MÉMOIRES DE LA S. M. F.

BERNADETTE PERRIN-RIOU

Arithmétique des courbes elliptiques et théorie d'Iwasawa

Mémoires de la S. M. F. 2^e série, tome 17 (1984)

<http://www.numdam.org/item?id=MSMF_1984_2_17__1_0>

Mémoire de la Société Mathématique de France, n° 17
Supplément au Bulletin de la S.M.F.
Tome 112, 1984, fascicule 4

ARITHMÉTIQUE DES COURBES ELLIPTIQUES ET THÉORIE D'IWASAWA

Bernadette PERRIN-RIOU

RÉSUMÉ

On applique à l'arithmétique des courbes elliptiques à multiplication complexe les méthodes d'Iwasawa sur les $\mathbb{Z}_p$-extensions et l'on relie la série caractéristique du groupe de Selmer relatif à un nombre premier ordinaire sur une $\mathbb{Z}_p$-extension aux hauteurs p-adiques construites de manière analogue à la hauteur complexe de Néron-Tate.

ABSTRACT

We apply the methods of the theory of $\mathbb{Z}_p$-extensions of Iwasawa to study the arithmetic of elliptic curves with complex multiplication. We link the characteristic power series of the Selmer group of the elliptic curve, relative to an ordinary prime p, to a canonical p-adic height on the curve which is analogous to the archimedean canonical height of Néron-Tate.

Bernadette PERRIN-RIOU
U. E. R. 48
Tour 45-46, 3ème étage
Université Pierre et Marie Curie
4, place Jussieu
75230 PARIS CEDEX 05
FRANCE

Texte reçu le 19 décembre 1983, révisé le 13 décembre 1984

0037-9484/84 04/01.130/$ 130/

Je dois tout d'abord remercier J. Coates qui m'a initié aux courbes elliptiques. Mes remerciements vont également à G. Poitou qui m'a introduit à l'arithmétique, à D. Bertrand pour l'intérêt qu'il a bien voulu accorderà ce travail, à P. Cassou-Noguès pour avoir accepté de faire partie du jury et à J. Sjöstrand qui m'a donné un sujet de seconde thèse. Je remercie D. Bernardi pour de nombreuses discussions fructueuses, en particulier à propos des exemples numériques.

C'est Mme Le Bronnec qui a assuré la frappe de ce texte. Je la remercie pour le goût et la gentillesse avec lesquels elle l'a fait.

COURBES ELLIPTIQUES ET THÉORIE D'IWASAWA

Introduction

Le résultat fondamental dû à Mordell et Weil concernant une courbe elliptique E définie sur un corps de nombres F est que le groupe $E(F)$ de ses points rationnels sur F est un groupe abélien de type fini. En fait, trouver un algorithme pour calculer le groupe $E(F)$ et son rang est un problème remontant à Diophante qui n'est toujours pas résolu. Dans la recherche du rang de $E(F)$ par la méthode classique de la descente apparaissent naturellement d'autres invariants arithmétiques comme le groupe de Shafarevitch et Tate de E sur F et la hauteur canonique de Néron et Tate qui est une forme bilinéaire sur $E(F)$ modulo torsion à valeurs dans $\mathbb{R}$ non dégénérée sur $E(F) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Dans les années trente, Hasse et Weil ont associé à la courbe elliptique E/F une fonction $L(E,s)$ d'une variable complexe construite comme produit sur les places v de F des fonctions zêta de la courbe réduite en v et conjecturé que cette fonction admet un prolongement analytique et une équation fonctionnelle pour le changement de s en $2-s$. Inspirés par les travaux de Siegel, Birch et Swinnerton-Dyer ont ensuite conjecturé que le comportement de $L(E,s)$ au point critique $s=1$ est lié aux invariants arithmétiques précédents. Dans le cas des courbes elliptiques à multiplication complexe, l'existence d'un Grössencharakter associé à E/F montrée par Deuring et Weil permet de démontrer la conjecture de Hasse-Weil. Par contre, nous connaissons très peu de choses sur le moyen de démontrer la conjecture de Birch et Swinnerton-Dyer.

Nous prenons dans cette thèse le point de vue p-adique qui a été inspiré à la fois par les travaux de Artin et Tate sur l'analogue géométrique de la conjecture de Birch et Swinnerton-Dyer et par les idées d'Iwasawa sur les $\mathbb{Z}_p$-extensions de corps de nombres. Nous supposons que E est une courbe elliptique à multiplication complexe et que p est un nombre premier tel que E a bonne réduction ordinaire en toute place de F au dessus de p. Soit $F_\infty = F(E_{p^\infty})$ le corps obtenu en rajoutant à F les points de p^n-torsion de E $(n \geq 1)$. Appelons dans cette introduction module d'Iwasawa de E/F_∞ le dual de Pontryagin du groupe de Selmer de E sur F_∞ relatif à p^∞. C'est un $\mathbb{Z}_p[[G(F_\infty/F)]]$-module de type fini. L'objet de cette thèse est l'étude de ce module et de sa série caractéristique lorsqu'il est de torsion. Nous commençons donc par donner des conditions pour que le module d'Iwasawa de E/F_∞ soit de torsion. Ces conditions sont liées aux conjec-

tures de Leopoldt. Nous montrons aussi, toujours sous des hypothèses de Leopoldt, qu'il est de dimension projective inférieure à 1.

