THEORIE DES NOMBRES

BESANCON

Année 1988/1989

Fascicule 1

QUOI DE NEUF SUR LA CONJECTURE DE BIRCH ET SWINNERTON-DYER ?

Catherine GOLDSTEIN

Quoi de neuf sur la conjecture de Birch et Swinnerton-Dyer ?

Combien y-a-t-il de points à coordonnées rationnelles sur une courbe algébrique définie sur un corps de nombres ? Lorsque la courbe est de genre strictement plus grand que 1, la réponse est fournie par le théorème de Faltings (ex-conjecture de Mordell): il n'y en a qu'un nombre fini, que l'on ne sait d'ailleurs toujours pas évaluer pour le moment; le genre 0, quant à lui, se ramène au cas des droites et des coniques, il est bien connu. En genre 1, il peut n'y avoir aucun point rationnel (exemple de la courbe de Selmer $3x^3+4y^3+5z^3= 0$), mais dès qu'il en existe au moins un (la courbe est alors une courbe elliptique), une réponse partielle à notre question est fournie par le théorème de Mordell-Weil:
Les points rationnels d'une courbe elliptique E forment un groupe abélien de type fini,

$$E(\mathbb{Q}) \approx \mathbb{Z}^r \times E(\mathbb{Q})_{tors}.$$

Le groupe fini $E(\mathbb{Q})_{tors}$ se calcule assez aisément. Le calcul du rang et a fortiori de points générateurs du groupe de Mordell-Weil $E(\mathbb{Q})$ est une autre affaire. La démonstration du théorème de Mordell-Weil permet seulement de borner le rang, je rappellerai un peu plus loin comment. On dispose d'autre part maintenant d'un réseau de conjectures faisant intervenir ce rang, ainsi que d'autres invariants arithmétiques de la courbe, organisées autour de la conjecture de Birch et Swinnerton-Dyer; des progrès importants ont été faits dans ces directions depuis une quinzaine d'années, mais la complexité des relations entre toutes ces conjectures et les résultats partiels obtenus masque parfois le type de connaissances qu'elles permettent d'obtenir. C'est à démêler quelque peu cette situation que vise ce qui suit.

I La conjecture de Birch et Swinnerton-Dyer

Je me contenterai ici d'étudier le cas d'une courbe elliptique E définie sur $\mathbb{Q}$, quitte à préciser au passage dans quelle mesure les résultats obtenus sont plus généraux. La courbe E sera si besoin est donnée par un modèle de Weierstrass:

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

avec les coefficients a_i dans . Ceci revient à préciser sur la courbe E une forme différentielle de première espèce

$$\omega = \frac{dx}{2y+a_1x+a_3}$$

Le nombre de points N_p de la courbe, réduite modulo p, sur $\mathbb{F}_p$, diffère de p+1

par une contribution inférieure en module à $2\sqrt{p}$, pour tout nombre premier p.
L'idée originelle de Birch et Swinnerton-Dyer est la suivante: si le rang est >0, autrement dit si la courbe E a des points rationnels d'ordre infini, ceux-ci doivent fournir des contributions stables modulo p, pour tout nombre premier p, en particulier le produit $\Pi N_p/p$ doit diverger. Cette approche heuristique ne paraît d'ailleurs pas avoir inspiré les preuves partielles qui vont suivre.
Pour préciser ceci, il est nécessaire d'introduire la fonction L complexe de la courbe elliptique, définie pour Re(s) > 3/2 par le produit convergent:

$$L(E/\quad,s) = \prod \left(1 - c_p\, p^{-s} + \varepsilon(p)\, p^{1-2s}\right)^{-1}$$

où ε (p) = 0 ou 1 selon la courbe E réduite sur $\mathbb{F}_p$ est de genre 0 ou 1, c'est-à-dire selon que la courbe E n'a pas ou a bonne réduction en p,
et où $c_p = p + 1 - N_p$.

Cette fonction L pourrait s'interpréter comme le produit de fonctions Zéta relatives aux courbes réduites modulo un nombre premier; une autre manière de l'écrire est la suivante:

$$L(E/\mathbb{Q}, s) = \prod \text{dét}\left(1 - p^{-s}\rho_l(Frob_p)\,|\,V_l^{I_p}\right)^{-1}$$

où $Frob_p$ est l'endomorphisme de Frobenius,

$$V_l = lim\ E_l{}^n \otimes Q$$

est l'espace de Tate, pour $p \neq l$,
I_p est le groupe d'inertie en p et
ρ_l: Gal $(\overline{\mathbb{Q}}\ /\mathbb{Q}) \to$ Aut $(V_l) \approx Gl_2(\mathbb{Q}_l)$, la représentation l-adique.
En particulier, c_p est ici la trace du Frobenius en p dans la représentation l-adique (on démontre que tout ceci ne dépend pas du choix de $l \neq p$).

