A course in
Analytic Number Theory

Taught by Barry Mazur

Spring 2012

Last updated: January 19, 2014

Contents

1. January 24

1.1. Arithmetic functions and first example. An arithmetic function is a function $\mathbb{N} \to \mathbb{C}$, which we will denote $n \mapsto c(n)$. For example, let $r_{k,d}(n)$ be the number of ways n can be expressed as a sum of d k^{th} powers. Waring's problem asks what this looks like asymptotically. For example, we know $r_{3,2}(1729) = 2$ (Ramanujan). Our aim is to derive statistics for (interesting) arithmetic functions via a study of the analytic properties of generating functions that package them. Here is a generating function:

$$F_c(q) = \sum_{n=1}^{\infty} c(n)q^n$$

(You can think of this as a Fourier series, where $q = e^{2\pi iz}$.) You can retrieve $c(n)$ as a Cauchy residue:

$$c(n) = \frac{1}{2\pi i} \oint \frac{F_c(q)}{q^n} \cdot \frac{dq}{q}$$

This is the Hardy-Littlewood method. We can understand Waring's problem by defining

$$f_k(q) = \sum_{n=1}^{\infty} q^{n^k}$$

(the generating function for the sequence that tells you if n is a perfect k^{th} power). Then $f_k^d(q)$ is the generating function of the thing we want:

$$\left(\sum q^{n^k}\right)^d = f_k^d = \sum r_{k,d}(n)q^n$$

Take the case when $k = 1$; you get a geometric series. If $k = 2$, then

$$f_2(q) = \prod (1 - q^{2m})(1 + q^{2m-1})(1 - q^{2m+1})$$

by a theorem of Jacobi.

Another example is the partition function: $p(n)$ is the number of ways that n can be expressed as a sum of positive integers:

$$\sum_{n=1}^{\infty} p(n)q^n = \prod_{m=1}^{\infty} \frac{1}{1 - q^m}$$

A third example is

$$\omega(q) = q \cdot \prod (1 - q^m)^2(1 - q^{11m})^2 = \sum a(n)q^n$$

If $n \neq 11$ is a prime, then $a(p) = 1 + p - |E(\mathbb{F}_p)|$ where $E = y^2 + y = x^3 - x^2$ (here $|E(\mathbb{F}_p)|$ is the number of points on the curve with values in $\mathbb{F}_p$). When you replace $q = e^{2\pi iz}$ there's a symmetry where you can replace $z \mapsto \frac{-1}{11z}$.

1.2. Formal Dirichlet Series.

$$D_c(s) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s}$$

Suppose we have two arithmetic functions $n \mapsto a(n)$ and $n \mapsto b(n)$. Define a product $a * b = c$ where

$$c(n) = \sum_{d|n} a(d) b\left(\frac{n}{d}\right)$$

(Divisors are assumed always to be positive.) Why do we care? If you have Dirichlet series $D_a(s) = \sum \frac{a(n)}{n^s}$ and $D_b(s) = \sum \frac{b(n)}{n^s}$ then

$$D_{a*b} = \sum \frac{a * b(n)}{n^s} = D_a(s) D_b(s)$$

The star product is commutative, associative, and has the identity ε where

$$\varepsilon(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{else} \end{cases}$$

This is *not* the identity function $1 : n \mapsto 1$. The identity function is invertible, and the inverse is the Moebius function

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is not square-free} \\ (-1)^{\#\text{ of prime factors of } n} & \text{else} \end{cases}$$

Exercise: check that

$$\sum_{d|n} \mu(d) \cdot 1 = \varepsilon$$

so that

$$\sum \frac{\mu(n)}{n^s} \cdot \zeta(s) = 1 \ .$$

DEFINITION 1.1. An arithmetic function is called *multiplicative* if

$$c(u \cdot v) = c(u) \cdot c(v)$$

if $(u, v) = 1$. So

$$c(n) = \prod_{i=1}^{v} c(p_i^{k_i})$$

if $n = \prod_{i=1}^{v} p_i^{k_i}$.

Suppose $n \mapsto c(n)$ is multiplicative, and let p be prime. Let

$$D_{c,p}(s) = \sum_{m=0}^{\infty} \frac{c(p^m)}{p^{ms}}$$

$$D_c(s) = \sum \frac{c(n)}{n^s}$$

Formally

$$D_c(s) = \prod_{p} D_{c,p}(s) \tag{1.1}$$

BUT, even if $D_c(s)$ and $D_p(s)$ converge, you may not have the formula, because the product may not converge. If $\sum_{n=1}^{\infty} |c(n)n^{-s}|$ converges, then everything works.

$$\sum_{n=1}^{\infty} c(n) \cdot n^{-s} = \sum c(n)\frac{n^{-iy}}{n^x} = \sum c(n)\frac{e^{-log(n)iy}}{n^x}$$

If it converges at a point, then it converges at the entire vertical line through that point.

1.3. Riemann ζ function. Using the arithmetic function $n \mapsto 1$, then define

$$\zeta(s) = D_1(s) = \sum \frac{1}{n^s}$$

This converges absolutely if $Re(s) > 1$, by calculus.

There is an infinite product expansion

$$\sum \frac{1}{n^s} = \sum_{p\ prime} \frac{1}{1-\frac{1}{p^s}} = \prod_{p\ prime} (\sum_{m=0}^{\infty} p^{-ms})$$

(This is in the HW.)

Theorem 1.2.

$$\zeta(s)^{-1} = \sum \frac{\mu(n)}{n^s} = D_\mu(s)$$

PROOF.

$$D_\mu(s)\zeta(s) = D_\mu \cdot D_1 = D_\varepsilon = 1$$

□

This is analytically true when $Re(s) > 1$.

Basic reason for interest in $D_c(s)$ for any $c : n \mapsto c(n)$: If we know enough, we will be able to give very good estimates for $\sum_{p \le X} c(p) := \pi_c(X)$.

In particular, when $c = 1$, we get estimates for $\pi(X)$, the number of primes $\le X$.

Theorem 1.3 (Euler)**.** $\sum_{p \le X} \frac{1}{p}$ diverges as $X \to \infty$.

PROOF. Define $\lambda(X) = \prod_{p \le X}(1 - \frac{1}{p})^{-1}$. Write this as $\prod_{p \le X} \sum_{m=0}^{\infty} p^{-m}$. But

$$\sum_{n \le X} \frac{1}{n} \le \lambda(X)$$

because each $\frac{1}{n}$ is a term in the expansion of λ. But $\sum \frac{1}{n}$ diverges (which immediately proves that there are infinitely many primes). Take the log of the infinite product:

$$\log \lambda(X) = -\sum_{p \leq X} \log\left(1 - \tfrac{1}{p}\right)$$

But

$$\begin{aligned} -\log\left(1 - \tfrac{1}{p}\right) &= \frac{1}{p} + \frac{1}{2p^2} + \frac{1}{3p^3} + \cdots \\ &\leq \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots \\ &= \frac{1}{p} + \underbrace{\frac{1}{p^2} \cdot \frac{1}{1 - \frac{1}{p}}}_{\substack{\sum_{n \in \mathbb{N}^*} \\ \text{converges}}} \end{aligned}$$

for some c constant. So we have

$$\lim_{X \to \infty} \log \lambda(X) = \sum \frac{1}{p} + \text{ something convergent}$$

We showed above that $\lambda(X)$ goes to ∞, which means its log does too; if the LHS diverges, then so does the RHS. □

1.4. Arithmetic functions related to the ζ-function. a will be an arithmetic function, and let $A(n) = \sum_{d|n} a(d)$. Equivalently, $a = \mu * A$ so $a(n) = \sum \mu(d) A\left(\frac{n}{d}\right)$. In terms of Dirichlet series,

$$D_A(s) = \zeta(s) \cdot D(a)$$

Define A as the series where

$$n \mapsto \sigma_k(n) = \sum_{d|n} d^k$$

and $a : n \mapsto n^k$. Then

$$D_A(s) = \sum \frac{\sigma_k(n)}{n^s} = \zeta(s) D_a(s) = \zeta(s) \cdot \zeta(s-k)$$

$$D_a(s) = \sum \frac{n^k}{n^s} = \sum \frac{1}{n^{s-k}} = \zeta(s-k)$$

If $k = 0$ then define $\sigma_0(n) = \nu(n)$ which counts the number of divisors of n. Then

$$\sum \frac{\nu(n)}{n^s} = \zeta(s)^2$$

We call $a = \Phi$, the Euler Phi function; then $A(n) = \sum_{d|n} \Phi(d)$; you can check that $A(n) = n$.

$$D_\Phi(s) = \frac{\zeta(s-1)}{\zeta(s)}$$

Recall $r_{k,d}(n)$, the number of ways that n is expressible as a sum of d k^{th} powers, and recall that when $k = 2$ we had a nice formula for this. Let $R_{2,d}(n)$ be the number of ways

that n is expressible as the sum of d squares, *counting* $(+\alpha)^2$ *and* $(-\alpha)^2$ *as different, and including 0.* Also, *order matters here!* For example,

$$R_{2,24}(2) = 1104$$

Slightly more generally,

$$R_{2,24}(n) = \frac{16}{691}\sigma_{11}(n) + e(n)$$

where $e(n)$ is the error term: up to taking logs, it is $< \sqrt{\text{other term}}$. We have a complete description of the error term.

2. January 26

Define

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}$$

and recall

$$f_2 = \sum q^{n^2} \ .$$

It turns out that

$$\Delta \equiv f_2 \pmod 2 \ .$$

RECALL, a Dirichlet series is a formal expression that looks like $D(s) = \sum a(n)n^{-s}$. We also had arithmetic functions $n \mapsto a(n) \in \mathbb{C}$. L-functions will be a special case.

2.1. Some properties to learn about.

- **Domain of definition.** For example, $\zeta(s)$ doesn't make sense as a power series to the left of the line $Re(s) = 1$. However, there is a meromorphic continuation, with pole only at $s = 1$. (We have good control to the right of the line, but the most interesting information comes from the other half.) Also, there are symmetries: usually a relationship between $L(s)$ and $L(1-s)$ (i.e. you can sort of reflect across the line).
- **Poles and Zeroes.** One way (the only way) of understanding $\sum_{p\leq X} a(p)$ is to understand the poles and zeroes. In the case of $\zeta(s)$, this gives information about $\sum_{p\leq X} 1 = \pi(X)$, the number of primes $\leq X$. The Riemann hypothesis says that the zeroes of the ζ-function are at the negative even integers, on the line $Re(s) = \frac{1}{2}$, and nowhere else. If you're interested in statistics, consider $\sum w(p)a(p)$ (i.e. a weighted sum). A good thing to study is $\sum_{p\leq X}\log(p)$.
- **Special values of $L(s)$.** For example,

$$\zeta(1-2k) = \frac{(-1)^k B^{2k}}{2k} \ .$$

- **Estimating density of primes p where $a(p)$ has some property.** For example, there are asymptotically equal numbers of primes of the form $4n-1$ as of the form

$4n+1$. Also consider prime races: it turns out that $4n-1$ wins almost all the time. We will call this a Chebotarev-t question.

2.2. Wedge uniform convergence. Suppose you have a Dirichlet series $D(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ which we assume converges at some complex point s_0.

NOTATION 2.1. We will denote complex numbers as

$$s = \sigma + it$$

for $\sigma, t \in \mathbb{R}$.

Make any wedge in $\mathbb{C}$ with vertex s_0, pointing towards positive real infinity, where $c|t-t_0| < \sigma - \sigma_0$ for $c > 0$.

Theorem 2.2. $D(s)$ converges uniformly in any such wedge.

Define a remainder term

$$R(X) = \sum_{n>X} a(n)n^{-s_0}$$

Since everything converges, this goes to zero as $X \to \infty$. Check that

$$a(n) = (R(n-1) - R(n))n^{s_0}$$

so we can write

$$\begin{aligned}
\sum_{n=M+1}^{N} a(n)n^{-s} &= \sum_{M+1}^{N} (R(n-1) - R(n))n^{s_0-s} \\
&= \sum_{M+1}^{N} R(n-1)n^{s_0-s} - \sum_{M+1}^{N} R(n)n^{s_0-s} \\
&= R(M)(M+1)^{s_0-s} - R(N)\cdot N^{s_0-s} - \underbrace{\sum_{M+2}^{N} R(n-1)((n-1)^{s_0-s} - n^{s_0-s})}_{\mathcal{A}}
\end{aligned}$$

$$\begin{aligned}
\mathcal{A} &= -(s_0-s)\sum R(n-1)\int_{n-1}^{n} u^{s_0-s-1}du \\
&= -(s_0-s)\int_{M+1}^{N} R(u)u^{s_0-s-1}du
\end{aligned}$$

So in total this is

$$\sum_{M+1}^{N} a(n)n^{-s} = R(M)(M+1)^{s_0-s} - R(N)\cdot N^{s_0-s} + (s_0-s)\int_{M+1}^{N} R(u)u^{s_0-s-1}du \tag{2.1}$$

This gives an estimate (using the fact that $R(n)$ is supposed to be "small" for sufficiently large n):

$$\left|\sum_{M+1}^{N} a(n)n^{-s}\right| \leq \varepsilon + \varepsilon(s_0 - s)\int_{M+1}^{N} u^{s_0-s-1}du$$

when $u \geq M$ and $\sigma > \sigma_0$. As long as we have $|s_0 - s| < C(\sigma_0 - \sigma)$, the integral is bounded. If $|t_0 - t| < c(\sigma - \sigma_0)$, then by Cauchy's inequality we have $|s_0 - s| \leq |\sigma_0 - \sigma| + |t_0 - t|$ implies $|s_0 - s| < C|\sigma_0 - \sigma|$ as desired.

This show that $D(s)$ converges uniformly in any wedge with vertex s_0.

Corollary 2.3. If $D(s)$ is analytic in any s_0-wedge then $D(s)$ converges uniformly in any neighborhood of any point in this wedge.

Corollary 2.4. Differentiating term-by-term,

$$D'(s) = \sum_{n=1}^{\infty} -\log(n)a(n)n^{-s}$$

converges in the wedge.

Making the wedges larger and larger, we get

Corollary 2.5. If $D(s)$ converges at $s = s_0$, then it converges in the open half-plane of $Re(s) > Re(s_0) = \sigma_0$.

How far to the left does it converge? Either it converges everywhere, it converges nowhere, or it stops somewhere.

DEFINITION 2.6 (Abscissa of convergence of $D(s)$). The abscissa of convergence is a number $\sigma_c \in \mathbb{R} \cup \{\pm\infty\}$ such that $D(s)$ converges or not depending on whether $Re(s) > \sigma_c$ or $Re(s) < \sigma_c$. (In general, we don't have control over the line.)

Landau: if the series has positive real coefficients, then if σ_c is finite, it is a singularity of some sort.

2.3. Sums. It is much easier to estimate $A(X) := \sum_{n \leq X} a(n)$ than $\sum_{p \leq X} a(p)$. $A(X)$ is not differentiable, because it is a step function. So the derivative is a Dirac delta function, normalized by the coefficients $a(n)$. If you want to understand $\int f(X)dA(X)$, this is not a classical Riemann integral. The mess above is basically a hands-on integration by parts. Integrals of this form are called Riemann-Stieltjes integrals. (Read appendix A in the book.)

$$\sum_{1}^{N} a(n)n^{-s} = \int_{1-}^{N+} x^{-s}dA(x)$$

(The 1- and $N+$ refer to starting a little before and ending a little after the point, respectively; this is necessary because we are adding up Dirac deltas.)

$$\sum_1^N a(n)n^{-s} = \int_{1-}^{N+} x^{-s}dA(x)$$

$$= A(x)x^{-s}|_{1-}^{N+} - \int_1^N A(x)dx^{-s}$$

$$\sum_1^N a(n)n^{-s} = A(N)N^{-s} + s\int_1^N A(x)x^{-s-1}dx$$

If $\sigma > 0$ then $A(N)N^{-s}$ goes to zero. By hypothesis, $\sigma_c \geq 0$.

Lemma 2.7. If $\sigma > \sigma_c$ then $\sum_1^\infty a(n)n^{-s} = s\int_1^\infty A(u)u^{-s-1}du$

($\sigma > \sigma_c$ means that the $A(N)$'s converge.)

DEFINITION 2.8. $L = \max\{0, \limsup_{x\to\infty} \frac{\log|A(x)|}{\log(x)}\}$

If $\sigma > L$ then the RHS and LHS of Lemma 2.7 converge and are equal.

Corollary 2.9.

$$\sigma_c \leq L$$

PROOF. Use (2.1) ... Actual proof next time. □

NOTATION 2.10. $A(x) \ll X^\tau$ means that $|A(x)| < C \cdot x^\tau$, for sufficiently large x and for some finite constant $C > 0$.

