Une construction modulaire d'extensions non ramifiées de $\mathbf{Q}(\mu_p)$

Kenneth A. Ribet
Princeton

Reçu le 13 avril 1976

1. Introduction

Un nombre premier impair p est dit *irrégulier* si le nombre de classes du corps $\mathbf{Q}(\mu_p)$ est divisible par p (μ_p étant, comme d'habitude, le groupe des racines p-ièmes de l'unité). D'après le critère de Kummer, p est irrégulier si et seulement s'il existe un entier pair k avec $2 \leq k \leq p-3$ tel que p divise (le numérateur de) le k-ième nombre de Bernoulli B_k, donné par le développement

$$\frac{t}{e^t - 1} + \frac{t}{2} - 1 = \sum_{n \geq 2} \frac{B_n}{n!} t^n.$$

Le but de cet article est de renforcer le critère de Kummer.
Soit $\mathcal{A}$ le groupe des classes d'idéaux de $\mathbf{Q}(\mu_p)$, et soit C le $\mathbf{F}_p$-espace vectoriel A/A^p. Le groupe de Galois $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ agit sur C par l'intermédiaire de son quotient $G = \mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$. Comme tous les caractères de G à valeurs dans $\mathbf{F}_p^*$ sont des puissances du caractère standard

$$\chi\colon\ \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to G \xrightarrow{\sim} \mathbf{F}_p^*$$

donnant l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur μ_p, l'espace vectoriel C possède une décomposition canonique

$$C = \bigoplus_{i \bmod (p-1)} C(\chi^i),$$

où

$$C(\chi^i) = \{c \in C \mid \sigma c = \chi^i(\sigma) c \text{ pour tout } \sigma \in G\}.$$

Théorème 1 (Théorème principal)**.** *Soit k pair, $2 \leq k \leq p-3$. Alors $p \mid B_k$ si et seulement si $C(\chi^{1-k}) \neq 0$.*

En fait, l'affirmation selon laquelle $C(\chi^{1-k}) \neq 0$ implique $p \mid B_k$ est bien connue [8, Th. 3]. Sa réciproque est également familière comme une conséquence de la conjecture selon laquelle p est premier au nombre de classes du sous-corps réel $\mathbf{Q}(\mu_p)^+$ de $\mathbf{Q}(\mu_p)$ [8, p. 434]. Ainsi, la contribution de cet article est de prouver que $p \mid B_k$ implique $C(\chi^{1-k}) \neq 0$ sans faire d'hypothèse supplémentaire. Par une formule de "fonctorialité" pour le symbole d'Artin [20, Th. 11.5, p. 199], cette implication est équivalente à

Théorème 2. *Supposons $p \mid B_k$. Alors il existe une extension galoisienne $E/\mathbf{Q}$ contenant $\mathbf{Q}(\mu_p)$ avec les propriétés suivantes :*

1. *L'extension $E/\mathbf{Q}(\mu_p)$ est non ramifiée.*
2. *Le groupe $H = \mathrm{Gal}(E/\mathbf{Q}(\mu_p))$ est un groupe abélien non nul de type $(p, \ldots, p)$, c'est-à-dire tué par p.*
3. *Si $\sigma \in G$ et $\tau \in H$, alors*
$$\sigma\tau\sigma^{-1} = \chi(\sigma)^{1-k} \cdot \tau.$$

En fait, nous prouverons (1.2) avec $\mathbf{Q}(\mu_p)$ remplacé par l'unique sous-corps $\mathbf{Q}(\mu_p^{\otimes(1-k)})$ de $\mathbf{Q}(\mu_p)$ dont le degré sur $\mathbf{Q}$ est $(p-1)/(p-1, k-1)$. Ce sous-corps est le corps correspondant au noyau dans $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ de χ^{1-k}.

Théorème 3. *Supposons $p \mid B_k$. Alors il existe un corps fini $\mathbf{F} \supseteq \mathbf{F}_p$ et une représentation continue*
$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{F})$$
avec les propriétés :

1. *$\overline{\rho}$ est non ramifiée en tous les nombres premiers $l \neq p$.*
2. *La représentation $\overline{\rho}$ est réductible (sur $\mathbf{F}$) de telle sorte que $\overline{\rho}$ est isomorphe à une représentation de la forme*
$$\begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix}.$$
C'est-à-dire que $\overline{\rho}$ est une extension de la représentation 1-dimensionnelle de caractère χ^{k-1} par la représentation 1-dimensionnelle triviale.
3. *L'image de $\overline{\rho}$ est d'ordre divisible par p. En d'autres termes, $\overline{\rho}$ n'est pas diagonalisable.*
4. *Soit D un groupe de décomposition pour p dans $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Alors $\overline{\rho}(D)$ est d'ordre premier à p, c'est-à-dire que $\overline{\rho}|_D$ est diagonalisable.*

Remarquons que (1.3) implique (1.2). En effet, si $\overline{\rho}$ satisfait aux propriétés ci-dessus, alors l'image de $\overline{\rho}$ est le groupe de Galois d'une extension $E/\mathbf{Q}$ telle que E est de type $(p, \ldots, p)$ sur le corps $\mathbf{Q}(\mu_p^{\otimes(1-k)})$. Maintenant, $E/\mathbf{Q}$ est non ramifiée en dehors de p par (i), et la couche $(p, \ldots, p)$ est une extension non triviale par (iii). Cette extension $(p, \ldots, p)$ est non ramifiée en (l'unique idéal au-dessus de) p par (iv) ; elle est donc non ramifiée partout. Enfin, la formule de conjugaison (c) de (1.2) découle de l'identité matricielle
$$\begin{pmatrix} \chi^{1-k} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \chi^{k-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \chi^{1-k}* \\ 0 & 1 \end{pmatrix}.$$

