UNIVERSITÉ CLERMONT AUVERGNE

École doctorale des sciences fondamentales

HABILITATION À DIRIGER DES RECHERCHES

Spécialité : mathématiques
n° d'ordre : 502

CONGRUENCES, FORMES MODULAIRES ET REPRÉSENTATIONS GALOISIENNES

par

Nicolas Billerey

Maître de conférences en mathématiques à l'Université Clermont Auvergne

Soutenue le 3 décembre 2018 devant le jury composé de MM. :

Christophe Delaunay	Université de Franche-Comté	Examinateur
Fred Diamond	King's College London	Rapporteur
Mladen Dimitrov	Université de Lille	Rapporteur
Éric Gaudron	Université Clermont Auvergne	Examinateur
Samir Siksek	University of Warwick	Rapporteur

UNIVERSITÉ CLERMONT AUVERGNE
Laboratoire de Mathématiques Blaise Pascal
UMR 6620 CNRS
Campus des Cézeaux
63178 Aubière cedex
France

Téléphone : +33 (0)4 73 40 76 32
U.R.L : http://math.univ-bpclermont.fr/~billerey/
Courriel : Nicolas.Billerey@uca.fr

Table des matières

Remerciements

J'adresse tout d'abord mes remerciements aux trois rapporteurs de ce mémoire, Fred Diamond, Mladen Dimitrov et Samir Siksek, pour leur lecture attentive de mes résultats. Toutes leurs remarques et appréciations me sont très précieuses. Leurs travaux personnels sont pour moi une source d'inspiration tout autant que d'admiration. Je suis très honoré qu'ils fassent partie de mon jury.

Ce travail doit beaucoup aux encouragements d'Éric Gaudron et à sa bienveillante insistance. Je l'en remercie vivement.

J'apprécie la reconnaissance que Christophe Delaunay m'a témoignée en acceptant de faire partie de mon jury. Avec lui, comme avec l'ensemble des membres du jury, je souhaite que ce mémoire ouvre la voie à des discussions dont je sais qu'elles me seront extrêmement profitables.

Ce manuscrit restitue la plupart des travaux que j'ai effectués depuis mon arrivée à Clermont-Ferrand en 2011. Je suis très heureux de pouvoir remercier ici l'ensemble de mes collègues mathématiciens, informaticiens ou gestionnaires pour leur compétence, leur sympathie et leur disponibilité. Ces travaux n'auraient pas la même saveur sans l'excellente ambiance qui, grâce à eux, règne au sein du laboratoire.

Aux membres de l'équipe de théorie des nombres et notamment à Éric Gaudron, François Martin, Marusia Rebolledo et Emmanuel Royer, je voudrais dire le plaisir que j'ai à échanger avec eux sur nos centres d'intérêts communs.

Le monde est vaste et j'ai la chance de pouvoir travailler avec des chercheurs issus de tous horizons. Je remercie en particulier mon directeur de thèse, Alain Kraus, pour le rôle important qu'il a joué dans ma formation ainsi que Gabor Wiese qui m'a accueilli chaleureusement en post-doctorat à Essen. Les travaux de ce mémoire sont tous issus de collaborations. Je remercie profondément Michael Bennett, Imin Chen, Luis Dieulefait, Nuno Freitas, Ricardo Menares et Filippo Nuccio pour les discussions que nous avons eues ensemble. J'espère vivement qu'elles continueront à porter leurs fruits dans le futur.

En 2014-2015, j'ai bénéficié d'une année de délégation au Pacific Institute for the Mathematical Sciences à Vancouver. Je remercie l'Institut National des Sciences Mathématiques

et de leurs Interactions et la direction du laboratoire (en particulier, Sinnou David et Emmanuel Royer) de la confiance et du soutien qu'ils m'ont accordés. Ce fut une expérience très riche qui m'a permis de tisser des liens forts avec la communauté mathématique à Vancouver. Au delà de mes travaux avec Michael Bennett et Imin Chen présentés dans ce mémoire, j'ai également pu bénéficier, durant mon séjour, de discussions stimulantes avec Christopher Skinner et Vinayak Vatsal.

Il y a beaucoup de façons de faire des mathématiques et j'apprécie toutes les possibilités qui me sont offertes d'échanger et d'apprendre. Je remercie en particulier l'Agence Nationale de la Recherche (via le projet Gardio), la Fédération de Recherche en Mathématiques Rhône-Alpes-Auvergne, le Centre National de la Recherche Scientifique (via notamment son programme « Projet Exploratoire Premier Soutien »), le laboratoire de mathématiques Blaise Pascal et l'Université Clermont Auvergne pour leur soutien en faveur de projets que j'ai portés ou dont j'ai bénéficié. Grâce au site `mathoverflow.net` j'ai pu dialoguer avec des mathématiciens que je ne connaissais pas, obtenir des réponses à mes questions ou découvrir de nouveaux problèmes. C'est passionnant ! J'utilise LMFDB, Magma, PARI/GP ou Sage dans une grande partie de mes travaux pour conjecturer ou confirmer un résultat, explorer une question ou simplement éviter une erreur grossière. Je remercie vivement toutes les personnes investies dans le développement de ces outils pour l'aide précieuse qu'elles m'apportent.

Enfin, pour leur indispensable soutien direct ou indirect, je remercie toute ma famille et en particulier Perrine et nos enfants, Étienne, Suzanne et Sophie.

Chapitre 1

Introduction

Ce mémoire constitue un rapport sur mes travaux de recherche depuis ma thèse de doctorat. Il a pour thème principal la notion de congruence dans la théorie des formes modulaires. Un exemple historique est fourni par la fonction τ de Ramanujan. Celle-ci est définie de la façon suivante. Posons

$$D(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24}, \quad |q|<1.$$

Le coefficient de q^n $(n \geq 1)$ dans le développement en série entière de $D(q)$ est noté $\tau(n)$ de sorte que l'on a

$$D(q) = \sum_{n=1}^{\infty}\tau(n)q^n = q - 24q^2 + 252q^3 - 1472q^4 + \dots.$$

Les entiers $\tau(n)$ $(n \geq 1)$ jouissent de propriétés arithmétiques remarquables héritées du fait que la fonction

$$\Delta(z) = D(e^{2i\pi z}), \quad z \in \mathbf{C},\ \mathrm{im}(z) > 0,$$

est, à un facteur multiplicatif près, l'unique forme modulaire parabolique de poids 12 et de niveau 1. En particulier, τ est multiplicative et pour tout nombre premier p, on a

$$\tau(p^{n+1}) = \tau(p^n)\tau(p) - p^{11}\tau(p^{n-1}), \quad n \geq 1.$$

La fonction τ vérifie de plus certaines congruences [1] modulo $2, 3, 5, 7, 23$ et 691 qui pour un nombre premier p s'énoncent ainsi :

$\tau(p) \equiv 1 + p \pmod 2, \quad (p \neq 2)$;

$\tau(p) \equiv 1 + p \pmod 3, \quad (p \neq 3)$;

1. On renvoie à [Ser69], [SD73] et [Ran77] pour des énoncés plus précis et des références historiques sur la fonction τ.

$$\tau(p) \equiv p + p^2 \pmod 5 \ ;$$
$$\tau(p) \equiv p + p^4 \pmod 7 \ ;$$
$$\tau(p) \equiv \begin{cases} 0 \pmod{23} & \text{si } p \text{ est non résidu quadratique modulo 23,} \\ 2 \pmod{23} & \text{si } p \text{ est de la forme } u^2 + 23v^2, \\ -1 \pmod{23} & \text{si } p \text{ est résidu quadratique modulo 23} \\ & \quad \text{mais n'est pas de la forme } u^2 + 23v^2, \end{cases} \qquad (p \neq 23) \ ;$$
$$\tau(p) \equiv 1 + p^{11} \pmod{691}.$$

À la fin des années 1960, Serre a proposé ([Ser69]) une interprétation, conjecturale, de ces congruences fondée sur l'existence de représentations galoisiennes associées aux formes modulaires, et en particulier à Δ. Son intuition, consolidée par des résultats de Swinnerton-Dyer, a rapidement été confirmée par Deligne [Del71]. Cette découverte a ouvert la voie à d'innombrables travaux qui ont fortement contribué au développement de la géométrie arithmétique depuis lors. C'est dans ce contexte que se situent les résultats présentés dans ce mémoire.

1.1 Principaux rappels et notations

1.1.1 Formes modulaires

Étant donnés un entier $N \geq 1$, un entier $k \geq 2$ et un caractère de Dirichlet χ modulo N, on désigne par $M_k(N, \chi)$ (resp. $S_k(N, \chi)$) le $\mathbf{C}$-espace vectoriel des formes modulaires (resp. paraboliques) de poids k, niveau N et caractère χ sous l'action du groupe $\Gamma_0(N)$. On note

$$M_k(N) = \bigoplus_{\chi \colon (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times} M_k(N, \chi) \quad (\text{resp. } S_k(N) = \bigoplus_{\chi \colon (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times} S_k(N, \chi))$$

l'ensemble de toutes les formes modulaires (resp. paraboliques) de poids k et de niveau N. Lorsque χ est trivial, on note $M_k(\Gamma_0(N))$ (resp. $S_k(\Gamma_0(N))$) l'espace $M_k(N, \chi)$ (resp. $S_k(N, \chi)$) des formes invariantes par $\Gamma_0(N)$.

Soit $f \in M_k(N, \chi)$ une forme modulaire dont le q-développement à l'infini est donné par $f(z) = \sum_{n \geq 0} a_n q^n$ où $q = e^{2i\pi z}$. On dit que f est propre si elle est vecteur propre des opérateurs de Hecke $\{T_n\}_{n \geq 1}$ avec $\mathrm{pgcd}(n, N) = 1$. Si de plus elle vérifie $a_1 = 1$, alors on dit qu'elle est normalisée. Dans ce cas, on a $T_n f = a_n f$ pour tout entier $n \geq 1$ premier à N et l'ensemble $\mathbf{Q}_f = \mathbf{Q}(\{a_n \mid n \geq 1, \mathrm{pgcd}(n, N) = 1\})$ est un corps de nombres appelé corps des coefficients de f. Les valeurs du caractère χ ainsi que les coefficients $\{a_n\}$, avec $n \geq 1$ et $\mathrm{pgcd}(n, N) = 1$, appartiennent à l'anneau des entiers du corps $\mathbf{Q}_f$.

On note $S_k^{\text{new}}(N)$ le $\mathbf{C}$-espace vectoriel des formes primitives de poids k et de niveau N au sens d'Atkin et Lehner. Il existe alors une base de $S_k^{\text{new}}(N)$ constituée de formes modulaires paraboliques, normalisées et propres pour l'ensemble de tous les opérateurs de Hecke appelées formes nouvelles (« newforms » en anglais).

1.1.2 Représentations galoisiennes

On désigne par $\overline{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$ et on munit le groupe $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ de la topologie profinie. Soit l un nombre premier. On note $\overline{\mathbf{F}}_l$ une clôture algébrique du corps $\mathbf{F}_l = \mathbf{Z}/l\mathbf{Z}$ et on munit $\overline{\mathbf{F}}_l$ de la topologie discrète. Tout homomorphisme continu $\varepsilon\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_l^\times$ a pour image un sous-groupe cyclique fini de $\overline{\mathbf{F}}_l^\times$, d'ordre premier à l. En particulier, il se factorise par $(\mathbf{Z}/M\mathbf{Z})^\times$ pour un certain entier $M \geq 1$. Le plus petit entier M satisfaisant à cette propriété est appelé conducteur de ε. Il coïncide avec le conducteur de ε au sens d'Artin ([Ser68, VI §2]).

Inversement, tout homomorphisme de $(\mathbf{Z}/M\mathbf{Z})^\times$ dans $\overline{\mathbf{F}}_l^\times$ avec $M \geq 1$, s'identifie à un homomorphisme continu de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ à valeurs dans $\overline{\mathbf{F}}_l^\times$ en le précomposant par l'application de projection $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})/\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\mu_M)) \simeq (\mathbf{Z}/M\mathbf{Z})^\times$ où μ_M désigne le groupe des racines M-ièmes de l'unité dans $\overline{\mathbf{Q}}$.

On désigne par $\chi_l\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{F}_l^\times$ le caractère cyclotomique modulo l ; c'est le caractère qui donne l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur les racines l-ièmes de l'unité.

Par représentation galoisienne, on entend dans ce mémoire, un homomorphisme continu

$$\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_l)$$

où l'on a muni $\mathrm{GL}_2(\overline{\mathbf{F}}_l)$ de la topologie discrète. L'image d'un tel homomorphisme est un groupe fini, noté G.

À toute représentation galoisienne ρ, Serre associe dans [Ser87, §§1-2] un triplet noté $(N(\rho), k(\rho), \varepsilon(\rho))$ constitué

— d'un entier $N(\rho) \geq 1$ appelé niveau de Serre de la représentation ρ ;

— d'un entier $k(\rho) \geq 2$ appelé poids de Serre de la représentation ρ ;

— d'un caractère $\varepsilon(\rho)\colon (\mathbf{Z}/N(\rho)\mathbf{Z})^\times \to \overline{\mathbf{F}}_l^\times$ appelé caractère de Serre de la représentation ρ.

Rappelons les points clés de sa construction.

L'entier $N(\rho)$ mesure la ramification de ρ hors de l ; c'est la partie première à l du conducteur d'Artin de ρ. En particulier, pour tout nombre premier p, on a l'équivalence suivante :

$$p \text{ divise } N(\rho) \Longleftrightarrow p \neq l \text{ et } \rho \text{ est ramifiée en } p.$$

L'exposant d'un nombre premier p dans la décomposition de $N(\rho)$ est donné par la formule (1.2.2) de [Ser87] ; elle fait appel à la suite des groupes de ramification de G relativement à une extension à $\overline{\mathbf{Q}}$ de la valuation p-adique de $\mathbf{Q}$.

Le déterminant de la représentation ρ est un caractère de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ dont le conducteur divise $lN(\rho)$. Il s'identifie donc à un homomorphisme de $(\mathbf{Z}/lN(\rho)\mathbf{Z})^\times$ à valeurs dans $\overline{\mathbf{F}}_l^\times$. On le décompose alors, de façon unique, en un produit $\det\rho = \varepsilon(\rho)\chi_l^h$ où h est un entier bien défini modulo $l-1$ et $\varepsilon(\rho)\colon (\mathbf{Z}/N(\rho)\mathbf{Z})^\times \to \overline{\mathbf{F}}_l^\times$ est non ramifié en l.

Le poids $k(\rho)$ ne dépend que de la restriction de la représentation ρ à un sous-groupe d'inertie en l. C'est un entier compris entre 2 et l^2-1 dont la définition précise est délicate et fait l'objet du §2 de [Ser87]. Précisions que sa classe modulo $l-1$ est celle de $h+1$, de sorte que la formule précédente s'écrit :

$$\det\rho = \varepsilon(\rho)\chi_l^{k(\rho)-1}.$$

L'action du groupe de Galois absolu de $\mathbf{Q}$ sur l'ensemble des points de torsion d'une courbe elliptique (ou plus généralement d'une variété abélienne de type GL_2 comme on le verra aux chapitres 3 et 5) fournit des exemples importants de représentations galoisiennes. Le théorème suivant, démontré par Eichler et Shimura dans le cas du poids 2 et par Deligne dans le cas général, établit l'existence de représentations galoisiennes associées à certaines formes modulaires. Il est d'une importance capitale dans notre étude.

On identifie $\overline{\mathbf{Q}}$ à un sous-corps de $\mathbf{C}$ et on fixe une place λ de $\overline{\mathbf{Q}}$ au-dessus de l. Cela induit un homomorphisme de réduction $\overline{\mathbf{Z}} \to \overline{\mathbf{F}}_l$ où $\overline{\mathbf{Z}}$ désigne l'anneau des entiers de $\overline{\mathbf{Q}}$.

Théorème 1.1 (Deligne)**.** *Soit f une forme modulaire propre de poids $k \geq 2$, niveau N et caractère χ. On suppose que l'on a $T_n f = a_n f$ pour tout entier $n \geq 2$ premier à N. Il existe alors une représentation galoisienne semi-simple $\rho_{f,\lambda}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_l)$, unique à isomorphisme près, caractérisée par la propriété suivante : pour tout nombre premier $p \nmid Nl$, la représentation $\rho_{f,\lambda}$ est non ramifiée en p et si Frob_p désigne une substitution de Frobenius en p, alors le polynôme caractéristique de $\rho_{f,\lambda}(\mathrm{Frob}_p)$ est l'image de*

$$X^2 - a_p X + \chi(p)l^{k-1} \tag{1.1}$$

dans $\overline{\mathbf{F}}_l[X]$ via l'homomorphisme $\overline{\mathbf{Z}} \to \overline{\mathbf{F}}_l$ associé à la place λ.

