Journal de Théorie des Nombres de Bordeaux

Christophe Delaunay

Computing modular degrees using L-functions

Journal de Théorie des Nombres de Bordeaux, tome 15, nº 3 (2003), p. 673-682

<http://www.numdam.org/item?id=JTNB_2003__15_3_673_0>

Journal de Théorie des Nombres
de Bordeaux **15** (2003), 673–682

Computing modular degrees using L-functions

par CHRISTOPHE DELAUNAY

RÉSUMÉ. Nous donnons un algorithme pour calculer le degré modulaire d'une courbe elliptique définie sur $\mathbb{Q}$. Notre méthode est basée sur le calcul de la valeur spéciale en $s = 2$ du carré symétrique de la fonction L attachée à la courbe elliptique. Cette méthode est assez efficace et facile à implémenter.

ABSTRACT. We give an algorithm to compute the modular degree of an elliptic curve defined over $\mathbb{Q}$. Our method is based on the computation of the special value at $s = 2$ of the symmetric square of the L-function attached to the elliptic curve. This method is quite efficient and easy to implement.

1. Introduction

From the recent and difficult work of [14], [11] and [3], it is now known that every elliptic curves $E/\mathbb{Q}$ is modular. If N denotes its conductor, this implies that there exists a covering map φ from $X_0(N)$ to E. The pull-back by φ of the unique (up to multiplication) invariant differential form ω on E is $2i\pi cf(\tau)d\tau$, where $f(\tau)$ is a normalized newform of level N and weight 2 on $\Gamma_0(N)$ and where the 'Manin's constant' c is rational and can be assumed positive. Furthermore, the L-function associated to f coincides with the Hasse-Weil L-function of E.

The question of computing the degree of φ is natural and interesting because of important conjectures related to this number $\deg(\varphi)$. It is well known (cf. [15]) that there exists a simple relation between $\deg(\varphi)$ and $\|f\|_N^2$, where $\|.\|_N$ denotes the Petersson norm. In [15], D. Zagier explains how to compute explicitly $\|f\|_N$ in the general case of a congruence subgroup Γ. J. Cremona, in [7] interprets Zagier's method in the langage of "M-symbols" and computes $\deg(\varphi)$ for many elliptic curves (large tables of elliptic curves are given in [6]). Both methods are geometric and efficient but tend to be quite slow when the conductor is large. The purpose of this paper is to give an alternative way of computing $\|f\|_N$. This is an analytic method based on well-known results which relate the special value of the L-function associated to the symmetric square of E with $\|f\|_N$.

Manuscrit reçu le 5 juin 2002.

2. The imprimitive symmetric square of E

Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N. The normalized newform attached to E is $f(\tau) = \sum_n a_n q^n$ ($q = e^{2i\pi\tau}$). We have $\varphi^*(\omega) = 2i\pi c f(\tau)d\tau$, and a conjecture of Manin asserts that $c = 1$ whenever E is a strong Weil curve (there is exactly one such curve in an isogeny class). We then have ([15]):

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

where $\mathrm{vol}(E)$ is the volume of a minimal period lattice Λ with $E \simeq \mathbb{C}/\Lambda$. Now, the Hasse-Weil function $L(E,s)$ is equal to $\sum_n a_n n^{-s}$ and can be expanded as an Euler product:

$$L(E,s) = \prod_p L_p(E, p^{-s})^{-1} \quad ,$$

where $L_p(E,X) = (1 - \alpha_p X)(1 - \beta_p X)$, with:

- if $p \nmid N$:

$$\begin{cases} |\alpha_p| = |\beta_p| = \sqrt{p} \\ \alpha_p + \beta_p = a_p. \end{cases}$$

- If $p \mid N$ then $\beta_p = 0$, $a_p = \alpha_p$ and :

$$\alpha_p = \begin{cases} -1 & \text{if } E \text{ has non-split multiplicative reduction at } p \ (p\|N); \\ 1 & \text{if } E \text{ has split multiplicative reduction at } p \ (p\|N); \\ 0 & \text{if } E \text{ has additive reduction at } p \ (p^2 \mid N). \end{cases}$$

