Lecture 16.1

Applications of L-functions

We saw how useful L-functions are for proving things about prime numbers, such as Dirichlet's Theorem.

Today, I want to show you a few of their many other applications.

Consider the series

$$F(s) = \sum_{\substack{(x,y)\in\mathbb{Z}^2 \\ (x,y)\neq 0}} \frac{1}{(x^2+y^2)^s}.$$

The terms $\frac{1}{(x^2+y^2)^s}$ are exactly those $\frac{1}{n^s}$ for

which $n = x^2 + y^2$ for <u>some</u> $x, y \in \mathbb{Z}$,

but there are duplicates (e.g. $(\pm x, \pm y)$).

Let's define an arithmetic function

$$r(n) = \#\{(x,y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n\}$$

$$= \#\text{ of ways of writing } n \text{ as a sum of two squares.}$$

Then automatically, $F(s)$ is a Dirichlet series

$$F(s) = \sum_{\substack{(x,y) \in \mathbb{Z}^2 \\ (x,y) \neq (0,0)}} \frac{1}{(x^2+y^2)^s} = \sum_{n=1}^{\infty} \frac{r(n)}{n^s}.$$

We know from our sum of squares theorem (Lecture 10.2) that $r(n) = 0$ if and

only if $n = d^2 2^k p_1 \cdots p_r$ where $p_j \equiv 1 \pmod 4$.

Moreover, by the identity

$$(x^2+y^2)(z^2+w^2) = (xz+yw)^2 + (xw-yz)^2$$

we know that $\frac{r(n)}{4}$ is a multiplicative function.

↖ adjusting for $(\pm x, \pm y)$

By HW9, Problem 2, $\frac{1}{4}F(s)$ has a product formula:

$$\frac{1}{4}F(s) = \sum_{n=1}^{\infty} \frac{r(n)}{n^s}$$

$$= \prod_p \sum_{k=0}^{\infty} r(p^k) p^{-sk}$$

$$r(p^k) = \begin{cases} k+1, & p \equiv 1 \pmod 4 \\ 0, & p \equiv 3 \pmod 4 \text{ and } k \text{ odd} \\ 1, & p \equiv 3 \pmod 4 \text{ and } k \text{ even} \end{cases}$$

$$= \left(\sum_{k=0}^{\infty} 2^{-sk}\right)\left(\prod_{p\equiv 1\,(4)} \sum_{k=0}^{\infty} (k+1)p^{-sk}\right)\left(\prod_{p\equiv 3\,(4)} \sum_{k=0}^{\infty} p^{-2sk}\right)$$

$$= \left(\frac{1}{1-2^{-s}}\right)\left(\prod_{p\equiv 1\,(4)} \frac{1}{(1-p^{-s})^2}\right)\left(\prod_{p\equiv 3\,(4)} \frac{1}{1-p^{-2s}}\right)$$

$$(1-p^{-s})(1-p^{-s}) \qquad\qquad (1-p^{-s})(1+p^{-s})$$

$$= \left(\prod_{p} \frac{1}{1-p^{-s}}\right)\left(\prod_{p\equiv 1\,(4)} \frac{1}{1-p^{-s}}\right)\left(\prod_{p\equiv 3\,(4)} \frac{1}{1+p^{-s}}\right)$$

$$= \zeta(s) \prod_{p} \frac{1}{1-\chi(p)p^{-s}}$$

where $\chi(p) = \begin{cases} 1, & p \equiv 1 \ (4) \\ -1, & p \equiv 3 \ (4). \end{cases}$

Do we know any function like that?

Yes! $\chi(p) = \left(\frac{-1}{p}\right)$!!

Extending to all $n = 2^{k_0} p^{k_1} \cdots {}^{k_r}$ …

Extending to all $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$ by

$$\chi(n) = \left(\frac{-1}{p_1}\right)^{k_1} \cdots \left(\frac{-1}{p_r}\right)^{k_r}$$

we get a completely multiplicative function

$\chi(n) = \left(\frac{-1}{n}\right)$ with Dirichlet series

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)p^{-s}}.$$

Lemma χ is the unique nontrivial character mod 4.

Pf: There are only $\phi(4) = 2$ characters mod 4 and $\chi \neq \chi_0$ since for example

$\chi(3) = -1 \neq 1 = \chi_0(3)$.

It's routine to check that χ is a character. □

Exercise 1: Check that χ is a character mod 4.

Corollary $F(s) = \sum_{n=1}^{\infty} \frac{r(n)}{n^s} = 4\zeta(s)L(\chi, s)$

where $\chi(n) = \left(\frac{-1}{n}\right)$.

We can prove this in an alternate way.

Here's a useful fact:

Prop $r(n) = 4 \sum_{d \mid n} \chi(d)$ where $\chi = \left(\frac{-1}{\cdot}\right)$.

Pf: Let $f(n) = 4 \sum_{d \mid n} \chi(n)$.

For any distinct primes p, q,

$$f(pq) = 4\left(\chi(1) + \chi(p) + \chi(q) + \chi(pq)\right)$$

$$= 4\left(\chi(1) + \chi(p) + \chi(q) + \chi(p)\chi(q)\right)$$

$$= \begin{cases} 4(1+1+1+1) = 16, & p, q \equiv 1 \pmod 4 \\ 4(1+1-1-1) = 0, & p \equiv 1, q \equiv 3 \pmod 4 \\ 4(1-1+1-1) = 0, & p \equiv 3, q \equiv 1 \pmod 4 \\ 4(1-1-1+1) = 0, & p, q \equiv 3 \pmod 4 \end{cases}$$

$$= f(p) f(q).$$

So f is multiplicative.