La série caractéristique de ce module est conjecturalement liée aux fonctions L p-adiques à deux variables construites par Katz. Nous montrons pour cette série caractéristique l'analogue p-adique de la conjecture de Birch et Swinnerton-Dyer (Théorème V.17). Remarquons qu'il est possible de formuler cette conjecture p-adique même si le groupe de Shafarevitch-Tate n'est pas fini. La démonstration consiste à construire une famille de formes bilinéaires algébriques sur $E(F)$, associées aux caractères de $G(F_\infty/F)$ à valeurs dans $\mathbb{Z}_p^*$. Elles se déduisent en fait d'un pseudo-isomorphisme canonique entre le module d'Iwasawa de E/F_∞ et une version tordue de son adjoint (remarquons que ce pseudo-isomorphisme permet aussi de montrer une équation fonctionnelle sur sa série caractéristique (Théorème V.6), version fidèle des équations fonctionnelles des fonctions L complexes et p-adiques). D'autre part, ont été construites des formes bilinéaires appellées hauteurs p-adiques, analogues de la hauteur complexe de Néron-Tate, de nature analytique et facilement calculables. Le coeur de la démonstration est de montrer l'égalité entre ces deux familles de formes bilinéaires.

Enfin, pour égayer cette introduction de quelques exemples numériques, remarquons que la connaissance des propriétés arithmétiques de E/F et de ces formes bilinaires donne des renseignements sur la croissance du rang de E le long d'une $\mathbb{Z}_p$-extension de F contenue dans F_∞. Les exemples sont choisis parmi les courbes elliptiques $E : y^2 = x^3 - dx$ ($d \in \mathbb{Z}$) à multiplication complexe par $K = \mathbb{Q}(i)$. On prend comme nombre premier $p = 5$. Une $\mathbb{Z}_5$-extension de K joue un rôle particulier : c'est l'unique $\mathbb{Z}_5$-extension de K galoisienne sur $\mathbb{Q}$ et non abélienne sur $\mathbb{Q}$; on la note K_∞^-.

$E : y^2 = x^3 - x$. Le rang de $E(\mathbb{Q})$ sur $\mathbb{Z}$ est nul. Pour toute $\mathbb{Z}_5$-extension L_∞ de K, $E(L_\infty)$ modulo torsion est nul.

$E : y^2 = x^3 - 36x$. Le rang de $E(\mathbb{Q})$ sur $\mathbb{Z}$ est 1. Pour toute $\mathbb{Z}_5$-extension L_∞ de K sauf peut-être K_∞^-, $E(L_\infty)$ modulo torsion est de type fini.

$E : y^2 = x^3 - 2x$. Le rang de $E(\mathbb{Q})$ sur $\mathbb{Z}$ est 1. Pour toute $\mathbb{Z}_5$-extension L_∞ de K sauf peut-être K_∞^-, $E(L_\infty)$ modulo torsion est de type fini. De plus si N_∞ est l'unique $\mathbb{Z}_5$-extension de K non ramifiée au dehors de $(2+i)$, $E(N_\infty)$ modulo torsion est de rang 2 sur $\mathbb{Z}$.

$E : y^2 = x^3 + 14x$. Le rang de $E(\mathbb{Q})$ sur $\mathbb{Z}$ est 2. Pour toute $\mathbb{Z}_5$-extension L_∞ de K sauf peut-être pour deux d'entre elles, $E(L_\infty)$ modulo torsion est de rang fini. Les niveaux finis de ces deux $\mathbb{Z}_5$-extensions peuvent être calculés explicitement.

$E : y^2 = x^3 - 226x$. Le rang de $E(\mathbb{Q})$ sur $\mathbb{Z}$ est 3. Pour toute $\mathbb{Z}_5$-extension L_∞ sauf peut-être K_∞^-, $E(L_\infty)$ modulo torsion est de type fini.

Finalement, donnons un résumé de chacun des chapitres. Dans le chapitre I, on rappelle les résultats sur les $\mathbb{Z}_p[[T_1,\ldots,T_r]]$-modules qui seront nécessaires par la suite[1]. Dans le chapitre II, après avoir introduit les objets qui seront utilisés (par exemple divers groupes de Selmer) et les avoir comparés, on étudie la structure de $G(F_\infty/F)$-module du groupe de Selmer de E/F_∞ et on montre que son dual de Pontryagin est de dimension projective sur $\mathbb{Z}_p[[G(F_\infty/F)]]$ inférieure ou égale à 1 sous certaines hypothèses reliées à la conjecture de Leopoldt que nous supposerons par la suite. Dans le chapitre III, on définit les hauteurs p-adiques attachées à une $\mathbb{Z}_p$-extension et on donne un moyen pratique de les calculer. Dans le chapitre IV, on construit une forme bilinéaire algébrique attachée à la $\mathbb{Z}_p$-extension particulière N_∞ et on la relie à la hauteur p-adique définie dans le chapitre III. Dans le chapitre V, on étudie le cas d'une $\mathbb{Z}_p$-extension quelconque de F contenue dans F_∞ et on démontre l'analogue p-adique de la conjecture de Birch et Swinnerton-Dyer pour la série caractéristique du module d'Iwasawa de E/F_∞ et l'équation fonctionnelle p-adique.