3. January 31

Recall we had a Dirichlet series $D(s) = \sum_{n=1}^\infty a(n) \cdot n^{-s}$. We talked about wedge uniform convergence, which guarantees that if it converges at any point s_0, then it converges in a wedge to the right of s_0. You can compute the derivatives term-by-term. We defined the abscissa of convergence σ_c to denote the largest half-plane where it converges. Suppose the Dirichlet series converges at $s = s_c$. Define the remainder sum

$$R(x) = \sum_{n>x} a(n)n^{-s_0}$$

which goes to 0 as $x \to \infty$. Via "manual" integration by parts, we integrated $U^{s_0-s}dR$ (the Stieltjes integral) to get

$$\sum_{M+1}^N a(n)n^{-s} = R(M)M^{s_0-s} - R(N)N^{s_0-s} + (s_0 - s)\int_M^N R(u)u^{s_0-s-1}du \tag{3.1}$$

In particular, try sending $M \to 0$ and $N \to \infty$:

$$\sum_1^\infty a(n)n^{-s} = (s_0 - s)\int_0^\infty R(u)u^{s_0-s-1}du$$

Denote the partial sums by

$$A(x) = \sum_{n \le x} a(n)$$

Play the same Riemann-Stieltjes game:

$$\sum_1^N a(n)n^{-s} = A(N)N^{-s} + s\int_1^N A(u)u^{-s-1}du$$

Case 1: $\sigma_c < 0$ and $\sigma = \mathrm{Re}(s) > 0$. So it converges at zero, and the $A(N)$ have a limit. Letting $N \to \infty$, we get

$$\sum_1^\infty a(n)n^{-s} = s\int_1^\infty A(u)\cdot u^{-s-1}du$$

Case 2: $\sigma_c \ge 0$. Let

$$L = \limsup_{x\to\infty} \frac{\log|A(x)|}{\log x}$$

We already have $\mathrm{Re}(s) = \sigma > L$. Choose τ between σ and L. Then $A(x) \ll x^\tau$. *Here is the calculation:*

$$x^{\frac{\log|A(x)|}{\log x}} = \left(x^{\log|A(x)|}\right)^{\frac{1}{\log x}} = \left(\left(e^{\log x}\right)^{\log|A(x)|}\right)^{\frac{1}{\log x}} = \left(\left(e^{\log|A(x)|}\right)^{\log x}\right)^{\frac{1}{\log x}} = |A(x)|$$

If $\sigma > \tau$ then $A(N)N^{-s} \ll x^\tau N^{-s}$ goes to zero. The integral term converges for the same reason: $\int A(u)u^{-s-1}du$ should be compared to $\int u^\tau u^{-\sigma-1}du = u^{-1-(\sigma-\tau)}du$; as long as $\sigma > \tau$, this converges.

Corollary 3.1. If $\sigma > \tau > L$ and $\sigma_c \ge 0$, then $D(s)$ converges for $\mathrm{Re}(s) = \sigma$, and

$$\sum_1^\infty a(n)n^{-s} = s\int_1^\infty A(u)\cdot u^{-s-1}du$$

In this case, $\sigma_c \le \sigma$; but σ is *any* number $> L$, so $\sigma_c \le L$. (So this says something about σ_c in terms of the growth rate of the coefficients.) Use

$$\sum_{M+1}^N a(n)n^{-s} = R(M)M^{s_0-s} - R(N)N^{s_0-s} + (s_0 - s)\int_M^N R(u)u^{s_0-s-1}du$$

Use $M = s = 0$ and this simplifies to

$$\sum_1^N a(n)n^{-s} = -R(N)N^{s_0} + s_0\int_0^N R(u)u^{s_0-1}du$$

Stuff converges at s_0 so $R(u)$ is bounded. Since $R(N)$ is bounded, $R(N)N^{s_0}$ is growing no faster than x^{σ_0} (using absolute value), and similarly for the integral term.

$$|A(N)| \ll N^{\sigma_0}$$

But there are points where it converges, but not absolutely. This suggests we should pay attention to the abscissa of absolute convergence σ_a. We say that a Dirichlet series converges absolutely at s if $\sum |a(n)| \cdot n^{-\sigma}$ converges. (Of course, absolute convergence implies convergence, so $\sigma_c \leq \sigma_a$.) An absolutely convergent series does not change when you rearrange the terms.

Theorem 3.2.

$$\sigma_c \leq \sigma_a \leq \sigma_c + 1$$

PROOF. Suppose there is a sequence $b(n) \to 0$ as $n \to \infty$. The modified sequence

$$\sum b(n) n^{-1-\varepsilon}$$

is convergent, if $b(n)$ is *any* bounded sequence. Suppose $D(s_0)$ converges. Then let $b(n) = a(n) \cdot n^{-s_0}$. If the sum converges, then the terms go to zero; in order to make it converge absolutely, we just have to tuck in an extra $-1-\varepsilon$ in the exponent: $\sum a(n) n^{-s_0-1-\varepsilon}$ converges absolutely. Letting $\varepsilon \to 0$ this proves the theorem. □

For example, the zeta function has a pole at $s = 1$, so it doesn't have a chance of converging beyond that point as a Dirichlet series. But we can multiply by the offending factor $(1 - 2^{1-s})$ to eliminate the pole:

$$(1 - 2^{1-s}) \cdot \zeta(s) = \sum \frac{c(n)}{n^s}$$

where $c(n) = (-1)^{n+1}$. Letting Σ_c and Σ_a denote the abscissas for the modified functions, we have $\Sigma_c = 0$ and $\Sigma_a = 1$.

Suppose you have two Dirichlet series $D^{(1)}(s)$ and $D^{(2)}(s)$, where $\sigma_c^{(1)} > \sigma_c^{(2)}$. Then $D^{(1)}(s) \cdot D^{(2)}(s)$ makes sense for $\mathrm{Re}(s) > \max\{\sigma_c^{(1)}, \sigma_c^{(2)}\}$ We also talked about the star-product of Dirichlet series: $D(s) = \sum \frac{a^{(1)} * a^{(2)}}{n^s}$ which also makes sense in that domain. But the product might make sense but not converge. (For example, the abscissa of convergence for $(1 - 2^{1-s})\zeta(s)$ is $\frac{1}{4}$ and not zero.)

We had a lot of formal product formulas in the first lecture, for example $\zeta(s)D(s)$. Do these make sense as functions (instead of just formal Dirichlet series)? Yes, if you have absolute convergence (the star product just rearranges terms).

Theorem 3.3. $D^{(1)}(s) \cdot D^{(2)}(s)$ converges to the formal product of Dirichlet series if $\sigma > \sigma_a^{(2)}$.

Can you retrieve the coefficients from the functions? Yes.

Proposition 3.4. Suppose we have two Dirichlet series $\sum a(n)n^{-s}$ and $\sum b(n)n^{-s}$ that converge somewhere. Then, if they are equal as functions in some right half-plane of convergence, then they "are the same Dirichlet series" (i.e. the coefficients are the same).

PROOF. By shifting, suppose they both converge at $s = 0$. Let $c(n) = b(n) - a(n)$; we will show that all $c(i) = 0$.

$$c(1) = -\sum_{n=2}^{\infty} c(n)n^{-s}$$

$c(1)$ is constant, but the rest depends on s, so it's zero. Keep going. □

Note that it's not enough, in general, for complex continuous functions to be equal at a discrete set of points, in order to show that they are equal (example: $\sin(x)$ and zero). But Dirichlet series are indeed determined by their values at certain sequences.

For elliptic curves, $\sigma_c = 1$; in dynamical systems, it represents the entropy of the system. In the case we're dealing with, it will usually be 1 or 0.

Theorem 3.5 (Landau's Theorem)**.** Start with a Dirichlet series $D(s) = \sum a(n)n^{-s}$ where $a(n)$ is real and nonnegative for sufficiently large n. Also assume that $-\infty < \sigma_c < \infty$.

Then σ_c is a singularity (it can't be analytically continued there).

If a power series converges in a disc, you can ask what the largest disc of convergence is; then the power series is singular everywhere on that largest circle.

Let s be such that $\sigma > \sigma_c$ (i.e. it converges there). Take the k^{th} derivative:

$$D^{(k)}(s) = \sum_n a(n)(-\log n)^k n^{-s}$$

Assume $\sigma_c = 0$ (that is, replace a_n by $a_n n^{-\sigma_c}$, which does not change the fact that the coefficients are nonnegative). Take $s = 1$: this is analytic here, so it converges as a power series in the interior of some maximal circle:

$$D(s) = \sum_k c(k)(s-1)^k$$

Certainly, the radius of this maximal circle is at least 1. But suppose, for the sake of contradiction, the series is analytic at $s = 0$. Then it is analytic in some little circle $D_\delta(0)$ around $s = 0$. There aren't any obstacles to convergence anywhere to the right of the line $\sigma = 0$, so the maximal circle of power series convergence is allowed to extend to the left of $\sigma = 0$, as long as it is still contained in $\{\sigma > 0\} \cup D_\delta(0)$.

$c(k)$ can be gotten by taking the appropriate derivative:

$$\begin{aligned} c(k) &= \frac{1}{k!} D^{(k)}(s)|_{s=1} \\ &= \frac{1}{k!} \sum_n a(n)(-\log n)^k n^{-1} \end{aligned}$$

Watching the negative sign, rewrite

$$D(s) = \sum_{k=0}^{\infty} \frac{(1-s)^k}{k!} \sum_n a(n) \cdot (\log n)^k n^{-1}$$

This is absolutely convergent, so you can rearrange terms (i.e. swap the sums)

$$\begin{aligned} D(s) = \sum_n a(n) n^{-1} \sum_{k=0} \frac{((1-s)\log n)^k}{k!} &= \sum a(n) n^{-1} exp((1-s)\log n) \\ &= \sum a(n) n^{-s} \end{aligned}$$

We assumed that the power series converged past $s = 0$, and then transformed the power series into the original Dirichlet series, showing that this too converges past $s = 0$, a contradiction.

4. February 2

Standard way of dealing with the Gamma function:

$$\Gamma(s) = \int_0^{\infty} e^{-x} x^s \frac{dx}{x}$$

(Integrate by parts.)

There was a recap of Landau's theorem, which I added to the notes on the previous lecture.

4.1. Euler Products. Let $a(n)$ be a multiplicative function: that is, if $n = \prod_{i=1}^{\nu} p_i^{e_i}$, then $a(n) = \prod_{i=1}^{\nu} a(p_1^{e_i})$. Define

$$D_p(s) = \sum_{m=0}^{\infty} a(p^m) p^{-ms}$$

The Fundamental Theorem of Arithmetic says that

$$\prod_{p \ prime} D_p(s) = D(s)$$

at least formally. But, is this true analytically?

Proposition 4.1. If $D(s)$ converges absolutely then $D_p(s)$ converges absolutely for all p, and

$$\prod_p D_p(s) = D(s)$$

(i.e. both sides converge, and they converge to the same thing).

Let $\mathcal{N}(X)$ be the set of numbers with prime divisors $\leq X$. If $D(s)$ converges absolutely, then $\sum |a(n)|n^{-s}$ converges; for $D_p(s)$ to converge, we only need a subset of these terms to converge, so that is OK. To show that $\prod_p D_p(s)$ converges, it suffices to show that $\prod_{p \geq X} D_p(s) \to 0$ (so you're getting the terms where *all* of the divisors are $> X$).

$$\left| D(s) - \sum_{n \in \mathcal{N}(X)} a(n) n^{-s} \right|$$

represents the set of summands of $D(s)$ corresponding to terms where at least some divisor is $> X$. But this difference is $\leq \sum_{n \geq X} |a(n) \cdot n^{-s}|$, which goes to zero by absolute convergence, so we are done.

4.2. Facts about the Ramanujan τ function. Define

$$L_\Delta(s) = \sum_{n=1}^{\infty} \tau(n) n^{-s}$$

$$L_{\Delta,p}(s) = \sum_m \tau(p^m) p^{-ms} = \frac{1}{1 - \tau(p)p^{-s} + p^{11}p^{-2s}}$$

Theorem 4.2 (Mordell)**.**

$$\tau(m \cdot n) = \tau(m) \cdot \tau(n)$$

if $(m, n) = 1$.

$$\tau(p^{m+1}) = \tau(p)\tau(p^m) + p^{11}\tau(p^{m-1})$$

Together with the Mordell theorem, this shows that τ is determined by its values at primes.

4.3. Log of the zeta function. Using the definition $\zeta(s) = \prod (1 - p^{-s})^{-1}$:

$$\log((1 - p^{-s})^{-1}) = \sum_{m=1}^{\infty} \frac{p^{-ms}}{m}$$

$$\log \zeta(s) = \sum_p \sum_{m=1}^{\infty} \frac{p^{-ms}}{m}$$

DEFINITION 4.3. The Von Mangoldt Lambda function is:

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^e \text{ for some } e \\ 0 & \text{else} \end{cases}$$

$$\log \zeta(s) = \sum_p \sum_{m=1}^{\infty} \frac{p^{-ms}}{m} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{\log n} n^{-s}$$

(If n is not a power of p, then the coefficient is zero. If $n = p^m$, then we get $\frac{\log(p)}{\log(p^m)}p^{-ms}$ which produces the right thing.)

$$-(\log \zeta(s))' = \sum_{p,m} p^{-ms} = \sum \Lambda(n) n^{-s}$$

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum \Lambda(n) n^{-s}$$

4.4. Meromorphic continuation.

NOTATION 4.4. For $u \in \mathbb{R}$ write $u = [u] + \{u\}$, where $\{u\}$ is the fractional part, and $[u]$ is the greatest integer $\leq u$.

Similarly, for differentials we can write $du = d[u] + d\{u\}$. Then $d[u]$ is basically a delta function at each integer.

Break up the zeta function:

$$\zeta(s) = \sum_{n \leq x} n^{-s} + \sum_{n > x} n^{-s} \tag{4.1}$$

The second piece is

$$\sum_{n>x} n^{-s} = \int_{x^+}^{\infty} u^{-s} d[u]$$

$$= \underbrace{\int_{x}^{\infty} u^{-s} du}_{A} - \underbrace{\int_{x^+}^{\infty} u^{-s} d\{u\}}_{B}$$

$$A = \frac{u^{1-s}}{s-1}$$

$$\int_{x+}^{\infty} u^{-s} d\{u\} + \int_{x+}^{\infty} \{u\} du^{-s} = du^{-s}\{u\}\,]_{x^+}^{\infty} = -x^{-s}\{x\}$$

$$B = -x^{-s}\{x\} - \int_{x+}^{\infty} \{u\} du^{-s}$$

$$\sum_{n>x} n^{-s} = \frac{x^{1-s}}{s-1} + x^{-s}\{x\} + \left(-s \int_{x+}^{\infty} \{u\} \cdot u^{-s-1} du\right)$$

Going back to (4.1), we have

$$\zeta(s) = \sum_{n \leq x} n^{-s} + \frac{x^{1-s}}{s-1} + x^{-s}\{x\} - s \int_{x+}^{\infty} \{u\} u^{-s-1} du$$

The integral is bounded by $|s| \int_{x+}^{\infty} 1 \cdot u^{\sigma-1} du$. This is bounded if $\sigma > 0$. The formula on the right makes sense for $\mathrm{Re}(s) > 0$. The LHS is a Dirichlet series that makes sense for $\mathrm{Re}(s) > 1$. The RHS is analytic in s. Take the limit as $x \to 1^+$. The decomposition

reduces to

$$\zeta(s) = \underbrace{1 + \frac{1}{s-1}}_{\frac{s}{s-1}} - s\int_1^\infty \{u\}u^{-s-1}du$$

This shows that the RHS is meromorphic, with a simple pole at $s = 1$, in the region $\mathrm{Re}(s) > 0$.

Let's estimate the behavior of $\zeta(s)$ in the strip $0 < \sigma < 1$. Take $s = \sigma \in \mathbb{R}$. The integral is bounded by replacing $\{u\}$ by 1; now take the antiderivative, and we have $0 \leq \sigma \int_1^\infty u^{-\sigma-1}du \leq 1$. This gives

$$\frac{1}{\sigma-1} = \frac{\sigma}{\sigma-1} - 1 \leq \zeta(\sigma) \leq \frac{\sigma}{\sigma-1}$$

for this range.

4.5. Euler's constant. Many equivalent definitions in the notes.

DEFINITION 4.5.

$$C := 1 - \int_1^\infty \{u\}u^{-2}du$$

Alternatively, it's the unique constant approximated by

$$\sum_{n\leq x} \frac{1}{n} - \log x$$

as $x \to \infty$. More precisely,

$$\sum_{n\leq x} \frac{1}{n} - \log x = C + O\left(\frac{1}{x}\right)$$

NOTATION 4.6. $A = O(f(x))$ means that $A \leq c \cdot f(x)$ for large x, and some constant c.

To prove the equivalence,

$$\sum_{n\leq x} \frac{1}{n} = \int_{1-}^{x+} u^{-1}d[u] = \int_{1-}^{x+} u^{-1}du - \int_{1-}^{x+} u^{-1}d\{u\}$$

where the last integral is $\int \{u\}d(u^{-1}) + u^{-1}\{u\}]_{1-}^{x+}$ by Riemann-Stieltjes calculations. Finish this later.

5. February 7

5.1. Euler's constant.

(1) $C = 1 - \int_1^\infty \{u\}u^{-2}\,\mathrm{d}u$
(2) $\sum_{n\leq x} \frac{1}{n} - \log x = C + O(\frac{1}{x})$

(3) $\zeta(s) = \frac{1}{s-1} + C + a_1(s-1) + a_2(s-1)^2 + \cdots$

PROOF. Write

$$\sum_{n \le x} \frac{1}{n} = \int_{1-}^{x} u^{-1} d[u] = \underbrace{\int_{1-}^{x} u^{-1}\,\mathrm{d}u}_{\log x} - \int_{1-}^{x} u^{-1} d\{u\}$$

where integration by parts gives

$$\int_{1-}^{x} d\{u\} + \int_{1-}^{x} \{u\} d(u^{-1}) = \{u\}u^{-1}|_{x^{1-}} = -1$$

This gives (2).

$$\zeta(s) - \frac{x^{1-s}}{s-1} = \sum_{n \le x} n^{-s} + \frac{\{x\}}{x^s} - s\int_{x}^{\infty} \{u\}u^{-s-1}\,\mathrm{d}u$$

Now use $x = 1$:

$$\zeta(s) - \frac{1}{s-1} = 1 - s\int_{1}^{\infty} \{u\}u^{-s-1}\,\mathrm{d}u$$

and take the limit as $s \to 1$, getting (3). □

Everyone thinks that C is transcendental, but we can't prove it's irrational!

5.2. Fourier transforms. Schwartz functions on the real line are rapidly decreasing C^∞ functions: we require $f \cdot P(X)$ to be bounded for any polynomial. (One easy way to have this is to consider compactly supported functions.)

