phi)$  soit une pseudo-immersion formelle en caractéristique  $p$  au point  $P_1/\mathbf{F}_p = P_2/\mathbf{F}_p$ . On a alors  $P_1 = P_2$ .

#### Démonstration

C’est une application facile de la proposition 1 avec  $\mathcal{X} = \mathcal{X}_0(p)$ ,  $\mathcal{A} = \mathcal{J}_0(p)$ ,  $\phi_\chi = \phi$ ,  $L = \mathbf{Q}_p(\mu_p)$  et  $K = \mathbf{Q}_p$ . L’hypothèse (i) est satisfaite. Considérons l’élément  $\sum_{\sigma \in \text{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})} t_\chi \chi(\sigma) \sigma(\phi_\chi \circ s_1 - \phi_\chi \circ s_2)$  de  $\mathcal{J}_0(p)(\mathbf{Z}[\mu_p]) \otimes \mathbf{Z}[\chi]$ . Il est nul dans la fibre en  $p$  et d’ordre fini dans la fibre générique. Il est donc nul d’après le corollaire de la proposition 2 et par platitude de  $\mathbf{Z}[\chi]$ . Cela prouve que (ii) est vérifié puisque  $\text{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q}) \simeq \text{Gal}(\mathbf{Q}_p(\mu_p)/\mathbf{Q}_p)$ .  $\square$

#### COROLLAIRE 1

Soit  $K$  un sous-corps de  $\mathbf{Q}(\mu_p)$  d’anneau des entiers  $\mathcal{O}_K$ . Soit  $P$  un point  $\mathbf{Q}(\mu_p)$ -rationnel de  $Y_0(p)$  non  $p$ -supersingulier. Notons  $P/\mathbf{F}_p$  le point  $\mathbf{F}_p$ -rationnel obtenu en restreignant à la fibre en  $p$  l’extension en une  $\text{spec } \mathbf{Z}[\mu_p]$ -section de  $P$ . Supposons que pour tout caractère de  $\text{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$  qui est non trivial sur  $\text{Gal}(\mathbf{Q}(\mu_p)/K)$ , il existe  $t_\chi \in \mathbf{T} \otimes \mathbf{Z}[\chi]$  tel que la composante  $\chi$ -isotypique de  $t_\chi J_0(p)(\mathbf{Q}(\mu_p)) \otimes \mathbf{Z}[\chi]$  soit finie et que le couple  $(t_\chi, \phi)$  soit une pseudo-immersion formelle au point  $P/\mathbf{F}_p$ . Alors  $P$  est  $K$ -rationnel.

#### Démonstration

Il suffit évidemment de prouver qu’on a  $P_1 = P_2$  pour  $P_1 = P$  et  $P_2 = P^{\sigma_0}$ , où  $\sigma_0$  engendre le groupe cyclique  $\text{Gal}(\mathbf{Q}(\mu_p)/K)$ . Comme l’extension  $\mathbf{Q}(\mu_p)|\mathbf{Q}$  est totalement ramifiée en  $p$ , les extensions  $s_1$  et  $s_2$  de  $P_1$  et  $P_2$  à  $\mathcal{X}_0(p)$  coïncident dans la fibre en  $p$ . Si  $\chi$  est non trivial sur  $\text{Gal}(\mathbf{Q}(\mu_p)/K)$ , la classe de  $t_\chi((P_1) - (P_2))$  est d’ordre fini dans la composante  $\chi$ -isotypique de  $J_0(p)(\mathbf{Q}(\mu_p))$ . Sinon, on a, puisque

$$P_2 = P_1^{\sigma_0},$$

$$\sum_{\sigma \in \text{Gal}(\mathbf{Q}(\mu_p)/K)} \chi(\sigma)(P_1^\sigma - P_2^\sigma) = 0.$$

On peut donc appliquer la proposition 6 à  $P_1$  et  $P_2$ , d'où  $P_1 = P_2$ .  $\square$

#### COROLLAIRE 2

Soit  $P$  un point  $p$ -cuspidal  $\mathbf{Q}(\mu_p)$ -rationnel de  $Y_0(p)$ . Si on a  $H_p(\chi)$  pour tout caractère de Dirichlet de  $(\mathbf{Z}/p\mathbf{Z})^*$  non quadratique pair, alors  $P$  est un point quadratique réel.

#### Démonstration

Notons  $K$  le plus grand sous-corps totalement réel de  $\mathbf{Q}(\mu_p)$  de degré 1 ou 2. Appliquons le corollaire 1 de la proposition 6 pour prouver que  $P$  est  $K$ -rationnel. Observons d'abord qu'il suffit de prouver que pour tout caractère  $\chi \neq 1$  de  $\text{Gal}(\mathbf{Q}(\mu_p)/K)$  il existe  $t_\chi \in \mathbf{T} \otimes \mathbf{Z}[\chi]$ ,  $t_\chi \neq 0$ , tel que la composante  $\chi$ -isotypique de  $t_\chi J_0(p)(\mathbf{Q}(\mu_p))$  soit finie. (Cette dernière propriété est inchangée si on remplace  $t_\chi$  par un élément de  $\mathbf{Q}[\chi]_{t_\chi}$ .) D'après le lemme d'approximation dans les anneaux de Dedekind, il existe  $a \in \mathbf{Q}[\chi]$  tel que  $at_\chi \in \mathbf{T} \otimes \mathbf{Z}[\chi]$  et tel que l'image de  $at_\chi$  dans  $\mathbf{T}[\chi]/p\mathbf{T}[\chi]$  soit un  $\mathbf{F}_p[\chi]$ -module libre. D'après le corollaire de la proposition 3, le couple  $(t_\chi, \phi_\chi)$  est une pseudo-immersion formelle au point  $\infty_{\mathbf{F}_p} = P_{\mathbf{F}_p}$ . Cela permet de conclure par application du corollaire 1 de la proposition 6.

Il reste à établir que  $H_p(\chi)$  entraîne l'existence de  $t_\chi$ . Soit  $f \in S_2(\Gamma_0(p))$  telle que  $L(f, \chi, 1) \neq 0$ . Toute forme primitive  $f'$  conjuguée de  $f$  par  $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}[\chi])$  vérifie également  $L(f', \chi, 1) \neq 0$  (cela se voit par exemple en utilisant l'intégration sur les classe d'homologie comme dans la section 2.1). Soit  $t_\chi \in \mathbf{T}[\chi]$  tel que  $t_\chi$  annule toute forme primitive  $f'$  qui n'est pas conjuguée de  $f$  par  $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}[\chi])$ . Le sous-anneau de  $\mathbf{T}[\chi]$  engendré par  $t_\chi$  est alors intègre. La finitude de la composantes  $\chi$ -isotypique de  $t_\chi J_0(p)(\mathbf{Q}(\mu_p))$  résulte des travaux de Kato (voir section 1.5).  $\square$

*Remarque.* Nous ne prétendons pas que  $L(f, \chi, 1) \neq 0$  entraîne  $L(g, \chi, 1) \neq 0$  lorsque  $f$  et  $g$  sont des formes primitives conjuguées par  $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ . Comme on le verra dans la proposition 7, l'hypothèse  $H_p(\chi)$  ne dépend que de la classe de conjugaison de  $\chi$ .

#### COROLLAIRE 3

Si  $p$  est congru à 1 modulo 4,  $p > 17$  et  $p \neq 37$ , supposons qu'on ait  $H_p(\chi)$  pour tout caractère  $\chi$  non quadratique. Alors  $Y_0(p)$  ne possède pas de points  $\mathbf{Q}(\mu_p)$ -rationnels  $p$ -cuspidaux.

Si  $p$  est congru à  $-1$  modulo 4, et  $p \notin \{3, 7\}$ , supposons qu'on ait  $H_p(\chi)$

pour tout caractère  $\chi$ . Alors  $Y_0(p)$  ne possède pas de points  $\mathbf{Q}(\mu_p)$ -rationnels  $p$ -cuspidaux.

*Démonstration*

Soit  $P$  un point  $\mathbf{Q}(\mu_p)$ -rationnel et  $p$ -cuspidal de  $Y_0(p)$ . Si  $p$  est congru à  $-1$  modulo 4, le corollaire 3 entraîne que  $P$  est  $\mathbf{Q}$ -rationnel. D’après [16, corollaire 4.4],  $Y_0(p)$  ne possède pas de point  $\mathbf{Q}$ -rationnel  $p$ -cuspidal lorsque  $p \notin \{2, 3, 5, 7, 13\}$ .

Si  $p$  est congru à 1 modulo 4, le point  $P$  est quadratique d’après le corollaire 2. Mais cela est exclu d’après la proposition 5.  $\square$

*Remarques.* William Stein a vérifié l’hypothèse  $H_p(\chi)$  lorsque  $\chi$  n’est pas quadratique pair et  $p \notin \{2, 3, 5, 7, 13\}$  et  $p < 1000$ . Cela prouve que l’ensemble  $S_{0,c}$  ne contient aucun élément  $p < 1000$  en dehors de l’ensemble  $\{2, 3, 5, 7, 13, 17, 37\}$ .

Lorsque  $K$  est un sous-corps de  $\mathbf{Q}(\mu_p)$ , on peut démontrer l’inexistence de points  $K$ -rationnels  $p$ -cuspidaux comme ci-dessus en se contentant de l’hypothèse  $H_p(\chi)$  pour les caractères  $\chi$  qui se factorisent par le groupe quotient de  $(\mathbf{Z}/p\mathbf{Z})^*$  correspondant à  $\text{Gal}(K/\mathbf{Q})$ .

Une démonstration analogue à celle que nous venons de proposer, et ses applications aux points rationnels de  $X_0(p)$  comme ci-dessus, mais sous l’hypothèse plus forte que le morphisme  $\phi_\chi$  peut être choisi indépendamment de  $\chi$  et que  $t_\chi = 1$  figure implicitement dans [17] (voir la formalisation figurant dans [17, corollaire 4.3]).

## 2. Méthodes non-analytiques et séries de Dirichlet

### 2.1. Rappels sur les symboles modulaires

Dans cette deuxième partie la courbe modulaire  $X_0(p)$  sera exclusivement vue comme la surface de Riemann compacte et connexe  $X_0(p)(\mathbf{C}) = \Gamma_0(p) \backslash \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$ , où  $\mathcal{H}$  est le demi-plan de Poincaré. On notera  $ptes$  l’ensemble  $\Gamma_0(p) \backslash \mathbf{P}^1(\mathbf{Q})$  de ses pointes.

