Conjecture de Zagier pour l'extension des scalaires d'une courbe elliptique

François Brunault (ÉNS Lyon)
francois.brunault@ens-lyon.fr

20 juin 2011

Soit E une courbe elliptique définie sur $\mathbf{Q}$.

$$E : y^2 = x^3 + ax + b \qquad a, b \in \mathbf{Z} \qquad \Delta := 4a^3 + 27b^2 \neq 0$$

Pour p premier $\nmid 2\Delta$, on pose

$$E_p : y^2 = x^3 + \overline{a}x + \overline{b} \qquad \overline{a}, \overline{b} \in \mathbf{Z}/p\mathbf{Z} \qquad \overline{\Delta} \neq 0$$
$$a_p := p + 1 - \#E_p(\mathbf{Z}/p\mathbf{Z}).$$

Pour $s \in \mathbf{C}$, on pose

$$L_{\{2\Delta\}}(E, s) = \prod_{p \nmid 2\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Remarque

$|a_p| \leq 2\sqrt{p} \Rightarrow L_{\{2\Delta\}}(E, s)$ converge pour $\Re(s) > \frac{3}{2}$.

Soit E une courbe elliptique définie sur $\mathbf{Q}$.

Pour p premier quelconque, on définit E_p comme la réduction modulo p d'une équation *minimale en p*, et on pose

$$a_p := p + 1 - \#E_p(\mathbf{Z}/p\mathbf{Z})$$

$$\varepsilon(p) := \begin{cases} 1 & \text{si } E_p \text{ est une courbe elliptique} \\ 0 & \text{sinon.} \end{cases}$$

Définition

$$L(E, s) = \prod_{p \text{ premier}} \frac{1}{1 - a_p p^{-s} + \varepsilon(p) p^{1-2s}}.$$

Propriétés

1. $L(E,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \qquad a_n \in \mathbf{Z}$.
2. $L(E,s)$ converge absolument pour $\Re(s) > \frac{3}{2}$.
3. Grâce à la modularité de E [Breuil, Conrad, Diamond, Taylor, Wiles], $L(E,s)$ se prolonge en une fonction entière sur $\mathbf{C}$ et vérifie une équation fonctionnelle.

$$\Lambda(E,s) := N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$$
$$\Lambda(E,s) = w_E\Lambda(E,2-s) \qquad w_E = \pm 1 \quad \text{« root number ».}$$

Le calcul de $L(E,s)$ est implémenté dans Pari/GP.

Méthode générale pour calculer $L(s) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s}$:

1. On pose $f(z) := \sum_{n=1}^{\infty} a_n e^{2i\pi nz} \qquad (z \in \mathbf{C}, \Im(z) > 0)$.
2. Par construction $(2\pi)^{-s}\Gamma(s)L(s) = \int_0^{+\infty} f(iy) y^{s-1} dy$.
3. Lorsque $y \to +\infty$ on a $f(iy) = O(e^{-2\pi y})$.
4. Éq. fonctionnelle de $L(s) \leftrightarrow$ Éq. fonctionnelle de $f(iy)$.

$\longrightarrow$ Algorithme de T. Dokchitser (*ComputeL*).

Remarque

On suppose le prolongement et l'équation fonctionnelle de $L(s)$.

Le *dilogarithme de Bloch-Wigner* $D : \mathbf{P}^1(\mathbf{C}) \to \mathbf{R}$ est défini par

$$\begin{cases} D(x) = \Im\left(\sum_{n=1}^{\infty} \frac{x^n}{n^2}\right) + \log|x| \arg(1-x) \text{ si } |x| \leq 1, \\ D(x) = -D(1/x) \text{ si } |x| \geq 1, \\ D(0) = D(1) = D(\infty) = 0. \end{cases}$$

Propriétés

1. D est continue sur $\mathbf{P}^1(\mathbf{C})$, analytique-réelle sur $\mathbf{C} - \{0,1\}$.
2. Relations de distribution $D(x^m) = m \cdot \sum_{\zeta^m=1} D(x\zeta)$.
3. Lien entre $\zeta_F(2)$ et $D|_{\mathbf{P}^1(F)}$ si F est un corps de nombres (conjecture de Zagier).

Pari/GP : $D(x) = \mathrm{polylog}(2,x,2)$.