On dit qu'une représentation galoisienne $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ est modulaire s'il existe une place λ de $\overline{\mathbf{Q}}$ au-dessus de l et une forme modulaire propre et *parabolique* f telle que ρ est isomorphe à la représentation $\rho_{f,\lambda}$ définie au théorème 1.1. Dans ce cas, on dit également que ρ provient de f.

D'après le théorème de Chebotarev et la relation (1.1), on a $\det(\rho_{f,\lambda}) = \varepsilon\chi_l^{k-1}$ où $\varepsilon\colon (\mathbf{Z}/N\mathbf{Z})^\times \to \overline{\mathbf{F}}_l^\times$ est la composée de χ avec l'homomorphisme de réduction $\overline{\mathbf{Z}} \to \overline{\mathbf{F}}_l$

associé à la place λ. On en déduit ainsi qu'une représentation galoisienne modulaire ρ est nécessairement impaire, c'est-à-dire qu'elle vérifie $\det(\rho(c)) = -1$ où c désigne la conjugaison complexe dans $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Un résultat de Carayol ([Car86]) montre que le conducteur de Serre $N(\rho_{f,\lambda})$ de la représentation $\rho_{f,\lambda}$ divise le niveau N de f. Si $l \nmid N$, on a alors en particulier, $k(\rho_{f,\lambda}) \equiv k \pmod{l-1}$ et $\varepsilon\colon (\mathbf{Z}/N\mathbf{Z})^\times \longrightarrow (\mathbf{Z}/N(\rho_{f,\lambda})\mathbf{Z})^\times \xrightarrow{\varepsilon(\rho_{f,\lambda})} \overline{\mathbf{F}}_l^\times$.

L'essence du théorème de Deligne concerne le cas où f est parabolique. Néanmoins, l'énoncé s'applique également au cas où f est une série d'Eisenstein propre de $M_k(N,\chi)$. Dans ce cas, il existe deux caractères de Dirichlet

$$\chi_1, \chi_2\colon (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$$

de produit égal à χ tels que $a_p = \chi_1(p) + \chi_2(p)p^{k-1}$ pour tout nombre premier $p \nmid N$. On définit alors la représentation galoisienne associée à f et à la place λ par

$$\varepsilon_1 \oplus \varepsilon_2 \chi_l^{k-1}$$

où ε_i $(i = 1, 2)$ est la composée de χ_i avec l'homomorphisme de réduction $\overline{\mathbf{Z}} \to \overline{\mathbf{F}}_l$, vu comme caractère galoisien ([Rib85, p. 28]).

Enfin, supposons $l \nmid N$ et soit $\varepsilon\colon (\mathbf{Z}/N\mathbf{Z})^\times \to \overline{\mathbf{F}}_l^\times$ un caractère galoisien. Il existe alors un unique caractère de Dirichlet $\chi\colon (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$ tel que

$$\widetilde{\chi(x)} = \varepsilon(x), \quad \text{pour tout } x \in (\mathbf{Z}/N\mathbf{Z})^\times$$

où $\widetilde{z}$ désigne l'image de $z \in \overline{\mathbf{Z}}$ dans $\overline{\mathbf{F}}_l$ par l'application de réduction $\overline{\mathbf{Z}} \to \overline{\mathbf{F}}_l$ associée à la place λ. On appelle χ le relèvement multiplicatif de ε (par rapport à λ). Il est de conducteur égal à celui de ε.

1.1.3 Congruences et formes modulaires

Soit $f = \sum_{n\geq 0} a_n q^n$ et $g = \sum_{n\geq 0} b_n q^n$ deux formes modulaires de niveaux respectifs N et N'. On suppose que f et g sont propres et normalisées.

Soit λ une place de $\overline{\mathbf{Q}}$ au-dessus d'un nombre premier l. On dit que f et g sont congrues modulo λ si on a

$$a_n \equiv b_n \pmod{\lambda},$$

pour tout entier $n \geq 1$ tel que $\mathrm{pgcd}(n, lNN') = 1$, i.e. a_n et b_n se réduisent sur le même élément de $\overline{\mathbf{F}}_l$ par l'application $\overline{\mathbf{Z}} \to \overline{\mathbf{F}}_l$ associée à λ. Par multiplicativité des coefficients de Fourier, cela équivaut à dire d'après le théorème 1.1 et le théorème de densité de Chebotarev

que $\rho_{f,\lambda}$ et $\rho_{g,\lambda}$ sont isomorphes ; on écrit alors $\rho_{f,\lambda} \simeq \rho_{g,\lambda}$. Autrement dit, f et g sont congrues modulo λ si et seulement si on a

$$a_p \equiv b_p \pmod{\lambda}$$

pour tout nombre premier p dans un ensemble de nombres premiers de densité 1.

On ne requiert pas ici que les formes f et g soient paraboliques. En l'occurrence une partie substantielle de ce mémoire (section 2.3 et chapitre 4 notamment) est consacrée à la situation où une certaine forme parabolique est congrue à une série d'Eisenstein.

1.2 Organisation du manuscrit et liste des travaux présentés

Plusieurs questions abordées dans ce mémoire visent à généraliser les congruences de la fonction τ de Ramanujan ainsi que les travaux de Serre et Swinnerton-Dyer mentionnés précédemment.

Dans un premier temps, on étudie en détail le défaut d'image « large » des représentations galoisiennes $\rho_{f,\lambda}$ associées à une forme parabolique propre f fixée, supposée sans multiplication complexe. D'après un théorème de Ribet, cela revient à déterminer l'ensemble fini des nombres premiers l pour lesquels la représentation $\rho_{f,\lambda}$ est soit réductible, soit d'image d'ordre premier à l. Lorsque f est de caractère trivial, on donne au chapitre 2 une borne explicite pour un tel nombre premier l en fonction du poids k et du niveau N de f, généralisant ainsi un résultat de Serre et Swinnerton-Dyer ([Ser73], théorème 10 et §3.3).

Au chapitre 3, on s'intéresse aux représentations galoisiennes d'image projective diédrale. On montre, sous certaines hypothèses qu'elles proviennent de formes à multiplication complexe dont on précise le poids, le niveau et le caractère en fonction du type de Serre de la représentation considérée. Appliqué au cas d'une variété abélienne de type GL_2 dont la représentation galoisienne est d'image incluse dans le normalisateur d'un sous-groupe de Cartan non déployé, ce résultat fournit notamment une généralisation d'un théorème de Chen sur les courbes elliptiques.

Le chapitre 4 traite de la modularité des représentations galoisiennes réductibles. Diverses questions, inspirées par le cas irréductible, sont abordées parmi lesquelles l'analogue des conjectures de modularité faible et forte de Serre ou le problème de l'augmentation du niveau. Une application des résultats de ce chapitre est donnée au problème de minorer le plus haut degré des corps de coefficients de formes nouvelles à caractère trivial, de niveau et poids donnés.

On étudie au chapitre 5 plusieurs applications de la méthode modulaire à l'étude de certaines équations diophantiennes, notamment de type Fermat. Les résultats obtenus

exploitent les progrès récents, théoriques et numériques, concernant l'arithmétique des courbes elliptiques sur les corps de nombres, le calcul des formes modulaires de Hilbert ou la résolution des équations de Thue-Mahler.

Enfin, le dernier chapitre détaille quelques pistes de recherches futures inspirées par les travaux présentés dans ce mémoire.

Liste des travaux présentés

[BB17] Michael A. Bennett et Nicolas Billerey : Sums of two S-units via Frey-Hellegouarch curves. *Math. Comp.*, 86(305):1375–1401, 2017.

[BCDF17] Nicolas Billerey, Imin Chen, Luis V. Dieulefait et Nuno Freitas : A result on the equation $x^p + y^p = z^r$ using Frey abelian varieties. *Proc. Amer. Math. Soc.*, 145(10):4111–4117, 2017.

[BCDF] Nicolas Billerey, Imin Chen, Luis V. Dieulefait et Nuno Freitas : A multi-Frey approach to Fermat equations of signature (r, r, p). *Trans. Amer. Math. Soc. (à paraître).*

[BD14] Nicolas Billerey et Luis V. Dieulefait : Explicit large image theorems for modular forms. *J. Lond. Math. Soc. (2)*, 89(2):499–523, 2014.

[BM16] Nicolas Billerey et Ricardo Menares : On the modularity of reducible mod l Galois representations. *Math. Res. Lett.*, 23(1):15–41, 2016.

[BM18] Nicolas Billerey et Ricardo Menares : Strong modularity of reducible Galois representations. *Trans. Amer. Math. Soc.*, 370(2):967–986, 2018.

[BN] Nicolas Billerey et Filippo A. E. Nuccio : Représentations galoisiennes diédrales et formes à multiplication complexe. *J. Théor. Nombres Bordeaux (à paraître).*

Chapitre 2

Théorème d'image large explicite pour les représentations galoisiennes des formes paraboliques

---

Travail présenté

[BD14] Nicolas Billerey et Luis V. Dieulefait : Explicit large image theorems for modular forms. *J. Lond. Math. Soc. (2)*, 89(2):499–523, 2014.

On adopte les notations de l'introduction. Le point de départ de l'étude menée dans ce chapitre est le théorème suivant de Ribet ([Rib85]) dont la démonstration repose notamment sur les résultats de Carayol [Car86].

Théorème 2.1 (Ribet)**.** *Soit f une forme nouvelle (« newform ») sans multiplication complexe. Alors pour presque toute place λ de $\overline{\mathbf{Q}}$ (i.e. toutes sauf un nombre fini), les assertions suivantes sont satisfaites :*

1. *la représentation $\rho_{f,\lambda}$ est irréductible ;*
2. *l'ordre du groupe $\rho_{f,\lambda}(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}))$ est divisible par la caractéristique résiduelle de λ.*

Ce théorème est une généralisation d'un travail antérieur ([Rib75]) de Ribet qui traite du cas où f est de niveau $N = 1$. Celui-ci a lui-même été obtenu à la suite des travaux fondateurs de Serre [Ser73] et Swinnerton-Dyer [SD73] sur le cas $N = 1$ et $\mathbf{Q}_f = \mathbf{Q}$, couvrant notamment le cas de la fonction Δ mentionné dans l'introduction. Dans ce chapitre, on s'attache à rendre effectif ce résultat de Ribet en montrant que la caractéristique résiduelle

d'une place de $\overline{\mathbf{Q}}$ en laquelle l'une des conclusions du théorème 2.1 n'est pas satisfaite est majorée par une borne explicite dépendant uniquement de k et N.

Dans la suite, on fixe une forme nouvelle $f = \sum_{n\geq 1} a_n q^n$ de poids $k \geq 2$ invariante par $\Gamma_0(N)$ où N est un entier ≥ 1. Étant donnée une place λ de $\overline{\mathbf{Q}}$ au-dessus d'un nombre premier l, on note $\mathbf{P}(\rho_{f,\lambda})$ la projectivisation de la représentation $\rho_{f,\lambda}$, c'est-à-dire la composée de $\rho_{f,\lambda}$ avec l'homomorphisme $\mathrm{GL}_2(\overline{\mathbf{F}}_l) \to \mathrm{PGL}_2(\overline{\mathbf{F}}_l)$. On convient de noter $G_{f,\lambda}$ (resp. $\mathbf{P}(G_{f,\lambda})$) l'image de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ par $\rho_{f,\lambda}$ (resp. $\mathbf{P}(\rho_{f,\lambda})$).

Une place λ pour laquelle l'une des conclusions du théorème de Ribet ci-dessus n'est pas satisfaite est dite exceptionnelle. Compte tenu de la classification de Dickson des sous-groupes finis de $\mathrm{PGL}_2(\overline{\mathbf{F}}_l)$ (voir [Hup67, II.8.27]), si λ est exceptionnelle, alors on est dans l'une des situations suivantes :

(i) la représentation $\rho_{f,\lambda}$ est réductible ;

(ii) le groupe $\mathbf{P}(G_{f,\lambda})$ est diédral ;

(iii) le groupe $\mathbf{P}(G_{f,\lambda})$ est isomorphe à l'un des groupes A_4, S_4 ou A_5.

Par ailleurs, si λ n'est pas exceptionnelle, alors le groupe $\mathbf{P}(G_{f,\lambda})$ est isomorphe à l'un des groupes $\mathrm{PGL}_2(\mathbf{F})$ ou $\mathrm{PSL}_2(\mathbf{F})$ où $\mathbf{F}$ est un sous-corps fini de $\overline{\mathbf{F}}_l$. On dit alors que $\rho_{f,\lambda}$ est d'image large.

Dans la suite, on considère une place exceptionnelle λ de caractéristique résiduelle l. Dans chacun des trois cas (i), (ii) et (iii) ci-dessus, on donne une borne explicite pour l en fonction du poids k et du niveau N de f à l'aide d'une majoration ou d'une relation de divisibilité. Lorsque la représentation $\rho_{f,\lambda}$ est réductible (resp. d'image projective diédrale), on montre que la forme f est alors congrue modulo λ à une série d'Eisenstein particulière (resp. à l'une de ses tordues galoisiennes).

2.1 Cas où le groupe $\mathbf{P}(G_{f,\lambda})$ est isomorphe à A_4, S_4 ou A_5

On suppose que l'on a $l \nmid N$ et $l > k$. D'après des résultats de Deligne et Fontaine ([Edi92, p. 567]), l'image d'un sous-groupe d'inertie en l fournit ([BD14, lemma 1.2]) un sous-groupe cyclique d'ordre m de $\mathbf{P}(G_{f,\lambda})$ avec

$$m = \begin{cases} (l-1)/\mathrm{pgcd}(l-1,k-1) & \text{si } f \text{ est ordinaire en } \lambda, \text{ i.e. } a_l \not\equiv 0 \pmod{\lambda} ; \\ (l+1)/\mathrm{pgcd}(l+1,k-1) & \text{si } f \text{ est non ordinaire en } \lambda, \text{ i.e. } a_l \equiv 0 \pmod{\lambda}. \end{cases}$$

Dans le cas (iii) ci-dessus, on en déduit alors le résultat suivant ([BD14, theorem 4.1]).

Théorème 2.2. *Si $\mathbf{P}(G_{f,\lambda})$ est isomorphe à A_4, S_4 ou A_5, alors $l \mid N$ ou $l \leq 4k-3$.*

2.2 Cas où le groupe $\mathbf{P}(G_{f,\lambda})$ est diédral

Dans ce cas, le groupe $\mathbf{P}(G_{f,\lambda})$ est une extension de $\{\pm 1\}$ par un groupe cyclique. On en déduit un homomorphisme quadratique

$$\epsilon_{f,\lambda}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \xrightarrow{\mathbf{P}(\rho_{f,\lambda})} \mathbf{P}(G_{f,\lambda}) \longrightarrow \{\pm 1\}.$$

La proposition suivante ([BD14, proposition 3.3]) décrit la ramification du caractère $\epsilon_{f,\lambda}$. Sa démonstration utilise les résultats de Deligne et Fontaine mentionnés précédemment ainsi que la description locale, dûe à Langlands, de la représentation $\rho_{f,\lambda}$ en un nombre premier p tel que $p \mid N$ mais $p^2 \nmid N$ ([BD14, §1.1]).

Proposition 2.1. *Supposons l impair et $l \nmid N$.*

1. *Si $\epsilon_{f,\lambda}$ est ramifié en un nombre premier $p \neq l$, alors $p^2 \mid N$.*
2. *On suppose de plus $l > k$ et*
   (a) *soit f est ordinaire en λ et $l \neq 2k-1$;*
   (b) *soit f n'est pas ordinaire en λ et $l \neq 2k-3$.*

   Alors, $\epsilon_{f,\lambda}$ est non ramifié en l.

Dans le cas où le niveau N de f est sans facteur carré, on note que la forme f est automatiquement sans multiplication complexe. La proposition 2.1, combinée à un lemme de Dieulefait ([Die15, lemma 3.2]), fournit le théorème suivant qui généralise et précise un résultat de Ribet sur le cas $N = 1$ (voir la remarque après [Rib75, corollary 4.5] et la démonstration du point (ii) p. 264).

Théorème 2.3. *Si le groupe $\mathbf{P}(G_{f,\lambda})$ est diédral et si N est sans facteur carré, alors soit $l \mid N$, soit $l \leq k$, soit $l = 2k-1$.*

Le cas où l'entier N n'est plus supposé sans facteur carré est plus délicat et nécessite de supposer que la forme f est sans multiplication complexe. Dans ce cas, on commence par identifier $\epsilon_{f,\lambda}$ à un caractère de Dirichlet. Lorsque $l > 2k-1$, on montre, à l'aide notamment de la proposition 2.1 ci-dessus, que le conducteur $\mathfrak{c}$ de $\epsilon_{f,\lambda}$ vérifie $\mathfrak{c}^2 \mid 2^4 N$.