Pour prouver (1.3), nous commençons par "trouver" $\overline{\rho}$ dans la représentation p-adique associée à la variété modulaire $J_1(p)$ attachée aux formes de poids 2 sur $\Gamma_1(p)$. En supposant que $p \mid B_k$, nous construisons une forme propre normalisée $f = \sum a_n q^n$ dans l'espace de ces formes paraboliques qui satisfait
$$a_l \equiv 1 + l^{k-1} \bmod \mathcal{M}$$
pour tous les nombres premiers $l \neq p$, où $\mathcal{M}$ est un certain idéal fixé au-dessus de p dans le corps engendré par les coefficients a_n. Cela conduit à notre $\overline{\rho}$, et au moment où nous avons construit $\overline{\rho}$,

nous savons de la construction que (i), (ii) et (iii) de (1.3) sont satisfaites par $\overline{\rho}$. Il reste alors à prouver (iv). Nous utilisons alors le théorème de Deligne-Rapoport selon lequel la variété $J_1(p)/J_0(p)$ acquiert une bonne réduction partout sur le sous-corps réel $\mathbf{Q}(\mu_p)^+$ de $\mathbf{Q}(\mu_p)$ [5]. Cela implique que, localement en p, $\overline{\rho}|\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\mu_p)^+)$ est la représentation attachée à un schéma en groupes commutatif fini plat de type $(p,\dots,p)$ sur l'anneau des entiers du complété $\mathbf{Q}(\mu_p)^+ \otimes \mathbf{Q}_p$. Nous notons en particulier que l'indice de ramification absolu de ce complété est $(p-1)/2 < p-1$; cela nous permet de prouver (iv) en appliquant les résultats de Raynaud [15] sur les schémas en groupes de type $(p,\dots,p)$.

Notre preuve est motivée par deux idées clés de Serre. La première idée (cf. [16]) est que la divisibilité de B_k par p implique une congruence similaire à celle ci-dessus pour une certaine forme parabolique de poids k sur $\mathbf{SL}(2,\mathbf{Z})$; par conséquent, une représentation telle que notre $\overline{\rho}$ devrait être obtenue à partir de la représentation de Deligne ρ_k attachée aux formes de poids k sur $\mathbf{SL}(2,\mathbf{Z})$. Bien que nos méthodes "trouvent" dans ρ_k une représentation $\overline{\rho}$ qui satisfait les trois premières propriétés de (1.3), une preuve que cette représentation satisfait (iv) semblerait nécessiter des propriétés galoisiennes inconnues de la cohomologie étale. Cela conduit à la deuxième idée de Serre, que les représentations (mod p) provenant de ρ_k devraient être visibles (au moins à un twist près) sur la variété jacobienne $J_1(p)$. (Une idée similaire est le point de départ d'un article récent de Koike [10].) C'est ce qui nous a conduit à examiner les formes de poids 2.

Nous espérons que notre méthode s'appliquera également à des critères plus généraux de type Kummer, comme celui donné par Greenberg [7]. Quelques calculs pertinents ont été effectués par Yamauchi [21].

L'auteur tient à reconnaître l'assistance inestimable de N. Katz pendant la réalisation de ce travail. Il est en outre redevable à J. Coates, P. Deligne, B. Mazur, et J-P. Serre pour de nombreuses conversations utiles.

2. Réductions de représentations réductibles

Soit K une extension finie de $\mathbf{Q}_p$. Soit $\mathcal{O}$ son anneau d'entiers, $\mathbf{F}$ le corps résiduel, et π une uniformisante. Soit V un module libre de rang 2 sur K. Un *réseau* dans V est un $\mathcal{O}$-module libre de rang 2 dans V qui engendre V sur K.

Nous supposons donnée une représentation

$$\rho\colon G \to \mathbf{GL}(V)$$

d'un groupe G dans V telle que G laisse stables certains réseaux de V. (Cette dernière condition est toujours satisfaite si G est compact et ρ est continue, par exemple.) Si $T \subset V$ est stable par G, alors G agit sur $T/\pi T$, qui est libre de rang 2 sur $\mathbf{F}$. L'application associée

$$\overline{\rho}\colon G \to \mathbf{GL}(T/\pi T)$$

sera appelée la *réduction* de ρ attachée à T. Il est connu que la semi-simplification de $\overline{\rho}$ (en tant que représentation sur $\mathbf{F}$) est indépendante du choix de T [4, 30.16], de sorte que $\overline{\rho}$ est unique si une réduction (et donc toute réduction) est simple.

Nous considérons cependant la situation opposée, où les réductions sont toutes réductibles. Leurs semi-simplifications sont alors décrites par deux caractères $\varphi_1, \varphi_2\colon G \to \mathbf{F}^*$, qui ne dépendent pas

du choix de T. Une réduction donnée peut s'écrire matriciellement sous l'une des formes :

$$\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} \varphi_1 & 0 \\ * & \varphi_2 \end{pmatrix}.$$

Elle est diagonalisable (c'est-à-dire semi-simple) si et seulement si son image est d'ordre premier à p.

