Séminaire BOURBAKI Juin 2003
55e année, 2002-2003, nO 919, p. 251 à 319

LA CONJECTURE DE BIRCH ET SWINNERTON-DYER p-ADIQUE

par **Pierre COLMEZ**

NOTATIONS

Dans tout l'article, $\overline{\mathbf{Q}}$ désigne la clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$ et un plongement de $\overline{\mathbf{Q}}$ dans $\overline{\mathbf{Q}}_p$ est fixé ; en particulier, $\mathscr{G}_{\mathbf{Q}_p} = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ est un sous-groupe bien déterminé de $\mathscr{G}_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. On note χ_{cycl} le caractère cyclotomique. Si $\mathrm{M} \geqslant 1$ est un entier, on note $\zeta_{\mathrm{M}} \in \overline{\mathbf{Q}}$ la racine de l'unité $\exp(\frac{2i\pi}{\mathrm{M}})$.

0. INTRODUCTION

Si $\mathbb{M}$ est un motif défini sur un corps de nombres, on sait lui associer (au moins conjecturalement) une fonction analytique complexe $\mathrm{L}(\mathbb{M}, s)$ définie par un produit eulérien convergeant dans un demi-plan. La quantité d'information arithmétique contenue dans les valeurs aux entiers de ces fonctions L est absolument fascinante, et on dispose d'un faisceau de conjectures la décrivant (conjectures de Deligne [63], de Beilinson [7, 177, 160], et de Bloch-Kato [27, 74, 76]). Ces conjectures sont de lointaines descendantes de la conjecture de Birch et Swinnerton-Dyer [25, 26, 183], elle-même inspirée par la formule analytique du nombre de classes d'idéaux qui reste le seul cas général que l'on sache traiter. En p-adique, on a plus de mal à définir les fonctions L mais, une fois définies, celles-ci livrent un peu plus facilement l'information qu'elles contiennent comme nous le verrons dans ce texte pour les fonctions L p-adiques de courbes elliptiques définies sur $\mathbf{Q}$ ou, plus généralement, de formes modulaires.

0.1. La formule analytique du nombre de classes

Soit K un corps de nombres d'anneau des entiers $\mathscr{O}_{\mathrm{K}}$. La fonction zêta de Dedekind ζ_{K} de K est définie, pour $\mathrm{Re}(s) > 1$, par le produit eulérien $\zeta_{\mathrm{K}}(s) = \prod_{\mathfrak{p}} \frac{1}{1-\mathrm{N}\mathfrak{p}^{-s}}$, le produit portant sur les idéaux maximaux de $\mathscr{O}_{\mathrm{K}}$, et possède un prolongement à $\mathbf{C}$ tout entier, holomorphe en dehors d'un pôle simple en $s = 1$. On dispose des résultats suivants :

THÉORÈME 0.1. — (i) *Le groupe $\mathscr{O}_{\mathrm{K}}^*$ des unités de $\mathscr{O}_{\mathrm{K}}$ est de type fini sur* $\mathbf{Z}$. *Son rang $r(\mathrm{K})$ est égal à $r_1 + r_2 - 1$, où r_1 est le nombre de places réelles de* K *et r_2 le nombre de ses places complexes.*

(ii) *Le régulateur*[1] $\mathrm{R}_\infty(\mathrm{K})$ *est non nul.*

THÉORÈME 0.2. — *Le groupe* $\mathrm{Pic}(\mathscr{O}_{\mathrm{K}})$ *des classes d'idéaux de $\mathscr{O}_{\mathrm{K}}$ est un groupe fini.*

THÉORÈME 0.3. — *La fonction $\zeta_{\mathrm{K}}(s)$ a, en $s = 0$, un zéro d'ordre $r(\mathrm{K})$ et on a*

$$\lim_{s\to 0} s^{-r(\mathrm{K})}\zeta_{\mathrm{K}}(s) = -|\mathrm{Pic}(\mathscr{O}_{\mathrm{K}})| \cdot \mathrm{R}_\infty(\mathrm{K}).$$

0.2. La conjecture de Birch et Swinnerton-Dyer

Soit E une courbe elliptique définie[2] sur $\mathbf{Q}$ de conducteur N_{E}. Si p est un nombre premier, on définit l'entier a_p par :