On considère dès lors la forme $g = f \otimes \epsilon_{f,\lambda} = \sum_{n\geq 1} b_n q^n$. Par construction, on a $b_n = a_n \epsilon_{f,\lambda}(n)$ quel que soit $n \geq 1$. D'après un résultat de Shimura ([Shi71a, proposition 3.64]), g est une forme modulaire de poids k, niveau $2^4 N$ et caractère trivial. On vérifie alors que f et g sont congrues modulo λ.

En utilisant l'hypothèse que f est sans multiplication complexe, on montre ensuite à l'aide d'un résultat de Murty ([Mur97, theorem 1]) qu'il existe un nombre premier q en

lequel la représentation $\rho_{f,\lambda}$ est non ramifiée tel que

$$a_q \neq 0, \quad \epsilon_{f,\lambda}(q) = -1 \quad \text{et} \quad q \leq 2kN^2 \prod_{p|N} \left(1 + \frac{1}{p}\right),$$

où le produit porte sur les diviseurs premiers p de N.

Enfin nous donnons, avec la congruence $\rho_{f,\lambda} \simeq \rho_{g,\lambda}$ ci-dessus combinée à des résultats de théorie analytique des nombres et aux bornes de Deligne, une majoration explicite pour q en fonction de k et N. Cela fournit le théorème général suivant ([BD14, theorem 3.2]).

Théorème 2.4. *Si le groupe $\mathbf{P}(G_{f,\lambda})$ est diédral et si f est sans multiplication complexe de niveau $N \geq 2$, alors on a*

$$l \leq \left(2\left(8kN^2(1 + \log\log N)\right)^{(k-1)/2}\right)^{[\mathbf{Q}_f:\mathbf{Q}]},$$

où $[\mathbf{Q}_f : \mathbf{Q}]$ désigne le degré du corps de coefficients de f.

Remarque. L'entier $[\mathbf{Q}_f : \mathbf{Q}]$ est majoré par la dimension de l'espace des formes nouvelles de poids k pour $\Gamma_0(N)$. Une formule, ainsi que des estimations asymptotiques, pour cette dimension sont données dans [Mar05].

Dans le chapitre 3, on aborde la question générale de la modularité des représentations galoisiennes d'image projective diédrale. En particulier, on montre sous certaines hypothèses, qu'une telle représentation provient d'une forme à multiplication complexe d'un type (poids, niveau, caractère) bien précis.

2.3 Cas où la représentation $\rho_{f,\lambda}$ est réductible

C'est la situation la plus délicate. Néanmoins, dans certains cas, on peut déduire facilement une majoration satisfaisante pour l à partir de la décomposition de N en produit de facteurs premiers. Pour ce faire, on utilise la classification, obtenue indépendamment par Carayol ([Car89, §§1.2–1.3]) et Livné ([Liv89]), des cas de dégénérescence du conducteur des représentations l-adiques. On rappelle brièvement de quoi il s'agit.

Étant donnés un entier $n \geq 2$ et nombre premier p, on convient de noter $v_p(n)$ la valuation de n en p. D'après un résultat de Carayol ([Car86]) le conducteur de Serre $N(\rho_{f,\lambda})$ de la représentation $\rho_{f,\lambda}$ divise le niveau N de la forme f considérée. On dit alors qu'il y a dégénérescence en un nombre premier $p \neq l$ lorsque $e_p \overset{\text{déf}}{=} v_p(N) - v_p(N(\rho_{f,\lambda})) > 0$. Les cas possibles de dégénérescence sont résumés dans le tableau 2.1. De plus, lorsque $e_p > 0$ et $v_p(N) \geq 2$, on déduit de [Car86, §1.5] que l'on a $p \equiv \pm 1 \pmod{l}$.

Supposons que la représentation $\rho_{f,\lambda}$ est réductible. Elle s'écrit alors $\rho_{f,\lambda} = \nu_1 \oplus \nu_2$ avec $\nu_i \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_l^{\times}$ pour $i = 1, 2$. Chaque caractère ν_i $(i = 1, 2)$ se décompose

$v_p(N)$	$b+1 \geq 2$	1	2
$v_p(N(\rho_{f,\lambda}))$	$b \geq 1$	0	0
e_p	1	1	2

TABLE 2.1 – Classification des cas de dégénérescence

en $\nu_i = \varepsilon_i \chi_l^{a_i}$ où ε_i non ramifié en l et $0 \leq a_i \leq l-2$. Comme f est supposée de caractère trivial, il vient $\varepsilon_2 = \varepsilon_1^{-1}$. On a donc $N(\rho_{f,\lambda}) = \mathfrak{c}^2$ où $\mathfrak{c}$ désigne le conducteur de ε_1 (ou ε_2).

Avec les travaux de Carayol et Livné mentionnés ci-dessus, le résultat que l'on obtient est alors le suivant (voir [BD14], theorem 2.4 et theorem 2.5 (ii)(a)).

Théorème 2.5. *On suppose que la représentation $\rho_{f,\lambda}$ est réductible. Soit $p \neq l$ un nombre premier. On suppose de plus que l'on est dans l'une des situations suivantes :*

1. *$v_p(N) \geq 3$ est impair ;*
2. *$p = 2$ et $v_2(N) = 2$.*

Alors, l divise $p^2 - 1$.

Soit à présent $p \neq l$ un nombre premier tel que $v_p(N) = 1$. D'après ce qui précède, on a $v_p(N(\rho_{f,\lambda})) = 0$ (on rappelle qu'on suppose f de caractère trivial). On est donc dans une situation de dégénérescence, mais les congruences de Carayol utilisées ci-dessus ne s'appliquent plus. Dans ce cas, on peut néanmoins obtenir une borne sur l à partir de la description locale en p de la représentation $\rho_{f,\lambda}$. En effet, celle-ci est non ramifiée en p et Langlands a montré que le polynôme caractéristique de $\rho_{f,\lambda}(\mathrm{Frob}_p)$ est de la forme $(X - a)(X - ap)$ avec $a \in \overline{\mathbf{F}}_l^{\times}$. Par ailleurs, si l'on suppose de plus $l \geq k-1$ et $l \nmid N$, la description locale en l de $\rho_{f,\lambda}$ dûe à Deligne et Fontaine implique, avec les notations précédentes, que l'on a $\{a_1, a_2\} = \{0, k-1\}$. Autrement dit, on a

$$\rho_{f,\lambda} = \varepsilon \oplus \varepsilon^{-1} \chi_l^{k-1},$$

avec $\varepsilon \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_l^{\times}$ de conducteur $\mathfrak{c}$ tel que $N(\rho_{f,\lambda}) = \mathfrak{c}^2$.

À l'aide de ces arguments, on déduit le résultat suivant (voir [BD14], theorem 2.5(ii)(b)) où l'on a posé $c = \max\{d \geq 1;\ d^2 \mid N\}$.

Théorème 2.6. *On suppose que la représentation $\rho_{f,\lambda}$ est réductible. Soit $p \neq l$ un nombre premier tel que $v_p(N) = 1$. Il existe alors un caractère de Dirichlet pair $\eta \colon (\mathbf{Z}/c\mathbf{Z})^{\times} \to \mathbf{C}^{\times}$ tel que*

$$l \text{ divise la norme de } \eta(p)p^k - 1 \text{ ou } \eta(p)p^{k-2} - 1.$$

Remarque. Le caractère η de l'énoncé est le relèvement multiplicatif de ε^{-2} vu comme caractère de Dirichlet modulo c.

Posons $N = mc^2$ où, par construction, l'entier m est sans facteur carré. Les théorèmes 2.5 et 2.6 suffisent à majorer la caractéristique résiduelle d'une place λ en laquelle la représentation $\rho_{f,\lambda}$ est réductible sauf si $\mathrm{pgcd}(m, c) = 1$, $v_2(c) \neq 1$ et si l'on est dans l'une des situations suivantes

1. $m > 1$ et $k = 2$;
2. $m = 1$.

Outre les arguments utilisés précédemment, la stratégie employée pour aborder les cas restants fait de plus apparaître une congruence entre la forme parabolique f et une certaine série d'Eisenstein E dont la construction dépend du poids k et du niveau N de f ([BD14], §§2.3, 2.5 et 2.6). Sous certaines hypothèses (garantissant notamment l'injectivité de l'opérateur Θ de Katz), les théories de Serre et Katz nous permettent d'interpréter cette congruence comme une égalité entre formes modulaires sur $\overline{\mathbf{F}}_l$. Le résultat se déduit alors d'une étude précise du terme constant de E en les différentes pointes de $\Gamma_0(N)$ (*loc. cit.*, §§2.5 et 2.6).

On présente ci-dessous des énoncés permettant de traiter chacun des cas restants. On rappelle que les nombres de Bernoulli associés à un caractère de Dirichlet primitif $\psi\colon (\mathbf{Z}/d\mathbf{Z})^\times \to \mathbf{C}^\times$ sont définis par

$$\sum_{n=1}^{d} \psi(n) \frac{te^{nt}}{e^{dt} - 1} = \sum_{m \geq 0} B_{m,\psi} \frac{t^m}{m!}.$$

Théorème 2.7 ([BD14, theorem 2.5(iii)])**.** *On suppose que $N = c^2$ est un carré et que la représentation $\rho_{f,\lambda}$ est réductible. Alors, l'une des assertions suivantes est satisfaite :*

1. *il existe un nombre premier $p \neq l$ tel que $v_p(N) = 2$ et $p \equiv \pm 1 \pmod{l}$;*
2. *il existe un caractère de Dirichlet primitif pair $\eta_0\colon (\mathbf{Z}/c_0\mathbf{Z})^\times \to \mathbf{C}^\times$ avec $c_0 \mid c$ tel que*
   (a) *soit l divise la norme de $\eta_0(p)p^k - 1$ pour un certain nombre premier p divisant c ;*
   (b) *soit l divise le numérateur de la norme de $B_{k,\eta_0}/2k$.*

Remarque. Le caractère de Dirichlet η_0 de l'énoncé est le caractère primitif associé au relèvement multiplicatif η de ε^{-2}.

Avant d'énoncer le dernier résultat (concernant le poids $k = 2$), on rappelle que si p est un nombre premier tel que $p \mid N$, mais $p^2 \nmid N$, alors on a $a_p = \pm p^{\frac{k}{2}-1}$.

Théorème 2.8 ([BD14, theorems 2.6(ii) et 2.7])**.** *On suppose $k = 2$ et $N = p_1 \cdots p_t c^2$ avec $t \geq 1$, $p_1, \ldots, p_t$ nombres premiers distincts ne divisant pas c et $v_2(c) \neq 1$. Si la représentation $\rho_{f,\lambda}$ est réductible, alors, on est dans l'une des situations suivantes.*

1. *On a $c = 1$ (i.e. N est sans facteur carré) et pour tout $l \nmid 6N$ les assertions suivantes sont satisfaites :*
   (a) *pour tout $1 \leq i \leq t$ tel que $a_{p_i} = -1$, on a $p_i \equiv -1 \pmod{l}$;*
   (b) *on a $(a_{p_1}, \ldots, a_{p_t}) \neq (-1, \ldots, -1)$;*
   (c) *si $(a_{p_1}, \ldots, a_{p_t}) = (+1, \ldots, +1)$, alors l divise l'entier non nul $\prod_{i=1}^{t}(p_i - 1)$.*
2. *On a $c > 1$ et pour tout nombre premier $l \nmid N$, l'une des assertions suivantes est satisfaite :*
   (a) *il existe un nombre premier $p \neq l$ tel que $v_p(N) = 2$ et $p \equiv \pm 1 \pmod{l}$;*
   (b) *il existe un caractère de Dirichlet primitif pair $\eta_0 \colon (\mathbf{Z}/c_0\mathbf{Z})^\times \to \mathbf{C}^\times$ avec $c_0 \mid c$ tel que si $l > 3$, on a*
      i. *soit l divise la norme de $\eta_0(p_i)p_i^2 - 1$ pour un certain entier $1 \leq i \leq t$;*
      ii. *soit l divise la norme de $\eta_0(p)p^2 - 1$ pour un certain premier $p \mid c$;*
      iii. *soit l divise $p_i - 1$ pour un certain entier $1 \leq i \leq t$;*
      iv. *soit l divise le numérateur de la norme de $B_{k,\eta_0}/2k$.*

La première partie du théorème 2.7 (concernant le poids 2 et le niveau sans facteur carré) est due à Ribet et étend partiellement un résultat de Mazur sur le niveau premier ([Maz77, proposition 5.12]). Elle a été publiée par Yoo qui a prolongé les travaux de Ribet ; voir [Yoo13] et [Yoo14]. En raison de la vacuité de l'espace des formes modulaires de poids 2 et de niveau 1, il a été nécessaire, pour démontrer ce résultat, de travailler directement avec des formes modulaires sur $\overline{\mathbf{F}}_l$ ([BD14, §2.5]).

La stratégie de démonstration des théorèmes 2.7 et 2.8 est reprise et développée au chapitre 4 où l'on énonce, sous forme de congruences, des conditions nécessaires et suffisantes permettant de garantir la modularité de certains représentations réductibles.

Chapitre 3

Représentations diédrales et formes à multiplication complexe

---

Travail présenté

[BN] Nicolas Billerey et Filippo A. E. Nuccio : Représentations galoisiennes diédrales et formes à multiplication complexe. *J. Théor. Nombres Bordeaux (à paraître).*

On adopte à nouveau les notations de l'introduction et on dit qu'une représentation galoisienne $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ est diédrale si son image, vue dans $\mathrm{PGL}_2(\overline{\mathbf{F}}_l)$ est isomorphe au groupe diédral D_n d'ordre $2n$ avec $n \geq 3$. Un tel exemple est donné par la représentation $\rho_{\Delta,23}$ associée à Δ, l'unique forme parabolique de poids 12 et niveau 1 et au nombre premier $l = 23$; d'après [Ser69, §3.4(b)], elle est d'image projective isomorphe à D_3.

On rappelle par ailleurs qu'une forme nouvelle $g = \sum_{n\geq 1} c_n q^n$ est dite à multiplication complexe s'il existe un caractère de Dirichlet non trivial ν tel que pour tout p dans un ensemble de nombres premiers de densité 1, on a $c_p = \nu(p)c_p$. On montre alors que le corps F correspondant au noyau de ν est quadratique imaginaire et on dit aussi que g a multiplication complexe par ν ou par F ([Rib77, pp. 40-42]).

Les représentations galoisiennes attachées aux formes à multiplication complexe sont, en général, diédrales. Par ailleurs, c'est un cas particulier de la célèbre conjecture de modularité de Serre (qui était connu longtemps avant la démonstration générale de Khare–Wintenberger) qu'une représentation diédrale impaire provient d'une forme modulaire de poids ≥ 2. On trouve une preuve moderne de ce résultat dans [Wie04], optimale par rapport au poids et au niveau, mais qui ne fournit pas de renseignement sur la nature de la

forme modulaire correspondante. La construction d'une telle forme de poids ≥ 2 est aussi esquissée dans [DS74], en combinant l'exemple p. 517 avec les §§6.9 et 6.10 ; là encore, rien ne justifie qu'elle soit à multiplication complexe.

Dans ce chapitre, on s'intéresse à la question plus précise de déterminer si une représentation galoisienne diédrale ρ donnée provient d'une forme modulaire *à multiplication complexe de poids* $k(\rho)$, où $k(\rho)$ désigne le poids de Serre de la représentation ρ. Dans ce cas, on souhaite également déterminer, en fonction de $N(\rho)$, le niveau minimal de la forme correspondante.

3.1 Historique et résultats principaux

Cette question a été abordée dans un premier temps par Chen qui considère le cas où $\rho = \rho_{E,l}$ est la représentation associée aux points de l-torsion d'une courbe elliptique E. Le résultat suivant combine les théorèmes 1.6 et 1.7 de [Che02].

Théorème 3.1 (Chen)**.** *Soit E une courbe elliptique (modulaire) définie sur $\mathbf{Q}$ de conducteur N_E et soit l un nombre premier tel que $l > 3$ et $l \nmid N_E$. On suppose que la représentation $\rho_{E,l}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_l)$ est d'image incluse dans le normalisateur d'un sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbf{F}_l)$. Alors, $\rho_{E,l}$ provient d'une forme modulaire à multiplication complexe g de poids 2 et de niveau $N(\rho_{E,l}) \mid N_E$. Si, de plus, on a $16 \nmid N_E$, alors g peut être choisie de caractère trivial.*

Dans la démonstration de Chen, la modularité de E (démontrée en toute généralité par Breuil, Conrad, Diamond et Taylor [BCDT01] pendant la rédaction de l'article de Chen) n'intervient pas ; mais l'auteur met en évidence une congruence entre la forme nouvelle f_E associée à E et la forme à multiplication complexe g.

