LECTURE 23: ZETA FUNCTIONS OF CURVES

LARRY ROLEN, VANDERBILT UNIVERSITY, FALL 2020

> Der Baron (Zeta) gab heute sein Bestes, Wir bringen ihm ein dreifach Hoch! (Zeta gave his best today, so we give him a triple toast!))
>
> From Lehar's "The Merry Widow"

We have seen the Riemann zeta function and L-functions attached to modular forms. These are L-functions attached to analytic objects. We now wish to describe L-functions attached to geometric ones.

Given a sequence $N_1, N_2, \ldots$, we define the associated **zeta function transform** as

$$Z(T) := e^{\sum_{r\geq 1} N_r T^r/r.}$$

Here, the exponential is *formal*, namely, the exponential of a formal power series $f(T)$ is

$$e^{f(T)} := \sum_{k\geq 0} \frac{f(T)^k}{k!}.$$

Now for the geometry. An (affine) **variety over a field** K in n-dimensions is the solution set to a finite list of polynomial equations $f_j(x_1, \ldots, x_n) = 0$. A projective variety is a zero set of a system of homogenous polynomials $f_j(x_1, \ldots, x_{n+1})$ over projective space $\mathbb{P}^n_K$.

Suppose that V is an (affine or projective) variety over a finite field $\mathbb{F}_q$ with $q = p^n$. Then consider the sequence $N_r := \#V(\mathbb{F}_{q^r})$, that is, the number of points on the variety over finite field extensions. The **congruence zeta function** is then

$$Z(F/\mathbb{F}_q; T) := e^{\sum_{r\geq 1} \#V(\mathbb{F}_{q^r})T^r/r}.$$

For instance, $Z(V/\mathbb{F}_p; T)$ "knows" about the number of points on the variety over all finite fields of characteristic p.

Example. *Let $N_1 = N_2 = \ldots = 1$. This arises geometrically by letting V be the variety consisting of a single point. For example, let $V = \{0\}$ be the set of solutions to the one-variable polynomial $x = 0$. Then*

$$Z(T) = e^{\sum_{r\geq 1} T^r/r} = e^{-\log(1-T)} = \frac{1}{1-T}.$$

Example. *Let V be the projective line over $\mathbb{F}_q$. Then over $\mathbb{F}_{q^r}$, there are $q^r + 1$ points (one point at infinity). That is, $N_r = q^r + 1$. Then*

$$\sum_{r\geq 1} \frac{T^r}{r} N_r = \sum_{r\geq 1} \frac{(qT)^r}{r} + \sum_{r\geq 1} \frac{T^r}{r} = -\log(1-qT) - \log(1-T).$$

Thus, the zeta function is

$$Z(T) = \frac{1}{(1-T)(1-qT)}.$$

Example. *Let V be an elliptic curve E. Then it turns out that*

$$Z(E/\mathbb{F}_q;T) = \frac{1-2a_ET+qT^2}{(1-T)(1-qT)},$$

where $a_E \in \mathbb{C}$. Assuming this fact, let's recover N_r to see what this is really saying.

Factoring

$$(1-2a_ET+qT^2) = (1-\alpha T)\left(1-\frac{q}{\alpha}T\right),$$

and taking log derivatives, we find that the point counts N_r are given by

$$N_r = q^r + 1 - \alpha^r - \left(\frac{q}{\alpha}\right)^r.$$

Then

$$N_1 = \#E(\mathbb{F}_q) = q+1-\alpha-\frac{q}{\alpha} = q+1-2a_E.$$

Thus, the above expression for the zeta function is really

$$V(E/\mathbb{F}_q;T) = \frac{1+(\#E(\mathbb{F}_q)-q-1)+qT^2}{(1-T)(1-qT)}.$$

This last example is a basic instance of the **Weil Conjectures**, which are now a theorem of Deligne. Let's describe these in the case of curves.

Conjecture 1 (Weil Conjectures for Curves, Theorem of Deligne)**.** *Let V be a smooth projective curve. Then the following are true.*

(1) *The zeta function $Z(V/\mathbb{F}_q;T)$ is a rational function of the form*

$$\frac{P(T)}{(1-T)(1-qT)},$$

where $P(T) \in \mathbb{Z}[T]$ has constant term 1.

