

SOME CONJECTURES ON ELLIPTIC CURVES OVER CYCLOTOMIC FIELDS

BY

D. GOLDFELD AND C. VIOLA

ABSTRACT. We give conjectures for the mean values of Hasse-Weil type L -functions over cyclotomic fields. In view of the Birch-Swinnerton-Dyer conjectures, this translates to interesting arithmetic information.

1. In 1967 A. Weil [6] showed that if the Dirichlet series

$$L_1(s) = \sum_{n=1}^{\infty} a(n)n^{-s}, \quad L_1(s, \chi) = \sum_{n=1}^{\infty} a(n)\chi(n)n^{-s} \quad (\chi \bmod q)$$

satisfy the functional equations

$$(1) \quad (\sqrt{N}/2\pi)^s \Gamma(s) L_1(s) = w_1 (\sqrt{N}/2\pi)^{k-s} \Gamma(k-s) L_1(k-s), \quad |w_1| = 1,$$

$$(\sqrt{N}/2\pi q)^s \Gamma(s) L_1(s, \chi) = w_\chi (\sqrt{N}/2\pi q)^{k-s} \Gamma(k-s) L_1(k-s, \bar{\chi}),$$

$$(2) \quad w_\chi = w_1 \varepsilon(q) \frac{\tau_\chi}{\tau_{\bar{\chi}}} \chi(-N), \quad \tau_\chi = \sum_{a=1}^q \chi(a) e^{2\pi i a/q},$$

for “sufficiently many” q such that $(q, N) = 1$ and all primitive characters $\chi \bmod q$, where N and k are positive integers and ε is a primitive character mod N , then $f(z) = \sum_{n=1}^{\infty} a(n) e^{2\pi i n z}$ is a modular form with multiplier ε of weight k for the congruence subgroup

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}, ad - bc = 1, c \equiv 0 \pmod{N} \right\}.$$

Our aim is to propose some conjectures on the asymptotic behaviour of the mean value

$$S(X; h) = \sum_{\substack{p \leq X \\ p \equiv 1(h)}} \prod_{\substack{\chi \bmod p \\ \chi^h = \chi_0 \\ \chi^r \neq \chi_0 \text{ for } r < h}} L_1(k/2, \chi) \quad (h \geq 2 \text{ a fixed integer})$$

where the sum is restricted to primes p , and χ_0 is the principal character mod p .

Let $L_h(s, \chi) = \sum_{n=1}^{\infty} a(n^h) \chi(n) n^{-s}$. If $L_1(s)$ satisfies (1) and (2), then we propose the following

Received by the editors June 12, 1981.

1980 *Mathematics Subject Classification*. Primary 12A70.

© 1983 American Mathematical Society
0002-9947/81/0000-0759/\$09.00

MAIN CONJECTURE. For $h = 2$ ($\chi^2 = \chi_0$, $\chi \neq \chi_0$, $\chi \bmod p$):

$$S(X; 2) = \sum_{p \leq X} L_1(k/2, \chi) \\ \sim \sum_{p \leq X} \frac{1 + w_1 \varepsilon(p) \chi(-N)}{\Gamma(k/2)} \cdot \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \Gamma(k/2+z) \left(\frac{\sqrt{N}}{2\pi} p \right)^z L_2(k+2z, \chi_0) \frac{dz}{z}.$$

For $h > 2$:

$$S(X; h) \sim \sum_{\substack{p \leq X \\ p \equiv 1(h)}} \frac{1 + (w_1 \varepsilon(p))^{\phi(h)}}{\Gamma(k/2)^{\phi(h)}} \\ \cdot \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \Gamma(k/2+z)^{\phi(h)} \left(\frac{\sqrt{N}}{2\pi} p \right)^{\phi(h)z} H(z)^{\phi(h)/2} \frac{dz}{z} \quad (c > 0),$$

where

$$H(z) \equiv \sum_{n=1}^{\infty} \frac{a(n)^2 \chi_0(n)}{n^{k+2z}} + L_h(h(k/2 + z), \chi_0)^2.$$

The integrals in the above conjecture can be easily evaluated asymptotically by shifting the line of integration and computing the residues at $z = 0$. If we assume that $L_1(s)$ has an Euler product of the form

$$(3) \quad L_1(s) = \prod_{p|N} \left(1 - \frac{a(p)}{p^s} \right)^{-1} \cdot \prod_{p \nmid N} \left(1 - \frac{\gamma_p}{p^s} \right)^{-1} \left(1 - \frac{\bar{\gamma}_p}{p^s} \right)^{-1},$$

with $|\gamma_p|^2 = p^{k-1}$ (see [1]), then we have the following

PROPOSITION. Assuming the Main Conjecture and the Euler product (3), it follows that

$$(i) \quad S(X; 2) \sim \frac{48\pi}{N} \prod_{p|N} (1 - p^{-2})^{-1} \cdot \langle f, f \rangle \cdot \frac{X}{\log X},$$

where

$$\langle f, f \rangle = \iint_{\Gamma_0(N) \backslash H} \left| \sum_{n=1}^{\infty} a(n) e^{2\pi i n z} \right|^2 y^{k-2} dx dy$$

is the Petersson inner product of f with itself;

