LECTURE 24: FROM ZETA TO L-FUNCTIONS

LARRY ROLEN, VANDERBILT UNIVERSITY, FALL 2020

A tram journey to Nikko at the 1955 conference on algebraic number theory. Shown are (left to right) T. Tamagawa, J.-P. Serre, Y. Taniyama and A. Weil.

Picture of participants at conference where the Modularity Theorem was conjectured, from Shimura's article "Yutaka Taniyama and his time: very personal recollections."

We have been studying elliptic curves over finite fields via zeta functions. What we are really after is the structure of elliptic curves over fields like $\mathbb{Q}$. To do this, we can try to do a local-global principle. Recall that this means that we try to understand points over $\mathbb{Q}$ by understanding it over $\mathbb{R}$ and over all p-adic fields $\mathbb{Q}_p$. There is a result called **Hensel's Lemma** which allows one to lift "good" solutions to polynomial equations mod primes to solutions mod powers of primes in infinite sequences (think of this as a version of Newton's Method for real functions, but its much more stable). This basically says that to know the $\mathbb{Q}_p$ points its enough to know the points over the finite fields $\mathbb{F}_{p^r}$.

The points over $\mathbb{R}$ are the easy ones, and the points over the finite fields are exactly what's encoded by the congruence zeta functions! So if we believe in the local-global principle, we would expect that the solutions over $\mathbb{R}$ and the data of all congruence zeta functions for all primes p should tell us something about the $\mathbb{Q}$-points. This is where the Birch and Swinnerton-Dyer conjecture will come in.

Essentially, there will be one object which encodes all of the congruence zeta functions at once. To motivate this, recall the Euler product for the Riemann zeta function:

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}}.$$

We get something the looks like one of the factors in this product if we plug in $T = p^{-s}$ in the congruence zeta function at a good prime p not dividing the discriminant of a curve E:

$$Z(E/\mathbb{F}_p; p^{-s}) = \frac{1 - 2a_p p^{-s} + p^{1-2s}}{(1-p^{-s})(1-p^{1-s})}.$$

Note that before the term in the numerator was denoted by a_E as we were thinking of the curve as moving but for some fixed prime, but here I want the curve fixed and the prime moving, so I call it a_p to show that dependence.

Take the product over the good primes

$$\prod_{p\nmid\Delta(E)} Z(E/\mathbb{F}_p;p^{-s}) = \prod_{p\nmid\Delta(E)} \frac{1-2a_pp^{-s}+p^{1-2s}}{(1-p^{-s})(1-p^{1-s})}.$$

The stuff in the bottom essentially gives us a factor $\zeta(s)\zeta(s-1)$, which is kind of uniform and doesn't contain the interesting data about finite field point counts. So we'll try to omit it. But more importantly, what about the primes of bad reduction? For those, we have to define an analogue of the polynomial $1-2a_pp^{-s}+p^{1-2s}$. This choice isn't obvious, and the precise reason for it would take us too far afield, so we'll just state what it is.

Long Definition. Let $E/\mathbb{Q}$ be a rational elliptic curve. If there is bad reduction at a prime p, we saw before there can be two types of bad behavior. There can be a **node** (self-intersection point) or a **cusp** (sharp point). In the case of a node, we say the reduction is **multiplicative**, and if its a cusp, we say its **additive**. There are two types of multiplicative reduction: **split and non-split**. Split means that the two tangent lines at the node have slopes in $\mathbb{F}_p$.

The **conductor** of E is the product

$$N = N(E) := \prod_p p^{e_p}$$

where

$$e_p := \begin{cases} 0 & \text{if } E \text{ has good reduction at } p, \\ 1 & \text{if } E \text{ has multiplicative reduction at } p, \\ 2 & \text{if } E \text{ has additive reduction at } p \text{ and } p \neq 2,3, \\ 2+\delta_p & \text{if } E \text{ has additive reduction at } p \text{ and } p \in \{2,3\}, \end{cases}$$

where δ_p is a complicated number that depends on **wild ramification** (we won't define this here). This can be thought of as a refinement of the discriminant. It has the same primes dividing it, but the exponents of those primes determine the type of bad reduction. For an elliptic curve E, the **local factors** are the polynomials in p^{-s}:

$$L_p(E,s) := \begin{cases} 1-a_pp^{-s}+p^{1-2s} & p\nmid N, \\ 1-a_pp^{-s} & p|N,\ p^2\nmid N, \\ 1 & p^2|N. \end{cases}$$

Here, $a_p = p+1-\#E(\mathbb{F}_p)$ if p is a prime of good reduction, and $a_p = \pm 1$ if E has multiplicative reduction depending on if its split or non-split.