(2) *If V is the reduction mod p of a variety of genus g over $\mathbb{Q}$, then $\deg(P) = 2g$.*

(3) *If α is a reciprocal root of the numerator, then so is q/α.*

(4) *We have the following* **Riemann Hypothesis for curves***: All reciprocal roots of of the numerator have absolute value $\sqrt{q}$.*

We will **prove this in the special case** of the congruent number curves $E_n\colon y^2 = x^3 - n^2x$. This proof is not completely special to E_n, but what's really going on is that these curves have **complex multiplication**, a theory we'll discuss more later.

So we need to compute the number of points of E_n over finite fields. To do this, the first helpful step is to *diagonalize*. Assume that $p \nmid 2n$, that is, that p is of good reduction (recall: this means the reduction mod p is still an elliptic curve). Then we'll relate points between the two curves

$$E_n \leftrightarrow E_n',$$

where $E_n'\colon u^2 = v^4 + 4n^2$. This correspondence works as follows. To map from $E_n' \to E_n$, send

$$(u, v) \mapsto \left(\frac{1}{2}(u + v^2), \frac{1}{2}v(u + v^2)\right).$$

Then by basic algebra we check that

$$\left(\frac{1}{2}v(u + v^2)\right)^2 - \left(\frac{1}{2}(u + v^2)\right)^3 + n^2 \cdot \frac{1}{2} \cdot (u + v^2) = 0,$$

so that the image is indeed on E_n.

In the reverse direction, let $(x, y) \in E_n$ with $x \neq 0$. Then

$$(u, v) = \left(2x - \frac{y^2}{x^2}, \frac{y}{x}\right) \in E_n.$$

This is thus a bijection

$$E_n'(\mathbb{F}_q) \leftrightarrow E_n(\mathbb{F}_q) \setminus \{0, 0\}.$$

Thus, its sufficient to count $\mathbb{F}_q$ solutions to E_n', call the number of points N'. Then $N_1 = \#E_n(\mathbb{F}_q) = N' + 2$ (there is a point at infinity as well as the one point missed in the above bijection).

Counting points over finite fields on diagonal hypersurfaces (hypersurfaces are things of codimension 1) can be done using Gauss and Jacobi sums. To set these up, we first discuss characters. A **multiplicative character** is a homomorphism $\chi\colon \mathbb{F}_q^\times \to \mathbb{C}^\times$. An **additive character** is a homomorphism $\psi\colon \mathbb{F}_q \to \mathbb{C}^\times$ where the domain is the additive group of the field. We'll consider the character

$$\psi(x) = \zeta^{\mathrm{Tr}(x)},$$

where $\zeta = e(1/p)$ is a primitive p-th order root of unity and Tr is the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$ (the sum of Galois conjugates $x + x^p + \ldots + x^{p^{n-1}}$). This gives a non-trivial additive character, which we'll fix.

Assuming the notation above, we define the **Gauss sum**

$$g(\chi) := \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x).$$

We don't have to consider the value at 0 as $\chi(0) = 0$ for all characters even the trivial one χ_{triv}. We also need the **Jacobi sum** of two multiplicative characters

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(1 - x).$$

We list some of the classical properties of these character sums.

Proposition. *Let χ denote a non-trivial character, and let $\overline{\chi}$ be the conjugate character such that $\overline{\chi}(x) = \overline{\chi(x)}$. Then the following hold.*

(1) *We have* $g(\chi_{\text{triv}}) = -1$ *and* $J(\chi_{\text{triv}}, \chi_{\text{triv}}) = q - 2$. *Further,* $J(\chi_{\text{triv}}, \chi) = -1$, $J(\chi, \overline{\chi}) = -\chi(-1)$, *and* $J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$.
(2) *We have the product formula* $g(\chi)g(\overline{\chi}) = \chi(-1)q$ *and* $|g(\chi)| = \sqrt{q}$.
(3) *If* $\chi_2 \neq \overline{\chi_1}$, *then*

$$J(\chi_1, \chi_2) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)}.$$

We now return to computing N'. The key step now we have diagonalized our curve is based on the following.