La première conjecture de la théorie est celle de Hasse:
L(E/,s) admet un prolongement analytique à tout le plan complexe et vérifie de plus l'équation fonctionnelle

$$\Lambda(S) = \pm \Lambda(2-s),$$

avec $\Lambda(s) = N^{s/2}\,(2\pi)^{-s}\,\Gamma(s)\,L(E/,s)$ *(N étant ici le conducteur de la courbe, un entier divisible uniquement par les premiers p où la courbe E a mauvaise réduction).*

Cette conjecture est en fait connue dans deux situations:

(Mod): La courbe elliptique E est modulaire, c'est-à-dire est un quotient de la jacobienne $J_0(N)$ de la courbe modulaire $X_0(N)$, modèle sur du quotient du demi-plan de Poincaré H par le sous-groupe d'automorphismes $\Gamma_0(N)$, avec

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sl_2(Z), \text{ avec } c \equiv 0 \bmod (N) \right\}$$

compactifié par l'adjonction des pointes. Dans cette situation, E est paramétrée par des fonctions modulaires, plus précisément, si π: $X_0(N) \rightarrow E$, est un morphisme surjectif défini sur , la forme différentielle ω se relève en une forme différentielle $\pi^*(\omega) = cf(z)dz$, où c est un nombre rationnel non nul et $f(z) = \Sigma c_n e^{2i\pi nz}$ est une forme modulaire parabolique de poids 2, propre pour l'action des opérateurs de Hecke, dont la transformée de Mellin $L(f, s) = \Sigma c_n n^{-s}$ coïncide avec la fonction L(E/,s).

(MC): La courbe elliptique E a des multiplications complexes, autrement dit son anneau d'endomorphismes sur une clôture algébrique de $\mathbb{Q}$ est un ordre dans l'anneau des entiers d'un corps quadratique imaginaire $K = (\sqrt{-d})$. Dans ce cas, la fonction $L(E/\mathbb{Q}, s)$ est la fonction L d'un caractère de Hecke, ψ, de K. Le groupe de Mordell-Weil sur K, E(K) a une structure de O-module libre de type fini (O est l'ordre formé par les endomorphismes de E, on supposera pour simplifier dans la suite que c'est tout l'anneau des entiers de K, ce qui est toujours le cas à isogénie près), de rang $r = r_K/2$ si r_K est le -rang de E(K).

Le deuxième cas est en fait un cas particulier du premier; d'ailleurs, une conjecture de Taniyama-Weil affirme que ce premier cas est tout à fait général, c'est-à-dire que toute courbe elliptique sur est modulaire; il y a beaucoup d'arguments en faveur de cette conjecture et il est en principe assez facile de la vérifier dans chaque cas concret qu'on souhaite étudier.
Pourtant, le second cas spécial mérite d'être distingué: les méthodes qui s'y appliquent sont un peu différentes et c'est celui dans lequel les premiers résultats sur la conjecture de Birch et Swinnerton-Dyer ont été obtenus (cf infra). Ceux-ci s'étendent en général au cas de courbes elliptiques définies sur un corps de nombres autre que (contrairement au cas modulaire), au moins sous certaines hypothèses restrictives (essentiellement celle que les points de torsion de la courbe elliptique engendrent sur K une extension abélienne). L'analogie des points de division d'une courbe elliptique à multiplication complexe avec les racines de l'unité y a été systématiquement développée: **(MC)** relève de techniques typiquement "abéliennes". Les travaux de Kolyvagin ont pourtant infléchi ce point de vue en développant des traitements parallèles des cas cyclotomique, elliptique à

multiplication complexe et elliptique modulaire.

Dans tous les cas où la conjecture de Hasse est connue, on peut s'intéresser au comportement de la fonction L(E/,s) au point 1, point critique au sens de Deligne, situé au centre de la bande critique que détermine l'équation fonctionnelle. La conjecture de Birch et Swinnerton-Dyer, sous sa forme raffinée, prédit exactement ce comportement:

Conjecture de Birch et Swinnerton-Dyer

(i) $r_\infty =: \mathrm{ord}_{s=1} L(E/\mathbb{Q},s) = r$

(ii)

$$lim_{s\to 1}\frac{L(E/\mathbb{Q},s)}{(s-1)^r} = \frac{Vol(E/\mathbb{Q})}{|E_{tors}(\mathbb{Q})|^2}|Ш(E/\mathbb{Q})|\,\Omega\,\Pi m_p$$

où Vol(E/$\mathbb{Q}$) est un régulateur elliptique calculé à l'aide de la hauteur canonique de Néron-Tate sur une base du groupe de Mordell-Weil,

$$\Omega = \int_{E(\mathbb{R})} |\omega|$$

est une période complexe , les nombres $m_p = |E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)|$ sont les facteurs (rationnels) de Tamagawa, égaux à 1 si la courbe a bonne réduction en p — $E_0(\mathbb{Q}_p)$ désigne ici le groupe des points de E sur $\mathbb{Q}_p$ se réduisant modulo p en un point non singulier— et |Ш(E/$\mathbb{Q}$)| est le cardinal du groupe de Tate-Safarevic de la courbe sur $\mathbb{Q}$, dont une définition précise sera rappelée plus loin.

Remarques sur la conjecture: —Sa formulation même est conjecturale comme je l'ai déjà mentionné; elle suppose, outre l'existence du prolongement analytique de la fonction L, la finitude du groupe de Tate-Safarevic. Celle-ci n'est pour l'instant prouvée que dans certains cas qui seront précisés dans la suite.