On the other hand,

$$f(p^k) = \sum_{j=0}^{k} \chi(p^j) = \sum_{j=0}^{k} \chi(p)^j$$

$$= \begin{cases} \sum_{j=0}^{k} 1, & p \equiv 1 \pmod 4 \\ \sum_{j=0}^{k} (-1)^j, & p \equiv 3 \pmod 4 \end{cases}$$

$$= \begin{cases} k+1, & p \equiv 1 \pmod 4 \\ 0, & p \equiv 3 \pmod 4,\ k \text{ odd} \\ 1, & p \equiv 3 \pmod 4,\ k \text{ even}. \end{cases}$$

(similar for $f(2^k)$)

So $f(n)$ and $r(n)$ are multiplicative

and their values on p^k match. Therefore they are equal. □

Corollary $F(s) = \sum_{n=1}^{\infty} \frac{r(n)}{n^s} = 4\,\beta(s)\,L(\chi,s).$

Pf: We have

$$4\,\beta(s)\,L(\chi,s) = \left(\sum_{n=1}^{\infty} \frac{4}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}\right)$$

$$= \sum_{n=1}^{\infty} \frac{\sum_{d\mid n} 4\cdot\chi(d)}{n^s}$$

$$= \sum_{n=1}^{\infty} \frac{r(n)}{n^s} \quad \text{by the lemma.} \quad \square$$

The character $\left(\frac{-1}{\cdot}\right)$ describes one of our laws

of quadratic reciprocity; what can L-functions

say about $\left(\frac{a}{p}\right)$?

For $a \in \mathbb{Z}$, set $\chi_a = \left(\frac{a}{\cdot}\right)$.

Then by definition, χ_a is completely multiplicative,

so its Dirichlet series has a product

formula:

$$L(\chi_a, s) = \sum_{n=1}^{\infty} \frac{\chi_a(n)}{n^s} = \prod_p \frac{1}{1-\left(\frac{a}{p}\right)p^{-s}}.$$

Consider the product

$$\zeta_a(s) = \zeta(s) L(\chi_a, s).$$

Theorem For any $a \neq -1$, $\zeta_a(s)$ has a

product formula

$$\zeta_a(s) = \left(\prod_{p \text{ la}} \frac{1}{1-p^{-s}}\right)\left(\prod_{\substack{a=QR \\ mod\, p}} \frac{1}{(1-p^{-s})^2}\right)\left(\prod_{\substack{a=NR \\ mod\, p}} \frac{1}{1-p^{-2s}}\right).$$

Pf: Quadratic reciprocity. □

Exercise 2: Check the details carefully.

In fact, both formulas

$$\zeta_{-1}(s) = \sum_{\substack{(x,y)\in\mathbb{Z}^2 \\ (x,y)\neq(0,0)}} \frac{1}{x^2+y^2} = 4\zeta(s)L(\chi_{-1},s)$$

and $\zeta_a(s) = \zeta(s)L(\chi_a,s)$

can be proven <u>without</u> quadratic reciprocity, using algebraic number theory.

They can then be used to prove quadratic reciprocity again:

Take distinct primes p and q and set

$$a = (-1)^{\frac{q-1}{2}} p.$$

Then $\zeta_a(s) = \zeta(s) L(\chi_a, s)$ so they must have the same terms.

It can be shown that

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

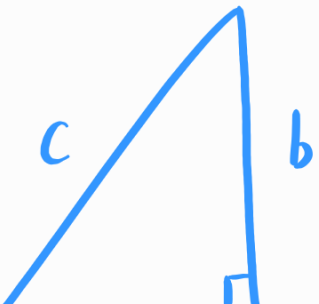
$$\left(\varphi_a(s) = \sum_{n=1}^{\infty} \frac{f_a(n)}{n^s} \quad \text{where} \quad f_a(n) = \sum_{d \mid n} \left(\frac{d}{a}\right) \right)$$

so by matching up p^{-s} terms, we get

$$\left(\frac{p}{q}\right) p^{-s} = \left(\frac{a}{p}\right) p^{-s} = \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) p^{-s}$$

which is equivalent to quadratic reciprocity.

Bonus application: a number $n \in \mathbb{N}$ is a **congruent number** if n is the area of a rational right triangle:



a

$a^2 + b^2 = c^2$, $ab = 2n$ and $a, b, c \in \mathbb{Q}$.

It turns out that there is a solution to

$$\begin{cases} a^2 + b^2 = c^2 \\ ab = 2n \end{cases}$$

if and only if there is a solution to

$$E_n : y^2 = x^3 - n^2 x.$$

This equation traces out a curve in $\mathbb{R}^2$ called an elliptic curve and there's an L-function attached to it,

$$L(E_n, s) = \prod_p L_p(E_n, s)$$

where

$$L_p(E_n, s) = \frac{1}{1 - a_p(n)p^{-s} + p^{1-2s}}$$

$$a_p(n) = 1 + p - \#\left\{x, y \in \mathbb{Z}/p\mathbb{Z} \mid y^2 \equiv x^3 - n^2 x \pmod{p}\right\}.$$

(for almost all p; there's a more complicated formula for finitely many p!)

A deep conjecture called the Birch and Swinnerton-Dyer Conjecture implies certain properties of $L(E_n, s)$ which, among other things, indicates when n is a congruent number:

Conjecture There are infinitely many rational points on E_n if and only if

$$L(E_n, 1) = 0.$$

But having infinitely many rational points on E_n guarantees that n is a congruent number — in fact, these conditions are equivalent too.

Fortunately, the Conjecture is known for many elliptic curves. Solving it in general is a major goal of arithmetic geometry.