

18.785: Analytic Number Theory, MIT, spring 2007 (K.S. Kedlaya)
***L*-functions of elliptic curves**

The standard book on elliptic curves is Silverman's *The Arithmetic of Elliptic Curves*.

1 Elliptic curves and their *L*-functions

An *elliptic curve* over a field K is a nonsingular cubic plane curve. If K has characteristic > 2 , any such curve can be put in the form $y^2 = P(x)$, where $P(x) = x^3 + ax^2 + bx + c$ is a polynomial with no repeated roots. (This is a pretty *ad hoc* definition; see Silverman's book for a proper definition.)

If $E : y^2 = P(x)$ is an elliptic curve over \mathbb{Q} , then for all but finitely many primes p , the reduction of E modulo p is a nonsingular cubic, and hence elliptic curve over \mathbb{F}_p . (Warning: the finite set of bad primes depends on the choice of the equation $y^2 = P(x)$, not just on the isomorphism class of E . There is an optimal choice of the defining equation, but we won't use that here.) We define the *L-function* of E as the product

$$L(E, s) = \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

over all of the nonexceptional primes, where $p + 1 - a_p$ is the number of points on E modulo \mathbb{F}_p . (Remember that E is being drawn in the projective plane, so you have to count the one point $[0 : 1 : 0]$ at infinity.)

It's obvious that there are at most $2p + 1$ points on E , two for each possible x -coordinate plus one point at infinity; that implies that $L(E, s)$ converges absolutely for $\operatorname{Re}(s) > 2$. Actually one can do better.

Lemma 1 (Hasse). *We have $|a_p| \leq 2\sqrt{p}$ for all p .*

This means that $L(E, s)$ actually converges absolutely for $\operatorname{Re}(s) > 3/2$.

In a few cases, the a_p exhibit predictable behavior. For instance, if E is the curve $x^3 + y^3 = 1$, then for $p \equiv 2 \pmod{3}$, we have $a_p = 0$, whereas for $p \equiv 1 \pmod{3}$, we can write a_p in terms of integers A, B for which $A^2 + 3B^2 = p$ (this was first observed by Gauss). In most cases, however, no such easy formula exists.

By contrast, suppose E is a nonsingular conic curve passing through at least one \mathbb{Q} -rational point; then $\#E(\mathbb{F}_p) = p + 1$ always. (The points on the curve are in bijection with the lines through the given point.)

Theorem 2. *The function $L(E, s)$ extends to a holomorphic function on \mathbb{C} , satisfying a functional equation between s and $2 - s$.*

This is a consequence of the *modularity of elliptic curves*. This theorem is the result of work of Wiles, Taylor-Wiles, Diamond, Fujiwara, Conrad-Diamond-Taylor, and Breuil-Conrad-Diamond-Taylor. (Whew!) When combined with a theorem of Ribet (part of Serre's

conjecture), the modularity of elliptic curves (actually just the special case proved by Wiles) resolves the Fermat problem.

There is also an amazing conjecture relating the L-function to the \mathbb{Q} -rational points of E . (The Mordell-Weil theorem states that $E(\mathbb{Q})$ is a finitely generated abelian group.)

Conjecture 3 (Birch, Swinnerton-Dyer). *The order of vanishing of $L(E, s)$ at $s = 1$ equals the rank of the finitely generated abelian group $E(\mathbb{Q})$.*

This is known by work of Kolyvagin, Kato, Gross-Zagier, etc. in case the order of vanishing is 0 or 1.