— Cette conjecture apparaît comme une variante elliptique de la formule analytique du nombre de classes, le groupe de Tate-Safarevic jouant ici le rôle du groupe des classes. Il a bien la fonction de mesurer un défaut de localisation! Une analogie assez profonde est développée dans des travaux récents de Kolyvagin. Les démonstrations des résultats partiels connus à ce jour confirment d'ailleurs cette interprétation de (ii).

— Quel intérêt cette conjecture a-t-elle dans le calcul effectif du rang ? Plutôt moins grand qu'on pourrait le penser ! Il n'est pas évident de calculer l'ordre du zéro de la fonction L en un point; on ne peut de toute façon numériquement qu'espérer le borner par l'ordre de la première dérivée non nulle. Bien sûr, le rang est a priori donné par la valeur de la dérivée logarithmique de la fonction L au point 1, mais je

ne connais aucun moyen de calculer cette dernière.. La partie (ii) laisse espérer, via une estimation de la hauteur de générateurs éventuels, un moyen effectif pour déterminer ces derniers; l'estimation de la hauteur provient par exemple des travaux sur la conjecture de Lang, cf [Lang, 83]. Outre cela, il y a bien sûr un intérêt théorique: la conjecture lie un objet construit analytiquement à des invariants arithmétiques, mais surtout, elle lie des objets définis localement (la fonction L, la hauteur de Néron-Tate) à des invariants globaux; c'est donc une manière de récupérer un principe de Hasse pour les courbes de genre 1 qui ne le vérifient pas...

II Les résultats théoriques.

Les résultats obtenus sont de deux natures: d'une part des résultats théoriques amorcés par les travaux de Coates et Wiles en 1976-1977, d'autre part, une foule de vérifications numériques, pour des familles de courbes à multiplication complexe par l'anneau des entiers de $\mathbb{Q}(i)$ ou de $\mathbb{Q}(\sqrt{-3})$ par exemple; de plus, le mélange de calculs explicites et de considérations issues des résultats théoriques permet souvent dans des cas concrets d'aller plus loin que ce que la théorie semble le promettre; j'en donnerai des exemples plus tard. La majeure partie des résultats concernent les petits rangs. Ils sont souvent obtenus à l'intersection de travaux dans plusieurs directions désignés dans ce qui suit par le nom de leurs auteurs et la date (renvoyant à la bibliographie pour les détails). On suppose ici que la courbe E est définie sur et modulaire.

Cas où $r_\infty=0$. Une grande partie de la conjecture de Birch et Swinnerton-Dyer est vraie:

le rang r vaut 0 (le groupe de Mordell - Weil est fini) ,
le groupe de Tate-Safarevic est fini.

Sous cette forme, cette assertion résulte de Kolyvagin [88a,88b]. On obtient une estimation pour l'ordre du groupe de Tate-Safarevic, proche de celle contenue dans (ii).
Plus précisément, le cas ***(MC)*** a été traité d'abord: en 1976, Coates et Wiles [77] ont démontré que dans ce cas, $r_\infty = 0$ implique que r =0. Rubin [87] a montré, toujours dans ce cas, que si $r_\infty =0$, alors le groupe de Tate-Safarevic est fini et que les diviseurs de son ordre sont, à l'exception peut-être de 2 et 3, ceux prédits par la partie (ii) de la conjecture de Birch et Swinnerton-Dyer. Dans Kolyvagin [88a] figure la preuve que r=0 et que le groupe de Tate-Safarevic est fini, dans le cas modulaire, moyennant l'existence d'un point d'ordre infini particulier sur des courbes tordues de E; la liaison entre cette hypothèse et l'ordre du zéro de la fonction L est assurée par les résultats de Gross et Zagier [88], si l'on connaît l'existence d'une tordue de E pour laquelle la dérivée de la fonction L ne s'annule pas; ce dernier fait ("conjecture analytique") a été prouvé indépendamment par

Kumar et Ram Murty, d'une part, à l'aide de méthodes analytiques, et par Bump, Friedberg et Hoffstein, d'autre part (cf Perrin-Riou [89] pour les détails).

Cas où $r_\infty = 1$. Par Kolyvagin [88b], on sait que $r = 1$ et que le groupe de Tate-Safarevic est fini; il est possible de vérifier (ii) dans de nombreux exemples , entre autre celui de la courbe d'équation

$$y^2 + y = x^3 - x ,$$

de conducteur 37, de rang 1, et de groupe de Tate-Safarevic trivial.
Là encore, les travaux antérieurs de Gross et Zagier [86] montraient déjà que $r \geq 1$ et que si de plus $r = 1$, un point explicite d'ordre infini sur E (point de Heegner) permet de prouver la conjecture de Birch et Swinnerton Dyer (ii) à $\mathbb{Q}^\times$ près .

Si la courbe est ***(MC),*** on savait déjà que r=1 grâce à Rubin [87], qui fait intervenir également les résultats de Gross et Zagier [86] déjà mentionné, plus un analogue p-adique de ces résultats dû à Perrin-Riou [87].