Certains des exemples numériques s'appuient sur les calculs faits dans [3]. D'autre part, précisons que, dans le but d'être complet, nous avons repris les démonstrations de résultats précédemment parus ([25], [26]), la partie réellement nouvelle étant le chapitre V.

(1) voir aussi la thèse de 3ème cycle de Patrick Billot (Orsay 1984).

Notations.

Si M est un ensemble fini, on note $\#(M)$ son cardinal.

Si L est un sous-$\mathbb{Z}_p$-module de L' d'indice fini, on note $[L' : L]$ cet indice.

Si F'/F est une extension finie, on note $N_{F'/F}$ la norme de F' sur F et $tr_{F'/F}$ la trace.

Si F'/F est une extension galoisienne, $G(F'/F)$ désigne le groupe de Galois de F' sur F.

Si M est un $\mathbb{Z}_p$-module, on note $\hat{M}$ son dual de Pontryagin : $\hat{M} = \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$.

Si A est un anneau commutatif intègre unitaire et a et b deux éléments de A, le symbole $a \sim b$ signifie que $a = ub$ avec u unité de A; si M est un A-module, M_a désigne le noyau de la multiplication par a sur M et $M(a)$ est la réunion des M_{a^n} pour $n \in \mathbb{N}$; l'expression "M est un A-module de torsion" signifie que M est un A-module de A-torsion.

Si M est un $\mathbb{Z}_p$-module et G un groupe opérant sur M, M_G désigne le plus grand $\mathbb{Z}_p$-module quotient de M sur lequel G opère trivialement et M^G le plus grand sous $\mathbb{Z}_p$-module de M sur lequel G opère trivialement. Le dual de Pontryagin $\hat{M}$ est muni de l'action de G suivante

$$(g\phi)(m) = \phi(g^{-1}m)$$

pour $g \in G$, $\phi \in \hat{M}$, $m \in M$.

Chapitre I. Généralités sur les Λ-modules.

Soit Λ un anneau local régulier complet de dimension r et de corps résiduel fini de caractéristique p. Tous les Λ-modules considérés dans ce paragraphe sont supposés compacts et de type fini. Ils sont caractérisés de la manière suivante : si m est l'idéal maximal de Λ, un Λ-module compact M est de type fini si et seulement si M/mM est fini.

1. Généralités ([5]).

1.1. Définitions.

Si $\mathfrak{q}$ est un idéal premier, le localisé $\Lambda_{\mathfrak{q}}$ de Λ en $\mathfrak{q}$ est défini comme le sous-anneau du corps des fractions de Λ formé des éléments x/y avec x et y appartenant à Λ et y n'appartenant pas à $\mathfrak{q}$. Le localisé $M_{\mathfrak{q}}$ d'un Λ-module M est $M \otimes_{\Lambda} \Lambda_{\mathfrak{q}}$. On peut de même définir le localisé d'un homomorphisme de Λ-modules. Un Λ-module est dit pseudo-nul si son localisé en tout idéal premier de hauteur 1 est nul. Cela est équivalent à ce qu'il est annulé par deux éléments de Λ premiers entre eux. Un homomorphisme de Λ-modules est dit pseudo-isomorphisme si son localisé en tout idéal premier de hauteur 1 est un isomorphisme. Cela est équivalent à ce que son noyau et conoyau sont pseudo-nuls. Un Λ-module sans torsion est dit réflexif si il est égal à l'intersection de ses localisés en tout idéal premier de hauteur 1 (les localisés étant plongés dans l'espace vectoriel engendré par le Λ-module sur le corps de fractions de Λ).

Exemple 1. Si $r = 1$, les modules pseudo-nuls sont nuls; si r est égal à 1 ou 2, les Λ-modules réflexifs sont les Λ-modules libres.

1.2. Théorème de structure.

Les Λ-modules compacts de type fini sont caractérisés à pseudo-isomorphisme près par le théorème de structure bien connu suivant.

Théorème 1. (i) *Si M est un Λ-module compact de type fini sans torsion, il existe un homomorphisme injectif de M dans un Λ-module réflexif dont le conoyau est pseudo-nul et déterminé à isomorphisme près par M.*

(ii) *Si M est un Λ-module compact de type fini de Λ-torsion, il existe un unique Λ-module de la forme*