We define the imprimitive symmetric square L-function of f to be:

$$L(\mathrm{Sym}_{\mathrm{i}}^2 f, s) = \frac{\zeta_N(2s-2)}{\zeta_N(s-1)} \sum_{n=1}^{\infty} \frac{a_n^2}{n^s} \quad , \quad \Re e(s) > 2$$

$$\text{(2)} \qquad = \prod_p \left(1 - \alpha_p^2 p^{-s}\right)^{-1} \left(1 - \alpha_p\beta_p p^{-s}\right)^{-1} \left(1 - \beta_p^2 p^{-s}\right)^{-1}.$$

The subscript N means that we have omitted the Euler factors at the primes dividing N.

It can be shown that $L(\mathrm{Sym}_{\mathrm{i}}^2 f, s)$ has a holomorphic continuation to the whole complex plane, and by Rankin's method that (cf. [10]):

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

This formula allows us to study quadratic twists of an elliptic curve. Indeed, assume that E is the quadratic twist of an elliptic curve E' with conductor N' such that $\mathrm{ord}_p(N') \le \mathrm{ord}_p(N)$ for all prime p. We denote by χ the underlying quadratic character and by $\mathrm{cond}(\chi)$ its conductor. From classical results about twists of newforms (cf. [2]) and from the fact that for an odd prime p the p-adic valuation of $\mathrm{cond}(\chi)$ is ≤ 1 , we can obtain the following. Let $p \geq 3$ be a prime number with $p \mid \mathrm{cond}(\chi)$;

- if $p^2 \mid N'$ then $\mathrm{ord}_p(N) = \mathrm{ord}_p(N')$;
- if $p \| N'$ or if $p \nmid N$ then $\mathrm{ord}_p(N) = 2$.

Thus, we can write $N = MD_1^2D_2^2 2^k$ and $N' = MD_2 2^\lambda$ where D_1 (resp. D_2) is the product of the odd primes p such that $p \mid \mathrm{cond}(\chi)$ and $p \nmid N'$ (resp. $p \mid \mathrm{cond}(\chi)$ and $p \| N'$), $\lambda = \mathrm{ord}_2(N')$, $k = \mathrm{ord}_2(N)$ so that $\lambda \leq k$ and M, D_1, D_2 are odd. We can now state :

Theorem 1. *Assume that E is the quadratic twist of E' with conductor N' such that $\mathrm{ord}_p(N') \leq \mathrm{ord}_p(N)$ for all p. Write $f' = \sum_n a'_n n^{-s} = \prod_p (1 - \alpha'_p p^{-s})^{-1}(1 - \beta'_p p^{-s})^{-1}$ for the newform attached to E'. Let $N = MD_1^2D_2^2 2^k$ and $N' = MD_2 2^\lambda$ as explained above. Then:*

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

REMARK : From this theorem, it is easy to relate $\deg(\varphi)$ with $\deg(\varphi')$.

PROOF: We observe that we have $\alpha_p = \chi(p)\alpha'_p = \pm\alpha'_p$ and that the Euler product (2) for f and f' are clearly related since χ^2 is the trivial character modulo $\mathrm{cond}(\chi)$. Furthermore, this Euler product allows us to give a "local" proof of the theorem. So, suppose that E is the twist of E' by a character of prime conductor $p \geq 3$ with $\mathrm{ord}_p(N') < \mathrm{ord}_p(N)$ (if $\mathrm{ord}_p(N') = \mathrm{ord}_p(N)$ then we have $L(\mathrm{Sym}_{\mathrm{i}}^2 f', s) = L(\mathrm{Sym}_{\mathrm{i}}^2 f, s)$). We have $N = \mathrm{lcm}(N', p^2) = N'p^2$ (resp., $= N'p$) if $(N', p) = 1$ (resp., $(N', p) = p$). For $q \neq p$ the Euler factor at q of both $L(\mathrm{Sym}_{\mathrm{i}}^2 f, s)$ and $L(\mathrm{Sym}_{\mathrm{i}}^2 f', s)$ are the same. Since $p^2 \mid N$ we have $a_p = 0$ ([1]), and there is no Euler factor at p in $L(\mathrm{Sym}_{\mathrm{i}}^2 f, s)$.