Cas où $r_\infty \geq 2$. Il n'y a plus de résultats directs, concernant (ii) ! Il est toutefois possible de tirer des renseignements sur le rapport de r_∞ et r des articles déjà utilisés.
Si l'ordre du zéro de la fonction L est impair, on peut par exemple appliquer Gross et Zagier [86] et Perrin-Riou [87], pour en conclure que l'ordre du zéro d'une certaine fonction p-adique doit être ≥2, pour certains premiers p. Les travaux de Kolyvagin [88b] et Perrin-Riou [83] dans le cas ***(MC)*** ou Schneider [82,85] dans le cas ***(ML)***, permettent d'en déduire que le rang de E est au moins 2, à condition que la p- composante du groupe de Tate-Safarevic soit finie et que la hauteur p-adique ne soit pas dégénérée pour un de ces premiers p , cf infra pour des exemples.

On peut aussi légitimement se poser la question des réciproques: si r = 0, on sait par Gross et Zagier [86], que $r_\infty = 0$ ou est ≥2. Sous l'hypothèse que le groupe de Tate-Safarevic est fini (dont je ne crois pas qu'elle se déduise des travaux mentionnés), on peut en utilisant une chaîne de raisonnements analogues à celle évoquée ci-dessus montrer que $r_\infty = 0$. De même si r = 1,dans le cas ***(MC)***, ou pour des exemples numériques particuliers.

Les travaux mentionnés entrent grosso modo dans deux grandes familles; les uns sont des résultats de rationalité sur des valeurs particulières de fonctions L et de leurs dérivées, tel est le cas de Gross et Zagier [86]. La majeure partie des autres font appel à l'étude de la courbe elliptique sur des extensions obtenues en rajoutant au corps de base des points de division convenables: on y applique des adaptations elliptiques de méthodes d'Iwasawa pour étudier la "suite de descente", qui intervient déjà dans la démonstration du théorème de Mordell-Weil et traite sur le même plan les points rationnels de E et le groupe de Tate-Safarevic. Ces méthodes ont surtout été développées dans le cas ***(MC)***, mais Kolyvagin en a

étendu certains principes au cas modulaire général. Je vais me consacrer ici au cas ***(MC)***, d'une part parce qu'il est le mieux connu, d'autre part parce que le cadre en est plus facile à expliquer.

III La suite de descente.

Je supposerai donc dans la suite que que la courbe elliptique E, définie sur , a multiplication complexe par l'anneau des entiers de K. Soient F un corps contenant K et m un entier de K non nul. La multiplication par m sur $E(\overline{F})$ induit une suite exacte de cohomologie courte:

$$0 \to E(F) / m\,E(F) \to H^1(G_F, E_m) \to H^1(G_F, E)(m) \to 0,$$

où G_F désigne le groupe de Galois absolu de F. Cette suite est analogue à la suite de Kummer des extensions de F, i.e. à la suite

$$0 \to F^x / F^{xm} \to H^1(G_F, \mu_m) \to H^1(G_F, F^x)(m) \to 0,$$

où μ_m est le groupe des racines de l'unité : dans cette situation, le dernier terme de la suite est nul grâce au théorème 90 de Hilbert ! Ce n'est (mal)heureusement pas le cas dans la situation elliptique. Le véritable analogue dans la théorie cyclotomique est en fait obtenu en remplaçant le groupe multiplicatif du corps F par son groupe d'unités, de type fini si F est un corps de nombres, tout comme le groupe de Mordell- Weil.

Des suites analogues sont valables lorsque, F étant une extension de , on considère également ses localisés en toute place. Les applications de restriction aux groupes de décomposition fournissent alors un diagramme:

$$\begin{array}{ccccccc}
0 \to & E(F) / m\,E(F) & \to & H^1(G_F, E_m) & \to & H^1(G_F, E)(m) & \to 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
0 \to & \Pi\, E(F_v) / m\,E(F_v) & \to & \Pi\, H^1(G_v, E_m) & \to & \oplus H^1(G_v, E)(m) & \to 0;
\end{array}$$

Le groupe $H^1(G_F, E)$ peut être interprété comme le groupe des espaces homogènes sur E: le noyau de la flèche

$$H^1(G_F, E) \to \oplus H^1(G_v, E)$$

représente les espaces homogènes partout localement triviaux, mais non globalement, autrement dit, les courbes définies sur ayant E pour jacobienne, qui

possèdent des points dans tous les complétés de F, mais pas dans F (donc sont isomorphes à E localement, mais pas sur): c'est le groupe Ш de Tate - Safarevic. On note S(E/F, m) l' image réciproque de ses éléments d'ordre m dans $H^1(G_F, E_m)$ et on dispose alors du diagramme commutatif suivant:

$$
\begin{array}{ccccccc}
 & & & & & & 0 \\
 & & & & & & \downarrow \\
0 \to & E(F)/mE(F) & \to & S(E/F, m) & \to & Ш(E/F)(m) & \to 0 \\
 & \| & & \cap & & \downarrow & \\
0 \to & E(F)/mE(F) & \to & H^1(G_F, E_m) & \to & H^1(G_F, E)(m) & \to 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
0 \to & \Pi\, E(F_v)/mE(F_v) & \to & \Pi\, H^1(G_v, E_m) & \to & \oplus H^1(G_v, E)(m) & \to 0,
\end{array}
$$

où les lignes horizontales et la ligne verticale à droite sont exactes.
En particulier, le groupe de Selmer S(E/F, m) est l'ensemble des cocycles c de G_F à valeurs dans E_m qui proviennent par restriction aux groupes de décomposition de points de $E(F_v)$, c'est-à-dire sont donnés par:
$c(\sigma_v) = (1/m\ P_v)\,\sigma_v - 1/m\ P_v$, avec $P_v \in E(F_v)$, pour tout $\sigma_v \in G_v$.

