L-series of an elliptic curve

Canonical name	LseriesOfAnEllipticCurve
Date of creation	2013-03-22 13:49:43
Last modified on	2013-03-22 13:49:43
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	8
Author	alozano (2414)
Entry type	Definition
Classification	msc 14H52
Synonym	L-function of an elliptic curve
Related topic	EllipticCurve
Related topic	DirichletLSeries
Related topic	ConductorOfAnEllipticCurve
Related topic	HassesBoundForEllipticCurvesOverFiniteFields
Related topic	ArithmeticOfEllipticCurves
Defines	L-series of an elliptic curve
Defines	local part of the L-series
Defines	root number

Let E be an elliptic curve over $\mathbb{Q}$ with Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with coefficients $a_i \in \mathbb{Z}$. For p a prime in $\mathbb{Z}$, define N_p as the number of points in the reduction of the curve modulo p, this is, the number of points in:

$$\{O\} \cup \{(x, y) \in {\mathbb{F}_p}^2 \colon y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \equiv 0 \ mod\ p\}$$

where O is the point at infinity. Also, let $a_p = p + 1 - N_p$. We define the *local part at p of the L-series* to be:

$$L_p(T) = \begin{cases} 1 - a_pT + pT^2, \text{ if } E \text{ has good reduction at } p, \\ 1 - T, \text{ if } E \text{ has split multiplicative reduction at } p, \\ 1 + T, \text{ if } E \text{ has non-split multiplicative reduction at } p, \\ 1, \text{ if } E \text{ has additive reduction at } p. \end{cases}$$

Definition. *The L-series of the elliptic curve E is defined to be:*

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

where the product is over all primes.

Note: The product converges and gives an analytic function for all $Re(s) > 3/2$. This follows from the fact that $\mid a_p \mid \leq 2\sqrt{p}$. However, far more is true:

Theorem (Taylor, Wiles)**.** *The L-series $L(E, s)$ has an analytic continuation to the entire complex plane, and it satisfies the following functional equation. Define*

$$\Lambda(E, s) = (N_{E/\mathbb{Q}})^{s/2}(2\pi)^{-s}\Gamma(s)L(E, s)$$

where $N_E/\mathbb{Q}$ is the conductor of E and Γ is the Gamma function. Then:

$$\Lambda(E, s) = w\Lambda(E, 2 - s) \quad \textit{with } w = \pm 1$$

The number w above is usually called the *root number* of E, and it has an important conjectural meaning (see Birch and Swinnerton-Dyer conjecture).

This result was known for elliptic curves having complex multiplication (Deuring, Weil) until the general result was finally proven.

References

[1] James Milne, *Elliptic Curves*, http://www.jmilne.org/math/CourseNotes/math679.htmlonli course notes.

[2] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.

[3] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1994.

[4] Goro Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, Princeton, New Jersey, 1971.