De même, pour la première partie de son résultat (qui correspond au théorème 1.6 de [Che02]), seules certaines propriétés classiques de la représentation $\rho_{E,l}$ sont utilisées (comme la formule $\det \rho_{E,l} = \chi_l$ ou la description locale de $\rho_{E,l}$ en l). La démonstration de la dernière partie concernant la précision apportée au caractère de la forme g fait en revanche intervenir des propriétés plus fines de E (*loc. cit.* théorème 1.7 et §5).

Ces remarques conduisent donc naturellement à considérer la question ci-dessus dans son cadre général. Une première réponse, partielle, est donnée par le résultat suivant de Nualart ([Nua11, theorem 1]) où, pour une représentation ρ d'image projective D_n donnée, on note K le sous-corps quadratique de $\overline{\mathbf{Q}}$ laissé fixe par le noyau du caractère

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \xrightarrow{\mathbf{P}\rho} D_n \longrightarrow D_n/C_n \simeq \{\pm 1\}$$

avec C_n l'unique sous-groupe cyclique d'ordre n de D_n et $\mathbf{P}\rho$ la composée de ρ avec la projection $\mathrm{GL}_2(\overline{\mathbf{F}}_l) \to \mathrm{PGL}_2(\overline{\mathbf{F}}_l)$.

Théorème 3.2 (Nualart). *Soit $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$, avec $l \geq 5$, une représentation galoisienne diédrale de poids de Serre $k(\rho) = 2$ et de caractère $\varepsilon(\rho)$ trivial telle que le corps K est quadratique imaginaire. Alors, ρ provient d'une forme à multiplication complexe de poids 2, niveau $N(\rho)$ et caractère trivial.*

L'énoncé que l'on obtient est une généralisation du résultat de Nualart aux représentations diédrales de poids de Serre ≥ 2.

Théorème 3.3 ([BN, théorème 1.1]). *Soit ρ une représentation galoisienne diédrale. Avec les notations précédentes, on suppose que le corps quadratique K est imaginaire et que les inégalités $2 \leq k(\rho) \leq l-1$ et $l \geq 5$ sont vérifiées.*

Alors, ρ est modulaire et provient d'une forme nouvelle à multiplication complexe g par le corps K, de poids $k(\rho)$ et de niveau divisant

$$\begin{cases} N(\rho) & \text{si } l \text{ est non ramifié dans } K \\ l^2 N(\rho) & \text{si } l \text{ est ramifié dans } K. \end{cases}$$

De plus, on a les propriétés suivantes :

1. *si l est ramifié dans K, alors $l \in \{2k(\rho)-1,\ 2k(\rho)-3\}$;*
2. *si $\varepsilon(\rho)$ est trivial, alors la forme g peut être choisie de caractère trivial.*

Remarque. Le résultat ci-dessus est optimal par rapport au niveau. En effet, d'une part si ρ provient d'une forme g, alors celle-ci est de niveau divisible par $N(\rho)$ d'après un résultat de Carayol ([Car86]). Par ailleurs, l'exemple de la représentation galoisienne associée à la forme Δ et au nombre premier $l = 23$ montre qu'on ne peut pas abaisser le niveau de la forme à multiplication complexe dans le cas où K est ramifié en l.

La démonstration du théorème 3.3 suit globalement la même stratégie que celle employée par Chen et Nualart, mais fait néanmoins apparaître de nouvelles difficultés. Celles-ci sont notamment liées à la possible ramification de l dans K contrairement au cas du poids 2 où cette situation ne se produit pas pour $l \geq 5$ d'après un résultat de Ribet (voir [Nua11, proposition 4] ou [Rib97, p. 280]). On explique ci-dessous les grandes lignes de la preuve.

On considère une représentation diédrale $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$. On identifie $\overline{\mathbf{Q}}$ à un sous-corps de $\mathbf{C}$ et on fixe un plongement $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_l$ où $\overline{\mathbf{Q}}_l$ désigne une clôture algébrique de $\mathbf{Q}_l$ de corps résiduel $\overline{\mathbf{F}}_l$. Cela induit une place de $\overline{\mathbf{Q}}$ au-dessus de l notée λ.

Avec les notations de l'énoncé, il existe un caractère $\varphi\colon \mathrm{Gal}(\overline{\mathbf{Q}}/K) \to \overline{\mathbf{F}}_l^{\times}$ tel que $\rho = \mathrm{Ind}_{\mathrm{Gal}(\overline{\mathbf{Q}}/K)}^{\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})}(\varphi)$. Une première étape de la démonstration du théorème 3.3 consiste à étudier précisément la ramification en λ du corps K et du caractère φ. C'est l'objet de la proposition 3.2 de [BN].

La théorie du corps de classes globale nous permet d'identifier (le relèvement multiplicatif par rapport à la place λ de) φ à un caractère d'image finie $\alpha\colon \mathbf{A}_K^\times \to \mathbf{C}^\times$ où $\mathbf{A}_K^\times$ désigne les idèles de K.

À l'aide de la proposition 2.1 de *loc. cit.* on construit alors un Größencharakter δ de K aux propriétés bien spécifiques. Il est en particulier de type à l'infini $k(\rho)-1$ et de même réduction que α aux places de bonne réduction $\neq \lambda$. Notons $\mathfrak{f}_\delta$ son conducteur et $-D$ le discriminant du corps quadratique imaginaire K. Le caractère δ s'identifie à un homomorphisme $J(\mathfrak{f}_\delta) \to \mathbf{C}^\times$ où $J(\mathfrak{f}_\delta)$ désigne le groupe des idéaux fractionnaires de K premiers à $\mathfrak{f}_\delta$. On pose alors

$$g_\delta(z) = \sum_{\mathfrak{a}} \delta(\mathfrak{a}) q^{\mathrm{N}_{K/\mathbf{Q}}(\mathfrak{a})}, \quad \text{avec } q = e^{2i\pi z},$$

où $\mathfrak{a}$ parcourt les idéaux entiers de K premiers à $\mathfrak{f}_\delta$. Par un résultat de Hecke, précisé par Shimura (voir [Hec59, p. 717] ainsi que [Shi71b, lemma 3] et [Shi72, p. 138]), la série g_δ est une forme nouvelle de poids $k(\rho)$ et de niveau $M = \mathrm{N}_{K/\mathbf{Q}}(\mathfrak{f}_\delta)D$ à multiplication complexe par K (*loc. cit.* théorème 3.5). Le reste de la démonstration consiste à exprimer le niveau de la forme g_δ en fonction de l et $N(\rho)$ dans chacun des cas de la proposition 3.2 de [BN] mentionnée ci-dessus. On s'assure enfin que la représentation ρ provient bien de g_δ ([BN, §3.4]).

La dernière assertion, portant sur le caractère de la forme à multiplication g de l'énoncé lorsque $\varepsilon(\rho)$ est trivial, résulte d'une étude minutieuse du caractère de g_δ ([BN, lemme 3.7]). Dans ce cas, on montre alors que g peut-être choisie parmi les tordues galoisiennes de g_δ (fin du §3.4 de *loc. cit.*).

3.2 Application aux variétés abéliennes de type GL_2

Soit $A/\mathbf{Q}$ une variété abélienne simple. On note $\mathrm{End}_{\mathbf{Q}}(A)$ l'anneau de ses endomorphismes définis sur $\mathbf{Q}$. Suivant une terminologie de Ribet, on dit que A est de type GL_2 si $E = \mathrm{End}_{\mathbf{Q}}(A) \otimes \mathbf{Q}$ est un corps de nombres de degré $\dim(A)$. Pour toute place finie λ de E au-dessus de l de corps résiduel $\mathbf{F}_\lambda$, on note alors

$$\rho_{A,\lambda}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathbf{F}_\lambda)$$

la représentation donnant l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur $A[\lambda]$ (voir [Rib04, page 247]). Le corollaire suivant au théorème 3.3 ci-dessus généralise [Che02, theorem 1.6] et justifie [GP12, remark 4.4].

Corollaire 3.1 ([BN, corollaire 1.3])**.** *Soit $A/\mathbf{Q}$ une variété abélienne de type GL_2 de conducteur N_A et λ une place finie de $E = \mathrm{End}_{\mathbf{Q}}(A)\otimes\mathbf{Q}$ au-dessus de l. On suppose $l \geq 5$,*

$l \nmid N_A$ et l'image de $\rho_{A,\lambda}$ contenue dans le normalisateur d'un sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbf{F}_\lambda)$. Alors, $\rho_{A,\lambda}$ provient d'une forme nouvelle à multiplication complexe de poids 2 et de niveau $N(\rho_{A,\lambda})$ qui, de plus, est de caractère trivial lorsque $\dim(A) = 1$ (i.e. A est une courbe elliptique) ou lorsque E est totalement réel et A a tous ses endomorphismes définis sur $\mathbf{Q}$.

Remarque. Sous les hypothèses de l'énoncé, on montre que l'on a $k(\rho_{A,\lambda}) = 2$. De plus, si $\dim(A) = 1$ (ou si E est totalement réel et A a tous ses endomorphismes définis sur $\mathbf{Q}$, d'après [Rib04, lemma 3.1]), on a $\det(\rho_{A,\lambda}) = \chi_l$.

Chapitre 4

Modularité des représentations galoisiennes réductibles

Travaux présentés

[BM16] Nicolas Billerey et Ricardo Menares : On the modularity of reducible mod l Galois representations. *Math. Res. Lett.*, 23(1):15–41, 2016.

[BM18] Nicolas Billerey et Ricardo Menares : Strong modularity of reducible Galois representations. *Trans. Amer. Math. Soc.*, 370(2):967–986, 2018.

Les congruences entre formes modulaires paraboliques et séries d'Eisenstein interviennent dans plusieurs résultats très importants de géométrie arithmétique, comme par exemple l'étude par Mazur des points rationnels des courbes modulaires $X_0(N)$ ([Maz77]) ou la construction par Ribet ([Rib76]) de p-extensions abéliennes non ramifiées du corps cyclotomique $\mathbf{Q}(e^{2i\pi/p})$ avec p premier (voir à ce propos le texte de Mazur [Maz11]).

Dans ce chapitre, on reformule ces congruences en termes de représentations galoisiennes. Cela nous amène à considérer les questions fondamentales abordées dans le cas irréductible et notamment :

1. la conjecture de modularité « faible » [Ser87, (3.2.3?)] de Serre ;
2. la conjecture de modularité « forte » [Ser87, (3.2.4?)] de Serre ;
3. le problème de l'augmentation du niveau.

La conjecture de modularité forte a été démontrée en 2005 par Khare et Wintenberger ([KW09a, KW09b] ; voir également [Die09] pour le cas du niveau 1) à la suite de travaux de

très nombreux mathématiciens. Auparavant, Ribet ([Rib90]) avait prouvé la « conjecture ϵ » de Serre qui stipulait que la forme faible de la conjecture de modularité entraîne la forme forte, autrement dit que ces deux énoncés sont équivalents. Son résultat, dit d'abaissement du niveau, est une étape cruciale dans la démonstration du dernier théorème de Fermat par Wiles. Enfin, le problème de l'augmentation du niveau a été résolu par Diamond et Taylor ([DT94]) après des travaux précurseurs de Ribet ([Rib84]).

Dans les sections qui suivent, on interroge tour à tour la validité des énoncés mentionnés ci-dessus dans le cadre des représentations galoisiennes réductibles et semi-simples, i.e. somme de deux caractères.

4.1 Modularité faible

Soit l un nombre premier. On rappelle qu'une représentation $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ est dite modulaire s'il existe une place λ de $\overline{\mathbf{Q}}$ au-dessus de l et une forme modulaire propre et *parabolique* f telle que ρ est isomorphe à la représentation $\rho_{f,\lambda}$ définie au théorème 1.1. Par construction, la représentation $\rho_{f,\lambda}$ est semi-simple et impaire. Il s'agit donc là de deux conditions nécessairement satisfaites par toute représentation modulaire.

Le résultat que l'on démontre est l'exact analogue, dans le cas réductible, de l'énoncé $(3.2.3_?)$ de [Ser87] concernant les représentations irréductibles. Il affirme que ces conditions nécessaires sont également suffisantes.

Théorème 4.1 ([BM16, theorem 2.1])**.** *Toute représentation galoisienne impaire qui est somme directe de deux caractères est modulaire.*

La démonstration du théorème 4.1, d'une difficulté sans commune mesure avec celle de [Ser87, $(3.2.3_?)$], est totalement explicite ; en particulier, on précise le poids, le niveau et le caractère de la forme parabolique associée. On décrit cette construction dans le cas particulier, mais important, où la représentation considérée s'écrit $\rho = \mathbf{1} \oplus \varepsilon\chi_l^b$ où $\mathbf{1}$ désigne le caractère trivial, ε est non ramifié en l et b est un entier compris entre 0 et $l-2$. La condition de parité s'énonce alors $\varepsilon(-1) = (-1)^{b+1}$.

Soit λ une place de $\overline{\mathbf{Q}}$ au-dessus de l. On désigne par N le conducteur de ε. Soit χ le relèvement multiplicatif de ε par rapport à λ que l'on identifie à un caractère de Dirichlet de conducteur N (voir §1.1.2). On a $\chi(-1) = (-1)^{b+1}$ sauf si $l = 2$, auquel cas on a $\chi(-1) = 1$.

On définit alors un entier $k \geq 3$ de la façon suivante :

$$k = \begin{cases} 4 & \text{si } b = 0 \text{ et } l = 2 \text{ ;} \\ l & \text{si } b = 0 \text{ et } l \geq 3 \text{ ;} \\ l+1 & \text{si } b = 1 \text{ ;} \\ b+1 & \text{si } b \geq 2. \end{cases}$$

On note que l'on a $\chi(-1) = (-1)^k$ et $k - 1 \equiv b \pmod{l-1}$, de sorte que $\rho \simeq \mathbf{1} \oplus \varepsilon\chi_l^{k-1}$.

L'énoncé ci-dessous est une version explicite du théorème 4.1 dans ce cas-là. Sa démonstration nécessite un calcul précis du terme constant d'une certaine série d'Eisenstein en chaque pointe de la courbe modulaire ([BM16, proposition 1.2]) et l'emploi d'un lemme de relèvement dû à Deligne et Serre ([DS74, lemme 6.11]).

Théorème 4.2 ([BM16, theorem 2.3])**.** *On conserve les notations ci-dessus. La représentation $\mathbf{1} \oplus \varepsilon\chi_l^b$ provient d'une forme propre et parabolique $f \in S_k(Np, \chi)$ pour tout nombre premier $p \nmid Nl$ tel que λ divise le nombre algébrique non nul $\frac{B_{k,\chi}}{2k}\left(\chi(p)p^k - 1\right)$.*

Remarque. La non nullité de $B_{k,\chi}$ résulte de la relation $\chi(-1) = (-1)^k$.

Dans [BM16], on indiquait que le théorème 4.1 était sans doute connu, mais que nous n'en avions pas trouvé de démonstration écrite dans la littérature. Après la publication de notre résultat, nous avons cependant pris connaissance du travail de Ghitza [Ghi06] qui offre une démonstration, totalement différente de la nôtre, du théorème 4.2 (*loc. cit.* theorem 1). Notre choix pour le poids k tend à s'approcher de la définition du poids « optimal » donnée par Edixhoven dans [Edi92] (pour la représentation $\rho = \mathbf{1} \oplus \varepsilon\chi_l^b$, le poids optimal est $b + 1$) tout en évitant les poids 1 et 2 en lesquels la construction et la manipulation des séries d'Eisenstein sont plus compliquées. Le poids utilisé par Ghitza n'est en revanche pas optimal. À l'opposé, son résultat garantit que la forme parabolique obtenue est de niveau N, ce qui n'est pas le cas avec notre énoncé.

À titre d'exemple, on peut comparer [1] nos deux résultats sur le cas considéré dans l'exemple 1 de [Ghi06] où $\rho = \mathbf{1} \oplus \chi_5^3$ est la représentation modulo 5 associée à la série d'Eisenstein, propre et normalisée, de poids 4 et de niveau 1 donnée par

$$E_4(z) = \frac{1}{240} + \sum_{n \geq 1} \left(\sum_{0 < m \mid n} m^3 \right) q^n, \quad \text{avec } q = e^{2i\pi z}.$$

Il existe une unique forme nouvelle f de poids 24 et de niveau 1. Les premiers termes de son q-développement sont donnés par

$$f(z) = q + (-24y + 552)q^2 + (1152y + 169164)q^3 + (-25920y + 12676288)q^4 + (360960y + 36354030)q^5 + (-3451680y - 903110688)q^6 + (23659776y - 691422088)q^7 + \cdots$$

où y est une racine complexe du polynôme $X^2 - X - 36042$. On note $K = \mathbf{Q}(y)$ le corps quadratique engendré par y et $\mathcal{O}_K$ son anneau d'entiers. Soit λ une place de $\overline{\mathbf{Q}}$ au-dessus de

1. L'ensemble des calculs de cette section a été mené avec PARI-GP [PAR18].

l'idéal premier (de norme 5) engendré par 5 et $y-2$ dans $\mathcal{O}_K$. Le résultat de Ghitza fournit alors une congruence modulo λ entre f et la série E_4 ; autrement dit, on a [2] $\rho_{f,\lambda} \simeq \mathbf{1} \oplus \chi_5^3$.

