SÉMINAIRE N. BOURBAKI

BERNADETTE PERRIN-RIOU

Travaux de Kolyvagin et Rubin

Séminaire N. Bourbaki, 1989-1990, exp. n° 717, p. 69-106.

<http://www.numdam.org/item?id=SB_1989-1990__32__69_0>

Séminaire BOURBAKI Novembre 1989
42e année, 1989/90, n° 717

TRAVAUX DE KOLYVAGIN ET RUBIN

par Bernadette PERRIN-RIOU

Soit F un corps de nombres. Le théorème de Dirichlet détermine le rang du groupe des unités $\mathfrak{E}_F$ de l'anneau des entiers de F. Construire effectivement des unités est un problème beaucoup plus difficile. Cela est possible dans deux cas particuliers. Lorsque F est une extension abélienne de $\mathbb{Q}$ ou d'un corps quadratique imaginaire K, on construit un sous-groupe $\mathfrak{C}_F$ des unités (appelé groupe des unités cyclotomiques dans le premier cas et groupe des unités elliptiques dans le second cas) dont l'indice est fini et à peu près égal au nombre de classes de F, c'est-à-dire au cardinal du groupe des classes C_F de F. On peut alors se demander quel est le rapport entre les deux modules galoisiens $\mathfrak{E}_F/\mathfrak{C}_F$ et C_F.

Soit E une courbe elliptique sur $\mathbb{Q}$ paramétrée par des fonctions modulaires (conjecturalement, c'est toujours le cas). Grâce au théorème de Mordell-Weil, on sait que le groupe $E(F)$ des points de E rationnels sur F est de rang fini. Mais le calcul du rang est beaucoup plus difficile. Cependant, Birch (en reprenant une idée de Heegner) a construit de manière systématique des points sur E rationnels sur certaines extensions abéliennes d'un corps quadratique imaginaire (soumis à des conditions supplémentaires). Engendrent-ils un sous-groupe d'indice fini et si oui cet indice est-il relié au cardinal du groupe de Shafarevich-Tate qui est dans cette situation l'analogue du groupe des classes d'idéaux?

Rappelons que jusqu'aux travaux de Kolyvagin et Rubin, aucun exemple de courbe elliptique ayant un groupe de Shafarevich-Tate fini n'avait été trouvé.

Les travaux de Kolyvagin et Rubin apportent une réponse aux problèmes qui viennent d'être évoqués. Ils permettent aussi de redémontrer de manière élémentaire la conjecture principale d'Iwasawa sur $\mathbb{Q}$ (démontrée par Mazur et Wiles [38]) et de prouver la conjecture principale de Coates-Wiles sur un corps quadratique imaginaire. Disons seulement pour l'instant que ces conjectures relient l'arithmétique des extensions abéliennes de $\mathbb{Q}$ avec les fonctions L p-adiques construites par interpolation de valeurs de fonctions L complexes.

Nous allons d'abord donner un résultat de formulation aussi simple que possible pour chacune de ces trois situations. Puis, après un bref historique, nous parlerons des conjectures principales et des conséquences sur les courbes elliptiques sur $\mathbb{Q}$ en direction de la conjecture de Birch et Swinnerton-Dyer. Nous essaierons ensuite de donner quelques idées des techniques de démonstration utilisées.

Notations. Soit $\overline{\mathbb{Q}}$ la fermeture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$; tous les corps de nombres considérés sont supposés contenus dans $\overline{\mathbb{Q}}$. Si F est un corps de nombres, on note C_F son groupe de classes d'idéaux et $\mathcal{E}_F$ le groupe des unités de l'anneau des entiers de F. Si G est un groupe abélien fini, si M est un $\mathbb{Z}[G]$-module fini et si χ est un caractère de G, on pose

$$M^{(\chi)} = \{m \in M \otimes_{\mathbb{Z}} \mathbb{Z}[\chi] \text{ tel que } gm = \chi(g)m \text{ pour } g \in G\}$$

où $\mathbb{Z}[\chi]$ est l'anneau engendré par les valeurs de χ. Si p est un nombre premier, on note M(p) la composante p-primaire de M. Soit μ_n le groupe des racines n-ièmes de l'unité.

1. Présentation des résultats.

1.1. Premiers résultats.

Regardons d'abord le cas cyclotomique. Soit F une extension abélienne réelle de $\mathbb{Q}$. Le groupe des unités cyclotomiques de F est défini de la manière suivante: si L est une sous-extension de F cyclique sur $\mathbb{Q}$ de conducteur f, soit $\mathfrak{H}_L$ le sous-groupe de $L^\times$ engendré par les conjugués de $N_{\mathbb{Q}(\mu_f)/L}(1-\zeta_f)$ où ζ_f est une racine de l'unité d'ordre f. Le groupe des unités cyclotomiques de F est défini par

$$\mathfrak{C}_F = \mathfrak{E}_F \cap (\prod \mathfrak{H}_L)$$

où L parcourt les sous-extensions cycliques de $F/\mathbb{Q}$.

Théorème 1.1. Soient F une extension abélienne réelle de $\mathbb{Q}$ et χ un caractère de $\mathrm{Gal}(F/\mathbb{Q})$. Alors, pour tout nombre premier p ne divisant pas $2[F:\mathbb{Q}]$,

$$\#((\mathfrak{E}_F/\mathfrak{C}_F)(p)^{(\chi)}) = \#(C_F(p)^{(\chi)}).$$

Passons au cas elliptique. Soient K un corps quadratique imaginaire. On suppose pour simplifier que l'anneau des entiers $\mathfrak{O}_K$ de K est principal. On peut alors trouver une courbe elliptique E définie sur K et à multiplication complexe par $\mathfrak{O}_K$. Soit

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

une équation minimale de E sur $\mathfrak{O}_K$ et $\Delta(E)$ son discriminant. On considère la coordonnée x comme une fonction rationnelle sur E. Soit $\mathfrak{a}=(\alpha)$ un idéal de K premier à 6. On sait [45] que $\Delta(E)^{N\alpha-1}$ est une puissance 12-ième dans K. On considère la fonction rationnelle sur E

$$\Theta_0(z,\mathfrak{a}) = \Delta(E)^{(N\alpha-1)/12}\alpha^{-1}\prod_{b\in E_\alpha-\{0\}}(x(z)-x(b))^{-6}$$

(elle est définie à une racine de l'unité de K près). Soit ψ le caractère de Hecke de K associé à E et $\mathfrak{F}$ son conducteur. Si $\mathfrak{m}$ est un idéal de K, on note

$$I(\mathfrak{M})=\{\text{idéaux entiers de } K \text{ premiers à } 6\mathfrak{F}\mathfrak{M}\},$$

$$J_0(\mathfrak{M})=\{\mu: I(\mathfrak{M}) \to \mathbb{Z} \ , \ \mu(\mathfrak{A}) = 0 \text{ pour presque tout } \mathfrak{A}, \ \sum \mu(\mathfrak{A})(N\mathfrak{A}-1)=0\}.$$

Pour $\mu \in J_0(\mathfrak{M})$, on pose

$$\Theta_0(z,\mu)=\prod_{\mathfrak{A}} \Theta_0(z,\mathfrak{A})^{\mu(\mathfrak{A})}$$

Si L est une extension abélienne de K de conducteur $\mathfrak{M}$ premier à $6\mathfrak{F}$, on note Ω_L le sous-groupe engendré par les $N_{L(E_{\mathfrak{F}\mathfrak{M}})/L}(\Theta_0(a,\mu))$ pour $\mu \in J_0(\mathfrak{M})$ et a un point de $\mathfrak{F}\mathfrak{M}$-torsion. Enfin, si F est une extension abélienne de K, on définit le groupe des unités elliptiques $\mathfrak{C}_F$ comme étant le groupe des unités de F engendré par les $\Omega_L^{\cdot}$ pour toute sous-extension cyclique L de F/K et par le groupe des racines de l'unité de F.

Théorème 1.2. Soient F une extension abélienne de K et χ un caractère de $\mathrm{Gal}(F/K)$. Alors, pour tout nombre premier p ne divisant pas $[F:\mathbb{Q}]$ et tel que F ne contienne pas μ_p,

$$\#((\mathfrak{E}_F/\mathfrak{C}_F)(p)^{(\chi)})=\#(C_F(p)^{(\chi)}).$$

Enfin, introduisons le cas modulaire : une courbe elliptique E définie sur $\mathbb{Q}$ est dite de Weil [35] s'il existe un entier N et un morphisme non nul φ de $X_0(N)$ dans E qui envoie la pointe ∞ de $X_0(N)$ sur l'origine de E. Soit K un corps quadratique imaginaire tel que les facteurs premiers de N se décomposent dans K. Choisissons un idéal $\mathfrak{N}$ de l'anneau des entiers $\mathfrak{O}$ de K tel que $\mathfrak{O}/\mathfrak{N} \simeq \mathbb{Z}/N\mathbb{Z}$. Alors, l'isogénie cyclique de degré N

$$\mathbb{C}/\mathfrak{O} \to \mathbb{C}/\mathfrak{N}^{-1}$$

définit un point de $X_0(N)$ qui est rationnel sur le corps de Hilbert $K(1)$ de K. Soit τ_1 son image par φ dans $E(K(1))$. On note τ_K la trace de $K(1)$ à K de τ_1. Le sous-groupe de $E(K)$ engendré par τ_K et par le sous-groupe de torsion de $E(K)$ est indépendant des choix faits, on l'appelle groupe des points de Heegner de $E(K)$. D'autre part, le groupe de Shafarevich-Tate $Ш(E/K)$ est défini comme le

sous-groupe de $H^1(\mathrm{Gal}(\bar{K}/K),E(\bar{K}))$, noyau des applications de localisation

$$H^1((\mathrm{Gal}(\bar{K}/K),E(\bar{K})) \to \prod_v H^1((\mathrm{Gal}(\bar{K}_v/K_v),E(\bar{K}_v))\ .$$

Soit S_E l'ensemble suivant de nombres premiers : si E n'est pas à multiplication complexe, $p\in S_E \Leftrightarrow p=2$ ou le groupe de Galois de $\mathbb{Q}(E_p)/\mathbb{Q}$ est différent de $GL_2(\mathbb{Z}/p\mathbb{Z})$; si E a multiplication complexe par un ordre $\mathcal{O}$, $p\in S_E \Leftrightarrow$ $p=2$ ou p divise le discriminant de $\mathcal{O}$ ou p divise le cardinal du sous-groupe de torsion de $E(K)$ ou le groupe de Galois de $\mathbb{Q}(E_p)/\mathbb{Q}$ est différent de $(\mathcal{O}/p\mathcal{O})^*$

Théorème 1.3. Supposons τ_K d'ordre infini dans $E(K)$. Alors,

(i) le groupe $E(K)$ est de rang 1 et $Ш(E/K)$ est fini;

(ii) si $p\notin S_E$, l'ordre de $Ш(E/K)(p)$ divise $[E(K):\mathbb{Z}\tau_K]^2$ et $[E(K):\mathbb{Z}\tau_K]$ annule $Ш(E/K)(p)$.

Remarques. a) Le théorème 1.3 démontre une partie de la conjecture suivante. On note m_p le nombre de Tamagawa de $E/\mathbb{Q}$ en p [55] et c est le rationnel positif défini de la manière suivante: si ω est l'unique forme différentielle de E sur $\mathbb{Q}$ telle que $\varphi^*\omega$ soit la forme différentielle $\sum a_n q^n dq/q$ associée à une forme modulaire normalisée ($a_1=1$), $c\omega$ est une forme différentielle de Néron sur E.

Conjecture 1.4. Supposons que τ_K est d'ordre infini dans $E(K)$. Alors,

(i) le groupe $E(K)$ est de rang 1 ;

(ii) le groupe de Shafarevich-Tate $Ш(E/K)$ est fini et l'on a

$$\#(Ш(E/K))= ([E(K):\mathbb{Z}\tau_K]/c\textstyle\prod_{p|N} m_p)^2\ .$$

Cette conjecture est l'analogue dans le cas modulaire des théorèmes 1.1 et 1.2 pour le caractère trivial. On peut énoncer une conjecture plus générale pour un caractère de $\mathrm{Gal}(K(n)/K)$ d'ordre premier à p.

b) Soit $L(E/\mathbb{Q},s)=\sum_n a_n n^{-s}$ la fonction L complexe de $E/\mathbb{Q}$ et

$L(E/K,s)$ la fonction L complexe de E/K. Gross et Zagier [26] ont établi une formule liant la dérivée de la fonction L de E/K avec la hauteur de Néron-Tate de τ_K. En particulier, ils montrent que si $L'(E/K,1)$ est non nul, le point τ_K est d'ordre infini.

c) Rappelons enfin l'énoncé de la conjecture de Birch et Swinnerton-Dyer pour une courbe elliptique E définie sur $\mathbb{Q}$ [55].

