Degré modulaire d'une courbe elliptique

Christophe Delaunay

3 juin 2002

Université Bordeaux I, Laboratoire A2X,
351 Cours de la Libération, 33 405 Talence, France
e-mail : delaunay@math.u-bordeaux.fr

Résumé

On décrit une méthode pour le calcul du degré du revêtement modulaire d'une courbe elliptique E définie sur $\mathbb{Q}$. Celle-ci est basée sur l'évaluation du carré symétrique de la série L de E.

1 Introduction

Soit E une courbe elliptique définie sur $\mathbb{Q}$. Les récents travaux de [Wil], [Ta-Wi] et [Br-Co-Di-Ta] sur la modularité des courbes elliptiques, entraînent l'existence d'une application φ (le revêtement modulaire) :

$$\varphi \ : \ X_0(N) \longrightarrow \mathbb{C}/\Lambda \simeq E(\mathbb{C}) \ ,$$

où N désigne le conducteur de E et $X_0(N)$ le complété de l'espace quotient du demi-plan de Poincarré $\mathbb{H}$ par le sous groupe de congruence :

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \quad N \mid c \right\} \ .$$

L'image réciproque par φ de l'unique (à multiplication près) forme différentielle invariante dz est $2i\pi c f(\tau)d\tau$, où c est la constante de Manin (que l'on peut supposer positive) et où f est la forme modulaire de poids 2 et de niveau N classiquement associée à E. Le nombre entier $\deg(\varphi)$ est donc un invariant qui apparait naturellement et il semble intéressant de pouvoir le calculer efficacement. Ceci peut permettre entre autres de vérifier les conjectures qui lui sont reliées (nombres congruents, croissance en fonction de N, ...). Des méthodes plutôt géométriques sont bien connues ([Cre], [Zag]) mais elles deviennent vite inutilisables lorsque le conducteur est grand. Ici, nous décrivons une méthode plus analytique, basée sur le calcul de la valeur spéciale en $s = 2$ du carré symétrique de la série L de f, qui permet de déterminer rapidement $\deg(\varphi)$. Ce texte est un résumé de [Del], où l'on pourra trouver plus de détails.

2 Le carré symmetrique imprimitif

On suppose que E est une courbe de Weil forte et que la conjecture de Manin est vérifiée pour E (de sorte que $c = 1$). On écrit $f(\tau) = \sum_{n\geq 1} a_n q^n$ (où $q = e^{2i\pi\tau}$) ; la série de Dirichlet $L(E,s) = L(f,s) = \sum_{n\geq 1} a_n n^{-s}$ converge pour $\Re e(s) > 3/2$, se prolonge en une fonction entière et vérifie une équation fonctionnelle. On obtient alors $\varphi(\tau) = \sum_{n\geq 1} \frac{a_n}{n} q^n \pmod{\Lambda}$ et on a :

$$\frac{4\pi^2 \|f\|_N^2}{\mathrm{vol}(E)} = \deg(\varphi) \ , \tag{1}$$

où $\mathrm{vol}(E)$ est le volume d'un réseau minimal Λ de E et $\|f\|_N^2$ est la norme de f au sens de Petterson. On voit donc que le calcul de $\deg(\varphi)$ se ramène à celui de $\|f\|_N^2$.

Proposition 1 (Rankin–Shimura) *On pose :*

$$\mathrm{L}(\mathcal{I}^2 f, s) = \frac{\zeta_N(2s-2)}{\zeta_N(s-1)} \sum_{n=1}^{\infty} \frac{a_n^2}{n^s} \ , \tag{2}$$

où $\zeta_N(s) = \sum_{(n,N)=1} n^{-s}$.
La série $\mathrm{L}(\mathcal{I}^2 f, s)$ *converge pour* $\Re e(s) > 2$ *et se prolonge en une fonction entière. De plus on a :*

$$\|f\|_N^2 = \frac{N}{8\pi^3} \mathrm{L}(\mathcal{I}^2 f, 2) \ .$$

On peut déduire de cette proposition des relations entre les degrés des revêtements modulaires pour les différentes tordues quadratiques de E :