Par ailleurs, soit à présent λ une place (quelconque) de $\overline{\mathbf{Q}}$ au-dessus de 5. Si $p \neq 5$ est un nombre premier, alors λ divise le nombre algébrique $\frac{B_4}{8}(p^4-1) = -\frac{1}{240}(p^4-1)$ si et seulement si on a $p^4 \equiv 1 \pmod{25}$. Ainsi, pour tout nombre premier $p \equiv 1, 7, 18$ ou $24 \pmod{25}$, le théorème 4.2 garantit l'existence d'une forme parabolique $f \in S_4(\Gamma_0(p))$, propre et normalisée, telle que $\rho_{f,\lambda} \simeq \mathbf{1} \oplus \chi_5^3$. Par exemple, l'unique forme nouvelle ([LMF13, 7.4.1.a])

$$f(z) = q - q^2 - 2q^3 - 7q^4 + 16q^5 + 2q^6 - 7q^7 + 15q^8 - 23q^9 - 16q^{10} - 8q^{11} + \dots$$

de $S_4(\Gamma_0(7))$ vérifie $\rho_{f,\lambda} \simeq \mathbf{1} \oplus \chi_5^3$. Il en est de même pour $f \in S_4^{\mathrm{new}}(\Gamma_0(43))$ telle que $\mathbf{Q}_f$ est le corps de nombres engendré par une racine y de $X^6 - 32X^4 - 16X^3 + 251X^2 + 276X + 60$ vérifiant $y - 2 \in \lambda$.

4.2 Modularité forte

La lettre l désigne toujours un nombre premier. Soit $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ une représentation galoisienne. On convient de dire que ρ est fortement modulaire s'il existe une place λ de $\overline{\mathbf{Q}}$ au-dessus de l et une forme modulaire parabolique f, propre et normalisée, de poids $k(\rho)$, niveau $N(\rho)$ et caractère χ, où χ désigne le relèvement multiplicatif de $\varepsilon(\rho)$ par rapport à la place λ (voir §1.1.2), tels que l'on a $\rho \simeq \rho_{f,\lambda}$. Dans ce cas, une telle forme f est nouvelle. Cela résulte d'un résultat de Carayol ([Car86]).

Avec cette terminologie, le théorème de Khare et Wintenberger affirme que toute représentation irréductible et impaire $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ avec $l \geq 5$ est fortement modulaire (le résultat s'applique encore pour $l = 2$ et $l = 3$ à condition d'exclure certaines représentations diédrales ou d'autoriser un caractère d'ordre non premier à l ; voir [Rib94, p. 641] ou [Dia95]).

Le théorème 4.1 ci-dessus nous garantit la modularité de toute représentation galoisienne réductible et semi-simple (i.e. somme directe de deux caractères) impaire. En revanche, une telle représentation n'est pas nécessairement fortement modulaire. Pour s'en convaincre, il suffit par exemple de considérer la représentation $\mathbf{1} \oplus \chi_l$ qui est de niveau 1 et de poids 2. Dans cette section, on énonce un critère nécessaire et suffisant garantissant, sous certaines conditions, qu'une représentation réductible et semi-simple est fortement modulaire.

2. D'après [Stu87, theorem 1], si $f = \sum_{n\geq 1} a_n q^n$, pour obtenir une vérification numérique rigoureuse de cet isomorphisme, il suffit de montrer que pour tout nombre premier $p \neq 5$, $p \leq 60$, on a la congruence $a_p \equiv 1 + p^3 \pmod{\lambda}$.

Un tel résultat est connu lorsque la représentation considérée est de conducteur 1 (voir [Rib75, lemma 5.2]). Dans ce cas, le critère affirme que la représentation $\mathbf{1} \oplus \chi_l^{k-1}$ (avec $k \geq 2$ pair et $l > k+1$) est fortement modulaire si et seulement si l divise le numérateur du k-ième nombre de Bernoulli (classique) B_k. Notre critère est une généralisation de ce résultat de Ribet. Avant de l'énoncer, on commence par introduire un peu de terminologie. Soit η un caractère galoisien non ramifié en l. Pour tout entier $k \geq 2$ tel que $l > k+1$, on construit dans [BM18, §1.2] un élément $B_{k,\eta}$ de $\overline{\mathbf{F}}_l$ appelé k-ième nombre de Bernoulli associé à η. Lorsque η est trivial, $B_{k,\eta}$ n'est rien d'autre que l'image du k-ième nombre de Bernoulli B_k dans $\overline{\mathbf{F}}_l$, bien définie d'après un résultat classique de Von Staudt et Clausen. Dans le cas général, la construction de $B_{k,\eta}$ repose sur des résultats analogues de Carlitz [Car59a, Car59b] pour les nombres de Bernoulli généralisés. On identifie enfin η à un caractère de $(\mathbf{Z}/\mathfrak{c}\mathbf{Z})^\times$ à valeurs dans $\overline{\mathbf{F}}_l^\times$ où $\mathfrak{c}$ désigne le conducteur de η et on pose $\eta(p) = 0$ pour tout nombre premier p en lequel η est ramifié.

Théorème 4.3 ([BM18, theorem 1])**.** *Soit $\nu_1, \nu_2 \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_l^\times$ deux caractères définissant une représentation galoisienne $\rho = \nu_1 \oplus \nu_2$ impaire de conducteur $N = N(\rho)$. On suppose que l'on a $l > k+1$ avec $k = k(\rho)$. Alors, il existe $\varepsilon_1, \varepsilon_2 \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_l^\times$ non ramifiés en l tels que $\rho = \varepsilon_1 \oplus \varepsilon_2 \chi_l^{k-1}$. Posons $\eta = \varepsilon_1^{-1}\varepsilon_2$. La représentation ρ est fortement modulaire si et seulement si on a*

$$B_{k,\eta} = 0 \quad \textit{ou} \quad \eta(p)p^k = 1 \textit{ pour un certain diviseur premier } p \textit{ de } N.$$

La première partie du théorème résulte de la définition du poids de Serre et des hypothèses de l'énoncé. Lorsque $\rho = \varepsilon_1 \oplus \varepsilon_2 \chi_l^{k-1}$ est fortement modulaire, i.e. $\rho \simeq \rho_{f,\lambda}$ avec $f = \sum_{n \geq 1} a_n q^n$ du type souhaité, on montre notamment que l'on a

$$\varepsilon_1(p) + \varepsilon_2(p)p^{k-1} = a_p \pmod{\lambda}, \quad \text{pour tout nombre premier } p \neq l.$$

La vérification, à la proposition 3.2 de [BM18], de cette relation pour les nombres premiers p divisant N constitue la principale difficulté de la démonstration du théorème 4.3. Elle repose sur la correspondance de Langlands locale et sur l'étude comparée de l'action de l'opérateur de Hecke en p sur f et sa représentation automorphe associée (*loc. cit.*, section 2). Les conditions de l'énoncé se déduisent alors du calcul précis du coefficient constant du q-développement en toute pointe des séries d'Eisenstein propres et normalisées de poids ≥ 2 et niveau quelconque (*loc. cit.*, proposition 4).

D'après les congruences de l'introduction, la représentation associée à la fonction $\Delta \in S_{12}(1)$ et au nombre premier $l = 691$ est réductible et vaut $\rho_{\Delta,l} = \mathbf{1} \oplus \chi_l^{11}$. En particulier, cette dernière représentation est donc fortement modulaire ; cela résulte du fait bien connu

que le numérateur du nombre de Bernoulli B_{12} est divisible par 691. Dans d'autres situations cependant, la modularité forte d'une représentation résulte de la seconde condition du théorème 4.3. On présente un exemple concret ci-dessous.

Notons $\varepsilon_1 \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{F}_{41}^\times$ l'unique caractère de conducteur 3 tel que $\varepsilon_1(2) = -1$ (autrement dit, ε_1 est la réduction modulo 41 du symbole de Kronecker $\left(\frac{-3}{\cdot}\right)$, vu comme caractère de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$). De même, soit $\eta \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{F}_{41}^\times$ l'unique caractère de conducteur 5 tel que $\eta(2) = -1$ (c'est la réduction de $\left(\frac{5}{\cdot}\right)$ modulo 41). On vérifie alors avec SAGE [SD18] que $B_{4,\eta} = -8 \pmod{41}$ est non nul dans $\mathbf{F}_{41}$, mais que l'on a $\eta(3)3^4 = 1 \pmod{41}$. Ainsi, d'après le théorème 4.3, la représentation $\rho = \varepsilon_1 \oplus \varepsilon_1\eta\chi_{41}^3$ est fortement modulaire.

Pour s'en assurer, on calcule à l'aide de la commande `mf=mfinit([45,4,5],0)` de PARI-GP l'espace $S_4^{\mathrm{new}}(45, \chi)$ des formes nouvelles de poids 4, niveau 45 et de caractère χ, extension du symbole de Kronecker $\left(\frac{5}{\cdot}\right)$ à $(\mathbf{Z}/45\mathbf{Z})^\times$. L'espace $S_4^{\mathrm{new}}(45, \chi)$ est de dimension 6 et engendré par les orbites galoisiennes de deux formes nouvelles. Soit f celle dont le corps des coefficients est de degré 4. Elle est donnée par la commande `mfeigenbasis(mf)[2]` et admet un développement à l'infini dont les premiers termes sont

$$f(z) = q + \left(-\frac{1}{10}y^3 - \frac{1}{10}y\right)q^2 + (3y^2+27)q^4 + \left(-\frac{1}{2}y^3 + 3y^2 - \frac{13}{2}y + 30\right)q^5 + \left(\frac{3}{5}y^3 + \frac{63}{5}y\right)q^7 + \left(\frac{5}{2}y^3 + \frac{53}{2}y\right)q^8 + (3y^3 + 3y^2 + 27y + 35)q^{10} + \cdots$$

avec $y^4 + 21y^2 + 100 = 0$. Si λ est une place de $\overline{\mathbf{Q}}$ au-dessus de l'idéal engendré par 41 et $y + 16$ dans l'anneau des entiers de $\mathbf{Q}(y)$, on vérifie [3] alors que l'on a $\rho_{f,\lambda} \simeq \varepsilon_1 \oplus \varepsilon_1\eta\chi_{41}^3$.

4.3 Le problème de l'augmentation du niveau

Soit $\rho \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ une représentation galoisienne. Le problème de l'augmentation du niveau pour ρ s'attache à décrire, un entier $k \geq 2$ étant donné, l'ensemble des entiers $M \geq 1$ premiers à l pour lesquels il existe une forme *nouvelle* $g \in S_k(M)$ et une place λ de $\overline{\mathbf{Q}}$ au-dessus de l tels que $\rho \simeq \rho_{g,\lambda}$. Un tel entier M est nécessairement divisible par $N(\rho)$, justifiant ainsi la terminologie. On dit qu'il s'agit d'un niveau de ρ (ou encore que ρ apparaît en niveau M et poids k). Suivant Diamond et Taylor ([DT94]), lorsque $M = N(\rho)$ (resp. $M \neq N(\rho)$), on parle de niveau optimal (resp. non optimal). On insiste sur le fait qu'on requiert que la forme g ci-dessus soit *nouvelle*.

La proposition suivante se déduit de la classification des cas de dégénérescence des conducteurs des représentations l-adiques mentionnée à la section 2.3.

3. D'après la commande `mfsturm(mf)`, il suffit d'évaluer les neuf premiers coefficients de f modulo λ.

Proposition 4.1. *Soit* $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ *une représentation galoisienne. On suppose que* ρ *provient d'une forme nouvelle* f *de poids* k *et de niveau* Mp *avec* $k \geq 2$, $M \geq 1$ *un entier premier à* l *et* p *un nombre premier,* $p \nmid N(\rho)Ml$. *Supposons de plus que* f *est invariante par* $\Gamma_1(M) \cap \Gamma_0(p)$. *Alors, on a*

$$p\,(\mathrm{tr}\rho(\mathrm{Frob}_p))^2 = (1+p)^2 \det \rho(\mathrm{Frob}_p), \tag{4.1}$$

où Frob_p *désigne un élément de Frobenius en* p.

Démonstration. Supposons $\rho \simeq \rho_{f,\lambda}$ avec f comme dans l'énoncé. Comme $p \nmid N(\rho)$, le conducteur de la représentation λ-adique associée à f dégénère en p après réduction modulo λ. De plus le caractère de f est non ramifié en p par hypothèse. On est donc dans le type (ii) de la classification de [Car89, proposition 2]. Dans ce cas, le polynôme caractéristique de $\rho_{f,\lambda}(\mathrm{Frob}_p)$ est de la forme $(X-a)(X-ap)$ avec $a \in \overline{\mathbf{F}}_l^{\times}$. On en déduit le résultat. □

Remarque. La relation (4.1) s'appelle la condition d'augmentation du niveau en p. Elle intervient fréquemment dans la méthode modulaire pour la résolution de certaines équations diophantiennes.

4.3.1 Tour d'horizon des résultats connus

Le résultat ci-dessous est une reformulation due à Ribet ([Rib94, §5]) d'un résultat de Diamond ([Dia91, theorem 1]). Il peut être vu comme une sorte de réciproque à la proposition 4.1.

Théorème 4.4 (Diamond)**.** *Soit* $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ *une représentation galoisienne. On suppose que* ρ *provient d'une forme nouvelle de poids* $2 \leq k \leq l+1$ *et de niveau* M *premier à* l. *Soit* p *un nombre premier,* $p \nmid Ml$. *Alors,* ρ *provient d'une forme propre* $f \in S_k(Mp)$ *invariante par* $\Gamma_1(M) \cap \Gamma_0(p)$ *pour laquelle la forme nouvelle associée est de niveau divisible par* p *(i.e.* f *est « p-new ») si et seulement si on a*

$$p\,(\mathrm{tr}\rho(\mathrm{Frob}_p))^2 = (1+p)^2 \det \rho(\mathrm{Frob}_p).$$

Remarque. Dans [Rib94], Ribet considère des représentations irréductibles. Néanmoins, le théorème de Diamond auquel il se réfère n'utilise pas cette hypothèse.

La difficulté principale à laquelle on est confronté lorsqu'on cherche à appliquer récursivement ce résultat pour décrire les niveaux non optimaux d'une représentation ρ réside dans le fait qu'on n'est pas assuré de pouvoir conserver à chaque étape les nombres premiers introduits précédemment. Par exemple, il se pourrait a priori qu'une représentation ρ

apparaisse en niveaux Mp et Mq (avec p, q deux nombres premiers distincts ne divisant pas Ml) sans pour autant apparaître en niveau Mpq.

À l'aide d'arguments délicats et de la correspondance de Jacquet-Langlands, Diamond et Taylor ont montré qu'il n'en est rien pour les représentations irréductibles. Leur résultat s'énonce ainsi.

Théorème 4.5 ([DT94, theorem B]). *Soit* $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ *une représentation galoisienne* irréductible. *On suppose que* ρ *provient d'une forme nouvelle de poids* $k \geq 2$ *et de niveau* M *premier à* l. *Soit* r *un entier sans facteur carré, premier à* Ml. *Si* $l > k+1$ *et si pour tout diviseur premier* p *de* r, *on a* $p\,(\mathrm{tr}\rho(\mathrm{Frob}_p))^2 = (1+p)^2 \det\rho(\mathrm{Frob}_p)$, *alors* ρ *provient d'une forme propre de poids* k, *de niveau* Mr, *invariante par* $\Gamma_1(M) \cap \Gamma_0(r)$ *et telle que sa forme nouvelle associée est de niveau divisible par* r.

Avec d'autres résultats et techniques (utilisant notamment un lemme de Carayol [Car89], §3.2 et proposition 3), ils sont alors parvenus à donner une classification complète ([DT94, theorem A [4]]) des niveaux non optimaux d'une représentation irréductible ρ (lorsque $l > k(\rho)+1$).

4.3.2 Le cas de la représentation $\mathbf{1} \oplus \chi_l^{k-1}$

Le reste de cette section est consacré à la description de certains résultats obtenus en collaboration avec Menares à propos du problème de l'augmentation du niveau dans le cas des représentations *réductibles*. Les énoncés que l'on présente concernent tous le cas particulier mais important de la représentation $\mathbf{1} \oplus \chi_l^{k-1}$ avec $k \geq 2$ pair.