When $(N', p) = 1$ (i.e. $p \mid D_1$) we have:

$$L(\mathrm{Sym}_{\mathrm{i}}^2 f, s) = L(\mathrm{Sym}_{\mathrm{i}}^2 f', s) \times (1 - \alpha'^2_p p^{-s})(1 - pp^{-s})(1 - \beta'^2_p p^{-s}).$$

A little calculation with $s = 2$ shows that:

$$\|f\|_N^2 = \|f'\|_{N'}^2 (p-1)(p+1-a'_p)(p+1+a'_p)/p.$$

When $(N', p) = p$ (i.e. $p \mid D_2$) the Euler factor of $L(\mathrm{Sym}_{\mathrm{i}}^2 f', s)$ is equal to $(1 - p^{-s})^{-1}$ so:

$$L(\mathrm{Sym}_{\mathrm{i}}^2 f, s) = L(\mathrm{Sym}_{\mathrm{i}}^2 f', s)(1 - p^{-s}),$$

and $\|f\|_N^2 = \|f'\|_{N'}^2 (p-1)(p+1)/p$.

The case $p = 2$ follows by the same argument except that there is no character of conductor 2 and so we have to deal with $\mathrm{cond}(\chi) = 4$ or 8. This also explains why some cases cannot (and do not) occur in list of cases relating $\|f\|_N$ and $\|f'\|_{N'}$. □

This theorem asserts that we only have to consider elliptic curves E which are *not* twists of another curve E' having a lower conductor.

3. The primitive symmetric square of E

The imprimitive symmetric square $L(\mathrm{Sym}^2_{\mathrm{i}} f, s)$ does not have a "traditional" functional equation and there is no simple method to compute $L(\mathrm{Sym}^2_{\mathrm{i}} f, 2)$ directly. Thus, we consider the primitive symmetric square L-function of E, $L(\mathrm{Sym}^2 f, s)$:

$$L(\mathrm{Sym}^2 f, s) = L(\mathrm{Sym}^2_{\mathrm{i}} f, s) \prod_{p \in S} L_p(\mathrm{Sym}^2_{\mathrm{i}} f, p^{-s})^{-1},$$

where the product is over the finite set S of bad primes where E has bad but potentially good reduction, in other words primes p such that $p \mid N$ and $\mathrm{ord}_p(j(E)) \geq 0$, $j(E)$ being the j-invariant of E. The properties of the primitive symmetric square function are studied in [4]. In particular, the following is proved:

Theorem 2 (Coates-Schmidt). *The function $L(\mathrm{Sym}^2 f, s)$ has a holomorphic continuation to the whole complex plane and there exists $B \in \mathbb{Z}$ such that the completed function:*

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

is entire and admits the functional equation:

$$\Lambda(\mathrm{Sym}^2 f, s) = \Lambda(\mathrm{Sym}^2 f, 3 - s).$$

REMARKS: 1. If $p^2 \nmid N$, the Euler factor at p of the primitive and imprimitive symmetric square functions of E are the same and we have $\mathrm{ord}_p(B) = \mathrm{ord}_p(N)$. In particular, if N is squarefree, then $L(\mathrm{Sym}^2 f, s) = L(\mathrm{Sym}^2_{\mathrm{i}} f, s)$ and $B = N$.

2. The function $L(\mathrm{Sym}^2 f, s)$ is invariant if we twist E by a quadratic character of $\mathbb{Q}$. This is not true in general for the imprimitive symmetric square function.

In order to write down the correct Euler factor at $p \mid N^2$, we assume that E is not the quadratic twist of a curve E' of lower conductor. For the cases $p = 2$ and $p = 3$, we have the following tables coming from [4] (we should mention that two cases have been initially forgotten in [4] whenever $2^8 \mid N$, and that [13] corrects this mistake).