Proposition 4. *Supposons que la représentation ρ sur K soit simple mais que ses réductions soient réductibles. Soient φ_1 et φ_2 les caractères associés aux réductions de ρ. Alors G laisse stable un certain réseau $L \subset V$ pour lequel la réduction associée est de la forme $\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$ mais n'est pas semi-simple.*

Démonstration. Choisissons un réseau G-stable de V ainsi qu'une base $\mathcal{O}$-libre de ce réseau. Alors ρ peut être vue comme une application $G \to \mathbf{GL}(2, \mathcal{O})$. Toute matrice $M \in \mathbf{GL}(2, K)$ telle que $M\rho(G)M^{-1} \subseteq \mathbf{GL}(2, \mathcal{O})$ définit alors un autre réseau G-stable ainsi qu'une base de celui-ci. La réduction attachée à ce nouveau réseau est l'application

$$G \to M\rho(G)M^{-1} \subset \mathbf{GL}(2, \mathcal{O}) \to \mathbf{GL}(2, \mathbf{F}).$$

Pour prouver la proposition, nous effectuons quelques calculs basés sur la formule

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = P^{-1} \begin{pmatrix} a & \pi^{-1}b \\ \pi c & d \end{pmatrix} P,$$

où P est la matrice $\begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix}$.
Nous notons d'abord que nous pouvons supposer au départ que la réduction de l'application donnée $G \to \mathbf{GL}(2, \mathcal{O})$ est de la forme $\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$ plutôt que $\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$; en effet, si la seconde se produit, nous pouvons diviser les coefficients du coin supérieur droit par π et multiplier ceux du coin inférieur gauche par π en utilisant la formule ci-dessus. Faisons cette hypothèse ainsi que la suivante : chaque réduction $\overline{\rho}$ de la forme $\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$ est semi-simple. Avec ces hypothèses, nous allons montrer que ρ est elle-même réductible, et ainsi prouver (2.1) par contradiction.
Posons $M_0 = I$ (matrice identité 2×2). De manière inductive, nous allons définir une suite convergente de matrices $M_i = \begin{pmatrix} 1 & t_i \\ 0 & 1 \end{pmatrix}$ telles que $M_i\rho(G)M_i^{-1}$ consiste en des éléments de $\mathbf{GL}(2, \mathcal{O})$ dont les coefficients du coin inférieur gauche sont divisibles par π et ceux du coin supérieur droit sont divisibles par π^i. Cela prouvera que ρ est réductible car la matrice $M = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ avec $t = \lim t_i$ sera alors telle que $M\rho(G)M^{-1}$ consiste en des matrices dont les coefficients du coin supérieur droit sont nuls.
D'après la formule de conjugaison ci-dessus, l'hypothèse d'induction peut être reformulée comme suit : $P^iM_i\rho(G)M_i^{-1}P^{-i}$ consiste en des matrices entières dont les coefficients du coin inférieur gauche sont divisibles par π^{i+1}. Avec cette hypothèse, la représentation $\sigma \mapsto P^iM_i\rho(\sigma)M_i^{-1}P^{-i}$

(mod π) est de la forme $\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$ car $\sigma \mapsto \rho(\sigma) \pmod{\pi}$ est de cette forme. La représentation en question est alors par hypothèse semi-simple, donc nous pouvons choisir un élément u de $\mathcal{O}$ tel que la matrice $U = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ diagonalise la représentation (mod π). C'est-à-dire que nous pouvons trouver un u dans $\mathcal{O}$ tel que

$$UP^i M_i \rho(G) M_i^{-1} P^{-i} U^{-1}$$

consiste en des matrices dont les coefficients du coin supérieur droit sont divisibles par π (et dont les coefficients du coin inférieur gauche sont encore divisibles par π^{i+1} : la conjugaison par U laisse inchangé le coin inférieur gauche de toute matrice). Cela donne que

$$(P^{-i}UP^iM_i)\rho(G)(P^{-i}UP^iM_i)^{-1}$$

consiste en des matrices entières dont les coefficients du coin inférieur gauche sont divisibles par π et dont les coefficients du coin supérieur droit sont divisibles par π^{i+1}. Ainsi, nous pouvons poursuivre l'induction en posant

$$M_{i+1} = P^{-i}UP^iM_i.$$

Cette formule rend visible le fait que $\{M_i\}$ converge. □

3. Une congruence entre une forme parabolique et une série d'Eisenstein

Soit p un nombre premier impair et soit μ_{p-1} le groupe des racines complexes $(p-1)$-ièmes de l'unité. Nous considérons les formes modulaires de poids 1 et 2 sur $\Gamma_1(p)$. Pour un caractère

$$\epsilon\colon (\mathbf{Z}/p\mathbf{Z})^* \to \mu_{p-1}$$

(possiblement trivial), nous disons qu'une forme est de *type* ϵ si elle satisfait l'équation

$$f\left(\frac{az+b}{cz+d}\right) = \epsilon(d)(cz+d)^k f(z)$$

pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\Gamma_0(p)$. (Nous relevons ϵ comme d'habitude en une fonction sur $\mathbf{Z}$.) Une forme de type ϵ est une *forme parabolique* si son développement en q et celui de $f\left|\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}\right.$ commencent tous deux par 0 ; si le développement en q de f commence par 0, alors nous disons que f est une *semi-forme parabolique*.

