Qiao Zhang's Lectures: Intro to Zeta Functions and L-functions

Almost everything in Number Theory can be interpreted in terms of L-functions. This is a very broad subject. We will have a very brief discussion here, including the most important algebraic properties.

Construction, Properties, Examples

The Riemann Zeta Function is the father of all L-functions. The definition is

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

for $Re(s) > 1$.

Properties:

1. $\zeta(s)$ has an analytic continuation to $\mathbb{C}$ with a simple pole at $s = 1$.
2. $\zeta(s)$ satisfies a functional equation.

$$\Lambda(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\prod_p\left(1 - \frac{1}{p^s}\right)^{-1}.$$

   The functional equation is

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

   The part $\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)$ comes from the ordinary absolute value, and $\left(1 - \frac{1}{p^s}\right)^{-1}$ p-adic evaluation. Note Λ has poles only at $s = 0, 1$.

3. $\zeta(s)$ has trivial zeros at $s = -2, -4, -6, \ldots$, but there are also infinitely many nontrivial zeros in the critical strip $0 \leq Re(s) \leq 1$.
4. Riemann Hypothesis: all the nontrivial zeros are on the line $Re(s) = \frac{1}{2}$.

Langlands Program/Conjecture: every L-function comes from an automorphic form.

Generalizations:

The Euler product

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_p \left(1 - \frac{1}{|p|^s}\right)^{-1}$$

is equivalent to $\mathbb{Z}$ is a UFD. To generalize, we need a UFD. The sum over n is a sum over ideals. Also, the $\prod_p$ is a product over prime ideals. EG - the algebraic number field case: integral ideals vs. prime ideals. We must work with norms of ideals. Sometimes 1 in the numerator of the prime product is replaced by a general complex number that is connected to the local properties of some object (and on p). Maybe there will be several factors for each p.

In general, the L-function may look like

$$L(s, X) = \sum_{n=1}^{\infty} \frac{\lambda_X(n)}{n^s} = \prod_p \left(1 - \frac{\lambda_{X,1}(p)}{p^s}\right)^{-1}\left(1 - \frac{\lambda_{X,2}(p)}{p^s}\right)^{-1}\cdots\left(1 - \frac{\lambda_{X,r}(p)}{p^s}\right)^{-1}$$

Additional desired properties:

1. analytic continuation (usually without poles)
2. Functional equation, eg

$$\Lambda(s,X) = *L(s,X)$$
$$\Lambda(s,X) = \Lambda(1-s,X^*)$$

3. Trivial zeros, Nontrivial zeros
4. GRH (Generalized Riemann Hypothesis)

In many cases, these properties are unsolved problems.

Usually, L-functions include global properties, also for the zeta functions, we might also be interested in local properties (eg mod p).

Concrete Examples:

Example **Dirichlet L-function**: Given a character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$

$$L(s,\chi) = \sum \frac{\chi(n)}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

Example **Elliptic Curves**

Let $E/\mathbb{Q}$ be an elliptic curve (genus 1). All such have a cubic equation:

$$y^2 = 4x^3 - g_2 x - g_3$$

with $g_2, g_3 \in \mathbb{Q}$. Question: Are there integer points on this curve? At each p, let

$$a_p = p - \#\{(x,y) \in \mathbb{F}_p^2 : y^2 = 4x^3 - g_2 x - g_3 (\operatorname{mod} p)\}$$

$$L(s,E) = \prod_{p \text{ prime}} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}$$
$$= \prod_{p \text{ prime}} \left(1 - \frac{\alpha_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p}{p^s}\right)^{-1}$$

where $\alpha_p + \beta_p = a_p$, $\alpha_p \beta_p = p$. This converges for $Re(s) > \frac{3}{2}$. We would like to find an analytic continuation (only proved by Wiles in 1993).

Example **Modular L-function**. Let f be a cusp form of weight k for $SL_2(\mathbb{Z})$. This is a holomorphic section of a line bundle of weight k over $SL_2(\mathbb{Z})\backslash\mathfrak{h}$. In other words,

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z),$$

for $a,b,c,d \in \mathbb{Z}$, $ad-bc = 1$. Note that the "forms" of type "$f(z)(dz)^{k/2}$" that are invariant have these $f(z)$'s above. Note that

$$f(z+1) = f(z)$$
$$f(z) = \sum_{n=1}^{\infty} a_n \exp(-2\pi ny + 2\pi inx)$$
$$L(s,f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{"="} \prod_{p \text{ prime}} \left(1 - \frac{\alpha_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p}{p^s}\right)^{-1}$$
$$= \prod_{p \text{ prime}} \left(1 - \frac{\alpha_p}{p^s} + \frac{1}{p^{2s-(k-1)}}\right)^{-1}$$

The analytic properties of this one are known.