Conjecture 1.5. La fonction $L(E/\mathbb{Q},s)$ a un zéro en $s=1$ de multiplicité $g_{E(\mathbb{Q})}$ égale au rang de $E(\mathbb{Q})$. Le groupe de Shafarevich-Tate est fini et on a

$$L^{(g_{E(\mathbb{Q})})}(E/\mathbb{Q},1) = (\prod_{p|N} m_p)\#(Ш(E/\mathbb{Q}))R_\infty(E)\Omega_\infty$$

où $R_\infty(E)$ est le volume de $E(\mathbb{Q})$ pour la forme bilinéaire de Néron-Tate et où Ω_∞ est la période réelle positive de E.

1.2. Intermède.

En s'appuyant sur des calculs numériques, Gras [19] a conjecturé que les facteurs de Jordan-Hölder des modules galoisiens $\mathfrak{C}_F/\mathfrak{T}_F$ et C_F d'ordre premier à $2[F:\mathbb{Q}]$ sont les mêmes et ont la même multiplicité, ce qui équivaut au théorème 1.1. En reprenant une idée de Ribet [43], Mazur et Wiles [38] ont montré ce théorème en utilisant la géométrie des courbes modulaires pour construire des extensions non ramifiées d'extensions cyclotomiques de $F(\mu_p)$ dans la partie - du groupe de classes et en utilisant la théorie d'Iwasawa (voir plus loin). Dans [56], Thaine montre que $\#((\mathfrak{C}_F/\mathfrak{T}_F)(p)^{(\chi)})$ annule $C_F(p)^{(\chi)}$ de manière directe et élémentaire. Rubin [50] adapte sa démonstration au cas elliptique; il peut alors montrer la finitude du groupe de Shafarevich-Tate pour les courbes elliptiques à multiplication complexe définies sur le corps de multiplication complexe telles que $L(E/\mathbb{Q},1)$ est non nul (paragraphe 1.5).

D'autre part, des calculs numériques ont permis à Birch et Stephens [4]

de suggérer une forme de la conjecture 1.4 . Celle-ci a été ensuite écrite sous une forme définitive par Gross et Zagier [26] à la lumière de leur travail sur la dérivée de la fonction L de E/K et de la conjecture de Birch et Swinnerton-Dyer. Kolyvagin démontre d'abord une partie du théorème 1.3 ([31],[32]) et trouve un annulateur d'une partie du groupe de Shafarevich-Tate. Il se rend alors compte que sa méthode et celle de Thaine sont de fait similaires et une itération de cette méthode permet à Kolyvagin de démontrer les trois théorèmes.

L'idée est la suivante. Dans tous les cas précédents, les sous-groupes spéciaux de $\mathcal{E}_F$ ou de E(K) n'arrivent pas tous seuls. A tout entier n sont associés une extension abélienne K(n) de $\mathbb{Q}$ ou de K et un élément spécial τ_n (unité cyclotomique, elliptique ou point de Heegner) de "niveau n" , défini sur cette extension . Ces points sont reliés entre eux par des formules. C'est ce que Kolyvagin appelle un système d'Euler. L'utilisation de ce système d'Euler permet de trouver des relations dans le groupe des classes ou le groupe de Shafarevich-Tate. L'idée fondamentale de Kolyvagin est alors de construire à partir d'un système d'Euler d'autres systèmes d'Euler qu'il appelle systèmes d'Euler dérivés paramétrés par des suites de nombres premiers $\ell_1,\ldots,\ell_s$ et qui fournissent d'autres relations dans le groupe des classes d'idéaux ou dans le groupe de Shafarevich-Tate. Le théorème de Cebotarev permet de choisir les ℓ_i de manière à avoir le plus de relations indépendantes possibles. On obtient ainsi une divisibilité de l'indice par le cardinal de la χ-partie du groupe de classes. L'égalité est alors obtenue en utilisant la formule donnant le nombre de classes de F .

Kolyvagin explique de plus comment la connaissance du système d'Euler des unités cyclotomiques ou elliptiques détermine complètement la structure des groupes de classes en tant que groupe abélien et en particulier son rang.

Les théorèmes 1.1 et 1.2 admettent des généralisations à des caractères de conducteur une puissance de p , que l'on appelle conjectures principales cyclotomique et elliptique. La conjecture cyclotomique d'Iwasawa a été démon-

trée par Mazur et Wiles [38]. L'utilisation des systèmes d'Euler dérivés de Kolyvagin et les techniques de la théorie d'Iwasawa ont permis à Rubin de redémontrer la conjecture principale dans le cas cyclotomique [34] et de la démontrer dans le cas elliptique [50]. On obtient ainsi une démonstration élémentaire de ces conjectures dont nous allons maintenant rappeler l'énoncé.

1.3. Conjectures principales (cas cyclotomique et elliptique)

On fixe ici un nombre premier p impair. On note $\mathbb{Q}_\infty$ l'unique sous-corps de $\mathbb{Q}(\mu_{p^\infty})$ tel que $\Gamma = Gal(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p$ et pour tout n, $\mathbb{Q}_n$ la sous-extension de $\mathbb{Q}_\infty/\mathbb{Q}$ de degré p^n. Soit F une extension abélienne réelle de $\mathbb{Q}$ de degré premier à p; on pose $\Delta = Gal(F/\mathbb{Q})$, $F_\infty = F\mathbb{Q}_\infty$, $G_n = Gal(F_n/\mathbb{Q})$ et $G_\infty = Gal(F_\infty/\mathbb{Q}) = \Gamma \times \Delta$. On choisit une clôture algébrique $\overline{\mathbb{Q}}_p$ de $\mathbb{Q}_p$ contenant $\overline{\mathbb{Q}}$. Fixons un caractère de Δ dans $\overline{\mathbb{Q}}_p^{\times}$. Si M est un $\mathbb{Z}_p[[\Delta]]$-module, on note

$$M^{(\chi)} = \{m \in M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\chi] \text{ tel que } gm = \chi(g)m \text{ pour } g \in \Delta\}.$$

Soient $\mathfrak{C}_{F_n}$ le groupe des unités cyclotomiques de F_n et A_{F_n} le p-groupe de Sylow de C_{F_n}. Soient $\overline{\mathfrak{C}}_{F_n}$ et $\overline{\mathfrak{C}}_{F_n}$ les séparés complétés de $\mathfrak{C}_{F_n}$ et $\mathfrak{C}_{F_n}$ pour la toplogie p-adique. On note A_{F_∞} (resp. $\overline{\mathfrak{C}}_{F_\infty}$, resp. $\overline{\mathfrak{C}}_{F_\infty}$) la limite projective des A_{F_n} (resp. $\overline{\mathfrak{C}}_{F_n}$, resp. $\overline{\mathfrak{C}}_{F_n}$) relativement aux homomorphismes induits par la norme. Tous ces $\mathbb{Z}_p$-modules sont de manière naturelle des $\mathbb{Z}_p[[G_\infty]]$-modules. L'anneau $\mathbb{Z}_p[[G_\infty]]^{(\chi)}$ s'identifie à $\mathbb{Z}_p[\chi][[\Gamma]]$ (qui est isomorphe à $\mathbb{Z}_p[\chi][[T]]$). Rappelons que, pour tout module M de type fini et de torsion sur $B = \mathbb{Z}_p[\chi][[\Gamma]]$ (ou plus généralement un anneau local complet régulier), il existe des éléments non nuls $f_1, \ldots, f_d$ de B et un homomorphisme injectif de B-modules de $\oplus_{1 \leq i \leq d} B/(f_i)$ dans M dont le conoyau est fini (resp. annulé par un idéal de hauteur ≥ 2) ; l'idéal de B engendré par $f_1 \ldots f_d$ ne dépend que de M, c'est l'idéal caractéristique de M. Les $\mathbb{Z}_p[\chi][[\Gamma]]$-modules $(A_{F_\infty})^{(\chi)}$ et $(\overline{\mathfrak{C}}_{F_\infty}/\mathfrak{C}_{F_\infty})^{(\chi)}$ sont de type fini et de torsion

([29],[34], le second est même monogène à un groupe fini près).

Théorème 1.6 (conjecture principale pour $\mathbb{Q}$). Les idéaux caractéristiques de $(A_{F_\infty})^{(\chi)}$ et de $(\overline{\mathfrak{C}}_{F_\infty}/\overline{\mathfrak{C}}_{F_\infty})^{(\chi)}$ sont égaux.

D'habitude, ce théorème est énoncé en faisant intervenir les fonctions L p-adiques. Si χ est un caractère de Dirichlet p-adique primitif non trivial, on notera de la même manière le caractère galoisien associé. La fonction L complexe attachée à χ est $L(\chi,s)=\sum_n \chi(n)n^{-s}$. Soit ω le caractère de Teichmüller (en tant que caractère galoisien, il est donné par l'action sur μ_p). Soit ν le caractère de $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ dans $1+p\mathbb{Z}_p$ tel que $\omega\nu$ donne l'action du groupe de Galois sur μ_{p^∞}. Il existe [28] une unique fonction $L_p(\chi,s)$ continue pour $s\in\mathbb{Z}_p$ telle que pour tout entier $k\geqslant 1$

$$L_p(\chi,1-k)=(1-\chi_k(p)p^{k-1})L(\chi_k,1-k)$$

où χ_k est le caractère primitif associé à $\chi\omega^{-k}$. C'est la fonction L p-adique de Kubota-Leopoldt (si χ est impair (i.e. $\chi(-1)=-1$), elle est identiquement nulle). On peut de plus lui associer un unique élément $G_p(\chi)$ de $\mathbb{Z}_p[\chi][\![\Gamma]\!]$: un élément de cet anneau peut être considéré comme une fonction sur le groupe $\mathrm{Hom}_{\mathrm{cont}}(\Gamma,\mathbb{C}_p^\times)$ (où $\mathbb{C}_p$ est la complétion de $\overline{\mathbb{Q}}_p$) et $G_p(\chi)$ est caractérisé par

$$G_p(\chi)(\nu^k)=L_p(\chi,1-k) \text{ pour tout entier } k\geqslant 1.$$

Soient M_{F_n} la plus grande p-extension abélienne de F_n non ramifiée au dehors de p, M_{F_∞} la réunion des M_{F_n} et X_{F_∞} le groupe de Galois de M_{F_∞}/F_∞. C'est encore un $\mathbb{Z}_p[\![\mathrm{Gal}(F_\infty/\mathbb{Q})]\!]$-module de type fini. La théorie du corps de classes permet de construire une suite exacte

$$0\to U_{F_\infty}/\overline{\mathfrak{C}}_{F_\infty}\to X_{F_\infty}\to A_{F_\infty}\to 0.$$

où U_{F_∞} est la limite projective relativement aux normes des unités semi-locales en p de F_n congrues à 1 modulo les places au dessus de p. On peut donc

relier les idéaux caractéristiques des χ-composantes de X_{F_∞}, A_{F_∞}, $U_{F_\infty}/\overline{\mathcal{C}}_{F_\infty}$ et $\overline{\mathcal{C}}_{F_\infty}/\overline{\mathcal{C}}_{F_\infty}$. D'autre part, Iwasawa a montré qu'une série caractéristique de $(U_{F_\infty}/\overline{\mathcal{C}}_{F_\infty})^{(\chi)}$ est $G_p(\chi)$ si χ est non trivial [34, Th. 5.2]. Le théorème 1.6 est alors équivalent au théorème suivant.

Théorème 1.7. Soit χ un caractère de $\mathrm{Gal}(F/\mathbb{Q})$ non trivial. Alors, l'idéal caractéristique de $X_{F_\infty}^{(\chi)}$ est engendré par $G_p(\chi)$.

Donnons-en une dernière formulation. Supposons maintenant que F est une extension abélienne de $\mathbb{Q}$ contenant μ_p de degré premier à p (c'est donc une extension quadratique imaginaire d'une extension réelle). Soit $\mathcal{A}_{F_\infty}$ la limite inductive des A_{F_n} et $\hat{\mathcal{A}}_{F_\infty} = \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{A}_{F_\infty}, \mathbb{Q}_p/\mathbb{Z}_p)$ son dual de Pontryagin. En utilisant la théorie de Kummer, Iwasawa a montré [29] qu'il existe un homomorphisme injectif à conoyau fini de A_{F_∞} dans $(\hat{\mathcal{A}}_{F_\infty})^*$ (le point indique que l'action de $\mathrm{Gal}(F_\infty/\mathbb{Q})$ est modifiée par $\gamma.m = \gamma^{-1}m$)); de plus, si χ est un caractère pair non trivial, $X_{F_\infty}^{(\chi)}$ et $\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{A}_{F_\infty}, \mu_{p^\infty})^{(\chi)}$ sont des $\mathbb{Z}_p[\chi][[\Gamma]]$-modules de torsion isomorphes.

Théorème 1.8. Si χ est un caractère impair de $\mathrm{Gal}(F/\mathbb{Q})$ différent de ω^{-1}, l'idéal caractéristique de $\hat{\mathcal{A}}_{F_\infty}^{(\chi)}$ est engendré par la fonction $\rho \mapsto G_p(\chi\omega)(\nu\rho)$.

