

# SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

GÉRARD LIGOZAT

## Fonction L des courbes modulaires

*Séminaire Delange-Pisot-Poitou. Théorie des nombres*, tome 11, n° 1 (1969-1970),  
exp. n° 9, p. 1-10

[http://www.numdam.org/item?id=SDPP\\_1969-1970\\_\\_11\\_1\\_A5\\_0](http://www.numdam.org/item?id=SDPP_1969-1970__11_1_A5_0)

© Séminaire Delange-Pisot-Poitou. Théorie des nombres  
(Secrétariat mathématique, Paris), 1969-1970, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

FONCTION L DES COURBES MODULAIRES

par Gérard LIGOZAT

Le but de ce travail est la vérification, pour certaines courbes modulaires de la conjecture de Swinnerton-Dyer.

1. Courbe elliptique définie sur  $\underline{\mathbb{Q}}$ .

Nous désignons le plus souvent par courbe elliptique définie sur  $\underline{\mathbb{Q}}$ , une variété abélienne de dimension 1 définie sur  $\underline{\mathbb{Q}}$ , c'est-à-dire une courbe de genre 1 définie sur  $\underline{\mathbb{Q}}$ , munie d'un point rationnel sur  $\underline{\mathbb{Q}}$ . Une telle courbe se met sous la forme

$$(E) \quad y^2 = x^3 + Ax + B, \quad A, B \in \underline{\mathbb{Q}},$$

l'origine étant le point à l'infini.

2. Espace vectoriel de dimension 1.

Les différentielles de première espèce sur  $E$  forment un espace vectoriel de dimension 1. Sur  $E$ , on peut prendre pour représentante

$$\Omega = \frac{dx}{y}.$$

3. Bonne et mauvaise réduction.

Il existe un ensemble fini non vide de nombres premiers  $p$ , en lesquels la réduction de  $E$  modulo  $p$  n'est pas elliptique. On dit qu'il y a mauvaise réduction, sinon bonne réduction. Si  $E$  a bonne réduction en  $p$ , la fonction  $\zeta$  locale est définie par

$$\zeta_p(E, s) = \frac{(1 - \alpha_p p^{-s})(1 - \overline{\alpha}_p p^{-s})}{(1 - p^{-s})(1 - p^{1-s})},$$

où  $\alpha_p, \overline{\alpha}_p$  sont caractérisés par

$$N_p = p - \alpha_p - \overline{\alpha}_p + 1, \quad \alpha_p \overline{\alpha}_p = 1,$$

où  $N_p$  est le nombre des points de  $E_p$ , réduction de  $E$  modulo  $p$ , rationnels sur  $\underline{\mathbb{F}}_p = \underline{\mathbb{Z}}/p\underline{\mathbb{Z}}$ .

#### 4. Fonction L globale.

On définit une fonction L globale par

$$L(E, s) = \prod_{p \text{ bon}} \{(1 - \alpha_p p^{-s})(1 - \overline{\alpha}_p p^{-s})\}^{-1} .$$

#### Résultats connus.

(a) Le produit converge pour  $\text{Re}(s) > 3/2$ . WEIL a conjecturé que  $L(s)$  peut être prolongé dans tout le plan complexe, et qu'une équation fonctionnelle lie  $L(s)$  et  $L(2 - s)$ .

(b) Lorsque E est une courbe elliptique avec multiplication complexe, ou plus généralement une variété abélienne de type CM, L vérifie l'hypothèse de WEIL ([7]).

(c) Lorsque E est définie par certains groupes modulaires, la conjecture est, là encore, vérifiée d'après [1], [6]. C'est un cas particulier qui nous occupe. Pour les courbes que nous considérons, nous savons que la fonction L est définie pour  $s = 1$ , et vérifie une équation fonctionnelle.