Nous aurons besoin des séries d'Eisenstein. Soit ϵ un caractère pair non trivial. Alors les deux séries

$$G_{2,\epsilon} = \frac{L(-1,\epsilon)}{2} + \sum_{n\geq 1}\sum_{d|n}\epsilon(d)dq^n,$$

$$s_{2,\epsilon} = \sum_{n\geq 1}\sum_{d|n}\epsilon(n/d)dq^n$$

sont chacune de poids 2 et de type ϵ. L'espace des formes modulaires de poids 2 et de type ϵ est engendré par les formes paraboliques et ces deux séries, tandis que l'espace des semi-formes paraboliques de poids 2 et de type ϵ est engendré par $s_{2,\epsilon}$ et les formes paraboliques. Lorsque ϵ est le caractère trivial, nous avons encore une série d'Eisenstein $G_{2,\epsilon}$ comme ci-dessus ; elle peut s'écrire

$$\frac{p-1}{24} + \sum_{n\geq 1} \sum_{\substack{d|n \\ p\nmid d}} dq^n.$$

En poids 1, nous utilisons la série

$$G_{1,\epsilon} = \frac{L(0,\epsilon)}{2} + \sum_{n\geq 1} \sum_{d|n} \epsilon(d) q^n$$

lorsque ϵ est un caractère impair. Les séries d'Eisenstein sont des formes propres pour les opérateurs de Hecke $T(n)$, au moins lorsque n est premier à p.
Fixons maintenant un idéal premier $\mathfrak{p} \mid p$ du corps $\mathbf{Q}(\mu_{p-1})$. Alors soit $\omega\colon (\mathbf{Z}/p\mathbf{Z})^* \xrightarrow{\sim} \mu_{p-1}$ l'unique caractère qui satisfait

$$\omega(d) \equiv d \pmod{\mathfrak{p}}$$

pour tout $d \in \mathbf{Z}$.
Soit k pair, $2 \leq k \leq p-3$. Alors les formes modulaires $G_{2,\omega^{k-2}}$ et $G_{1,\omega^{k-1}}$ ont des développements en q $\mathfrak{p}$-entiers dans $\mathbf{Q}(\mu_{p-1})$ qui sont congrus modulo $\mathfrak{p}$ au développement en q

$$-\frac{B_k}{2k} + \sum_{n\geq 1} \sum_{d|n} d^{k-1} q^n.$$

Démonstration. Mis à part les termes constants des séries, l'assertion découle immédiatement du choix de ω. Pour prouver les assertions sur les termes constants, nous utilisons les expressions

$$L(0,\epsilon) = \frac{-1}{p} \sum_{n=1}^{p-1} \epsilon(n)(n - p/2),$$

$$L(-1,\epsilon) = \frac{-1}{2p} \sum_{n=1}^{p-1} \epsilon(n)(n^2 - pn + p^2/6)$$

des valeurs L comme nombres de Bernoulli généralisés, valables pour tout caractère $\epsilon \pmod p$, cf. [11]. En utilisant la congruence $\omega(n) \equiv n^p \pmod{p^2}$, nous trouvons

$$pL(0,\omega^{k-1}) \equiv -\sum_{n=1}^{p-1} n^{1+p(k-1)} \pmod{p^2},$$

$$pL(-1,\omega^{k-2}) \equiv \frac{-1}{2} \sum_{n=1}^{p-1} n^{2+p(k-2)} \pmod{p^2}.$$

D'autre part, si t est un entier pair positif, nous avons

$$pB_t \equiv \sum_{n=1}^{p-1} n^t \pmod{p^2}$$

d'après [1, (8.8), p. 385]. Le résultat désiré découle en combinant ces faits avec la congruence de Kummer [1, Th. 5, p. 385]. □

Corollaire 5. *Soit k comme ci-dessus, et soient n et m des entiers pairs, $2 \leq n, m \leq p-3$, satisfaisant $n+m \equiv k \mod (p-1)$. Alors le produit*

$$G_{1,\omega^{n-1}} G_{1,\omega^{m-1}}$$

est une forme modulaire de poids 2 et de type ω^{k-2} dont les coefficients du développement en q sont des p-entiers dans $\mathbf{Q}(\mu_{p-1})$. Son terme constant est une p-unité à condition que ni B_n ni B_m ne soit divisible par p.

Démonstration. Clair. □

Théorème 6. *Soit k comme ci-dessus. Alors il existe une forme modulaire g de poids 2 et de type ω^{k-2} dont les coefficients du développement en q sont des p-entiers dans $\mathbf{Q}(\mu_{p-1})$ et dont le terme constant est 1.*