Soit E une courbe elliptique définie sur $\mathbf{R}$.

$$E(\mathbf{C}) \cong \frac{\mathbf{C}}{\mathbf{Z}+\tau\mathbf{Z}} \cong \mathbf{C}^*/q^{\mathbf{Z}} \qquad (q = e^{2i\pi\tau})$$
$$[z] \mapsto [e^{2i\pi z}].$$

Définition (Dilogarithme elliptique de Bloch)

$$D_E : \mathbf{C}^*/q^{\mathbf{Z}} \to \mathbf{R}$$
$$[x] \mapsto \sum_{n=-\infty}^{\infty} D(xq^n).$$

$$D_E([x]) = \sum_{n=-\infty}^{\infty} D(xq^n)$$

Propriétés

1. Convergence exponentielle de la série définissant D_E.
2. D_E est continue sur $E(\mathbf{C})$, analytique-réelle sur $E(\mathbf{C}) - \{0\}$.
3. Relations de distribution $D_E(mP) = m \cdot \sum_{Q \in E[m]} D(P+Q)$.
   En particulier $D_E(-P) = -D_E(P)$.
4. Si E est une courbe elliptique à multiplication complexe, Bloch a relié $L(E,2)$ à $D_E|_{E_{\mathrm{tors}}}$.

Soit E une courbe elliptique définie sur $\mathbf{Q}$.

On étend D_E à $\mathbf{Z}[E(\mathbf{C})]$ par linéarité :

$$D_E\left(\sum_{i=1}^{r} n_i[P_i]\right) := \sum_{i=1}^{r} n_i D_E(P_i).$$

Conjecture de Zagier (1re version)

Il existe $\ell \in \mathbf{Z}[E(\overline{\mathbf{Q}})]^{\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})}$ *et* $\alpha \in \mathbf{Q}^*$ *tel que*

$$L(E,2) = \alpha \cdot \pi \cdot D_E(\ell).$$

Remarque

Nombreux exemples numériques, mais très peu sont prouvés !

Cohen et Zagier ont déterminé expérimentalement des conditions sur $\ell \in \mathbf{Z}[E(\mathbf{Q})]$ pour que $D_E(\ell) \in \mathbf{Q} \cdot \frac{L(E,2)}{\pi}$.

Soit $\ell = \sum_{i=1}^r n_i [P_i] \in \mathbf{Z}[E(\overline{\mathbf{Q}})]^{\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})}$ et $K = \mathbf{Q}(P_1, \ldots, P_r)$.

1. $\sum_{i=1}^r n_i P_i^3 = 0$ dans $\mathrm{Sym}^3 E(K) \otimes \mathbf{Q}$.
2. Condition de hauteur locale en toute place v de K.
3. Condition d'intégralité en tout premier p tel que E a réduction multiplicative déployée en p.

On pose $\mathcal{A}_{E/\mathbf{Q}} = \{\ell \in \mathbf{Z}[E(\overline{\mathbf{Q}})]^{\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})} \text{ vérifiant } (1), (2) \text{ et } (3)\}$.

Conjecture de Zagier (2e version)

$D_E(\mathcal{A}_{E/\mathbf{Q}}) = \alpha \frac{L(E,2)}{\pi} \cdot \mathbf{Z}$ avec $\alpha \in \mathbf{Q}^*$.

Lien avec la K-théorie : Goncharov et Levin ont construit une application naturelle surjective $\delta : \mathcal{A}_{E/\mathbf{Q}} \otimes \mathbf{Q} \longrightarrow K_2(E_{\mathbf{Z}}) \otimes \mathbf{Q}$.

On a un diagramme commutatif

$$\begin{tikzcd}
\mathcal{A}_{E/\mathbf{Q}} \otimes \mathbf{Q} \arrow[r, "\delta"] \arrow[dr, "D_E"'] & K_2(E_{\mathbf{Z}}) \otimes \mathbf{Q} \arrow[d, "\mathrm{rég}_E"] \\
& \mathbf{R}
\end{tikzcd}$$

Une préimage de $\{f, g\} \in K_2(E_{\mathbf{Z}}) \otimes \mathbf{Q}$ est donnée par la convolution des diviseurs de f et g.

Le noyau de δ est engendré par les relations de distribution et les « relations de Steinberg » provenant de $K_2(\mathbf{Q}(E))$.
$\longrightarrow$ Cela permet (au moins en théorie) de ramener un calcul dans K_2 à un calcul de diviseurs.

Théorème (Goncharov-Levin)

Pour toute courbe elliptique $E/\mathbf{Q}$, il existe $\ell \in \mathcal{A}_{E/\mathbf{Q}}$ tel que $D_E(\ell) \in \mathbf{Q}^* \cdot \frac{L(E,2)}{\pi}$.

Remarque

La preuve repose sur la paramétrisation modulaire de E, ce qui rend ℓ inexplicite en général. En particulier :

1. On ne sait pas borner a priori le corps de nombres engendré par les points du support de ℓ.
2. On ne sait pas borner a priori la hauteur de ces points.

Question ouverte : trouver un ℓ explicite lorsque la paramétrisation modulaire de E est de degré ≥ 2.

Soit $E/\mathbf{Q}$ une courbe elliptique, et F un corps de nombres.

On note $E/F := E \otimes_{\mathbf{Q}} F$ l'extension des scalaires à F.

On dispose de $L(E/F, s)$ définie de manière analogue.