La conjecture principale (maintenant théorème) dans le cas elliptique s'énonce de manière analogue. Soient F une extension abélienne de K de degré premier à p, K_∞ une $\mathbb{Z}_p$- ou $\mathbb{Z}_p^2$-extension de K et $F_\infty = K_\infty F$. On remplace unités cyclotomiques par unités elliptiques. Rubin a annoncé le théorème suivant [50] :

Théorème 1.9 (Rubin). Les idéaux caractéristiques de $(A_{F_\infty})^{(\chi)}$ et de $(\overline{\mathcal{C}}_{F_\infty}/\overline{\mathcal{C}}_{F_\infty})^{(\chi)}$

sont égaux dans chacun des cas suivants

(i) lorsque $p=\mathfrak{P}\mathfrak{P}^*$ se décompose dans K et que K_∞ est la $\mathbb{Z}_p$-extension de K non ramifiée en dehors de $\mathfrak{P}$, pour tout caractère χ de $\mathrm{Gal}(F/K)$,

(ii) lorsque p se décompose dans K, que K_∞ est l'unique $\mathbb{Z}_p^2$-extension de K et que, soit μ_p n'est pas contenu dans F, soit $\chi\chi^g\neq\omega$ pour tout $g\in\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$,

(iii) lorsque p est inerte dans K.

Ce théorème a une traduction en termes de fonctions L p-adiques lorsque p se décompose dans K ([13],[60],[54]). Nous ne rappelons ici que le cas où K_∞ est l'unique $\mathbb{Z}_p^2$-extension de K. Soit E la courbe elliptique utilisée pour construire le groupe des unités elliptiques. Soit $L(\psi,s)$ la fonction L du caractère de Hecke ψ de K associé à E. La fonction L de E/K est donnée par

$$L(E/K,s)=L(\psi,s)L(\overline{\psi},s).$$

Si E est définie sur $\mathbb{Q}$, la fonction L de $E/\mathbb{Q}$ est donnée par $L(E/\mathbb{Q},s)=L(\psi,s)$.

Choisissons un idéal premier $\mathfrak{P}$ de K au dessus de p. Soit $\overline{W}$ l'anneau des entiers du complété de l'extension maximale non ramifiée de $K_{\mathfrak{P}}$. Rappelons ([12], [14], [30], [61]) qu'il existe un unique élément $G_{\mathfrak{P}}(\chi)$ de $\overline{W}[[\mathrm{Gal}(F_\infty/F)]]$ tel que pour tout caractère ρ d'ordre fini de $\mathrm{Gal}(F_\infty/F)$

$$G_{\mathfrak{P}}(\chi)(\rho)/\Omega_{\mathfrak{P}}(\rho)=(1-\psi\rho(\mathfrak{P})/p)(1-\overline{\psi}(\mathfrak{P}^*)\rho^{-1}(\mathfrak{P}^*)/p)L(\psi\rho,1)/\Omega_\infty(\rho)$$

(ici, $\Omega_\infty(\rho)$ et $\Omega_{\mathfrak{P}}(\rho)$ sont des périodes respectivement complexes et $\mathfrak{P}$-adiques attachées à ψ et à ρ que l'on peut explicitement décrire).

Soit M_{F_n} la plus grande p-extension abélienne de F_n non ramifiée en dehors de $\mathfrak{P}$, M_{F_∞} la réunion des M_{F_n} et X_{F_∞} le groupe de Galois de M_{F_∞}/F_∞. Grâce au théorème de Coates-Wiles [14] et de Yager [60], le théorème 1.9 (ii) est équivalent au théorème suivant.

Théorème 1.10. Soit χ un caractère de $\mathrm{Gal}(F/K)$. On suppose que F ne contient

pas μ_p ou que $\chi\chi^g \neq \omega$ pour tout $g \in Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. L'idéal caractéristique de $X_{F_\infty}^{(\chi)}$ dans $\overline{W}[[\Gamma]]$ est engendré par $G_{\mathfrak{P}}(\chi)$.

1.4. Courbes elliptiques sur $\mathbb{Q}$.

Les résultats qui précèdent (à la fois dans le cas elliptique et modulaire) permettent d'avancer en direction de la conjecture de Birch et Swinnerton-Dyer. Nous aurons besoin des deux résultats suivants sur les fonctions L complexes attachées aux courbes elliptiques de Weil.

Théorème 1.11. (i) Supposons $L(E/\mathbb{Q},1)=0$. Il existe une infinité de caractères quadratiques imaginaires χ tels que $\chi(\ell)=1$ pour $\ell | N$ et $L(E/\mathbb{Q},\chi,1)\neq 0$.
(ii) Supposons $L(E/\mathbb{Q},1)\neq 0$. Il existe une infinité de caractères quadratiques imaginaires χ tels que $\chi(\ell)=1$ pour $\ell | N$ et que $L(E/\mathbb{Q},\chi,s)$ a un zéro d'ordre 1 en $s=1$.

La partie (i) a été montrée par Waldspurger (citée dans [57]). La partie (ii) vient d'être montrée indépendamment par Bump, Friedberg et Hoffstein [8] et par M. Ram Murty et V. Kumar Murty [39]. Si E est une courbe elliptique de Weil sur $\mathbb{Q}$, on obtient alors le théorème suivant.

Théorème 1.12. Si $L(E/\mathbb{Q},1)$ est non nul, alors $E(\mathbb{Q})$ et $Ш(E/\mathbb{Q})$ sont finis. Si $L(E/\mathbb{Q},s)$ a un zéro simple en $s=1$, $E(\mathbb{Q})$ est de rang 1 et $Ш(E/\mathbb{Q})$ est fini.

Démonstration. La valeur propre ε de l'involution d'Atkin-Lehner w_N sur f vaut -1 si $L(E/\mathbb{Q},1)\neq 0$ (resp. $+1$ si $L(E/\mathbb{Q},s)$ a un zéro simple en $s=1$). Soit K le corps quadratique imaginaire associé à un caractère χ donné par (ii) (resp. (i)) du théorème 1.11. Alors $L(E/K,s)$ a un zéro simple en $s=1$. Grâce au résultat de [26] rappelé dans 1.1, τ_K est un point d'ordre infini et si σ est la conjugai-

son complexe, on a $\sigma\tau_K=\varepsilon\tau_K$ modulo torsion. Il n'appartient donc pas (resp. appartient) à $E(\mathbb{Q})$ modulo torsion. On déduit alors le résultat du théorème 1.3 .

Supposons maintenant que E est une courbe elliptique à multiplication complexe par l'anneau des entiers $\mathcal{O}$ d'un corps quadratique imaginaire k et est définie sur k . Soit $w_k\in\{2,4,6\}$ le nombre de racines de l'unité de k. Les résultats dans le cas elliptique (avec $K=k$) permettent d'obtenir des résultats plus précis sur la conjecture de Birch et Swinnerton-Dyer.

Théorème 1.13. Si $L(E/k,1)\neq 0$, alors $E(k)$ et $Ш(E/k)$ sont finis et la conjecture de Birch et Swinnerton-Dyer est vraie à multiplication par une unité de $\mathcal{O}[1/w_k]$ près .

Théorème 1.14. Si $L(E/k,1)=0$, soit $E(k)$ est infini, soit la composante $\mathfrak{P}$-primaire de $Ш(E/k)$ est infinie pour tout idéal $\mathfrak{P}$ de k ne divisant pas w_k .

La démonstration de ces deux théorèmes utilise des techniques de descente. Lorsque p se décompose dans k, on utilise [40] et le théorème 1.10 (Kolyvagin-Rubin + Coates-Wiles). Lorsque p est inerte dans k, Rubin utilise de plus la loi explicite de réciprocité de Wiles [58].

Théorème 1.15. Si E est définie sur $\mathbb{Q}$ et si $L(E/\mathbb{Q},s)$ a un zéro simple en $s=1$, alors $E(\mathbb{Q})$ est de rang 1 , $Ш(E/\mathbb{Q})$ est fini; si p est premier à w_k et se décompose dans k , la conjecture de Birch et Swinnerton-Dyer est vraie à multiplication par une unité de $\mathbb{Z}_p$ près.

Démonstration. On utilise dans la démonstration la fonction L p-adique $L_p(E/\mathbb{Q})$ construite par Mazur et Swinnerton-Dyer [37] qui coincide avec une spécialisation de la fonction L p-adique attachée au caractère de Hecke ψ (paragraphe

1.3). Soit χ un caractère quadratique imaginaire tel que $\chi(\ell)=1$ pour tout ℓ divisant N et $L(E/\mathbb{Q},\chi,1)\neq 0$. On déduit de [26] et de [42] que la fonction L p-adique $L_p(E/\mathbb{Q})$ de $E/\mathbb{Q}$ a un zéro simple en 1. Le théorème 1.10 implique qu'il en est de même de la série caractéristique du dual de Pontryagin du groupe de Selmer $S(\mathbb{Q}_\infty)$ (on a une suite exacte

$$0 \to E(\mathbb{Q}_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p \to S(\mathbb{Q}_\infty) \to Ш(E/\mathbb{Q}_\infty)(p) \to 0;$$

voir [40] pour le lien avec X_{F_∞}). Le corollaire 1.9 de [42] (qui dépend lui-même du théorème de Gross-Zagier, de son analogue p-adique et de [40]) implique alors le théorème.

Ainsi, ces théorèmes relient un invariant analytique (l'ordre du zéro de la fonction L complexe) avec un invariant arithmétique (le rang de $E(\mathbb{Q})$). Le premier résultat dans cette direction a été celui de Coates et Wiles [13] dans le cas des courbes elliptiques à multiplication complexe: si $E(\mathbb{Q})$ est infini, alors $L(E/\mathbb{Q},1)$ est nul.

Théorème 1.16. Le groupe $E(\mathbb{Q}_\infty)$ est un $\mathbb{Z}$-module de type fini (conjecture de Mazur).

En effet, Rohrlich [46] a montré que la fonction L p-adique $L_p(E/\mathbb{Q})$ est non nulle. On en déduit par le théorème 1.10 que le dual de Pontryagin du $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}]]$-module $S(\mathbb{Q}_\infty)$ est de torsion (voir démonstration du théorème 1.15), ce qui permet de conclure [40].

Par manque de place, nous avons choisi de ne pas donner la démonstration des conjectures principales. Nous donnons dans le paragraphe 3 une idée de la démonstration des théorèmes 1.1 et 1.3 en suivant Kolyvagin [33] (des modifications ont été faites dans [25] et dans l'appendice de [34]). Dans le paragraphe 2, nous parlerons d'un outil essentiel de la démonstration de Kolyvagin, les sys-

tèmes d'Euler.

2. Systèmes d'Euler.

Dans la suite, p est un nombre premier fixé et M, M',... désigneront des puissances de p. Si L/F est une extension galoisienne, on note

$$H^i(L/F,\blacksquare)=H^i(\mathrm{Gal}(L/F),\blacksquare) \text{ et } H^i(F,\blacksquare)= H^i(\overline{\mathbb{Q}}/F,\blacksquare).$$

Si x est un élément de $H^i(\blacksquare/\blacksquare, C_M)$ et si $M'|M$, on note x(M') l'image de x dans $H^i(\blacksquare/\blacksquare,C_{M'})$ par l'application induite par la multiplication par M/M'. Si $x \in H^1(F,\blacksquare)$ et si v est une place de F, on note x_v l'image de x dans $H^1(F_v,\blacksquare)$.

En suivant Kolyvagin, nous allons construire à partir d'unités des familles d'éléments de $F^\times/F^{\times M}$ qui sont des unités en dehors d'un ensemble fini de places et dont on peut décrire la valuation. On fait une construction analogue dans le cas modulaire (cas d'une courbe elliptique). Le résultat utile pour la démonstration des théorèmes 1.1 et 1.3 (démonstration esquissée dans le paragraphe 3) est le théorème 2.1 . On explique ensuite dans ce paragraphe la manière dont Kolyvagin l'obtient. Pour ne pas alourdir d'avantage le texte, nous ne considèrerons que le cas de représentations p-adiques sur $\mathbb{Q}$ (dans le cas elliptique, la représentation p-adique associée à la situation est une représentation de $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, il faut remplacer les nombres premiers ℓ de $\mathbb{Q}$ par des idéaux premiers...).

2.1. Représentations p-adiques.

Donnons quelques définitions relatives aux représentations p-adiques aussi générales que possibles bien que les applications que nous ayons en vue soient le cas des modules de Tate $\mathbb{Z}_p$, $\mathbb{Z}_p(1)$ et $T_p(E)$ de $\mathbb{Q}_p/\mathbb{Z}_p$, μ_{p^∞} et de E_{p^∞}.