Démonstration. Il suffit de construire un g dont le terme constant est une p-unité. Nous essayons d'abord la série d'Eisenstein $G_{2,\omega^{k-2}}$. D'après (3.1), cette forme commencera par un coefficient unité à moins que $p \mid B_k$. Si cela se produit, nous essayons alors les produits $G_{1,\omega^{n-1}} G_{1,\omega^{m-1}}$ comme dans (3.2). Si aucun de ces produits ne fonctionne, alors pour chaque paire n, m comme dans (3.2), au moins l'un des deux nombres B_n, B_m est divisible par p. Soit maintenant t le nombre d'entiers pairs n, $2 \leq n \leq p-3$, tels que p divise B_n. Un raisonnement élémentaire montre que $t \geq (p-1)/4$ si le théorème est faux. Cependant, nous avons $p^t \mid h_p^*$, où l'entier h_p^* est le soi-disant premier facteur du nombre de classes de $\mathbf{Q}(\mu_p)$ (voir ci-dessous). Donc, pour prouver le théorème, il suffira de prouver que

$$h_p^* < p^{(p-1)/4}.$$

D'après Carlitz et Olson [3], nous pouvons écrire h_p^* sous la forme $\pm D/p^{(p-3)/2}$, où D est un certain déterminant de dimension $(p-1)/2$ dont les coefficients sont des entiers compris entre 1 et $p-1$. Comme Carlitz l'a fait remarquer [2], l'inégalité de Hadamard donne alors immédiatement

$$h_p^* < p^{(p+3)/4} 2^{-(p-1)/4}.$$

Cela implique l'inégalité désirée car $h_p^* = 1$ pour $p \leq 19$ et $p \leq 2^{(p-1)/4}$ pour $p > 19$.
Pour prouver que p^t divise h_p^*, nous utilisons l'expression

$$h_p^* = \alpha p \prod_{k=2}^{p-1} L(0, \omega^{k-1}),$$

où α est une certaine puissance de 2 [7, p. 250]. Il suffira de montrer que p^t divise h_p^* puisque p est non ramifié. Or, d'après la formule pour $L(0,\epsilon)$ donnée ci-dessus, la quantité $p \cdot L(0, \omega^{p-2})$ est un entier algébrique. Ainsi, ce que nous voulons découle de (3.1) : si $p \mid B_k$ avec $2 \leq k \leq p-3$, alors p divise $L(0, \omega^{k-1})$. □

1. Masley et Montgomery [13] donnent les bornes

$$(2\pi)^{-p/2} p^{(p-2.5)/4} \leq h_p^* \leq (2\pi)^{-p/2} p^{(p+3.1)/4}$$

pour les nombres premiers p plus grands que 200. Cela montre que la borne supérieure élémentaire pour h_p^* que nous utilisons est en fait raisonnablement précise.

2. Le Théorème (3.3) peut être prouvé de manière plus conceptuelle par les méthodes de Mazur [14], en utilisant l'étude de Deligne-Rapoport de la courbe modulaire $X_1(p)$ au premier p [5, p. DeRa-108]. On voit par la technique de Mazur que g peut être choisi de manière à s'annuler à la pointe 0 de $X_1(p)$.
À partir de maintenant, nous fixons un entier pair k ($2 \leq k \leq p-3$) et faisons l'hypothèse que $p \mid B_k$. Nous posons $\epsilon = \omega^{k-2}$. Puisque $B_2 = 1/6$, k est en fait au moins 4 ; donc ϵ est un caractère pair non trivial. Toutes les formes modulaires seront désormais de poids 2 et de type ϵ.

Proposition 7. *Il existe une semi-forme parabolique $f = \sum_{n\geq 1} a_n q^n$ telle que les a_n sont des p-entiers dans $\mathbf{Q}(\mu_{p-1})$ et telle que*

$$f \equiv G_k \equiv G_{2,\epsilon} \pmod{p}$$

dans les développements en q.

Démonstration. Prenons $f = G_{2,\epsilon} - c \cdot g$, où c est le terme constant de $G_{2,\epsilon}$. Alors f est une semi-forme parabolique par construction, et nous avons $f \equiv G_{2,\epsilon}$ car $\mathfrak{p} \mid c$ par (3.1) et l'hypothèse $p \mid B_k$. De plus, $G_{2,\epsilon} \equiv G_k$ par (3.1). □

Proposition 8. *Il existe une forme parabolique non nulle f' de type ϵ qui est une forme propre pour tous les opérateurs de Hecke T_n avec $(n,p) = 1$ et qui a la propriété que pour chaque nombre premier $l \neq p$, la valeur propre $\lambda(l)$ de $T(l)$ agissant sur f' satisfait*

$$\lambda(l) \equiv 1 + l^{k-1} \equiv 1 + \epsilon(l) \pmod{\mathcal{M}},$$

où $\mathcal{M}$ est un certain idéal (indépendant de l) au-dessus de p dans le corps $\mathbf{Q}(\mu_{p-1}; \lambda(n))$ engendré par les valeurs propres sur $\mathbf{Q}(\mu_{p-1})$.

Démonstration. (cf. Koike [9]). La semi-forme parabolique f de (3.4) est une forme propre modulo p pour les opérateurs de Hecke, car elle est congrue à la forme propre $G_{2,\epsilon}$. Ses valeurs propres modulo p sont congruentes à celles désirées pour f'. Par conséquent, nous pouvons appliquer le lemme de Deligne-Serre [6, 6.11] pour obtenir une semi-forme parabolique f' comme dans l'énoncé de la proposition. Nous devons alors montrer que ce f' est en fait une forme parabolique. Mais comme remarqué ci-dessus, l'espace des semi-formes paraboliques est engendré par l'espace des formes paraboliques et la forme propre $s_{2,\epsilon}$. Il suffit donc de montrer que f' ne peut pas être $s_{2,\epsilon}$. Cependant, la valeur propre de $T(l)$ agissant sur $s_{2,\epsilon}$ est $\epsilon(l) + l$, et il est clair que nous ne pouvons pas avoir

$$\epsilon(l) + l \equiv 1 + l\epsilon(l) \pmod{\mathfrak{p}}$$

à moins que $\epsilon(l) = 1$. Puisque ϵ est un caractère non trivial, cela donne ce que l'on veut. □