Soit  $(\alpha, \beta) \in \mathbf{P}^1(\mathbf{Q})^2$ . Notons  $\{\alpha, \beta\}$  la classe d’homologie, dite symbole modulaire, dans  $H_1(X_0(p)(\mathbf{C}), ptes; \mathbf{Z})$  définie par la classe de l’image dans  $X_0(p)$  d’un chemin continu reliant  $\alpha$  à  $\beta$  dans  $\mathcal{H}$ . Observons que, lorsque  $\alpha$  et  $\beta$  ont des dénominateurs premiers à  $p$  (resp. divisibles par  $p$ ), ils sont conjugués par  $\Gamma_0(p)$  et  $\{\alpha, \beta\}$  appartient au sous-groupe  $H_1(X_0(p)(\mathbf{C}), \mathbf{Z})$  de  $H_1(X_0(p)(\mathbf{C}), ptes; \mathbf{Z})$ .

Lorsque  $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbf{Z})$ , le symbole modulaire  $\{g0, g\infty\}$  ne dépend que de  $\Gamma_0(p)g$ , c’est-à-dire que de la classe de  $(c, d)$  dans  $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$ . Notons le  $\xi(c, d)$ , ou encore, en notation inhomogène,  $\xi(c/d)$ . Lorsque  $c$  et  $d$  parcourent les entiers



premiers à  $p$ , les classes  $\xi(c/d)$  engendrent  $H_1(X_0(p)(\mathbf{C}); \mathbf{Z})$ . Lorsque  $a \in \mathbf{Z}$ , on a  $\xi(a) = \{0, 1/a\}$ . On a  $\xi(1) = 0$ . L'involution  $W_p$  de  $X_0(p)$  est déduite de  $z \mapsto -1/pz$  sur  $\mathcal{H}$ . On a donc la formule

$$W_p(\xi(a)) = -\{-a/p, \infty\}.$$

L'espace  $H_1(X_0(p)(\mathbf{C}), \text{ptes}; \mathbf{Z})$  est muni de l'involution donnée par la conjugaison complexe. Cette involution est déduite de l'involution  $z \mapsto -\bar{z}$  de  $\mathcal{H}$ . Elle agit donc par  $\xi(u) \mapsto -\xi(1/u) = \xi(-u)$  sur les symboles modulaires. Elle induit une involution sur  $H_1(X_0(p)(\mathbf{C}); \mathbf{Z})$ . On notera  $H_1(X_0(p)(\mathbf{C}); \mathbf{Z})_+$  et  $H_1(X_0(p)(\mathbf{C}); \mathbf{Z})_-$  les parties invariantes et anti-invariantes de  $H_1(X_0(p)(\mathbf{C}); \mathbf{Z})$  par la conjugaison complexe. Rappelons que  $H_1(X_0(p)(\mathbf{C}); \mathbf{Z})$  est un module acyclique sous l'action de la conjugaison complexe (voir [20, section 1.3]).

## 2.2. Reformulation topologique

Dans le reste de cette seconde partie, par *caractère* on entendra caractère de Dirichlet  $(\mathbf{Z}/p\mathbf{Z})^* \rightarrow \mathbf{C}^*$ .

### PROPOSITION 7

Soit  $\chi$  un caractère différent de 1. On a  $H_p(\chi)$  si et seulement si le symbole modulaire

$$\theta_\chi = \sum_{a=1}^{p-1} \chi(a) \left\{ \frac{a}{p}, \infty \right\} \in H_1(X_0(p)(\mathbf{C}), \mathbf{Z}[\chi])$$

est non nul.

### Démonstration

Notons  $\tau(\chi)$  la somme de Gauss  $\sum_{a=0}^{p-1} \chi(a) e^{-2i\pi a/p}$ . On a  $H_p(\chi)$  si et seulement si l'expression

$$L(f, \chi, 1) = -\frac{\chi(-1)2\pi i \tau(\chi)}{p} \sum_{a=1}^{p-1} \bar{\chi}(a) \int_{a/p}^{\infty} f(z) dz$$

est non nulle pour une forme modulaire  $f$  de poids 2 pour  $\Gamma_0(p)$ . Notons  $\omega_f$  la forme différentielle sur  $X_0(p)$  déduite de  $f(z) dz$  par passage au quotient.

On a alors

$$L(f, \chi, 1) = -\frac{\chi(-1)2\pi i \tau(\chi)}{p} \int_{\theta_\chi} \omega_f.$$

Observons que  $\theta_\chi$  est invariant (resp. anti-invariant) par la conjugaison complexe lorsque  $\chi$  est pair (resp. impair). En effet, cette conjugaison est déduite de l'involution

$z \mapsto -\bar{z}$  sur  $\mathcal{H}$  ; elle transforme donc le symbole modulaire  $\{\alpha, \beta\}$  en  $\{-\alpha, -\beta\}$  et donc  $\theta_\chi$  en  $\chi(-1)\theta_\chi$ .

Comme  $a/p$  (pour  $a$  entier premier à  $p$ ) et  $\infty$  sont conjugués par  $\Gamma_0(p)$ , le symbole modulaire  $\{\infty, \frac{a}{p}\}$ , et donc  $\theta_\chi$ , sont éléments de  $H_1(X_0(p)(\mathbf{C}), \mathbf{Z}[\chi])$ .

L'intégration des formes différentielles holomorphes fournit un accouplement parfait entre  $H^0(X_0(p)(\mathbf{C}), \Omega^1)$  et la partie invariante (resp. anti-invariante) par la conjugaison complexe de  $H_1(X_0(p)(\mathbf{C}), \mathbf{C})$ .

Comme toute forme différentielle holomorphe sur  $X_0(p)$  s'obtient de façon unique comme image d'une forme modulaire par  $f \mapsto \omega_f$ , l'hypothèse  $H_p(\chi)$  équivaut à la nullité de  $\theta_{\bar{\chi}}$ , qui elle-même équivaut à la nullité de  $\theta_\chi$ .  $\square$

### 2.3. Reformulation élémentaire

Commençons par traiter le cas du caractère trivial. La proposition suivante est bien connue au moins depuis les travaux de Mazur [16] (i.e., le quotient d'Eisenstein de  $J_0(p)$  est non trivial si et seulement si le numérateur de  $(p-1)/12$  est différent de 1). Nous en donnons une preuve facile.

#### PROPOSITION 8

On a  $H_p(1)$  pour tout nombre premier  $p \notin \{2, 3, 5, 7, 13\}$ .

#### Démonstration

D'après [21], il suffit de prouver que l'élément d'enroulement  $e \in H_1(X_0(p)(\mathbf{C}), \mathbf{Q})$  est non nul. Rappelons que cet élément d'enroulement est défini de la façon suivante. Posons  $V = \text{Hom}_{\mathbf{C}}(H^0(X_0(p), \Omega^1), \mathbf{C})$ . Notons  $L$  le plongement dans  $V$  de  $H_1(X_0(p)(\mathbf{C}), \mathbf{Z})$  par l'application qui à  $c$  associe  $\omega \mapsto \int_c \omega$ . Cette image est un réseau de  $V$  et  $J_0(p)(\mathbf{C})$  s'identifie canoniquement à  $V/L$  par la théorie d'Abel. Soit  $c_e$  un 1-cycle donné par l'image dans  $X_0(p)(\mathbf{C})$  d'un chemin reliant zéro à  $i\infty$  dans  $\mathcal{H}$ . Il a pour bord le diviseur  $(\infty) - (0)$  de  $X_0(p)$ . L'élément d'enroulement  $e$  est, par définition, l'image de  $\omega \mapsto \int_{c_e} \omega$  par l'isomorphisme d'espaces vectoriels réels  $V \simeq H_1(X_0(p)(\mathbf{C}), \mathbf{R})$ . Il est donc nul si et seulement si  $\omega \mapsto \int_{c_e} \omega$  est non nul.

Cette application  $\omega \mapsto \int_{c_e} \omega$  est un élément de  $V$  dont l'image dans  $V/L \simeq J_0(p)(\mathbf{C})$  est la classe du diviseur  $(\infty) - (0)$ . La classe d'un diviseur formé par la différence de deux points distincts est non nulle dans la jacobienne d'une courbe de genre non nul. L'application  $\omega \mapsto \int_{c_e} \omega$  et donc a fortiori  $e$  sont non nuls lorsque le genre de  $X_0(p)$  est non nul. Or le genre de  $X_0(p)$  est nul si et seulement si on a  $p \in \{2, 3, 5, 7, 13\}$ .  $\square$

Pour  $k \in \{1, 2, \dots, p-1\}$ , notons  $k_*$  l'unique élément de  $\{1, 2, \dots, p-1\}$ , tel que  $kk_* \equiv -1 \pmod{p}$ . Pour  $u \in (\mathbf{Z}/p\mathbf{Z})^*$  et pour  $\chi$  caractère différent de 1, posons

$$F(\chi, u) = \sum_{x=u}^{-1/u} ' \chi(x) - \chi(-1/x)$$

où le symbole  $'$  signifie que la somme ne tient pas compte des termes pour lesquels  $x \in p\mathbf{Z}$  et par abus de notation les bornes sont des représentants quelconques de  $u$  et  $-1/u$  dans  $\mathbf{Z}$ .

PROPOSITION 9

Soit  $\chi$  un caractère différent de 1. On a  $H_p(\chi)$  si et seulement si il existe  $u \in (\mathbf{Z}/p\mathbf{Z})^*$  tel que  $F(\chi, u) \neq 0$ .

Démonstration

D'après la proposition 7, il suffit d'étudier la nullité de  $\theta_\chi$ , ou, ce qui en revient au même puisque  $W_p$  est une involution, de  $-\chi(-1)W_p\theta_\chi$ . Or, on a

$$-\chi(-1)W_p\theta_\chi = \sum_{k=1}^{p-1} \chi(a)\zeta(a).$$

Utilisons les produits d'intersection sur  $H_1(X_0(p)(\mathbf{C}), \mathbf{Z})$ . Ils constituent un accouplement bilinéaire non dégénéré à valeurs dans  $\mathbf{Z}$  noté  $\bullet$ .