Soit $T_p(X)$ un $\mathbb{Z}_p$-module libre de type fini de dimension d muni d'une action linéaire et continue de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. On note X le groupe p-divisible (au

sens des groupes abéliens) associé ($X_M = T_p(X)/MT_p(X)$). On considère le groupe p-divisible X' défini par

$$T_p(X') = \mathrm{Hom}_{\mathbb{Z}_p}(T_p(X), \mathbb{Z}_p(1)).$$

On suppose que $T_p(X)$ est une représentation de de Rham en p [15]. Soit $\mathfrak{N}$ le produit (supposé fini) des nombres premiers de $\mathbb{Q}$ où $T_p(X)$ a mauvaise réduction (si ℓ ne divise pas p (resp. $\ell=p$), $T_p(X)$ a bonne réduction en ℓ si l'action du sous-groupe d'inertie en ℓ est triviale (resp. si $T_p(X)$ est cristalline en p [15]). Si ℓ est un nombre premier ne divisant pas $\mathfrak{N}p$, soit P_ℓ le polynôme caractéristique du Frobenius (arithmétique) Fr_ℓ sur $T_p(X)$. Si L une extension de $\mathbb{Q}$ et v une place de L, on associe à $T_p(X)$ un sous-groupe $H^1_f(L_v, X_M)$ de $H^1(L, X_M)$ défini par $H^1_f(L_v, X_M) = H^1(L_v^{nr}/L_v, X_M)$ si v ne divise pas $\mathfrak{N}p$ (où L_v^{nr} est la plus grande extension de L_v non ramifiée) et en utilisant les méthodes de Greenberg et Bloch-Kato en général ([6],[23]).

Exemples. Si $X = \mu_{p^\infty}$, $H^1(L_v, X_M) = L_v^*/L_v^{*M}$ par la théorie de Kummer et $H^1_f(L_v, X_M) = U(L_v)/U(L_v)^M$ (où $U(L_v)$ est le groupe des unités de L_v); si $X = \mathbb{Q}_p/\mathbb{Z}_p$, $H^1(L_v, X_M) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(\bar{L}_v/L_v), \mathbb{Z}/M\mathbb{Z})$ et $H^1_f(L_v, X_M) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(L_v^{nr}/L_v), \mathbb{Z}/M\mathbb{Z})$. Si $X = E_{p^\infty}$, $H^1_f(L_v, E_M)$ est l'image réciproque de $H^1(L_v^{nr}/L_v, E(L_v^{nr}))_M$ dans $H^1(L_v, E_M)$ et on a la suite exacte

$$0 \to E(L_v)/ME(L_v) \to H^1_f(L_v, E_M) \to H^1(L_v^{nr}/L_v, E(L_v^{nr}))_M \to 0.$$

L'accouplement naturel $[\blacksquare,\blacksquare]_M : X_M \times X'_M \to \mu_M$ induit un accouplement local non dégénéré $\langle \blacksquare, \blacksquare \rangle_v$

$$H^1(L_v, X_M) \times H^1(L_v, X'_M) \to H^2(L_v, \mu_M) = \mathbb{Z}/M\mathbb{Z} ;$$

Si x (resp. y) est un élément de $H^1(L, X_M)$ (resp. $H^1(L, X'_M)$), on a

$$\sum_v \langle x, y \rangle_v = 0. \tag{2.1}$$

Les sous-groupes $H^1_f(L_v, X_M)$ et $H^1_f(L_v, X'_M)$ sont exactement orthogonaux ([6], [52]). On en déduit un isomorphisme

$$H^1(L_v, X'_M)/H^1_f(L_v, X'_M) \simeq \mathrm{Hom}_{\mathbb{Z}_p}(H^1_f(L_v, X_M), \mu_M).$$

Soit v une place de L au dessus de ℓ première à $\mathfrak{N}p$ totalement décomposée dans $L(X_M)/L$ et non ramifiée sur $\mathbb{Q}$ de degré résiduel f. Choisissons une racine de l'unité $\zeta_{M,v}$ d'ordre M. L'application de $H^1_f(L_v, X_M)$ dans X_M donnée par $x \mapsto x(\mathrm{Fr}_\ell^f)$ est un isomorphisme. On en déduit un isomorphisme $\mathfrak{C}_v$ de $H^1(L_v, X'_M)/H^1_f(L_v, X'_M)$ sur X'_M (dépendant de $\zeta_{M,v}$) caractérisé par

$$[x(\mathrm{Fr}_\ell^f), \mathfrak{C}_v(y)]_M = \zeta_{M,v}^{\langle x,y\rangle_v}.$$

Remarque. Si $X = E_{p^\infty}$, l'accouplement de Weil permet d'identifier X et X' (on le note encore $[\blacksquare,\blacksquare]_M$). L'accouplement $\langle .,. \rangle_v$ induit alors l'accouplement local de Tate $E(L_v)/ME(L_v) \times H^1(L_v, E_M) \to \mathbb{Z}/M\mathbb{Z}$. Si $X = \mathbb{Z}_p$ et $X' = \mu_{p^\infty}$, on a $\mathfrak{C}_v(y) = \zeta_{M,v}^{\mathrm{ord}_v(y)}$ si ord_v est la valuation de L_v normalisée par $\mathrm{ord}_v(L_v) = \mathbb{Z}$.

Si T est un ensemble fini de places de L, on note $S_T(X/L)^{(M)} = S_T(T_p(X)/L)^{(M)}$ le sous-$\mathbb{Z}_p$-module de $H^1(L, X_M)$ formé des éléments dont l'image dans $H^1(L_v, X_M)$ appartient à $H^1_f(L_v, X_M)$ pour toute place v de L ne divisant aucune place de T. On pose $S(T_p(X)/L)^{(M)} = S(X/L)^{(M)} = S_\emptyset(X/L)^{(M)}$. C'est le "groupe de Selmer". Lorsque $X = E_{p^\infty}$, on retrouve le groupe de Selmer classique attaché à la courbe elliptique E. On vérifie facilement que $S(\mathbb{Z}_p/L)^{(M)} = \mathrm{Hom}_{\mathbb{Z}_p}(A_L, \mathbb{Z}/M\mathbb{Z})$ où A_L est le p-groupe de Sylow du groupe C_L des classes d'idéaux de L. Si T est un ensemble de places finies, $S_T(\mathbb{Z}_p(1)/L)^{(M)} = \mathfrak{C}_{L,T}/\mathfrak{C}_{L,T}^M$ où $\mathfrak{C}_{L,T}$ est le groupe des T-unités de L.

2.2. Théorème clé.

On se donne maintenant une extension abélienne K de $\mathbb{Q}$, un ensemble fini de places S_0 et pour chaque entier m non nul, une extension abélienne $K(m)$ de K vérifiant les propriétés suivantes:

(i) si $n|m$, alors $K(n)\subset K(m)$; $K(n)\cap K(m)=K(pgcd(n,m))$; $K(n)K(m)=K(ppcm(n,m))$;

(ii) pour ℓ premier, $K(\ell)/K(1)$ est de degré premier à ℓ ;

(iii) $K(\ell)/K$ est non ramifiée en dehors des places au dessus de ℓ et de S_0.

En fait, nous ne considèrerons que l'un des deux cas particuliers suivants:

(2.2) (i) si $X=\mu_{p^\infty}$, on prend $K=\mathbb{Q}$ et $\mathbb{Q}(m)=\mathbb{Q}(\mu_m)$; (ii) si $X=E_{p^\infty}$, K est un corps quadratique imaginaire tel que tout nombre premier divisant le conducteur de E est décomposé dans K ; $K(m)$ est l'extension de K associée par le corps de classes à l'ordre $\mathcal{O}_m$ de $\mathcal{O}_K$ de conducteur m .

On se fixe un entier $\mathfrak{N}_0$ divisible par $2\mathfrak{N}$ et par les nombres premiers ramifiés dans $K/\mathbb{Q}$. On suppose désormais que <u>tous les nombres premiers ℓ considérés sont premiers à $\mathfrak{N}_0$</u>. On note M_ℓ la plus grande puissance de p divisant $[K(\ell):K(1)]$ telle que les éléments de X_M sont rationnels sur K_v où v est une place de K au dessus de ℓ.

On définit inductivement [1] un ensemble $\mathfrak{P}^{(k)}$ de l'ensemble des $k+1$-uples $[m;\ell_1,\dots,\ell_k]$ où m est un entier et où les ℓ_i sont des nombres premiers distincts : $\mathfrak{P}^{(0)}=\{[m],m\in\mathbb{N}\}$, $\mathfrak{P}^{(k)}$ est l'ensemble des $[m;\ell_1,\dots,\ell_k]$ où $[m;\ell_1,\dots,\ell_{k-1}]$ est un élément de $\mathfrak{P}^{(k-1)}$ et où ℓ_k est un nombre premier ne divisant pas $\mathfrak{N}_0 mp\ell_1\dots\ell_{k-1}$, inerte dans K, totalement décomposé dans $K(m\ell_1\dots\ell_{k-1})/K$ et tel que si $M_0(m,\ell_1,\dots,\ell_{k-1})$ est le ppcm des annulateurs de $X_{p^\infty}(K(m\ell_1\dots\ell_{k-1}))$ et des

[1] Une méthode légérement différente permet d'enlever certaines des conditions techniques de la définition de cet ensemble, voir [49], [50] et article en préparation de Kolyvagin.

$X_{p^\infty}(K(m\ell_1..\ell_{k-2}/\ell_j)_v)$ pour $j=1,...,k-2$ et pour toute place v au dessus de ℓ_j, $M_0(m,\ell_1,...,\ell_{k-1})M_{\ell_{k-1}}$ divise M_{ℓ_k}.

Dans le cas (2.2),(i), pour tout entier m, on choisit des racines de l'unité ζ_m d'ordre m vérifiant $\zeta_{nm}=\zeta_n^m$. On pose $\tau_m=1-\zeta_m$. Dans le cas (2.2),(ii), rappelons la définition des points de Heegner de niveau quelconque. Si m est un entier positif, notons $\mathcal{O}_m$ l'ordre de $\mathcal{O}$ de conducteur m. Fixons un idéal $\mathfrak{N}$ de $\mathcal{O}$ tel que $\mathcal{O}/\mathfrak{N}\simeq\mathbb{Z}/N\mathbb{Z}$. La classe d'isomorphismes de l'isogénie cyclique de degré N

$$\mathbb{C}/\mathcal{O}_m \to \mathbb{C}/(\mathfrak{N}\cap\mathcal{O}_n)^{-1}.$$

définit un élément de $X_0(N)(K(m))$. On note τ_m son image dans $E(K(m))$ ou dans $E(K(m))\otimes_{\mathbb{Z}}\mathbb{Z}_p$.

Théorème 2.1(Kolyvagin). Supposons (2.2). On se donne un entier m, un entier $k\geqslant 1$, une puissance M de p. Alors, il existe pour $j=1,...,k$ des nombres premiers ℓ_j et des éléments $\tau_{[m;\ell_1,...,\ell_j]}$ de $S_{(\ell_1,...,\ell_j)}(X/K(m))^{(M_{\ell_1})}$ avec $\tau_{[m]}=\tau_m$ tels que $M\mid M_{\ell_1}$, $[m;\ell_1,...,\ell_k]\in\mathcal{P}^{(k)}$ et tel que pour tous $j\leqslant i$ et pour v_{ℓ_j} une place de $K(m)$ au dessus de ℓ_j, on ait (2.3)

$$\mathfrak{S}_{v_{\ell_j}}(\tau_{[m;\ell_1,...,\ell_i]}(M))=Fr_{\ell_j}^{-1}(\tau_{\varepsilon_j([m;\ell_1,...,\ell_i])}(M)(Fr_{\ell_j}^d)=Fr_{\ell_j}^{-1}(Fr_{\ell_j}^d-1)(\tau_{\varepsilon_j([m;\ell_1,...,\ell_i])}(M)/M)$$

dans X_M si $\varepsilon_j([m;\ell_1,...,\ell_i])=[m;\ell_1,...\ell_{j-1},\ell_{j+1},...,\ell_i]$.

De plus, une fois trouvés $\ell_1,...,\ell_{k-1}$ et les éléments $\tau_{[m;\ell_1,...,\ell_j]}$ pour $j\leqslant k-1$, si M' est une puissance de p divisible par $M_{\ell_{k-1}}$, si L est une extension finie de $K(m)(X_{M'})$ et si h est un élément de $Gal(L/K(m)(X_{M'}))$, on peut choisir ℓ_k tel que $h=Fr_{\ell_k}$.

On indique dans les paragraphes 2.3 et 2.4 une idée de la démonstration de Kolyvagin.