L'intérêt de se restreindre ainsi aux éléments localement triviaux est que le groupe de Selmer est fini: c'est ce fait, exprimé bien sûr à l'origine dans un langage différent, qui est à la base de la démonstration du théorème de Mordell -Weil. Considérons en effet un corps F contenant E_m, le groupe de Selmer s'interprète alors comme un groupe d'homomorphismes d'un quotient de G_F, déterminé par une extension de F dont on démontre qu'elle ne peut ramifier qu'aux places divisant m ou aux places de mauvaise réduction: une telle extension est nécessairement finie, donc aussi le groupe de Selmer, et le quotient E(F)/mE(F). Pour achever, on applique alors une procédure de descente, très proche dans son principe de l'algorithme d'Euclide: tout point P de E(F) s'écrit $P=mQ + P_i$, où P_i ne prend qu'un ensemble fini de valeurs; la taille (la hauteur) de Q est plus petite que celle de P, et il suffit d'itérer le procédé. Rappelons qu'en pratique, on ne sait toujours pas trouver effectivement des générateurs de E(F)/mE(F), c'est-à-dire les points P_i.

C'est à cette suite fondamentale de descente que vont s'appliquer les méthodes de la théorie d'Iwasawa. Plus précisément, on regarde les suites obtenues en choisissant pour m des puissances croissantes d'un même premier; elles sont compatibles entre elles et l'étude de leur limite est en principe plus simple que l'étude de chacune d'elles (il y a un phénomène de régularisation à la limite). C'est dans ce cadre que s'inscrivent une bonne partie des travaux que j'ai mentionnés plus haut.

IV Théorie d'Iwasawa elliptique.

Pour continuer, je choisirai donc $m = \pi^n$, où π engendre un idéal de K de hauteur 1 tel que la courbe E a bonne réduction au-dessus de $N\pi = p$ —dans ce cas, E a bonne réduction ordinaire en p. Par passage à la limite inductive sur les suites exactes de descente, on obtient la suite exacte (*)

$$0 \to \quad E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \quad S(E/F, \pi^\infty) \quad \to \quad Ш(E/F)(\pi^\infty) \to 0,$$

où le second terme est la limite inductive des $S(E/F, \pi^n)$ et où $Ш(E/F)(\pi^\infty)$ est la composante π-primaire du groupe de Tate-Safarevic.
$S(E/F, \pi^\infty)$ est un sous-groupe de $H^1(G_F, E_{\pi^\infty})$, qu'il est possible d'identifier plus précisément quand F est engendré par les points de π^n-division (pour tout n).

Proposition (Coates): *Soit F_∞ l'extension $K(E_{\pi^\infty})$. On a alors un isomorphisme de $\mathbb{Z}_p[Gal(F_\infty/K)]$-modules:*

$$S(E/F_\infty, \pi^\infty) \approx Hom_p(X_\infty, E_{\pi^\infty}),$$

où X_∞ est le groupe de Galois sur F_∞ de la plus grande pro-p-extension abélienne de F_∞ non ramifiée en dehors de π, qu'on notera dans la suite M_∞.

L'action de $Gal(F_\infty/K)$ sur X_∞ se fait par automorphismes "intérieurs" dans le groupe de Galois de M_∞ sur K, par relèvement arbitraire à ce groupe de l'élément de $Gal(F_\infty/K)$ considéré (l'extension M_∞ étant abélienne, cette action ne dépend pas du relèvement choisi). Tout revient désormais à l'étude du groupe de Galois X_∞, qui est un $\mathbb{Z}_p$- module compact, et au contrôle de l'action galoisienne dessus, ce qui permettra de redescendre à K les renseignements obtenus. A cause de mes hypothèses sur *p*, l'extension F_∞/K se décompose en une extension d'ordre p—1 et une $\mathbb{Z}_p$-extension: l'extension K_∞ de K incluse dans F_∞, et fixée par le sous-groupe Δ d'ordre p—1 est une $\mathbb{Z}_p$—extension de K.
Soit χ le caractère de Δ donnant l'action sur les points de E_π: on notera comme d'habitude X_∞^χ la χ-composante isotypique de X_∞ correspondant à χ, autrement dit, $X_\infty^\chi = e_\chi X_\infty$ avec

$$e_\chi = \frac{1}{|\Delta|} \sum_{\sigma \in \Delta} \chi(\sigma)\, \sigma^{-1}$$

l'idempotent de Δ associé à χ.

On a alors: $S(E/K_\infty, \pi\infty) \approx \mathrm{Hom}_{Z_p}(X_\infty, E\pi\infty)^{\Delta}$, autrement dit,

$$\overline{S(E/K_\infty, \pi^{\infty})} \approx X_\infty^{\chi}(-1)$$

où le chapeau désigne le dual de Pontryagin et (—1) le twist à la Tate, c'est-à-dire, le même $\mathbb{Z}_p$-module avec une structure galoisienne tordue par le caractère χ. Reste à étudier ce dual comme $\mathbb{Z}_p[\Gamma]$ - module, où Γ est le groupe de Galois de l'extension $F_\infty/F(E_\pi)$ (ou, ce qui revient au même, le groupe de Galois de K_∞ sur K). On pourrait alternativement l'interpréter comme le tordu du groupe de Galois d'une extension M_∞^{χ}, définie comme M_∞, avec la condition supplémentaire que Δ agit dessus par le caractère χ.