Comme on l'a rappelé dans la section 2.1, les éléments  $\zeta(k)$  engendrent  $H_1(X_0(p)(\mathbf{C}), \mathbf{Z})$  lorsque  $k$  parcourt  $\{1, 2, \dots, p-1\}$ . On a donc  $W_p\theta_\chi = 0$  si et seulement si  $W_p\theta_\chi \bullet \zeta(k) = 0$  pour tout  $k \in \{1, 2, \dots, p-1\}$ .

Rappelons [21, lemme 4] (lemme des cordes). On désigne par corde  $C_k$  le segment de droite orienté de  $\mathbf{C}$  reliant  $e^{2\pi i k_*/p}$  à  $e^{2\pi i k/p}$ . Soient  $k$  et  $k'$  deux éléments de  $\{1, \dots, p-1\}$  tels que  $k \neq k', k \neq k'_*$ . Le produit d'intersection  $\zeta(k) \bullet \zeta(k')$  est égal au nombre d'intersection (égal à  $-1, 0$  ou  $1$ ) des cordes  $C_{k'}$  et  $C_k$ .

On en déduit immédiatement la formule

$$W_p\theta_\chi \bullet \zeta(k) = \sum_{x=u}^{-1/u} ' \chi(x) - \chi(-1/x) = F(\chi, u). \quad \square$$

*Remarque.* Au vu de la proposition 9, la condition  $H_p(\chi)$  n'est jamais satisfaite lorsque  $\chi$  est un caractère quadratique pair. Si on admet la conjecture de Birch et Swinnerton-Dyer, cela entraîne que  $J_0(p)(\mathbf{Q}(\sqrt{p}))$  contient un  $\mathbf{T}$ -module libre de rang 1. Peut-on en mettre en évidence un générateur ?

#### 2.4. Congruences élémentaires

##### PROPOSITION 10

*Supposons que  $p$  soit un nombre premier congru à 11 ou 19 modulo 20 et que  $\chi$  soit un caractère impair. Alors on a  $H_p(\chi)$ .*

##### Démonstration

Puisque  $p$  est congru à 1 ou  $-1$  modulo 5, 5 est un carré modulo  $p$ , par la loi de réciprocité quadratique. L'équation  $x^2 + 3x + 1 = 0$  possède donc des solutions dans  $\mathbf{Z}/p\mathbf{Z}$ . Notons  $u_1$  et  $u_2$  ces solutions. On a  $-1/u_1 = u_1 + 3$  et  $(u_1 + 1)(u_1 + 2) = 1$ . Appliquons le critère élémentaire de la proposition 9 à  $u = u_1$ . Cela donne

$$\sum_{x=u_1}^{-1/u_1} {}'\chi(x) - \chi(-1/x) = \chi(u_1 + 1) - \chi(-1/(u_1 + 1)) + \chi(u_1 + 2) + \chi(-1/(u_1 + 2)).$$

En utilisant les relations  $-1/u_1 = u_1 + 3$  et  $(u_1 + 1)(u_1 + 2) = 1$  et l'impairité de  $\chi$ , on obtient

$$\sum_{x=u_1}^{-1/u_1} {}'\chi(x) - \chi(-1/x) = 2\chi(u_1 + 1) + 2\bar{\chi}(u_1 + 1) = 2\bar{\chi}(u_1 + 1)(1 + \chi(u_1 + 1)^2).$$

Comme  $p$  est congru à  $-1$  modulo 4, il n'y a pas de racine primitive quatrième de l'unité dans  $\mathbf{Z}/p\mathbf{Z}$  et donc  $\chi(u_1 + 1)^2 \neq -1$ . La somme  $\sum_{x=u_1}^{-1/u_1} {}'\chi(x) - \chi(-1/x)$  n'est donc pas nulle et on a  $H_p(\chi)$ .  $\square$

##### PROPOSITION 11

*Supposons que  $\chi$  soit un caractère quadratique impair et que  $p \notin \{3, 7\}$ . Alors on a  $H_p(\chi)$ .*

##### Démonstration

On a alors  $p \equiv -1 \pmod{4}$ . Comme  $\chi$  est quadratique et impair on a

$$F(\chi, u) = 2 \sum_{x=u}^{-1/u} {}'\chi(x).$$

Le caractère  $\chi$  est à valeurs dans  $\{-1, +1\}$ . Il suffit donc d'établir l'existence de  $a \in \{1, 2, \dots, p-1\}$  avec  $a$  et  $a_*$  de même parité pour conclure. En effet dans ce cas la somme qui définit  $F(\chi, u)$  possède un nombre impair de termes égaux à 1 ou  $-1$ , ce qui entraîne la non nullité de  $F(\chi, a + p\mathbf{Z})$ .

Supposons que pour tout  $a \in \{1, 2, \dots, p-1\}$ , les entiers  $a$  et  $a_*$  soient de parités opposées. Comme  $p$  est congru à  $-1$  modulo 4, on a  $4_* = (3p - 1)/4$ . Soient  $i$  et  $j$  deux entiers plus que zéro tels que  $(3p - 1)/4 = ij$ . On a  $(2i)_* = 2j$  sauf si  $i$  ou  $j$

est égal à 1. On en conclut que  $(3p - 1)/4$  est premier et donc impair sauf si  $p = 3$ , cas désormais exclu.

Par conséquent  $(7p - 1)/8$  est entier. Par un raisonnement analogue à celui qui précède on obtient que  $(7p - 1)/8$  est un nombre premier sauf si  $p < 8$ , cas que l'on peut désormais écarter. Cela nous donne que  $(7p - 1)/8$  est premier à 3.

C'est pourquoi on a  $3|(2p - 1)$  et donc  $3_* = (2p - 1)/3$  qui est un nombre impair. Cela est absurde.  $\square$

#### PROPOSITION 12

*Supposons que  $\chi$  soit un caractère injectif. Alors on a  $H_p(\chi)$  pour tout nombre premier  $p \notin \{2, 3, 5, 7, 13, 1487\}$ .*

#### Démonstration

Le nombre premier  $p$  est totalement décomposé dans le corps  $\mathbf{Q}[\chi] = \mathbf{Q}(\mu_{p-1})$ . Soit  $\mathcal{P}$  un idéal de  $\mathbf{Q}[\chi]$  au-dessus de  $p$ . Le caractère  $\tilde{\chi}$ , obtenu en composant  $\chi$  avec la réduction modulo  $\mathcal{P}$  coïncide donc avec l'élévation à une certaine puissance  $k$  dans  $(\mathbf{Z}/p\mathbf{Z})^*$ . Comme  $\chi$  est injectif, l'entier  $k$  est premier à  $p - 1$ . Quitte à remplacer  $\mathcal{P}$  par un idéal conjugué, on peut supposer qu'on a  $k = 1$ . Notons  $\bar{F}$  la réduction modulo  $\mathcal{P}$  de  $F$ .

On a donc dans  $\mathbf{Z}/p\mathbf{Z}$ ,

$$\bar{F}(\chi, u) = \sum_{x=u}^{-1/u} x + 1/x.$$

L'un des trois nombres 3, 5 et 15 est un carré modulo  $p$ . En d'autres termes, l'une des trois équations  $x^2 + 4x + 1 = 0$ ,  $x^2 + 3x + 1 = 0$  et  $x^2 + 8x + 1 = 0$  admet des solutions dans  $\mathbf{Z}/p\mathbf{Z}$ . Il existe donc  $u \in (\mathbf{Z}/p\mathbf{Z})^*$  tel que  $-1/u$  soit égal à  $u + 4$ ,  $u + 3$  ou  $u + 8$ .

Calculons  $\bar{F}(\chi, u)$  lorsqu'on a  $P_d(u) = u^2 + du + 1 \equiv 0 \pmod{p}$ . Soit  $i$  un entier vérifiant  $0 < i < d$ . On a, en utilisant la relation  $(u+i)(u+d-i) \equiv i(d-i) - 1 \pmod{p}$ ,

$$\begin{aligned} u + i + \frac{1}{u+i} + u + d - i + \frac{1}{u+d-i} &\equiv \frac{i(d-i)}{u+d-i} + \frac{i(d-i)}{u+i} \\ &\equiv \frac{i(d-i)(2u+d)}{i(d-i)-1} \pmod{p}. \end{aligned}$$

Notons qu'on a  $P'_d(u) = 2u + d$  et que le polynôme  $P_d$  n'a pas de racine multiple pour  $p \nmid d^2 - 4$ . Plus précisément les polynômes  $P_3$ ,  $P_5$  et  $P_{15}$  sont sans racine multiple pour  $p$  distinct de 2, 3 et 5. On a alors  $P'_d(u) \neq 0$ . Lorsque  $u + i \neq 0$ , pour

$0 < i < d$ , on obtient la relation

$$\bar{F}(\chi, u) = \frac{1}{2} P'_d(u) \sum_{0 < i < d} ' \frac{i(d-i)}{i(d-i)-1},$$

où le signe ' signifie que l'on a oublié les pôles dans la somme. Lorsqu'il existe  $i \in \{1, 2, \dots, d\}$  tel que  $u + i = 0$ , la quantité  $\sum_{0 < i < d} i(d-i)/(i(d-i)-1)$  admet un pôle en  $d = p$ . Elle vaut respectivement 2, 13/3 et 2.1487/5.7.11 lorsque  $d$  vaut 3, 4 et 8 respectivement. Lorsque  $p$  est un nombre premier qui n'apparaît pas dans ces fractions, on a  $H_p(\chi)$ . On a  $H_{11}(\chi)$  d'après la proposition 10.  $\square$

*Remarque.* Ces méthodes permettent-elles de démontrer que  $H_p(\chi)$  est vérifiée pour tout  $p$  supérieur à une quantité dépendant seulement de l'ordre du noyau de  $\chi$  ?

### 2.5. Congruences d'Eisenstein ( $\chi$ pair)

Notons  $v$  le plus grand commun diviseur de  $p-1$  et 12. L'idéal d'Eisenstein  $\mathcal{I}$  de  $\mathbf{T}$  est par définition l'idéal engendré par les  $T_q - (q+1)$  ( $q$  nombre premier distinct de  $p$ ) et par  $1 + W_p$ . On a  $\mathbf{T}/\mathcal{I} \simeq \mathbf{Z}/((p-1)/v)\mathbf{Z}$  (voir [16]).