$\mathrm{ord}_2(N)$	$\mathrm{ord}_2(B)$	$L_2(\mathrm{Sym}^2 f, X)$
2	1	$1+pX$
3	2	1
5	3	1
7	4	1
8	3	$1+pX$
	3	$1-pX$
	4	1

$\mathrm{ord}_3(N)$	$\mathrm{ord}_3(B)$	$L_3(\mathrm{Sym}^2 f, X)$
2	1	$1+pX$
3	2	1
4	2	$1+pX$
	2	$1-pX$
5	3	1

When several possibilities occur in theses tables, the correct Euler factor is given by certain properties of the fields $\mathbb{Q}_p(E_\ell)/\mathbb{Q}_p$. The cases $2^4||N$ and $2^6||N$ never appear since we assumed that E is minimal among its quadratic twists. If $p \neq 2, 3$ then $\mathrm{ord}_p(B) = 1$ and $L_p(\mathrm{Sym}^2 f, X) = 1-pX$ or $1+pX$ depending on whether or not $\mathbb{Q}_p(E_\ell)/\mathbb{Q}_p$ is abelian. Nevertheless, for each ambiguous case, one can find in [13][1] the correct Euler factor: first assume that $p \geq 5$. Then we have $L_p(\mathrm{Sym}^2 f, X) = 1 - pX$ if and only if one of the following conditions holds, where c_6 and c_4 are the classical invariants attached to E:

- $p \equiv 1 \pmod{12}$;
- $p \equiv 5 \pmod{12}$, $p^2 \mid c_6$ and $p^2 \nmid c_4$;
- $p \equiv 7 \pmod{12}$ and either $p^2 \nmid c_6$, or $p^2 \mid c_6$ and $p^2 \mid c_4$.

For $p = 2$, $2^8||N$ is the only ambiguous case and:

- if $2^9 \mid c_6$ then $L_p(\mathrm{Sym}^2 f, X) = 1$;
- if $2^9 \nmid c_6$ and $c_4 \equiv \varepsilon 32 \pmod{128}$ then $L_p(\mathrm{Sym}^2 f, X) = 1 + \varepsilon pX$, where $\varepsilon = \pm 1$.

For $p = 3$, $3^4||N$ is the only ambiguous case and we have $L_p(\mathrm{Sym}^2 f, X) = 1 - pX$ when one of the two following holds:

- $c_4 \equiv 27 \pmod{81}$;
- $c_4 \equiv 9 \pmod{27}$ and $c_6 \equiv \pm 108 \pmod{243}$.

4. Computation of $L(\mathrm{Sym}^2 f, s)$

For simplicity, we write:

$$\begin{aligned}\Lambda(\mathrm{Sym}^2 f, s) &= C^s \Gamma(s) \Gamma\left(\frac{s}{2}\right) L(\mathrm{Sym}^2 f, s) \\ &= \gamma(s) L(\mathrm{Sym}^2 f, s),\end{aligned}$$

where $C = \frac{B}{2\pi^{3/2}}$ and $L(\mathrm{Sym}^2 f, s) = \sum_n b_n n^{-s}$. Note that the coefficients b_n are easily computable from the definitions. Furthermore, it follows from Deligne's bounds and the Euler product for $L(\mathrm{Sym}^2 f, s)$ that $|b_n| \leq n^2$. Classical estimates coming from the functional equation of

[1]During the preparation of this paper, we were informed of the preprint [13] of M. Watkins where a similar (but not so detailed) method of computing $\deg(\varphi)$ is described and used to compute several interesting modular degrees.

$\Lambda(\mathrm{Sym}^2 f, s)$ give:

$$L(\mathrm{Sym}^2 f, 2) = \sum_{n \leq X} \frac{b_n}{n^2} + O(B^2 X^{-1}). \tag{3}$$

This formula implies that the series $\sum_n b_n/n^2$ converges to $L(\mathrm{Sym}^2 f, 2)$. Of course, this is not an efficient method to compute $\|f\|_N^2$ because the convergence is very slow. However, it easily gives us a first approximation of $\|f\|_N^2$.