DEFINITION 5.1. The Fourier transform of f is

$$\int_{-\infty}^{\infty} e^{-2\pi i x y} f(x)\,\mathrm{d}x = \widehat{f}(y)$$

If f is Schwartz then $\widehat{\widehat{f}} = f$. We have a bilinear map

$$\mathbb{R} \times \mathbb{R} \to \mathbb{C}^* = \mathbb{C}_1^* = \{z \in \mathbb{C} : |z| = 1\} \qquad (x, y) \mapsto e^{-2\pi i x y}$$

which shows that $\mathbb{R}$ is self-dual. One of the beautiful consequences of this symmetry is

Theorem 5.2 (Poisson summation)**.** $\sum_{n\in\mathbb{Z}} f(n+x) = \sum_{n\in\mathbb{Z}} \widehat{f}(n)e^{-2\pi i n x}$

Letting $x \to 0$, we have

$$\sum f(n) = \sum \widehat{f}(n)$$

DEFINITION 5.3. The Gaussian is $f(x) = e^{-\pi x^2}$.

Lemma 5.4. The Gaussian is its own Fourier transform.

PROOF. Integrals without limits will mean $\int_{\mathbb{R}}$.

$$\widehat{f}(y) = \int e^{-\pi x^2} e^{-2\pi i x y}\,\mathrm{d}x = \int e^{-\pi(^2+2ixy+y^2-y^2)}\,\mathrm{d}x$$
$$= e^{-\pi y^2}\int e^{-\pi(x+iy)^2}\,\mathrm{d}x$$

The contour is now $-\infty+0 \to +\infty+0$, and we want to change it to $-\infty+iy \to +\infty+iy$. Using a large R instead of ∞, turn this into a rectangle, where the contribution to the integral from the sides $\to 0$ as $R\to\infty$. So we can ignore the sides of the rectangle.

$$\int_{-\infty}^{+\infty} e^{-\pi x^2}dx = \left(\int_{-\infty}^{+\infty} e^{-\pi x^2}\,\mathrm{d}x \cdot \int_{-\infty}^{+\infty} e^{-\pi y^2}\,\mathrm{d}y\right)^{\frac{1}{2}}$$
$$= \int\int e^{-\pi(x^2+y^2)}\,\mathrm{d}x\,\mathrm{d}y = \int_\theta \int_{r=0}^{\infty} e^{-\pi r^2} r\,\mathrm{d}r\,\mathrm{d}\theta = 1$$

□

We can renormalize the Gaussian to $e^{-\pi x^2/t}$, and its Fourier transform is $\sqrt{t}e^{-\pi x^2 t}$ (you're replacing $x \mapsto \frac{x}{t}$). We're thinking of $t>0$, so we can take $\sqrt{t}>0$.

DEFINITION 5.5 (Theta function).

$$\Theta(z) = \frac{1}{2}\sum_{n\in\mathbb{Z}} e^{\pi i n^2 z} = \frac{1}{2} + \sum_{n\geq 1} e^{\pi i n^2 z}$$

Write $z = x+iy$, which makes

$$\Theta(z) = \frac{1}{2}\sum_{n\in\mathbb{Z}} e^{2\pi i n^2 x}\cdot e^{-2\pi n^2 y}$$

But $e^{2\pi i n^2 x}$ has absolute value 1, so it will not play much of a role in convergence. But in order for $e^{-2\pi n^2 y}$ to make sense, we need $y>0$. We will consider it on the imaginary axis $z=iy$, and think of it as a function of y.

Analytic continuation will show that symmetries in $\Theta(iy)$ relate to symmetries on the entire upper half-plane.

$$\Theta(iy) = \frac{1}{2}\sum_{n\in\mathbb{Z}} e^{-\pi i n^2 y}$$

We have $\Theta(z+2)=\Theta(z)$, just from the definition (and noticing $e^{2\pi i n}=1$). Apply Poisson summation (and remember the Gaussian Fourier transform from above):

$$\Theta\left(\tfrac{-1}{iy}\right) = \frac{1}{2}\sum \sqrt{y} e^{-\pi n^2/y} = \sqrt{y}\cdot\Theta(iy)$$

(Define our square roots so that they are positive on the positive real axis.) So

$$\Theta\left(\tfrac{-1}{z}\right) = \sqrt{\frac{z}{i}}\cdot\Theta(z)$$

$$\Theta^{4k}\left(\tfrac{-1}{z}\right) = z^{2k} \cdot \Theta^{4k}(z)$$

5.3. Gamma function.

DEFINITION 5.6.

$$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t}\, \mathrm{d}t$$

Also define a function

$$F(s) = \pi^{-s}\Gamma(s) \cdot \zeta(2s)$$

which we will write in a bunch of ways. Now work in the domain where the Dirichlet series makes sense, and write

$$\begin{aligned} F(s) &= \sum_{n=1}^{\infty} (\pi n^2)^{-s}\Gamma(s) \\ &= \sum \int_0^\infty (\pi n^2)^{-s} t^{s-1} e^{-t}\, \mathrm{d}t \end{aligned}$$

Make the substitution $t = \pi n^2 y$, and $dt = \pi n^2 dy$

$$\begin{aligned} \cdots &= \sum \int (\pi n^2)^{-s} (\pi n^2)^{s-1} y^{s-1} e^{-\pi n^2 y} \pi n^2\, \mathrm{d}y \\ &= \sum_{n=1}^{\infty} \int_0^\infty y^{s-1} e^{-\pi n^2 y}\, \mathrm{d}y \end{aligned}$$

We can interchange the summation and the integral, because the integrand is positive and $\sum \int \cdots = F(s)$ is known to be convergent (use Fubini/Tonelli):

$$\begin{aligned} \cdots &= \int_0^\infty y^{s-1} \sum_{n=1}^{\infty} e^{-\pi n^2 y} \cdot\, \mathrm{d}y \\ &= \int_0^\infty y^{s-1} \left(\Theta(iy) - \frac{1}{2}\right)\, \mathrm{d}y \end{aligned}$$

HW: $\Theta(iy) - \frac{1}{2} = O(e^{-cy})$

Split the range of integration: $\int_0^\infty = \int_1^\infty + \int_0^1$. The problematic part is $\int_0^1$. Split the $\frac{1}{2}$ off from the Θ in this part:

$$\begin{aligned} \cdots &= \int_1^\infty * + \int_0^1 y^{s-1}\Theta(iy)\, \mathrm{d}y - \frac{1}{2} \cdot \frac{y^s}{s}\Big|_0^1 \\ &= \int_1^\infty + \int_0^1 y^{s-1}\Theta(iy)\, \mathrm{d}y - \frac{1}{2s} \end{aligned}$$

Now do the transformation $y \mapsto y^{-1}$:

$$\cdots = \int_1^\infty + \int_\infty^1 y^{1-s} \cdot \Theta\left(\frac{i}{y}\right) \underbrace{\mathrm{d}(y^{-1})}_{-y^{-2}\,\mathrm{d}y} - \frac{1}{2s}$$

$$= \int_1^\infty + \int_1^\infty y^{-1-s} \cdot \Theta\left(\frac{-1}{iy}\right) \, \mathrm{d}y - \frac{1}{2s}$$

Make the transformation

$$\cdots = \int_1^\infty + \underbrace{\int_1^\infty y^{-1-s} \cdot y^{\frac{1}{2}} \Theta(iy) \cdot \, \mathrm{d}y}_{\int_1^\infty y^{-\frac{1}{2}-s} \Theta(iy) \, \mathrm{d}y} - \frac{1}{2s}$$

$$= \int_1^\infty + \int_1^\infty y^{-\frac{1}{2}-s} \left(\Theta(iy) - \frac{1}{2}\right) \, \mathrm{d}y + \frac{1}{2} \underbrace{\int_1^\infty y^{-\frac{1}{2}-2} \, \mathrm{d}y}_{\frac{-1}{1-2s}}$$

$$= \underbrace{\int_1^\infty (y^{s-1} + y^{-\frac{1}{2}-s}) \left(\Theta(iy) - \frac{1}{2}\right) \, \mathrm{d}y}_{I(s)} - \frac{1}{1-2s} - \frac{1}{2s}$$

$$= F(s)\pi^{-s}\Gamma(s) \cdot \zeta(2s)$$

Note: $I(s) = \int (y^{s-1} + y^{-\frac{1}{2}-s}) \left(\Theta(iy) - \frac{1}{2}\right) \, \mathrm{d}y$ has an integrand that is a polynomial times a very quickly decreasing function. It is entire. If we replace $s \mapsto \frac{1}{2} - s$, then y^{s-1} switches with $y^{-\frac{1}{2}-s}$, and $-\frac{1}{1-2s}$ switches with $-\frac{1}{2s}$. Therefore,

Proposition 5.7.

$$F(s) = F\left(\frac{1}{2} - s\right)$$

Usual definition:

$$\Lambda(s) = \pi^{-\frac{s}{2}} \cdot \Gamma\left(\frac{s}{2}\right) \cdot \zeta(s)$$

Then we've proven

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

To get from Θ to ζ, we've passed through $\Theta(iy)$ and gotten to $\zeta(s)$ by a Mellin transform. Can you go the other way? Yes!

$$\Theta(iy) - \frac{1}{2} = \frac{1}{2\pi i} \int_{\mathrm{Re}(s)=\sigma \gg 0} u^{-s} F(s) \, \mathrm{d}s$$

Θ is a modular form, whose transformation law gives the symmetry of the functional equation. Θ is completely determined by its transformation law, and growth rate. This translates to a characterization of $\zeta(s)$ in terms of properties of its functional equation.

6. February 9

6.1. One way to prove the functional equation. For $\mathrm{Re}(s) > 0$

$$\zeta(s) = \frac{1}{s-1} + 1 + s \int_1^\infty \frac{\{x\}}{x^{s+1}}$$

You can check that

$$-s\int_1^\infty \frac{\frac{-1}{2}}{x^{s+1}}\,\mathrm{d}x = \frac{1}{2}$$

"Subtracting and adding" this to the previous line:

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} - s\int_1^\infty \frac{\{x\}-\frac{1}{2}}{x^{s+1}}\,\mathrm{d}x$$

for $\mathrm{Re}(s) > 0$. But claim that this is true for $\mathrm{Re}(s) > -1$. Write $f(x) = \{x\} - \frac{1}{2}$ and define $F(x) = \int_1^x f(y)\,\mathrm{d}y$ which is bounded because the sawtooth is centered around $y = 0$. Integration by parts:

$$\int_1^b \frac{f(x)}{x^{s+1}}\,\mathrm{d}x = \left[\frac{F(x)}{x^{s+1}}\right]_1^b + (s+1)\int_1^b \frac{F(x)}{x^{s+1}}\,\mathrm{d}x$$

The second integral is convergent for $s > -1$.

Claim 6.1.

$$-s\int_0^1 \frac{\{x\}-\frac{1}{2}}{x^{s+1}}\,\mathrm{d}x = \frac{1}{s-1} + \frac{1}{2}$$

PROOF. Since $\{x\} = x$ for $x \in [0,1)$, we can split up the LHS so that

$$LHS = -s\int_0^1 x^{-s}\,\mathrm{d}x + \underbrace{\frac{s}{2}\int_0^1 x^{-s-1}\,\mathrm{d}x}_{\frac{s}{2}\left[\frac{x^{-s}}{-s}\right]_0^1}$$

When $-s > 0$ then the lower bound of zero is OK. Now it is easy to evaluate this. □

Now we can plug this into the previous expression of $\zeta(s)$ and get

$$\zeta(s) = -s\int_0^\infty \frac{\{x\}-\frac{1}{2}}{x^{s+1}}\,\mathrm{d}x$$

for $-1 < \mathrm{Re}(s) < 0$. (We need > -1 so that the integral to ∞ will work out, and < 0 for the lower bound.) By Fourier series,

$$\{x\} - \frac{1}{2} = \sum_{n=1}^\infty \frac{\sin(2\pi n x)}{\pi n}$$

and the HW implies you can switch the integral and sum, giving

$$\begin{aligned}
\zeta(s) &= -\frac{s}{\pi}\sum_{n=1}^\infty \frac{1}{n}\int_0^\infty \frac{\sin(2\pi n x)}{x^{s+1}\,\mathrm{d}x} \\
&= -\frac{s}{\pi}\sum \frac{(2\pi n)^s}{n}\int_0^\infty \frac{\sin y}{y^{s+1}}\,\mathrm{d}y \\
&= -\frac{s}{\pi}\zeta(1-s)(2\pi)^s[-\Gamma(-s)\sin(\frac{1}{2}\pi s)] \qquad \text{by next lemma}
\end{aligned}$$

Lemma 6.2.

$$\int_0^\infty \frac{\sin(y)}{y^{s+1}}\,\mathrm{d}y = -\Gamma(-s)\sin\left(\frac{1}{2}\pi s\right)$$

Use the contour obtained by going counterclockwise around the quarter radius-X circle in the right upper half-plane, and letting X go to ∞. Recall $\sin y = \frac{e^{iy}-e^{-iy}}{2i}$. Here $|e^{it}| \leq 1$ and

$$\left|\frac{1}{y^{s+1}}\right| \leq \frac{1}{X^{\mathrm{Re}(s)+1}}$$

The arc length is $\frac{X\pi}{2}$ and $\frac{\pi X}{2}\cdot\frac{1}{X^{\mathrm{Re}(s)+1}} \to 0$ as $X \to +\infty$. So we can concentrate on the straight pieces.

$$\mathit{Residues} = 0 = \int_0^\infty \frac{e^{iy}}{y^{s+1}}\,\mathrm{d}y + \int_{arc} + \int_{+i\infty}^0 \frac{e^{iy}}{y^{s+1}}\,\mathrm{d}y$$

Make the substitution $z = iy$:

$$\int_0^{+i\infty} \mathrm{d}y = \int_0^\infty e^{-z}(iz)^{-s-1}i\,\mathrm{d}z = (e^{\frac{1}{2}\pi i})^{-s}\underbrace{\int_0^\infty e^{-z}z^{-s-1}\,\mathrm{d}z}_{\Gamma(-s)}$$

Actually, the integral isn't defined at zero, so we need to make a little arc of radius r around zero, and integrate on that instead.

We need to do something similar for e^{-iy} in $\sin y = \frac{e^{iy}-e^{-iy}}{2i}$; this involves flipping the contour over the x-axis.

$$\int_0^\infty \frac{\sin y}{y^{1+s}}\,\mathrm{d}y = -\sin\frac{1}{2}\pi s\cdot\Gamma(-s)$$

Here we extended the domain of $\zeta(s)$ by a strip to the left. But you can keep doing this, and, adding as many strips as you want, you can get the entire left half-plane.

6.2. The filter. Recall we had a normalized version of the functional equation from last time:

$$F(s) = \pi^{-s}\Gamma(s)\zeta(2s)$$

Using contour integration along a vertical line:

$$\Theta(it) - \frac{1}{2} = \frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\sigma_0} t^{-s}F(s)\,\mathrm{d}s$$

Let $X > 0$, and assume σ_0 is sufficiently large (at least, > 0).

Theorem 6.3.

$$\frac{1}{2\pi i}\int_{\sigma_0-i\infty}^{\sigma_0+i\infty}\frac{X^s}{s}\,\mathrm{d}s=\begin{cases}1 & X>1\\ \frac{1}{2} & X=1\\ 0 & X<1\end{cases}$$

We will do the first case; the second is HW. Use a rectangle between the lines $\mathrm{Re}(s)=-A$ and $\mathrm{Re}(s)=\sigma_0$, cut off between $s+iT$ and $s-iT$. So there are four integrals, around the sides of the rectangle, and the goal is to show that the ones other than $\int_{\sigma_0-iT}^{\sigma_0+iT}$ go to zero. Let's do the top piece:

$$\int_{\sigma=-A}^{\sigma=\sigma_0}\frac{X^\sigma}{|\sigma+iT|}\le\frac{1}{T}\int_{-A}^{\sigma_0}y^\sigma\,\mathrm{d}\sigma\le T^{-1}\frac{y^{\sigma_0}}{\log y}$$

The left-hand line is

$$\int_{t=-T}^{t=+T}\frac{X^{-A}}{|-A+it|}\,\mathrm{d}t\le 2T\frac{X^{-A}}{A}$$

As $A\to\infty$, this goes to zero.

6.3. Unrigorous Mellin transform. Recall for a Dirichlet series $D(s)=\sum a(n)n^{-s}$, we can define a counting function $A(x)=\sum_{n\le x}a(n)$. Actually, modify this:

$$A'(x)=\begin{cases}A(x) & x\notin\mathbb{Z}\\ \sum_{n<N}a(n)+\frac{1}{2}a(N) & \text{else}\end{cases}$$

(Basically, $A'(x)=\frac{A(x+)+A(x-)}{2}$.)

Recall

$$\Lambda(n)=\begin{cases}\log p & n=p^e\\ 0 & \text{else}\end{cases}$$

We also care about the counting function $\psi(x)=\sum_{n\le x}\Lambda(n)$ and the associated function $\psi'(x)=\frac{\psi(x+)+\psi(x-)}{2}$.

Roughly, $D(s)$ and $A(x)$ encode the same information. How do you get from one to the other?

$$D(s)=\int_{1-}x^{-s}\,\mathrm{d}A(x)=-\int_{1-}^{\infty}A(x)\,\mathrm{d}(x^{-s})=s\int_1^\infty A(x)x^{-s-1}\,\mathrm{d}x$$

This is the Mellin transform: reading right-to-left, you recover $D(s)$ from $A(x)$. The inverse Mellin transform is getting $A(x)$ out of $D(s)$. Consider

$$\frac{1}{2\pi i}\int_{\sigma_0}D(s)\frac{X^s}{s}\,\mathrm{d}s=\frac{1}{2\pi i}\int_{\sigma_0}\sum_{n=1}^{\infty}a(n)\cdot\frac{1}{s}\left(\frac{x}{n}\right)^s\,\mathrm{d}s$$

This is just applying the filter to each term, with $\frac{x}{n}$ playing the role of x in the definition, and you get a factor of 1 exactly when $\frac{X}{n}\ge 1\implies X\ge n$, and these are the terms $a(n)$ that get selected. This just gets you $A'(x)$. Now do this rigorously.