(ii) For $h > 2$,

$$S(X; h) \sim 2 \left(\frac{24\pi}{N} \prod_{p|N} (1 + p^{-1})^{-1} \cdot \langle f, f \rangle \right)^{\phi(h)/2} \frac{X(\phi(h) \log X)^{\phi(h)/2-1}}{(\frac{1}{2}\phi(h))!}.$$

In the case that the weight k is 2, that (1), (2) and (3) are satisfied and the $a(n)$ are rational, it is known (see [4, Theorems 7.14, 7.15]) that $L_1(s)$ is the Hasse-Weil L -function of some elliptic curve E , and $\langle f, f \rangle$ can always be expressed as the product of an algebraic number, a power of π , and the two periods of E . For example (see [5]), when $k = 2$, $N = 11$ there is a unique cusp form of weight 2:

$$f(z) = e^{2\pi i z} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z})^2 \prod_{n=1}^{\infty} (1 - e^{2\pi i n z})^2 = \sum_{n=1}^{\infty} a(n) e^{2\pi i n z},$$

and $L_1(s) = L_E(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ is the Hasse-Weil L -function of the elliptic curve $E: y^2 + y = x^3 - x^2$. For this curve, our conjectures take the following form:

$$S(X; 2) \sim \frac{11}{5\pi} \Omega^+ \Omega^- \frac{X}{\log X},$$

$$S(X; h) \sim 2 \left(\frac{\Omega^+ \Omega^-}{\pi} \right)^{\phi(h)/2} \frac{X(\phi(h) \log X)^{\phi(h)/2-1}}{(\frac{1}{2}\phi(h))!} \quad (h > 2).$$

Here $\Omega^+ = 0.6346047 \dots$ and $\Omega^- = 1.4588166 \dots$ are the real period and the absolute value of the imaginary period of E , respectively.

Now let p be an odd prime. The Hasse-Weil L -function of E over the cyclotomic field $\mathbb{Q}(\sqrt[p]{1})$ is given by

$$L_{\mathbb{Q}(\sqrt[p]{1}) \setminus E}(s) = \prod_{\chi \bmod p} L_E(s, \chi).$$

It is reasonable to expect that the average value (as p varies) is given by

$$\text{average value of } L_{\mathbb{Q}(\sqrt[p]{1}) \setminus E}(1) \sim L_E(1) \cdot \frac{11}{5\pi} \Omega^+ \Omega^- \cdot \prod_{\substack{h|(p-1) \\ h > 2}} \frac{2 \left(\frac{\phi(h)}{\pi} \Omega^+ \Omega^- \log p \right)^{\phi(h)/2}}{\phi(h)(\frac{1}{2}\phi(h))!}.$$

Sharper forms of part (ii) of the Proposition can be derived on assuming the analytic continuation of $L_h(s)$ for $h > 2$. Then there will be extra terms involving lower powers of $\log X$, whose coefficients are expressible in terms of the special values of $L_h(s)$, some of which can be given by the conjectures of Deligne [2].

2. In order to lend credence to our Main Conjecture, we give the following arguments. Firstly, the conjecture for $S(X; 2)$ has already been dealt with in [3]. We therefore consider $S(X; h)$ for $h > 2$. For any prime $p \equiv 1 \pmod{h}$ there are $\phi(h)$ characters mod p of exact order h , and moreover these characters are all primitive. It follows by (2) that, for $p \nmid N$,

$$\left(\left(\frac{\sqrt{N}}{2\pi} p \right)^s \Gamma(s) \right)^{\phi(h)} \prod'_{\chi \bmod p} L_1(s, \chi) = W \left(\left(\frac{\sqrt{N}}{2\pi} p \right)^{k-s} \Gamma(k-s) \right)^{\phi(h)} \prod'_{\chi \bmod p} L_1(k-s, \chi),$$

$$W = W(p, h) = \prod'_{\chi \bmod p} w_{\chi} = (w_1 \varepsilon(p))^{\phi(h)},$$

where $\prod'$ means that the product is taken over all characters of exact order h , which we denote by $\chi_1, \dots, \chi_{\phi(h)}$. By Lavrik's method (see [3]), we have

$$\prod' L_1(k/2, \chi) = \frac{1+W}{\Gamma(k/2)^{\phi(h)}} \sum_{n_1} \dots \sum_{n_{\phi(h)}} a(n_1) \dots a(n_{\phi(h)}) \chi_1(n_1) \dots \chi_{\phi(h)}(n_{\phi(h)}) (n_1 \dots n_{\phi(h)})^{-k/2}$$

$$\cdot \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \left(\Gamma\left(\frac{k}{2} + z\right) \left(\frac{\sqrt{N}}{2\pi} p \right)^z \right)^{\phi(h)} (n_1 \dots n_{\phi(h)})^{-z} \frac{dz}{z}.$$

