

Courbes elliptiques, fonctions L et conjecture de Zagier

François Brunault

Exposé au séminaire de mathématiques pures, Université de
Clermont-Ferrand, mardi 15 novembre 2005

Les courbes elliptiques sont nées de l'étude au début du 19ème siècle des intégrales de la forme

$$\int \frac{dx}{\sqrt{P(x)}}$$

où P est un polynôme de degré 3 ou 4 à racines simples. La courbe C définie par l'équation $y^2 = P(x)$ est une courbe elliptique et l'intégrale ci-dessus se ramène à celle de la forme différentielle régulière dx/y sur C .

Soient $a, b \in \mathbf{Z}$ deux entiers tels que $\Delta := 4a^3 + 27b^2 \neq 0$. Considérons la courbe E définie par l'équation

$$E : y^2 = x^3 + ax + b.$$

D'un point de vue géométrique, E est une courbe projective non singulière (après ajout d'un point à l'infini). Étudions maintenant E d'un point de vue arithmétique : que peut-on dire sur l'ensemble $E(\mathbf{Q})$ des solutions rationnelles de l'équation ci-dessus ? Une idée naturelle consiste à réduire cette équation modulo différents nombres premiers. Pour tout nombre premier p , notons E_p la réduction de E modulo p : c'est une courbe projective sur le corps fini \mathbf{F}_p (non singulière pour $p \nmid 2\Delta$).

Question. Est-il possible de prédire l'arithmétique globale de E , par exemple l'ensemble $E(\mathbf{Q})$, à partir des données locales $E_p(\mathbf{F}_p)$, où p parcourt les nombres premiers ?

Le but de cet exposé est de montrer que la fonction L de E est l'outil approprié pour répondre à cette question. La fonction L de E est une fonction d'une variable complexe définie purement à partir des données locales $E_p(\mathbf{F}_p)$; conjecturalement, elle gouverne toute l'arithmétique de E .

1. Fonction L d'une courbe elliptique

La fonction L associée à une courbe elliptique sur \mathbf{Q} a été définie par Hasse et Weil. Considérons $E : y^2 = x^3 + ax + b$ comme ci-dessus. Soit p un nombre premier.

Définition 1. — On appelle équation minimale en p une équation obtenue par changement de variables affine à partir de E , de la forme

$$\tilde{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in \mathbf{Z}),$$

telle que la valuation p -adique du discriminant de cette équation soit minimale.

Théorème 2. — Il existe une équation $\tilde{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ qui est minimale en p pour tout nombre premier p .

Notons \tilde{E}_p la réduction modulo p d'une équation minimale en p pour E . D'après la propriété de minimalité de la valuation p -adique du discriminant, \tilde{E}_p ne dépend pas du choix de l'équation minimale en p . Plusieurs cas de figure sont possibles :

- \tilde{E}_p est une courbe elliptique sur \mathbf{F}_p . On dit que E a *bonne réduction* en p .
- \tilde{E}_p possède un point singulier ordinaire : E a *réduction multiplicative* en p .
- \tilde{E}_p possède un point de rebroussement : E a *réduction additive* en p .

Exemples. —

bonne réduction réduction multiplicative réduction additive

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

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

$$y^2 = x^3$$

Dans tous les cas, notons $\tilde{E}_p(\mathbf{F}_p)$ l'ensemble des points \mathbf{F}_p -rationnels de \tilde{E}_p (y compris le point à l'infini), et posons

$$a_p = p + 1 - \text{Card } \tilde{E}_p(\mathbf{F}_p)$$

Définition 3. — Soit S l'ensemble des nombres premiers en lesquels E a bonne réduction. La fonction L associée à E est définie par

$$L(E, s) = \prod_{p \notin S} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \cdot \prod_{p \in S} \frac{1}{1 - a_p p^{-s}} \quad (\Re(s) > \frac{3}{2}).$$