Exercise 1. *Show that if* $a \in \mathbb{F}_q^\times$ *with* $m|(q-1)$, *then*

$$\#\{x \in \mathbb{F}_q | x^m = a\} = \sum_{\chi^m = 1} \chi(a).$$

That is, the number of solutions over $\mathbb{F}_q$ *to* $x^m = a$ *is the sum of values at* a *of multiplicative characters whose* m*-th power is the trivial character. Both sides are* m *if* a *is an* m*-th power, and are* 0 *otherwise.*

We've already shown that $N_1 = q + 1$ if $q \equiv 3 \pmod 4$ a long time ago. So let's assume $q \equiv 1 \pmod 4$. Then we break up our point count into the sum of solutions to the equations where $v = 0$, where $u = 0$, and then where neither u nor v is 0:

$$N' = \#\{u \in \mathbb{F}_q | u^2 = 4n^2\} + \#\{v \in \mathbb{F}_q | 0 = v^4 + 4n^2\} + \#\{u, v \in \mathbb{F}_q^\times | u^2 = v^4 + 4n^2\} =: N_1' + N_2' + N_3'.$$

Since $p \nmid 2n$, we immediately see that $N_1' = 2$. The number N_2' can be computed using the exercise. When is $-4n^2$ a $4 - th$ power? To use the exercise, we consider the characters of order dividing 4. Since $\mathbb{F}_q^\times$ is cyclic, say we choose $\mathbb{F}_q^\times = \langle g \rangle$, we get one character of order 4 by choosing $\chi_4(g) = i$. This is a character of order 4, and the characters of order dividing 4 are just the powers of this. Thus, using the exercise and the fact that $-4n^2$ is a square in $\mathbb{F}_q$ since $q \equiv 1 \pmod 4$,

$$N_2' = \sum_{j=1}^{4} \chi_4^j(-4n^2) = 2 + 2\chi_4(-4n^2).$$

Now we evaluate N_3'. Take $\chi_2 := \chi_4^2$, a character of order 2. Then the exercise implies that

$$N_3' = \sum_{\substack{a,b \in \mathbb{F}_q^\times \\ a = b + 4n^2}} \#\{u^2 = a\} \cdot \#\{v^4 = b\}$$

$$= \sum_{\substack{a \in \mathbb{F}_q^\times \\ a - 4n^2 \neq 0}} \sum_{\substack{j=1,2,3,4 \\ k=1,2}} \chi_2^k(a)\chi_4^j(a - 4n^2).$$

Using our assumption that $\chi_4(a-4n^2)=0$ if $a-4n^2=0$, we can delete the bottom condition on the first sum. We then change variables to $x=a/4n^2$ and reverse the order of summation to obtain

$$\sum_{\substack{j=1,2,3,4\\k=1,2}} \chi_4^j(-4n^2)\sum_{x\in\mathbb{F}_q^\times}\chi_2^k(x)\chi_4^j(1-x)=\sum_{\substack{j=1,2,3,4\\k=1,2}}\chi_4^j(-4n^2)J(\chi_2^k,\chi_4^j).$$

Combining all three pieces together gives

$$N'=4+2\chi_4(-4n^2)+\sum_{j=1,3}\chi_4^j(-4n^2)J(\chi_2,\chi_4^j)+q-2+3\cdot(-1)+2\chi_4(-4n^2)\cdot(-1).$$

Here, the first two summands on the right hand side were $N_1'+N_2'$, the sum with $j=1,3$ are the terms from N_3' with $k=1$, $j=1,3$, and the rest of the terms were simplified by using the properties above for Jacobi sums when one of the characters is trivial or conjugate to the other. Simplifying further, this becomes

$$q-1+\chi_4(-4n^2)\left(J(\chi_2,\chi_4)+J(\chi_2,\overline{\chi_4})\right).$$

We need one additional small fact.

Exercise 2. *Show that* $\chi_4(-4)=1$.