Propriétés

1. $L(E/F, s)$ converge pour $\Re(s) > \frac{3}{2}$.
2. Si F est contenu dans une extension *résoluble* de $\mathbf{Q}$, on connaît le prolongement holomorphe et l'équation fonctionnelle de $L(E/F, s)$ (théorie du changement de base pour les formes automorphes). Mais en général, le prolongement et l'équation fonctionnelle de $L(E/F, s)$ sont conjecturaux.

Propriétés (suite)

3. Si $F/\mathbf{Q}$ est galoisienne, on a

$$L(E/F,s) = \prod_{\rho} L(E \otimes \rho, s)^{\dim \rho}$$

où ρ parcourt les représentations irréductibles de $\mathrm{Gal}(F/\mathbf{Q})$.

4. En général, si K est la clôture galoisienne de F, alors

$$L(E/F,s) = \prod_{\rho} L(E \otimes \rho, s)^{m_\rho}$$

où ρ parcourt les représentations irréductibles de $\mathrm{Gal}(K/\mathbf{Q})$ et m_ρ est la multiplicité de ρ dans $\mathbf{C}[\mathrm{Gal}(K/\mathbf{Q})/\mathrm{Gal}(K/F)]$.

Pour simplifier, supposons F totalement réel, de degré $n \geq 1$. Notons $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$ les plongements de F dans $\mathbf{R}$.

Posons $\mathcal{A}_{E/F} = \{\ell \in \mathbf{Z}[E(\overline{\mathbf{Q}})]^{\mathrm{Gal}(\overline{\mathbf{Q}}/F)} \text{ vérifiant } (1), (2) \text{ et } (3)\}$.

Chaque $\sigma \in \Sigma$ induit une injection $\mathbf{Z}[E(\overline{\mathbf{Q}})]^{\mathrm{Gal}(\overline{\mathbf{Q}}/F)} \hookrightarrow \mathbf{Z}[E(\mathbf{C})]$.

Conjecture

1. *Il existe $\ell_1, \ldots, \ell_n \in \mathcal{A}_{E/F}$ tels que $L(E/F, 2) \sim_{\mathbf{Q}^*} \pi^n \det(D_E(\sigma_i(\ell_j)))_{1 \leq i,j \leq n}$.*
2. *On pose $\vec{D}_E = (D_E \circ \sigma_1, \ldots, D_E \circ \sigma_n)$. Alors $\vec{D}_E(\mathcal{A}_{E/F})$ est un réseau de $\mathbf{R}^n$ de covolume $\alpha \pi^{-n} L(E/F, 2)$ avec $\alpha \in \mathbf{Q}_{>0}$.*

On suppose $F/\mathbf{Q}$ finie *abélienne*. On note $\widehat{G}$ l'ensemble des caractères de $G = \mathrm{Gal}(F/\mathbf{Q})$.

Théorème (B.)

Il existe $\ell \in \mathcal{A}_{E/F}$ tel que pour tout $\chi \in \widehat{G}$, on ait

$$L'(E \otimes \chi, 0) \sim_{\mathbf{Q}^*} \begin{cases} \frac{1}{\pi} \cdot \sum_{\sigma \in G} \chi(\sigma) D_E(\sigma(\ell)) & si\ \chi\ pair \\ \frac{1}{\pi \Im(\tau)} \cdot \sum_{\sigma \in G} \chi(\sigma) J_E(\sigma(\ell)) & si\ \chi\ impair. \end{cases}$$

Corollaire

La version faible de la conjecture de Zagier pour $L(E/F, 2)$ est vraie.

Idée de la preuve : soit $\varphi : X_1(N) \to E$ une paramétrisation modulaire.

$$\begin{tikzcd} X_1(N)_F \arrow[r] \arrow[d, "\varphi_F"'] & X_1(N) \arrow[d, "\varphi"] \\ E_F \arrow[r] & E. \end{tikzcd}$$

Point-clé : $X_1(N)_F$ est une courbe modulaire (au sens adélique).
On utilise alors un théorème de Beilinson pour $X_1(N)_F$.

Remarque

Le diviseur ℓ est inexplicite en général.

On peut expliciter ℓ dans le cas suivant :

$E = X_1(11) : y^2 + y = x^3 - x^2 \qquad F = \mathbf{Q}(\zeta_{11})^+$

$E(F)$ est le sous-groupe de $X_1(11)$ engendré par les pointes (on a $E(F) \cong \mathbf{Z}/25\mathbf{Z}$). On obtient

$$L(E/F, 2) = \frac{2^{10}5^9}{11^{11}}\pi^5 \det M$$

où $M \in \mathcal{M}_5(\mathbf{R})$ est définie par

$$M_{i,j} = 2D_E(2P + 2(i-j)Q) - D_E(P + (i-j)Q)$$

avec $P \in E(F)$ d'ordre 25 tel que $5P = Q = (0,0) \in E(\mathbf{Q})$.