Remarque. — La convergence du produit infini ci-dessus pour $\Re(s) > \frac{3}{2}$ résulte des bornes de Hasse et Weil

$$|a_p| \leq 2\sqrt{p} \quad (p \text{ premier}).$$

La fonction $L(E, s)$ s'écrit sous la forme d'une série de Dirichlet

$$L(E, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Les coefficients a_n vérifient les relations suivantes.

$$\begin{aligned} a_{mn} &= a_m a_n && ((m, n) = 1) \\ a_{p^r} &= a_{p^{r-1}} a_p - p a_{p^{r-2}} && (p \notin S, r \geq 2) \\ a_{p^r} &= a_p^r && (p \in S, r \geq 0) \end{aligned}$$

On peut voir la fonction $L(E, s)$ comme une fonction rassemblant les propriétés locales de E . A priori le prolongement analytique d'une telle série de Dirichlet n'a rien d'évident !

2. Prolongement analytique de la fonction L

L'ingrédient essentiel pour prolonger la fonction $L(E, s)$ au plan complexe est le célèbre théorème suivant.

Théorème 4 (Wiles, Breuil, Conrad, Diamond, Taylor)

Toute courbe elliptique sur \mathbf{Q} est paramétrée par une courbe modulaire (quotient convenablement compactifié du demi-plan de Poincaré par un sous-groupe de congruence).

Plus précisément, notons N le *conducteur* de E . C'est un entier ≥ 1 qui mesure la complexité arithmétique de la réduction de E modulo les nombres premiers. En particulier, les nombres premiers divisant N sont exactement les nombres premiers de mauvaise réduction pour E . Le théorème ci-dessus prend la forme suivante : il existe un morphisme fini (surjectif) défini sur \mathbf{Q}

$$\phi : X_1(N) \rightarrow E,$$

où $X_1(N)$ est la courbe modulaire associée au sous-groupe de congruence

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}), a \equiv d \equiv 1 \pmod{N}, c \equiv 0 \pmod{N} \right\}.$$

L'existence du morphisme ϕ entraîne le prolongement holomorphe de $L(E, s)$, comme nous allons le voir. Considérons une équation \tilde{E} pour E qui est minimale en tous les nombres premiers. La *forme différentielle de Néron* ω_E est définie par $\omega_E = dx/(2y + a_1x + a_3)$. Notons ψ la composition

$$\psi : \mathcal{H} \rightarrow X_1(N)(\mathbf{C}) \rightarrow E(\mathbf{C})$$

où la première flèche est la projection naturelle. L'image réciproque $\psi^*\omega_E$ de ω_E par ψ est une forme différentielle holomorphe sur \mathcal{H} , invariante sous l'action de $\Gamma_1(N)$. On a

$$\psi^*\omega_E = 2\pi icf(z)dz$$

avec $c \in \mathbf{Q}^*$ et f forme parabolique primitive de poids 2 pour $\Gamma_1(N)$. Rappelons succinctement la définition des formes paraboliques primitives de poids 2 pour $\Gamma_1(N)$:

- $f : \mathcal{H} \rightarrow \mathbf{C}$ est holomorphe
- $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$ pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$.
- f “s’annule aux pointes” (parabolique).
- f est primitive, c'est-à-dire propre pour l'algèbre de Hecke, nouvelle et normalisée.

La fonction f admet un développement de Fourier

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2i\pi n z} \quad (z \in \mathcal{H})$$

où les coefficients a_n coïncident avec ceux de la série de Dirichlet $L(E, s)$ (ceci est crucial pour démontrer le prolongement analytique de cette dernière fonction).

Conjecture 5 (Manin). — *Si ϕ est une paramétrisation optimale de E alors $c = \pm 1$.*

Manin a initialement formulé cette conjecture avec la courbe $X_0(N)$ au lieu de $X_1(N)$. Stevens a raffiné cette conjecture et a montré en particulier qu'il existe toujours une paramétrisation optimale de E par $X_1(N)$ (ce résultat est faux pour $X_0(N)$).