Proposition 9. *Toute forme f' comme dans (3.5) est une forme propre pour tous les opérateurs de Hecke $T(n)$ (y compris ceux pour lesquels $p \mid n$). Par conséquent, après avoir remplacé f' par un multiple de f', nous avons*

$$f' = \sum_{n=1}^{\infty} \lambda(n) q^n$$

avec $f'|T(n) = \lambda(n) f'$.

Démonstration. Cela découle directement de (3.5) et de la théorie des newforms (voir, par exemple, [12, Th. 3]) puisqu'il n'y a pas de formes non nulles de poids 2 sur $\mathbf{SL}(2, \mathbf{Z})$. □

Nous récapitulons ce que nous avons conclu de l'hypothèse $p \mid B_k$:

Théorème 10. *Il existe une forme parabolique $f = \sum_{n\geq 1} a_n q^n$ de poids 2 et d'un certain type ϵ qui est une forme propre normalisée ($a_1 = 1$) pour tous les opérateurs de Hecke $T(n)$ et qui satisfait*

$$a_l \equiv 1 + l^{k-1} \equiv 1 + \epsilon(l) \pmod{\mathfrak{p}}$$

pour tous les nombres premiers $l \neq p$, où $\mathfrak{p}$ est un certain idéal premier au-dessus de p dans le corps K engendré par les coefficients de f, qui ne dépend pas de l.

Notons que nous pouvons voir ϵ comme un caractère (non trivial) à valeurs dans K^*, puisque les formules pour les opérateurs de Hecke montrent que les valeurs de ϵ se trouvent dans le corps engendré par les coefficients de f.

4. Construction et étude de la représentation (mod p)

Nous conservons les notations $f, \mathfrak{p}, K$ de (3.7). De plus, nous notons $\mathcal{O}$ l'anneau des entiers de K, $\mathcal{O}_\mathfrak{p}$ son complété en $\mathfrak{p}$, $K_\mathfrak{p}$ le complété de K en $\mathfrak{p}$, $\mathbf{F}$ le corps résiduel de $\mathcal{O}_\mathfrak{p}$, $\pi \in \mathcal{O}_\mathfrak{p}$ une uniformisante. Soit $A/\mathbf{Q}$ la variété abélienne attachée à f par la construction de Shimura [18, Th. 7.14]. Nous rappelons les propriétés suivantes de A :

1. La dimension de A est égale à l'entier $[K : \mathbf{Q}]$, et K est inclus comme sous-anneau de la $\mathbf{Q}$-algèbre $(\mathrm{End}_\mathbf{Q} A) \otimes \mathbf{Q}$ des endomorphismes de A définis sur $\mathbf{Q}$. Ainsi, le module de Tate p-adique
$$V_\mathfrak{p} = V_\mathfrak{p}(A) \otimes_K K_\mathfrak{p}$$
est un $K_\mathfrak{p}$-module libre de rang 2 sur lequel $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ agit.
2. La variété A est un facteur (sur $\mathbf{Q}$) du quotient de la variété modulaire $J_1(p)$ par l'image dans $J_1(p)$ de la variété $J_0(p)$. En particulier, A a bonne réduction en tous les nombres premiers $l \neq p$, de sorte que $V_\mathfrak{p}$ est non ramifiée en tous ces premiers. De plus, par un théorème de Deligne-Rapoport [5, Ex. 3.7(i), p. DeRa-113], A acquiert une bonne réduction partout sur le corps cyclotomique réel $\mathbf{Q}(\mu_p)^+$.
3. (Relation d'Eichler-Shimura [19, Th. 1.4]). Si $F_l \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ est un élément de Frobenius pour un nombre premier $l \neq p$, alors la trace (resp. le déterminant) de son action sur le $K_\mathfrak{p}$-espace vectoriel $V_\mathfrak{p}$ est a_l (resp. $l \cdot \epsilon(l)$), considéré comme un élément de $K_\mathfrak{p}$.

Définissons maintenant $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}_{K_\mathfrak{p}} V_\mathfrak{p}$ comme l'application provenant de l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur $V_\mathfrak{p}$. De (iii), nous déduisons que le déterminant de ρ est le produit $\chi\epsilon$ où nous considérons maintenant ϵ comme un caractère de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ et où χ est le caractère cyclotomique standard

$$\chi\colon\ \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}_p^* \subseteq K_\mathfrak{p}^*.$$

Proposition 11. *La représentation ρ sur $K_\mathfrak{p}$ est irréductible.*

Démonstration. Supposons le contraire. Alors la semi-simplification de ρ, qui est abélienne, est décrite par deux caractères $\rho_1, \rho_2 : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to K_\mathfrak{p}^*$. Elle est localement algébrique par [17, p. III-20] (ou parce qu'elle provient d'une variété abélienne), de sorte que chaque ρ_i peut s'écrire comme une puissance entière χ^{n_i} de χ sur un sous-groupe ouvert d'un groupe d'inertie pour p dans