#### 5. Fonction L normalisée.

S désigne un ensemble fini de nombres premiers tels que E et une différentielle  $\Omega$ , choisie sur E, aient bonne réduction en dehors de S. On définit

$$L_S^*(E, s) = \prod_{p \in S} \{M_p(E)\}^{-1} \prod_{p \notin S} \{(1 - \alpha_p p^{-s})(1 - \overline{\alpha}_p p^{-s})\}^{-1} ,$$

où  $M_p(E)$  est appelé le nombre de Tamagawa associé à p,

$$M_p(E) = \int_{E(\mathbb{Q}_p)} |\Omega|_p \mu_p ,$$

où  $|\cdot|_p$  est la valuation p-adique,  $\mu_p$  la mesure de Haar sur  $\mathbb{Q}_p$  normalisée par

$$\mu_p(\mathbb{Z}_p) = 1 \quad \text{et} \quad M_\infty(E) = \int_{E(\mathbb{R})} \Omega .$$

(a) Pour S donnée,  $L_S^*(E, s)$  ne dépend pas de la forme  $\Omega$  choisie, à condition qu'il y ait bonne réduction.

(b) Si  $S_1, S_2$  sont deux ensembles de cette forme,

$$L_{S_1}^*(E, s) / L_{S_2}^*(E, s) \rightarrow 1 \quad \text{lorsque} \quad s \rightarrow 1 .$$

En effet, si on a bonne réduction,

$$M_p(E) = N_p/p = (1 - \alpha_p^{-1})(1 - \overline{\alpha_p^{-s}}) .$$

Par la suite, nous désignons par  $L^*(E, s)$  un tel produit d'Euler qui diffère par un nombre fini de facteurs de  $L(E, s)$  et tel que

$$L^*(E, s)/L_S^*(E, s) \rightarrow 1, \quad \text{pour } s \rightarrow 1 .$$

### 6. Le groupe de Tate-Šafarevič.

On rappelle que le groupe de Weil-Châtelet  $WC(E, \underline{Q})$  est le groupe des espaces homogènes sur  $E$  modulo une relation d'équivalence, qui s'interprète comme

$$H^1(G, E(\underline{Q})) , \quad \text{où } G = \text{Gal}(\underline{Q}/\underline{Q}) .$$

Le groupe de Šafarevič est alors défini par

$$0 \rightarrow \mathbb{III} \rightarrow H^1(G, E(\underline{Q})) \rightarrow \bigoplus H^1(G_p, E(\underline{Q}_p)) , \quad \text{pour toutes les valuations } p ;$$

c'est le sous-groupe des espaces homogènes qui sont partout localement triviaux, c'est-à-dire ont un point rationnel sur tous les complétés de  $\underline{Q}$ , y compris  $\underline{R}$ .

- (a) On n'a jamais calculé  $\mathbb{III}$  directement.
- (b) On conjecture que  $\mathbb{III}$  est un groupe fini.
- (c) CASSELS a montré que, si  $\mathbb{III}$  est fini, son ordre est un carré.
- (d) Dans des cas particuliers, on sait calculer des  $p$ -composantes de  $\mathbb{III}$ .

La conjecture de Swinnerton-Dyer suppose que  $\mathbb{III}$  est fini.

### 7. La conjecture de Swinnerton-Dyer.

Soit  $E$  une courbe elliptique définie sur  $\underline{Q}$ . Le groupe  $E(\underline{Q})$  des points rationnels de  $E$  est de type fini, d'après Mordell-Weil.

Soient  $r$  le rang de  $E(\underline{Q})$ ,  $\eta$  l'ordre du sous-groupe des points d'ordre fini. La conjecture s'énonce sous sa forme la plus élaborée ([8]),

$$L^*(E, s) \sim 2^r (s-1)^r f \frac{\#(\mathbb{III})}{\eta^2} ,$$

où  $f$  est un coefficient dépendant des hauteurs des points rationnels d'ordre fini,  $f = 1$  pour  $r = 0$ .

