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 $5P = Q = (0,0) \in E(\mathbf{Q})$.

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

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

21 juin 2011

On s'intéresse à la conjecture de Zagier pour $L(E/F,2)$ où E est une courbe elliptique définie sur $\mathbf{Q}$ et F est un corps de nombres.

Soit Σ l'ensemble des plongements de F dans $\mathbf{C}$. On note

$$\begin{aligned}
\Sigma_{\mathbf{R}} &= \{\sigma_1, \ldots, \sigma_{r_1}\} \\
\Sigma_{\mathbf{C}} &= \{\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}\} \\
[F:\mathbf{Q}] &= n = r_1 + 2r_2.
\end{aligned}$$

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

On dispose des fonctions dilogarithmes de Bloch $D_E : E(\mathbf{C}) \to \mathbf{R}$ et $J_E : E(\mathbf{C}) \to \mathbf{R}$. On a $D_E(\overline{P}) = D_E(P)$ et $J_E(\overline{P}) = -J_E(P)$ pour tout $P \in E(\mathbf{C})$.

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

Définition

On définit $\vec{D_E} : \mathbf{Z}[E(\overline{\mathbf{Q}})]^{\mathrm{Gal}(\overline{\mathbf{Q}}/F)} \to \mathbf{R}^n$ par

$$\vec{D_E} = \begin{pmatrix} D_E \circ \sigma_1 \\ \vdots \\ D_E \circ \sigma_{r_1+r_2} \\ J_E \circ \sigma_{r_1+1} \\ \vdots \\ J_E \circ \sigma_{r_1+r_2} \end{pmatrix}$$

Conjecture

Il existe $\ell_1, \ldots, \ell_n \in \mathcal{A}_{E/F}$ *tels que*

$$L(E/F,2) \sim_{\mathbf{Q}^*} \frac{\pi^n}{\mathfrak{I}(\tau)^{r_2}} \det(\vec{D_E}(\ell_1), \ldots, \vec{D_E}(\ell_n)).$$

Lorsque $F/\mathbf{Q}$ n'est pas abélienne, on ne sait démontrer *aucun exemple* de cette conjecture.

On va vérifier numériquement cette conjecture sur un exemple.

Idée : soit $K_m = \mathbf{Q}(E[m])$ avec $m \geq 1$.
L'extension $K_m/\mathbf{Q}$ est galoisienne et en général non abélienne.
Comme $E[m] \subset E(K_m)$, on peut espérer utiliser les points de $E[m]$ pour vérifier la conjecture pour $L(E/K_m, 2)$.

Pour $m = 2$ on a génériquement $\mathrm{Gal}(\mathbf{Q}(E[2])/\mathbf{Q}) \cong \mathfrak{S}_3$.
Problème : D_E et J_E sont impaires donc s'annulent sur $E[2]$...
$\longrightarrow$ On choisit E telle que $E(K_2)$ contient strictement $E[2]$.

Exemple

$E = X_1(11) : y^2 + y = x^3 - x^2$

$E(\mathbf{Q}) \cong \mathbf{Z}/5\mathbf{Z}$ engendré par $P = (0,0)$.

On note (Q_1, Q_2) une base de $E[2]$ telle que $Q_1 \in E(\mathbf{R})$.

$$\begin{tikzcd}[arrows=dash]
K = \mathbf{Q}(E[2]) \arrow[d, "2"] \arrow[dd, bend right=60, "\mathfrak{S}_3"'] \\
F = \mathbf{Q}(Q_1) \arrow[d, "3"] \\
\mathbf{Q}
\end{tikzcd}$$

$E(F) \cong \mathbf{Z}/10\mathbf{Z}$ engendré par $P + Q_1$.

On vérifie que $\mathbf{Z}[E(F)] \subset \mathcal{A}_{E/F}$ (cf. Magma).

Par imparité de $\vec{D}_E$, il suffit de considérer les diviseurs à support dans $\{P, 2P, P+Q_1, 2P+Q_1\}$. De plus $2\vec{D}_E(2P) = 3\vec{D}_E(P)$. On prend donc

$$\ell_1 = [P] \qquad \ell_2 = [P+Q_1] \qquad \ell_3 = [2P+Q_1]$$

$$R := \begin{vmatrix} D_E(P) & D_E(P+Q_1) & D_E(2P+Q_1) \\ D_E(P) & D_E(P+Q_2) & D_E(2P+Q_2) \\ 0 & J_E(P+Q_2) & J_E(2P+Q_2) \end{vmatrix}$$

Numériquement (à 30 décimales) $L(E/F,2) \stackrel{?}{=} -\frac{(10\pi)^3}{11^4 \Im(\tau)} \cdot R$.