• si $p^2 \mid \mathrm{N}_{\mathrm{E}}$ (*i.e.* si E a réduction additive en p), alors $a_p = 0$;

• si $p \mid \mathrm{N}_{\mathrm{E}}$ et $p^2 \nmid \mathrm{N}_{\mathrm{E}}$ (*i.e.* si E a réduction multiplicative en p), alors $a_p = 1$ (resp. $a_p = -1$) si E a réduction multiplicative déployée (resp. non déployée) ;

• si $p \nmid \mathrm{N}_{\mathrm{E}}$ (*i.e.* si E a bonne réduction en p), alors $a_p = p + 1 - |\mathrm{E}(\mathbf{F}_p)|$.

Ceci nous permet de définir la fonction L complexe $\mathrm{L}(\mathrm{E}, s)$ attachée à E par le produit eulérien (convergeant pour $\mathrm{Re}(s) > 3/2$ car $|a_p| \leqslant 2\sqrt{p}$ d'après le théorème de Hasse) :

$$\mathrm{L}(\mathrm{E}, s) = \prod_{p\nmid \mathrm{N}_{\mathrm{E}}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p\mid \mathrm{N}_{\mathrm{E}}} \frac{1}{1 - a_p p^{-s}} = \sum_{n=1}^{+\infty} a_n n^{-s}.$$

La fonction $\mathrm{L}(\mathrm{E}, s)$ est holomorphe sur le demi-plan $\mathrm{Re}(s) > 3/2$ et possède un prolongement analytique à tout le plan complexe (voir cor. 0.18).

Les rôles joués par ζ_{K}, $\mathscr{O}_{\mathrm{K}}^*$ et $\mathrm{Pic}(\mathscr{O}_{\mathrm{K}})$ dans la formule analytique du nombre de classes sont ici joués respectivement par $\mathrm{L}(\mathrm{E}, s)$, le groupe $\mathrm{E}(\mathbf{Q})$ des points de E rationnels sur $\mathbf{Q}$ et le groupe de Tate-Shafarevitch[3] Ш(E) de E, et les théorèmes 0.1, 0.2 et 0.3 deviennent respectivement :

---

[1] Ce régulateur est défini de la manière suivante : on part d'une famille $\varepsilon_1, \ldots, \varepsilon_{r(\mathrm{K})}$ d'éléments de $\mathscr{O}_{\mathrm{K}}^*$ engendrant un sous-groupe d'indice fini U de $\mathscr{O}_{\mathrm{K}}^*$ et de plongements $\sigma_1, \ldots, \sigma_{r(\mathrm{K})}$ de K dans $\mathbf{C}$ induisant des places différentes et on pose $e_i = 1$ si σ_i induit une place réelle et $e_i = 2$ si σ_i induit une place complexe ; alors $\mathrm{R}_\infty(\mathrm{K}) = \frac{1}{[\mathscr{O}_{\mathrm{K}}^* : \mathrm{U}]} |\det(e_i \log|\sigma_i(\varepsilon_j)|)_{1\leqslant i,j\leqslant r(\mathrm{K})}|$ ne dépend d'aucun des choix que l'on a faits.

[2] On se restreint aux courbes définies sur $\mathbf{Q}$ car ce sont les seules pour lesquelles on peut démontrer quoi que ce soit grâce à leur modularité (*cf.* § 0.4).

[3] $Ш(\mathrm{E}) = \mathrm{Ker}\big(\mathrm{H}^1(\mathscr{G}_{\mathbf{Q}}, \mathrm{E}(\overline{\mathbf{Q}})) \to \prod_p \mathrm{H}^1(\mathscr{G}_{\mathbf{Q}_p}, \mathrm{E}(\overline{\mathbf{Q}}_p))\big)$ est un groupe de torsion qui représente en quelque sorte l'obstruction à la détermination du groupe $\mathrm{E}(\mathbf{Q})$: si m est un entier $m \geqslant 1$, le sous-groupe de m-torsion $Ш_m(\mathrm{E})$ de $Ш(\mathrm{E})$ vit dans une suite exacte $0 \to \mathrm{E}(\mathbf{Q})/m\mathrm{E}(\mathbf{Q}) \to \mathrm{S}_m(\mathrm{E}) \to Ш_m(\mathrm{E}) \to 0$, où le m-groupe de Selmer $\mathrm{S}_m(\mathrm{E})$ est un groupe fini « effectivement calculable ».