Fortunately, a classical method for computing Dirichlet series with functional equation can be applied to our case (cf. [5], Chapter 10):

Proposition 3. *We have:*

$$\Lambda(\mathrm{Sym}^2 f, s) = \sum_{n \geq 1} \frac{b_n}{n^s} F(s, n) + \sum_{n \geq 1} \frac{b_n}{n^{3-s}} F(3 - s, n), \tag{4}$$

where

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

for all $\delta > 0$.

This is a rapidly convergent series since we have:

Proposition 4. *Let* $s = \sigma + it$ *and* $A = \frac{x}{2^{1/4} C}$ *then:*

$$|F(s, x)| \leq 3.6\sqrt{\pi} \frac{x^\sigma}{A - \sigma A^{1/3}} e^{-\frac{3}{2} A^{2/3}}.$$

PROOF: We have:

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

Hence,

$$|F(s, x)| \leq \frac{1}{2\pi} C^\delta \frac{x^{\sigma - \delta}}{\delta - \sigma} \int_{\mathbb{R}} \left| \Gamma\left(\frac{\delta + iT}{2}\right) \Gamma(\delta + iT) \right| dT.$$

We put $I = \int_0^\infty \left|\Gamma\left(\frac{\delta+iT}{2}\right) \Gamma(\delta + iT)\right| dT = I_1 + I_2$ where,

$$\begin{aligned} I1 &= \int_0^\delta \left| \Gamma\left(\frac{\delta + iT}{2}\right) \Gamma(\delta + iT) \right| dT, \\ I2 &= \int_\delta^\infty \left| \Gamma\left(\frac{\delta + iT}{2}\right) \Gamma(\delta + iT) \right| dT. \end{aligned}$$

The formula $\Gamma(s) = \sqrt{2\pi} s^{s-1/2} e^{-s} e^{R(s)}$, $|R(s)| \le 1/(6|s|)$ gives the estimates:

$$\left|\Gamma\left(\frac{\delta+iT}{2}\right)\Gamma(\delta+iT)\right| \le \pi 2^{\frac{\delta}{4}+1} T^{\frac{3\delta}{2}-1} e^{-\frac{3\pi T}{4}} e^{\frac{1}{2\sqrt{2\delta}}+\frac{\delta}{2}} \text{ for } T > \delta,$$

$$\left|\Gamma\left(\frac{\delta+iT}{2}\right)\Gamma(\delta+iT)\right| \le \pi 2^{\frac{\delta}{4}+1} \delta^{\frac{3\delta}{2}-1} e^{-\frac{3\delta}{2}} e^{\frac{1}{2\delta}} e^{-\frac{T2}{2\delta}(\frac{T2}{\delta 2}-3)} \text{ for } T \le \delta.$$

With an easy but tedious calculation, we obtain:

$$I \le 3.6\pi^{3/2} \delta^{\frac{3\delta-1}{2}} e^{-\frac{3\delta}{2}} 2^{\frac{\delta}{4}}.$$

Thus, we have:

$$|F(s,x)| \le 3.6\sqrt{\pi}\frac{x^\sigma}{\delta-\sigma}\left(\frac{x}{2^{1/4}C}\right)^{-\delta} \delta^{-\frac{3\delta-1}{2}} e^{-\frac{3\delta}{2}}.$$

The proposition is then proved by taking $\delta = \left(\frac{x}{2^{1/4}C}\right)^{2/3}$. □

This proposition allows us to estimate the tail of the series in (4) (we have $|b_n| \le n^2$). In order to compute $F(s,x)$, we push the line of integration to the left catching all the residues of $t^{-z}\gamma(z)$:

Proposition 5.