Theorem 6.4.

$$A'(x) = \lim_{T\to\infty} \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} D(s)\frac{x^s}{s}\,\mathrm{d}s$$

where the limit is taken with fixed X.

Let $D^N(s) = \sum_{n\le N} a(n)n^{-s}$, $D_N(s) = \sum_{n>N} a(n)n^{-s}$. So $D = D^N + D_N$. (And yes, the upper and lower N's are kind of bad notation...)

It suffices to prove that

$$\int_{\sigma_0 - iT}^{\sigma_0 + iT} D_N(s)\frac{X^s}{s}\,\mathrm{d}s \to 0 \text{ as } T \to \infty$$

Use a rectangle with vertices $\{\sigma_0 \pm iT, T \pm iT\}$, with counterclockwise direction. Everything is regular here, assuming that $\sigma_0 > \max\{0, \sigma_c\}$; the only pole is at $s = 0$. We know that

$$\int A + \int B + \int C + \int D = 0$$

The claim is that all except $\int A = \int_{\sigma_0 - iT}^{\sigma_0 + iT}$ go to zero; this will imply that $\int A \to 0$.

Lemma 6.5.

$$\int B, \int C, \int D \to 0$$

$$D_N(s) = \int_N^\infty u^{-s}\,\mathrm{d}(A(u) - A(N))$$

(The $\mathrm{d}A(N)$ doesn't actually do anything, but we put it there for clarity.) This is

$$\cdots = s\int_N^\infty (A(u) - A(N)) \cdot u^{-s-1}\,\mathrm{d}u$$

Choose some θ between σ_c and σ_0. Claim

$$A(u) - A(N) \ll u^\theta$$

(This comes from the lim sup discussion from earlier.) Next time, we use the integral and the inequality to produce immediate estimates on all the contours.

7. February 14

7.1. Perron's theorem. We have a Dirichlet series $D(s) = \sum a(n)n^{-s}$, have defined $A(x) = \sum_{n\le x} a(n)$ and A' as before. The Mellin transform is

$$D(s) = s\int_1^\infty A(x)x^{-s-1}\,\mathrm{d}x$$

Using the unrigorous method from last time,

$$A'(x) \stackrel{?}{=} \frac{1}{2\pi i}\int_{\sigma_0 - i\infty}^{\sigma_0 + i\infty} D(x)\frac{x^s}{s}\,\mathrm{d}s$$

where $\sigma_0 > \sigma_c$. This is certainly true if we're allowed to swap the sum (in $D(s)$) with the integral: one term looks like

$$\int_{\sigma_0-i\infty}^{\sigma_0+i\infty} a(n)\cdot n^{-s}\frac{x^s}{s}\,\mathrm{d}s = \frac{a(n)}{2\pi i}\int \frac{\left(\frac{x}{n}\right)^s}{s}\,\mathrm{d}s = \begin{cases} a(n) & n<x \\ \frac{1}{2}a(n) & n=x \\ 0 & n>x \end{cases}$$

The $\frac{1}{2}$ in the middle case is why we had to use the averaging procedure for $A'(x)$ instead of $A(x)$. So

$$\sum_{n=1}^{\infty}\frac{1}{2\pi i}\int a(n)\cdot n^{-s}\frac{x^s}{s}\,\mathrm{d}s = A'(x)$$

Now we need to make this rigorous.

Fix x. Choose $N \gg x$. Write

$$D(s) = \underbrace{\sum_{n\le N} a(n)n^{-s}}_{D^N(s)} + \underbrace{\sum_{n>N} a(n)n^{-s}}_{D_N(s)}$$

Since swapping sums and integrals is fine when the sums are finite, we can say

$$A'(x) = \frac{1}{2\pi i}\int D^N(s)\frac{x^s}{s}\,\mathrm{d}s$$

We need to show that

$$\int D_N(s)\frac{x^s}{s}\,\mathrm{d}s \to 0 \text{ as } N\to\infty$$

Make the rectangle with vertices $\{\sigma_0 \pm iT, T \pm iT\}$ We want to show that $\int_{\sigma_0-iT}^{\sigma_0+iT} *$ (the left vertical piece) is small; to do that, we show that the other integrals are small. We can write

$$D_N(s) = \int_{N+}^{\infty} u^{-s}\,\mathrm{d}(A(u)-A(N)) = s\int_N^{\infty}(A(u)-A(N))u^{-s-1}\,\mathrm{d}u$$

by Riemann-Stieltjes. Assume

$$A(u)-A(N) \ll u^{\theta}$$

for $\theta \in (\max\{0,\sigma_c\},\sigma_0)$.

$$D_N(s) \ll |s|\cdot\int_N^{\infty} u^{\theta-\sigma-1}\,\mathrm{d}u = |s|\cdot\frac{N^{\theta-\sigma}}{\sigma-\theta}$$

Now the integral we want to evaluate is

$$\int_* \frac{|s|}{\sigma-\theta}N^{\theta-\sigma}\frac{x^{\sigma}}{|s|}\,\mathrm{d}s = N^{\theta}\int_*\frac{\left(\frac{x}{N}\right)^{\sigma}}{\sigma-\theta}\,\mathrm{d}s \tag{7.1}$$

When * is one of the horizontal pieces:

$$\cdots \le \frac{N^{\theta}}{\sigma_0-\theta}\int_*\left(\frac{x}{N}\right)^{\sigma}\,\mathrm{d}s = \frac{N^{\theta}}{\sigma_0-\theta}\left[\frac{\left(\frac{x}{N}\right)^{\sigma}}{\log\frac{x}{N}}\right]_{\sigma_0}^{T}$$

$$= \frac{N^{\theta}}{\sigma_0-\theta}\cdot\frac{\left(\frac{x}{N}\right)^{T}-\left(\frac{x}{N}\right)^{\sigma_0}}{-\log\frac{N}{x}} \qquad N \text{ is large so } \left(\frac{x}{N}\right)^{T} \text{ is small}$$

$$\leq \frac{N^\theta}{\sigma_0 - \theta} \frac{N^{-\sigma_0} x^{\sigma_0}}{\log \frac{N}{x}} = \frac{N^{\theta-\sigma_0} x^{\sigma_0}}{\log \frac{N}{x} \cdot (\sigma_0 - \theta)} \qquad \theta < \sigma_0 \text{ by assumption}$$

To do the right-hand vertical integral $\int_{T-iT}^{T+iT}$, plug in $\sigma = T$ to (7.1) (obtaining an integrand that does not depend on t):

$$N^\theta \int_{-T}^{+T} N^{-T} \cdot \frac{x^T}{(T-\theta)} \, \mathrm{d}t = N^\theta \cdot N^{-T} \cdot \frac{x^T}{T-\theta} \cdot (T - (-T))$$
$$= N^\theta \left(\frac{x}{N}\right)^T \cdot \underbrace{\frac{2T}{T-\theta}}_{bounded}$$

Choose N large such that $N^{\frac{T}{2}} \gg x$ and

$$N^\theta \left(\frac{x}{N}\right)^T = N^{\theta - \frac{T}{2}} \cdot \frac{x}{N^{\frac{T}{2}}} \approx N^{\theta - \frac{T}{2}}$$

Remember, we were taking $\lim_{T\to\infty}$ before taking $\lim_{N\to\infty}$, because we were trying to find $\lim_{T\to\infty} \int_{T-iT}^{T+iT} D_N(s) \frac{x^s}{s} \, \mathrm{d}s$ for each N, and then hope that those integrals approached zero as $N \to \infty$. So here, $\lim_{T\to\infty} N^{\theta - \frac{T}{2}} \to 0$ for every N.

7.2. Gamma facts. We're interested in the behavior of Γ on upper vertical strips: $\sigma + it$, where $|t| > 1$ and σ is in some strip.

Theorem 7.1 (Stirling's formula)**.**

$$|\Gamma(s)| \ll e^{-\frac{\pi}{2}|t|}$$

By definition,

$$\Gamma(s) = \int_0^\infty e^{-t} t^s \frac{\mathrm{d}t}{t}$$

It is the Mellin transform of e^{-t}. So we can do the inverse Mellin transform:

$$e^{-t} = \frac{1}{2\pi i} \int_{line\ \sigma} \Gamma(s) t^{-s} \, \mathrm{d}s$$

(It's a little like applying the filter to $s\Gamma(s)\dots$)

7.3. Hecke's theorem. Let λ, k be positive reals, and choose $\{a(n), b(n)\} \ll c > 0$. Define the Dirichlet series

$$\varphi(s) = \sum_{n=1} a(n) n^{-s} \qquad \psi(s) = \sum_{n=1} b(n) n^{-s}$$

(Note that $a(0)$ and $b(0)$ are not used here. This will be a constant annoyance.) These act like $\zeta(2s)$, and are defined in some right half-plane. However, we want expressions for $\psi(k-s)$ (which aren't even defined yet.) To get a better relationship, we introduce Γ-factors:

$$\Phi(s) = \left(\frac{\lambda}{2\pi}\right)^s \Gamma(s)\varphi(s) \qquad \Psi(s) = \left(\frac{\lambda}{2\pi}\right)^s \Gamma(s)\psi(s)$$

Define

$$f(z) = \sum_{n=0}^{\infty} a(n)e^{2\pi inz/\lambda} \qquad g(z) = \sum_{n=0}^{\infty} b(n)e^{2\pi inz/\lambda}$$

We need to show:

(1) $\varphi(s), \psi(s)$ are analytic in the right half-plane $\sigma > c+1$. (Use the bounds $a(n), b(n) \ll n^c$)
(2) $f(z), g(z)$ are analytic in the upper half plane. Also,
$$f(x+iy), g(x+iy) \ll y^{-c-1} \text{ as } y \to 0_+$$
(3) $\Phi(s) = \int_0^\infty (f(iy) - a(0))y^{s-1}\,\mathrm{d}y$ and similarly for Ψ. (Unrigorously, this is obvious; the exercise is to justify the commutation of $\sum$ and $\int$.)
(4) Crux: the following statements are equivalent:
   (a) The function $\Phi(s) + \frac{a(0)}{s} + \frac{\varepsilon b(0)}{k-s}$ is entire on $\mathbb{C}$, and is bounded on every vertical strip, and
   $$\Phi(s) = \varepsilon\Psi(k-s)$$
   (b)
   $$\varepsilon \cdot g\left(\frac{-1}{z}\right) = \left(\frac{z}{i}\right)^k f(z)$$

EXAMPLE 7.2. Θ-function: $k = \frac{1}{2}, \varepsilon = 1, g = f = \theta$

$$\Theta^m\left(\frac{-1}{z}\right) = \left(\frac{z}{i}\right)^{m/2} \cdot \Theta^m(z)$$

This helps you estimate the function that counts the # of ways to write n as a sum of m squares

Equivalence in the forward direction is what we did in the case of the Riemann zeta function.

7.4. Digression: Lattice theory in dimension 24. Let $L \subset \mathbb{R}^N$ be a lattice. You can produce a theta function θ_L associated to the lattice:

$$\theta_L(z) = \sum a(n)q^n$$

where $a(n) - \#\{\lambda \in L : \langle \lambda, \lambda \rangle = n\}$ If $N = 1$, then this is *our* θ. But any of them satisfies a transformation law. If $L \subset \mathbb{R}^{24}$, then elementary analysis shows that we can write

$$\theta_L(z) = E(z) + D(z)$$

where E and D are both modular forms of weight 12. $E(z)$ has large coefficients, but is very elementary (it's an Eisenstein series). $D(z)$ has smaller coefficients, but is somewhat deep; this gives the dominant term for the arithmetic function $n \mapsto a(n)$. It turns out that $D(z)$ is a multiple of $\Delta(q) = q \cdot \prod_{n=1}^{\infty}(1-q^n)^{24}$. For higher Waring problems, we don't have symmetries as nice.

8. February 16

8.1. Phragmen-Lindelöf Theorem.

Theorem 8.1. Let $f(s)$ be analytic in some upper vertical strip: $\sigma_1 \leq \sigma \leq \sigma_2$ and $t \geq T_1$. Require

$$|f(s)| = O(e^{t^a})$$

on the entire strip, and

$$|f(s)| = O(t^M)$$

on the vertical boundary. Then $|f(s)| \leq O(t^M)$ on the whole strip.

Corollary 8.2. If $|f(s)|$ is bounded on the boundary, and $|f(s)| = O(e^{t^a})$ on the strip, then it's bounded on the whole strip.

Clearly, the theorem implies the corollary. But:

Claim 8.3. The corollary implies the theorem.

PROOF. Suppose $f(s)$ satisfies the hypotheses of the theorem. Then $g(s) = f(s)/s^M$ is still analytic on the strip, and still satisfies the interior bound. But, it's also now bounded on the boundary. By the corollary, $g(s)$ is bounded everywhere on the strip. So $f(s) = g(s) \cdot s^M$ is $O(t^M)$. □

So it suffices to prove the corollary.

COROLLARY. Let $f(s) \leq B$ on the boundary, and $O(e^{t^a})$ on the entire strip. Choose $m > a$ such that $m \equiv 2 \pmod 4$. Write $s^m = r^m \cdot e^{im\theta}$. It's OK to move T_1 once, so assume that the line from s (in the strip) to the origin makes an angle with the real axis that is almost 90^o. That is, s in the strip looks like $r \cdot e^{i\theta}$ where $\theta \approx \frac{\pi}{2}$. Furthermore, assume that $m\theta \approx \pi$ (this is why we want $m \equiv 2 \pmod 4$). So if $s^m = r^m(\cos m\theta + i \sin m\theta)$ where $\sin m\theta$ is close to zero, and $\cos m\theta \approx -1$, then $s^m \approx -r^m$.

For the moment choose a constant $c > 0$, and define

$$g_c(s) = f(s)e^{c \cdot s^m}$$

(recall $s^m < 0$). This is bounded on the boundary, and on the interior it's not so bad:

$$|g_c(s)| = O(e^{t^a + c \cdot r^m \cos m\theta})$$

(recall $\cos m\theta < 0$). The second term will eventually swamp the first: we can find T_2 large enough such that if $t \geq T_2$, then $t^a + c \cdot r^m \cos m\theta \leq 0$. (Recall that these things are related by $s = r \cdot e^{i\theta} = \sigma + it$, and here $r^m \cos m\theta \approx s^m$.) Let $T_3 \geq T_2$ be arbitrary. Then

g_c is bounded on all four sides of the rectangle $T_1 \leq t \leq T_3$, $\sigma_1 \leq \sigma \leq \sigma_2$, because:

$$|f(s)| \leq Be^{t^a} \implies g_c(s) \leq Be^{t^a + cr^m \cos m\theta} \implies |g_c(s)| \leq B$$

Use the maximum modulus principle for g_c on our rectangle. g_c is analytic on the region, and has absolute value bounded by B. That is,

$$|f(s)| \leq B \cdot e^{cr^m \cos m\theta}$$

for any θ in this strip.

This is true for every c. Taking the limit gives

$$|f(s)| \leq \lim_{c \to 0} B \cdot e^{-cr^m \cos m\theta} = B$$

as desired.

□

8.2. Stuff about the HW.

- We had
$$\sum_{n=1}^{\infty} a(n)e^{-ny}$$
for $a(n) \ll n^c$. Break this up as
$$\sum_{n=1}^{\infty} \underbrace{a(n)e^{-ny/2}}_{replace\ by\ 1} \cdot e^{-ny/2}$$
- (New HW.) Assuming the functional equation (i.e. $\varphi(s) = stuff \cdot \psi(k-s)$), Stirling's formula, and Phragmen-Lindelöf, but not assuming Hecke's theorem, you can show that $|\varphi(s)| = O(|t|^M)$ in vertical strips.
- Important case: assume that $a(0) = b(0) = 0$. Break up
$$\Phi(s) = \int_0^{\infty} f(iy)y^{-s}\,\mathrm{d}s = \int_1^{\infty} + \int_0^1$$
We know that $f(iy)$ is rapidly decreasing, so $\int_1^{\infty}$ is absolutely convergent. Convert $\int_0^1$ into a similar integral with bounds $\int_1^{\infty}$ that is absolutely convergent.
- Assume that $a(0) = b(0) = 0$. From what we've just said, we know that $\Phi(s)$ is bounded in vertical strips. Also, it satisfies the functional equation $\Phi(s) = \varepsilon\Psi(k-s)$. You can show
$$\varepsilon g\left(\frac{-1}{z}\right) = \left(\frac{z}{i}\right)^k f(z)$$
We have:
$$f(iy) = \frac{1}{2\pi i}\int_{\sigma - i\infty}^{\sigma + i\infty} y^{-s}\Phi(s)\,\mathrm{d}s$$

$$g(iy) = \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} y^{-s}\Psi(s)\,\mathrm{d}s$$

for $\sigma \gg 0$. But this isn't so useful if we want to use $\Phi(s) = \varepsilon\Psi(k-s)$. First, think of $\int_{\sigma-i\infty}^{\sigma+i\infty}$ as a limit of $\int_{\sigma-iT}^{\sigma+iT}$. We'll have to move σ far to the left, so that $k-s$ corresponds to something that is safe for Φ. Let $\sigma > k$. Integrate around the box with vertices $\{-\sigma \pm iT, \sigma \pm iT\}$. The claim is that the contribution of the horizontal bits goes to zero as $T \to \infty$, so you end up integrating

$$\lim_{T\to\infty}\left(\int_{-\sigma-iT}^{-\sigma+iT} y^{-s}\Phi(s)\,\mathrm{d}s - \int_{\sigma-iT}^{\sigma+iT} y^{-s}\Phi(s)\,\mathrm{d}s\right) = \mathit{Residue}$$

If you integrate along the top edge of the rectangle you get

$$\left|\int_{-\sigma_0+iT}^{+\sigma_0+iT} y^{s}\Phi(s)\,\mathrm{d}s\right| \leq \int y^{\sigma}\left(\frac{\lambda}{2\pi}\right)^{\sigma}|\Phi(s)|\cdot|\varphi(s)|\,\mathrm{d}\sigma$$

By Phragmen-Lindelöf, and maybe Stirling, we have $\varphi(s) = O(t^M)$. By Stirling, $\Gamma(s) = e^{-\frac{\pi}{2}t}$. The integral

$$\int_{\mathrm{Re}(s)=\sigma_0} y^{\sigma}\left(\frac{\lambda}{2\pi}\right)^{\sigma}\,\mathrm{d}\sigma$$

is just a constant. So you get a bound out of the other two parts. This bound goes to zero as $T \to \infty$. Eventually, you've shown that you can move the line of integration from $+\sigma$ to $-\sigma$.