THÉORÈME 0.4. — (i) *Le groupe* $\mathrm{E}(\mathbf{Q})$ *est un groupe abélien de type fini.*

(ii) *Le régulateur*[4] $\mathrm{R}_\infty(\mathrm{E})$ *est non nul.*

CONJECTURE 0.5. — *Le groupe* $Ш(\mathrm{E})$ *est un groupe fini. Plus généralement, si* K *est une extension finie de* $\mathbf{Q}$*, alors* $Ш(\mathrm{E}/\mathrm{K})$ *est un groupe fini.*

On note $r(\mathrm{E})$ le rang de $\mathrm{E}(\mathbf{Q})$ et $r_\infty(\mathrm{E})$ l'ordre du zéro de $\mathrm{L}(\mathrm{E}, s)$ en $s = 1$.

CONJECTURE 0.6 (Birch et Swinnerton-Dyer). — *On a* $r_\infty(\mathrm{E}) = r(\mathrm{E})$ *et*[5]

$$\lim_{s\to 1}(s-1)^{-r(\mathrm{E})}\mathrm{L}(\mathrm{E}, s) = \Omega_{\mathrm{E}}^{+} \cdot |Ш(\mathrm{E})| \cdot \mathrm{R}_\infty(\mathrm{E}) \cdot \prod_v m_v.$$

Les résultats concernant les conjectures 0.5 et 0.6 sont très partiels ; ce sont les suivants :

• $(\Omega_{\mathrm{E}}^{+})^{-1}\mathrm{L}(\mathrm{E}, 1)$ est un nombre rationnel (c'est une conséquence du théorème de Manin-Drinfeld) ;

• si $\mathrm{L}(\mathrm{E}, 1) = 0$, alors $\lim_{s\to 1}(s-1)^{-1}\mathrm{L}(\mathrm{E}, s)$ est un multiple rationnel de $\Omega_{\mathrm{E}}^{+}\cdot\mathrm{R}_\infty(\mathrm{E})$ (cela suit du théorème de Gross-Zagier [84, 40]) ;

• si $r_\infty(\mathrm{E}) \leqslant 1$, alors $Ш(\mathrm{E})$ est fini et $r(\mathrm{E}) = r_\infty(\mathrm{E})$ (théorème de Kolyvagin ; la démonstration utilise le théorème de Gross-Zagier et la technique des dérivées de Kolyvagin introduite à cette occasion [105, 135]).