Proposition 6. — Soit $\phi : X_1(N) \rightarrow E$ une paramétrisation de E . La fonction $L(E, s)$ admet un prolongement holomorphe au plan complexe et nous avons la formule

$$L(E, 1) = -\frac{1}{c} \int_{\psi_*\{0, \infty\}} \omega_E$$

où $\psi_*\{0, \infty\}$ est l'image directe par ψ de la géodésique reliant 0 à ∞ dans \mathcal{H} .

Démonstration. — Puisque f est une forme parabolique, l'intégrale $\int_0^\infty y^{s-1} f(iy) dy$ converge pour tout $s \in \mathbf{C}$ et définit une fonction holomorphe de s . Pour $\Re(s) > \frac{3}{2}$ nous avons

$$\begin{aligned} \int_0^\infty y^{s-1} f(iy) dy &= \sum_{n=1}^\infty a_n \int_0^\infty y^{s-1} e^{-2\pi n y} dy \\ &= \sum_{n=1}^\infty \frac{a_n}{(2\pi n)^s} \int_0^\infty u^{s-1} e^{-u} du \quad (u = 2\pi n y) \\ &= (2\pi)^{-s} \Gamma(s) L(E, s). \end{aligned}$$

Puisque la fonction Γ ne s'annule pas, on en déduit le prolongement holomorphe de $L(E, s)$ à \mathbf{C} . Pour $s = 1$ nous obtenons

$$\begin{aligned} L(E, 1) &= 2\pi \int_0^\infty f(iy) dy \\ &= -\frac{1}{c} \int_0^\infty \psi^* \omega_E \\ &= -\frac{1}{c} \int_{\psi_*\{0, \infty\}} \omega_E. \end{aligned}$$

□

Corollaire 7. — Notons Ω_E^+ la période réelle de E , définie par $\Omega_E^+ = \int_{E^0(\mathbf{R})} \omega_E$, où $E^0(\mathbf{R})$ est la composante neutre de $E(\mathbf{R})$. Alors $L(E, 1) \in \mathbf{Q} \cdot \Omega_E^+$.

Remarque. — Dans le cas où $L(E, 1) \neq 0$, la conjecture de Birch et Swinnerton-Dyer prédit la quantité $L(E, 1)/\Omega_E^+ \in \mathbf{Q}^*$.

Nous voyons donc une interprétation géométrique de la valeur spéciale $L(E, 1)$: à un facteur rationnel près, $L(E, 1)$ est une période de la forme différentielle ω_E . Peut-on trouver une interprétation géométrique analogue pour la valeur spéciale $L(E, 2)$?

3. Conjecture de Zagier pour $L(E, 2)$

Dans le cas où E est à multiplication complexe, Bloch a découvert une formule étonnante donnant $L(E, 2)$ en termes d'une fonction appelée dilogarithme elliptique, définie uniquement en termes de la géométrie de E . Nous commençons par énoncer les résultats de Bloch, qui sont à l'origine de la conjecture de Zagier pour $L(E, 2)$.

Soit K un corps quadratique imaginaire, que nous supposons plongé dans \mathbf{C} . Supposons que l'anneau des entiers \mathcal{O}_K de K est principal. Considérons la courbe elliptique $E(\mathbf{C}) = \mathbf{C}/\mathcal{O}_K$. La théorie de la multiplication complexe et le fait que \mathcal{O}_K soit principal entraînent que E est définie sur \mathbf{Q} .