Iwasawa et Serre ont précisé le théorème de structure de tels modules, lorsqu'ils sont compacts et de type fini (c'est le cas ici). On identifie traditionnellement Γ à $\mathbb{Z}_p$ et $\mathbb{Z}_p[\Gamma]$ à $\Lambda=\mathbb{Z}_p[[T]]$, en envoyant un générateur γ de Γ sur 1+T. On a alors

$$X_\infty^{\chi}(-1) \approx \prod \Lambda/f_i^{m_i} \times \prod \Lambda/p^{r_j} \times \Lambda^s$$

le signe $\approx$ désigne ici un pseudo-isomorphisme (i.e. à noyau et conoyau fini), les f_i sont des polynômes distingués.
Dans notre cas particulier, le module est de torsion (ce ne serait pas le cas si *p* n'était pas décomposé par exemple), donc s=0. Il a été aussi prouvé par Schnepps et Gillard que les r_j sont nuls. On pose alors

$$L_\pi(K_\infty, T) = \prod f_i^{m_i}(T)$$

qui n'est bien définie qu'à une unité près dans Λ et qu'on appelle une série caractéristique du module $X_\infty^{\chi}(-1)$; remarquons au passage que sous nos hypothèses, ce dernier est un $\mathbb{Z}_p$-module de type fini dont le rang est le degré total des f_i. Le théorème suivant est une version algébrique d'une conjecture de Birch et Swinnerton-Dyer p-adique et figure dans Perrin-Riou [83]:

Théorème (Perrin-Riou): Si Ш (E/K, $\pi\infty$) est fini et si un équivalent p-adique de la hauteur de Néron-Tate n'est pas dégénéré, alors

(i)$_\pi$ *T^r divise exactement $L_\pi(K_\infty , T)$*

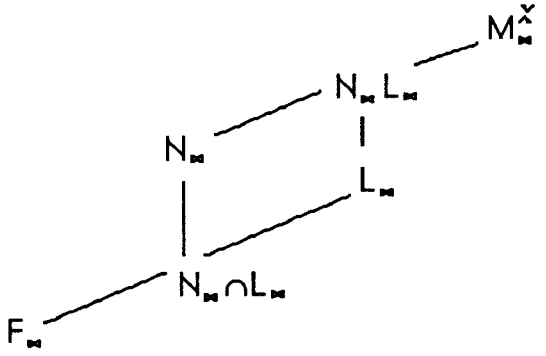
(ii)$_\pi$

$$\lim_{T\to 0} \frac{L_\pi(K_\infty, T)}{T^r} \cong \left(1-\frac{\pi}{p}\right) \frac{\left|I(E/K)(\pi^\infty)\right|}{\left|E(K)\,(\pi^\infty)\right|} \mathrm{Vol}_\pi(E(K))$$

où le signe $\cong$ désigne l'égalité à une unité p-adique près et où le Volume p-adique est calculé à partir de l'analogue p-adique de la hauteur de Néron-Tate non dégénérée.

Ce théorème a été démontré par Schneider [85] dans le cas général ordinaire (sans hypothèses de multiplication complexe).

En fait, X_∞^χ a un quotient isomorphe à $T_\pi^r = \left(\lim E_\pi\right)^r$: celui-ci correspond, du point de vue des extensions de corps, à l'extension kummérienne F_∞ ($\cup$ $(1/\pi^n)E(K)$) /F_∞ c'est-à-dire au morceau correspondant à $E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ dans le groupe de Selmer. Les autres zéros de la fonction $L_\pi(K_\infty , T)$ correspondent aux inverses des caractères intervenant effectivement dans l'action du groupe de Galois sur X_∞, mais il n'est pas facile d'imaginer comment construire les extensions correspondantes; de même d'ailleurs pour les zéros des séries caractéristiques des modules correspondant à l'action de Δ par d'autres caractères que χ . On peut cependant préciser un peu la situation dans le diagramme de corps suivant:



On a bien sûr: Gal $(M_\infty^\chi / F_\infty) = X_\infty^\chi$

Comme expliqué plus haut, $N_\infty = F_\infty (E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$, Gal $(N_\infty / F_\infty) \cong T_\pi^r$.

L'extension L_∞ est l'extension maximale de F_∞ contenue dans M_∞^χ non ramifiée; en particulier, Gal (L_∞/F_∞) est isomorphe à la χ-partie du groupe de classes d'idéaux de F_∞ par la théorie du corps de classes.

Celle-ci permet d'identifier aussi le sous-groupe Z_∞ = Gal (M_∞^χ / L_∞) à la limite projective des groupes

$$\left(U_n \big/ \overline{E_n}\right)^\chi$$

où U_n est le groupe des unités locales de $F_{n,\pi}$, $\equiv 1$ modulo π, et E_n les unités globales de F_n, dont on prend la clôture dans U_n. Le corps F_n est ici le n-ième corps intermédiaire de l'extension F_∞/K, c'est-à-dire le corps engendré par les points de $E_{\pi^{n+1}}$.

