ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 26, Number 3, Summer 1996

ESTIMATES FOR L-FUNCTIONS ASSOCIATED WITH SOME ELLIPTIC CURVES

FERNANDO CHAMIZO AND HENRYK IWANIEC

1. Introduction. Among the elliptic curves over **Q** written in the canonical form $y^2 = x^3+Ax+B$, only two families have automorphisms different from the identity and the hyperelliptic involution, namely (see [**1**, p. 93])

$$E : y^2 = x^3 - Dx \tag{1}$$

$$E : y^2 = x^3 + D. \tag{2}$$

All of these curves have complex multiplication, and it follows from the work of M. Deuring (see [**3**]) that they are modular. Consequently, there are various Dirichlet series naturally associated with them. In this note we examine the Hasse-Weil L-function and its symmetric square and obtain, by quite familiar means, estimates of their special values which are explicit with respect to the conductor. The analogue of these results for the Dirichlet L-functions is considered to be out of reach by current methods.

For simplicity we assume D is squarefree and $2, 3 \nmid D$. Hence the conductor, N, is a multiple of D^2 (see Appendix C of [**12**]).

In the next three sections we shall deal with the curve (1) and later we show how to modify the result for the curve (2). In the aforementioned sections, p and q will denote prime numbers satisfying $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$.

2. The Hasse-Weil L-function and its symmetric square. The Hasse-Weil L-function of (1) is defined by (see [**5**, Chapter 18])

$$\begin{aligned} L(s) = L_E(s+1/2) &= \sum_n a(n) n^{-s} \\ &= \prod_{q\nmid N} (1+q^{-2s})^{-1} \prod_{p\nmid N} (1-a(p)p^{-s}+p^{-2s})^{-1}, \end{aligned}$$

Received by the editors on December 28, 1994.

where

$$a(p) = \left(\frac{D}{\wp}\right)_4 \frac{\bar{\wp}}{\sqrt{p}} + \left(\frac{D}{\bar{\wp}}\right)_4 \frac{\wp}{\sqrt{p}}, \tag{3}$$
$$\text{with} \quad p = \wp\bar{\wp}, \quad \wp \in \mathbf{Z}[i].$$

From the modularity of E, it follows that L is entire and satisfies the functional equation

$$\Lambda(s) = \pm\Lambda(1-s),$$

where

$$\Lambda(s) = (\sqrt{N}/2\pi)^s\Gamma(s+1/2)L(s).$$

The symmetric square of $L(s)$ is

$$B(s) = \mathcal{A}(s)/\zeta(s),$$

where $\mathcal{A}(s)$ is the Rankin-Selberg convolution

$$\mathcal{A}(s) = \zeta(2s)\sum_n |a(n)|^2 n^{-s}.$$

Note that we have introduced $\zeta(2s)$ in the usual definition (see [**8**]) in order to clear up the functional equation and the definition of the symmetric square. Also $\mathcal{A}(s)$ has a simple pole at $s=1$ and satisfies [**8**, Theorem 2.2]

$$\Lambda(s) = \Lambda(1-s),$$

where

$$\Lambda(s) = (\sqrt{NM}/4\pi^2)^s\Gamma(s)\Gamma(s+1/2)\mathcal{A}(s),$$

and M is the greatest squarefree number dividing N. In our case $M \asymp \sqrt{N}$.

G. Shimura [**11**] proved the remarkable fact that $B(s)$ is entire. From the functional equations for $\mathcal{A}(s)$ and $\zeta(s)$ one concludes that

$$\Lambda(s) = \Lambda(1-s),$$

where

$$\Lambda(s) = (NM/2\pi^{3/2})^s\Gamma(s/2+1/2)\Gamma(s+1/2)B(s).$$

3. Results. If p factors in $\mathbf{Z}[i]$ as $p = \wp\bar{\wp}$, it is plain that one of the complex numbers $\pm\wp$, $\pm i\wp$, $\pm\bar{\wp}$, $\pm i\bar{\wp}$ has argument, say α_p, belonging to $(0, \pi/4)$. We define

$$F_N = \prod_{p|N}\left(1 - \frac{2\cos\alpha_p}{p}\right), \qquad G_N = \prod_{p|N}\left(1 - \frac{4\cos^2\alpha_p}{p}\right),$$
$$H_N = \prod_{p|N}\left(1 - \frac{4\sin^2\alpha_p}{p}\right).$$

Note that these quantities are bounded from above and from below by a constant if N has a fixed number of prime factors; in any case we have the sharp inequalities

$$(\log\log N)^{-4} \ll \left(\frac{\phi(N)}{N}\right)^4 \ll F_N^2, G_N, H_N < 1.$$

Following these definitions we can state our results.