- (a) Conséquence : Pour  $r = 0$ ,

$$L^*(1) = \frac{\#(\mathbb{III})}{\eta^2} .$$

Pour  $r \neq 0$ ,

$$L^*(1) = 0 .$$

A l'origine de cette conjecture se trouvent les calculs de SWINNERTON-DYER et BRICH, concernant les courbes de la forme

$$\begin{aligned} y^2 &= x^3 + Dx , \\ y^2 &= x^3 + D , \end{aligned}$$

qui ont une multiplication complexe. Récemment ([8]), STEPHENS a réussi à évaluer, dans certains cas particuliers (pour des courbes  $X^3 + Y^3 = D$ ), le coefficient intervenant dans des cas où  $r = 1$  ou  $r = 2$ .

(b) CASSELS a démontré que la conjecture est "invariante" par isogénie.

(c) TATE a généralisé cette conjecture pour des variétés abéliennes de dimension arbitraire ([10]).

#### 8. Equation minimale de Weierstrass.

Soit  $E$  une variété abélienne de dimension 1 définie sur  $\underline{Q}$ . Il existe un modèle de  $E$  de la forme

$$(1) \quad y^2 + \lambda xy + \mu y = x^3 + \alpha x^2 + \beta x + \gamma ,$$

où  $\alpha, \beta, \gamma, \lambda, \mu \in \underline{Z}$ , et où le discriminant de (1), soit  $\Delta$ , est minimal ([5], [9]).

Soit  $E$  de la forme (1), posons

$$(A) \quad L_p(s) = \{(1 - \alpha_p p^{-s})(1 - \overline{\alpha_p} p^{-s})\}^{-1} ,$$

s'il y a bonne réduction,

$$(B) \quad L_p(s) = (1 - \epsilon_p p^{-s})^{-1} ,$$

s'il y a réduction de type B ([9]), avec  $\epsilon_p = +1$  si les tangentes sont rationnelles,  $\epsilon_p = -1$  sinon.

$$(C) \quad L_p(s) = 1 ,$$

si la réduction est de type C.

Alors, d'après TATE,

$$M_p(E) = c_p / L_p(1) ,$$

pour tout  $p$ , où  $c_p$  désigne le nombre des composantes simples du modèle réduit

de Néron qui sont rationnelles.

Nous posons

$$L^*(E, s) = \{M_\infty(E) \prod c_p\}^{-1} \prod_{\text{tous les } p} L_p(s) .$$

### 9. Courbes modulaires.

Soient  $H$  le demi-plan complexe, et  $\Gamma_0(N)$  le groupe des transformations

$$z \mapsto \left( \frac{az + b}{cz + d} \right), \quad \begin{cases} a, b, c, d \in \mathbb{Z} , \\ ad - bc = 1 , \\ c \equiv 0 \pmod{N} . \end{cases}$$

Soient  $\Gamma_0^*(N)$  le sous-groupe du groupe modulaire  $\Gamma$  engendré par  $\Gamma_0(N)$ , et

$$W_N(z) = -\frac{1}{Nz} .$$

Dans ces conditions,  $\widehat{H/\Gamma_0(N)}$  et  $\widehat{H/\Gamma_0^*(N)}$  sont des surfaces de Riemann compactes.  $\widehat{H/\Gamma_0(N)}$  est une surface de Riemann de genre  $\Delta$  pour

$$N = 11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49 .$$

Le corps des fonctions de  $\widehat{H/\Gamma_0^*(N)}$  est  $\mathbb{C}(j(z), j(Nz))$ . On peut définir la courbe modulaire  $\Phi_N$  par l'équation modulaire  $\Phi_N(j(z), j(Nz)) = 0$ , c'est un des modèles de  $\mathbb{Q}(j(z), j(Nz))$ . On désigne par  $F_N$  un modèle complet non singulier.

(a) IGUSA [4] a montré qu'il existe un tel modèle ayant bonne réduction en tout  $p$  ne divisant pas  $N$ .

(b) Un résultat plus précis résulte d'une conjecture de Weil.

### 10. Une conjecture de Weil.

Revenons à une courbe  $E$  définie sur  $\mathbb{Q}$  par (1),

$$y^2 + \lambda xy + \mu y = x^3 + \alpha x^2 + \beta x + \gamma .$$

(a) Conducteur : La courbe  $E$  peut être considérée comme courbe sur  $\mathbb{Q}_p$ .