$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Cela implique que $\rho_i = \chi^{n_i}\epsilon_i$, où ϵ_i est un caractère d'ordre fini ramifié seulement en p. En considérant les ϵ_i comme des caractères de Dirichlet, nous avons (pour $l \neq p$) les équations

$$l^{n_1+n_2}\epsilon_1(l)\epsilon_2(l) = l\epsilon(l),$$

$$a_l = \epsilon_1(l)l^{n_1} + \epsilon_2(l)l^{n_2}$$

à cause de (iii). De la première équation, nous obtenons $n_1 + n_2 = 1$, de sorte que l'un des n_i, disons n_1, est au moins 1. Par conséquent, $n_2 \leq 0$. En regardant la deuxième équation, nous voyons maintenant que $|a_l| \geq l - 1$ pour tout $l \neq p$. Lorsque $l \geq 7$, cependant, cela contredit "l'hypothèse de Riemann" $|a_l| \leq 2\sqrt{l}$. □

Désormais, nous utilisons χ pour désigner le caractère "χ mod p", à savoir la composition

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \xrightarrow{\chi} \mathbf{Z}_p^* \to \mathbf{F}_p^* \hookrightarrow \mathbf{F}^*.$$

Proposition 12. *Il existe un réseau $\mathcal{O}_\mathfrak{p}$-libre $L \subset V_\mathfrak{p}$ invariant par $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ pour lequel l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur $L/\pi L$ peut être décrite matriciellement par*

$$\begin{pmatrix} 1 & * \\ 0 & \chi^{k-1} \end{pmatrix}$$

et n'est en outre pas semi-simple.

Démonstration. Compte tenu de (4.1) et de (2.1), il suffit de montrer qu'il existe un réseau $T \subset V_\mathfrak{p}$ stable par $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ pour lequel l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur $T/\pi T$ est réductible de telle sorte que sa semi-simplification est donnée par les deux caractères 1 et χ^{k-1}. En effet, soit T un réseau $\mathcal{O}_\mathfrak{p}$-libre quelconque stable par $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Par la relation d'Eichler-Shimura, si $l \neq p$, alors un élément de Frobenius pour l agit sur $T/\pi T$ avec une trace $a_l \pmod{\pi}$ et un déterminant $l\epsilon(l) \pmod{\pi}$. À cause de (3.7), ces nombres sont respectivement congrus à $l^{k-1} + 1$ et $l^{k-1} \pmod{\pi}$. Par le théorème de densité de Čebotarev, la trace et le déterminant de l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur $T/\pi T$ sont respectivement $1 + \chi^{k-1}$ et χ^{k-1}. D'après le théorème de Brauer-Nesbitt [4, Th. 30.16], cela implique l'assertion désirée sur $T/\pi T$. □

Posons $M = L/\pi L$. Ce sera l'espace de représentation pour le $\overline{\rho}$ de (1.3). En fait, la propriété (ii) de ce paragraphe, ainsi que (4.2), montrent que les trois premières conditions de (1.3) sont satisfaites par la représentation. Il reste seulement à vérifier la quatrième condition.
Nous considérons le sous-groupe $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\mu_p)^+)$ de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ correspondant au corps cyclotomique réel $\mathbf{Q}(\mu_p)^+$. Dans ce sous-groupe, nous considérons un groupe de décomposition D pour l'unique idéal de $\mathbf{Q}(\mu_p)^+$ au-dessus de p. Puisque $p \nmid [\mathbf{Q}(\mu_p)^+ : \mathbf{Q}]$, pour vérifier la dernière condition de (1.3), il suffit de prouver que l'action de D sur M est semi-simple, c'est-à-dire que l'image de D dans $\mathrm{Aut}\, M$ est d'ordre premier à p. Il sera commode de noter E le complété du corps cyclotomique réel en p et d'identifier D à $\mathrm{Gal}(\overline{E}/E)$.

Proposition 13. *Le $\mathrm{Gal}(\overline{E}/E)$-module M est le module de Galois attaché à un schéma en groupes commutatif fini plat de type $(p, \ldots, p)$ sur l'anneau des entiers $\mathcal{R}$ de E.*

Démonstration. Après avoir changé A par une isogénie sur $\mathbf{Q}$, nous pouvons supposer que $\mathcal{O}$ opère sur A et que M est isomorphe au "noyau de p" sur A. Cela rend M isomorphe à un sous-module du module des points de p-division de A. Par le théorème de Deligne-Rapoport mentionné ci-dessus, A acquiert une bonne réduction sur E. Par conséquent, le module des points de p-division a la propriété affirmée pour M : c'est le module de Galois attaché au noyau schématique $\mathcal{A}_p$ de l'application "multiplication par p" sur le modèle de Néron pour A sur $\mathcal{R}$. Alors M, pour sa part, est le module de Galois attaché à la fermeture de Zariski $\mathcal{M}$ de M dans $\mathcal{A}_p$, cf. [15, § 2]. □

Avant de terminer la preuve que M est semi-simple en tant que D-module, nous résumons les propriétés de M que nous utiliserons :

1. Il est libre de rang 2 sur $\mathbf{F}$.
2. D agit trivialement sur un sous-espace 1-dimensionnel X de M et par l'intermédiaire du caractère $\chi(=\chi^{k-1})$ sur le quotient $Y = M/X$.
3. M est le module attaché à un schéma en groupes fini plat $\mathcal{M}$ de type $(p, \ldots, p)$ sur $\mathcal{R}$.