Soit $p \neq l$ un nombre premier. La condition (4.1) d'augmentation du niveau en p pour la représentation $\mathbf{1} \oplus \chi_l^{k-1}$ s'écrit alors

$$(p^k - 1)(p^{k-2} - 1) \equiv 0 \pmod{l}. \tag{4.2}$$

En particulier, elle est automatiquement satisfaite lorsque $k = 2$.

À la section 4.2, on a caractérisé les paires (l, k) avec $l > k+1$ telles que $\mathbf{1} \oplus \chi_l^{k-1}$ provienne d'une forme propre de poids k et de niveau 1 (i.e. telles que $\mathbf{1} \oplus \chi_l^{k-1}$ est fortement modulaire) : ce sont précisément celles pour lesquelles l divise B_k.

Le premier résultat sur les niveaux non optimaux de la représentation $\mathbf{1} \oplus \chi_l^{k-1}$ est dû à Mazur et concerne le poids 2 ([Maz77, proposition 5.12]).

Proposition 4.2 (Mazur). *Soient* l *et* p *deux nombres premiers. La représentation* $\mathbf{1} \oplus \chi_l$ *provient d'une forme (nouvelle) de poids* 2, *niveau* p *et caractère trivial si et seulement si* l *divise le numérateur de* $(p-1)/12$.

4. Dans leur énoncé, Diamond et Taylor supposent que ρ est modulaire de poids ≥ 2 et de niveau $N(\rho)$. Le théorème de Khare et Wintenberger a rendu cette hypothèse caduque.

Remarque. Dans le résultat de Mazur, on a une précision concernant le caractère des formes nouvelles qui interviennent (celui-ci est trivial). On note cependant que si $\mathbf{1} \oplus \chi_l$ provient d'une forme de poids 2, niveau premier p et caractère χ non trivial, alors $p \equiv 1 \pmod{l}$. En effet, χ se réduisant sur le caractère trivial modulo l, il est d'ordre divisible par l et donc $p \equiv 1 \pmod{l}$. Lorsque $l \geq 5$, on déduit de la proposition ci-dessus que, dans ce cas, $\mathbf{1} \oplus \chi_l$ provient aussi d'une forme de poids 2, niveau p et caractère trivial.

Ribet et Yoo ont récemment étendu le résultat de Mazur (voir [Yoo13, chapters 3-4] et [Yoo14]). Lorsque $l \geq 5$, ils obtiennent notamment une classification complète des entiers de la forme $M = pq$ avec p, q deux nombres premiers distincts et différents de l pour lesquels $\mathbf{1} \oplus \chi_l$ provient d'une forme nouvelle de poids 2, niveau M et caractère trivial.

On présente ci-dessous une variante, non publiée, de leurs résultats où le caractère des formes nouvelles considérées est arbitraire.

Théorème 4.6. *Soit p, q deux nombres premiers distincts et $M = pq$. On suppose $l \geq 5$ et l divise $\phi(M)$ où ϕ est la fonction indicatrice d'Euler. Alors, $\mathbf{1} \oplus \chi_l$ apparaît en poids 2 et niveau M, i.e. il existe une place λ de $\overline{\mathbf{Q}}$ au-dessus de l et une forme nouvelle f de poids 2, niveau M et caractère* quelconque *telles que $\rho_{f,\lambda} \simeq \mathbf{1} \oplus \chi_l$.*

Démonstration. Par hypothèse, on a, disons, $p \equiv 1 \pmod{l}$. D'après la proposition 4.2, la représentation $\mathbf{1} \oplus \chi_l$ provient d'une forme nouvelle de poids 2, niveau p (et caractère trivial). De plus, la condition d'augmentation du niveau (4.2) en q est automatiquement satisfaite. D'après le théorème 4.4 de Diamond, il existe $f_0 \in S_2(pq)$ propre et invariante par $\Gamma_1(p) \cap \Gamma_0(q)$ telle que $\mathbf{1} \oplus \chi_l$ provienne de f_0 et dont la forme nouvelle associée f est de niveau divisible par q.

Si f est de niveau q, alors son caractère est trivial et une nouvelle application (dans le sens réciproque) de la proposition 4.2 donne $q \equiv 1 \pmod{l}$. D'où le résultat si $q \not\equiv 1 \pmod{l}$.

Si en revanche on a $q \equiv 1 \pmod{l}$, alors le théorème 4.2.2 de [Yoo13] garantit [5] que la représentation $\mathbf{1} \oplus \chi_l$ provient d'une forme nouvelle f de niveau pq. □

Remarque. Le théorème 4.6 peut être vu comme un résultat d'augmentation du niveau sans contrainte. Ainsi, la représentation $\mathbf{1} \oplus \chi_5$ par exemple provient d'une forme nouvelle de poids 2 et niveau 11 (la courbe elliptique $X_1(11)$ de conducteur 11 a un point rationnel d'ordre 5). Pour tout nombre premier $p \neq 11$, on en déduit [6] que $\mathbf{1} \oplus \chi_5$ provient d'une forme nouvelle de poids 2 et niveau $11p$. Bien entendu, le fait que le caractère de la forme

5. En réalité, le résultat est plus précis. Dans notre cas, il affirme que $\mathbf{1} \oplus \chi_l$ provient d'une forme nouvelle f de poids 2, niveau pq et caractère trivial telle que $U_p(f) = f = U_q(f)$ avec U_p (resp. U_q) l'opérateur de Hecke en p (resp. q) agissant sur $S_2(\Gamma_0(pq))$.

6. Pour le cas $p = 5$, non couvert par le théorème 4.6, on a vérifié le résultat à l'aide de PARI-GP. Soit χ

nouvelle considérée soit autorisé à être quelconque est crucial : il n'existe pas de forme nouvelle de poids 2, niveau 22 et caractère trivial par exemple.

Le résultat principal sur la classification des niveaux non optimaux que l'on obtient est une généralisation de la proposition 4.2 aux poids ≥ 4.

Théorème 4.7 ([BM16, theorem 1])**.** *Soit $k \geq 4$ un entier pair, l un nombre premier tel que $l > k+1$ et p un nombre premier $\neq l$. Alors, la représentation $\mathbf{1} \oplus \chi_l^{k-1}$ provient d'une forme nouvelle de poids k, niveau p et caractère trivial si et seulement si l'une des conditions suivantes est satisfaite :*

1. *on a $p^k \equiv 1 \pmod{l}$;*
2. *on a $p^{k-2} \equiv 1 \pmod{l}$ et l divise le numérateur de B_k.*

Dans la démonstration de ce théorème, le sens direct résulte d'un raffinement des méthodes employées pour démontrer [BD14, theorem 2.5(ii)(b)] (voir également le théorème 2.6 de ce mémoire). Il se généralise aux niveaux sans facteur carré premiers à l ([BM16, theorem 3.3]).

Le sens réciproque est plus délicat. La difficulté principale réside dans la présence possible de formes anciennes ayant $\mathbf{1} \oplus \chi_l^{k-1}$ comme représentation modulo l. Le théorème de Diamond [Dia91, theorem 1] mentionné précédemment joue un rôle essentiel dans notre démonstration.

Remarques.

1. Dans leur article [DF14], Dummigan et Fretwell montrent que pour tout nombre premier $l > 3$ tel que $v_l((B_k/2k)(p^k-1)) > 0$, la représentation $\mathbf{1} \oplus \chi_l^{k-1}$ provient d'une forme propre $f \in S_k(\Gamma_0(p))$. C'est essentiellement le résultat [BM16, theorem 3.5] dans le cas particulier des niveaux premiers.
2. Gaba et Popa ont proposé récemment une démonstration totalement différente du théorème 4.7. Leur résultat ([GP16, theorem 1]) est un raffinement du nôtre en ce sens qu'ils sont en mesure de spécifier le signe de la valeur propre de f sous l'action de l'opérateur d'Atkin-Lehner en p. Néanmoins, leur méthode nécessite de faire une hypothèse additionnelle lorsque $p^k \not\equiv 1 \pmod{l}$.

le caractère de $(\mathbf{Z}/55\mathbf{Z})^\times$ de conducteur 11 tel que $\chi(3 \pmod{55}) = \zeta_5$ et $\chi(54 \pmod{55}) = 1$ avec ζ_5 une racine primitive 5-ième de l'unité. Il existe alors une forme nouvelle $f \in S_4(55, \chi)$ dont le développement à l'infini commence par

$$f(z) = q + \left((\zeta_5+1)y - \zeta_5^2 - 1\right)q^2 + (-y-\zeta_5^3)q^3 + \left((-\zeta_5^3-1)y + 2\zeta_5^2\right)q^4 + \left(-\zeta_5^3 - \zeta_5^2 - \zeta_5 - 1\right)q^5 + \cdots$$

avec $y^2 + \zeta_5^3 y + \zeta_5^2 - 2\zeta_5 + 1 = 0$. Si λ est une place de $\overline{\mathbf{Q}}$ telle que $\zeta_5 - 1, y \in \lambda$, on vérifie alors que l'on a $\rho_{f,\lambda} \simeq \mathbf{1} \oplus \chi_5$.

4.3.3 Minoration du degré maximal des corps de coefficients de formes nouvelles

Dans ce paragraphe, on donne une application du théorème 4.7 au problème de minorer le degré maximal des corps de coefficients de certaines formes nouvelles. Plus précisément, pour deux entiers $k \geq 2$ et $N \geq 1$, on pose

$$d_k^{\mathrm{new}}(N) = \max\left\{[\mathbf{Q}_f : \mathbf{Q}];\ f \text{ forme nouvelle de poids } k \text{ et niveau } \Gamma_0(N)\right\}.$$

Un théorème de Royer [7] ([Roy00]) implique que pour $k \geq 2$ fixé, on a

$$d_k^{\mathrm{new}}(N) \gg_k \sqrt{\log\log N}, \quad \text{lorsque } N \to \infty \text{ avec } N \text{ premier},$$

où $\gg_k$ signifie que la constante implicite dépend de k.

Pour un entier $m \geq 2$, on convient de noter $P^+(m)$ le plus grand facteur premier de m. Soit alors

$$\mathcal{P} = \left\{N \text{ premier impair tel que } P^+(N-1) > N^{1/4}\right\}.$$

On montre dans [BM16, lemme 4.1] que l'ensemble $\mathcal{P}$ est de densité naturelle $\geq 3/4$ dans l'ensemble des nombres premiers. À l'aide la proposition 4.2 et du théorème 4.7, on obtient alors le résultat suivant.

Théorème 4.8 ([BM16, theorem 2])**.** *Pour tout entier $k \geq 2$ pair et pour tout nombre premier $N \in \mathcal{P}$ avec $N \geq (k+1)^4$, on a*

$$d_k^{\mathrm{new}}(N) \geq c_k \log(N), \quad \textit{où } c_k = \left(8\log\left(1 + 2^{(k-1)/2}\right)\right)^{-1}.$$

7. Le théorème de Royer est valable plus généralement pour tout entier N avec une constante dépendant d'un nombre premier fixé ne divisant par N. Il n'est en revanche énoncé que dans le cas du poids $k = 2$, mais sa preuve s'applique sans changement à tout poids ≥ 2.

Chapitre 5

Variétés abéliennes de Frey et équations diophantiennes

Travaux présentés

[BB17] Michael A. Bennett et Nicolas Billerey : Sums of two S-units via Frey-Hellegouarch curves. *Math. Comp.*, 86(305):1375–1401, 2017.

[BCDF17] Nicolas Billerey, Imin Chen, Luis V. Dieulefait et Nuno Freitas : A result on the equation $x^p + y^p = z^r$ using Frey abelian varieties. *Proc. Amer. Math. Soc.*, 145(10):4111–4117, 2017.

[BCDF] Nicolas Billerey, Imin Chen, Luis V. Dieulefait et Nuno Freitas : A multi-Frey approach to Fermat equations of signature (r, r, p). *Trans. Amer. Math. Soc. (à paraître).*

On présente dans ce chapitre plusieurs applications de la notion de congruence entre formes modulaires à la résolution de certaines équations diophantiennes. Cette stratégie, initiée par Frey ([Fre86]), Ribet ([Rib90]) et Serre ([Ser87]) et utilisée par Wiles dans sa démonstration du dernier théorème de Fermat ([Wil95]) porte désormais le nom de « méthode modulaire ».

5.1 Sommes de deux S-unités

Soit S un ensemble fini de nombres premiers. On convient d'appeler S-unité tout *entier* dont les facteurs premiers appartiennent tous à S. L'arithmétique des S-unités est un sujet

d'étude classique en théorie des nombres. L'équation

$$x + y = z^2 \tag{5.1}$$

d'inconnues x, y, z entiers avec x, y des S-unités et z non nul a notamment été considérée par de Weger dans sa thèse [dW89, chapter 7] qui la résout entièrement lorsque $S = \{2, 3, 5, 7\}$. Son algorithme utilise la théorie des formes linéaires de logarithmes complexes et p-adiques. L'équation (5.1) apparaît aussi naturellement lorsqu'on cherche à rendre effectif le théorème de Shafarevich sur la finitude du nombre de classes d'isomorphismes de courbes elliptiques rationnelles ayant bonne réduction en dehors d'un ensemble fini de nombres premiers fixé (voir l'introduction de [BB17]).

Plus généralement, on s'intéresse à l'équation

$$x + y = z^n \tag{5.2}$$

avec n un entier ≥ 2, x, y des S-unités et z un entier non nul. On dit qu'un quadruplet (x, y, z, n) est une solution *primitive* de (5.2) si $\mathrm{pgcd}(x, y)$ est libre de puissance n-ième. Cette équation fait l'objet du chapitre 9 du livre [ST86] de Shorey et Tijdeman, en raison de sa connexion avec le problème de caractériser les puissances parfaites dans les suites binaires non dégénérées de nombres algébriques.

Le premier résultat que l'on obtient sur l'équation (5.2) est un énoncé de finitude.

Théorème 5.1 ([BB17, corollary 3.4])**.** *Soit S un ensemble fini de nombres premiers. Pour un entier $n \geq 2$ fixé, il n'y a qu'un nombre fini de triplets (x, y, z) tels que (x, y, z, n) est une solution primitive de* (5.2)*. De plus, il n'y a qu'un nombre fini de solutions primitives à l'équation* (5.2) *si et seulement si $2 \notin S$.*

La démonstration que l'on propose de ce théorème repose sur l'emploi combiné de plusieurs courbes de Frey de signatures $(n, n, 2)$, $(n, n, 3)$ et (n, n, n) et fait notamment usage du théorème d'abaissement du niveau de Ribet ([Rib90]). La majeure partie de notre travail avec Bennett a ensuite consisté à expliciter ces ensembles de solutions pour certains ensembles S et certaines valeurs de n.

Lorsque $n \in \{2, 3\}$, on développe aux §§5-6 de [BB17] une approche « modulaire » de l'équation (5.2) basée sur les constructions et les propriétés des courbes de Frey données dans [BS04] et [BVY04]. Il convient de signaler que notre méthode requiert la connaissance de certaines tables de courbes elliptiques comme celle de Cremona [Cre97] (telle qu'elle est implémentée dans SAGE [SD18] ou PARI-GP [PAR18] par exemple). À cet égard, elle doit donc plutôt être considérée comme une illustration de la réciproque du lien existant entre la résolution de l'équation (5.1) et la détermination de courbes elliptiques de conducteur donné.

Cette approche nous permet néanmoins de résoudre l'équation (5.2) lorsque $n \in \{2, 3\}$ et $S = \{2, 3, 5, 7\}$ (retrouvant ainsi le résultat de de Weger [dW89, theorem 7.2] mentionné auparavant) ou lorsque $n \in \{2, 3\}$ et $S = \{2, 3, p\}$ avec p premier, $p < 100$.