Remarques

1. Comme R est divisible par $D_E(P)$ et grâce à la formule $L(E,2) = \frac{10\pi}{11} D_E(P)$, on obtient une expression conjecturale pour $L(E \otimes \rho, 2)$, où ρ est l'unique représentation irréductible de dimension 2 de $\mathrm{Gal}(K/\mathbf{Q})$.
2. Il serait intéressant de vérifier numériquement la conjecture sur d'autres exemples (par exemple pour une extension non résoluble de $\mathbf{Q}$, ou pour des familles de courbes elliptiques).
3. Un obstacle est le temps de calcul de $L(E/F, s)$ qui devient rapidement prohibitif lorsque le discriminant de F augmente.

Idée : si $F/\mathbf{Q}$ est finie galoisienne et $G = \mathrm{Gal}(F/\mathbf{Q})$, alors

$$V := \mathbf{Z}[E(F)] \cap \mathcal{A}_{E/F}$$

est un $\mathbf{Z}[G]$-module. Soit ρ une représentation irréductible de G qui apparaît dans $V \otimes \overline{\mathbf{Q}}$. On note V_ρ la composante ρ-isotypique de $V \otimes \overline{\mathbf{Q}}$. Si $\vec{D}_E(V_\rho) \neq 0$ alors on peut espérer exprimer $L(E \otimes \overline{\rho}, 2)$ en termes d'un déterminant de $\vec{D}_E(V_\rho)$.

Soit E une courbe elliptique sur $\mathbf{Q}$. On rappelle que D_E vérifie une relation de *m-distribution* pour tout $m \in \mathbf{Z} - \{0\}$:

$$D_E(mP) = m \sum_{Q \in E[m]} D_E(P+Q) \qquad (P \in E(\mathbf{C})).$$

Pour $f, g \in \mathbf{C}(E)^\times$, posons

$$\begin{aligned} \operatorname{div}(f) &= \sum_i m_i [P_i] \\ \operatorname{div}(g) &= \sum_i n_j [Q_j] \\ \beta(f,g) &:= \sum_{i,j} m_i n_j [P_i - Q_j] \in \mathbf{Z}[E(\mathbf{C})]. \end{aligned}$$

L'application $(f,g) \mapsto \beta(f,g)$ est bilinéaire.

Théorème (Bloch)

Pour tout $f \in \mathbf{C}(E) - \{0,1\}$, *on a*

$$D_E\big(\beta(f, 1-f)\big) = 0$$

Remarques

1. Le théorème de Bloch et le théorème de Matsumoto entraînent que $D_E \circ \beta$ se factorise par $K_2(\mathbf{C}(E))$. Le morphisme $K_2(\mathbf{C}(E)) \to \mathbf{R}$ ainsi défini est l'*application régulateur* associée à E.
2. L'application β est compatible à l'action de Galois. En particulier si $f \in \mathbf{Q}(E) - \{0,1\}$ alors $\beta(f, 1-f) \in \mathbf{Z}[E(\overline{\mathbf{Q}})]^{\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})}$.

Le théorème de Bloch permet de montrer des relations de dépendance linéaire entre les valeurs de D_E en des points algébriques de E.

Zagier et Gangl ont conjecturé que le noyau de $D_E : \mathcal{A}_{E/\mathbf{Q}} \to \mathbf{R}$ est engendré par :

- les relations de m-distribution pour $m \in \{-1, 2\}$;
- les relations de Bloch $\beta(f, 1-f)$ pour $f \in \mathbf{Q}(E) - \{0, 1\}$.

Remarque

En notant $\mathcal{C}_{E/\mathbf{Q}}$ le groupe engendré par ces relations, la conjecture de Zagier prédit que $\mathcal{A}_{E/\mathbf{Q}}/\mathcal{C}_{E/\mathbf{Q}}$ est de rang 1.

On appelle *relation exotique* une relation de dépendance linéaire entre valeurs de D_E qui ne provient pas des relations de distribution.

Exemple

$E : y^2 + y = x^3 - x^2 \qquad P = (0,0) \qquad 2P = (1,-1)$
On prend $f = -y$. Alors

$$\begin{aligned} \mathrm{div}(f) &= \mathrm{div}(y) = 2[P] + [-2P] - 3[0] \\ \mathrm{div}(1-f) &= \mathrm{div}(y+1) = 2[-P] + [2P] - 3[0] \\ \beta(f, 1-f) &= -11[P] + 4[2P] + 4[-P] - 6[-2P] + 9[0] \end{aligned}$$

$$\begin{aligned} &\Rightarrow -15D_E(P) + 10D_E(2P) = 0 \\ &\Rightarrow 3D_E(P) = 2D_E(2P). \end{aligned}$$

Il est facile de détecter numériquement des relations $D_E(\ell) \stackrel{?}{=} 0$, au moyen de l'algorithme LLL implémenté dans Pari/GP.