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

with

$$u_{2q} = \frac{2(-1)^q}{C^{2q} q!(2q)!},$$

$$u_{2q+1} = \frac{(-1)^q \sqrt{\pi} 2^{2q+1} q!}{(2q+1)!^2 C^{2q+1}},$$

$$v_{2q} = \frac{2(-1)^q}{C^{2q} q!(2q)!}\left(\log(C) - \frac{3}{2}\gamma + \frac{1}{2}\sum_{j=1}^{q} j^{-1} + \sum_{j=1}^{2q} j^{-1}\right).$$

It is clear that the terms in this expression can be recursively computed. In practice, we compute N_0 such that:

$$\left|\sum_{n=N_0+1}^{\infty} \frac{b(n)}{n^2} F(2,n)\right| < \varepsilon \qquad \text{and}$$

$$\left|\sum_{n=N_0+1}^{\infty} \frac{b(n)}{n} F(1,n)\right| < \varepsilon.$$

We then compute i_0 terms in the series of proposition 5, where i_0 is the smallest integer such that (cf. [12]):

$$C^2 N_0^{-i_0-1/2} \left\lfloor \frac{i_0}{2} \right\rfloor ! \, i_0! > \frac{10N_0}{\pi\varepsilon}.$$

We thus obtain $\Lambda(\mathrm{Sym}^2 f, 2)$ with a sufficiently high accuracy and we deduce from it the value of $\|f\|_N^2$, hence of $\deg(\varphi)$. Using this method, we can quickly compute modular degrees of strong Weil curves. As a check on the computations, we use the fact that $\deg(\varphi)$ is an integer.

REMARK. In fact, what is really obtained here is an algorithm to compute $L(\mathrm{Sym}^2 f, 2)$ from which $\|f\|$ and then $\deg(\varphi)$ can be easily recovered. Nevertheless, the quantity $\|f\|$ makes sense and is also interesting in greater generality, namely for any holomorphic form f of integral weight $k \geq 2$ and level N, not necessarily related to an elliptic curve. In this general case, one can also define $L(\mathrm{Sym}^2 f, s)$ the primitive symmetric square L-function related to the L-function of f and we have:

$$\|f\|^2 = \frac{N}{2^{k-1}\pi^{k+1}} L(\mathrm{Sym}^2 f, k).$$

This L-function does have a traditional functional equation and the adaptation of the method above is possible. However, in our case (f is related to an elliptic curve), computing the Euler factors involves looking at the elliptic curve whenever the reduction is additive ($p^2 \mid N$); in general, such a study is not possible and the case of non-squarefree N seems not to be easy. When N is squarefree the adaptation of the method is very simple since the Euler factors of $L(\mathrm{Sym}^2 f, s)$ are all given by (2) and the functional equation is :

$$\Lambda(\mathrm{Sym}^2 f, s) = \Lambda(\mathrm{Sym}^2 f, 2k - 1 - s),$$

where,

$$\Lambda(\mathrm{Sym}^2 f, s) = \left(\frac{N^s}{2^s \pi^{3s/2}}\right) \Gamma(s) \Gamma\left(\frac{s}{2} - \left\lfloor \frac{k-1}{2} \right\rfloor\right) L(\mathrm{Sym}^2 f, s).$$

Furthermore, when N is squarefree, one can adapt the method to compute (conjecturally) special values of general symmetric powers $L(\mathrm{Sym}^n f, k)$ since they also satisfy a traditional (and conjectural) functional equation.

5. Some estimates

From the functional equation of $L(\mathrm{Sym}^2 f, s)$, one can show that $\|f\|_N^2 \ll_\varepsilon N^{1+\varepsilon}$. In fact, N^ε can be replaced by a suitable power of $\log(N)$. Thus, estimates for $\mathrm{vol}(E)$ provide upper bounds on $\deg(\varphi)$ (modulo Manin's conjecture).

Proposition 6. *Let C be a nonnegative real number. There exist $a \in \mathbb{R}$ and $A \in \mathbb{R}$ depending on C such that:*

$$|j(E)| \leq C \Longrightarrow a\Delta_{min}^{-1/6} < \mathrm{vol}(E) < A\Delta_{min}^{-1/6},$$

where Δ_{min} is the discriminant of the minimal model of E.

PROOF: This proposition comes from a straightforward estimate for the fundamental periods ω_1 and ω_2 of E, since we have $\mathrm{vol}(E) = |\Im m(w_2\bar{w}_1)|$. □

Assuming Manin 's conjecture, we see that proposition 6 gives the upper bound $\deg(\varphi) \ll N^{1+\epsilon}\Delta^{1/6}$ for elliptic curves with bounded j-invariant.