Soit  $G_p = \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ .

Soit  $B$  un  $G_p$ -module fini avec  $\ell.B = 0$  pour un  $\ell \neq p$ . SERRE a défini une mesure de ramification sauvage de  $B$  :

$$\delta(\mathbb{Q}_p, B) .$$

En particulier, soit  $E_\ell$  le groupe des points d'ordre  $\ell$ . On peut donc définir

$$\delta(\underline{Q}_p, E_\ell), \quad \text{pour } \ell \neq p.$$

Alors ([4]),  $\delta(\underline{Q}_p, E_\ell) = \delta_p$  ne dépend pas de  $\ell$ .

Soient  $\text{ord}_p(\Delta)$  la valuation de  $\Delta$  minimal, et  $n_p$  le nombre de composantes du modèle minimal de Néron ; et soit  $\varepsilon_p = 0, 1, 2$ , suivant que la réduction est de type A, B, C.

Alors

$$\text{ord}_p(\Delta) - n_p + 1 = \delta_p + \varepsilon_p.$$

Ceci est nul en particulier en cas de bonne réduction.

On définit le conducteur de  $E$  par

$$N = \prod_p p^{\delta_p + \varepsilon_p}.$$

Les  $p$  intervenant avec un exposant non nul sont ceux divisant le discriminant minimal  $\Delta$ .

(b) Conjecture de Weil : Soient  $E$  une courbe elliptique définie sur  $\underline{Q}$  de conducteur  $N$ , et  $J_N$  la jacobienne de  $F_N$ .  $E$  est isogène à une courbe tracée sur  $J_N$ .

COROLLAIRE 1. - Il n'y a pas de courbes elliptiques de conducteurs

$$N = 1 \text{ à } 10, 12, 13, 16, \text{ etc.}$$

pour lesquels  $F_N$  est de genre 0.

COROLLAIRE 2. - Soit  $E$  de conducteur  $N = 11, 14, 15, 17$ . Alors  $E$  est isogène à  $F_N$  (qui est de conducteur  $N$ ).

Ceci a été vérifié par OGG [5] pour  $N = 24, 36$ . Le premier corollaire a été vérifié pour un certain nombre de valeurs de  $N$ .

(c) Les résultats obtenus ici entraînent :

Pour  $N = 11, 14, 15, 17, \text{ etc.}$ , la courbe  $F_N$  est de conducteur  $N$ . (On le vérifie facilement à l'aide du tableau.)

### 11. Les courbes de Fricke.

FRICKE [2] a considéré les  $N$  pour lesquels  $\widehat{H/\Gamma_0^*(N)}$  est de genre 0. Il y en a 36. En particulier, les 12 cas pour lesquels  $\widehat{H/\Gamma_0(N)}$  est de genre 1 en sont.

Dans ces conditions, si  $\tau$  est une uniformisante de  $\widehat{H/\Gamma_0^*(N)}$ ,

$$K(z) = j(z) - j(Nz)$$

change de signe sous  $W_N$ . Donc  $K^2(z)$  est une fonction rationnelle de  $\tau$ ,

$$K^2 = \psi(\tau) .$$

FRICKE obtient ainsi des équations de la forme

$$\sigma^2 = \tau^4 + a\tau^3 + b\tau^2 + c\tau + d ,$$

qui sont des modèles de  $\mathbb{Q}(j(z), j(Nz))$ .

## 12. Théorie de Hecke et résultats de Eichler-Shimura.

(a) Soit  $f(z)$  une forme parabolique de poids  $-2$  pour  $\Gamma_0(N)$ . L'espace de ces formes est de dimension égale au genre de  $F_N$ , donc à 1 pour

$$N = 11, 14, 15, 17, \dots .$$

(b)  $f(z) \mapsto f(z) dz$  est un isomorphisme de l'espace des formes paraboliques de poids  $-2$  sur celui des différentielles de première espèce sur  $F_N$ . Donc, si  $\Omega = f(z) dz$ ,  $f(z)$  est vecteur propre pour tous les opérateurs de Hecke  $T_p$ ,

$$T_p f = \alpha_p f .$$

(c) D'après la théorie de Hecke, à toute  $f(z)$ ,  $f(z) = \sum a_n e^{2\pi i n z}$ , on associe à la série de Dirichlet  $D(s) = \sum a_n n^{-s}$ .