On peut montrer que Gal($N_\infty L_\infty/L_\infty$) est isomorphe à T_π dès que le rang r de la courbe E est ≥ 1: en fait , ce groupe est bien sûr isomorphe à Gal($N_\infty/N_\infty \cap L_\infty$). Un raisonnement analogue à celui fait plus haut, mais cette fois sur les localisés en π, montre en effet que $N_{\infty,\pi}$ est engendré sur $F_{\infty,\pi}$ (ou $L_{\infty,\pi}$) par les points de $E(K_\pi)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$: mais le groupe des points de E sur un corps local est de rang ≤ 1 sur l'anneau des entiers du corps local !
En particulier, Z_∞ a T_π comme quotient.

Ce groupe Z_∞ n'est pas le plus simple à décrire: on introduit généralement des unités spéciales, dans le cas elliptique les unités de Robert, et le groupe

$$Y_\infty = \lim \left(U_n \big/ C_n\right)^\chi$$

Les unités de Robert sont des unités globales, donc Y_∞ s'envoie surjectivement dans Z_∞; en particulier, si $r \geq 1$, Y_∞ a un quotient isomorphe à T_π.
Pour résumer, on dispose donc de la suite exacte (**) suivante, qui est une suite de $\mathbb{Z}_p$[Gal(K_∞/K)]—, ou encore de $\Lambda = \mathbb{Z}_p[[T]]$—modules:

$$0 \to \lim \left(\overline{E_n} \big/ C_n\right)^\chi \to Y_\infty = \lim \left(U_n \big/ C_n\right)^\chi \to X_\infty^\chi \to A_\infty^\chi = \lim A_n^\chi \to 0$$

où A_n est le groupe de classes d'idéaux dans F_n.

L'intérêt de Y_∞ réside principalement dans son lien avec les valeurs de la fonction L complexe: les unités de Robert sont en effet définies à partir de produits et de quotients de valeurs de la fonction coordonnée *x* sur la courbe, évaluée en des points de division. Si on fixe une uniformisante τ_π en π de U_n et qu'on calcule le

développement en série de τ_π des unités de Robert, on trouve comme coefficients des expressions liées aux valeurs de la fonction L complexe. La série caractéristique du Λ-module Y_∞ est ainsi égale à une unité près à la série d'interpolation définie par la proposition suivante:

Proposition: Il existe une unique série à coeeficients dans l'anneau des entiers de l'extension maximale non ramifiée de K_π, telle que pour tout entier $k \geq 1$, avec $k \equiv 1 \bmod (p-1)$,

$$\Omega_\pi^{-k} L_\pi(\kappa(\gamma)^{k-1} - 1) = (k-1)! \left(1 - \frac{\psi^k(\pi)}{p}\right) \Omega^{-k} L(\psi^{-k}, k)$$

Ω_π est une prériode p-adique analogue à la période Ω, et permettant tout comme celle-ci de rendre algébrique les valeurs des fonctions L (et donc de les comparer !), κ est le caractère de Γ donnant l'action de Γ sur $E_{\pi\infty}$, et ψ est le caractère de Hecke déjà mentionné attaché à E/K, en particulier

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

Il n'est peut-être pas inutile à ce moment de faire un peu le bilan de ce que nous avons obtenu: tout s'organise autour du diagramme de corps expliqué ci-dessus et des suites exactes (*) (ou plutôt de la suite qui s'en déduit par dualité de Pontryagin) et (**), qui en décrivent essentiellement les "deux branches": pour démontrer des propriétés relatives aux groupes de Mordell-Weil ou de Tate-Safarevic, c'est-à-dire, à l'intérieur du groupe X_∞^χ, dual du goupe de Selmer, à la branche du diagramme d'extensions contenant N_∞ , on utilise les renseignements fournis en particulier par la théorie du corps de classes, relatifs à la branche contenant L_∞. Le théorème de Perrin-Riou et nos espoirs qu'une conjecture analogue à celle de Birch et Swinnerton-Dyer soit vraie pour les fonctions L *p*-adiques d'interpolation amènent à la

Conjecture principale: Les séries caractéristiques des Λ-modules Y_∞^χ et X_∞^χ sont les mêmes.

Cette conjecture vient d'être démontrée par Rubin [88], utilisant des arguments venant de Kolyvagin [88b]. La démonstration consiste d'ailleurs à fabriquer, comme le suggère la suite exacte (**) des annulateurs du groupe des classes à l'aide des unités de Robert.

V Des résultats

La majeure partie des résultats atteints dans ce cadre sont obtenus en parcourant les suites exactes fondamentales ou le diagramme. Par exemple, si le rang r est supérieur ou égal à 1, Y_∞ a un quotient isomorphe à T_π, donc sa série caractéristique est divisible par T, donc s'annule en 0; d'après la conjecture principale, il en est de même de la série analytique d'interpolation. Pour k =1, l'équation définissant cette dernière donne $\Omega^{-1} L(\psi, 1) = 0$, donc r_∞ est supérieur ou égal à 1. C'est la démonstration du théorème de Coates et Wiles [77] mentionnée au début de ce texte.