Now, summing over p should give a lot of cancellation except for those $\phi(h)$ -tuples

$(n_1, \dots, n_{\phi(h)})$ for which

$$(5) \quad \prod_{i=1}^{\phi(h)} \chi_i(n_i) = 1$$

for all $p \nmid n_i$ ($i = 1, \dots, \phi(h)$). We can arrange the characters so that $\chi_i = \bar{\chi}_{\phi(h)-i+1}$. It follows that

$$\chi_i(n_i) \chi_{\phi(h)-i+1}(n_{\phi(h)-i+1}) = 1$$

whenever $n_i = n_{\phi(h)-i+1}$ and $p \nmid n_i$. Also $\chi_i(n_i) = 1$ whenever $n_i = m_i^h$ is an h th-power and $p \nmid m_i$. Combinations of these two cases are the only ways in which the aforementioned tuples can be constructed. Hence, every tuple $(n_1, \dots, n_{\phi(h)})$ satisfying (5) is given as follows. Let $0 \leq r \leq \frac{1}{2}\phi(h)$; choose an r -tuple $(i_1, \dots, i_r)$ with $1 \leq i_1 < \dots < i_r \leq \frac{1}{2}\phi(h)$. Put $n_{i_j} = n_{\phi(h)-i_j+1}$ ($j = 1, \dots, r$). Also let $n_i = m_i^h$ be a perfect h th-power for $i \neq i_j$, $i \neq \phi(h) - i_j + 1$ ($j = 1, \dots, r$). Since there are exactly $\binom{\phi(h)/2}{r}$ such r -tuples, it is reasonable to expect that, after summing (4) over primes $p \equiv 1 \pmod{h}$, $S(X; h)$ should be given asymptotically as

$$\begin{aligned} S(X; h) &\sim \sum_{\substack{p \leq X \\ p \equiv 1(h)}} \frac{1+W}{\Gamma(k/2)^{\phi(h)}} \sum_{r=0}^{\phi(h)/2} \binom{\frac{1}{2}\phi(h)}{r} \\ &\quad \times \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \left(\Gamma\left(\frac{k}{2} + z\right) \left(\frac{\sqrt{N}}{2\pi} p\right)^z \right)^{\phi(h)} \\ &\quad \cdot \left(\sum_{n=1}^{\infty} \frac{a(n)^2 \chi_0(n)}{n^{k+2z}} \right)^r \left(\sum_{m=1}^{\infty} \frac{a(m^h) \chi_0(m)}{m^{h(k/2+z)}} \right)^{\phi(h)-2r} \frac{dz}{z} \\ &= \sum_{\substack{p \leq X \\ p \equiv 1(h)}} \frac{1+W}{\Gamma(k/2)^{\phi(h)}} \cdot \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \left(\Gamma\left(\frac{k}{2} + z\right) \left(\frac{\sqrt{N}}{2\pi} p\right)^z \right)^{\phi(h)} H(z)^{\phi(h)/2} \frac{dz}{z}. \end{aligned}$$

In order to derive the Proposition from the Main Conjecture, note that the Rankin-Selberg L -function $\sum_{n=1}^{\infty} |a(n)|^2 n^{-s}$ has a simple pole at $s = k$ with residue

$$\frac{48\pi}{N} \prod_{p \mid N} (1 + p^{-1})^{-1} \cdot \langle f, f \rangle.$$

If $L_1(s)$ satisfies (3), then the coefficients $a(n)$ are real, and $w_1 \varepsilon(p) = \pm 1$. Also, $L_h(s)$ is regular for $\operatorname{Re}(s) > 1 + h(k-1)/2$. Hence, for $h > 2$, $H(z)$ is regular for $\operatorname{Re}(z) > \frac{1}{h} - \frac{1}{2}$ except for a simple pole at $z = 0$, with residue

$$\frac{24\pi}{N} \prod_{p \mid N} (1 + p^{-1})^{-1} \cdot \langle f, f \rangle.$$

Shifting the line of integration to $c = \frac{1}{h} - \frac{1}{2} + \varepsilon$ ($0 < \varepsilon < \frac{1}{2} - \frac{1}{h}$) and using standard estimates for the growth of the Rankin-Selberg L -function, the proposition follows on computing the main term of the residue and applying the prime number theorem for arithmetic progressions.

REFERENCES

1. P. Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. **43** (1973), 273–307.
2. ———, *Valeurs de fonctions L et périodes d'intégrales*, Proc. Sympos. Pure Math., vol. 33, part 2, Amer. Math. Soc., Providence, R.I., 1979, pp. 313–346.

3. D. Goldfeld and C. Viola, *Mean values of L -functions associated to elliptic, Fermat and other curves at the centre of the critical strip*, J. Number Theory **11** (1979), 305–320.
4. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, Princeton, N.J., 1971.
5. J. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.
6. A. Weil, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. **168** (1967), 149–156.

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MASSACHUSETTS 02139

ISTITUTO DI MATEMATICA, UNIVERSITÀ DI PISA, PISA, ITALY