The **Hasse-Weil L-function** of E is the product

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

That indeed was a long definition! However, the conductor will soon turn out to be very important to us, and there is no getting around the fact that 2's and 3's are nasty to deal with. Hasse and Weil, after whom this L-function is named, made the following.

Conjecture (Hasse-Weil)**.** *The function $L(E,s)$ has an analytic continuation to the complex plane and satisfies a functional equation.*

In the case of the congruent number curves E_n, this is easier than usual to prove. The idea is that $L(E,s)$ can be related to the L-function of a **modular form**. This is again possible because E_n has CM. Koblitz's book continues the calculations we've done on the congruence zeta functions of these and proves that in fact

$$L(E_n,s)=\sum_I \widetilde{\chi}_n(I)(N(I))^{-s},$$

where I runs over the non-zero ideals of $\mathbb{Z}[i]$, $N(I)$ denotes the "norm" of an ideal, and $\widetilde{\chi}_n$ is what's known as a **Hecke character**. This implies that

$$L(E_n,s)=L(f,s)$$

where f is a **theta function** for the Hecke character.

It turns out that something similar holds for all elliptic curves over $\mathbb{Q}$, but its very difficult to prove.

Theorem (The Modularity Theorem, previously a conjecture of Taniyama–Shimura-Weil and now a theorem of Wiles and Breuil-Conrad-Diamond-Taylor)**.** *Given any elliptic curve $E/\mathbb{Q}$ of conductor N, there is a weight 2, level N Hecke eigenform with*

$$L(E,s)=L(f,s).$$

That is, there is a modular form in $S_2(N)$ with

$$a_f(p)=p+1-\#E(\mathbb{F}_p)$$

for all but finitely many primes p.

Getting the level of the modular form right, that is as the conductor, is a very important part of this conjecture. We've shown that modular forms have an Euler product if and only if they're eigenforms, and elliptic curve L-functions are *defined* as Euler products. So there's no hope in such a connection if the modular form isn't an eigenform. Since the Euler product of the L-function of such a form is of the shape

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

its also apparent from the definition of $L(E,s)$ that the only possibility is that f has weight 2.

This seems like a strange conjecture to believe at first. Initial evidence in small dimensional spaces gave the first hints (for example, there is no elliptic curve with level

less than 11, and there is also no non-zero cusp form in $S_2(N)$ until $N = 11$). This was formulated into a grand conjecture at a famous conference in Japan.

Since modular form L-functions have analytic continuations and functional equations (in this case under $s \mapsto 2 - s$), the Modularity Theorem implies the following result. This is still the only known way to prove this.

Theorem. *The conjecture of Hasse-Weil is true.*

Before it was a theorem, many authors assumed it was true and proved conditional results based on it. Fortunately, all of those older papers are now rigorous theorems. So many stronger results can be proven for elliptic curves which are connected to a modular form. Of course, the main application Wiles had in mind was that it proves **Fermat's Last Theorem**.

Finally, to cap up our story on local-global, I claimed earlier that the L-function, which "knows" all the local data of the elliptic curve, should know something about the global data of the curve over $\mathbb{Q}$. This is the content of the (weak) BSD conjecture.

Conjecture (BSD)**.** *For any rational elliptic curve, the order of vanishing at the central critical point $s = 1$ of the critical strip gives the rank of the elliptic curve. That is,*

$$\mathrm{ord}_{s=1} L(E, s) = \mathrm{rk}(E/\mathbb{Q}).$$

In particular, $L(E, s) = 0$ if and only if there are infinitely many rational points on E.

Since $L(f, s) = L(E, s)$ for some modular form f, the L-function of a modular form near the central critical value determines the rank of the curve. The last step we'll need to apply this to the Congruent Number Problem will be that in families of quadratic twists, the L-values at $s = 1$ are actually encoded by the Fourier coefficients of a single modular form of half-integral weight.