Proposition 2 *Soit* E' *une courbe elliptique tordue quadratique de* E *de conducteur* $N' < N$ *avec* $L(E',s) = \sum_n a'_n n^{-s}$. *On pose* $N = MD_1^2 D_2^2 2^k$ *et* $N' = MD_2 2^\lambda$ *où* M, D_1 *et* D_2 *sont impairs et sans facteur carré et où* $\lambda \leq k$. *On a :*

$$\begin{aligned}
\|f\|_N^2 = \quad & \|f'\|_{N'}^2 \quad \frac{1}{D_1} \prod_{p|D_1} (p-1)(p+1-a'_p)(p+1+a'_p) \\
& \times \quad \frac{1}{D_2} \prod_{p|D_2} (p-1)(p+1) \\
& \times \quad \begin{cases} 2^{k-3}(3-a'_2)(3+a'_2) & \text{if } \lambda = 0 \ , \ k \geq 4 \\ 2^{k-3} \times 3 & \text{if } \lambda = 1 \ , \ k \neq \lambda \\ 2^{k-\lambda} & \text{if } 2 \leq \lambda \leq k \quad \text{ou si } \lambda = k \end{cases} .
\end{aligned}$$

On peut donc supposer que E est minimale (au sens du conducteur) parmi la famille de ses tordues quadratiques.

3 Le carré symétrique primitif

On suppose dans cette partie que E n'est pas tordue quadratique d'une courbe ayant un plus petit conducteur. Le carré symétrique imprimitif ne possède pas d'équation fonctionnelle, afin de palier ce problème on corrige quelques facteurs eulériens, et on définit ainsi le carré symétrique primitif :

$$\mathrm{L}(\mathcal{P}^2 f, s) = \mathrm{L}(\mathcal{I}^2 f, s) \prod_{p \in S} \mathrm{L}_p(\mathcal{P}^2 f, p^{-s})^{-1} \quad , \tag{3}$$

où le produit porte sur tous les nombres premiers p dont le carré divise N. Les facteurs locaux pour $p \in S$ sont de la forme 1, $1 - pX$ ou $1 + pX$ et s'expriment facilement en fonction des coefficients de la courbe E ([Del], [Wat]).

Théorème 3 (Coates-Schmidt) *La fonction* $\mathrm{L}(\mathcal{P}^2 f, s)$ *se prolonge en une fonction holomorphe sur tout le plan complexe et il existe un nombre* $B \in \mathbb{Z}$ *(explicite en fonction des coefficients de* E*) tel que :*

$$\Lambda(\mathcal{P}^2 f, s) = \Lambda(\mathcal{P}^2 f, 3 - s) \quad ,$$

où

$$\Lambda(\mathcal{P}^2 f, s) = \left(\frac{B}{2\pi^{3/2}}\right)^s \Gamma(s)\Gamma\left(\frac{s}{2}\right) \mathrm{L}(\mathcal{P}^2 f, s) \quad .$$

Pour la suite, on pose $C = B/(2\pi^{3/2})$ et $\mathrm{L}(\mathcal{P}^2 f, s) = \sum_{n \geq 1} b_n n^{-s}$ où les coefficients b_n s'obtiennent facilement grâce à (2) et (3). Des techniques classiques de théorie analytique des nombres permettent d'obtenir grâce à l'équation fonctionnelle :

$$\mathrm{L}(\mathcal{P}^2 f, 2) = \sum_{n \leq X} \frac{b_n}{n^2} + O(B^2 X^{-1}) \quad . \tag{4}$$

En particulier la série $\mathrm{L}(\mathcal{P}^2 f, s)$ converge pour $s = 2$.
Remarques :
1) Les bornes sur les coefficients des formes modulaires donnent seulement $|b_n| \leq n^2$, et on a convergence absolue pour $s > 2$.
2) La convergence de la série est trop lente en $s = 2$ pour calculer $\|f\|_N^2$.

Exemple : Soit E la courbe elliptique de conducteur $N = 11$, d'équation : $y^2 + y = x^3 - x^2 - 10x - 20$. Il faut environ 10000 termes dans la série (4) pour obtenir $\mathrm{L}(\mathcal{P}^2 f, 2)$ à 10^{-3} près.

4 Calcul de $\Lambda(\mathcal{P}^2 f, s)$

On garde les notations de la partie précédente. On peut maintenant utiliser les outils pour le calcul des séries de Dirichlet possédant une équation fonctionnelle de type classique ([Coh]) :

Proposition 4 *On a :*

$$\Lambda(\mathcal{P}^2 f, s) = \sum_{n\geq 1} \frac{b_n}{n^s} F(s,n) + \sum_{n\geq 1} \frac{b_n}{n^{3-s}} F(3-s,n) \quad , \tag{5}$$

où

$$F(s,x) = C^s \Gamma(s)\Gamma\left(\frac{s}{2}\right) - \int_0^x \frac{1}{2i\pi} \int_{\Re e(z)=\delta} t^{-z} C^z \Gamma(z)\Gamma(z/2) dz\, t^{s-1} dt$$

pour tout $\delta > 0$.