- Hint for Carl's problem: you're trying to switch the order of summation in

$$\int_0^\infty \frac{\sum \sin(2\pi nx)}{n\pi x^{s+1}}\,\mathrm{d}x$$

Break this up into

$$\int_0^B + \int_B^\infty$$

where you can use the dominated convergence theorem on the first part, and the second part should go to zero. Use lemma (D.1) in the book to help bound the partial sums.

8.3. Entire holomorphic functions (Levent). References: Elkies' Math 229 in 2009

DEFINITION 8.4. Let $p_i \in \mathbb{C}$. We say that $\sum_{i=1}^\infty p_i$ converges to $p \neq 0$ iff

$$\lim_{N\to\infty}\prod_{i\leq N} p_i \to p$$

If any $p_i = 0$, then say the product is zero. Now, assume that none of the terms are zero.

Proposition 8.5. $\prod_{n\geq 1}(1+a_n)$ converges iff $\sum_{n\geq 1}\log(1+a_n) < \infty$.

PROOF. ($\Longleftarrow$) $\exp(\sum_1^N \log(1+a_n)) = \prod_1^N (1+a_n)$

($\implies$) Fix a branch of log. Write $P_n = \prod_{i=1}^{n} p_i$, and $P = \lim P_i$. We know that $P_n/P \to 1$. Write $s_n = \sum_{i=1}^{n} \log(1 + a_i)$. Define the integer h_n by

$$\log P_n - \log P + 2\pi i h_n = S_n$$

But also

$$2\pi i(h_{n+1} - h_n) = \log(P_{n+1}/P) - \log(P_n/P) \to 0$$

For n sufficiently large, $|2\pi i(h_{n+1} - h_n)| < \pi$, which implies that $h_{n+1} = h_n$. □

DEFINITION 8.6. $\prod(1 + a_n)$ converges absolutely if $\sum |\log(1 + a_n)| < \infty$.

Proposition 8.7. $\prod(1 + a_n)$ converges absolutely iff $\sum |a_n| < \infty$.

Lemma 8.8. Let f be entire and holomorphic such that $f \neq 0$ anywhere. Then there is some g that is entire and holomorphic such that $f = exp(g)$.

Corollary 8.9. Let f be entire and holomorphic, with zeroes at $a_1 \cdots a_n$. Then there is some $m \in \mathbb{N}$, and g entire such that

$$f = z^m e^g \prod_{i=1}^{n} \left(1 - \frac{z}{a_n}\right)$$

Note: this product converges absolutely iff $\sum \frac{1}{a_n}$ converges absolutely.

Theorem 8.10. Let f be entire, $\{a_n\}$ its zeroes. Then: there exists $m \in \mathbb{N}$, polynomials $p_n(z)$, and an entire function g such that

$$f(z) = z^m e^{g(s)} \prod_{n=1}^{\infty} \left(1 - \frac{z}{m}\right) e^{p_n(z)}$$

Moreover, if $\{a_n\}$ is a sequence of complex numbers such that $|a_n| \to \infty$, then there exists $m_n \in \mathbb{N}$ such that

$$\prod_{n=}^{\infty} \left(1 - \frac{1}{a^n}\right) \exp\left(\frac{z}{a_n} + \frac{1}{2}\left(\frac{z}{a_n}\right)^2 + \cdots + \frac{1}{m^n}\left(\frac{z}{a_n}\right)^{m_n}\right)$$

converges to an entire function.

Note: one can choose p_n to have degree h iff $\sum \frac{1}{|a_n|^{n+1}}$ converges.

9. February 21

9.1. More on Weierstrass' theorem.

Theorem 9.1. Let a_n be nonzero complex numbers, where $|a_n| \to \infty$. Then

(1) There exist $p_n(z)$ for which $\prod \left(1 - \frac{z}{a_n}\right) e^{p_m(z)}$ converges uniformly (absolutely) to an entire function;
(2) If $f \neq 0$ is entire, and $\{a_n\}$ are its (nonzero) zeroes with multiplicity, then there exist $m \in \mathbb{N}$, a sequence $m_n \in \mathbb{N}$, and an entire function g such that

$$f(z) = e^{g(z)} z^m \prod \left(1 - \frac{z}{a_n}\right) e^{-\left(\frac{z}{a_n} + \frac{1}{2}\left(\frac{z}{a_n}\right)^2 + \cdots + \frac{1}{m_n}\left(\frac{z}{a_n}\right)^{m_n}\right)}$$

General idea: if there are finitely many $a_n \neq 0$, then you can write

$$f(z) = z^m \prod \left(1 - \frac{z}{a_n}\right) \times \textit{entire function}$$

where m is the order of vanishing (if at all) at zero, and the entire function can be written $e^{something}$. When we introduce infinitely many zeroes $a_n \neq 0$, then we need to worry whether $\prod \left(1 - \frac{z}{a_n}\right)$ converges. In general, it doesn't. But I claim that we can fix this by multiplying by $e^{polynomial}$. To see this, use the "definition" from last time that says that you can check convergence of products by first taking the log, and then checking convergence of the resulting sum. After taking logs, we want

$$\sum \left|\log\left(1 - \frac{z}{m}\right)\right| + \textit{polynomial}$$

to converge for some polynomial. In fact, this polynomial can be solved for by writing out the Taylor expansion for log.

REMARK 9.2. An interesting case is when $m_n = h$ (i.e. each "fudge" polynomial is the same length). In this case, the minimal such h is called the genus of $\{a_n\}$. If f is entire, such an h exists, and g is a polynomial, then the genus of f is $\max\{h, \deg g\}$. The point is that you can measure this, up to an order of 1, thanks to an estimate of Hadamard that measures growth rate.

Suppose $|f| \leq O(\exp |z|^a)$. The aim is to recover a.

DEFINITION 9.3. Let f be entire. Let $M(r) = \sup_{|z| \leq r} |f(z)|$. Then the order of f is

$$\lambda = \limsup_{r \to \infty} \frac{\log \log M(r)}{\log r}$$

Alternatively, λ is minimal such that, for all $\varepsilon > 0$,

$$|f| \leq O(\exp |z|^{\lambda + \varepsilon})$$

This is something we can actually measure!

Theorem 9.4 (Hadamard)**.** Let f be entire. Then $\lambda < \infty \iff h < \infty$, and in this case,

$$h \leq \lambda \leq h + 1$$

EXAMPLE 9.5. Recall that Euler used the factorization

$$\sin(\pi z) = \pi z \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2}\right)$$

to find $\zeta(2)$. We know where the zeroes of $\sin \pi z$ are: they are just the integers, and so a_n are the integers. Euler knew that $\sum \frac{1}{n^2}$ converges. We can take $h = 1$. Since $\sin \pi z$ has a simple zero at each integer,

$$\begin{aligned}\sin(\pi z) &= z e^g \prod_{n \neq 0} \left(1 - \frac{z}{n}\right) e^{\frac{z}{n}} \\ &= z e^g \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2}\right)\end{aligned}$$

Let's take logarithmic derivatives, and ignore convergence issues:

$$\cot(\pi z) = \frac{1}{z} + g'(z) + \sum_{n=1}^{\infty} \left(\frac{1}{n} + \frac{1}{z-n}\right)$$

By the expansion of cot, or using the Hadamard factorization theorem (which implies that g has degree at least $1\ldots$), this is also $\frac{1}{z} + \sum_{n \neq 0} \frac{1}{n} + \frac{1}{z-n}$. So g' is identically zero, and g is constant. Note that $\frac{\sin(\pi z)}{z} \to \pi$ as $z \to 0$, and $e^g = \pi$.

9.2. The Riemann ξ function. Recall the Weierstrass product expansion of the gamma function:

$$\Gamma(s) = \frac{e^{-Cs}}{s} \prod_{n=1}^{\infty} \frac{e^{\frac{s}{n}}}{1 + \frac{s}{n}}$$

It has a pole at zero, and at every negative integer. Levent's g is e^{-Cs}. We can check the formula

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$$

If you unfold this, you will get Euler's formula. Plausibility check: there's a simple pole at every integer on the RHS, and on the LHS $\Gamma(s)$ gives the poles at nonpositive integers and $\Gamma(1-s)$ gives the poles at positive integers. Or, you can write it as

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(1 - \frac{s}{2}\right) = \frac{\pi}{\sin\left(\frac{\pi s}{2}\right)} \tag{9.1}$$

and

$$\Gamma(s)\Gamma\left(s + \frac{1}{2}\right) = \pi^{-\frac{1}{2}} 2^{1-2s} \Gamma(2s)$$

Riemann didn't define the ζ function; he defined the $\xi(s)$ function:

$$\xi(s) = \frac{1}{2} s(s-1) \underbrace{\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \cdot \zeta(s)}_{our\ \Lambda(s)}$$

Having killed the poles, $\xi(s)$ is entire, and it satisfies a functional equation:

$$\xi(s) = \xi(1-s)$$

We also have

$$\xi(\overline{s}) = \overline{\xi(s)} \qquad \Longrightarrow \qquad \xi(s) = \xi(1-\overline{s})$$

If ρ is a zero of $\xi(s)$, then the usual notation is to write $\rho = \beta + i\gamma$, and $1-\rho$ and $\overline{\rho}$ are zeroes. So related zeroes are:

$$\beta + i\gamma \qquad 1-\beta-i\gamma \qquad \beta - i\gamma \qquad 1-\beta+i\gamma$$

So if you have a zero that's off the line $\mathrm{Re}(s) = \frac{1}{2}$, then there's another one on the other side.

Theorem 9.6.

$$\zeta(s) = \underbrace{2^s \cdot \pi^{s-1}\Gamma(1-s)\sin\left(\frac{\pi s}{2}\right)}_{\substack{\text{stuff relating to the} \\ \text{functional equations of } \xi}} \zeta(1-s)$$

We might call this an inhomogeneous functional equation.

PROOF. A nuisance. But you just use the original functional equation of ξ, plus the prior formulas for $\Gamma(s)$.

In the formula for ξ, we can ignore $\frac{1}{2}s(s-1)$, because it's symmetric around $\frac{1}{2}$.

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{\frac{s-1}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

$$\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{s-\frac{1}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

$$\zeta(s) = \pi^{s-\frac{1}{2}}\frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\frac{s}{2}}\zeta(1-s)$$

But we have a formula for the fraction term, gotten by rearranging (9.1), and multiplying both sides by $\Gamma\left(\frac{1-s}{2}\right)$:

$$\frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)} = \Gamma\left(\frac{1-s}{2}\right)\frac{1}{\pi}\Gamma\left(1-\frac{s}{2}\right)\cdot\sin\left(\frac{\pi s}{2}\right)$$

which we plug in to get

$$\zeta(s) = \pi^{s-\frac{1}{2}}\Gamma\left(\frac{1-s}{2}\right)\frac{1}{\pi}\cdot\Gamma\left(1-\frac{s}{2}\right)\cdot\sin\frac{\pi s}{2}\cdot\zeta(1-s)$$

I claim we're done, by Legendre's formula

$$\Gamma\left(\frac{s}{2}\right)\cdot\Gamma\left(\frac{s+1}{2}\right) = \pi^{-\frac{1}{2}}2^{1-s}\Gamma(s)$$

in which we can replace s by $1-s$:

$$\Gamma\left(\frac{1-s}{2}\right)\cdot\Gamma\left(1-\frac{s}{2}\right) = \pi^{-\frac{1}{2}}2^{s}\Gamma(1-s)$$

Plug in and compare with what we want. All the terms are there; you can do the bookkeeping. □

9.3. Zeroes and poles of ζ. We know that ζ has a simple pole at $s = 1$. Beyond this line, there are no zeroes or poles. By what we just proved about the symmetry of the zeroes, $\zeta(1-s)$ does not contribute any zeroes to the left of $\sigma = 0$ (we're following the formula for ζ in the theorem.) $\sin\left(\frac{\pi s}{2}\right)$ has a zero at every even integer. $\Gamma(1-s)$ has a simple pole at all positive integers, and no zeroes. These poles cancel out the zeroes, except at the even negative integers. These are called the trivial zeroes of ζ. Other than these, there are no zeroes to the left of $\sigma = 0$. So there is a *critical strip* $0 \leq \sigma \leq 1$, where we don't know where the zeroes are. (It has been proven that there are no zeroes on the boundary lines.)

9.4. Bernoulli numbers. Curiously, Jacob Bernoulli introduced the numbers as the constant terms of polynomials, whose *growth* was studied. They appear everywhere: the numerators are related to the number of differentiable structures on spheres; the denominators are related to the image of the J-homomorphism in algebraic topology. Define

$$S_R(n) = \sum_{1 \leq a < n} a^k$$

This is a polynomial

$$\frac{1}{k+1} n^{k+1} + \cdots + (\pm B_k) \cdot n$$

where B_k, the Bernoulli number, is defined as above, as a part of the constant term in this polynomial. The Bernoulli numbers also arise in the generating function:

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{k=1}^{\infty} B_{2k} \frac{x^{2k}}{(2k)!}$$

(You can use the generating function form to prove that the coefficients are rational.) All the odd terms (except $B_1 = -\frac{1}{2}$) are zero, so we often write the Bernoulli numbers as B_{2k}. There are other useful formulas:

$$B_{2k} = -2(2k)!(2\pi i)^{-2k} \zeta(2k) n^{-2k}$$

We know that $\zeta(1-2k)$ is related to $\zeta(2k)$; this gives rise to a formula

$$-\frac{B_{2k}}{2k} = \zeta(1-2k)$$

9.5. Facts about the logarithmic derivative. Consider the operator

$$\mathcal{D} : f \mapsto \frac{f'}{f} = \frac{d}{dz} \log f(z)$$

Useful properties:

$$\mathcal{D}(fg) = \mathcal{D}(f) + \mathcal{D}(g)$$
$$\mathcal{D}((z-a)^m) = \frac{m}{z-a}$$

That is, $\oint_a \mathcal{D}((z-a)^m)\, \mathrm{d}z = m$. Since $\mathcal{D}$ is logarithmic, this counts multiplicities for any function. If $f(z) = (z-a)^m \cdot g(z)$, where $g(z)$ is regular and nonzero at $z = a$, then $\mathcal{D}f(z)$ has the same property:

$$\mathcal{D}f(z) = \frac{m}{z-a} + \text{regular part}$$

If $f(z)$ is analytic in the neighborhood of some contour, and has poles inside, then

$$\frac{1}{2\pi i}\int_0 \mathcal{D}f(z)\,\mathrm{d}z = \text{ algebraic sum of multiplicities}$$

EXAMPLE 9.7. Let $\sigma > 1$, and integrate

$$\int_\sigma \mathcal{D}\zeta(s)\cdot\frac{x^s}{s}\,\mathrm{d}s$$

Once we do this, we will get an explicit formula for sums of logs of primes up to x.

10. February 23

Let $f(s)$ be a meromorphic function. Let $\mathcal{D}$ be the logarithmic derivative:

$$f(s) \xrightarrow{\mathcal{D}} \mathcal{D}f(s) = \frac{f'}{f}(s) = \frac{d}{ds}\log f$$

Note that

$$\mathcal{D}((s-s_0)^m) = \frac{m}{s-s_0}$$

In particular, if $f(s)$ has a pole or zero at s_0, you can write it as $(s-s_0)^m g(s)$ where $g(s)$ has no zeroes or poles in a neighborhood of s_0. Then

$$\mathcal{D}(s-s_0)^m\cdot g(s) = \frac{m}{s-s_0} + \mathcal{D}g(s)$$

where $\mathcal{D}g(s)$ is harmless. Now consider a contour γ around some points m_i that are zeroes or poles. Integrating around γ is the same as integrating around a little neighborhood of each point. So you get

$$\mathcal{D}f(s) = \sum_i \frac{m_i}{s-s_i} + \text{something harmless}$$

Now let $h(s)$ be holomorphic in the region in question.

$$\frac{1}{2\pi i}\int_C \mathcal{D}f(s)\cdot h(s)\,\mathrm{d}s = m_1h(s_1) + \cdots + m_\nu h(s_\nu)$$

If $h(s)$ is meromorphic, then there will be an extra contribution corresponding to the poles of h.

We had a Dirichlet series for $\sigma > 1$:

$$\frac{\zeta'}{\zeta}(s) = -\sum_{n=1}^{\infty}\Lambda(n)\cdot n^{-s}$$

where we had defined

$$\Lambda(n) = \begin{cases}\log p & \text{if} n = p^e\\ 0 & \text{else}\end{cases}$$

Now use the filter:

$$-\frac{1}{2\pi i}\lim_{T\to\infty}\int_{\sigma_0-iT}^{\sigma_0+iT}\frac{\zeta'}{\zeta}(s)\frac{x^s}{s}\,\mathrm{d}s = \frac{1}{2\pi i}\lim_T\int_{\sigma_0-iT}^{\sigma_0+iT}\sum_{n=1}^{\infty}\Lambda(n)\frac{\left(\frac{x}{n}\right)^s}{s}\,\mathrm{d}s$$

Commuting sum and integration as in Perron's formula, this is just $\psi'(x) = \frac{1}{2}(\psi(x+) + \psi(x-))$, where $\psi(x) = \sum_{n \leq x} \Lambda(n)$.