À titre d'exemple, on donne ces solutions (avec $x \geq |y| > 0$, $z > 0$ et $\mathrm{pgcd}(x, y)$ libre de puissance n-ième) lorsque $S = \{2, 3, 61\}$ et $n = 2$ (resp. $n = 3$) dans le tableau 5.1 (resp. 5.2). Les solutions en gras, comme par exemple $2 \cdot 3^{10} \cdot 61 - 2 \cdot 61 = 2684^2$, sont celles pour lesquelles les courbes elliptiques associées sont de conducteur $> 350\,000$ et donc n'apparaissent pas dans les tables de Cremona (du moins au moment de l'écriture de [BB17]). Elles ont été calculées au moyen d'arguments *ad hoc* nécessitant parfois l'emploi de SAGE [SD18] pour déterminer les points entiers de certaines courbes elliptiques (voir notamment le lemme 5.1 et la proposition 5.4 de [BB17]).

x	y	z	x	y	z	x	y	z	x	y	z
2	−1	1	16	9	5	122	−1	11	**14823**	**61**	**122**
2	2	2	18	−2	4	192	−183	3	14884	−243	121
3	−2	1	24	1	5	243	−122	11	15616	9	125
3	1	2	27	−2	5	244	−243	1	59049	976	245
4	−3	1	48	1	7	288	1	17	237168	1	487
6	−2	2	61	−36	5	486	−2	22	1361886	3	1167
6	3	3	61	−12	7	732	−3	27	**7203978**	**−122**	**2684**
8	1	3	61	3	8	1024	−183	29			
9	−8	1	81	−32	7	3721	768	67			
12	−3	3	108	61	13	3904	−183	61			

TABLE 5.1 – solutions de $x + y = z^2$ avec $S = \{2, 3, 61\}$

x	y	z	x	y	z	x	y	z	x	y	z
2	−1	1	9	−1	2	64	61	5	2196	1	13
3	−2	1	12	−4	2	122	3	5	15616	9	25
4	−3	1	18	9	3	128	−3	5	36864	−33489	15
4	4	2	24	3	3	244	−243	1	**238144**	**−11163**	**61**
6	2	2	36	−9	3	576	−549	3	1808406	7442	122
9	−8	1	61	3	4	732	−3	9			

TABLE 5.2 – solutions de $x + y = z^3$ avec $S = \{2, 3, 61\}$

Récemment von Känel et Matschke ont développé des algorithmes puissants permettant notamment de résoudre ce genre d'équations ([vM16]). Leurs résultats s'accordent avec les

nôtres dans tous les cas communs traités.

Le résultat principal de [BB17] est la résolution *complète*, à la section 7, de l'équation (5.2) pour $S = \{2, 3\}$ et $S = \{3, 5, 7\}$. Dans ce dernier cas notamment, les techniques utilisées consistent en un usage combiné de plusieurs courbes de Frey et d'arguments locaux pour réduire le problème à la résolution d'un nombre raisonnable d'équations de Thue-Mahler (toutes de degré 5) ; voir la proposition 7.8 de [BB17]. Cette dernière étape résulte de l'application d'un algorithme de Hambrook (non publié). Parmi les résultats intermédiaires que l'on démontre, on peut mentionner la proposition suivante.

Proposition 5.1 ([BB17, proposition 7.6])**.** *Soient x et w deux entiers positifs premiers entre eux qui sont des $\{3, 5, 7\}$-unités et soit $y = \pm 1$. On suppose qu'il existe un entier $z > 0$ tel que $x + y = wz^n$ avec $n \geq 5$ premier. Alors, $y = -1$, $n = 5$, $z = 2$ et*

$$(x, w) = (7^4, 3 \cdot 5^2) \quad ou \quad (3^2 \cdot 5^2, 7).$$

Le résultat final que l'on obtient est le suivant ([BB17, theorem 7.2]).

Théorème 5.2. *L'ensemble des solutions primitives de l'équation* (5.2) *avec $S = \{3, 5, 7\}$ et $x > |y| > 0$ est donné par*

$$\begin{aligned}&(x, y) = (3, 1),\ (5, -1),\ (5, 3),\ (7, -3),\ (7, 1),\ (9, -5),\ (9, -1),\ (9, 7),\ (15, -7),\ (15, 1),\\ &(21, -5),\ (21, 15),\ (25, -21),\ (25, -9),\ (25, 7),\ (27, 5),\ (35, -27),\ (35, -3),\ (35, 1),\\ &(49, -45),\ (49, 15),\ (63, 1),\ (81, -49),\ (105, -5),\ (125, 3),\ (135, -35),\ (135, -7),\\ &(147, -3),\ (175, 21),\ (175, 81),\ (189, -125),\ (189, 7),\ (225, -9),\ (343, -243),\\ &(375, -343),\ (405, -5),\ (441, -225),\ (625, -49),\ (675, 1),\ (729, -245),\ (1029, -5),\\ &(1225, -225),\ (1323, -27),\ (1875, -147),\ (3375, 2401),\ (3969, -1225),\ (3969, -125),\\ &(9375, 1029),\ (10125, -125),\ (15625, -1701),\ (50625, -3969),\ (59535, 1),\\ &(540225, -2401),\ (688905, -5),\ (4782969, 4375)\ et\ (24310125, -10125).\end{aligned}$$

Dans le cas, plus simple, où $S = \{2, 3\}$, on démontre le résultat ci-dessous (on note au passage qu'on a bien une infinité de solutions primitives, conformément au théorème 5.1).

Théorème 5.3 ([BB17, theorem 7.1])**.** *L'ensemble des solutions primitives de l'équation* (5.2) *avec $S = \{2, 3\}$ et $x > |y| > 0$ est donné par les familles*

$$\begin{aligned}&(x, y, z, n) = (2, -1, 1, n),\ (3, -2, 1, n),\ (4, -3, 1, n),\ (9, -8, 1, n),\ (2^{n-1}, 2^{n-1}, 2, n),\\ &(3 \cdot 2^{n-2}, 2^{n-2}, 2, n),\ (3 \cdot 2^{n-1}, -2^{n-1}, 2, n),\ (2 \cdot 3^{n-1}, 3^{n-1}, 3, n),\\ &(2^2 \cdot 3^{n-1}, -3^{n-1}, 3, n),\ (2^3 \cdot 3^{n-2}, 3^{n-2}, 3, n), \quad avec\ n \geq 2,\\ &(x, y, z, n) = (3^2 \cdot 2^{n-3}, -2^{n-3}, 2, n) \quad pour\ n \geq 3\end{aligned}$$

et par

$$\begin{aligned}&(x, y, z, n) = (16, 9, 5, 2),\ (18, -2, 4, 2),\ (24, 1, 5, 2),\ (27, -2, 5, 2),\ (81, -32, 7, 2),\\ &(48, 1, 7, 2),\ (128, -3, 5, 3),\ (288, 1, 17, 2)\ et\ (486, -2, 22, 2).\end{aligned}$$

5.2 Équations de type Fermat

Soit A, B, C trois entiers non nuls. L'équation de Fermat généralisée de signature (p, q, r), où $p, q, r \geq 2$ sont des nombres premiers, désigne l'équation

$$Ax^p + By^q = Cz^r \tag{5.3}$$

d'inconnues $x, y, z \in \mathbf{Z}$. On dit qu'un triplet $(x, y, z) \in \mathbf{Z}^3$ vérifiant (5.3) est une solution primitive de cette équation si $\mathrm{pgcd}(x, y, z) = 1$ et non triviale si $xyz \neq 0$. Pour (p, q, r) fixé tel que $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$, on sait qu'il n'y a qu'un nombre fini de solutions primitives et non triviales à l'équation (5.3) ([DG95, theorem 2]) et on conjecture qu'il n'y a qu'un nombre fini d'entiers x^p, y^q, z^r non nuls premiers entre eux tels que

$$x^p + y^q = z^r \quad \text{et} \quad \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1,$$

avec $p, q, r \geq 2$ premiers.

Dans cette section, on détaille les résultats obtenus en collaboration avec Chen, Dieulefait et Freitas sur certaines équations de Fermat généralisées de signatures (p, p, r) et (r, r, p) où r est fixé et p varie.

5.2.1 Signature (p, p, r)

Dans [Dar00], Darmon a initié un programme ambitieux d'étude des équations de Fermat généralisées. Sa stratégie suit la « méthode modulaire » employée par Wiles ([Wil95]), mais à la différence notable que l'objet géométrique associé à une solution éventuelle de l'équation de Fermat considérée est en général une variété abélienne de dimension ≥ 2 définie sur un corps de nombres. Or la plupart des arguments essentiels de la démonstration du dernier théorème de Fermat sont liés à l'arithmétique des courbes elliptiques rationnelles et n'admettent, au mieux, que des généralisations partielles ou conjecturales à ce contexte.

Dans [BCDF17], nous établissons néanmoins un résultat diophantien inconditionnel en suivant l'approche de Darmon. Notre étude repose sur certaines propriétés des variétés abéliennes construites dans [Dar00] et sur un nouveau critère d'irréductibilité que l'on énonce ci-dessous.

Soit A une variété abélienne définie sur un corps de nombres K. On rappelle que A est dite de type GL_2 si $F = \mathrm{End}_K(A) \otimes \mathbf{Q}$ est un corps de degré égal à $\dim(A)$. Dans ce cas, pour tout idéal premier $\mathfrak{p}$ au-dessus de p dans l'anneau des entiers de F, on note $F_\mathfrak{p}$ le complété de F en $\mathfrak{p}$ et $V_\mathfrak{p}(A)$ le module de Tate de A sur $\mathbf{Q}_p$. On désigne alors par

$$\rho_{A,\mathfrak{p}} \colon \mathrm{Gal}(\overline{\mathbf{Q}}/K) \to \mathrm{GL}_2(\mathbf{F}_\mathfrak{p})$$

la représentation galoisienne associée où $\mathbf{F}_\mathfrak{p}$ est le corps résiduel de $F_\mathfrak{p}$.

On note $\overline{\mathbf{Z}}$ l'anneau des entiers algébriques de $\overline{\mathbf{Q}}$. Notre critère d'irréductibilité s'énonce alors ainsi. Pour les définitions et le vocabulaire, on renvoie à [BCDF17].

Théorème 5.4 ([BCDF17, theorem 2])**.** *Soit K un corps de nombres totalement réel et $\mathfrak{q}$ un idéal premier de son anneau d'entiers de norme $\mathrm{N}(\mathfrak{q})$. Soit $c, f \geq 1$ deux entier avec c pair. On considère un ensemble $S_{\mathfrak{q}}(f)$ d'éléments de la forme $\alpha_1 + \alpha_2$ avec $\alpha_i \in \overline{\mathbf{Z}}$ de module (pour tout plongement de $\overline{\mathbf{Z}}$ dans $\mathbf{C}$) égal à $\mathrm{N}(\mathfrak{q})^{f/2}$ et tels que $\alpha_1\alpha_2 = \mathrm{N}(\mathfrak{q})^f$.*

Alors, il existe une constante $c_1 = c(K, c, f, S_f(\mathfrak{q}))$ avec la propriété suivante. Supposons que p est un nombre premier avec $p > c_1$ et A/K une variété abélienne telle que

(i) A est semi-stable en tout idéal premier de K au-dessus de p ;

(ii) A est de type GL_2 et a multiplication réelle par un corps F ;

(iii) tous les endomorphismes de A sont définis sur K ;

(iv) A/K a exposant d'inertie c ;

(v) A a potentiellement bonne réduction en $\mathfrak{q}$ avec degré résiduel f ;

(vi) la trace de $\mathrm{Frob}_{\mathfrak{q}}^f$ agissant sur $V_{\mathfrak{p}}(A)$ appartient à $S_f(\mathfrak{q})$, où $\mathfrak{p}$ désigne un idéal premier de F au-dessus de p.

Alors, la représentation $\rho_{A,\mathfrak{p}}$ est irréductible.

La démonstration de ce théorème utilise les résultats et techniques de l'article [LV14] de Larson et Vaintrob. À l'aide des propriétés des variétés abéliennes associées par Darmon aux solutions de l'équation de Fermat généralisée, on en déduit le résultat diophantien suivant.

Théorème 5.5 ([BCDF17, theorem 1])**.** *Soit r un nombre premier régulier. Il existe une constante $C(r) > 0$ telle que pour tout nombre premier $p > C(r)$ l'équation de Fermat*

$$x^p + y^p = z^r$$

n'admet aucune solution primitive et non triviale (a, b, c) telle que $r \mid ab$ et $2 \nmid ab$.

5.2.2 Signature (r, r, p)

On s'intéresse désormais à certaines équations de Fermat généralisées de signature (r, r, p) avec $r \in \{5, 13\}$. Les principaux résultats [1] que l'on obtient sont les suivants (théorèmes 1 et 2 de [BCDF] respectivement).

Théorème 5.6. *Pour tout nombre premier p, il n'y a pas de solution primitive et non triviale à l'équation*

$$x^5 + y^5 = 3z^p.$$

1. On renvoie à [BCDF] pour un historique avec références des résultats connus sur ces équations.

Théorème 5.7. *Pour tout nombre premier $p \neq 7$, il n'y a pas de solution primitive et non triviale à l'équation*

$$x^{13} + y^{13} = 3z^p. \tag{5.4}$$

Remarque. Dans un article en préparation avec Chen, Dembélé, Dieulefait et Freitas, nous sommes récemment parvenus à traiter également le cas $p = 7$ de l'équation (5.4).

Dans la suite, on discute uniquement le cas $r = 13$ et on renvoie à *loc. cit.* pour les détails et la démonstration du théorème 5.6. La démonstration du théorème 5.7 repose sur l'utilisation combinée de deux courbes de Frey associées à une hypothétique solution non triviale primitive (a, b, c) de l'équation (5.4). Elles sont notées $E = E_{a,b}$ et $F = F_{a,b}$ dans [BCDF] et définies respectivement sur $\mathbf{Q}(\sqrt{13})$ et le sous-corps cubique K de $\mathbf{Q}(\zeta + \zeta^{-1})$ avec ζ une racine primitive 13-ième de l'unité.

La construction de ces deux courbes est due à Freitas ([DF13, Fre15]) et repose sur l'idée suivante. On considère A, B, C trois éléments distincts non nuls de $\mathbf{Q}(\zeta + \zeta^{-1})$ tels que $A + B + C = 0$ et ABC divise $a^{13} + b^{13}$ (à des facteurs multiplicatifs bien contrôlés près). La courbe elliptique d'équation $Y^2 = X(X - A)(X + B)$ est alors une courbe de Frey associée à (a, b, c) et un choix judicieux de A, B, C permet parfois de montrer qu'elle est isomorphe à une courbe définie sur un sous-corps strict de $\mathbf{Q}(\zeta + \zeta^{-1})$.

Pour chacune des courbes ci-dessus, on note

$$\rho_{E,p} \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\sqrt{13})) \to \mathrm{GL}_2(\mathbf{F}_p) \quad \text{et} \quad \rho_{F,p} \colon \mathrm{Gal}(\overline{\mathbf{Q}}/K) \to \mathrm{GL}_2(\mathbf{F}_p)$$

la représentation galoisienne attachée à ses points de p-torsion. La généralisation de la méthode modulaire requiert de montrer l'irréductibilité de ces représentations. Nous obtenons à ce sujet le résultat ci-dessous.

Théorème 5.8. *Soit $p \geq 7$, $p \neq 13$ un nombre premier. Alors,*

1. *la représentation $\rho_{E,p}$ est irréductible ;*
2. *la représentation $\rho_{F,p}$ est irréductible sauf, peut-être, si $13 \nmid a + b$ et $p \in \{17, 37\}$.*

La première partie de l'énoncé concernant la courbe E ([BCDF, proposition 8]) se déduit essentiellement d'un critère de Freitas et Siksek [FS15, theorem 3]. Son application requiert de façon essentielle l'existence de premiers de bonne réduction explicites établie au lemme 5 de [BCDF]. L'irréductibilité de $\rho_{F,p}$ est plus délicate à obtenir en raison du facteur $a + b$ dans le discriminant de F (voir le paragraphe précédant le lemme 10 de *loc. cit.*). On y parvient grâce à des arguments de théorie du corps de classes et aux travaux récents de Bruin et Najman [BN16] sur les sous-groupes de torsion possibles des courbes elliptiques sur les corps de nombres. Lorsque $13 \nmid a+b$, on a également recours aux résultats de [DKSS17].

Concernant la modularité de ces courbes, celle de E est assurée par les résultats généraux de Freitas, Le Hung et Siksek [FLHS15]. Pour la courbe F, on applique un argument de Freitas [Fre15, theorem 6.3] qui exploite les propriétés arithmétiques de F, et notamment sa réduction en les idéaux divisant 3 ([BCDF, lemma 9]).

La dernière étape de la démonstration du théorème 5.7 consiste en une utilisation combinée des deux courbes E et F. Dans l'esprit de la méthode « multi-Frey » introduite par Bugeaud, Mignotte et Siksek ([BMS08]), on commence par montrer avec la courbe E que l'on a certaines relations de divisibilité portant sur $a+b$ ([BCDF, theorem 7]). Ceci nous permet d'éliminer certains niveaux pour les formes modulaires (de Hilbert) associées à $\rho_{F,p}$ après abaissement du niveau. Ces restrictions sont suffisantes pour permettre un calcul numérique, à l'aide de MAGMA [BCP97], des coefficients des formes nouvelles associées.

Chapitre 6

Perspectives

Beaucoup de travaux actuels s'attachent à étudier les représentations du groupe de Galois absolu d'un corps de nombres totalement réel. Dans ce contexte, les formes modulaires classiques sont remplacées par les formes modulaires de Hilbert et l'existence d'un système de représentations l-adiques associé aux formes propres a été démontrée par Taylor ([Tay89]). L'analogue du théorème 2.1 de Ribet est un résultat de Dimitrov [Dim05]. Compte tenu de la nature explicite de la démonstration de Dimitrov, il devrait être possible d'en déduire des énoncés analogues à ceux du chapitre 2 pour les formes modulaires de Hilbert.