Le fait d'être vecteur propre équivaut à l'existence pour  $D$  d'un produit d'Euler,

$$\sum a_n n^{-s} = \prod (1 - \alpha_p p^{-s} + p^{1-2s})^{-1} .$$

(d) D'après EICHLER [1] et SHIMURA [6], si l'on désigne par  $L(F_N, s)$  la série de  $F_N$ , on a, aux facteurs près correspondant aux  $p$  divisant  $N$ , l'égalité des  $p$ -facteurs de la série  $L$  et du produit d'Euler  $D$ .

Conjecturalement, la fonction  $L(s)$  (avec les  $p$ -facteurs définis au § 8) est exactement égale au produit d'Euler  $D(s)$  associé à la forme différentielle (à une constante près).

(e) Il suffit de vérifier qu'il en est ainsi pour tous les  $p$  divisant  $N$ . On constate que, dans tous les cas, en choisissant

$$\Omega = \frac{dx}{2y + \lambda x + \mu} = f(z) dz ,$$



$D(s)$  étant le produit d'Euler associé à  $f(z)$ , et  $L(s)$  la série de  $F_N$ , on a

$$(2) \quad L(s) = -\frac{1}{2\pi i} D(s) .$$

13. Calcul de  $L^*(F_N, 1)$ .

$$L^*(F_N, 1) = \{M_\infty(F_N) \times \prod_p c_p\}^{-1} L(F_N, 1) .$$

$$\text{Si } L(F_N, s) = \sum b_n \times n^{-s} ,$$

$$L(F_N, 1) = \sum b_n \times n^{-1} = -2\pi i \int_0^{i\infty} g(z) dz ,$$

où  $g(z)$  correspond à la série  $L$ , donc

$$g(z) dz = -\frac{1}{2\pi i} f(z) dz ,$$

$$L(F_N, 1) = \int_0^{i\infty} f(z) dz = \int_0^{i\infty} \Omega .$$

Les points correspondant à  $(0)$  et  $(i\infty)$  sont rationnels d'ordre fini, et de la sorte

$$\int_0^{i\infty} \Omega = \frac{M_\infty(F_N)}{m} ,$$

où  $m$  est un entier.

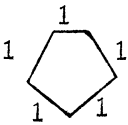
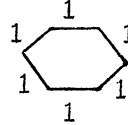
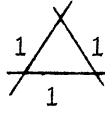
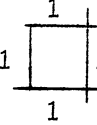
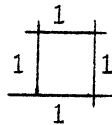
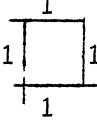

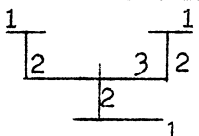
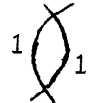
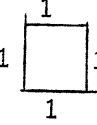
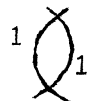
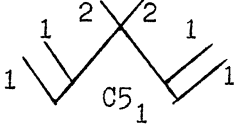
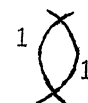
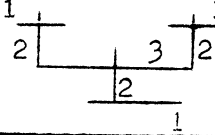
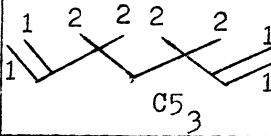
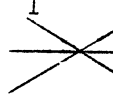

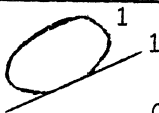
D'où

$$L^*(F_N, 1) = 1 / \left( m \prod_{p|N} c_p \right) .$$

14. Tableau des résultats obtenus.

Le tableau ci-après donne les résultats obtenus. Pour la courbe  $F_{11}$ , le calcul a été fait par SWINNERTON-DYER [9]. Les courbes  $F_{27}$ ,  $F_{32}$ ,  $F_{36}$  ont déjà été étudiées en tant que courbes admettant une multiplication complexe. Ce sont les seules avec  $F_{49}$  qui admettent une multiplication complexe.