Définition 8. — Soit $\mathfrak{m} \subset \mathcal{O}_K$ un idéal non nul et $l \in \mathbf{Z}$. Un Grössencharakter de K de niveau \mathfrak{m} et de type à l'infini l est un homomorphisme

$$\chi : \{\text{idéaux fractionnaires de } K \text{ premiers à } \mathfrak{m}\} \rightarrow \mathbf{C}^*$$

vérifiant

$$\chi(\alpha \mathcal{O}_K) = \alpha^l \quad (\alpha \in 1 + \mathfrak{m}).$$

D'après Deuring, il existe un Grössencharakter χ_E de K de niveau \mathfrak{m}_E tel que

$$L(E, s) = L(\chi_E, s) := \sum_{\substack{\mathfrak{a} \subset \mathcal{O}_K \\ (\mathfrak{a}, \mathfrak{m}_E) = 1}} \frac{\chi_E(\mathfrak{a})}{(N\mathfrak{a})^s}$$

où $N\mathfrak{a} = \text{Card}(\mathcal{O}_K/\mathfrak{a})$ désigne la norme d'un idéal \mathfrak{a} de \mathcal{O}_K . On en déduit que $L(E, 2)$ s'exprime à l'aide d'une série d'Eisenstein-Kronecker. Posons $\mathcal{O}_K = \mathbf{Z} + \tau\mathbf{Z}$ avec $\Im(\tau) > 0$.

Théorème 9 (Bloch, Deninger). — Sous ces hypothèses, il existe un entier $C \geq 1$ et une application $F : (\frac{\mathbf{Z}}{C\mathbf{Z}})^2 \rightarrow \mathbf{C}$ tels que

$$L(E, 2) = \sum_{\substack{(m,n) \in \mathbf{Z}^2 \\ (m,n) \neq (0,0)}} \frac{F(\bar{m}, \bar{n})}{(m + \tau n)^2 (m + \bar{\tau} n)}$$

où (\bar{m}, \bar{n}) désigne la classe de (m, n) dans $(\frac{\mathbf{Z}}{C\mathbf{Z}})^2$. De plus, l'application F/π est à valeurs algébriques.

Pour $P \in E(\mathbf{C}) \cong \mathbf{C}/\mathcal{O}_K$, nous pouvons écrire $P = [u + \tau v]$ avec $u, v \in \mathbf{R}$, bien déterminés à l'addition d'un entier près.

Définition 10. — La fonction $R_\tau : E(\mathbf{C}) \rightarrow \mathbf{C}$ est définie par

$$R_\tau(P) = \sum_{\substack{(m,n) \in \mathbf{Z}^2 \\ (m,n) \neq (0,0)}} \frac{e^{2\pi i(mv - nu)}}{(m + \tau n)^2 (m + \bar{\tau} n)} \quad (P = [u + \tau v]).$$

On vérifie que $R_\tau(P)$ ne dépend pas du choix de u et v . Pour $(a, b) \in (\frac{\mathbf{Z}}{C\mathbf{Z}})^2$, posons $P_{a,b} = [\frac{a + \tau b}{C}] \in E(\mathbf{C})$: c'est un point de C -torsion de la courbe elliptique E . En décomposant la fonction F du théorème 9 en série de Fourier, nous obtenons l'expression suivante pour $L(E, 2)$

$$(1) \quad L(E, 2) = \sum_{(a,b) \in (\frac{\mathbf{Z}}{C\mathbf{Z}})^2} \widehat{F}(a, b) \cdot R_\tau(P_{a,b}),$$

où nous avons posé $\widehat{F}(a, b) = \sum_{(m,n) \in (\mathbf{Z}/C\mathbf{Z})^2} F(m, n) \cdot e^{2\pi i(mb - na)/C}$ pour $(a, b) \in (\frac{\mathbf{Z}}{C\mathbf{Z}})^2$.