Modularity

For example, if f is a modular form of weight $k = 2$, then

$$L(s,f) = \prod_{p \text{ prime}} \left(1 - \frac{\alpha_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1},$$

similar to elliptic curve. This was proved in the 1950s by Eichler-Shimura. The converse: given an elliptic curve, is it the same as a modular form L-function (Taniyama-Shimura Conjecture, proved by Weils in 1993 using Galois machinery). If the L-series has sufficiently good properties, then it must come from some f. This is only for elliptic curves over $\mathbb{Q}$. But what about other fields? This is the modularity problem.

Example: the Selberg zeta function over $SL(2,\mathbb{Z})$.

Birch-Swinnerton-Dyer Conjecture

Assume f is a polynomial in $\mathbb{Q}[x,y]$. Does the equation $f(x,y) = 0$ have a rational solution? Note that this is a plane curve in $\mathbb{C}^2$; assume that the curve is smooth. We desire solutions in $\mathbb{Q}^2$. The geometry is studied in $\mathbb{C}^2$. In the case that the genus is zero $g = \frac{1}{2}(d-1)(d-2)$, we have that the rational points form a group isomorphic to $\mathbb{Q}$. If the genus is > 1, then there are only finitely many rational points (Faltings: Mordell Conjecture 1974(?)). If the genus is 1, the curve is elliptic, and we can write the equation as

$$y^2 = 4x^3 - g_2 x - g_3.$$

This is a general formula for all elliptic curves, up to birational equivalence. We can give it a group structure. The sum of two points is computing by looking at collinear points (sum of two is the third point, after a reflection). This is the same operation on divisors given by the Picard group. In particular, $E(\mathbb{Q}) = \{\text{rational points on the curve}\} \cup \{\infty\}$, then it has an abelian group structure. It turns out that it is always finitely generated, and

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus \mathcal{F},$$

and the finite part $\mathcal{F}$ is easily determined. Masur showed there are only 15 possibilities for $\mathcal{F}$. The rank r is very hard to compute. It is conjectured (wildly believed) that r may take any nonnegative integer values. However, there are only known examples through $r = 18$, and then also $r = 28$. If r is very large, there should be many rational solutions modulo p. This also implies many solutions over $\mathbb{F}_p$. Even $\frac{\#(E(\mathbb{F}_p))}{p}$ should be large, so that

$$\prod_{p \le x} \frac{\#(E(\mathbb{F}_p))}{p}$$

should be large. In the 1960s, B-S-D noticed that the product

$$\prod_{p \le x} \frac{\#(E(\mathbb{F}_p))}{p} \sim C(\log x)^r$$

through numerical calculations. This is unkown whether this is true. Letting

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

we define

$$L(s,E) = \prod_p \left(1 - \frac{a_E(p)}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}.$$

Note that this is normalized so that $s \mapsto 2-s$ yields a functional equation.

Now we apply the numerical calculation to get

$$\prod_{p \le x} \frac{p+1-a_E(p)}{p} \sim C(\log x)^r,$$

or

$$\prod_{p \le x}\left(1 - \frac{a_E(p)}{p} + \frac{1}{p}\right) \sim C(\log x)^r, \text{ or}$$

$$\prod_{p \le x} L_p(1,E) \sim C(\log x)^r$$

This implies (using a Tauberian argument)

$$\mathrm{ord}_{s=1} L(s,E) = r.$$

This is conjectured but not known. The BSD conjecture is that

$$L(s,E) = (*)(s-1)^r + O(|s-1|^{r+1}),$$

where $(*)$ is explicit. The (Tate-)Shafarevich group measures the failure of the local-global principle. The cardinality of this group is a factor of $(*)$. The analytic continuation of $L(s,E)$ was proved by Wiles et. al., from his proof of the Taniyama-Shimura Conjecture in 1995. If $r = 0, 1$ the conjecture is known. For other Shimura varieties, we can ask the same (harder) question.

Riemann Hypothesis

In 1859, Riemann published his only paper on number theory. The **Riemann hypothesis** states that all the nontrivial zeros of $\zeta(s)$ lie on the critical line $Re(s) = \frac{1}{2}$. This implies the Lindelöf hypothesis, the best rate of growth for primes, etc. This has been verified for the zeros s with $|\mathrm{Im}(s)| < 10000000000000$. People have shown that at least 40% of the zeros are on the critical line. Also we can show that there are no zeros $\sigma + it$ for with $\sigma > 1 - \frac{c}{(\log t)^{3/5}}$. One application of the RH is the distribution formula for prime numbers. That is, if

$$\sum_{n \le x} \Lambda(n) = x - \sum_{p \text{ prime}} \frac{x^p}{p} - \log(2\pi) - \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right)$$

as $x \to \infty$, where

$$\Lambda(n) = \begin{cases} \log p & n = p^m,\ p \text{ prime} \\ 0 & \text{otherwise} \end{cases}.$$

The RH implies

$$\sum_{n \le x} \Lambda(n) = x + O(x^{1/2+\varepsilon}).$$

(People have been able to show $O\left(xe^{-c(\log(x))^{3/5}}\right)$.)