This implies that $\chi_4(-4n^2)=\chi_2(n)$. Thus, recalling that $N_1=N'+2$,

$$N_1=q-1+\chi_2(n)\left(J(\chi_2,\chi_4)+\overline{J(\chi_2,\chi_4)}\right),$$

where we used $\chi_2=\overline{\chi_2}$ since χ_2 is real. The above properties then show that

$$N_1=q+1-\alpha-\overline{\alpha},$$

where

$$\alpha=-\chi_2(n)J(\chi_2,\chi_4)=-\chi_2(n)\frac{g(\chi_2)g(\chi_4)}{g(\chi_2\chi_4)}=-\chi_2(n)\frac{g(\chi_2)g(\chi_4)}{g(\overline{\chi_4})}.$$

By the properties Gauss sums above, we find that

$$|\alpha|^2=q,$$

which is where the "Riemann Hypothesis" in this case comes from. Its also useful for finding α. To determine it exactly, note that α is a **Gaussian integer**, that is, in $\mathbb{Z}[i]$, since the values of χ_2,χ_4 all are. So let's say $\alpha=a+bi$ with $a,b\in\mathbb{Z}$, with $a^2+b^2=q$. We say that α is a Gaussian integer with **norm** q.

There are not many Gaussian integers satisfying this. We will focus on the cases when q is a prime or a square of a prime. If $q=p\equiv 1 \pmod 4$, then there are 8 choices with this same absolute value:

$$\alpha=\pm a\pm bi,\pm b\pm ai.$$

If $q=p^2$ with $p\equiv 3 \pmod 4$ prime, then there are even fewer choices:

$$\alpha=\pm p,\pm pi.$$

The exact choice here can be determined with the following additional information:
Claim: We have that $1 + J(\chi_2, \chi_4)$ is divisible by $2 + 2i$ in $\mathbb{Z}[i]$.

Proof. By the property 3 in the Proposition above, applied to both $J(\chi_2, \chi_4)$ and $J(\chi_4, \chi_4)$, we find that

$$J(\chi_2, \chi_4) = J(\chi_4, \chi_4)\frac{g^2(\chi_2)}{g(\chi_4)g(\overline{\chi_4})} = \chi_4(-1)J(\chi_4, \chi_4).$$

Now

$$J(\chi_4, \chi_4) = \sum \chi_4(x)\chi_4(1-x) = \chi_4^2\left(\frac{q+1}{2}\right) + 2\sum{}'\chi_4(x)\chi_4(1-x),$$

where $\sum'$ denotes a sum over $(q-3)/2$ elements, one from each pair $(x, 1-x)$ with the pair $(\frac{q+1}{2}, \frac{q+1}{2})$ pulled out front. Now $\chi_4(x)$ is a power of i, so $\chi_4(x) = i^m \equiv 1 \pmod{1+i}$. To see that, note that $(1+i)(1-i) = 1+1 = 2 \equiv 0$, so $1 \equiv -1$ and hence $i \equiv -1 \equiv 1$. Thus,

$$2\chi_4(x)\chi_4(1-x) \equiv 2 \pmod{2+2i},$$

and so

$$J(\chi_4, \chi_4) = q - 3 + \chi_4^2\left(\frac{q+1}{2}\right) \equiv 2 + \chi_4(4) \pmod{2+2i}$$

as $q \equiv 1 \pmod 4$. Thus,

$$1 + J(\chi_2, \chi_4) = 1 + \chi_4(-1)J(\chi_4, \chi_4) \equiv 1 + \chi_4(-4) + 2\chi_4(-1) \pmod{2+2i}.$$

We saw above that $\chi_4(-4) = 1$, and

$$2(1 + \chi_4(-1)) \in \{0, 4\},$$

so the claimed divisibility follows. □

Thus, all of this work and our previous result on point counts when $p \equiv 3 \pmod 4$ has shown the following special case of the Weil Conjectures:

Theorem. *If p is a prime of good reduction, then the zeta function for E_n factors as*

$$Z(E_n/\mathbb{F}_p; T) = \frac{(1-\alpha T))(1-\overline{\alpha}T)}{(1-T)(1-pT)}.$$

Moreover, $\alpha = i\sqrt{p}$ if $p \equiv 3 \pmod 4$, and α is an element of $\mathbb{Z}[i]$ of norm p which is congruent to the Legendre symbol $\left(\frac{n}{p}\right)$ modulo $2+2i$ if $p \equiv 1 \pmod 4$.