Notons Li_2 la fonction dilogarithme

$$\text{Li}_2(z) = \sum_{n=1}^{\infty} \frac{z^n}{n^2} \quad (|z| < 1).$$

Cette fonction admet un prolongement (holomorphe, multivalué) à $\mathbf{C} - \{0, 1\}$. La fonction de Bloch-Wigner $D : \mathbf{P}^1(\mathbf{C}) \rightarrow \mathbf{R}$ est une version univaluée de Li_2 , définie par

$$D(z) = \Im(\operatorname{Li}_2(z)) + \log|z| \arg(1-z) \quad (z \in \mathbf{C} - \{0, 1\})$$

et prolongée par continuité en $0, 1, \infty$, de sorte que $D(0) = D(1) = D(\infty) = 0$. En utilisant l'exponentielle complexe $z \mapsto e^{2\pi iz}$, nous pouvons représenter $E(\mathbf{C})$ sous la forme

$$E(\mathbf{C}) \cong \frac{\mathbf{C}}{\mathbf{Z} + \tau\mathbf{Z}} \cong \frac{\mathbf{C}^*}{q^{\mathbf{Z}}}$$

où nous avons posé $q = e^{2\pi iz}$, $0 < |q| < 1$. Pour $P \in E(\mathbf{C})$, nous pouvons écrire $P = [x]$ avec $x \in \mathbf{C}^*$.

Définition 11 (Bloch). — La fonction dilogarithme elliptique $D_q : E(\mathbf{C}) \rightarrow \mathbf{R}$ est définie par

$$D_q(P) = \sum_{n=-\infty}^{\infty} D(xq^n) \quad (P = [x]).$$

En calculant le développement de Fourier de D_q vue comme fonction sur $\mathbf{C}/(\mathbf{Z} + \tau\mathbf{Z})$, Bloch a obtenu le résultat suivant.

Théorème 12 (Bloch). — Pour tout $P \in E(\mathbf{C})$ on a $D_q(P) = \Im(R_\tau(P))$.

En prenant la partie réelle de (1) et puisque $L(E, 2)$ est réel, on obtient l'expression suivante pour $L(E, 2)$

$$(2) \quad L(E, 2) = \sum_{(a,b) \in (\frac{\mathbf{Z}}{C})^2} \widehat{F}(a, b) \cdot D_q(P_{a,b}).$$

La quantité $L(E, 2)/\pi$ est donc combinaison linéaire à coefficients algébriques de la fonction dilogarithme elliptique, évaluée en des points de C -torsion de E . L'identité (2) relie d'une manière étonnante la valeur spéciale $L(E, 2)$ (quantité de nature arithmétique) à la géométrie de la courbe elliptique E .

Des expériences numériques initiées par Bloch et Grayson ont suggéré que ce phénomène vaut pour les courbes elliptiques en général. Soit donc E une courbe elliptique définie sur \mathbf{Q} (quelconque). Fixons un isomorphisme $E(\mathbf{C}) \cong \mathbf{C}^*/q^{\mathbf{Z}}$ compatible à la conjugaison complexe. Nous disposons, comme précédemment, d'une fonction dilogarithme elliptique $D_q : E(\mathbf{C}) \rightarrow \mathbf{R}$.

Conjecture de Zagier pour $L(E, 2)$ (version faible). — La valeur spéciale $L(E, 2)$ est combinaison \mathbf{Q} -linéaire des quantités $\pi D_q(P)$, avec $P \in E(\overline{\mathbf{Q}})$.

Cette conjecture est conséquence d'un théorème de Beilinson sur les courbes modulaires. Un ingrédient de cette implication est la paramétrisation modulaire $\phi : X_1(N) \rightarrow E$.

Goncharov et Levin ont donné des conditions arithmétiques extrêmement précises satisfaites par la combinaison linéaire fournie par le théorème de Beilinson.

Conjecture de Zagier pour $L(E, 2)$ (version forte). — Soit $l = \sum_i n_i [P_i]$ une combinaison linéaire formelle finie, avec $n_i \in \mathbf{Z}$ et $P_i \in E(\overline{\mathbf{Q}})$. Si l satisfait aux conditions de Goncharov et Levin, alors

$$\pi \sum_i n_i D_q(P_i) \in L(E, 2) \cdot \mathbf{Q}.$$