We know that $\zeta(s)$ has a pole at $s = 1$, might have zeroes ρ in the critical strip $0 < \sigma < 1$, and has zeroes at the negative even integers. Assume $\sigma_0 > 1$. The idea is to replace integration on the line $\sigma = \sigma_0$ with integration on a line far to the left. To do this, integrate along a rectangular contour with vertices $\{\sigma_0 \pm iT, \sigma_1 \pm iT\}$, where we take $\lim_{\sigma_1 \to -\infty}$. You have to be careful that σ_1 never falls on a negative even integer. Let's ignore this for the moment.

Just read the textbook. To recap, the idea is to evaluate $\psi'(x) = -\frac{1}{2\pi i} \int_{\sigma_0} \mathcal{D}\zeta(s) \frac{x^s}{s} \, \mathrm{d}s$ by evaluating the contour over an expanding rectangle in such a way that the horizontal components are zero. This contour is completely determined by the parameters σ_0, σ_1, T. Choose

$$\sigma_0 = 1 + \frac{1}{\log x}$$

You can't just choose any random T. Instead, in any interval $[T, T+1]$, we can find a "good" T, which we will notate T_1. Similarly, for σ_1 you also have to keep away from the zeroes. Just let σ_1 be the negative odd integers.

$$\int_{\sigma_0 - iT_1}^{\sigma_0 + iT_1} = \int_{side1} + \int_{side2} + \int_{side3} + \text{residues}$$

At $s = 0$, $\frac{x^s}{s}$ has a pole, and you get a residue $\frac{\zeta'}{\zeta}(0)$. At the negative integers $s = -2k$, the residue is the multiplicity of the zero, so we get a contribution of $-\frac{x^{-2k}}{2k}$. At $s = 1$, ζ has a pole (so $\frac{\zeta'}{\zeta}$ has a zero), and we get a contribution of $-x$. At $s = \rho$ (any zero in the critical strip, counted with multiplicity), we get a contribution of $\frac{x^\rho}{\rho}$. Unrigorously,

$$\psi'(x) = x - \sum \frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0) + \sum_{k=1}^{\infty} \frac{x^{-2k}}{2k}$$

Now clean this up. Just using the Taylor expansion of log, we have

$$\sum_{k=1}^{\infty} \frac{x^{-2k}}{2k} = -\frac{1}{2} \log\left(1 - \frac{1}{x^2}\right)$$

Define

$$s(x) = \frac{\zeta'}{\zeta}(0) + \frac{1}{2} \log\left(1 - \frac{1}{x^2}\right)$$

This is a smooth function. As $x \to \infty$, this goes to $\frac{\zeta'}{\zeta}(0)$; so it's basically a constant for large x.

Recall that every zero $\rho = \beta + i\gamma$ has a companion zero $\overline{\rho} = \beta - i\gamma$. So

$$\psi'(x) = x - \lim_{T \to \infty} x - \sum_{|\gamma| \leq T} \frac{x^\rho}{\rho} - s(x)$$

This illustrates a general principle: whenever your abscissa is too large, you can try to pull the line further to the left by taking a contour integral, and counting the residues inside.

Let's talk about $\sum_{|\gamma|\leq T} \frac{x^\rho}{\rho}$.

Theorem 10.1 ("The not-too-many-zeroes theorem")**.** If ρ are the nontrivial zeroes of $\zeta(s)$, counted with multiplicity, then

$$\sum_\rho \frac{1}{|\rho|^{1+\varepsilon}} < +\infty$$

for any ε.

We won't prove this now, but here's a corollary.

Corollary 10.2. If γ is the imaginary part of the corresponding ρ, then

$$\sum_{|\gamma|\leq T} \frac{1}{|\rho|} \ll T^\varepsilon$$

for any $\varepsilon > 0$.

PROOF.

$$(2T)^\varepsilon \sum_{|\gamma|\leq T} \frac{1}{|\rho|^{1+\varepsilon}} = \sum \frac{\left(\frac{(2T)}{|\rho|}\right)^\varepsilon}{|\rho|} \geq \sum_{|\gamma|\leq T} \frac{1}{|\rho|}$$

□

10.1. Explicit formula. Let

$$R(x,T) := \psi'(x) - x + \sum_{|\gamma|\leq T} \frac{x^\rho}{\rho} + s(x)$$

Theorem 10.3. Fix x. Then $R(x,T) \to 0$ as $T \to \infty$.

But, we can do better. Recall $R(x,T)$ is gotten by integrating three sides of a contour integral. Define

$$m(x,T) = \min\left\{1, \tfrac{x}{T\cdot\langle x\rangle}\right\}$$

where $\langle x\rangle$ is defined to be the distance between x and the nearest prime power, except if x is a prime power, in which case you go to the closest other prime power. (The issue is that ψ' jumps at prime powers.)

Theorem 10.4.

$$R(x,T) \ll \frac{x}{T}(\log x)^2 + m(x,T)\cdot \log x$$

where $\ll$ is to be interpreted as x, T both tending towards ∞.

We won't prove this now either.

Let $T \geq x^{\frac{1}{2}+\delta}$.

$$R(x,T) \ll \sqrt{x}$$

because all the log terms are insignificant compared to any $x^{something}$. This gives an estimate

$$\psi'(x) = x - \sum_{|\gamma|\leq x^{\frac{1}{2}+\delta}} \frac{x^\rho}{\rho} + O(\sqrt{x})$$

So this says that you don't have to compute that many zeroes to get a decent approximation.

10.2. Zero-free regions.

HYPOTHESIS 10.5. For $\frac{1}{2} < \alpha < 1$, there are no zeroes $\rho = \beta + i\gamma$ with $\beta \geq \alpha$.

(Call this "hypothesis α", where the Riemann hypothesis is "hypothesis $\frac{1}{2}$".)

$$\psi'(x) = \psi(x) = x - \sum \frac{x^\rho}{\rho} + O(x^{\frac{1}{2}+\delta})$$

The aim is to estimate $\sum \frac{x^\rho}{\rho}$, where $x^\rho = x^\beta \cdot x^{i\gamma}$, where $\beta \leq \alpha$. So

$$\left| x^{-\alpha} \sum_\rho \frac{x^{\beta+i\gamma}}{\rho} \right| \leq \sum \frac{x^{\beta-\alpha}}{|\rho|} \underbrace{\sum \frac{1}{|\rho|}}_{\ll T^\varepsilon}$$

so

$$\sum \frac{x^\rho}{\rho} \ll x^{\alpha+\delta}$$

for small δ.

It has been proven that there are no zeroes on the line $s = 1$. Hypothesis α gives

$$\psi(x) = x + O(x^{\alpha+\delta})$$

Every time you have a zero-free region, you get an estimate for $\sum \frac{x^\rho}{\rho}$.

We're interested in counting primes: finding $\pi(x)$. We have some chance of understanding $\psi(x)$, and we will see that this informs you about $\pi(x)$.

11. March 1

11.1. Tony. Recall we had defined

$$\Lambda(s) = \pi^{\frac{-s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

which satisfies the functional equation

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

The growth of Λ is dominated by the gamma term. Define $\xi(s) = \frac{s(s-1)}{2}\Lambda(s)$. Recall that the *order* of f is

$$\limsup_{r\to\infty} \frac{\log\log M_r|f|}{\log r}$$

If $|f| \approx e^{|t|^a}$ then this picks out the a.

Proposition 11.1.

$$order(\xi) = 1$$

We will do this by showing

(1) There is no c such that $|\xi(s)| \ll e^{c|s|}$
(2) There is some c' such that $|\xi(s)| \ll e^{c'|s|\log|s|}$

Along $\mathbb{R}$, $|\zeta(s)| = 1^{-s} + \cdots \geq 1$, so this doesn't really slow the growth rate. Stirling's approximation says that

$$n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$$

This dwarfs any exponential, which proves (1). It also means that

$$|\Gamma\left(\frac{s}{2}\right)| \ll e^{c'|s|\log|s|}$$

Now we need a bound for the zeta function. It suffices to show, then, that

$$|\zeta(s)| \ll |\zeta(|s|)| \ll D$$

sufficiently far to the right. Write

$$\zeta(s) = \sum \frac{1}{n^s} + \frac{1}{s-1} + \underbrace{\int_1^\infty x^{-s}\,\mathrm{d}x}_{\frac{x^{1-s}}{1-s}\Big|_0^\infty}$$

$$= \frac{1}{s-1} + \sum_{n=1}^{\infty}\int_n^{n+1} \underbrace{\frac{1}{n^s} - \frac{1}{x^s}}_{s\int_n^\infty \frac{1}{y^{s+1}}\,\mathrm{d}y}\,\mathrm{d}x$$

That is,

$$\left|\frac{s(s-1)}{2}\xi(s)\right| \leq \left|\frac{s}{2}\right| + \left|\frac{s^2(s-1)}{2}\right| \sum_{n=1}^{\infty}\int_n^{n+1}\int_n^x \frac{1}{y^{\sigma+1}}\,\mathrm{d}y\,\mathrm{d}x$$

We have

$$\left|\frac{1}{n^s} - \frac{1}{x^s}\right| \leq |s| \underbrace{\int_n^\infty \frac{1}{|y^{s+1}|}\,\mathrm{d}y}_{n^\sigma}$$

and $\int_1^\infty \frac{1}{y^{\sigma+1}}\,\mathrm{d}y = C$.

REMARK 11.2.

You can get zeroes of zeta in Mathematica as `ZetaZero[z]`.

11.2. Chebyshev.

NOTATION 11.3. We say $f(x) \asymp g(x)$ if there exist $c_1, c_2 > 0$ such that

$$c_2 g(x) < f(x) < c_1 g(x)$$

for x sufficiently large.

DEFINITION 11.4.

(1) $\pi(X) = \sum_{p \leq X} 1$
(2) $\theta(x) = \sum_{p \leq X} \log p$
(3) $\psi(x) = \sum_{n \leq X} \Lambda(n) = \sum_{p^e \leq X} \log p$

OBVIOUS 11.5.

$$\pi(X) \leq \theta(X) \leq \psi(X)$$

There is a formula for $\pi(X)$ in terms of the zeroes of zeta, but it is complicated. Easier is to use $\psi(X)$ to approximate $\theta(X)$, and $\theta(X)$ to approximate $\pi(X)$. The goal:

Theorem 11.6.

(1) $\theta(X) = \psi(X) + O(X^{\frac{1}{2}})$
(2) $\pi(X) = \frac{\psi(X)}{\log X} + O\left(\frac{X}{(\log X)^2}\right)$

This can be used to show

Theorem 11.7.

$$\psi(x) \asymp x$$

Recall that $\sum_{d|n} \Lambda(d) = \log n$. By Moebius transformations, we can write

$$\Lambda(n) = \sum_{d|n} \mu(d) \cdot \log \frac{n}{d}$$

which gives an alternate form of

$$\psi(x) = \sum_{n \le x} \Lambda(n) = \sum_{n \le x} \sum_{d|n} \mu(d) \cdot \log \frac{n}{d}$$
$$= \sum_{d \le x} \mu(d) \cdot \sum_{\frac{n}{d} \le \frac{x}{d}} \log \frac{n}{d}$$

We're going to make approximations to the Moebius functions, which we call mock Moebius functions. First, start with any $d \mapsto m(d)$, and denote

$$\psi_m(x) = \sum_{d \le x} m(d) \cdot \sum_{\substack{d|n \\ \frac{n}{d} \le \frac{x}{d}}} \log \frac{n}{d}$$

Now we restrict $m(d)$ by setting restrictions on the resulting $\psi_m(x)$. Let

$$T(x) = \sum_{a \le x} \log a$$

and in particular we care about

$$T\left(\frac{x}{d}\right) = \sum_{\substack{d|n \\ \frac{n}{d} \le \frac{x}{d}}} \log \frac{n}{d}$$

Approximate $T(x)$ by $\int_1^x \log t \, \mathrm{d}t = x \log x - x$ which gives the bound

$$N \log N - N \le T(N) \le (N+1)\log(N+1) - N - 1$$
$$T\left(\frac{x}{d}\right) = \sum_{\substack{d|n \\ \frac{n}{d} \le \frac{x}{d}}} \log \frac{n}{d} = N \log N + \text{a small error term of about } \log 2N$$

From now on, let O denote $O(\log 2N)$.

Now we get to impose a condition on m: we want $m(d) = 0$ for d sufficiently large (i.e. m has compact support).

$$\psi_m(d) = \sum m(d) \cdot T\left(\frac{x}{d}\right) = \sum_{d \le x} m(d) \left(\frac{x}{d} \log \frac{x}{d} - \frac{x}{d}\right) + O$$
$$= \sum \frac{m(d)}{d} x \cdot \log x - \sum \frac{m(d)}{d} \cdot x \log d - \sum_{d \le x} m(d) \frac{x}{d} \qquad \text{separating } \log \tfrac{x}{d}$$
$$= (x \log x - x) \cdot A + x \cdot B$$

where $A = \sum_{d \le x} \frac{m(d)}{d}$ and $B(x) = -\sum_{d \le x} \frac{m(d) \log d}{d}$.

We want $B = 1$, and $A \to 0$. So require

HYPOTHESIS 11.8. $A(x) = \sum_{d \le x} \frac{m(d)}{d} = 0$ for x large.

HYPOTHESIS 11.9. $B(x) = 1$

Under these restrictions, we have that $\psi_m(x) \sim x + O$.

Proposition 11.10.

$$\psi_m \asymp \psi$$

We are done if we show this, and show that there is some $m(d)$ meeting our hypotheses. At this point, just assume that $m(d)$ satisfies our hypotheses.

$$\begin{aligned}
\psi_m(x) &= \sum_{d\le x} m(d) \sum_{\substack{\frac{\nu}{d}\le\frac{x}{d}\\ d|\nu}} \log\frac{\nu}{d} \\
&= \sum_{(d,n),dn\le x} m(d)\log n = \sum_{(d,n)\,:\,dn\le x} m(d)\sum_{k|n}\Lambda(k) \\
&= \sum_{(k,d,\nu)\,:\,kdv\le x} m(d)\Lambda(k) && \text{collect indices and replace } n=k \\
&= \sum_{k=1}^{[x]}\Lambda(k)\sum_{(d,\nu)\,:\,d\nu\le\frac{x}{k}} m(d) \\
&= \sum_{k=1}^{[x]}\Lambda(k)\sum_{d\le\frac{x}{k}} m(d)\cdot\left\lfloor\frac{x}{kd}\right\rfloor && \text{number of } \nu\text{'s is } \left\lfloor\frac{x}{kd}\right\rfloor
\end{aligned}$$

Set

$$F(y) = \sum_{d\le y} m(d)\left\lfloor\frac{y}{d}\right\rfloor$$

So our previous expression is $\sum_{k=1}^{[x]}\Lambda(k)\cdot F\left(\frac{x}{k}\right)$. Now use the second hypothesis on the mock-Moebius functions: we can write

$$F(y) = \sum_{d\le y} m(d)\frac{y}{d} - \sum_{d\le y} m(d)\frac{y}{d} = y\sum_{d=1}^{\infty}\frac{m(d)}{d} - \sum_{d\le y} m(d)\frac{y}{d} = 0 - \sum_{d\le y} m(d)\frac{y}{d}$$

Notice that $F(y)$ is periodic: $F(y+D) = F(y)$, where D is the least common multiple of all the d's such that $m(d)\neq 0$ (i.e. the d's that are "actually" in the sum).

$$\psi_m(x) = \sum\Lambda(k)\cdot F\left(\frac{x}{k}\right) \qquad \text{if } x \text{ is large}$$

The aim was to compare ψ_m to $\psi = \sum\Lambda(k)\cdot 1$. So we hope we can make $F\left(\frac{x}{k}\right)$ close to 1.

12. March 6

RECALL: we are interested in

$$\psi(x) = \sum_{n\le x}\Lambda(n) = \sum_{d\le x}\mu(d)\sum_{\substack{\frac{n}{d}\le\frac{x}{d}\\ d|n}}\log\frac{n}{d}$$

We imitate this by creating a "mock Moebius function" $m(d)$, which is chosen to satisfy certain axioms:

(1) $m(d)$ has finite support
(2) $\sum_{d=1}^{\infty} \frac{m(d)}{d} = 0$

Define

$$\psi_m(x) = \sum_{d \le x} m(d) \sum_{\substack{\frac{n}{d} \le \frac{x}{d} \\ d|n}} \log \frac{n}{d}$$

We had

$$\psi_m(x) = (x \log x - x) \sum_{d \le x} \frac{m(d)}{d} - x \, \mathrm{d} \sum_{d \le x} \frac{m(d) \log d}{d} + O(\log 2x)$$

We were trying to show that $\psi(x) \asymp x$ by way of showing $\psi_m(x) \asymp x$. The second "axiom" guarantees that the first term in $\psi_m(x)$ is eventually zero; ideally, we want $\sum_d \frac{m(d) \log d}{d} = -1$. We won't get this, but we can make it close to -1.