Proposition 1. *If N is the conductor of* (1)

(A) $$L(1) \ll F_N \log^a N$$

(B) $$B(1) \ll G_N \log^b N$$

(C) $$B(1) \gg H_N \log^{-b} N$$

where $a = 2\sqrt{2}/\pi$, $b = 2/\pi$. Moreover, the implied constants are absolute and effective.

Remark. In general, if an elliptic curve is modular, $B(1)$ is closely related to the L^2-norm of a newform ϕ for $\Gamma_0(N)$; H. Iwaniec [**6**] proved $||\phi||_2 \ll N^\varepsilon$ for every newform ϕ for $\Gamma_0(N)$ and recently J. Hoffstein and P. Lockhart [**4**] proved $||\phi||_2 \gg N^{-\varepsilon}$. Our result allows one to replace N^ε and $N^{-\varepsilon}$ by a power of logarithm when ϕ corresponds to an elliptic curve of the type (1).

4. Proofs.

We shall use two lemmas that can be found in the literature. For convenience, we quote them here.

Lemma 1. *With the notation of Section* 3, *for any* $0 < \alpha < \pi/4$, *we have*

$$\sum_{\substack{p<x\\ 0<\alpha_p<\alpha}} 1 = \frac{2\alpha x}{\pi \log x} + O_\alpha\left(\frac{x}{\log^2 x}\right).$$

This lemma can be proved using standard arguments from the theory of Hecke L-functions. A proof of a more general and stronger result was given by I.P. Kubilius [**7**] and T. Mitsui [**9**]. I.V. Chulanovski [**2**] gave an elementary proof but with a worse error term.

Lemma 2. *Let* f *be a multiplicative function such that* $f(q^k) = 0$, $0 \le f(p^k) \le 2$ *and*

$$\sum_{p<x} f(p) = \tau \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

Then

$$\sum_{n<x} f(x) \sim C \frac{x}{\log^{1-\tau} x},$$

where C *is a positive constant depending on* f.

This result was proved by E. Wirsing [**13**] in a more general case, using elementary methods.

Now we proceed to prove Proposition 1.

Proof. Firstly we observe that

$$2\sin\alpha_p \le |a(p)| \le 2\cos\alpha_p, \quad \text{if } p \nmid N.$$

By Lemma 1 and partial summation, if $1 < \sigma < 2$,

$$\sum_{p<x} \frac{2\cos\alpha_p}{p^\sigma} = -a\log(\sigma-1) + O(1).$$

Hence

$$\begin{aligned} L(\sigma+it) &\ll \prod_{p\nmid N}(1-|a(p)|p^{-\sigma}+p^{-2\sigma})^{-1} \\ &\ll \prod_{p\nmid N}\left(1-\frac{2\cos\alpha_p}{p^\sigma}\right)^{-1} \\ &= F_N\prod_{p}\left(1-\frac{2\cos\alpha_p}{p^\sigma}\right)^{-1} \\ &\ll F_N(\sigma-1)^{-a}. \end{aligned}$$

Hence, by the functional equation,

$$L(1-\sigma+it) \ll F_N(\sqrt{N}(|t|+1))^\sigma(\sigma-1)^{-a}.$$

Then the Praghmen-Lindelöf principle for $-\delta < \sigma < 1+\delta$, with $\delta^{-1} = \log(N(|t|+1))$, proves

$$\begin{gathered} L(\sigma+it) \ll F_N(\sqrt{N}(|t|+1))^{1-\sigma}\log^a(N(|t|+1)), \\ 0 \le \sigma \le 1, \end{gathered}$$

and (A) follows by choosing $\sigma + it = 1$.

The proof of (B) is similar; one uses the bound

$$\begin{aligned} B(\sigma+it) &\ll (\sigma-1)\sum_n |a(n)|^2 n^{-\sigma} \\ &\ll (\sigma-1)G_N\prod_p\left(1-\frac{4\cos^2\alpha_p}{p^\sigma}\right)^{-1}, \end{aligned}$$

and

$$\sum_{p<x}\frac{4\cos^2\alpha_p}{p^\sigma}=-(1+b)\log(\sigma-1)+O(1).$$

By the functional equation and the Praghmen-Lindelöf principle as before (note that $M\asymp\sqrt{N}$), one concludes that

$$B(\sigma+it)\ll G_N(\sqrt{N}(|t|+1))^{3(1-\sigma)/2}\log^b(N(|t|+1)),$$

and this proves (B) by choosing $\sigma+it=1$.

For the proof of (C) we define the multiplicative function, f, given by $f(p)=4\sin^2\alpha_p$, $f(p^k)=0$ if $k\geq 2$, and $f(q^k)=0$ if $k\geq 1$. Note that $|a(p)|\geq f(p)$ if $p\nmid N$, and by Lemma 1 and partial summation,

$$\sum_{p<x}f(p)=(1-b)\frac{x}{\log x}+O\left(\frac{x}{\log^2 x}\right).$$

Using that $\mathcal{A}(s)$ is holomorphic except for a simple pole at $s=1$ with residue $B(1)$, one proves by standard complex integration methods (compare with [**10**])

$$\sum_{n<x}|a(n)|^2=\frac{B(1)}{\zeta(2)}x+O(N^Ax^{1-\delta}),$$

for some A, $\delta>0$.