---

[4] Ce régulateur est défini à partir de l'accouplement *hauteur de Néron-Tate* $\langle\ ,\ \rangle_\infty$ sur l'espace vectoriel $\mathbf{R}\otimes_{\mathbf{Z}}\mathrm{E}(\mathbf{Q})$. Si $y^2 = 4x^3 + ax + b$ est une équation de Weiestrass de E, alors la fonction $\mathrm{P} = (x(\mathrm{P}), y(\mathrm{P})) \mapsto h(\mathrm{P}) = \frac{1}{2}\log d(\mathrm{P})$, où $d(\mathrm{P})$ est le dénominateur de $x(\mathrm{P})$, est presque quadratique, et la hauteur de Néron-Tate est l'unique forme bilinéaire symétrique $\langle\ ,\ \rangle_\infty$ sur $\mathrm{E}(\mathbf{Q})$ telle que $\mathrm{P}\mapsto h(\mathrm{P}) - \langle \mathrm{P}, \mathrm{P}\rangle_\infty$ soit bornée sur $\mathrm{E}(\mathbf{Q})$. Tate a remarqué que l'on pouvait définir $\langle \mathrm{P}, \mathrm{P}\rangle_\infty$ comme la limite de la suite de terme général $4^{-n}h(2^n\mathrm{P})$. Par ailleurs, Néron [127, 109], a démontré que l'accouplement $\langle\ ,\ \rangle_\infty$ pouvait s'exprimer comme une somme, sur toutes les places de $\mathbf{Q}$, de symboles locaux, les contributions aux places finies étant fournies par la théorie de l'intersection et celle à l'infini par la théorie du potentiel (fonctions de Green). Cette décomposition en somme de symboles locaux est fondamentale d'un point de vue théorique (elle est par exemple cruciale dans la démonstration du théorème de Gross-Zagier [84]), et sert de modèle pour la construction des hauteurs p-adiques (note 14). Si $\mathrm{P}_1, \ldots, \mathrm{P}_r$, $r = r(\mathrm{E})$ sont des éléments de $\mathrm{E}(\mathbf{Q})$ formant une base de $\mathbf{Q}\otimes_{\mathbf{Z}}\mathrm{E}(\mathbf{Q})$ sur $\mathbf{Q}$, alors $\mathrm{R}_\infty(\mathrm{E}) = e^{-2}\det(\langle \mathrm{P}_i, \mathrm{P}_j\rangle_\infty)_{1\leqslant i,j\leqslant r}$, où e est l'indice du sous-groupe engendré par $\mathrm{P}_1, \ldots, \mathrm{P}_r$ dans $\mathrm{E}(\mathbf{Q})$. La non nullité de $\mathrm{R}_\infty(\mathrm{E})$ suit de ce que l'accouplement $\langle\ ,\ \rangle_\infty$ est non dégénéré car $\langle \mathrm{P}, \mathrm{P}\rangle_\infty > 0$ si P n'est pas de torsion comme on le constate en utilisant la formule de Tate.

[5] Les termes non encore définis dans cette formule sont :

• Le nombre m_v de composantes connexes de $\mathrm{E}(\mathbf{Q}_v)$ si v est une place de $\mathbf{Q}$: si $v = \infty$, alors m_v est le nombre de composantes connexes de $\mathrm{E}(\mathbf{R})$ au sens habituel, et si $v = p$ est un nombre premier, alors m_v est le nombre de composantes connexes sur $\mathbf{F}_p$ de la réduction du modèle de Néron de E.

• La période réelle Ω_{E}^{+} d'une différentielle de Néron (ou de Kähler ?, [168, p.101]) ω_{E} ; on a donc $m_\infty\Omega_{\mathrm{E}}^{+} = |\int_{\mathrm{E}(\mathbf{R})}\omega_{\mathrm{E}}|$.

Remarque 0.7. — (i) En ce qui concerne le dernier point, on n'a pas de résultat dans l'autre sens : on ne sait pas démontrer que $r(\mathrm{E}) = 0$ implique $r_\infty(\mathrm{E}) = 0$ (de manière équivalente, on ne sait pas prouver que $\mathrm{L}(\mathrm{E}, 1) = 0$ entraîne l'existence d'un point d'ordre infini).

(ii) On ne dispose d'aucun résultat concernant le lien entre $r(\mathrm{E})$ et $r_\infty(\mathrm{E})$ ou la finitude de Ш(E) dans le cas $r_\infty(\mathrm{E}) \geqslant 2$.

(iii) Une des difficultés est que l'on ne connaît pas la valeur de $r(\mathrm{E})$ a priori ; on pense que si on prend une courbe E au hasard, alors $r(\mathrm{E}) \leqslant 1$ avec une probabilité tendant vers 1 quand N_E tend vers $+\infty$, mais on connaît des courbes de rang $\geqslant 24$, et il y a tout lieu de croire que $r(\mathrm{E})$ n'est pas majoré.

(iv) Par contraste, on ne connaît pas de courbe elliptique E pour laquelle on peut prouver que[6] $r_\infty(\mathrm{E}) \geqslant 4$; le problème est qu'il est impossible de prouver qu'un réel est nul[7] sauf si c'est un entier. C'est un peu dommage, car l'existence de telles courbes permettrait d'améliorer nettement les minorations effectives pour le nombre de classes des corps quadratiques imaginaires [81, 129].