#### PROPOSITION 13

Soit  $\chi$  un caractère d'ordre une puissance d'un nombre premier  $l > 3$  (cela impose que  $\chi$  n'est pas quadratique pair et que  $p \notin \{2, 3, 5, 7, 13\}$ ). Alors on a  $\theta_\chi \notin \mathcal{I}H_1(X_0(p)(\mathbf{C}); \mathbf{Z}[\chi])$ .

En particulier,  $\theta_\chi$  est non nul et on a  $H_p(\chi)$ .

#### Démonstration

Considérons  $\mathbf{Z}[(\mathbf{Z}/p\mathbf{Z})^*]$  comme un sous-groupe de  $\mathbf{Z}[\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})]$  (via le plongement canonique de  $(\mathbf{Z}/p\mathbf{Z})^*$  dans  $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$ ).

Posons  $G = (\mathbf{Z}/p\mathbf{Z})^*/\{-1, 1\}$ . Notons  $I_G$  l'idéal d'augmentation de l'anneau  $\mathbf{Z}[G]$ . En tenant compte du fait que l'action de la conjugaison complexe est acyclique sur l'homologie et des rappels de la section 2.1, on obtient que l'application  $\zeta^+ : \mathbf{Z}[G] \longrightarrow H_1(X_0(p)(\mathbf{C}); \mathbf{Z})_+$  qui à  $[\pm a + p\mathbf{Z}]$  associe  $\zeta(a) + \zeta(-a)$  est surjective. Comme  $\zeta(1) = 0$ , l'image par  $\zeta^+$  de  $I_G$  engendre  $H_1(X_0(p)(\mathbf{C}); \mathbf{Z})_+$ . On pourra consulter [20, section 1.3] pour plus de détails.

D'après [16, sections II.11 et II.18], la monodromie du revêtement de  $X_0(p)$  par la courbe modulaire  $X_1(p)$  (ou plus précisément le plus grand revêtement étale intermédiaire, appelé *revêtement de Shimura*) donne lieu à un homomorphisme de groupes  $\kappa$  :

$$H_1(X_0(p)(\mathbf{C}), \mathbf{Z}) \longrightarrow (\mathbf{Z}/p\mathbf{Z})^*/\mu_v$$

où  $\mu_v$  désigne ici le sous-groupe de  $(\mathbf{Z}/p\mathbf{Z})^*$  formé par les racines  $v$ -ième de l'unité.

Cet homomorphisme est caractérisé par la formule suivante sur les symboles modulaires :  $\kappa(\{0, a/b\})$  est congru à  $b$  modulo  $p$  dans  $(\mathbf{Z}/p\mathbf{Z})^*/\mu_v$  lorsque  $b$  n'est pas divisible par  $p$  (voir [16, section II.18] ; nous avons fait toutefois la convention de signe opposée à celle de Mazur dans la définition de  $\kappa$ ). Le noyau de cet homomorphisme est engendré par  $H_1(X_0(p)(\mathbf{C}); \mathbf{Z})_-$  et  $\mathcal{I}H_1(X_0(p)(\mathbf{C}); \mathbf{Z})$ , où  $\mathcal{I}$  est l'idéal d'Eisenstein de  $\mathbf{T}$  (voir [16] et, pour quelques arguments complémentaires, [20, section 5.1]). De plus  $\kappa$  est anti-invariant par l'involution  $W_p$  (car  $\mathcal{I}$  contient  $1 + W_p$ ), si bien qu'on a les formules

$$-\kappa\left(\left\{\infty, \frac{k}{p}\right\}\right) = -\kappa\left(W_p\left\{0, -\frac{1}{k}\right\}\right) = \kappa(\zeta(k)) = (k + p\mathbf{Z})^{-1}.$$

Comme  $H_1(X_0(p)(\mathbf{C}), \mathbf{Z})$  est acyclique pour l'action de la conjugaison complexe, on obtient un homomorphisme de groupes  $\kappa_1^+$  :

$$H_1(X_0(p)(\mathbf{C}), \mathbf{Z})_+ \longrightarrow G/\mu_v$$

par la formule

$$\kappa_1^+(\zeta^+([\pm g])) = \kappa(\zeta(g)).$$

Le noyau de  $\kappa_1^+$  est  $\mathcal{I}H_1(X_0(p)(\mathbf{C}), \mathbf{Z})_+$ . Par extension des scalaires on obtient un homomorphisme de groupes encore noté  $\kappa_1^+$  :

$$H_1(X_0(p)(\mathbf{C}), \mathbf{Z}[\chi])_+ \longrightarrow G/\mu_v \otimes \mathbf{Z}[\chi].$$

Calculons  $\kappa_1^+(\theta_\chi)$ . Soit  $g_0$  un générateur du groupe  $G$ . On a la formule  $\theta_\chi = \sum_{t=0}^{(p-1)/2} \chi(g_0^t) \zeta^+(g_0^t)$ . Cela donne

$$\kappa_1^+(\theta_\chi) = \prod_{t=0}^{(p-1)/2} g_0^{t\chi(g_0)^t} = g_0^{\sum_{t=0}^{(p-1)/2} t\chi(g_0)^t}.$$

Cette dernière quantité est nulle si et seulement si on a la relation  $\sum_{t=0}^{(p-1)/2} t\chi(g_0)^t \in ((p-1)/v)\mathbf{Z}[\chi]$ . Un calcul facile donne

$$\sum_{t=0}^{(p-1)/2} t\chi(g_0)^t = \frac{p-1}{2(1-\chi(g_0))}.$$

Lorsque  $\chi$  est d'ordre une puissance d'un nombre premier  $l > 3$ ,  $1 - \chi(g_0)$  n'est pas  $l$ -entier. On a donc  $(p-1)/(2(1-\chi(g_0))) \notin ((p-1)/v)\mathbf{Z}[\chi]$ .  $\square$

*Remarques.* La proposition 13 a des conséquences relatives à l'arithmétique du quotient d'Eisenstein de  $J_0(p)$ , que nous laissons deviner au lecteur. Nous n'avons pas

essayé de retrouver de telles propriétés directement par les méthodes de [16], cela laisse présager de l'utilité du quotient d'Eisenstein pour se passer des résultats de Kato.

On aimerait démontrer la non-nullité de  $\theta_\chi$  dans les cas où  $\chi$  est un caractère pair non quadratique, en démontrant que  $\theta_\chi \notin \mathcal{S}^t \mathrm{H}_1(X_0(p)(\mathbf{C}), \mathbf{Z}[\chi])$ , pour  $t$  entier assez grand. Pour cela on aimerait utiliser les faits suivants. La théorie de l'homomorphisme d'enroulement (voir [16, section II.18]) identifie canoniquement le groupe abélien  $\mathcal{S}/\mathcal{S}^2$  à  $\mathrm{H}_1(X_0(p)(\mathbf{C}), \mathbf{Z})_+/\mathcal{S}\mathrm{H}_1(X_0(p)(\mathbf{C}), \mathbf{Z})_+$  et donc, via  $\kappa$ , à  $G/\mu_v$ . Elle donne même lieu à un isomorphisme de  $\mathbf{T}_{\mathcal{S}}$ -modules entre les complétés  $\mathcal{S}$ -adiques de  $\mathcal{S}$  et de  $\mathrm{H}_1(X_0(p)(\mathbf{C}), \mathbf{Z})_+$  (voir [16, théorème II.18.10]). On a donc les isomorphismes canoniques de groupes, pour tout entier  $k \geq 1$ ,

$$\begin{aligned} (G/\mu_v)^{\otimes k} &\simeq (\mathcal{S}/\mathcal{S}^2)^{\otimes k} \simeq \mathcal{S}^k/\mathcal{S}^{k+1} \\ &\simeq \mathcal{S}^{k-1}\mathrm{H}_1(X_0(p)(\mathbf{C}), \mathbf{Z})_+/\mathcal{S}^k\mathrm{H}_1(X_0(p)(\mathbf{C}), \mathbf{Z})_+, \end{aligned}$$

d'où l'homomorphisme surjectif de groupes  $\kappa_k^+$ ,

$$\mathcal{S}^{k-1}\mathrm{H}_1(X_0(p)(\mathbf{C}), \mathbf{Z})_+ \longrightarrow (G/\mu_v)^{\otimes k}.$$

Comment calculer  $\kappa_k^+(\theta_\chi)$  ? Voici un problème élémentaire plus simple que nous ne savons pas résoudre. Soient  $x$  et  $y$  deux éléments de  $G$ . On a  $\zeta^+(x) + \zeta^+(y) - \zeta^+(xy) \in \mathcal{S}\mathrm{H}_1(X_0(p)(\mathbf{C}), \mathbf{Z})_+$ . À quoi est égal  $\kappa_2^+(\zeta^+(x) + \zeta^+(y) - \zeta^+(xy)) \in (G/\mu_v)^{\otimes 2}$  ? Ce n'est pas en général l'image de  $x \otimes y$  dans  $(G/\mu_v)^{\otimes 2}$ . En d'autres termes, la filtration de  $\mathrm{H}_1(X_0(p)(\mathbf{C}), \mathbf{Z})_+$  par les puissances de  $\mathcal{S}$  ne provient pas de la filtration de  $I_G$  par les puissances de  $I_G$  (où  $I_G$  désigne l'idéal d'augmentation de  $\mathbf{Z}[G]$ ).

Nous ignorons si la proposition 13 est encore vraie lorsque  $\chi$  est un caractère impair. On pourrait peut-être étudier cela à la lumière de la section 2.6.

Il serait probablement instructif de comparer les techniques utilisées dans la preuve de la proposition 13 avec les conjectures de Mazur et J. Tate [19] (tout particulièrement le cas où leur couche  $M$  est égale au niveau  $p$ ), qui proposent des filtrations de  $\mathrm{H}_1(X_0(p)(\mathbf{C}), \mathbf{Z}[G])_+$  par des puissances de  $I_G$ .