Théorème 14. *L'image de D dans* $\operatorname{Aut} M$ *est d'ordre premier à p.*

Démonstration. Soit $\mathcal{X}$ la fermeture de Zariski de X dans $\mathcal{M}$. Le D-module attaché à $\mathcal{X}$ est le module trivial X, et l'indice de ramification absolu de E est $(p-1)/2 < p-1$. Par conséquent, $\mathcal{X}$ est un schéma en groupes constant non nul sur $\mathcal{R}$ d'après le théorème de classification de Raynaud [15, Th. (3.3.3)]. Ainsi, $\mathcal{M}$ ne peut pas être connexe, puisqu'il possède le sous-groupe étale $\mathcal{X}$.
Prenons la suite exacte canonique de D-modules

$$0 \to M^0 \to M \to M^{\text{et}} \to 0,$$

où M^0 est associé au plus grand sous-groupe connexe de $\mathcal{M}$ et M^{et} au plus grand quotient étale. Parce que M a une structure d'espace vectoriel sur $\mathbf{F}$ compatible avec Galois, $\mathcal{M}$ est un "schéma en groupes dans les $\mathbf{F}$-espaces vectoriels" d'après le théorème de Raynaud mentionné ci-dessus. En particulier, la suite exacte ci-dessus est une suite d'espaces vectoriels sur $\mathbf{F}$.
Maintenant, M^0 n'est pas tout M car $\mathcal{M}$ n'est pas connexe. Et $M^0 \neq 0$ car M^{et} est non ramifié mais M ne l'est pas (puisqu'il a le quotient Y). Ainsi, M^0 est 1-dimensionnel. De plus, le fait que M^{et} soit non ramifié et Y ne le soit pas montre que l'image de M^0 dans M est distincte de X. Par conséquent, D laisse stable à la fois X et une droite dans M qui est distincte de X. Puisque tout élément d'ordre p dans $\operatorname{Aut} M$ laisse stable une unique droite, cela prouve ce que l'on veut. □

Références

[BS66] Borevich, Z. I., Shafarevich, I. R. : Number theory. New York : Academic Press 1966.

[Car61] Carlitz, L. : A generalization of Maillet's determinant and a bound for the first factor of the class number. Proc. A.M.S. 12, 256–261 (1961).

[CO55] Carlitz, L., Olson, F. R. : Maillet's determinant. Proc. A.M.S. 6, 265–269 (1955).

[CR62] Curtis, C., Reiner, I. : Representation theory of finite groups and associative algebras. New York : Interscience 1962.

[DR73] Deligne, P., Rapoport, M. : Les schémas de modules de courbes elliptiques. International Summer School on Modular Functions ; Antwerp, 1972. Lecture Notes in Math. 349, pp. 143–316. Berlin-Heidelberg-New York : Springer 1973.

[DS74] Deligne, P., Serre, J.-P. : Formes modulaires de poids 1. Ann. Scient. Ec. Norm. Sup., 4e série, 7, 507–530 (1974).

[Gre73] Greenberg, R. : A generalization of Kummer's criterion. Inventiones math. 21, 247–254 (1973).

[Her32] Herbrand, J. : Sur les classes des corps circulaires. J. Math. Pures et Appliquées, 9e série 11, 417–441 (1932).

[Koi75] Koike, M. : On the congruences between Eisenstein series and cusp forms. US-Japan Number Theory Seminar ; Ann Arbor, 1975. Photo-offset notes.

[Koi76] Koike, M. : Congruences between cusp forms of weight one and weight two and a remark on a theorem of Deligne and Serre. International Symposium on Algebraic Number Theory ; Kyoto, 1976.

[Leo58] Leopoldt, H.-W. : Eine Verallgemeinerung der Bernoullischen Zahlen. Abh. Math. Sem. Hamburg 22, 131–140 (1958).

[Li75] Li, W.-C. : Newforms and functional equations. Math. Ann. 212, 285–315 (1975).

[MM] Masley, J. M., Montgomery, H. L. : Cyclotomic fields with unique factorization. Preprint.

[Maz] Mazur, B. : Modular curves and the Eisenstein ideal. In preparation.

[Ray74] Raynaud, M. : Schémas en groupes de type $(p, \ldots, p)$. Bull. Soc. Math. France 102, 241–280 (1974).

[Ser68a] Serre, J.-P. : Une interprétation des congruences relatives à la fonction τ de Ramanujan. Sém. Delange-Pisot-Poitou 1967–68, ex. 14.

[Ser68b] Serre, J.-P. : Abelian l-adic representations and elliptic curves. New York : Benjamin 1968.

[Shi71] Shimura, G. : Introduction to the arithmetic theory of automorphic functions. Publ. Math. Soc. Japan, n° 11, Tokyo-Princeton 1971.

[Shi72] Shimura, G. : Class fields over real quadratic fields and Hecke operators. Ann. of Math. 95, 130–190 (1972).

[Tat67] Tate, J. : Global class field theory. In : Algebraic number theory. Washington : Thompson 1967.

[Yam74] Yamauchi, M. : On the fields generated by certain points of finite order on Shimura's elliptic curves. J. Math. Kyoto Univ. 14, 243–255 (1974).