0.3. La conjecture de Birch et Swinnerton-Dyer p-adique

En p-adique, le produit eulérien ci-dessus ne converge nulle part, mais on peut construire une fonction L p-adique[8] à partir des valeurs en 1 de la fonction L complexe tordue[9] par des caractères de Dirichlet de conducteur une puissance de p. Cette fonction L p-adique dépend d'un choix supplémentaire : on factorise le facteur d'Euler en p de $\mathrm{L}(\mathrm{E}, s)$ sous la forme $(1-\alpha_1 p^{-s})(1-\alpha_2 p^{-s})$ et on choisit $\alpha \in \{\alpha_1, \alpha_2\}$ vérifiant[10] $v_p(\alpha) < 1$.

---

[6] On peut, le cas échéant, vérifier que $r_\infty(\mathrm{E}) \geqslant 3$ grâce au théorème de Gross-Zagier.

[7] En particulier, démontrer la conjecture 0.6 sous la forme faible « $r_\infty(\mathrm{E}) = r(\mathrm{E})$ » ne fournit pas d'algorithme déterministe pour calculer $r(\mathrm{E})$ et $\mathrm{E}(\mathbf{Q})$. Par contre, la conjecture 0.6 (même un peu affaiblie sous la forme $\lim_{s\to 1}(s-1)^{-r(\mathrm{E})}\mathrm{L}(\mathrm{E}, s) = n \cdot \Omega_\mathrm{E}^+ \cdot \mathrm{R}_\infty(\mathrm{E})$, avec n entier $\geqslant 1$) fournit un tel algorithme, le point étant que plus $\mathrm{R}_\infty(\mathrm{E})$ est petit et plus les générateurs de $\mathrm{E}(\mathbf{Q})$ sont faciles à trouver.

[8] Il faut probablement supposer $p \neq 2$ ou $p \geqslant 5$ dans certains des énoncés qui suivent au niveau de ce qui est connu.

[9] Si χ est un tel caractère, on note $\mathrm{L}(\mathrm{E}, \chi, s)$ la fonction L de E tordue par χ ; elle est définie par la série de Dirichlet $\mathrm{L}(\mathrm{E}, \chi, s) = \sum_{n=1}^{+\infty} \chi(n) a_n n^{-s}$. Si le conducteur de χ n'est pas premier au conducteur de E, la fonction $\mathrm{L}(\mathrm{E}, \chi, s)$ n'est pas forcément primitive ; il peut manquer des facteurs d'Euler en les nombres premiers divisant N_E.

[10] Ce n'est pas toujours possible : si E a réduction additive en p, alors $\alpha_1 = \alpha_2 = 0$ et on ne sait pas construire de fonction L p-adique dans ce cas (sauf si la courbe acquiert bonne réduction sur une extension abélienne de $\mathbf{Q}$ (*cf.* [61])). Si E a réduction multiplicative, alors $\{\alpha_1, \alpha_2\} = \{a_p, 0\}$, et on peut prendre $\alpha = a_p \in \{\pm 1\}$. Si E a bonne réduction, il y a deux cas de figure possibles : si $v_p(a_p) > 0$ (*i.e.* si E a bonne réduction supersingulière), alors il y a deux choix possibles pour α puisque $v_p(\alpha_1) = v_p(\alpha_2) = 1/2$, et si $v_p(a_p) = 0$ (bonne réduction ordinaire), alors une seule des deux racines α_1, α_2 est de valuation < 1 (de valuation 0), alors que l'autre est de valuation 1 (voir [147] et la rem. 4.12 pour ce dernier cas).

La construction de la fonction L p-adique $\mathrm{L}_{p,\alpha}(\mathrm{E},s)$ de E associée à α repose sur la théorie des symboles modulaires[(11)] qui permet [116, 4, 110, 189] de démontrer :

THÉORÈME 0.8. — *Soient Ω_{E}^{+} et Ω_{E}^{-} les périodes réelles et imaginaires pures de ω_{E}. Alors*

(i) *si χ est un caractère de Dirichlet, $\mathrm{L}(\mathrm{E},\chi,1)\in\overline{\mathbf{Q}}\cdot\Omega_{\mathrm{E}}^{\chi(-1)}$;*