#### COROLLAIRE

*Soit  $\chi$  un caractère d'ordre une puissance d'un nombre premier plus que 3. Il existe une forme primitive  $f$  de poids 2 pour  $\Gamma_0(p)$  telle que  $L(f, \chi, 1) \neq 0$  et  $L(f, 1) \neq 0$ .*

#### Démonstration

Comme nous n'utiliserons pas ce résultat dans la suite, nous laissons la démonstration, qui est facile, au lecteur.  $\square$



### 2.6. Annulation simultanée de séries de Dirichlet ( $\chi$ impair)

Soit  $\chi$  un caractère impair. Notons  $B_{1,\chi}$  le nombre de Bernoulli généralisé associé à  $\chi$ , c'est-à-dire on a

$$B_{1,\chi} = \frac{1}{p} \sum_{a=1}^{p-1} a\chi(a).$$

#### PROPOSITION 14

*Si le nombre algébrique totalement réel*

$$12B_{1,\chi}\overline{B_{1,\chi}} + (p-1)(B_{1,\chi} + \overline{B_{1,\chi}})$$

*est non nul, il existe une forme primitive  $f$  de poids 2 pour  $\Gamma_0(p)$  telle que  $L(f, \chi, 1) \neq 0$  et  $L(f, 1) \neq 0$  (en particulier, on a  $H_p(\chi)$ ).*

#### Démonstration

Démontrons d'abord qu'il suffit pour cela de vérifier que le produit d'intersection  $e \bullet W_p \theta_\chi = W_p e \bullet \theta_\chi = -e \bullet \theta_\chi$  est non nul (voir la démonstration de la proposition 9).

Supposons que pour toute forme modulaire primitive  $f$ , on ait  $L(f, \chi, 1) = 0$  ou  $L(f, 1) = 0$ . Notons alors  $I_1$  et  $I_\chi$  les annulateurs de  $e$  et  $\theta_\chi$  dans  $\mathbf{T}[\chi]$ . L'idéal  $I_1 + I_\chi$  est d'indice fini dans  $\mathbf{T}[\chi]$ . On a donc dans  $\mathbf{T}[\chi]$  une relation  $1 = n_1 t_1 + n_\chi t_\chi$  avec  $n_1, n_\chi \in \mathbf{Q}$  et  $t_1 \in I_1, t_\chi \in I_\chi$ . Comme le produit d'intersection vérifie l'adjonction vis-à-vis de l'action de  $\mathbf{T}$ , on a la relation

$$e \bullet \theta_\chi = n_1 t_1 e \bullet \theta_\chi + n_\chi t_\chi e \bullet \theta_\chi = 0 + n_\chi e \bullet t_\chi \theta_\chi = 0.$$

Effectuons le calcul de  $e \bullet \theta_\chi$  en utilisant [21, lemme 3] (qui est essentiellement une formule de H. Rademacher [24] reprise par Mazur dans [18]) : On a pour tout  $k \in \{1, \dots, p-1\}$ ,

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

où la somme de Dedekind  $S(k, p)$  est donnée par la formule

$$S(k, p) = \sum_{h=0}^{p-1} \bar{B}_1\left(\frac{h}{p}\right) \bar{B}_1\left(\frac{kh}{p}\right)$$

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

En utilisant la formule donnant  $W_p\theta_\chi$  (démonstration de la proposition 9), on obtient

$$(p-1)e \bullet W_p\theta_\chi = \sum_{k=1}^{p-1} \chi(k) \frac{(k-k_*)}{p} (1-p) - \sum_{k=1}^{p-1} \chi(k) 12S(k, p).$$

Calculons d’abord le premier terme en utilisant l’impairité de  $\chi$  et le changement de variable  $k \mapsto k_*$  :

$$\sum_{k=1}^{p-1} \chi(k) \frac{(k-k_*)}{p} (1-p) = \sum_{k=1}^{p-1} (\chi(k) + \bar{\chi}(k)) \frac{k}{p} (1-p) = (1-p)(B_{1,\chi} + \overline{B_{1,\chi}}).$$

Le deuxième terme s’obtient directement par un calcul de convolution :

$$\sum_{k=1}^{p-1} \chi(k) 12S(k, p) = 12B_{1,\chi} \overline{B_{1,\chi}}.$$

Cela donne

$$(1-p)e \bullet W_p\theta_\chi = 12B_{1,\chi} \overline{B_{1,\chi}} + (p-1)(B_{1,\chi} + \overline{B_{1,\chi}}).$$

Cela suffit à démontrer notre proposition, d’après nos remarques préliminaires.  $\square$

*Remarques.* On peut espérer que les deux termes du nombre figurant dans l’énoncé de la proposition 14 sont d’ordres de grandeur différents lorsque  $p$  tend vers l’infini. Pour établir cela, on est tenté d’appliquer les techniques permettant d’encadrer les valeurs de fonction  $L$  de Dirichlet en 1.

Soit  $f_\chi$  l’unique forme modulaire de poids 2 pour  $\Gamma_0(p)$  telle que, pour toute forme modulaire  $f \in S_2(\Gamma_0(p))$ , on ait la relation

$$\langle f, f_\chi \rangle = L(f, \chi, 1),$$

où  $\langle \cdot, \cdot \rangle$  désigne le produit scalaire de Petersson. À quoi est égal  $\langle f_\chi, f_1 \rangle$  ? Tout récemment, L. Fourquaux établit le lien entre ce nombre complexe et le nombre algébrique qui figure dans [3, formule de la proposition 14]. Il calcule de plus  $\theta_\chi \bullet \theta_{\chi'}$  pour  $\chi$  et  $\chi'$  caractères non triviaux de parités opposées et traduit ce calcul en termes de produits scalaires de Petersson (voir [3]).

### 3. Compléments et résultats expérimentaux

#### 3.1. La question des points ordinaires et des points supersinguliers

Soit  $p$  un nombre premier distinct de 2 et 3. Soit  $K$  une extension finie de  $\mathbf{Q}_p$  d'indice de ramification  $e$ . Notons  $\mathcal{O}_K$  l'anneau des entiers de  $K$  et  $\mathcal{P}$  l'idéal maximal de  $\mathcal{O}_K$ . Soit  $E$  une courbe elliptique sur  $K$  ayant potentiellement bonne réduction.

Notons  $E_0(K)$  le sous-groupe (d'indice moins que ou égal à 4) de  $E(K)$  formé par les points dont l'extension au modèle de Néron de  $E$  sur  $\mathcal{O}_K$  est non singulière dans la fibre spéciale. Notons  $E_1(K)$  le sous-groupe de  $E_0(K)$  constitué par les points dont l'extension au modèle de Néron coïncide avec l'élément neutre dans la fibre spéciale.

Après avoir assisté à mes exposés au Chennai Mathematical Institute et Math-science (Chennai, Inde, janvier 1999), Oesterlé m'a indiqué un lemme sur les groupes formels dont voici un cas particulier (c'est un corollaire de [2, proposition 2]).

#### PROPOSITION 15

*Le nombre d'éléments d'ordre  $p$  de  $E_1(K)$  est moins que ou égal à  $e$ .*

#### Démonstration

La loi de groupe sur  $E_1(K)$  donne une loi de groupe formel sur  $\mathcal{P}$ . La multiplication par  $p$  dans  $E_1(K)$  est donnée par une série formelle  $[p](T) \in \mathcal{O}_K[[T]]$  sur  $\mathcal{P}$ . On a  $[p](T) = pT + \dots = Th(T)$ , avec  $h(T) \in \mathcal{O}_K[[T]]$ . Notons  $A_p$  l'ensemble des éléments d'ordre  $p$  de  $\mathcal{P}$  pour la loi de groupe formel. Soit  $t \in A_p$ . On a  $t \neq 0$  et  $[p](t) = 0$ , d'où  $h(t) = 0$ . Puisque  $(h(T) - h(t))/(T - t) \in \mathcal{O}_K[[T]]$ , on en déduit la relation de divisibilité dans  $\mathcal{O}_K[[T]]$  :

$$(T - t) \mid (T - t) \frac{h(T) - h(t)}{T - t} = h(T) - h(t) = h(T).$$

En spécialisant en  $T = 0$ , on obtient la relation dans  $\mathcal{O}_K$  :  $\prod_{t \in A_p} t \mid p$ . Cela entraîne l'inégalité  $e \geq |A_p|$ .  $\square$

Mentionnons le corollaire suivant qui nous intéresse directement. Rappelons que  $p > 3$ .

#### COROLLAIRE

*Soit  $E$  une courbe elliptique sur  $\mathbf{Q}_p(\mu_p)$  telle que  $K_p(E) = \mathbf{Q}_p(\mu_p)$  et  $j(E) \in \mathbf{Z}_p[\mu_p]$ . Alors la fibre spéciale du modèle de Néron de  $E$  n'a pas potentiellement bonne réduction supersingulière et possède un point  $\mathbf{F}_p$ -rationnel d'ordre  $p$ .*

#### Démonstration

Le groupe  $E(\mathbf{Q}_p(\mu_p))$  possède un sous-groupe  $C$  isomorphe à  $(\mathbf{Z}/p\mathbf{Z})^2$  car  $j(E) \in \mathbf{Z}_p[\mu_p]$ . Comme  $p > 3$ , ce sous-groupe est contenu dans  $E_0(\mathbf{Q}_p(\mu_p))$ . D’après la proposition 15, on a  $p - 1 \geq |(C - 0) \cap E_1(\mathbf{Q}_p(\mu_p))|$ . Cela interdit le cas supersingulier, car on a alors  $C \subset E_1(\mathbf{Q}_p(\mu_p))$ . On est donc dans le cas potentiellement ordinaire, ce qui entraîne que l’ordre de  $C \cap E_1(\mathbf{Q}_p(\mu_p))$  est  $p$ . Le groupe  $E_0(\mathbf{Q}_p(\mu_p))/E_1(\mathbf{Q}_p(\mu_p)) \simeq E(\mathbf{F}_p)$  contient donc un élément d’ordre  $p$ .  $\square$

### 3.2. Quelques données dues à William Stein

Par abus de notation, nous dirons qu’un élément  $j \in \mathbf{P}^1(\mathbf{F}_p)$  présente une anomalie s’il existe une courbe elliptique sur  $\mathbf{F}_p$  d’invariant modulaire  $j$  et possédant un point  $\mathbf{F}_p$ -rationnel d’ordre  $p$ .

#### PROPOSITION 16

Soit  $p$  un nombre premier congru à  $-1$  modulo 4. Supposons que pour tout  $j \in \mathbf{P}^1(\mathbf{F}_p)$  présentant une anomalie et tout caractère de Dirichlet  $\chi : (\mathbf{Z}/p\mathbf{Z})^* \rightarrow \mathbf{C}$ , il existe  $t_\chi \in \mathbf{T}[\chi]$  et  $\delta \in \Delta_S$  tels que  $L(t_\chi J_0(p), \chi, 1) \neq 0$  et  $\iota_1(t_\chi \delta) \neq 0$ . Alors on a  $p \notin S$ .