Comme l'ont montré Hida et Ribet dans le cas classique et Dimitrov (*loc. cit.*) dans le cas des formes de Hilbert, les congruences entre formes modulaires s'interprètent, dans certains cas, en termes des fonctions L qui leur sont associées. À l'aide de cette interprétation et du paragraphe 4.1 de [BM16], Kriz ([Kri16]) a récemment obtenu des résultats sur l'arithmétique des courbes elliptiques sur les corps quadratiques. Il serait intéressant d'étudier plus en détails les conséquences des résultats des chapitres 2, 3 et 4 de ce point de vue-là, y compris dans le cas Hilbert.

Dans le chapitre 3, on a fait le choix de fixer le poids des formes à multiplication complexe cherchées. On pourrait néanmoins faire varier ce poids. Quelle est alors la famille de formes que l'on obtient ? Quels en sont les éléments CM ? Il semble plausible que la théorie de Hida permette d'aborder ce genre de questions.

Je ne connais pas de contre-exemple à l'énoncé du théorème 4.5 de Diamond et Taylor (et plus généralement à [DT94, theorem A]) où l'hypothèse « irréductible » est remplacée par « semi-simple ». Il semble crédible, au moins numériquement, de penser que la plupart des représentations réductibles, sinon toutes, se comportent comme les irréductibles du point de vue du problème de l'augmentation du niveau. Ce constat est d'autant plus surprenant qu'il englobe des situations (comme au théorème 4.6) où la condition d'aug-

mentation du niveau est satisfaite en tout nombre premier. On aimerait dans un premier temps généraliser le théorème 4.7 pour obtenir une classification complète des niveaux sans facteur carré de la représentation $\mathbf{1} \oplus \chi_l^{k-1}$ (voir à ce propos la conjecture 3.2 de [BM16]). La stratégie de Diamond et Taylor ([DT94]) se heurte alors à plusieurs difficultés qu'il pourrait néanmoins être possible de surmonter, dans certains cas, si l'on avait une meilleure connaissance de l'action des opérateurs de Hecke sur le noyau de certaines applications qui interviennent dans un analogue du lemme de Ihara (*loc. cit.* lemma 2).

La formulation par Buzzard, Diamond et Jarvis ([BDJ10]) d'un analogue de la conjecture de Serre pour les représentations du groupe $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$ avec K corps de nombres totalement réel d'une part, et la démonstration par Freitas, Le Hung et Siksek ([FLHS15]) de la modularité des courbes elliptiques définies sur les corps quadratiques réels d'autre part, offrent un cadre favorable à la généralisation de la méthode modulaire. Par ailleurs, le développement de critères analogues à ceux du chapitre 4 dans ce contexte pourrait permettre une utilisation plus souple des résultats connus d'abaissement du niveau et, ainsi, la résolution de nouveaux problèmes diophantiens.

Bibliographie

[BB17] Michael A. Bennett et Nicolas Billerey : Sums of two S-units via Frey-Hellegouarch curves. *Math. Comp.*, 86(305):1375–1401, 2017.

[BS04] Michael A. Bennett et Chris M. Skinner : Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.*, 56(1):23–54, 2004.

[BVY04] Michael A. Bennett, Vinayak Vatsal et Soroosh Yazdani : Ternary Diophantine equations of signature $(p, p, 3)$. *Compos. Math.*, 140(6):1399–1416, 2004.

[BCDF17] Nicolas Billerey, Imin Chen, Luis V. Dieulefait et Nuno Freitas : A result on the equation $x^p + y^p = z^r$ using Frey abelian varieties. *Proc. Amer. Math. Soc.*, 145(10):4111–4117, 2017.

[BCDF] Nicolas Billerey, Imin Chen, Luis V. Dieulefait et Nuno Freitas : A multi-Frey approach to Fermat equations of signature (r, r, p). *Trans. Amer. Math. Soc. (à paraître).*

[BD14] Nicolas Billerey et Luis V. Dieulefait : Explicit large image theorems for modular forms. *J. Lond. Math. Soc. (2)*, 89(2):499–523, 2014.

[BM16] Nicolas Billerey et Ricardo Menares : On the modularity of reducible mod l Galois representations. *Math. Res. Lett.*, 23(1):15–41, 2016.

[BM18] Nicolas Billerey et Ricardo Menares : Strong modularity of reducible Galois representations. *Trans. Amer. Math. Soc.*, 370(2):967–986, 2018.

[BN] Nicolas Billerey et Filippo A. E. Nuccio : Représentations galoisiennes diédrales et formes à multiplication complexe. *J. Théor. Nombres Bordeaux (à paraître).*

[BCP97] Wieb Bosma, John Cannon et Catherine Playoust : The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond et Richard Taylor : On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[BN16] Peter Bruin et Filip Najman : A criterion to rule out torsion groups for elliptic curves over number fields. *Res. Number Theory*, 2:Art. 3, 13, 2016.

[BMS08] Yann Bugeaud, Maurice Mignotte et Samir Siksek : A multi-Frey approach to some multi-parameter families of Diophantine equations. *Canad. J. Math.*, 60(3):491–519, 2008.

[BDJ10] Kevin Buzzard, Fred Diamond et Frazer Jarvis : On Serre's conjecture for mod ℓ Galois representations over totally real fields. *Duke Math. J.*, 155(1):105–161, 2010.

[Car59a] Leonard Carlitz : Arithmetic properties of generalized Bernoulli numbers. *J. Reine Angew. Math.*, 202:174–182, 1959.

[Car59b] Leonard Carlitz : Some arithmetic properties of generalized Bernoulli numbers. *Bull. Amer. Math. Soc.*, 65:68–69, 1959.

[Car86] Henri Carayol : Sur les représentations l-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup. (4)*, 19(3):409–468, 1986.

[Car89] Henri Carayol : Sur les représentations galoisiennes modulo l attachées aux formes modulaires. *Duke Math. J.*, 59(3):785–801, 1989.

[Che02] Imin Chen : Surjectivity of mod l representations attached to elliptic curves and congruence primes. *Canad. Math. Bull.*, 45(3):337–348, 2002.

[Cre97] John E. Cremona : *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second édition, 1997.

[Dar00] Henri Darmon : Rigid local systems, Hilbert modular forms, and Fermat's last theorem. *Duke Math. J.*, 102(3):413–449, 2000.

[DG95] Henri Darmon et Andrew Granville : On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[dW89] B. M. M. de Weger : *Algorithms for Diophantine equations*, volume 65 de *CWI Tract*. Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[Del71] Pierre Deligne : Formes modulaires et représentations l-adiques. *In Séminaire Bourbaki. Vol. 1968/69 : Exposés 347–363*, volume 175 de *Lecture Notes in Math.*, pages Exp. No. 355, 139–172. Springer, Berlin, 1971.

[DS74] Pierre Deligne et Jean-Pierre Serre : Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7:507–530 (1975), 1974.

[DKSS17] Maarten Derickx, Sheldon Kamienny, William Stein et Michael Stoll : Torsion points on elliptic curves over number fields of small degree. *ArXiv e-prints*, juillet 2017.

[Dia91] Fred Diamond : Congruence primes for cusp forms of weight $k \geq 2$. *Astérisque*, (196-197):6, 205–213 (1992), 1991. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[Dia95] Fred Diamond : The refined conjecture of Serre. *In Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 22–37. Int. Press, Cambridge, MA, 1995.

[DT94] Fred Diamond et Richard Taylor : Nonoptimal levels of mod l modular representations. *Invent. Math.*, 115(3):435–462, 1994.

[Die09] Luis V. Dieulefait : The level 1 case of Serre's conjecture revisited. *Atti Accad. Naz. Lincei Rend. Lincei Mat. Appl.*, 20(4):339–346, 2009.

[Die15] Luis V. Dieulefait : Automorphy of $\mathrm{Symm}^5(\mathrm{GL}(2))$ and base change. *J. Math. Pures Appl. (9)*, 104(4):619–656, 2015.

[DF13] Luis V. Dieulefait et Nuno Freitas : Fermat-type equations of signature $(13, 13, p)$ via Hilbert cuspforms. *Math. Ann.*, 357(3):987–1004, 2013.

[Dim05] Mladen Dimitrov : Galois representations modulo p and cohomology of Hilbert modular varieties. *Ann. Sci. École Norm. Sup. (4)*, 38(4):505–551, 2005.

[DF14] Neil Dummigan et Daniel Fretwell : Ramanujan-style congruences of local origin. *J. Number Theory*, 143:248–261, 2014.

[Edi92] Bas Edixhoven : The weight in Serre's conjectures on modular forms. *Invent. Math.*, 109(3):563–594, 1992.

[Fre15] Nuno Freitas : Recipes to Fermat-type equations of the form $x^r + y^r = Cz^p$. *Math. Z.*, 279(3-4):605–639, 2015.

[FLHS15] Nuno Freitas, Bao V. Le Hung et Samir Siksek : Elliptic curves over real quadratic fields are modular. *Invent. Math.*, 201(1):159–206, 2015.

[FS15] Nuno Freitas et Samir Siksek : Criteria for irreducibility of mod p representations of Frey curves. *J. Théor. Nombres Bordeaux*, 27(1):67–76, 2015.

[Fre86] Gerhard Frey : Links between stable elliptic curves and certain Diophantine equations. *Ann. Univ. Sarav. Ser. Math.*, 1(1):iv+40, 1986.

[GP16] Radu Gaba et Alexandru A. Popa : A generalization of Ramanujan's congruence to modular forms of prime level. *ArXiv e-prints*, décembre 2016.

[GP12] Eknath Ghate et Pierre Parent : On uniform large Galois images for modular abelian varieties. *Bull. Lond. Math. Soc.*, 44(6):1169–1181, 2012.

[Ghi06] Alexandru Ghitza : All Siegel Hecke eigensystems (mod p) are cuspidal. *Math. Res. Lett.*, 13(5-6):813–823, 2006.

[Hec59] Erich Hecke : *Mathematische Werke*. Herausgegeben im Auftrage der Akademie der Wissenschaften zu Göttingen. Vandenhoeck & Ruprecht, Göttingen, 1959.

[Hup67] Bertram Huppert : *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin-New York, 1967.

[vM16] Rafael von Känel et Benjamin Matschke : Solving S-unit, Mordell, Thue, Thue-Mahler and generalized Ramanujan-Nagell equations via Shimura-Taniyama conjecture. *ArXiv e-prints*, mai 2016.

[KW09a] Chandrashekhar Khare et Jean-Pierre Wintenberger : Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[KW09b] Chandrashekhar Khare et Jean-Pierre Wintenberger : Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009.

[Kri16] Daniel Kriz : Generalized Heegner cycles at Eisenstein primes and the Katz p-adic *L-function*. *Algebra Number Theory*, 10(2):309–374, 2016.

[LV14] Eric Larson et Dmitry Vaintrob : Determinants of subquotients of Galois representations associated with abelian varieties. *J. Inst. Math. Jussieu*, 13(3): 517–559, 2014. With an appendix by Brian Conrad.

[Liv89] Ron Livné : On the conductors of mod l Galois representations coming from modular forms. *J. Number Theory*, 31(2):133–141, 1989.

[LMF13] The LMFDB Collaboration : *The L-functions and Modular Forms Database,* Home page of the L-function $L(s, E)$ for the Elliptic Curve Isogeny Class 234446.a. `http://www.lmfdb.org/L/EllipticCurve/Q/234446.a/`, 2013. [Online ; accessed 16 September 2013].

[Mar05] Greg Martin : Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$. *J. Number Theory*, 112(2):298–331, 2005.

[Maz77] Barry Mazur : Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Maz11] Barry Mazur : How can we construct abelian Galois extensions of basic number fields ? *Bull. Amer. Math. Soc. (N.S.)*, 48(2):155–209, 2011.

[Mur97] M. Ram Murty : Congruences between modular forms. *In Analytic number theory (Kyoto, 1996)*, volume 247 de *London Math. Soc. Lecture Note Ser.*, pages 309–320. Cambridge Univ. Press, Cambridge, 1997.

[Nua11] Joan Nualart : Minimal lifts of dihedral 2-dimensional Galois representations. *Bull. Braz. Math. Soc. (N.S.)*, 42(3):359–371, 2011.

[PAR18] The PARI Group : *PARI/GP version* `2.11.0`. Univ. Bordeaux, 2018. available from `http://pari.math.u-bordeaux.fr/`.

[Ran77] Robert A. Rankin : Ramanujan's unpublished work on congruences. pages 3–15. Lecture Notes in Math., Vol. 601, 1977.

[Rib75] Kenneth A. Ribet : On l-adic representations attached to modular forms. *Invent. Math.*, 28:245–275, 1975.

[Rib76] Kenneth A. Ribet : A modular construction of unramified p-extensions of $\mathbf{Q}(\mu_p)$. *Invent. Math.*, 34(3):151–162, 1976.

[Rib77] Kenneth A. Ribet : Galois representations attached to eigenforms with Nebentypus. pages 17–51. Lecture Notes in Math., Vol. 601, 1977.

[Rib84] Kenneth A. Ribet : Congruence relations between modular forms. *In Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983)*, pages 503–514. PWN, Warsaw, 1984.

[Rib85] Kenneth A. Ribet : On l-adic representations attached to modular forms. II. *Glasgow Math. J.*, 27:185–194, 1985.

[Rib90] Kenneth A. Ribet : On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[Rib94] Kenneth A. Ribet : Report on mod l representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *In Motives (Seattle, WA, 1991)*, volume 55 de *Proc. Sympos. Pure Math.*, pages 639–676. Amer. Math. Soc., Providence, RI, 1994.

[Rib97] Kenneth A. Ribet : Images of semistable Galois representations. *Pacific J. Math.*, (Special Issue):277–297, 1997. Olga Taussky-Todd : in memoriam.

[Rib04] Kenneth A. Ribet : Abelian varieties over $\mathbf{Q}$ and modular forms. *In Modular curves and abelian varieties*, volume 224 de *Progr. Math.*, pages 241–261. Birkhäuser, Basel, 2004.

[Roy00] Emmanuel Royer : Facteurs $\mathbf{Q}$-simples de $J_0(N)$ de grande dimension et de grand rang. *Bull. Soc. Math. France*, 128(2):219–248, 2000.

[SD18] The Sage Developers : *SageMath, the Sage Mathematics Software System (Version 8.2)*, 2018. `http://www.sagemath.org`.

[Ser68] Jean-Pierre Serre : *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Ser69] Jean-Pierre Serre : Une interprétation des congruences relatives à la fonction τ de Ramanujan. *In Séminaire Delange-Pisot-Poitou : 1967/68, Théorie des Nombres, Fasc. 1, Exp. 14*, page 17. Secrétariat mathématique, Paris, 1969.

[Ser73] Jean-Pierre Serre : Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]. pages 319–338. Lecture Notes in Math., Vol. 317, 1973.

[Ser87] Jean-Pierre SERRE : Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbf{Q}}/\mathbf{Q}$). *Duke Math. J.*, 54(1):179–230, 1987.

[Shi71a] Goro SHIMURA : *Introduction to the arithmetic theory of automorphic functions.* Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo ; Princeton University Press, Princeton, N.J., 1971. Kanô Memorial Lectures, No. 1.

[Shi71b] Goro SHIMURA : On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields. *Nagoya Math. J.*, 43:199–208, 1971.

[Shi72] Goro SHIMURA : Class fields over real quadratic fields and Hecke operators. *Ann. of Math. (2)*, 95:130–190, 1972.

[ST86] Tarlok N. SHOREY et Robert TIJDEMAN : *Exponential Diophantine equations*, volume 87 de *Cambridge Tracts in Mathematics.* Cambridge University Press, Cambridge, 1986.

[Stu87] Jacob STURM : On the congruence of modular forms. *In Number theory (New York, 1984–1985)*, volume 1240 de *Lecture Notes in Math.*, pages 275–280. Springer, Berlin, 1987.

[SD73] H. P. F. SWINNERTON-DYER : On l-adic representations and congruences for coefficients of modular forms. pages 1–55. Lecture Notes in Math., Vol. 350, 1973.

[Tay89] Richard TAYLOR : On Galois representations associated to Hilbert modular forms. *Invent. Math.*, 98(2):265–280, 1989.

[Wie04] Gabor WIESE : Dihedral Galois representations and Katz modular forms. *Doc. Math.*, 9:123–133, 2004.

[Wil95] Andrew WILES : Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[Yoo13] Hwajong YOO : *Modularity of residually reducible Galois representations and Eisenstein ideals.* ProQuest LLC, Ann Arbor, MI, 2013. Thesis (Ph.D.)–University of California, Berkeley.

[Yoo14] Hwajong YOO : Non-optimal levels of a reducible mod l modular representation. *ArXiv e-prints*, septembre 2014.