We want to transform ψ_m to make it look like ψ.

$$\begin{aligned}
\psi_m(x) &= \sum_{d \le x} m(d) \sum_{\substack{\frac{n}{d} \le \frac{x}{d} \\ d|n}} \log \frac{n}{d} \\
&= \sum_{dn \le x} m(d) \log n && \text{combine the two indices } n, d \text{ of summation into one sum} \\
&= \sum m(d) \cdot \sum_{k|n} \Lambda(k) \\
&= \sum_{dn \le x} m(d) \cdot \sum_{k|n} \Lambda(k) = \sum_{kdn \le x} m(d)\Lambda(k) \\
&= \sum_{k=1}^{x} \Lambda(k) \sum_{dn \le \frac{x}{k}} m(d) \\
&= \sum_{k=1}^{x} \Lambda(k) \sum_{d} m(d) \left[\frac{x}{kd}\right] && \text{How many } n \text{ are there?} \\
&= \sum_{k=1}^{x} \Lambda(k) F(x/k) && \text{define } F
\end{aligned}$$

That is, we've defined

$$\begin{aligned}
F(y) &= \sum m(d) \left[\frac{y}{d}\right] = \sum m(d) \left(\frac{y}{d} - \{\frac{y}{d}\}\right) \\
&= \underbrace{\sum m(d) \cdot \frac{y}{d}}_{0} - \sum m(d) \{\frac{y}{d}\} \\
&= -\sum m(d) \left\{\frac{y}{d}\right\}
\end{aligned}$$

This is a periodic function, with period $D = lcm\{d : m(d) \neq 0\}$. The simplest choice of $m(d)$ is:

$$m(1) = 1 \qquad m(2) = -2 \qquad m(d) = 0 \text{ if } d > 2$$

The period is 2. Assume $d \leq y$, so there is nothing at 0, the function is 1 for $y \in [1,2] \cup [3,4] \cup \cdots$ and zero elsewhere.

$$\psi_m(x) = \sum_{k=1}^{[x]} \Lambda(k) F\left(\tfrac{x}{k}\right)$$

If $x \geq k \geq \frac{x}{2}$ then $1 \leq \frac{x}{k} < 2$ and write

$$\psi_m(x) = \sum_{k=1}^{\frac{x}{2}} \Lambda(k) F\left(\frac{x}{k}\right) + \underbrace{\sum_{\frac{x}{2} < k \leq x} \Lambda(k)}_{\psi(x) - \psi\left(\frac{x}{2}\right)}$$

since $F\left(\frac{x}{k}\right) = 1$ in the second case. This gives

$$\psi(x) \geq \psi_m(x) \geq \psi(x) - \psi\left(\tfrac{x}{2}\right)$$

There is some constant c_m such that $\psi_m(x) = c_m x + O(\log x)$

$$\psi_m(x) = \sum_{j=0}^{\sim \log_2 x} \psi\left(\frac{x}{2^j}\right) - \psi\left(\frac{x}{2^{j+1}}\right) \leq c_m \sum_{j=1}^{\sim \log_2 x} \frac{x}{2^j} + O((\log x)^2)$$

This is gotten by plugging in the expression for $\psi_m(x)$, but noting that the error term compounds.

The claim is that any expression $\psi(x) \asymp x$, with whatever explicit constant, can give information about the $\pi(x) \leq \theta(x) \leq \psi(x)$ situation as

(1) $\theta(x) = \psi(x) + O(x^{\frac{1}{2}})$
(2) $\pi(x) = \frac{y(x)}{\log} x + O\left(\frac{x}{(\log x)^2}\right)$ which is essentially $\pi(x) = \frac{\psi(x)}{\log x} + o(x)$

$$\psi(x) = \sum_{p^k \leq x} \log p = \sum_{k=1}^{\infty} \theta(x^{\frac{1}{k}})$$

$$\psi(x) = \theta(x) + \sum_{k=2}^{\infty} \theta(x^{\frac{1}{k}})$$

Pull off the term for $k = 2$:

$$\psi(x) - \theta(x) \ll x^{\frac{1}{2}} + \underbrace{\sum_{k=3}^{\infty} \theta(x^{\frac{1}{k}})}_{x^{\frac{1}{3}} \sum_{k=3}^{\infty} x^{\frac{-1}{3}} \theta(x^{\frac{1}{k}})}$$

$\theta(x^{\frac{1}{k}})$ puts a $\log p$ for every prime p that occurs $\leq x^{\frac{1}{k}}$; the term $x^{\frac{-1}{3}}$ subsumes this. So $\sum_{k=3}^{\infty} x^{\frac{-1}{3}}\theta(x^{\frac{1}{k}}) \leq \log x$.

$$\begin{aligned}\pi(x) &= \int_{2-}^{x} \log(u)^{-1} \cdot d\theta(u) \\ &= \frac{\theta(x)}{\log x} - \int_{2}^{x} \theta(u) \cdot \underbrace{\mathrm{d}(\log u)^{-1}}_{\frac{1}{u \log u}}\end{aligned}$$

$$\pi(x) - \frac{\theta(x)}{\log x} = \pi(x) - \frac{\psi(x)}{\log x} + O\left(\frac{x^{\frac{1}{2}}}{\log x}\right)$$

We wanted to study $\pi(x) - \frac{\psi(x)}{\log x}$, but up to the error term, we can just study $\pi(x) - \frac{\theta(x)}{\log x}$. We have

$$\pi(x) - \frac{\theta(x)}{\log x} = -\int_{2-}^{x} \frac{\theta(u)}{u(\log u)^2\,\mathrm{d}u}$$

Since $\theta(u)$ is bounded by $const \cdot u$, this is

$$\cdots \ll \int_{2-}^{x} \frac{\mathrm{d}u}{(\log u)^2}$$

Estimate by

$$\int_{2-}^{x} \frac{\mathrm{d}u}{(\log u)^2} = \int_{2-}^{\sqrt{x}} + \underbrace{\int_{\sqrt{x}}^{x}}_{\text{bounded by } \int \frac{\mathrm{d}u}{(\log\sqrt{x})^2}}$$

so the first integral is essentially $\sqrt{x}$, and the second integral can be estimated by $\frac{x}{(\log x)^2}$. This gives statement (2).

12.1. Prime number theorem.

- **Find a zero-free region within the critical strip.**
- **Bounds for ζ in the zero-free region.**
- **Basic contour integrals.**
- **Compute error terms.**
- **Combine error terms.**

Take a safe vertical line $\sigma_0 > 1$, and a function $c(t)$ with $\frac{1}{2} < c(t) = c(-t) < 1$ with $c(|t|)$ monotone increasing, such that the wobbly strip $\mathcal{R}$ between $c(t)$ and the line $\sigma = \sigma_0 > 1$. The idea is that there should be no zeroes in the strip; so $\frac{1}{2} < c(t) < 1$. That is,

$$\mathcal{R} = \{s = \sigma + it \,:\, c(t) \leq \sigma \leq \sigma_0\}$$

Define a contour $\mathscr{C}$ that cuts out a wobbly rectangle with height between $t = \sigma + iT$ and $t = \sigma - iT$, and width bounded by σ_0 and $c(t)$. So this consists of two horizontal lines $\{\sigma \pm iT \,:\, c(t) \leq \sigma \leq \sigma_0\}$, and then a part of the line $\sigma = \sigma_0$ and part of the curve $c(t)$.

$$\frac{1}{2\pi i}\int_{\mathscr{C}} \frac{\zeta'}{\zeta}(s)\frac{x^s}{s}\,\mathrm{d}s = x$$

$$\psi(x) = \frac{-1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT} \frac{\zeta'}{\zeta}(s)\frac{x^s}{s}\,\mathrm{d}s + R(x,T)$$

where $R(x,T)$ is the error term from Perron's formula. The issue is to compute the integral over the other three sides; we will pick up error terms from each piece. Actually, we will make σ_0 a function of x, and move them to have more control over the error terms.

The region $\mathcal{R}$ contains the pole $s = 1$. Look for a specific $T_0 > 0$ (the book uses $\frac{7}{6}$). Call *the patch* the region bounding $s = 1$ by bounding the imaginary part by $-T_0 \le t \le T_0$; *the rest* will refer to, well, the rest. We have some estimates on the patch:

$$\frac{\zeta'}{\zeta}(s) = -\frac{1}{s-1} + O(1)$$

$$\frac{1}{\zeta(s)} \ll |s-1|$$

Outside the patch,

$$\frac{\zeta'}{\zeta}(s) \ll \log \tau$$

A zero of ζ would show up as a pole of $\frac{\zeta'}{\zeta}$; so this guarantees a zero-free region.

We will define $c(t) = 1 - \frac{constant}{\log \tau}$.

13. March 8

Recall from last time we described a hypothetical zero-free region, bounded on the right by the line $\sigma = \sigma_0$, on the left by some function $c(t)$ with $\frac{1}{2} < c(t) = c(-t) < 1$ where $c(|t|)$ is monotonically increasing, and bounded on the top and bottom by $\pm T$. This produces a contour $\mathcal{C}$. We're trying to integrate

$$x = -\frac{1}{2\pi i}\int_{\mathcal{C}(T)} \frac{\zeta'}{\zeta}(s)\frac{x^s}{s}\,\mathrm{d}s$$

The integral on the right can be done using Perron's formula, which gives an estimate for $\psi(x)$. The trick is to bound the others, and find the residue of the $s = 0$ pole; this will give an estimate for ψ in terms of other things.

To isolate the pole at 0, draw a rectangle around it, bounded vertically by $\pm T_0$, and call this the "patch".

Estimates on the patch:

- $\frac{\zeta'}{\zeta}(s) = -\frac{1}{s-1} + O(1)$
- $\log(\zeta(s)(s-1)) \ll 1$
- $\frac{1}{\zeta(s)} \ll |s-1|$

Estimate outside the patch:

- $\frac{\zeta'}{\zeta}(s) \ll \log \tau$

Label the contour $\mathcal{C}(T)$ as $\int_A + \int_B + \int_D + \int_C$ clockwise starting on the left.

Perron's formula:

$$\psi(x) = \int_{right} + \underbrace{R(x,T)}_{\ll \log x + \frac{x}{T}(\log x)^2}$$

On the top (assuming $T > T_0$ so we can use the estimate $\frac{\zeta'}{\zeta}(s) \ll \log \tau$, and assuming $x > 1$):

$$\int_{c(T)+iT}^{\sigma_0+iT} \frac{\zeta'}{\zeta}(s)\frac{x^s}{s}\,\mathrm{d}s \ll \int_{c(T)}^{\sigma_0} \log\tau \frac{|x^s|}{|s|}\,\mathrm{d}\sigma$$
$$\leq \int \log T \frac{x^{\sigma_0}}{T}\,\mathrm{d}\sigma \ll \frac{\log T}{T} x^{\sigma_0}(\sigma_0 - c(T)) \ll \frac{\log T}{T} x^{\sigma_0}$$

Break up the integral on the left into a few pieces, depending on whether we're in the patch or not.

$$\int_{c(T)-iT}^{c(T)+iT} = \int_{c(T)-iT_0}^{c(T)+iT_0} + \int_{c(T)-iT}^{c(T)-iT_0} + \int_{c(T)+iT_0}^{c(T)+iT}$$

First piece:

$$\int_{c(T_0)-iT_0}^{c(T_0)+iT_0} \underbrace{\frac{\zeta'}{\zeta}(s)}_{\approx \frac{1}{s-1}} \underbrace{\frac{x^s}{s}}_{\frac{\ll x^{c(T_0)}}{const.}}\,\mathrm{d}s \ll \int_{t=-T_0}^{t=+T_0} \frac{x^{c(T_0)}}{|c(T_0)+it-1|}\,\mathrm{d}t$$

$$\ll \frac{x^{c(T_0)}}{|1-c(T_0)|} \qquad \text{remove } it \text{ term}$$

Top part of this:

$$\int_{c(T)+iT_0}^{c(T)+iT} \frac{\zeta'}{\zeta}(s)\frac{x^s}{s}\,\mathrm{d}s \ll \int \log\tau \frac{x^{c(T)}}{\underbrace{c(T_0)+iT}_{denom. \approx t}}\,\mathrm{d}t \ll (\log T)^2 \cdot x^{c(T)}$$

Now add up the error terms we've gotten so far:

$$\psi(x) - x \ll \log x + \frac{x}{T}(\log x)^2 + \frac{\log T}{T}x^{\sigma_0} + \frac{x^{c(T)}}{1-c(T)} + x^{c(T)}(\log T)^2$$

For given x, chose T and σ_0 as functions of x. We can ignore the $\log x$ term, because it will always be beaten by the other terms. The problem is $\frac{\log T}{T}x^{\sigma_0}$, because $\sigma_0 > 1$.

Choose: $\sigma_0 = 1 + a(x)$, where $a(x) = \frac{1}{\log x}$.

Prove: If $T > 2$ then $c(T) = 1 - \delta(T)$ where $\delta(T) = \frac{c}{\log T}$ for $0 < c < 1$. (We will get a way of moving it around for $T < 2$.)

Take x out of the whole thing:

$$\psi(x) - x \ll x\left(\frac{(\log x)^2}{T} + \frac{\log T}{T}\underbrace{x^{\frac{1}{\log x}}}_{constant} + \frac{x^{-\delta(T)}}{\delta(T)} + x^{-\delta(T)(\log T)^2}\right)$$

The problematic error term turns into

$$\frac{x^{-\delta(T)}}{\delta(T)} \approx \frac{x^{-\frac{c}{\log T}}}{c} \cdot \log T$$

Do some bookkeeping, and you get

$$T = \exp(\sqrt{c \log x})$$

which gives an estimate

$$\psi(x) - x = O\left(\frac{x}{\exp(c'\sqrt{\log x})}\right)$$

(For the bound, see theorem 6.4 in the book. Read this!)

13.1. Heuristic argument for nonvanishing at $\sigma = 1$. Write

$$R(s) = \operatorname{Re}\frac{\zeta'}{\zeta}(s)$$

Assume $s = 1 + \delta + i\gamma > 1$, where we will be taking the limit $\delta \to 0$.

$$R(s) = -\sum \Lambda(n) n^{-1-\delta} \cdot \cos(\gamma \cdot \log n)$$

We know that $|R(1 + \delta + i\gamma)| \leq \mathbb{R}(1 + \delta)|$. Suppose ρ_0 is a zero of the form $1 + i\gamma_0$. Take $R(1 + \delta)$ close to the pole; you pick up a residue so $R(1 + \delta) \approx -\frac{1}{\delta}$. You have a zero at $1 + i\gamma$. So $R(1 + \delta + i\gamma_0) \approx \frac{1}{\delta}$. A lot of the cos terms are -1 at γ_0.

$$-R(1 + \delta + 2i\gamma_0) \approx \frac{1}{\delta}$$

So this has a pole here, which is a contradiction.

13.2. Actual argument. This starts with a trig formula:

$$\varphi(\theta) := 3 + 4\cos\theta + \cos 2\theta = 2(1 + \cos\theta)^2$$

(Use the fact that $1 + \cos 2\theta = 2\cos^2\theta$.)

$$-3R(1 + \delta) - 4R(1 + \delta + i\gamma) - R(1 + \delta + 2i\gamma) = \sum \Lambda(n) n^{-1-\delta} \underbrace{(\varphi(\gamma \cdot \log n))}_{\substack{\geq 0 \\ \text{because it's } 2 \times \text{ a square}}} \geq 0$$

Replace $\gamma = \gamma_0$, where $s = \beta_0 + i\gamma_0$ is a zero of $\zeta(s)$, where $\frac{5}{6} \leq \beta_0 \leq 1$ and $|\gamma_0| \geq \frac{7}{8}$. We won't prove the estimates in the following table:

	$-3R(1+\delta)$	$-4R(1+\delta+i\gamma)$	$-R(1+\delta+2i\gamma)$
Estimate	$\frac{3}{\delta}$	$-\frac{4}{\delta+1-\beta_0}$	0
Error	$O(1)$	$c_1 \cdot (\log\lvert\gamma_0\rvert + 4)$	$c_1 \cdot (\log\lvert 2\gamma_0\rvert + 4)$

$$\tau \approx \gamma_0$$

Set $C = c_1 \cdot (\log|\gamma_0| + 4)$ and take $\delta = \frac{1}{2C}$. Plugging everything in:

$$6C - \frac{4}{1 + \frac{1}{2c} - \beta_0} + C + C \geq 0$$

You eventually get

$$1 - \beta_0 \geq \frac{1}{14C}$$

The table is the application of a result described below. Let $f(z)$ be an analytic function on the disc $|z| \leq 1$, where $f(0) \neq 0$. Let $M = \max|f(z)|$. Choose a disc $D(0,R)$ inside. Then

Theorem 13.1.

$$\left| \frac{f'}{f}(z) - \sum_{\substack{\text{zeroes } z_k \\ \text{in } D(0,R)}} \frac{1}{z - z_k} \right| = O\left(\frac{M}{|f(0)|}\right)$$

14. March 20

14.1. Finite abelian groups. Let G be a finite abelian group; by the fundamental theorem of finite abelian groups, it can be written (non-uniquely) as a sum $C_1 \oplus \cdots \oplus C_\nu$ of finite cyclic groups. We can choose C_i to be the p_i-primary component, for p_i a prime factor.

Direct sum and direct product are not the same thing. If $G = G_1 \oplus G_2$, then G_1 and G_2 are two subgroups. If $G = G_1 \times G_2$, then there are quotients $G \twoheadrightarrow G_1$ and $G \twoheadrightarrow G_2$. Of course, if there are only finitly many factors, then $G_1 \times \cdots \times G_n$ and $G_1 \oplus \cdots \oplus G_n$ are isomorphic ... but they're "morally" different things and arise in different ways. (The book writes $\otimes$ instead of $\oplus$ ... oops.)

Let $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$ be the dual group. We would like a more symmetric definition. So let A and B be abelian groups. A bilinear pairing is a map

$$A \times B \xrightarrow{\psi} \mathbb{C}^* \text{ where } (a_1 a_2, b) \mapsto \psi(a_1, b) \cdot \psi(a_2, b)$$

Given $a \in A$, there is a map $A \to \widehat{B}$ that sends a to $\psi_a = \psi(a, -) \in \widehat{B}$. There is also an analogous map $B \to \widehat{A}$. If this is an isomorphism, it is called a *perfect pairing*.

Proposition 14.1.

$$\widehat{A \oplus B} = \widehat{A} \times \widehat{B}$$

PROOF. It is easy to show an isomorphism $\mathrm{Hom}(A \oplus B, \mathbb{C}^*) \cong \widehat{A} \times \widehat{B}$. □

If $C = \mathbb{Z}/n\mathbb{Z}$ is a finite cyclic group, then an element of $\widehat{C}$ is a root of unity; that is, $\widehat{C} = \{e^{\frac{2\pi i a}{n}}\}$. Clearly, $|C| = |\widehat{C}|$ here, so $C \cong \widehat{C}$. Using the previous proposition, we have

$$G \cong \widehat{G}$$

for any finite abelian group G.