#### Démonstration

La condition  $L(t_\chi J_0(p), 1) \neq 0$  impose  $H_p(\chi)$  (et donc  $p > 7$ ) et, par le théorème de Kato, la finitude de la composante  $\chi$ -isotypique de  $t_\chi J_0(p)(\mathbf{Q}(\mu_p))$ .

Si  $p \in S$ , on a  $p \in S_o$  ( $p \in S_c$  et  $p \in S_s$  sont exclus d’après le corollaire 3 de la proposition 6 et le corollaire de la proposition 15 respectivement). Soit  $E$  une courbe elliptique sur  $\mathbf{Q}(\mu_p)$  possédant  $p^2 - 1$  points  $\mathbf{Q}(\mu_p)$ -rationnels d’ordre  $p$ . Elle a donc bonne réduction en l’idéal au dessus de  $p$  et présente une anomalie (i.e., elle possède un point  $\mathbf{F}_p$ -rationnel d’ordre  $p$ ) d’après le corollaire 3 de la proposition 6 et le corollaire de la proposition 15. Elle définit un point  $\mathbf{Q}(\mu_p)$ -rationnel  $p$ -ordinaire de  $Y_0(p)$ . Ce point est  $\mathbf{Q}$ -rationnel par application du corollaire 1 de la proposition 6 (le critère de pseudo-immersion formelle est vérifié pour  $d = 1$ ). Dans ces conditions, d’après [17],  $Y_0(p)$  n’a pas de point  $\mathbf{Q}$ -rationnel pour  $p \notin \{3, 7, 11, 19, 43, 67, 163\}$  et pas de point  $\mathbf{Q}$ -rationnel sans multiplications complexes et donc pas de point  $p$ -ordinaire pour  $p \notin \{3, 7, 11\}$ . Le cas  $p = 11$ , qui revient à examiner trois courbes elliptiques (à  $\bar{\mathbf{Q}}$ -isomorphisme près), a été étudié en détail par G. Ligozat dans [14] (voir démonstration de [14, proposition 5.6.1]) qui démontre en examinant les réductions modulo 23 que ces courbes ne donnent pas lieu à un élément de  $S$ .  $\square$

William Stein a constaté que, pour  $p < 1000$ ,  $p > 7$  et  $p \equiv -1 \pmod{4}$ , les hypothèses de la proposition 16 sont vérifiées.

*Remerciements.* J’exprime ma gratitude envers ceux qui ont pris la peine d’écouter et parfois de répondre à mes questions : Jean-Marc Fontaine, Benedict Gross, Emmanuel Halberstadt, Emmanuel Kowalski, Alain Kraus, Barry Mazur, Jean-François Mestre, Philippe Michel, Joseph Oesterlé, Marusia Rebolledo, David Rohrlich, Anthony Scholl, William Stein.

Les résultats de ce cet article ont été partiellement exposés lors du colloque en l’honneur de Barry Mazur pour son soixantième anniversaire. La présente version présente des modifications par rapport à une version préliminaire et incomplète qui a diffusée sous forme de prépublication de l’Institut de mathématiques de Jussieu.

Ajoutons que cet article, dont les prémices datent de l’automne 1995 passé à l’été Institute for Advanced Studies (Princeton), a été essentiellement rédigé lors d’une visite à l’Université de Pondichéry.

## References

- [1] P. DELIGNE et M. RAPOPORT, “Les schémas de modules de courbes elliptiques” dans *Modular Functions of One Variable (Antwerp, 1972), II*, Lecture Notes in Math. **349**, Springer, Berlin, 1973, 143–316, MR 49:2762; “Correction” dans *Modular Functions of One Variable (Antwerp, 1972), IV*, Lecture Notes in Math. **476**, Springer, Berlin, 1975, 149. MR 52:3177
- [2] M. FLEXOR et J. OESTERLÉ, “Sur les points de torsion des courbes elliptiques” dans *Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988)*, Astérisque **183**, Soc. Math. France, Montrouge, 1990, 25–36. MR 91g:11057
- [3] L. FOURQUAUX, *Produits de Petersson de formes modulaires associées aux valeurs de fonctions  $L$* , Mémoire de Diplôme d’Études Approfondies, Université Pierre et Marie Curie, 2000.
- [4] B. H. GROSS, “Heights and the special values of  $L$ -series” dans *Number Theory (Montréal, 1985)*, CMS Conf. Proc. **7**, Amer. Math. Soc., Providence, 1987, 115–187. MR 89c:11082
- [5] B. H. GROSS et S. S. KUDLA, *Heights and the central critical values of triple product  $L$ -functions*, Compositio Math. **81** (1992), 143–209. MR 93g:11047
- [6] E. HALBERSTADT, lettre du 8 octobre 1998.
- [7] S. KAMIENNY, *Points of order  $p$  on elliptic curves over  $\mathbf{Q}(\sqrt{p})$* , Math. Ann. **261** (1982), 413–424. MR 84g:14047
- [8] ———,  *$p$ -torsion in elliptic curves over subfields of  $\mathbf{Q}(\mu_p)$* , Math. Ann. **280** (1988), 513–519. MR 90a:11061
- [9] ———, *Torsion points on elliptic curves and  $q$ -coefficients of modular forms*, Invent. Math. **109** (1992), 221–229. MR 93h:11054
- [10] ———, *Torsion points on elliptic curves over fields of higher degree*, Internat. Math. Res. Notices **1992**, 129–133. MR 93e:11072
- [11] S. KAMIENNY et B. MAZUR, “Rational torsion of prime order in elliptic curves over number fields ; appendix by A. Granville” dans *Columbia University Number Theory Seminar (New York, 1992)*, Astérisque **228**, Soc. Math. France,

- Montrouge, 1995, 3, 81–100. MR 96c:11058
- [12] V. A. KOLYVAGIN et D. YU. LOGACHËV, *Finiteness of the group of rational points for some abelian modular varieties*, Leningrad Math. J. **1** (1990), 1229–1253. MR 91c:11032
  - [13] E. KOWALSKI et P. MICHEL, *Deux théorèmes de non-annulation de valeurs spéciales de fonctions  $L$* , Manuscripta Math. **104** (2001), 1–19. MR 1 820 726
  - [14] G. LIGOZAT, “Courbes modulaires de niveau 11” dans *Modular Functions of One Variable (Bonn, 1976)*, V, Lecture Notes in Math. **601**, Springer, Berlin, 1977, 149–237. MR 57:3079
  - [15] YU. I. MANIN, *Parabolic points and zeta function of modular curves*, Math. USSR-Izv. **6** (1972), 19–64. MR 47:3396
  - [16] B. MAZUR, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186. MR 80c:14015
  - [17] ———, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162. MR 80h:14022
  - [18] ———, *On the arithmetic of special values of  $L$ -functions*, Invent. Math. **55** (1979), 207–240. MR 82e:14033
  - [19] B. MAZUR et J. TATE, *Refined conjectures of the “Birch and Swinnerton-Dyer type,”* Duke Math. J. **54** (1987), 711–750. MR 88k:11039
  - [20] L. MEREL, *L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de  $J_0(p)$* , J. Reine Angew. Math. **477** (1996), 71–115. MR 97f:11045
  - [21] ———, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), 437–449. MR 96i:11057
  - [22] J.-F. MESTRE, “La méthode des graphes: Exemples et applications” dans *Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields (Katata, 1986)*, Nagoya Univ., Nagoya, 1986, 217–242. MR 88e:11025
  - [23] J.-F. MESTRE et J. OESTERLÉ, *Courbes elliptiques de conducteur premier*, manuscrit non publié.
  - [24] H. RADEMACHER, *Zur Theorie der Modulfunktionen*, J. Reine Angew. Math. **167** (1931), 312–336.
  - [25] K. RUBIN, “Euler systems and modular elliptic curves” dans *Galois Representations in Arithmetic Algebraic Geometry (Durham, 1996)*, London Math. Soc. Lecture Note Ser. **254**, Cambridge Univ. Press, Cambridge, 1998, 351–367. MR 2001a:11106
  - [26] A. J. SCHOLL, “An introduction to Kato’s Euler systems” dans *Galois Representations in Arithmetic Algebraic Geometry (Durham, 1996)*, London Math. Soc. Lecture Note Ser. **254**, Cambridge Univ. Press, Cambridge, 1998, 379–460. MR 2000g:11057
  - [27] G. SHIMURA, *Introduction to the Arithmetic Theory of Automorphic Functions*, Kanô Memorial Lectures **1**, Iwanami Shoten, Tokyo; Publ. Math. Soc. Japan **11**, Princeton Univ. Press, Princeton, 1971. MR 47:3318

*Merel*

Théorie des nombres, case 247, Institut de mathématiques de Jussieu, 4 place Jussieu, F-75252 Paris CEDEX 05, France ; merel@math.jussieu.fr ; Unité de Formation et de Recherche de mathématiques, case 7012, Université Denis Diderot, 2 place Jussieu, F-75251 Paris CEDEX 05, France

## Appendice

### Vérification de l'hypothèse $H_p(\chi)$ pour $p$ grand

E. KOWALSKI et P. MICHEL\*

Dans le texte qui précède, Merel a introduit l'hypothèse  $H_p(\chi)$ , pour  $p$  premier et  $\chi$  un caractère de Dirichlet primitif modulo  $p$ . Il s'agit d'un problème de non-annulation pour certaines fonctions  $L$  automorphes. Il a également fourni l'assertion élémentaire suivante qui est équivalente à  $H_p(\chi)$  : *Il existe  $u$  modulo  $p$ ,  $u \neq 0$ , tel que*

$$\sum_{\substack{x=-\bar{u} \\ x=u}}^{x=-\bar{u}} (\chi(x) - \chi(-1)\bar{\chi}(x)) \neq 0.$$

La somme est prise entre des représentants entiers quelconques de  $u$  et de  $-\bar{u}$ , où  $\bar{u}$  est l'inverse de  $u$  modulo  $p$ .