On the other hand, by Lemma 2,

$$\sum_{n<x}|a(n)|^2\geq\sum_{\substack{(n,N)=1\\ n<x}}f(n)\geq H_N\sum_{n<x}f(n)\gg H_N\frac{x}{\log^{1-\tau}x}.$$

Combining both estimates for $x=N^\theta$ with θ sufficiently large, (C) follows. □

5. Modifications for the curve $y^2=x^3+D$. Our arguments for the curve (2) are quite similar to that for (1). In this case, if we denote by p and q prime numbers satisfying $p\equiv 1(\mathrm{mod}\,3)$ and $q\equiv 2(\mathrm{mod}\,3)$, the Hasse-Weil L-function has the same definition (see [**5**, Chapter 18]), but

$$a(p) = -\left(\frac{4D}{\wp}\right)_6 \frac{\bar{\wp}}{\sqrt{p}} - \left(\frac{4D}{\bar{\wp}}\right)_6 \frac{\wp}{\sqrt{p}},$$
$$\text{with} \quad p = \wp\bar{\wp}, \quad \wp \in \mathbf{Z}[\omega],$$

where $\omega = (1+\sqrt{-3})/2$. Observe that one of the complex numbers $\omega^j\wp$, $\omega^j\bar{\wp}$, $j = 0, 1, \dots, 5$, has argument, say β_p, belonging to $(0, \pi/6)$. In this case

$$2\sin(\pi/6 - \beta_p) \le |a(p)| \le 2\cos\beta_p, \quad \text{if } p \nmid N.$$

Consequently, we modify the definitions of F_N, G_N and H_N as

$$F_N = \prod_{p|N}\left(1 - \frac{2\cos\beta_p}{p}\right), \qquad G_N = \prod_{p|N}\left(1 - \frac{4\cos^2\beta_p}{p}\right),$$
$$H_N = \prod_{p|N}\left(1 - \frac{4\sin^2(\pi/6 - \beta_p)}{p}\right),$$

and the proof of Proposition 1 follows along the same lines. The only difference is that the constant in the main term of Lemma 1 changes from $2/\pi$ to $3/\pi$ (see the references mentioned there), which affects the constants a and b. The result is:

Proposition 2. *The estimates of Proposition* 1 *hold for the curve* (2) *with $a = 3/\pi$ and $b = 3\sqrt{3}/2\pi$.*

Remark. Note that in both propositions $b < 1$.

REFERENCES

1. J.W.S. Cassels, *Lectures on elliptic curves*, Cambridge University Press, 1991.

2. I.V. Chulanovski, *An elementary proof of the law of distribution of primes in the Gaussian field*, Vestn. Leningr. Univ. **13** (1956), 43–62 (in Russian).

3. M. Deuring, *Die Zetafunktion einer algebraischen Kurve von Geschechte Eins*, I, II, III, IV, Nach. Akad. Wiss. Göttingen (1953), 85–94, (1955), 13–42, (1956), 37–76 (1957), 55–80.

4. J. Hoffstein and P. Lockhart, *Coefficients of mass forms and the Siegel zero with appendix by D. Goldfield, J. Hoffstein, D. Lieman. An effective zero-free region*, Ann. Math. **140** (1994), 161–181.

5. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York, 1982.

6. H. Iwaniec, *Small eigenvalues of Laplacian for* $\Gamma_0(N)$, Acta Arith. **16** (1990), 65–82.

7. I.P. Kubilius, *On some problems of the geometry of prime numbers*, Mat. Sbornik **31** (1952), 507–542 (in Russian).

8. W.W. Li, *L-series of Rankin type and their functional equations*, Math. Ann. **244** (1979), 135–166.

9. T. Mitsui, *Generalized prime number theorem*, Japan J. Math. **26** (1956), 1–42.

10. R.A. Rankin, *Contributions to the theory of Ramanujan's function* $\tau(n)$ *and similar arithmetical functions*, Proc. Cambridge Philos. Soc. **35** (1939), 357–372.

11. G. Shimura, *On the holomorphy of certain Dirichlet series*, Proc. London Math. Soc. **31** (1975), 79–98.

12. J.H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

13. E. Wirsing, *Das asymptotische Verhalten von Summen über multiplikative Funktionen*, Math. Ann. **143** (1961), 75–102.

Universidad Autónoma De Madrid, Departamento De Matematicas, Madrid 28049, Spain

Rutgers University, Department of Mathematics, New Brunswick, NJ 08903-2101