Notons r_π l'ordre du zéro de la fonction L *p*-adique (d'interpolation ou liée au module de Selmer, puisque la conjecture principale énonce qu'ils sont les mêmes). Les renseignements sur la partie (i) de la conjecture de Birch et Swinnerton-Dyer que l'on sait obtenir procèdent comme suit:
Si la hauteur p-adique n'est pas dégénérée, $r \leq r_\pi$ (et égal si Ш (E/K)($\pi\infty$) est fini) par le théorème de Perrin- Riou [83].
La liaison entre r_π et r_∞ (on conjecture l'égalité bien sûr !) n'est connue que si $r_\pi = 0$ (c'est la définition de la fonction d'interpolation qui l'assure) ou 1 (grâce aux résultats de Gross et Zagier [86], d'une part, et de Perrin-Riou[87] d'autre part).

En pratique, on sait calculer la hauteur *p*-adique sur une famille de points indépendants , au moins pour des courbes de rang assez petit, et vérifier en calculant la dérivée r+1ème de la fonction d'interpolation que r_π est $\leq$ r donc =r. Joint éventuellement à la considération du signe de l'équation fonctionnelle, ceci peut permettre de vérifier (i) dans la conjecture de Birch et Swinnerton-Dyer (un calcul de la fonction L ou de ses dérivées permet seulement de donner une borne de l'ordre du zéro, mais pas de le calculer, un résultat du type 0,000000... n'étant pas concluant a priori !).
Par exemple, pour les courbes de rang 2 de Bernardi, Goldstein, Stephens [84], $r_\pi \geq 2$ par le théorème de Perrin-Riou [83] et le théorème de Kolyvagin-Rubin [88] (ex- conjecture principale); on vérifie que $L''_\pi(0) \neq 0$, donc $r_\pi = 2$. Le signe de l'équation fonctionnelle de la fonction L est +1, donc r_∞ est pair, il est ≥ 1 puisque $r_\pi \geq 1$ (par définition de L_π) et il suffit de calculer L"(E/$\mathbb{Q}$, 1) pour conclure.
De même, pour la courbe $y^2 = x^3 - 226x$ de rang 3, $r_\pi \geq 3$ (par la théorie et un calcul de la hauteur), donc =3 par un calcul de la dérivée 3-ième. Le signe de l'équation fonctionnelle est —1, donc r_∞ est impair: s'il valait 1, Perrin Riou [87] +Gross et Zagier [86] impliqueraient que $r_\pi = 1$, donc r_∞ est au moins égal à 3 et un calcul de la dérivée 3 ème de la fonction L permet de conclure.

Bibliographie

D. Bernardi, C. Goldstein et N.Stephens [84]: "Notes p-adiques sur les courbes elliptiques", *Journal für die reine und angewandte Mathematik*, **351**, (1984), 129-170.
J.Coates et A. Wiles [77]: "On the conjecture of Birch and Swinnerton-Dyer", *Inventiones Math.*, **39**, (1977), 223-251.
J.Coates et A.Wiles [78]: "On p-adic L-functions and elliptic units", *Journal of Austr. Math. Soc.* Series A, **26**, (1978), 1-25.
B.Gross et D.Zagier [86]: "Heegner points and derivatives of L-functions", *Inventiones Math.*, **84**, 225-320.
V.A. Kolyvagin [88a]: "Finiteness of E() and Ш(E/) for a class of Weil curves" (in Russian), *Izv. Akad. Nauk.SSSR* Series Mat., **52**, (1988).
V.A.Kolyvagin [88b]: "Euler systems" (transl. N.Koblitz), à paraître dans le recueil d'articles en hommage à Grothendieck.
S. Lang [1983]: "Conjectured Diophantine estimates on elliptic curves", in *Arithmetic and Geometry* , PM 35, Birkhauser Boston (1983).
B.Perrin-Riou [83]: "Arithmétique des courbes elliptiques et théorie d'Iwasawa", Thèse d'Etat, (1983), Orsay.
B.Perrin-Riou [87]: "Points de Heegner et dérivées de fonctions L p-adiques", *Inventiones Math.*, **89**, (1987), 455-510.
B.Perrin-Riou [89]: "Travaux de Kolyvagin et Rubin", exposé au séminaire Bourbaki, novembre 1989.
K. Rubin [87]: "Tate-Safarevic groups and L-functions of elliptic curves with complex multiplication", *Inventiones Math.*, **93**, (1987), 527-560.
K.Rubin [88]: "A proof of some "main conjectures" via methods of Kolyvagin", Preprint.
P. Schneider [82]: "P-adic height pairings I", *Inventiones Math.*, **69** (1982), 401-409.
P. Schneider [85]: "P-adic height pairings II", *Inventiones Math.*, **79** (1985), 329-374.

On pourra aussi consulter les textes consacrés à ces travaux dans les actes du colloque sur les fonctions L, qui a eu lieu à Durham, en juillet 1989:
B. Gross: "Kolyvagin's work on modular elliptic curves".
K. Rubin: "Main conjecture for cyclotomic fields".

Catherine Goldstein
URA D0752
Bat 425
Université de Paris XI
91405 Orsay Cedex