On voit que si  $\chi$  est quadratique et pair, l'expression en question est identiquement nulle. Nous montrons ici que réciproquement, si  $\chi$  n'est pas quadratique pair, et  $p$  assez grand ( $p > B$ , pour une constante absolue et effective  $B$ ), cette assertion est vraie, et donc  $H_p(\chi)$  l'est également. Dans la note [KM] nous établissons directement le théorème de non-annulation (sous une forme plus forte) et étudions le cas restant de  $\chi$  quadratique pair (c'est à dire la valeur centrale de la dérivée des fonctions  $L$  correspondantes).

## 1. Préliminaires

Dans tout ce qui suit,  $p$  est un nombre premier fixé et  $\chi \neq 1$  est un caractère modulo  $p$  également fixé. On étend comme d'habitude  $\chi$  à  $\mathbf{Z}/p\mathbf{Z}$  (et  $\mathbf{Z}$ ) en posant  $\chi(0) = 0$ .

La somme de Gauss associée à  $\chi$  est

$$\tau(\chi) = \sum_{a \bmod p} \chi(a) e\left(\frac{a}{p}\right) \quad (1)$$

et on a  $\tau(\chi)\tau(\bar{\chi}) = \chi(-1)p$ . On note  $W(\chi)$  le “signe” de la somme de Gauss, c'est à dire le nombre complexe de module 1 défini par  $W(\chi) = \tau(\chi)/\sqrt{p}$ . On a

\*Kowalski a bénéficié de la bourse National Science Foundation DMS-9202022.

$W(\chi)W(\bar{\chi}) = \chi(-1)$ ,  $W(\chi)^2 W(\bar{\chi})^2 = 1$ . De plus, pour tout  $x$  modulo  $p$  on a

$$\chi(x) = \frac{1}{\tau(\bar{\chi})} \sum_{a \bmod p} \bar{\chi}(a) e\left(\frac{ax}{p}\right). \quad (2)$$

LEMME 1

*Le caractère  $\chi$  vérifie  $W(\chi)^2 = 1$  si et seulement si  $\chi$  est quadratique et pair.*

*Démonstration*

En effet, soit  $\sigma_\alpha$ , pour  $\alpha \in (\mathbf{Z}/p\mathbf{Z})^\times$ , l'automorphisme du corps cyclotomique  $\mathbf{Q}(\mu_{p(p-1)})$  donné par  $e(1/p) \mapsto e(\alpha/p)$  et fixant  $e(1/(p-1))$ . La somme de Gauss, donc aussi  $W(\chi)^2$ , sont dans ce corps et on a

$$\sigma_\alpha(W(\chi)^2) = \frac{\sigma_\alpha(\tau(\chi)^2)}{p} = \bar{\chi}(\alpha)^2 W(\chi)^2$$

donc pour avoir  $W(\chi)^2 = 1$ , il faut que  $\chi(\alpha)^2 = 1$  pour tout  $\alpha \in \mathbf{Z}/p\mathbf{Z}$ ,  $\alpha \neq 0$ . Cela signifie que  $\chi$  is quadratique. Mais alors  $W(\chi)^2 = W(\chi)W(\bar{\chi}) = \chi(-1)$ , donc  $W(\chi)^2 = 1$  requiert aussi que  $\chi$  soit pair. La réciproque est évidente.  $\square$

## 2. Réductions

On pose

$$b_\chi(a) = \bar{\chi}(a) - W(\bar{\chi})^2 \chi(a)$$

pour  $a \in \mathbf{Z}/p\mathbf{Z}$ , et

$$F(\chi, u) = \sum_{x=u}^{x=-\bar{u}} (\chi(x) - \chi(-1)\bar{\chi}(x))$$

pour  $u \in \mathbf{Z}/p\mathbf{Z}$ ,  $u \neq 0$ . Le problème à résoudre est de montrer que si  $F(\chi, \cdot)$  est identiquement nulle, alors  $\chi$  est quadratique et pair.

LEMME 2

*On a pour tout  $u \neq 0$ ,*

$$F(\chi, u) = \frac{1}{\tau(\bar{\chi})} \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e(a/p)} \left( e\left(\frac{au}{p}\right) - e\left(\frac{a(1-\bar{u})}{p}\right) \right).$$

*Démonstration*

Soit

$$f(\chi, u) = \sum_{x=u}^{x=-\bar{u}} \chi(x);$$



on a  $F(\chi, u) = f(\chi, u) - \chi(-1)f(\bar{\chi}, u)$ .

On utilise (2) pour écrire  $\chi(x)$  en terme de caractères additifs. Choisissons le représentant  $u_1$  de  $u$  tel que  $0 < u_1 < p$ , et un représentant  $u_2 > u_1$  de  $-\bar{u}$ . Alors, (2) donne

$$f(\chi, u) = \frac{1}{\tau(\bar{\chi})} \sum_{a \neq 0} \bar{\chi}(a) \sum_{x=u_1}^{x=u_2} e\left(\frac{ax}{p}\right)$$

et la somme intérieure est une progression géométrique,

$$\sum_{x=u_1}^{x=u_2} e\left(\frac{ax}{p}\right) = e\left(\frac{au_1}{p}\right) \frac{1 - e((u_2 - u_1 + 1)a/p)}{1 - e(a/p)}$$

d'où, réduisant  $u_1$  et  $u_2$  modulo  $p$  de nouveau

$$f(\chi, u) = \frac{1}{\tau(\bar{\chi})} \sum_{a \neq 0} \frac{\bar{\chi}(a)}{1 - e(a/p)} \left( e\left(\frac{au}{p}\right) - e\left(\frac{a(1 - \bar{u})}{p}\right) \right). \quad (3)$$

Appliqué à  $\bar{\chi}$  au lieu de  $\chi$ , cela donne

$$\chi(-1)f(\bar{\chi}, u) = \frac{\chi(-1)}{\tau(\chi)} \sum_{a \neq 0} \frac{\chi(a)}{1 - e(a/p)} \left( e\left(\frac{au}{p}\right) - e\left(\frac{a(1 - \bar{u})}{p}\right) \right). \quad (4)$$

Puisque  $\tau(\chi)\tau(\bar{\chi}) = \chi(-1)p$ ,

$$\frac{\chi(-1)}{\tau(\chi)} = \frac{\tau(\bar{\chi})}{p} = \frac{1}{\tau(\bar{\chi})} \frac{\tau(\bar{\chi})^2}{p} = \frac{1}{\tau(\bar{\chi})} W(\bar{\chi})^2$$

donc le lemme découle des deux formules (3) et (4) pour  $f(\chi, u)$  et  $f(\bar{\chi}, u)$ .  $\square$

Définissons

$$G(u) = \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e(a/p)} e\left(\frac{au}{p}\right), \quad (5)$$

$$H(u) = \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e(a/p)} e\left(\frac{a}{p}\right) e\left(\frac{-au}{p}\right). \quad (6)$$

Le lemme s'écrit donc

$$F(\chi, u) = G(u) - H(\bar{u}). \quad (7)$$

On va maintenant appliquer l'analyse de Fourier sur le groupe multiplicatif  $(\mathbf{Z}/p\mathbf{Z})^\times$ , considérant l'identité hypothétique  $F(\chi, \cdot) = 0$  comme une relation de “modularité” entre  $G$  et  $H$  que l'on analyse par “transformation de Mellin”. Ce n'est que l'un de plusieurs choix possibles ici, d'autres solutions sont sans doute disponibles.

Soit  $X$  le groupe des caractères multiplicatifs de  $\mathbf{Z}/p\mathbf{Z}$ . On définit la transformée  $\hat{f}$  d'une fonction  $f$  définie sur  $(\mathbf{Z}/p\mathbf{Z})^\times$ ,

$$\hat{f}(\psi) = \sum_{u \neq 0} f(u) \psi(u). \quad (8)$$

Par (7), on a

$$\hat{F}(\chi, \psi) = \hat{G}(\psi) - \hat{H}(\bar{\psi}). \quad (9)$$

LEMME 3

On a

$$\hat{G}(\psi) = \tau(\psi) \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e(a/p)} \bar{\psi}(a), \quad (10)$$

$$\hat{H}(\psi) = \psi(-1) \tau(\psi) \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e(a/p)} e\left(\frac{a}{p}\right) \bar{\psi}(a). \quad (11)$$

*Démonstration*

Cela découle immédiatement des définitions et de (2).  $\square$

L'équation (9) peut s'écrire

$$\hat{F}(\chi, \psi) = \tau(\psi) \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e(a/p)} \bar{\psi}(a) - \frac{p}{\tau(\psi)} \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e(a/p)} e\left(\frac{a}{p}\right) \psi(a)$$

ou bien

$$\frac{\tau(\psi)}{p} \hat{F}(\chi, \psi) = \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e(a/p)} W(\psi)^2 \bar{\psi}(a) - \sum_{a \neq 0} \frac{b_\chi(\bar{a})}{1 - e(\bar{a}/p)} e\left(\frac{\bar{a}}{p}\right) \bar{\psi}(a). \quad (12)$$

LEMME 4

Soit  $f$  une fonction sur  $X$  de la forme

$$f(\psi) = \sum_{a \neq 0} c(a) W(\psi)^2 \bar{\psi}(a)$$

pour des nombres complexes  $c(a)$ . Alors pour tout  $b$  modulo  $p$ ,  $b \neq 0$ , on a

$$\frac{1}{p-1} \sum_{\psi \in X} \bar{\psi}(b) f(\psi) = \frac{1}{p} \sum_{a \neq 0} c(a) S(a, b; p)$$

où

$$S(a, b; p) = \sum_{x \neq 0} e\left(\frac{ax + b\bar{x}}{p}\right)$$

est la somme de Kloosterman.

*Démonstration*

Il suffit d'appliquer le lemme suivant, bien connu, et d'inverser l'ordre de sommation.