2.3. Construction auxiliaire: la corestriction de Kolyvagin.

La situation générale est la suivante. Soit G un groupe, H un sous-groupe distingué de G tel que G/H est cyclique d'ordre fini D. On choisit un générateur δ de G/H. Si C est un G-module discret, on note $H^1_G(H,C)$ le noyau de l'homomorphisme de corestriction

$$cor_{H,G}: H^1(H, C) \to H^1(G, C).$$

Soit c un entier tel que cD annule C et tel que $cC^G \subset (\delta-1)(cC)^H$ (par exemple tel que cC^G est nul). On définit alors un homomorphisme

$$cor'_{H,G} : H^1_G(H,C) \to H^1(G, cC)$$

de la manière explicite suivante. Soit $\tilde{\delta}$ un relèvement de δ à G. Soit φ un cocycle représentant x. La corestriction de x est représentée par l'unique cocycle φ_1 de G à valeurs dans C vérifiant

$$\varphi_1(h)=\sum_{i=0}^{D-1}\delta^i(\varphi)(h) \text{ si } h\in H \text{ et } \varphi_1(\tilde{\delta})=\varphi(\tilde{\delta}^D)$$

Si $x \in H^1_G(H,C)$, il existe donc un élément e de C tel que $\varphi_1(g)=(g-1)e$ pour tout $g \in G$. Considérons le polynôme $P(X)$ vérifiant

$$X^{D-1}+X^{D-2}+\ldots+X+1=(X-1)P(X)+D$$

Le fait que cD annule C implique qu'il existe un et un seul cocycle ψ de G à valeurs dans cC tel que

$$\psi(h)= cP(\delta)(\varphi)(h) \text{ si } h\in H \text{ et } \psi(\tilde{\delta}) = ce .$$

La condition imposée sur C^G implique que la classe $cores'_{H,G}(x)$ dans $H^1(F,cC)$ ne dépend pas du choix du relèvement $\tilde{\delta}$ de δ, du représentant φ de x, ni du choix de e.

Remarque. Lorsque C^G est nul, $H^i(L/F, C^H)=0$ pour $i=1,2$; la restriction

$$H^1(F,C) \to H^1(L,C)^{Gal(L/F)}$$

est alors un isomorphisme. Il est d'autre part clair que $P(\delta)x$ est un élément de $H^1(L,C)^{Gal(L/F)}$. Donc, $cores'_{H,G}(x)$ est alors simplement l'image réciproque de

$P(\delta)x$ dans $H^1(F,C)$ par la restriction.

Nous appliquerons cette construction au cas où $G=Gal(\overline{\mathbb{Q}}/F)$ avec F un corps de nombres, où $H = Gal(\overline{\mathbb{Q}}/L)$ avec L/F une extension cyclique de degré divisible par M et où $C=X_{cM}$ (on a $cX_{cM} = X_M$). On écrira alors $cor'_{L/F}$. On a la proposition suivante.

Proposition 2.2. Soit F un corps de nombres, L/F une extension cyclique de degré D. Soit $Ram(L/F)$ l'ensemble des places de ramification de L/F. On suppose que M est un diviseur de D et que $c=c(F)$ est un entier tel que $cX_{cM}^{Gal(\overline{F}/F)}=0$. Si T est un ensemble fini de places de F et si x appartient à l'intersection de $H^1_F(L,X_{cM})$ et de $S_T(X/L)^{(cM)}$, alors $cor'_{L/F}(x)$ appartient à $S_{T\cup Ram(L/F)}(X/F)^{(M)}$.

2.4. Systèmes d'Euler.

Plaçons-nous de nouveau dans la situation (2.2). Pour tout ℓ, on se donne un élément y_ℓ appartenant à l'algèbre de groupe du groupe de Galois sur $\mathbb{Q}$ de la plus grande extension non ramifiée en ℓ contenue dans $UK(m)$: si K est différent de $\mathbb{Q}(\sqrt{-3})$ et de $\mathbb{Q}(\sqrt{-1})$, on prend

$$y_\ell = Fr_{\ell'}^{-1}([K(\ell):K(1)]+ (-1)^{d-1} P_\ell(Fr_{\ell'}))$$

(ℓ' est au dessus de ℓ dans K ; si ℓ est inerte dans K, $y_\ell=a_\ell$ si $X=E_{p^\infty}$ et $y_\ell= 1-Fr_\ell^{-1}$ si $X=\mu_{p^\infty}$).

Soit T un ensemble fini de nombres premiers. Une famille d'Euler non ramifiée en dehors de T est la donnée pour tout entier m premier à T d'une puissance de p, éventuellement infinie, $M(m)$ et d'un élément $\tau_m=(\tau_m(M))_{M|M(m)}$ de $\lim proj_{M|M(m)} S_T(X/K(m))^{(M)}$ vérifiant pour ℓ premier à T et à $\mathfrak{N}_0 p$, non ramifié dans $K(m)/K$ et pour M divisant $M(m)$ et $M(m\ell)$

$$cores_{K(\ell m)/K(m)}(\tau_{\ell m}(M))=y_\ell \tau_m(M).$$

Un système d'Euler d'ordre k est la donnée pour toute suite $[\ell_1,\dots,\ell_k]$ de

nombres premiers distincts d'une famille d'Euler $(M(m;\ell_1,\dots,\ell_k),\tau_{m,[\ell_1,\dots,\ell_k]})_m$ non ramifiée au dehors de $\{\ell_1,\dots,\ell_k\}$.

Si $\pi=[m;\ell_1,\dots,\ell_k]$, on notera $\tau_\pi=\tau_{m,[\ell_1,\dots,\ell_k]}$, $M(\pi)=M(m;\ell_1,\dots,\ell_k)$. L'entier m est le niveau de π et de τ_π. On pose $\ell.\pi=[\ell m;\ell_1,\dots,\ell_k]$.

On fixe désormais pour tout nombre premier ℓ un générateur δ_ℓ du groupe cyclique $Gal(K(\ell)/K(1))$. Pour tout entier n premier à ℓ, il détermine un générateur (noté toujours δ_ℓ) de $Gal(K(n\ell)/K(n))$ grâce à l'isomorphisme $Gal(K(n\ell)/K(n)) \to Gal(K(\ell)/K(1))$. Les applications cor' seront définies à l'aide de ces choix. Le groupe des points d'ordre une puissance de p contenus dans $X(K(m))$ pour n premier à p est fini. On note son cardinal $c_p(m)$.

Soient $k\geq 1$ et τ_π un système d'Euler d'ordre $k-1$. Remarquons que si π est de niveau m, lorsque la place de K au dessus de ℓ se décompose totalement dans $K(m)$ et que $Mc_p(m)$ divise M_ℓ, on a $cores_{K(\ell m)/K(m)}(\tau_{\ell.\pi}(Mc_p(m)))=0$; $cores'_{K(\ell m)/K(m)}(\tau_{\ell.\pi})$ est donc définie dans $H^1(K(m), X_M)$. Si $\ell_1,\dots,\ell_k$ sont tous distincts, inertes dans K et totalement décomposés dans $K(m)/K$, posons

$$\tau_{[m;\ell_1,\dots,\ell_k]}(M) = cor'_{K(m\ell_1)/K(m)}(\tau_{[m\ell_1;\ell_2,\dots,\ell_k]})(M)$$

pour M divisant $M_{\ell_1}/c_p(m)$ et $M(m;\ell_2,\dots,\ell_k)/c_p(m)$. Sinon, posons $M(m;\ell_1,\dots,\ell_k)=1$ et $\tau_{[m;\ell_1,\dots,\ell_k]}=0$. On obtient ainsi un système d'Euler d'ordre k tel que si $\ell_1,\dots,\ell_k$ sont inertes dans K et totalement décomposés dans $K(m)/K$,

$$M(m;\ell_1,\dots,\ell_k)\geq pgcd(M_{\ell_1}/c_p(m),\ M(\ell m;\ell_2,\dots,\ell_k)/c_p(m), M(m;\ell_2,\dots,\ell_k)/c_p(m)).$$

En étant plus soigneux, on peut en fait prendre

$$M(m;\ell_1,\dots,\ell_k)\geq pgcd(M_{\ell_1},\ M(\ell m;\ell_2,\dots,\ell_k)/c_p(m), M(m;\ell_2,\dots,\ell_k)/c_p(m)).$$

Théoréme 2.3. Soit τ_m une famille d'Euler non ramifiée vérifiant $M(m)=p^\infty$. Alors, la construction précédente itérée fournit un système d'Euler d'ordre k vérifiant

$$M(m;\ell_1,\dots,\ell_k)\geq pgcd(M_{\ell_1},\ M(\ell m;\ell_2,\dots,\ell_k)/c_p(m), M(m;\ell_2,\dots,\ell_k)/c_p(m)).$$

Si de plus, τ_m vérifie pour tout ℓ premier à $pm\mathfrak{N}_0$

$$(2.4)_\ell \qquad \tau_{\ell m,w}=Fr_\ell^{-1}(\tau_{m,v})$$

pour toute place v de $K(m)$ au dessus de ℓ (ℓ' étant la place de K au dessus de ℓ et w l'unique place de $K(\ell m)$ au dessus de v) et si $\pi=[m;\ell_1,\dots,\ell_k]\in\mathfrak{P}^{(k)}$, alors $M(\pi)\geqslant M_{\ell_1}$ et pour toute place v_{ℓ_j} au dessus de ℓ_j, l'image $\tau_{\pi,v_{\ell_j}}(M)$ de $\tau_\pi(M)$ par localisation en v_{ℓ_j} appartient à

$$\mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(K(\ell_j m)_{v_{\ell_j}}/K(m)_{v_{\ell_j}}),\ X_M(K(m)_{v_{\ell_j}}))$$

et est donnée par la formule

$$(2.5) \qquad \tau_{\pi,v_{\ell_j}}(M)(\delta_{\ell_j})=Fr_{\ell_j}^{-1}\tau_{\varepsilon_j(\pi),v_{\ell_j}}(M)(Fr_{\ell_j}^d)=Fr_{\ell_j}^{-1}(Fr_{\ell_j}^d-1)(\tau_{\varepsilon_j(\pi),v_{\ell_j}}(M)/M)$$

où $\varepsilon_j(\pi)=[m;\ell_1,\dots,\ell_{j-1},\ell_{j+1},\dots\ell_k]$.

Remarquons que si L'/L est une extension totalement ramifiée en v et v' la place de L' au dessus de v, la restriction induit un isomorphisme de $H_f^1(L_v, X_M)$ sur $H_f^1(L'_{w'}, X_M)$ et que le Frobenius agit sur ces modules, ce qui donne un sens aux conditions (2.4). Les conditions imposées dans la définition de $\mathfrak{P}^{(k)}$ impliquent que les applications de Kolyvagin locales cor'_v pour v divisant ℓ_j sont bien définies et que des relations du type $(2.4)_{\ell_j}$ sont vraies pour le système d'Euler d'ordre k. Cela permet de faire le calcul local de τ_π et de montrer (2.5).

On démontre le théorème 2.1 à partir du théorème 2.3 en appliquant le théorème de Cebotarev. En effet dans les deux cas particuliers envisagés, on a exhibé une famille d'Euler non ramifiée ($M(m)=p^\infty$) vérifiant les relations $(2.4)_\ell$. Il s'agit des $(\tau_m)_m$ avec $\tau_m=1-\zeta_m$ (système des unités cyclotomiques: il est en fait non ramifié en dehors de ℓ si m est une puissance de ℓ mais cela se corrige lorsque l'on prend les χ-composantes) et τ_m point de Heegner de niveau m dans le cas modulaire (système des points de Heegner). Pour passer de la formule (2.5) à la formule (2.3), on choisit $\zeta_{M,v}=\zeta_{\delta_\ell}^{(\ell^d-1)/M}$ comme racine de l'unité d'or-

dre M intervenant dans la définition de $\mathfrak{E}_v$ où ζ_{δ_ℓ} est la racine de l'unité d'ordre ℓ^d-1 corespondant à δ_ℓ par l'isomorphisme d'Artin.

Enfin, remarquons que le théorème 2.3 peut se généraliser à une représentation p-adique comme en 2.1. Il ne resterait plus qu'à exhiber une famille d'Euler non ramifiée vérifiant $M(m)=p^\infty$, ce qui est beaucoup plus difficile.

3. Démonstrations des théorèmes 1.1 et 1.3.

3.1. Généralités.

Commençons par donner l'idée générale commune aux démonstrations des théorèmes 1.1, 1.3 (et 1.2). Soit $T_p(X)$ une représentation p-adique comme en 2.1. On désire étudier le groupe de Selmer $S(X'/L)^{(M)}$. Il est facile de construire des caractères de ce groupe: si v est une place de L au dessus de ℓ non ramifiée sur $\mathbb{Q}$ de degré résiduel f et totalement décomposée dans $L(X_M)/L$, si e est un élément de X_M, on note $\xi_{v,e}$ l'élément de $\mathrm{Hom}_{\mathbb{Z}_p}(S(X'/L)^{(M)},\mu_M)$ défini par $\xi_{v,e}(x)=[e, x_v(Fr_\ell^f)]_M$. La formule du produit (2.1) permet d'associer à tout élément de $S_T(X/L)^{(M)}$ une relation entre les caractères $\xi_{v,e}$: choisissons une base (e_i) de $T_p(X)$ et soit $e_i^{(M)}$ la projection de e_i dans X_M ; choisissons une racine de l'unité ζ d'ordre M et posons $(\zeta_{M,v})^{u_v}=\zeta$ (u_v est une unité de $\mathbb{Z}_p$); si τ est un élément de $S_T(X/L)^{(M)}$, posons $\mathfrak{E}_v(\tau)=\sum_{i=1}^d E_{v,i}(\tau)e_i^{(M)}$; on a alors

$$\prod_{i=1}^d \prod_{v\in T} (\xi_{v,e_i})^{u_v E_{v,i}(\tau)} = 1. \tag{3.1}$$

Nous allons utiliser les éléments fabriqués dans le théorème 2.1 pour un choix convenable de k. En reprenant les notations du théorème 2.1, on a ainsi une suite croissante d'ensembles $T_s=\{\ell_1,\dots,\ell_s\}$ et des éléments $\tau_{[m;\ell_1,\dots,\ell_s]} \in S_{T_s}(X/K(m))^{(M)}$ pour $s\leqslant k$. En choisissant bien l'élément h du théorème 2.1, on peut prendre $E_{v_{\ell_s},i}(\tau_{[m;\ell_1,\dots,\ell_s]})$ de valuation p-adique minimale. Remarquons que

les τ_m et τ_π peuvent être divisibles par p dans $S_T(X/L)^{(M)}$.; c'est ce qui fait intervenir l'indice que l'on trouve dans les théorèmes du paragraphe 1 .