Remark. *If $p \equiv 1 \pmod 4$, this explicitly means that we choose $\alpha = a + bi$ with a odd, b even, and where the sign of a is determined by the congruence. The choice between $a + bi$ and $a - bi$ doesn't change the formula, but just reverses the roles of α and $\overline{\alpha}$.*

Proof. We need N_r for $p \equiv 1 \pmod 4$ and N_{2r} for $p \equiv 3 \pmod 4$ (as we know all odd r values N_r when $p \equiv 3 \pmod 4$ already). We consider $q = p$ if $p \equiv 1 \pmod 4$ and $q = p^2$ if $p \equiv 3 \pmod 4$, and have to see what happens when we replace q by q^r. Let $\chi_{2,1}$ be the unique character of order 2 over $\mathbb{F}_q^\times$, and let $\chi_{4,1}$ be a choice of a character of order 4 (the two possibilities are complex conjugates of one another). Composing with the **norm map** $\mathbb{F}_{q^r} \to \mathbb{F}_q$ (the norm of an element g is the product of its Galois conjugates, namely $g^{1+q+\ldots+q^{r-1}}$) gives characters of order $2, 4$ over $\mathbb{F}_{q^r}^\times$. Call them $\chi_{2,r}$ and $\chi_{4,r}$. Call this norm map $\mathbb{N}_r$, so

$$\chi_{4,r} = \chi_4 \circ \mathbb{N}_r, \qquad \chi_{2,r} = \chi_2 \circ \mathbb{N}_r.$$

From the work above,

$$\#E_n(\mathbb{F}_{q^r}) = q^r + 1 - \alpha_{n,q^r} - \overline{\alpha_{n,q^r}},$$

where

$$\alpha_{n,q^r} = -\chi_{2,r}(n)\frac{g(\chi_{2,r})g(\chi_{4,r})}{g(\overline{\chi_{4,r}})}.$$

We now need the **Hasse-Davenport formula**, which describes how Gauss sums change over extensions:

$$-g(\chi \circ N_r) = (-g(\chi))^r.$$

Using this, and $\chi_{2,r}(n) = \chi_2(n^r) = \chi_2^r(n)$, we obtain

$$\alpha_{n,q^r} = \alpha_{n,q}^r.$$

Now if $q = p \equiv 1 \pmod 4$, then $\chi_2(n) = \left(\frac{n}{p}\right)$ by uniqueness of a character of order 2. By the above, $\alpha = \alpha_{n,p}$ is a Gaussian integer of norm p congruent to $\left(\frac{n}{p}\right)$ modulo $2+2i$, and by the above

$$N_r = p^r + 1 - \alpha^r - \overline{\alpha}^r.$$

Writing this out in the original generating function definition proves the theorem.

If $p \equiv 3 \pmod 4$ and $q = p^2$, then $\chi_2(n) = 1$ as all elements of $\mathbb{F}_p$ are squares in $\mathbb{F}_{p^2}$. By the same calculations as above, $\alpha_{n,q}$ is a Gaussian integer of norm q congruent to $1 \pmod{2+2i}$. There are 4 Gaussian integers of norm q, namely $i^j p$ for $j = 0, 1, 2, 3$. Only $\alpha_{n,q} = -p$ satisfies the congruence. Hence,

$$N_r = \#E_n(\mathbb{F}_{q^{\frac{r}{2}}}) = p^r + 1 - (-p)^{\frac{r}{2}} - (-p)^{\frac{r}{2}}.$$

As $N_r = p^r + 1$ for odd r, for any r we have

$$N_r = p^r + 1 - (i\sqrt{p})^r - (-i\sqrt{p})^r.$$

This finishes the proof. □

Next time, we will see how to connect the congruence zeta functions for different primes together to obtain the **L-function for the elliptic curve**.