□

LEMME 5

Pour tout  $x$  modulo  $p$ ,  $x \neq 0$ , on a

$$\sum_{\psi \in X} W(\psi)^2 \bar{\psi}(x) = \frac{p-1}{p} S(1, x; p).$$

*Démonstration*

On calcule, en développant le carré de la somme de Gauss :

$$\begin{aligned} \sum_{\psi \in X} W(\psi)^2 \bar{\psi}(x) &= \frac{1}{p} \sum_{\psi} \bar{\psi}(x) \sum_{y,z} \psi(y) \psi(z) e\left(\frac{y+z}{p}\right) \\ &= \frac{1}{p} \sum_{y,z} e\left(\frac{y+z}{p}\right) \sum_{\psi} \psi(\bar{x}yz) \\ &= \frac{p-1}{p} \sum_{yz=x} e\left(\frac{y+z}{p}\right) = \frac{p-1}{p} S(1, x, p). \end{aligned} \quad \square$$

Soit  $\hat{F}_1(\chi, \psi)$  le membre de gauche de (12). On calcule

$$\frac{1}{p-1} \sum_{\psi \in X} \psi(\bar{b}) \hat{F}_1(\chi, \psi)$$

et on obtient par le lemme et par orthogonalité des caractères, pour tout  $b \neq 0$ ,

$$\frac{1}{p-1} \sum_{\psi \in X} \psi(\bar{b}) \hat{F}_1(\chi, \psi) = \frac{1}{p} \sum_{a \neq 0} \frac{b_{\chi}(a)}{1 - e(a/p)} S(a, b; p) - \frac{b_{\chi}(b)}{1 - e(b/p)} e\left(\frac{b}{p}\right). \quad (13)$$

**3. Fin de la preuve**

On peut maintenant prouver la proposition suivante.

PROPOSITION 1

Il existe une constante absolue  $P$  telle que si  $p > P$ , et  $\chi$  n'est pas quadratique pair, alors  $F(\chi, \cdot)$  n'est pas identiquement nulle.

LEMME 6

On a pour  $0 \leq x \leq \pi$ ,

$$\sqrt{\frac{2}{5}}(2\pi x) \leq |1 - e(x)| \leq 2\pi x.$$

LEMME 7

Pour tout  $a \neq 0$ , on a

$$\frac{1}{p} \left| \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e(a/p)} S(a, b; p) \right| \leq \frac{2\sqrt{10}}{\pi} \sqrt{p} \log(2(p-1)) \leq 2.02 \sqrt{p} \log(2(p-1)).$$

*Démonstration*

On a  $|b_\chi(a)| \leq 2$ , et de plus l'estimation de Weil pour les sommes de Kloosterman, pour tout  $ab \neq 0$ ,

$$S(a, b; p) \leq 2\sqrt{p}$$

donc

$$\begin{aligned} \frac{1}{p} \left| \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e(a/p)} S(a, b; p) \right| &\leq \frac{4}{\sqrt{p}} \sum_{a \neq 0} \frac{1}{|1 - e(a/p)|} \\ &= \frac{8}{\sqrt{p}} \sum_{0 < a \leq (p-1)/2} \frac{1}{|1 - e(a/p)|} \\ &\leq \frac{2\sqrt{10}}{\pi} \sqrt{p} \sum_{0 < a \leq (p-1)/2} \frac{1}{a} \quad (\text{par le Lemme 6}) \\ &\leq \frac{2\sqrt{10}}{\pi} \sqrt{p} \log(2(p-1)). \quad \square \end{aligned}$$

LEMME 8

Supposons que  $\chi$  n'est pas quadratique. Soit  $\varepsilon > 0$  un réel fixé,  $A = p^{1/4+\varepsilon}$ . Alors

$$\sum_{1 \leq a \leq A} |b_\chi(a)|^2 = 2A + O(A^{1-\delta})$$

pour un  $\delta = \delta(\varepsilon) > 0$ , la constante implicite du  $O$  ne dépendant que de  $\varepsilon$ .

*Démonstration*

Soit  $w = W(\bar{\chi})$ . On a

$$\begin{aligned} \sum_{a \leq A} |b_\chi(a)|^2 &= \sum_{a \leq A} (2 - w^2 \chi(a)^2 - \bar{w}^2 \bar{\chi}(a)^2) \\ &= 2A - w^2 \sum_{a \leq A} \chi(a)^2 - \bar{w}^2 \sum_{a \leq A} \bar{\chi}(a)^2. \end{aligned}$$

Comme  $\chi$  n'est pas quadratique,  $\chi^2$  est un caractère non-trivial. D'après D. Burgess [Bur], [FI], on a alors

$$\sum_{a \leq A} \chi(a)^2 \ll A^{1-\delta}, \quad \sum_{a \leq A} \bar{\chi}(a)^2 \ll A^{1-\delta}$$

pour un certain  $\delta = \delta(\varepsilon) > 0$ ; c'est là que l'hypothèse  $A = p^{1/4+\varepsilon}$  avec  $\varepsilon > 0$  intervient.  $\square$

Notons que si l'on admet l'hypothèse de Riemann pour les fonctions  $L$  de caractères de Dirichlet, on peut raffiner considérablement cette inégalité.

*Démonstration de la Proposition 1*

Soit  $\chi$  un caractère tel que  $F(\chi, \cdot) = 0$ . Alors, d'après (13), on a pour tout  $b \neq 0$  l'égalité

$$\frac{b_\chi(b)}{1 - e(b/p)} e\left(\frac{b}{p}\right) = \frac{1}{p} \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e(a/p)} S(a, b; p). \quad (14)$$

L'idée est qu'une telle identité n'est pas possible car les deux membres ne sont pas du même ordre de grandeur. Le membre de droite, d'après le Lemme 8, est borné par

$$\frac{1}{p} \left| \sum_{a \neq 0} \frac{b_\chi(a)}{1 - e(a/p)} S(a, b; p) \right| \leq 2.02\sqrt{p} \log(2(p-1)). \quad (15)$$

Ainsi pour  $b < p/2$ , on déduit l'inégalité

$$\frac{p}{b} \frac{|b_\chi(b)|}{2\pi} \leq 2.02\sqrt{p} \log(2(p-1)). \quad (16)$$

En particulier, si  $\chi$  est quadratique pair,  $|b_\chi(b)| = 0$  et le membre de gauche est toujours nul. Si  $\chi$  est quadratique impair,  $|b_\chi(b)| = 2$  donc on obtient, en prenant  $b = 1$ , l'inégalité  $\sqrt{p} \leq 2.02\pi \log(2(p-1))$  qui est impossible dès que  $p \geq 3067$ .

Si  $\chi$  n'est pas quadratique, on peut appliquer le Lemme 8 : celui ci implique que, si l'on fixe  $\varepsilon > 0$  quelconque, alors si  $p > P$  il existe  $b \leq A = p^{1/4+\varepsilon}$  tel que  $|b_\chi(b)| \geq \sqrt{2}$ . Procédant comme ci-dessus avec ce  $b$  dans (16) on trouve que cette inégalité impliquerait

$$\frac{\sqrt{2}}{2\pi} p^{3/4-\varepsilon} \leq 2.02\sqrt{p} \log(2(p-1)).$$

Cela est impossible pour  $p$  assez grand si  $\varepsilon$  a été choisi moins que  $1/4$ .  $\square$

*Remarque.* Pour obtenir une constante explicite  $B$  telle que  $p > B$  est suffisant pour la validité de cet argument, il suffit d'avoir une forme explicite du lemme 8, ce qui

revient à avoir une forme explicite de l’estimation de Burgess (ou, en fait, de n’importe quelle estimation de sommes de caractères

$$S(\chi, A) = \sum_{a \leq A} \chi(a)$$

meilleure que l’inégalité de Polya-Vinogradov

$$|S(\chi, A)| \leq 4\sqrt{p} \log(p)$$

car il faut trouver  $b < \sqrt{p}(\log p)^{-1}$  tel que  $b_\chi(b)$  ne soit pas trop petit). Malheureusement, il ne semble pas que des constantes possibles aient été explicitées.

De plus, dans l’inégalité de Burgess, le  $\delta(\varepsilon)$  est en général très petit, d’autant plus que  $\varepsilon$  est petit ; par exemple, pour  $\varepsilon = 1/16$ , donc  $1/4 + \varepsilon = 5/16$ , on a  $\delta = 1/256$ . Cela signifie que si la constante implicite est mauvaise dans l’inégalité de Burgess, on aura le lemme seulement pour  $p$  très grand.

*Remarque.* En fait, on peut établir l’hypothèse  $H_p(\chi)$  de manière complètement élémentaire (i.e., sans avoir recours à l’inégalité de Burgess qui utilise l’hypothèse de Riemann pour les courbes sur les corps finis). Supposons que  $\chi$  n’est pas quadratique et que  $|W(\chi)^2 - 1| \leq p^{-1/4}$  (dans le cas contraire, on conclut à nouveau par (16) appliquée à  $b = 1$ ), on applique alors le lemme suivant, au caractère (non-trivial)  $\chi^2$  (c’est une variante de la célèbre majoration de Vinogradov du plus petit premier non-résidu quadratique ; sa preuve est élémentaire et n’utilise que des arguments simples de crible ; cf. [LK, Thm. 7.7.6]).

#### LEMME 9

*Soit  $p$  un nombre premier assez grand et  $\chi$  un caractère non-trivial modulo  $p$ , alors il existe un premier  $2 \leq \ell \leq p^{1/2\sqrt{e}} \log^2 p$  tel que  $|\chi(\ell) - 1| \geq 1/\log^3 p$ .*

On obtient alors la majoration

$$\frac{p^{(1-1/\sqrt{e})/2}}{\log^5 p \log(2(p-1))} \leq 4.04\pi$$

qui est impossible si  $p$  est assez grand.

#### References

- [Bur] D. A. BURGESS, *On character sums and L-series, II*, Proc. London Math. Soc. (3) **13** (1963), 524–536. MR 26:6133

- [FI] J. FRIEDLANDER et H. IWANIEC, *A mean-value theorem for character sums*, Michigan Math. J. **39** (1992), 153–159. MR 92k:11084
- [KM] E. KOWALSKI et P. MICHEL, *Deux théorèmes de non-annulation de valeurs spéciales de fonctions  $L$* , Manuscripta Math. **104** (2001), 1–19. MR 1 820 726
- [LK] L. K. HUA [HUA LOO KENG], *Introduction to Number Theory*, Springer, Berlin, 1982. MR 83f:10001

*Kowalski*

Université Bordeaux I-A2X, 351, cours de la Libération, 33405 Talence CEDEX, France;  
kowalski@math.u-bordeaux.fr

*Michel*

L’Institut Universitaire de France ; Université Montpellier II, Place Eugène Bataillon, 34095  
Montpellier CEDEX 05, France ; michel@math.univ-montp2.fr