3.2. Cas cyclotomique.

Soit χ un caractère pair non trivial de conducteur f ; pour simplifier, on suppose qu'il est à valeurs dans $\mathbb{Z}_p^*$ et on note e_χ le projecteur associé. On peut d'autre part supposer que F est le corps (réel) fixe par le noyau de χ . Kolyvagin démontre alors la proposition suivante.

Proposition 3.1. $\#(A_F^{(\chi)})$ divise $[\mathfrak{C}_F^{(\chi)}: \mathbb{Z}_p e_\chi(N_{\mathbb{Q}(\zeta_f)/F}(1-\zeta_f))]$.

Ici, $N_{\mathbb{Q}(\zeta_f)/F}(1-\zeta_f))=\tau_{F,f}$ est la norme sur F d'un point du système d'Euler que l'on a décrit. On peut facilement voir que $\mathbb{Z}_p e_\chi(N_{\mathbb{Q}(\zeta_f)/F}(1-\zeta_f))$ est égal à $\mathfrak{C}_F^{(\chi)}$. Pour montrer le théorème 1.1, c'est-à-dire l'égalité dans la proposition 3.1, on utilise la formule du nombre de classes que l'on rappelle dans le cas où p ne divise pas $2[F:\mathbb{Q}]$ [34].

Proposition 3.2. On a $\#(A_F)= \prod_{\chi\neq 1} [\mathfrak{C}_F^{(\chi)}: \mathfrak{C}_F^{(\chi)}]$ où le produit est pris sur les caractères χ de $\mathrm{Gal}(F/\mathbb{Q})$ non triviaux.

Dans le cas elliptique, la formule analogue est montrée dans [18]

Revenons à la démonstration de la proposition 3.1. Le choix d'une racine de l'unité ζ permet d'identifier $\mathrm{Hom}_{\mathbb{Z}_p}(S(\mathbb{Z}_p/F)^{(M)}, \mu_M)$ et $A_F = C_F(p)$ (si v est une place de F, la classe $[v]$ de l'idéal associé à v correspond au caractère $\xi_{v,\zeta}$). Soient $p^{n_1(\chi)},\ldots, p^{n_r(\chi)}$ les invariants de $A_F^{(\chi)}$ avec $n_1(\chi)\geq\ldots\geq n_r(\chi)$ et soient $c_1,\ldots c_r$ des éléments de $A_F^{(\chi)}$ tels que c_i soit d'ordre $p^{n_i(\chi)}$ dans $A_F^{(\chi)}/\mathbb{Z}_p c_1 +\ldots \mathbb{Z}_p c_{i-1}$. Si

x appartient à F^*/F^{*M}, on note J(x,M) l'annulateur de x et

$$J'(x,M)=\{a\in\mathbb{Z}_p \text{ tel que } aJ(x,M)\subset M\mathbb{Z}_p\}.$$

Pour M assez grand et $x\in F^*$, la valuation p-adique C(x) de J'(x,M) est le plus grand entier C tel que $x\in F^{*p^C}$. Lorsque $x\in\mathfrak{C}^{(\chi)}$, l'indice de $\mathbb{Z}_p x$ dans $\mathfrak{C}^{(\chi)}$ est égal à $p^{C(x)}$.

On définit $\alpha_v(x)\in\mathbb{Z}/M\mathbb{Z}$ par $(\zeta_{M,v})^{\alpha_v(x)}=(1-Fr_\ell^{-1})(x/M)$. Il s'agit maintenant d'appliquer plusieurs fois le théorème 2.1 en faisant un choix convenable de l'élément h qui assure les propriétés désirées de $[v_{\ell_k}]$ et de la valuation p-adique de $\alpha_{v_k}(e_\chi\tau_{\pi_k})$. Nous ne le faisons pas en détail ici et donnons simplement la suite logique de la démonstration. On choisit $\tilde{M}$ divisible par $\#(A_F)$, $M=\tilde{M}^3$ et k=r.

On choisit ℓ_1 tel que $e_\chi[v_{\ell_1}]=c_1$ et tel que

$$\mathrm{ord}_p(\alpha_{v_{\ell_1}}(e_\chi\tau_f))=C(e_\chi\tau_f)=_{\text{déf}}C_0(\chi)$$

et on pose $\pi_1=[f;\ell_1]$ et $C_1=C(e_\chi\tau_{\pi_1})$. On a donc $C_1\leqslant C_0(\chi)$ et la relation dans $A_F^{(\chi)}/A_F^{(\chi)M}=A_F^{(\chi)}$

$$p^{-C_1}\alpha_{v_1}(e_\chi\tau_f)e_\chi[v_{\ell_1}]=0,$$

d'où l'inégalité $C_0(\chi)-C_1\geqslant n_1(\chi)$. Supposons choisis $\ell_2,\ldots,\ell_{s-1}$ comme dans le théorème 2.1 tels que $e_\chi[v_{\ell_j}]=c_j$ et $C_{j-1}-C_j\geqslant n_j(\chi)$ avec $\pi_j=[f;\ell_1,\ldots\ell_j]$ et $C_j=C(e_\chi\tau_{\pi_j})$. On choisit ℓ_s tel que $e_\chi[v_{\ell_s}]=c_s$ et tel que $\mathrm{ord}_p(\alpha_{v_{\ell_s}}(e_\chi\tau_{\pi_{s-1}}))=C_{s-1}$. On pose $C_s=C(e_\chi\tau_{\pi_s},)$. On a alors dans $A_F^{(\chi)}/\mathbb{Z}_pc_1+\ldots+\mathbb{Z}_pc_{s-1}$

$$p^{-C_s}\alpha_{v_{\ell_s}}(e_\chi\tau_{\pi_{s-1}})[v_{\ell_s}]^{(\chi)}=0$$

d'où $C_{s-1}-C_s\geqslant n_s(\chi)$. On en déduit que $C_0(\chi)\geqslant n_1(\chi)+\ldots+n_r(\chi)=\#(A_F^{(\chi)})$.

Kolyvagin caractérise un certain sous-ensemble de suites $[f;\ell_1,\ldots,\ell_r]$ à partir desquelles on peut déterminer le rang et les invariants du groupe abélien $A_F^{(\chi)}$. Ce sous-ensemble est construit par récurrence en même temps qu'une suite

d'entiers $C_0(\chi)>\ldots> C_r(\chi)$. L'entier $C_0(\chi)$ est celui déjà défini. Choisissons M suffisamment grand ($\geqslant 3C_0(\chi)$ par exemple). Supposons construits les $C_i(\chi)$ et les ℓ_i pour $i\leqslant s$. On note $\pi_i=[f;\ell_1,\ldots\ell_i]$. Pour tout nombre premier ℓ ne divisant pas $pf\ell_1..\ell_s$ totalement décomposé dans $F(\mu_M)$, on pose

$$C(\pi_s,\ell)= \mathrm{ord}_p(J'(e_\chi \tau_{[\pi_s,\ell]}(M),M)).$$

On montre qu'il existe un nombre premier ℓ totalement décomposé dans $F(\mu_M)$ et tel que

$$\mathrm{ord}_p(\alpha_{v_\ell}(e_\chi \tau_{\pi_s}(M)))=C_s(\chi) \text{ et } \mathrm{ord}_p(\alpha_{v_\ell}(e_\chi \tau_{\pi_j}(M)))>C_j(\chi) \text{ pour } 0\leqslant j\leqslant s-1 .$$

On note $C_{s+1}(\chi)$ la borne inférieure des $C(\pi_s,\ell)$ pour ℓ vérifiant ces conditions et on choisit pour ℓ_{s+1} n'importe lequel des nombres premiers ℓ pour lesquels la borne inférieure est atteinte. Nous avons alors les propriétés suivantes

(i) $C_{s+1}(\chi)\leqslant C_s(\chi)$;

(ii) si $C_{s+1}(\chi)<C_s(\chi)$, alors $n_{s+1}(\chi)=C_s(\chi)-C_{s+1}(\chi)$

(iii) si $C_{s+1}(\chi)=C_s(\chi)$, alors s est le $\mathbb{Z}/p\mathbb{Z}$-rang de $A_F^{(\chi)}/A_F^{(\chi)p}$ $(s=r)$ et l'on a

$$n_1(\chi)=C_0(\chi)-C_1(\chi),\ n_2(\chi)=C_1(\chi)-C_2(\chi),\ n_s(\chi)=C_{s-1}(\chi)-C_s(\chi);$$

De plus si v_{ℓ_i} est une place de F au dessus de ℓ_i, l'homomorphisme

$$\mathbb{Z}^s \to A_F^{(\chi)}$$

$$(\alpha_1,\ldots,\alpha_s) \mapsto \sum \alpha_i\ e_\chi[v_{\ell_i}]$$

a comme noyau $p^{n_1}\mathbb{Z}\times\ldots p^{n_s}\mathbb{Z}$ et est surjectif pour $s=r$. Enfin, on peut écrire $e_\chi \tau_{\pi_i}(M)=y_i^{p^{C_i(\chi)}}$ dans $F^\times/F^{\times M}$ et les $y_1,\ldots,y_r$ sont linéairement indépendants dans $F^\times/F^{\times p}$.

3.3. Démonstration du théorème 1.3.

Soit $c=\#(E(K)_{tors})$. Soit t_p la p-partie du nombre de Tamagawa. Si P est un point d'ordre infini de $E(K)$, soit $C(P)$ le plus grand entier qui divise P

dans $E(K)/E(K)_{tors}$. Lorsque $E(K)$ est de rang 1, $C(P)$ est l'indice de $\mathbb{Z}P$ dans $E(K)/E(K)_{tors}$.

Lemme 3.3. Il existe un entier a tel que, pour tout nombre premier p et pour tous entiers n et m, le groupe $H^1(K(E_{p^{n+m}})/K, E_{p^n})$ est annulé par a. Il existe un entier b' tel que b'A est nul pour tout sous-module galoisien A de E_{p^n} tel que $(\sigma+1)A=0$ ou $(\sigma-1)A=0$ (on posera $b=2b'$).

La démonstration utilise la théorie de la multiplication complexe et le résultat suivant dû à Serre [53]: si E n'est pas à multiplication complexe, le groupe de Galois de $\mathbb{Q}(E_p)/\mathbb{Q}$ est isomorphe à $Gl_2(\mathbb{Z}/p\mathbb{Z})$ pour p suffisamment grand. Les facteurs premiers de ab appartiennent à S_E (th. 1.3).

Rappelons que le groupe de Selmer $S(F)^{(M)} = S(T_p(E)/F)^{(M)}$ est lié au groupe de Shafarevich-Tate par la suite exacte

$$0 \to E(F)/ME(F) \to S(F)^{(M)} \to Ш(E/F)_M \to 0.$$

On note $S(K)^{(M)(\pm)}$, $Ш(E/K)^{(\pm)}$ les espaces propres relatifs à ± 1 pour la conjugaison complexe σ de $S(K)^{(M)}$ et de $Ш(E/K)$. On choisit une base $e_\pm$ de $2T_p(E)$ telle que $\sigma e_\pm = \pm e_\pm$ et on note $e_\pm^{(M)}$ leurs projections dans $E_M^\pm$. Si ℓ est inerte dans K totalement décomposé dans $K(E_M)/K$, on note $\xi_{\alpha\ell}$ (pour $\alpha \in \{+,-\}$) le caractère $\xi_{\ell,e}$ pour $e = e_{-\alpha}^{(M)} \in E_M$ défini dans le paragraphe 3.1 (on a ici $f=2$) : $\xi_{\pm\ell} \in \mathrm{Hom}_{\mathbb{Z}_p}(S(K)^{(M)(\pm)}, \mu_M)$.

Plus généralement, si x est un élément de $H^1(K, E_M)$, on pose pour $\alpha \in \{+,-\}$

$$\eta_\ell^\alpha(x) = [x_v(Fr_\ell^2), e_{-\alpha}^{(M)}]_M .$$

La restriction de $\eta_\ell^\pm$ à $S(K)^{(M)(\pm)}$ est donc $\xi_{\pm\ell}$. On note ξ_0 le caractère trivial.