Dans les 12 cas, la conjecture est vérifiée avec une valeur conjecturale de  $\#(\text{III})$  égale à 1.

N	$\Delta$ minimal	j	Module $p_1$	Module $p_2$	$C_{p_1}$	$C_{p_2}$	$L^*(1)$	$\eta$
11	$11^5$	$- 2^{12} \cdot 31^3 \cdot 11^{-5}$	 B5		5		1/25	5
14	$2^6 \cdot 7^3$	$5^3 \cdot 43^3 \cdot 2^{-6} \cdot 7^{-3}$	 B6	 B3	2	3	1/36	6
15	$- 3^4 \cdot 5^4$	$13^3 \cdot 37^3 \cdot 3^{-4} \cdot 5^{-4}$	 B4	 B4	2	4	1/64	8
17	$17^4$	$- 3^3 \cdot 11^3 \cdot 17^{-4}$	 B4		4		1/16	4
19	$19^3$	$- 2^{18} \cdot 7^3 \cdot 19^{-3}$	 B3		3		1/9	3
20	$2^8 \cdot 5^2$	$2^4 \cdot 11^3 \cdot 5^{-2}$	 C6	 B2	3	2	1/36	6
21	$- 3^4 \cdot 7^2$	$193^3 \cdot 3^{-4} \cdot 7^{-2}$	 B4	 B2	4	2	1/64	8
24	$2^8 \cdot 3^2$	$2^4 \cdot 13^3 \cdot 3^{-2}$	 C5 <sub>1</sub>	 B2	4	2	1/64	8
27	$3^9$	0	 C6		3		1/9	3
32	$2^{12}$	$2^6 \cdot 3^3$	 C5 <sub>3</sub>		4		1/16	4
36	$2^4 \cdot 3^3$	0	 C3	 C2	3	2	1/36	6
49	$7^3$	$- 3^3 \cdot 5^3$	 C2		2		1/4	2

## BIBLIOGRAPHIE

- [1] EICHLER (M.). - Quaternäre quadratische Formen und die Riemann Vermutung für die Kongruenzzetafunktion, Archiv der Math., t. 5, 1954, p. 355-366.
- [2] FRICKE (R.). - Die elliptischen Funktionen und ihre Anwendungen. 2ter Teil. - Leipzig, B. G. Teubner, 1922.
- [3] NÉRON (A.). - Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. - Paris, Presses universitaires de France, 1964 (Institut des Hautes Etudes Scientifiques. Publications mathématiques, 21).
- [4] OGG (A. P.). - Elliptic curves and wild ramification, Amer. J. of Math., t. 89, 1967, p. 1-21.
- [5] OGG (A. P.). - Curves of small conductor, J. für die reine und angew. Math. (à paraître).
- [6] SHIMURA (G.). - Correspondances modulaires et les fonctions  $\zeta$  de courbes algébriques, J. Math. Soc. Japan, t. 10, 1958, p. 3-18.
- [7] SHIMURA (G.) and TANIYAMA (Y.). - Complex multiplication of abelian varieties and its applications to number theory. - Tokyo, Mathematical Society of Japan, 1961 (Publications of the Mathematical Society of Japan, 6).
- [8] STEPHENS (N. M.). - The diophantine equation  $X^3 + Y^3 = DZ^3 \dots$ , J. für die reine und angew. Math., t. 231, 1968, p. 121-162.
- [9] SWINNERTON-DYER (P.). - The conjectures of Birch and Swinnerton-Dyer and of Tate, Proceedings of a conference on local fields [1966. Driebergen], p. 132-157. - Berlin, Springer-Verlag, 1967.
- [10] TATE (J.). - On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, Séminaire Bourbaki, 1965/66, n° 306, 26 p.

(Texte reçu le 9 mars 1970)

Gérard LIGOZAT  
 6 clos d'Alençon  
 VILLEBON-sur-Yvette  
 91 - PALAISEAU

---