Proposition 7. *Let $\mathcal{E}$ be an infinite family of elliptic curves defined over $\mathbb{Q}$ such that:*

- *$j(E)$ is bounded for $E \in \mathcal{E}$.*
- *$\Delta_{min}(E)$ is squarefree.*

Then:

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

PROOF: The upper bound comes from the classical estimate $L(\mathrm{Sym}^2 f, 2) \ll \log(N)^3$ and from the fact that the Manin's constant is bounded whenever the conductor is squarefree. The last estimate comes from the lower bound $L(\mathrm{Sym}^2 f, 2) \gg 1/\log(N)$ for N squarefree (cf. [8]). □

The curves E_k defined by $y^2 + xy = x^3 + k$ (with $432k^2 + k$ squarefree) give a infinite family of elliptic curves for which the conditions in the proposition hold.

The lower bound of the proposition also holds in the more general setting where the condition "$\Delta_{min}(E)$ is squarefree" is replaced by "E is semi-stable (i.e. N is squarefree)".

We wrote a GP-PARI ([9]) program for computing the modular degrees using the method explained above. In the following table we give three examples for which the modular degree is very large. In each cases, $\deg(\varphi)$ was computed in a few minutes. The column $\sharp\{a_n\}$ indicates the number of coefficients a_n needed (for an accuracy of $\deg(\varphi) \approx 10^{-4}$).

$[a_1, a_2, a_3, a_4, a_6]$	N	$\deg(\varphi)$	$\sharp\{a_n\}$
$[1, 0, 0, -190366575, 325694589866937]$	3990	14857920	16000
$[1, -1, 1, -48728476146, 4140222075962097]$	4898	13895640	20000
$[1, -1, 1, 1082069572, 90485275778687]$	3870	8547840	5000

The last curve is in fact the quadratic twist of the curve E' with coefficients $[1, 0, 1, 120229952, -3351306510322]$ of conductor 1290. We need 5000 coefficients a_n to compute $\deg(\varphi(E')) = 1068480$.

References

[1] A. ATKIN, J. LEHNER, *Hecke operators on $\Gamma_0(m)$*. Math. Ann. **185** (1970), 134–160.

[2] A. ATKIN, W. LI, *Twists of newforms and pseudo-eigenvalues of W-operators*. Invent. Math. **48** (1978), 221–243.

[3] 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** no. **4** (2001), 843–939. (electronic).

[4] J. COATES, C.-G. SCHMIDT, *Iwasawa theory for the symmetric square of an elliptic curve*. J. reine angew. Math. **375** (1987), 104–156.

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

[6] J. CREMONA, *Algorithms for modular elliptic curves*. Second edition, Cambridge University Press, 1997.

[7] J. CREMONA, *Computing the degree of the modular parametrization of a modular elliptic curve*. Math. Comp. **64** (1995), 1235–1250.

[8] D. GOLDFELD, J. HOFFSTEIN, D. LIEMAN, *An effective zero-free region*. Ann. of Math. (2) **140** no. **1** (1994), 177–181.

[9] C. BATUT, K. BELABAS, D. BERNARDI, H. COHEN, M. OLIVIER, `pari-gp`, available by anonymous ftp.

[10] G. SHIMURA, *The special values of the zeta functions associated with cusp forms*. Com. Pure Appl. Math. **29** (1976), 783–804.

[11] R. TAYLOR, A. WILES, *Ring-theoretic properties of certain Hecke algebras*. Ann. of Math. (2) **141** no. **3** (1995), 553–572.

[12] E. TOLLIS, *Zeros of Dedekind zeta functions in the critical strip*. Math. Comp. **66** (1997), 1295–1321.

[13] M. WATKINS, *Computing the modular degree of an elliptic curve*. Experimental Maths **11** no. 4 (2003), 487–502.

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

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

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

et

Ecole Polytechnique Fédérale de Lausanne
CH- 1015 Lausanne, Suisse
E-mail : `christophe.delaunay@epfl.ch`