Soient $\ell_1, \ldots, \ell_{k-1}$ des nombres premiers inertes dans K totalement dé-

composés dans $K(E_M)/K$. On note $Y_M(\ell_1,\dots,\ell_{k-1})$ le sous-groupe de $\mathrm{Hom}_{\mathbb{Z}_p}(S(K)^{(M)((-1)^k\varepsilon)}, \mu_M)$ engendré par les caractères $\xi_{(-1)^k\varepsilon\ell_{k-1}},\dots,\xi_{(-1)^k\varepsilon\ell_1},\xi_0$ et on pose

$$\cdot\ Z_M(\ell_1,\dots,\ell_{k-1})=\mathrm{Hom}_{\mathbb{Z}_p}(S(K)^{(M)((-1)^k\varepsilon)}, \mu_M)/Y_M(\ell_1,\dots,\ell_{k-1}).$$

Si ξ est un élément de $\mathrm{Hom}_{\mathbb{Z}_p}(S(K)^{(M)((-1)^k\varepsilon)}, \mu_M)$, on note $\mathrm{ord}_{p,Z_M(\ell_1,\dots,\ell_{k-1})}(\xi)$ la valuation p-adique de l'ordre de ξ dans $Z_M(\ell_1,\dots,\ell_{k-1})$.

Enfin, donnons quelques propriétés des points de Heegner et du système d'Euler associé. Si π est de niveau 1, τ_π est défini sur $K(1)$. Si σ est la conjugaison complexe et si ε est la valeur propre de l'involution d'Atkin-Lehner agissant sur la forme modulaire f associée à E, on a

$$\sigma(\mathrm{cores}_{K(1)/K}(\tau_\pi))=(-1)^k\varepsilon\,\mathrm{cores}_{K(1)/K}(\tau_\pi) \text{ modulo torsion}$$

où $\pi=[1;\ell_1,\dots,\ell_k]$ (le cas des points de Heegner est bien connu [24], le cas d'ordre quelconque s'en déduit par récurrence en revenant à la définition de τ_π). Le point $\tau_{\pi,K}=(\sigma+(-1)^k\varepsilon)\mathrm{cores}_{K(1)/K}(\tau_\pi)$ est défini sur K et vérifie

$$\sigma\tau_{\pi,K}=(-1)^k\varepsilon\tau_{\pi,K}.$$

En particulier, $\tau_{1,K}=\tau_{[1],K}$ est un point de $E(K)$.

Théorème 3.4. *On suppose que le point de Heegner $\tau_{1,K}$ est d'ordre infini. Fixons un entier r. Soit $M=p^n$ une puissance de p telle que*

$$n\geqslant \mathrm{ord}_p(C(\tau_{1,K}))+r\,\mathrm{ord}_p(abc)+2\mathrm{ord}_p(2c)+1.$$

Il existe des nombres premiers $\ell_1,\dots,\ell_r$ inertes dans K totalement décomposés dans $K(E_M)/K$ tels que $[1;\ell_1,\dots,\ell_r]\in\mathfrak{P}^{(r)}$ et $M^3t_p\mid M_{\ell_1}$ et des entiers n_k vérifiant

$$n_0=\mathrm{ord}_p(C(\tau_{1,K})),\ 0\leqslant n_k\leqslant n,\ -\mathrm{ord}_p(abc)\leqslant n_{k-1}-n_k \text{ pour } k\geqslant 1$$

tels que l'on ait les inégalités

(3.2) $$0\leqslant \mathrm{ord}_p(\mathrm{exposant}(Z_M(\ell_1,\ell_2,\dots,\ell_{k-1})))-\mathrm{ord}_{p,Z_M(\ell_1,\dots,\ell_{k-1})}(\xi_{(-1)^k\varepsilon\ell_k})\leqslant \mathrm{ord}_p(ab)$$

(3.3) $$\mathrm{ord}_{p,Z_M(\ell_1,\dots,\ell_{k-1})}(\xi_{(-1)^k\varepsilon\ell_k}) \leqslant n_{k-1}-n_k+2\mathrm{ord}_p(2abc).$$

L'ordre de $\tau_{[1;\ell_1,\dots,\ell_j],K}(M)$ est égal à M/p^{n_j} et il existe un élément $\tau'_{[1;\ell_1,\dots,\ell_j]}(M)$ de $S_{\{\ell_1,\dots,\ell_j\}}(K)^{(M)}$ tel que

(3.4) $$c\tau_{[1;\ell_1,\dots,\ell_j],K}(M) = p^{n_j}\tau'_{[1;\ell_1,\dots,\ell_j]}(M)$$

et tel que $\eta_{(-1)^{k-1}\varepsilon\ell_k}(\tau'_{[1;\ell_1,\dots,\ell_{k-1}]}(M))$ soit une racine de l'unité d'ordre p^β avec

(3.5) $$n-\mathrm{ord}_p(abc)\leqslant\beta\leqslant n-\mathrm{ord}_p(c).$$

On déduit facilement du théorème 3.4 les résultats annoncés.

Corollaire 3.5. Si le point de Heegner $\tau_{1,K}$ est d'ordre infini, $Ш(E/K)^{(-\varepsilon)}$ est fini et annulé par $4(ab)^3c^2C(\tau_{1,K})$.

Démonstration. On utilise le théorème 3.4 avec $r=1$. Le groupe $Z_M = S(K)^{(M)(-\varepsilon)}$ est annulé par $2p^{n_0-n_1}(ab)^3c^2$ et donc par $2(ab)^3c^2\,C(\tau_{1,K})$. On en déduit que $4(ab)^3c^2\,C(\tau_{1,K})$ annule $Ш(E/K)^{(-\varepsilon)}$. Comme $Ш(E/K)^{(-\varepsilon)}$ est de type fini sur $\mathbb{Z}$, il est donc fini.

Corollaire 3.6. Si le point de Heegner $\tau_{1,K}$ est d'ordre infini, $E(K)$ est de rang 1, $Ш(E/K)$ est fini et annulé par $4d(ab)^5c^2C(\tau_{1,K})$.

Démonstration. On utilise ici le théorème 3.4 avec $r=2$ afin de contrôler $Ш(E/K)^{(\varepsilon)}$. Ainsi $2p^{n_1-n_2}(ab)^3c^2$ (donc $2(ab)^4c^2\,C(\tau_{1,K})$) annule $Z_M(\ell_1) = \mathrm{Hom}_{\mathbb{Z}_p}(S(K)^{(M)(\varepsilon)},\mu_M)/(\chi_{\varepsilon\ell_1})$ et donc $\ker\xi_{\varepsilon\ell_1}$. Mais $\xi_{\varepsilon\ell_1}(\tau'_1)$ est d'ordre p^γ avec $n-\mathrm{ord}_p(abc)\leqslant\gamma\leqslant n-\mathrm{ord}_p(c)$. On en déduit que $S(K)^{(M)(\varepsilon)}/\langle\ker\xi_{\varepsilon\ell_1},\tau'_1\rangle$ est un groupe cyclique annulé par abc et que $2(abc)(ab)^4c^2C(\tau_{1,K})$ annule $S(K)^{(M)}/\langle\tau'_1\rangle$. Donc $S(K)^{(M)\varepsilon}$ est de rang 1. On voit (lemme 3.8) qu'il existe $\tau\in E(K)$ tel que $c\tau=\tau'_1$

et on a alors $E(K)=E(K)_{tor}+\mathbb{Z}\tau$. Donc $S(K)^{(M)}/<\tau>+E(K)_{tor}$ est égal à $Ш(E/K)_M$. Ainsi, $4(ab)^5c^3C(\tau_{1,K})$ annule $Ш(E/K)$ qui est en particulier un groupe fini.

Corollaire 3.7. Supposons que p ne divise pas 2abc. Si le point de Heegner $\tau_{1,K}$ est d'ordre infini, le cardinal de $Ш(E/K)$ divise $C(\tau_{1,K})^2$.

Démonstration. On applique le théorème avec r supérieur à 2 fois le rang sur $\mathbb{Z}/p\mathbb{Z}$ de $Ш(E/K)^{(\pm)}$.

On peut déduire du théorème 3.4 une estimation du cardinal de $Ш(E/K)$ pour les nombres premiers p divisant 2abc.

On démontre facilement le lemme suivant qui est en fait le cas r=0 du théorème.

Lemme 3.8. Si $n\geqslant ord_p(cC(\tau_{1,K}))+1$, l'annulateur de $\tau_{1,K}$ modulo $p^nE(K)$ est de valuation p-adique $n-ord_p(C(\tau_{1,K}))$, c'est-à-dire que $n_0=ord_p(C(\tau_{1,K}))$. Il existe un point τ'_1 de $E(K)$ tel que $c\tau_{1,K}=p^{n_0}\tau'_1$.

Commençons la démonstration du théorème 3.4 en supposant p impair. Elle se fait par récurrence sur r. Supposons le théorème vrai pour r-1. On pose $\pi_{r-1}=[1;\ell_1,\dots,\ell_{r-1}]$ et lorsque ℓ_r sera choisi, $\pi_r=[1;\ell_1,\dots,\ell_r]$. Il s'agit de bien choisir le h du théorème 2.1. Il est facile de vérifier que $\tau'_{\pi_{r-1}}(M)$ est d'ordre $Mp^{-ord_p(c)}=p^{n-ord_p(c)}$.

On définit un sous-groupe $S_\pm$ de $S_{(\ell_1,\dots\ell_{r-1})}(K)^{(M)(\pm)}$ par

$$S_{(-1)^{r-1}\varepsilon}=\mathbb{Z}_p\tau'_{\pi_{r-1}}(M) \text{ et } S_{(-1)^r\varepsilon}=S(K)^{(M)((-1)^r\varepsilon)}.$$

On pose $Y_{M,r}=Y_M(\ell_1,\dots,\ell_{r-1})$ et $Z_{M,r}=Z_M(\ell_1,\dots,\ell_{r-1})$.

On choisit un entier M' assez grand (tel que M^3t_p (resp.

$M_0(m,\ell_1,\ldots\ell_k)M_{\ell_k}$) divise M' si $r=1$ (resp. $r>1$)).

Soit $S'_\pm$ l'image de $S_\pm$ dans $H^1(K(E_{M'}), E_M)$ par l'homomorphisme de restriction. Comme M divise M', ce dernier groupe est isomorphe à $\mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(\overline{K}/K(E_{M'})), E_M)$. Soit $F_\pm$ la plus petite extension de $K(E_{M'})$ telle que $S'_\pm$ soit contenu dans $\mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(F_\pm/K(E_{M'})), E_M)$. On pose

$$F=F_+F_-\ ,\ H_\pm=\mathrm{Gal}(F_\pm/K(E_{M'}))\ ,\ H=\mathrm{Gal}(F/K(E_{M'}))\ .$$

On a donc

$$S'_\pm \subset \mathrm{Hom}_{\mathbb{Z}_p}(H_\pm,E_M) \subset \mathrm{Hom}_{\mathbb{Z}_p}(H,E_M).$$

On définit un homomorphisme $\varphi_\pm : H \to \mathrm{Hom}_{\mathbb{Z}_p}(S'_\pm,\mu_M)$ par

$$\varphi_\alpha(h)(x)=[x(hh^\sigma),e_{-\alpha}^{(M)}]_M\ .$$

Soit $\psi_\pm$ le composé de $\varphi_\pm$ avec l'homomorphisme induit par la restriction

$$\mathrm{Hom}_{\mathbb{Z}_p}(S'_\pm,\mu_M) \to \mathrm{Hom}_{\mathbb{Z}_p}(S_\pm,\mu_M).$$

Le lemme suivant utilise le lemme 3.3.

Lemme 3.9. $\varphi_\pm(H) \supset b\,\mathrm{Hom}_{\mathbb{Z}_p}(S'_\pm,\mu_M)$ et ab annule $\mathrm{Hom}_{\mathbb{Z}_p}(S_\pm,\mu_M)/\psi_\pm(H)$.

Lemme 3.10. Il existe un élément η de H tel que l'ordre de $\psi_{(-1)^r\varepsilon}(\eta)$ (resp. $\psi_{(-1)^{r-1}\varepsilon}(\eta)$) dans $\psi_{(-1)^r\varepsilon}(H)/Y_{M,r}\cap\psi_{(-1)^r\varepsilon}(H)$ (resp. dans $\psi_{(-1)^{r-1}\varepsilon}(H)$) soit égal à l'exposant de $\psi_{(-1)^r\varepsilon}(H)/Y_{M,r}\cap\psi_{(-1)^r\varepsilon}(H)$ (resp. de $\psi_{(-1)^{r-1}\varepsilon}(H)$).

Pour montrer l'existence de η, on utilise la propriété que la réunion de deux sous-groupes de H distincts de H est strictement contenue dans H.