$\longrightarrow$ Comment démontrer ces relations ?

Idée de Goncharov et Levin : on se donne trois droites concourantes $(d_i)_{i \in \mathbf{Z}/3\mathbf{Z}}$ dans $\mathbf{P}^2(\mathbf{C})$ et on pose

$$\ell_i := d_i \cap E \in \mathbf{Z}[E(\mathbf{C})] \qquad (i \in \mathbf{Z}/3\mathbf{Z}).$$

D'après le théorème de Bézout, ℓ_i est un diviseur de degré 3.

Proposition

On a $\sum_{i \in \mathbf{Z}/3\mathbf{Z}} D_E\big(\beta(\ell_i, \ell_{i+1})\big) = 0.$

Proposition

On a $\sum_{i \in \mathbf{Z}/3\mathbf{Z}} D_E\big(\beta(\ell_i, \ell_{i+1})\big) = 0$.

Démonstration.

On peut choisir des équations $f_i = 0$ des droites d_i de telle sorte que $f_3 = f_1 + f_2$. On pose $f = \frac{f_1}{f_3}$ et donc $1 - f = \frac{f_2}{f_3}$. Grâce à la relation de Bloch D_E s'annule sur le diviseur

$$\beta\Big(\frac{f_1}{f_3}, \frac{f_2}{f_3}\Big) = \beta(f_1, f_2) + \beta(f_2, f_3) + \beta(f_3, f_1)$$

par bilinéarité de β. On termine le calcul en utilisant le fait que $\mathrm{div}(f_i) = \ell_i - 3[0]$. $\square$

Remarque

On peut montrer que si les d_i sont concourantes en un point de E alors la relation précédente est triviale i.e. est conséquence de l'imparité de D_E. On cherche donc des droites concourantes en un point situé hors de E.

On en déduit une méthode pour trouver des relations exotiques.

1. On se donne un ensemble fini de points $S \subset E(\overline{\mathbf{Q}})$.
2. On calcule l'ensemble $\mathcal{D}$ des droites d telles que $d \cap E \subset S$.
3. On calcule l'ensemble $\mathcal{T}$ des triplets de droites de $\mathcal{D}$ concourantes en un point non situé sur E.
4. Pour chaque $(d_1, d_2, d_3) \in \mathcal{T}$, on calcule $\sum_i \beta(\ell_i, \ell_{i+1})$.

Résultats numériques

- Pour les courbes elliptiques de conducteur ≤ 210, on trouve numériquement 27 relations exotiques entre valeurs de D_E en des points de torsion rationnels de E.
- La méthode des droites concourantes utilisée avec $S = E(\mathbf{Q})_{\mathrm{tors}}$ permet de montrer 17 de ces relations.
- Dans chacun des 10 cas restants, on peut trouver une isogénie $\varphi : E' \to E$ telle que la méthode des droites concourantes appliquée à $(E', \varphi^{-1}(S))$ permette de montrer la relation voulue.
- Si l'on excepte les courbes elliptiques d'invariant $j = 0$, il ne semble pas y avoir d'autre relation exotique entre valeurs de D_E aux points de torsion rationnels de E.

Une autre application de la méthode des droites concourantes :

Conjecture de Zagier explicite pour
$E = X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20$

$$(\ast) \quad L(E,2) \stackrel{?}{=} \frac{4\pi}{55}\big(2D_E(2P) - D_E(P)\big) \qquad P = (5,5).$$

- La méthode de Beilinson ne marche pas pour $X_0(11)$.
- On utilise l'isogénie $\varphi : X_1(11) = E' \to E$ pour traduire (*) en une identité sur E' (relation de φ-distribution).
- On sait que $L(E,2)$ est proportionnel à une valeur de $D_{E'}$.
- On est ramenés à montrer une relation de dépendance linéaire entre valeurs de $D_{E'}$, ce qui peut se faire par la méthode des droites concourantes avec $S = \varphi^{-1}(E(\mathbf{Q})) \subset E'(\overline{\mathbf{Q}})$.

En général, pour démontrer une relation de dépendance linéaire entre valeurs de D_E par la méthode des droites concourantes, on est obligés d'inclure dans S des points algébriques, ainsi que des points d'ordre infini.

- On ne sait pas borner a priori la taille de l'ensemble S ni le corps de nombres engendré par S (ce problème est essentiellement équivalent à savoir calculer dans $K_2(E)$).
- Autre question ouverte : peut-on généraliser la méthode des droites concourantes aux courbes de genre ≥ 2 ?