(ii) *il existe une* (unique) *distribution $\mu_{\mathrm{E},\alpha}$ d'ordre $v_p(\alpha)$ sur $\mathbf{Z}_p$, telle que l'on ait*

$$\int_{p\mathbf{Z}_p}\phi(x)\mu_{\mathrm{E},\alpha}(x)=\alpha^{-1}\int_{\mathbf{Z}_p}\phi(px)\mu_{\mathrm{E},\alpha}(x)$$

quelle que soit ϕ localement analytique sur $p\mathbf{Z}_p$, et

$$\int_{\mathbf{Z}_p}\mu_{\mathrm{E},\alpha}(x)=(1-\alpha^{-1})^{b}\frac{\mathrm{L}(\mathrm{E},1)}{\Omega_{\mathrm{E}}^{+}}\quad\text{et}\quad\int_{\mathbf{Z}_p}\chi(x)\mu_{\mathrm{E},\alpha}(x)=p^{n}\alpha^{-n}\frac{\mathrm{L}(\mathrm{E},\chi^{-1},1)}{\mathrm{G}(\chi^{-1})\cdot\Omega_{\mathrm{E}}^{\chi(-1)}}$$

si $n\geqslant 1$ et χ est un caractère de Dirichlet[(12)] de conducteur p^n, et $b=0$ (resp. $b=1$) si E *a mauvaise réduction multiplicative (resp. bonne réduction).*

DÉFINITION 0.9. — *La fonction* L *p-adique $s\mapsto\mathrm{L}_{p,\alpha}(\mathrm{E},s)$ de* E *associée à α est la fonction définie, pour $s\in\mathbf{Z}_p$, par la formule*

$$\mathrm{L}_{p,\alpha}(\mathrm{E},s)=\int_{\mathbf{Z}_p^{*}}\langle x\rangle^{s-1}\,\mu_{\mathrm{E},\alpha},\quad\text{avec }\langle x\rangle^{s-1}=\exp((s-1)\log x).$$

Remarque 0.10. — On déduit du théorème 0.8 la formule

$$\mathrm{L}_{p,\alpha}(\mathrm{E},1)=(1-\alpha^{-1})^{b+1}\frac{\mathrm{L}(\mathrm{E},1)}{\Omega_{\mathrm{E}}^{+}}.$$

En particulier, si $\alpha=1$, alors la fonction $\mathrm{L}_{p,\alpha}(\mathrm{E},s)$ a un zéro supplémentaire en $s=1$. La courbe E a alors réduction multiplicative déployée et le théorème d'uniformisation de Tate [182] nous fournit $q(\mathrm{E})\in\mathbf{Q}_p^{*}$, de valuation non nulle, tel que E soit isomorphe, en tant qu'espace analytique rigide, au quotient de $\mathbf{G}_m$ par le groupe engendré par $q(\mathrm{E})$. Ceci nous permet de définir l'invariant $\mathscr{L}$ de E par la formule $\mathscr{L}_{\mathrm{E}}=\frac{\log q(\mathrm{E})}{v_p(q(\mathrm{E}))}$.

THÉORÈME 0.11. — *Si $\alpha=1$, alors*[(13)] $\mathrm{L}'_{p,\alpha}(\mathrm{E},1)=\mathscr{L}_{\mathrm{E}}\cdot\dfrac{\mathrm{L}(\mathrm{E},1)}{\Omega_{\mathrm{E}}^{+}}$.

(11) Panchishkin [131] a récemment trouvé une définition alternative de cette fonction qui colle nettement plus à la construction que l'on obtient en utilisant le système d'Euler de Kato.

(12) On considère χ comme une fonction localement constante sur $\mathbf{Z}_p$, nulle sur $p\mathbf{Z}_p$, et on note $\mathrm{G}(\chi^{-1})=\sum_{a\in(\mathbf{Z}/p^n\mathbf{Z})^{*}}\zeta_{p^n}^{a}\chi^{-1}(a)$ la somme de Gauss de χ^{-1}.

(13) Ce théorème (cas particulier de la conjecture de Mazur-Tate-Teitelbaum) a été démontré par Greenberg et Stevens [83] en utilisant les familles de formes modulaires de Hida.