On peut ainsi déterminer $\Lambda(\mathcal{P}^2 f, s)$. En effet, la fonction $F(s,x)$ converge rapidement vers 0 et peut s'obtenir à l'aide d'une série rapidement convergente, plus précisement :

Proposition 5 *La fonction $f(s,x)$ peut se calculer par la formule :*

$$F(s,x) = \gamma(s) - \sum_{q=0}^{\infty} x^{s+2q} \left(\frac{v_{2q} - \log(x) u_{2q}}{s+2q} + \frac{u_{2q}}{(s+2q)^2} + \frac{x u_{2q+1}}{s+2q+1} \right) \quad , \tag{6}$$

avec :

$$\begin{aligned} u_{2q} &= \frac{2(-1)^q}{C^{2q} q! (2q)!} \quad , \quad u_{2q+1} = \frac{(-1)^q \sqrt{\pi} 2^{2q+1} q!}{(2q+1)!^2 C^{2q+1}} \quad , \\ v_{2q} &= \frac{2(-1)^q}{C^{2q} q! (2q)!} \left(\log(C) - \frac{3}{2}\gamma + \frac{1}{2} \sum_{j=1}^{q} j^{-1} + \sum_{j=1}^{2q} j^{-1} \right) \quad , \end{aligned}$$

où $\gamma = 0.57721\ldots$ est la constante d'Euler. De plus, on a :

$$|F(\sigma + it, x)| \leq 3.6\pi \frac{x^\sigma}{A - \sigma A^{1/3}}\, e^{-\frac{3}{2}A^{2/3}} \quad ,$$

où $A = \frac{x}{2^{1/4} C}$.

Ces formules explicites permettent aussi le contrôle des erreurs lorsque les séries sont tronquées. Ceci nous donne donc une méthode pour calculer $\Lambda(\mathcal{P}^2 f, s)$, en l'appliquant à $s = 2$, on en déduit $\deg(\varphi)$ (qui doit être un entier).

Exemple : Soit E la courbe elliptique de l'exemple précédent. Il faut environ 25 termes dans les séries (5) et pas plus de 25 termes dans la série (6) pour calculer $\mathrm{L}(\mathcal{P}^2 f, 2)$ à 10^{-3} près.

Des conjectures affirment que le degré de φ n'est pas trop grand en fonction du conducteur (en fait, on devrait avoir une majoration de la forme $\log(\deg(\varphi)) = O(\log(N))$). Le fait que, dans certains cas, le carré symétrique $\mathrm{L}(\mathcal{P}^2 f, s)$ soit assez bien contrôlé nous permet d'obtenir certaines estimations :

Proposition 6 *Soit $\mathcal{E}$ une famille de courbes elliptiques définies sur $\mathbb{Q}$ vérifiant :*

- *l'invariant $j(E)$ pour $E \in \mathcal{E}$ est uniformément borné.*
- *Le discriminant minimal $\Delta_{min}(E)$ est sans facteur carré.*

Alors :

- $\deg(\varphi) \ll N^{7/6}\log(N)^3 \quad (N \to +\infty)$,
- $\deg(\varphi) \gg N^{7/6}/\log(N) \quad (N \to +\infty)$.

Références

[Br-Co-Di-Ta] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises.* , J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).

[Co-Sc] J. Coates and C.-G. Schmidt, *Iwasawa theory for the symmetric square of an elliptic curve.*, J. reine angew. Math. **375** (1987), 104–156.

[Coh] H. Cohen, *Advanced topics in computational algebraic number theory*, Graduate Texts in Mathematics **193**, Springer-Verlag, New-York, 2000.

[Cre] J. Cremona, *Computing the degree of the modular parametrization of a modular elliptic curve* Math. Comp. **64** (1995), no. 211, 1235–1250.

[Del] C. Delaunay, *Computing modular degrees using* L*-series*, soumis.

[Ta-Wi] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2)**141** (1995), no. 3, 553–572.

[Wat] M. Watkins, *Computing the modular degree of an elliptic curve*, preprint.

[Wil] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[Zag] D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. **28** (1985), no. 3, 372–384.