Corollaire 3.11. On a les inégalités

$$n-\mathrm{ord}_p(abc)\leqslant \mathrm{ord}_p(\text{ordre } \psi_{(-1)^{r-1}\varepsilon}(\eta))\leqslant n-\mathrm{ord}_p(c)$$

$$\mathrm{ord}_p(\text{exposant } Z_{M,r})-\mathrm{ord}_p(ab)\leqslant \mathrm{ord}_{p,Z_{M,r}}(\psi_{(-1)^r\varepsilon}(\eta))\ .$$

Fixons maintenant un tel η et posons $h=\eta\sigma$. Choisissons un nombre premier ℓ_r comme dans le théorème 2.1 tel que le Frobenius de ℓ_r dans $F/\mathbb{Q}$ soit h. Comme $\eta\eta^{\sigma}=(\eta\sigma)^2=Fr_{\ell}^2$ (σ est d'ordre 2), $\psi_{(-1)^r\varepsilon}(\eta)$ et $\xi_{(-1)^r\varepsilon\ell_r}$ coincident et on a

$$\psi_{(-1)^{r-1}\varepsilon}(\eta)(\tau'_{\pi_{r-1}})=\eta_{(-1)^{r-1}\varepsilon\ell_r}(\tau'_{\pi_{r-1}}).$$

L'ordre p^{β} de ce dernier élément vérifie donc

$$n-ord_p(abc)\leqslant\beta\leqslant n-ord_p(c).$$

Cela montre les propriétés (3.2) et (3.5).

L'ordre de $\tau_{\pi_r}(M)$ est par définition M/p^{n_r}. Il est facile de voir que $\tau_{\pi_r}(M')$ est divisible par p^{n_r} dans $H^1(K,E_{M'})$: $\tau_{\pi_r}(M')=p^{n_r}\tau'_{\pi_r}(M'p^{-n_r})$. On vérifie que par projection dans $H^1(K,E_M)$, $\tau'_{\pi_r}(M)$ appartient à $S_{\{\ell_1,\dots\ell_j\}}(K)^{(M)}$.

Nous allons maintenant montrer que $n_{r-1}-n_r\geqslant -ord_p(abc)$. Rappelons que l'on a

$$\psi_{(-1)^{r-1}\varepsilon}(\eta)(x)=[(Fr_{\ell_r}^2-1)(x/M),e^{(M)}_{(-1)^r\varepsilon}]_M$$

pour tout x appartenant au sous-groupe engendré par $\tau'_{\pi_{r-1}}(M)$ et que d'après le corollaire 3.11,

$$n-ord_p(abc)\leqslant ord_p(\text{ordre } \psi_{(-1)^{r-1}\varepsilon}(\eta))\leqslant n-ord_p(c).$$

On en déduit que $(Fr_{\ell_r}^2-1)(\tau'_{\pi_{r-1}}(M)/M)$ est d'ordre p^{β} avec

$$n-ord_p(abc)\leqslant\beta\leqslant n-ord_p(c).$$

En utilisant les relations (2.3) du théorème 2.1 et le fait que Fr_{ℓ_r} et la conjugaison complexe coincident sur K, on trouve que si v_r est la place de K au dessus de ℓ_r

$$p^{n_r}\mathfrak{S}_{v_r}(\tau'_{\pi_r}(M))=(-1)^r\varepsilon p^{n_{r-1}}(Fr_{\ell_r}^2-1)(\tau'_{\pi_{r-1}}(M)/M).$$

Les deux termes sont des multiples de $e^{(M)}_{(-1)^{r-1}\varepsilon}$. On en déduit que

$n_r \leqslant n_{r-1} + n - \beta$ (car p^{n_r} divise M). D'où $n_{r-1} - n_r \geqslant -\mathrm{ord}_p(abc)$. La relation précédente devient alors

$$\mathfrak{C}_{v_r}(abc\tau'_{\pi_r}(M)) = (-1)^r \varepsilon(Fr^2_{\ell_r} - 1)(abcp^{n_{r-1}-n_r}\tau'_{\pi_{r-1}}(M)/M).$$

Si l'on pose

$$\mathfrak{C}_{v_k}(abc\tau'_{\pi_r}(M)) = E_k e_{(-1)^{r-1}\varepsilon},$$

on a $\mathrm{ord}_p(E_r) \leqslant (n_{r-1} - n_r) + 2\mathrm{ord}_p(abc)$. La relation (3.1) pour $\tau = abc\tau'_{\pi_r}(M)$ devient

$$\prod_{k=1}^{r} (\xi_{(-1)^r \varepsilon \ell_k})^{u_k E_k} = 1$$

et on en déduit que $\mathrm{ord}_{p, Z_M(\ell_1, \ldots, \ell_{r-1})}(\xi_{(-1)^r \varepsilon \ell_r}) \leqslant n_{r-1} - n_r + 2\mathrm{ord}_p(abc)$ (relation (3.3)). Cela termine la démonstration du théorème 3.4.

Références

[1] B. Birch. Diophantine analysis and modular functions, Proceedings of Bombay Colloquium on Algebraic Geometry (1968), 35-42.

[2] B. Birch. Elliptic curves and modular functions, Symposia Mathematica (1970), 27-32.

[3] B. Birch. Heegner points of elliptic curves, Symposia Mathematica (1975), 441-445.

[4] B. Birch et N. Stephens. Heegner's construction of points on the curve $y^2 = x^3 - 1728e^3$. Séminaire de théorie des nombres. Paris 1981-1982, Progress in Math. 38. Birkhäuser (1983), 1-19.

[5] B. Birch et H. Swinnerton-Dyer. Notes on elliptic curves II J. reine u. Angew. Math. 218 (1965), 79-108.

[6] S. Bloch et K. Kato. L-functions and Tamagawa nombers of motives, Grothendieck Festschrift, Progress in Math., Birkhaüser Boston.

[7] A. Brumer. Travaux récents d'Iwasawa et Leopoldt, Séminaire Bourbaki n° 325 (1966/1967).

[8] D. Bump, S. Friedberg et J. Hoffstein. A non vanishing theorem for derivatives of automorphic L-functions with applications to elliptic curves, Bull.

AMS. Math. Soc. 21 (1989), 89-93.

[9] J. Coates. p-adic L functions and Iwasawa's theory, in Algebraic Number Fields, édité par A. Fröhlich, Academic Press (1977), 269-353.

[10] J. Coates. The work of Mazur and Wiles on cyclotomic fields, Séminaire Bourbaki, n° 574 (1980-1981).

[11] J. Coates. On p-adic L-functions, Séminaire Bourbaki, n° 701 (1988-1989).

[12] J. Coates et C. Goldstein. Some remarks on the main conjecture for elliptic curves with complex multiplication, Am. Journal of Math. 105 (1983), 337-366.

[13] J. Coates et A. Wiles. On the conjecture of Birch and Swinnerton-Dyer, Invent. Math. 39 (1977), 223-251.

[14] J. Coates et A. Wiles. On p-adic L-functions and elliptic units, J. Austral. Math. Soc. (Series A) 26 (1978), 1-25.

[15] J.-M. Fontaine. Représentations p-adiques, Proc. Int. Cong. Math, Varszawa (1983), 475-486.

[16] R. Gillard. Unités cyclotomiques, unités semi-locales et $\mathbb{Z}_\ell$-extensions, Ann. Inst. Fourier 29,1 (1979), 49-79 et 29,4 (1979), 1-15.

[17] R. Gillard. Unités elliptiques et unités cyclotomiques, Math. Ann. 243 (1979), 181-189.

[18] R. Gillard et G. Robert. Groupes d'unités elliptiques, Bull. SMF 107 (1979), 305-317.

[19] G. Gras. Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés, Ann. Inst. Fourier 27 (1977), 1-66.

[20] R. Greenberg. On p-adic L-functions and cyclotomic fields, Nagoya Math. J. 56 (1975), 61-77 et 67 (1977), 139-158.

[21] R. Greenberg. Iwasawa's theory and p-adic L-functions for imaginary quadratic fields, dans Number theory related to Fermat's last theorem, édité par N. Koblitz, Progress in Math. 26, Birkhäuser (1982), 275-285.

[22] R. Greenberg. On the Birch et Swinnerton-Dyer conjecture, Invent. Math. 72 (1983), 241-265.

[23] R. Greenberg. Iwasawa theory for p-adic representations, Adv. Stud. Pure Math. 17 (1989).

[24] B.H. Gross. Heegner points on $X_0(N)$, dans Modular forms, édité par R.A. Rankin, Ellis Horwood Limited (1984), 87-105.

[25] B.H. Gross. Kolyvagin's work on modular elliptic curves (prépublication).

[26] B.H. Gross et D. Zagier. Heegner points et derivatives of L-series, Invent. Math. 84 (1986), 225-320.

[27] K. Iwasawa, On p-adic L functions, Ann. of Math. 89, (1969), 198-205.

[28] K. Iwasawa. Lectures on p-adic L-functions, Ann. Math. Studies 74, Princeton University Press (1972)

[29] K. Iwasawa, On $\mathbb{Z}_\ell$-extensions of algebraic number fields, Ann. of Math. 98 (1973), 246-326.

[30] N. Katz. p-adic L-functions for C.M. fields, Invent. Math. 49 (1978),199-297.

[31] V.A. Kolyvagin. Finiteness of $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ for a subclass of Weil curves, Izv. Akad. Nauk. SSSR Ser Mat. 52 (3) (1988), 522-540; Math. USSR Izvestiya 32 (1989), 523-541.

[32] V.A. Kolyvagin. On the Mordell-Weil group and the Shafarevich-Tate group of Weil elliptic curves, Izv. Akad. Nauk. SSSR Ser Mat. 52 (6) (1988),1154-1179.

[33] V.A. Kolyvagin. Euler systems, Grothendieck Festschrift, Progress in Math., Birkhaüser Boston.

[34] S. Lang. Cyclotomic fields I-II avec appendice de K. Rubin. GTM 121 ($2^{ième}$ édition) (1989), Springer Berlin.

[35] B. Mazur. Courbes elliptiques et symbole modulaire, Séminaire Bourbaki 414 (1971/1972), dans L. N. in Math. 317, Springer Berlin.

[36] B. Mazur. Modular curves and arithmetic, Proc. Int. Congress Math. (1983), Warszawa, 185-211.

[37] B. Mazur et P. Swinnerton-Dyer. Arithmetic of Weil curves, Invent. Math. 25 (1974), 1-61.

[38] B. Mazur et A. Wiles. Class fields of abelian extensions of $\mathbb{Q}$, Invent. Math. 76 (1984), 179-330.

[39] M. Ram Murty et V. Kumar Murty. Mean values of derivatives of modular L-series, prépublication (1989).

[40] B. Perrin-Riou. Arithmétique des courbes elliptiques et théorie d'Iwasawa, Mémoire de de la S.M.F. n° 17. Suppl. au Bull. de la S.M.F. 112 (1984).

[41] B. Perrin-Riou. Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner, Bull. Soc. Math. France, 115 (1987), 399-456.

[42] B. Perrin-Riou. Dérivées de fonctions L p-adiques et points de Heegner, Invent. Math. 89 (1987), 456-510.

[43] K. Ribet. A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, Invent. Math. 34 (1976), 151-162.

[44] G. Robert. Unités elliptiques, Bull. Soc. Math. France, mémoire 36 (1973).

[45] G. Robert. Nombres de Hurwitz et unités elliptiques, Ann. Sc. ENS (4) 11 (1978), 297-389.

[46] D. E. Rohrlich. On L-functions of elliptic curves and cyclotomic towers, Invent. Math. 75 (1984), 383-408 et 409-423.

[47] K. Rubin. Global units and ideal class groups, Invent. Math. 89 (1987), 511-526.

[48] K. Rubin. Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication, Invent. Math. 89 (1987), 527-560.

[49] K. Rubin. On the main conjecture of Iwasawa theory for imaginary quadratic fields, Invent. 93 (1988) 701-719 .

[50] K. Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields (1990).

[51] J.-P. Serre. Classes des corps cyclotomiques, d'après Iwasawa, Séminaire Bourbaki 174 (1958/1959).

[52] J.-P. Serre. Cohomologie galoisienne, Lectures Notes in Math 5 (1973), Springer Berlin.

[53] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. 15 (1972), 259-331.

[54] E. de Shalit. The Iwasawa theory of elliptic curves with complex multiplication, Perspec. in Math. 3, Orlando: Academic Press (1987).

[55] J. Tate. The arithmetic of elliptic curves, Invent. Math. 23 (1974), 179-206.

[56] F. Thaine. On the ideal class groups of real number fields, Ann. of Math. 128 (1987), 1-18.

[57] J.-L. Waldspurger. Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie, Comp. Math. 54 (1985), 173-242.

[58] A. Wiles. Higher explicit reciprocity laws, Ann. Math. 107 (1978), 235-254.

[59] A. Wiles. On p-adic representations for totally real fields, Ann. Math. 123 (1986), 407-456.

[60] R. Yager. On two variables p-adic L functions, Ann. Math. 115 (1982), 411-449.

[61] R. Yager. p-adic measures on Galois groups, Invent. Math. 76 (1984), 331-343.

Bernadette PERRIN-RIOU
Université Pierre et Marie Curie
UFR 21, LMF 45-46, 3ième étage
4 place Jussieu
F-75230 PARIS CEDEX 05