Fix $g \in G$. Then

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = e \in G \\ 0 & \text{otherwise} \end{cases}$$

(If $g \neq e$, since our pairings are perfect, there is some χ_1 such that $\chi_1(g) \neq 1$. Then $\sum \chi(g) = \sum(\chi_1 \chi)(g) = \chi_1(g) \cdot \sum \chi(g) \implies \sum \chi(g) = 0$.) Temporarily let χ_0 be the trivial character (the identity) in $\widehat{G}$. For fixed χ,

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise} \end{cases}$$

Recall the Chinese Remainder Theorem: if $(a, b) = 1$ and $n = ab$, then there are r, s such that $1 = ra + sb$, and

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

where the backwards map is $(x, y) \mapsto sbx + rag$. There is a similar isomorphism between groups of units:

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$$

For the rest of this lecture, n will have a prime decomposition $\prod_{i=1}^{\nu} p_i^{e_i}$. Apply the Chinese Remainder Theorem, to write

$$G := (\mathbb{Z}/n\mathbb{Z})^* = \prod_{i=1}^{\nu} (\mathbb{Z}/p_i^{e^i})^* = \prod_{i=1}^{\nu} G_{p_i}$$

If $m \mid n$ then there is a natural reduction

$$(\mathbb{Z}/n\mathbb{Z})^* \twoheadrightarrow (\mathbb{Z}/m\mathbb{Z})^*$$

If $p > 2$, then

$$(\mathbb{Z}/p^e\mathbb{Z})^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times \Gamma$$

where Γ is the group of units congruent to 1 mod p; it is "canonically" cyclic of order p^{e-1}, with generator $1 + p$. For $p = 2$, this is

$$(\mathbb{Z}/2^e\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z})^* \times \Gamma$$

where Γ contains units u with $u \equiv 1 \pmod 4$.

14.2. The Character. Let $q \in \mathbb{N}$, and let $G = (\mathbb{Z}/q\mathbb{Z})^*$. A Dirichlet character is a function

$$\widehat{G} \ni \ \chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$$

that is totally multiplicative: that is, $\chi(mn) = \chi(m)\,\chi(n)$.

DEFINITION 14.2.

(1) We say that q is the modulus of χ; this is implicit in the choice of χ (note that any character of modulus q gives a canonical character of modulus $n \cdot q$ for every n: just precompose with $(\mathbb{Z}/nq\mathbb{Z})^* \twoheadrightarrow (\mathbb{Z}/q\mathbb{Z})^*$).
(2) Let χ_0 be the principal character of modulus q: the map $(\mathbb{Z}/q\mathbb{Z})^* \to \{1\}$
(3) Since $G = \bigoplus_p G_p$, and $\widehat{G} = \prod_p \widehat{G_p}$, every $\chi : G \to \mathbb{C}^*$ induces homomorphisms $\chi_p : G_p \to \mathbb{C}^*$, so we can write $\chi = \prod \chi_p$. This is the *local factorization of* χ.
(4) The *minimal modulus* is the smallest q such that χ "comes from" $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$, in the sense of (1).
(5) If χ is a real character, then its image is $\mathbb{C} \subset \mathbb{C}^*$; either it's a quadratic character, or it's trivial.

Given a character $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$, we can extend it to a map $\mathbb{Z} \to \mathbb{C}^*$, where

$$a \mapsto \begin{cases} 0 & \text{if } (a,q) \neq 1 \\ \chi(a \pmod q) & \text{if } (a,q) = 1 \end{cases}$$

In $(\mathbb{Z}/p^e\mathbb{Z})^*$ (for $p \neq 2$) there is a unique quadratic character. If a is a square $\pmod p$, then $\chi(a) = 1$; otherwise $\chi(a) = -1$ (unless it's the trivial character). This is the Legendre character $\chi_a = \left(\frac{a}{q}\right)$. If $p \mid a$, then it is zero.

Dirichlet characters are *totally multiplicative*: that is, they are homomorphisms.

Take a quadratic extension $K = \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}$. Let A be the ring of integers of K. If p ramifies in A, then (p) lifts to a square of prime ideals $P^2 \subset A$ (this is only possible for divisors of the discriminant). If p is *split*, then there are two (conjugate) prime ideals $P, \overline{P}$ in A. If p is *non-split*, then (p) lifts to a prime ideal in A. So we can define a character

$$p \mapsto \ \chi_K(p) = \begin{cases} 0 & \text{if } p \text{ ramifies} \\ +1 & \text{if } p \text{ splits} \\ -1 & \text{if } p \text{ is inert (does not split)} \end{cases}$$

There is only one way to define $\chi_K(-1)$ in order to make a Dirichlet character. (It turns out to be the sign of d.) Exercise: show that this is a (quadratic) Dirichlet character; find the minimal modulus.

14.3. Dirichlet L-functions. For $\sigma > 1$ a Dirichlet L-function looks like

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

The proof of convergence is the same as the proof for ζ.

Case 1: $\chi = \chi_0$. If $p \mid$ modulus of χ_0, then the corresponding factor in the product is just 1. The rest look like the factors of ζ when written as a product; that is,

$$L = \prod_{p \nmid q} \left(1 - \frac{1}{p^s}\right)^{-1}$$

which is just the product expansion of ζ deprived of finitely many factors. As earlier in the course, define

$$A(x) = \sum_{n \leq x} \chi(n)$$

and we have

$$\sigma_c = \limsup_{x \to \infty} \frac{\log |A(x)|}{\log x}$$

But $|A(x)| \leq q$, because if you sum $\chi(n)$ over a full set of representatives mod q, you get zero. (So in $\sum \chi(n)$ only the last few terms matter.) This shows that $\sigma_c = 0$. There is a cottage industry around showing that

$$\left| \sum_{M \leq n \leq N} \chi(n) \right| \leq q^{1-\varepsilon}$$

where $\varepsilon > 0$.

Corollary 14.3.

$$L(1,\ \chi) = \sum \frac{\chi(n)}{n}$$

is convergent.

Exercise: show that

$$-\frac{L'}{L}(s,\ \chi) = \sum_{n=1}^{\infty} \Lambda(n)\ \chi(n) n^{-s}$$

14.4. Deprived L-functions. Let $L(s, \chi)$ be an L-function. In the χ_0 case, we noticed that $L(s, \chi)$ is the ζ-function, deprived of some factors. In general, let

$$L^D(s, X) = \prod_{p \nmid D} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = L(s, X) \cdot \prod_{p \mid D} \left(1 - \frac{\chi(p)}{p^s}\right)$$

The last factor has no poles or zeroes. The only thing that changes is the nature of the residue. For example, $L(s, \chi_0)$ has a pole at $s = 1$ with residue $\prod_{p \mid D} \left(1 - \frac{1}{p}\right)$.

14.5. ζ-functions of quadratic number fields. Let $K \to \mathbb{Q}$ be a quadratic extension; we defined χ_K to be the quadratic character associated to K, which encodes splitting information. Define

$$\zeta_K(s) = \zeta(s) \cdot L(s,\ \chi_K) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \cdot \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

To be continued.

15. March 22

Recall we had a quadratic extension $K \to \mathbb{Q}$, and an associated Dirichlet character χ_K. We were computing $\zeta(s) \cdot L(s, \chi_K)$, for $\sigma > 1$. (We've already shown that $L(s, \chi_K)$ extends to $\sigma > 0$, so everything is at least defined here.)

$$\zeta(s) \cdot L(s,\ \chi_K) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{\chi_K(p)}{p^s}\right)^{-1} = \begin{cases} \prod \left(1 - \frac{1}{p^s}\right)^{-1} & \text{ramified} \\ \prod \left(1 - \frac{1}{p^s}\right)^{-2} & \text{split} \\ \prod \left(1 - \frac{1}{(p^2)^s}\right)^{-1} & \text{inert} \end{cases}$$

		number of primes over p	$N_{K/\mathbb{Q}}P$
p ramified	$\left(1 - \frac{1}{p^s}\right)^{-1}$	1	p
p split	$\left(1 - \frac{1}{p^s}\right)^{-2}$	2	p
p inert	$\left(1 - \frac{1}{(p^2)^s}\right)^{-1}$	1	p^2

where $N_{K/\mathbb{Q}}P$ is the norm.

So this is

$$\prod_{P|_p} \left(1 - \frac{1}{(N_{K/\mathbb{Q}}P)^s}\right)^{-1}$$

We don't necessarily have unique factorization in quadratic number fields, but we do have unique factorization of ideals. By the same reasoning that produced the equivalence of the sum / product forms of the Riemann zeta function:

$$\zeta_K := \sum_{Ideals\ I \neq 0} \frac{1}{(NI)^s} = \prod_P \left(1 - \frac{1}{(NP)^s}\right)^{-1}$$

where NI is the norm of I. This is the Dedekind ζ-function.

Proposition 15.1. $L(1, \chi_K) \neq 0$ (so $s = 1$ is a pole of ζ_K)

PROOF. By contradiction. If L vanishes, then by Landau's theorem ζ_K would be analytic up to $\sigma = 0$. Write

$$\zeta_K(\frac{1}{2}) = \sum_{\substack{\text{single-element} \\ \text{ideals}}} + \underbrace{\sum_{\text{the rest}}}_{>0} = \sum_{0<n}(n^2)^{-s} + \sum * = \sum \frac{1}{n} + \textit{positive}$$

which diverges. □

Corollary 15.2 (of HW)**.** If χ is any quadratic Dirichlet character, then $L(1, \chi) \neq 0$.

15.1. Arithmetic progressions. Let χ be a Dirichlet character of modulus q, and an integer a with $(a, q) = 1$.

Proposition 15.3.

$$\frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi}(a) \cdot \ \chi(n) = \begin{cases} 1 & n \equiv a \pmod{q} \\ 0 & \text{else} \end{cases}$$

Applying the proposition:

$$\sum_{n \equiv a \pmod{q}} \Lambda(n) n^{-s} = \sum_{n} \Lambda(n) n^{-s} \cdot \frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi}(a)\ \chi(n)$$

$$\frac{1}{\varphi(q)} \sum \overline{\chi}(a) \underbrace{\sum_{n=1}^{\infty} \Lambda(n)\ \chi(n) n^{-s}}_{-\frac{L'}{L}(s,\chi)} = -\frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi}(a) \frac{L'}{L}(s,\ \chi)$$

$$= -\frac{1}{\varphi(q)} \frac{L'}{L}(s,\ \chi_0) + \frac{-1}{\varphi(q)} \sum_{\chi \neq \chi_0} \overline{\chi}(a) \frac{L'}{L}(s,\ \chi)$$

$$= \frac{1}{\varphi(q)(s-1)} + O(1) + \cdots$$

If $\frac{L'}{L}(s, \chi)$ for $\chi \neq \chi_0$ has a pole, then the L-function either has a zero or a pole. L does not have a pole. So we have to prove that $L(1, \chi) \neq 0$ for all $\chi \neq \chi_0$.

$$\prod_{\chi \ modulus \ q} L(s,\ \chi) = exp\left(\sum_{\chi} \log L(s,\ \chi)\right) = exp\left(\sum \frac{\Lambda(n)}{\log n}\ \chi(n) n^{-s}\right)$$

$$= exp\left(\sum_{n} \frac{\Lambda(n)}{\log n} \underbrace{\sum_{\chi}\ \chi(n) n^{-s}}_{1 \ or \ 0}\right)$$

$$= \exp\left(\sum_{n\equiv 1 \pmod q} \Lambda(n)\log n \cdot n^{-s}\right)$$

$$\prod_{\chi \text{ modulus } q} L(1,\ \chi) \geq 1$$

$$\prod_{\chi} L(s,\ \chi) = L(s,\ \chi_0) \prod_{\chi \text{ quadratic}} L(s,\ \chi) \cdot \prod_{\chi \text{ ord}>2} L(s,\ \chi)$$

If any of these are zero, then we get a finite number; if two factors are zero at $s = 1$, then this is zero, contradicting $\prod L(\sigma, \chi) \geq 1$ for $\sigma > 1$. So we have at most one factor contributing zero at $s = 1$. We know that factor of $\prod_{quadratic} L(s, \chi)$ do not contribute a zero. So we have to worry about the characters χ of order > 2. Then $\overline{\chi} \neq \chi$. Recall that $\sum \frac{\chi(n)}{n^s}$ is conjugate to $\sum \frac{\overline{\chi}(n)}{n^s}$. If χ contributes zero, then $\overline{\chi}$ also contributes zero, which is a contradiction.

Corollary 15.4.

$$\sum_{n\equiv a \pmod q} \frac{\Lambda(n)}{n^s}$$

We just showed that $\frac{1}{\varphi(q)} \sum_{\chi\neq\chi_0} \overline{\chi}(a)\frac{L'}{L}(s, \chi)$ is bounded. So using the earlier expression for $\sum_{n\equiv a \pmod q} \Lambda(n)n^{-s}$, we have

$$\sum_{n\equiv a \pmod q} \Lambda(n)n^{-s} = \frac{1}{\varphi(q)(s-1)} + O(1) \to \infty$$

as $s \to 1+$.

$$\sum_{n\equiv a \pmod q} \Lambda(n)n^{-s} = \sum_{p^k\equiv a \pmod q} \frac{\log p}{p^k} = \sum_{p\equiv a \pmod q} \frac{\log p}{p} + \underbrace{\sum_{k=2}^{\infty} \sum_{p^k\equiv a \pmod q} (\log p)\cdot p^{-k}}_{\leq \sum_p \log p \sum_{k=2}^{\infty} p^{-k} = \sum_p \frac{\log p}{p(p-1)}}$$

which converges.

Corollary 15.5.

$$\sum_{p\equiv a \pmod q} \frac{\log p}{p} = \infty$$

15.2. Gauss sums. Fix χ of modulus q. Let ζ (ugh) be a primitive q^{th} root of unity $e^{\frac{2\pi i}{q}}$.

$$\tau(\ \chi) = \sum_{a=1}^{q} \chi(a)e^{\frac{2\pi i a}{q}} = \sum_{a=1}^{q} \chi(a)\zeta^a$$

Treating the sum as a discrete integral, etc., this is sort of like a discrete version of the Γ-function.

Proposition 15.6. (1) If $(b,q)=1$, then $\overline{\chi}(b)\tau(\chi)=\sum_{a=1}^{q}\chi(a)\zeta^{ab}$ since

$$\tau(\chi)=\sum_a \chi(ab)\zeta^{ab}=\ \chi(b)\sum_a\ \chi(a)\zeta^{ab}$$

This is also true for all b if χ is primitive, because both sides are zero.

(2) Let χ be primitive. Then $|\tau(\chi)|=\sqrt{q}$.

PROOF. We will show that $|\tau(\chi)|^2=q$. Fix any b such that $(b,q)=1$. From (1),

$$|\tau(\chi)^2|=\left|\sum\ \chi(a)\zeta^{ab}\right|^2$$

because $\overline{\chi}(b)$ is nonzero and goes away when you take the absolute value. Sum over b.

$$\varphi(q)|\tau(\chi)|^2=\sum_{\substack{b\\(b,q)=1}}\left|\sum_a\ \chi(a)\zeta^{ab}\right|^2$$

$$=\sum_b\left|\sum_a\ \chi(a)\zeta^{ab}\right|^2 \qquad \text{if } (b,q)\neq 1, \text{ everything is zero.}$$

$$\left|\sum\ \chi(a)\zeta^{ab}\right|^2=\left(\sum_{a=1}^{q}\ \chi(a)\zeta^{ab}\right)\left(\sum_{c=1}^{q}\overline{\chi}(c)\cdot\zeta^{-c\cdot b}\right)$$

so

$$\varphi(q)\cdot|\tau(\chi)|^2=\sum_{b=1}^{a}\sum_{a=1}^{q}\sum_{c=1}^{q}\cdots=\sum_{a,c}\ \chi(a)\overline{\chi}(c)\sum_b\zeta^{b(a-c)}$$

If $a\not\equiv c \pmod q$ then the last sum is zero. Otherwise, the sum is q. So this is

$$\sum_{a\equiv c \pmod q}\ \chi(a)\cdot\overline{\chi}(c)\cdot q=\varphi(q)\cdot q=\varphi(q)\cdot|\tau(\chi)|^2$$

□

Putting these facts together, if χ is primitive mod q,

$$\chi(n)=\frac{1}{\tau(\overline{\chi})}\sum_{a=1}^{q-1}\overline{\chi}(a)\zeta^{an}$$

(Since $|\tau(\chi)|\neq 0$, we can divide by it.)

15.3. Evaluating $L(1,\chi)$. We know

- $$L(1,\ \chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n}$$

  converges (but not absolutely).

- If $1 \leq a < q$, then $\sum \frac{\zeta^{an}}{n}$ converges. (We had our old theorem about $\sigma_c = \frac{\log|A(x)|}{\log x}$. If A is controllable, then you control convergence. You can make the same argument for the additive character ζ^{an}.)

Substitute the old expression for $\chi(n)$ into the definition of $L(1, \chi)$.

$$L(1,\ \chi) = \frac{1}{\tau(\overline{\chi})} \sum_{n=1}^{\infty} \sum_{a=1}^{q} \overline{\chi}(a) \frac{\zeta^{an}}{n}$$
$$= \frac{1}{\tau(\overline{\chi})} \sum_{q} \overline{\chi}(a) \sum_{n=1}^{\infty} \frac{\zeta^{an}}{n}$$

We have written $L(1, \chi)$ as a finite sum, having switched summations, weighted by character of a function of a. Define

$$F(z) = \sum \frac{z^n}{n} = \log \frac{1}{1-z}$$

if $|z| \leq 1$ and $z \neq 1$. So

$$L(1,\ \chi) = \frac{1}{\tau(\overline{\chi})} \sum \overline{\chi}(a) F(\zeta^{an})$$

16. March 27

Recall we had a primitive Dirichlet character χ of modulus q.

$$L(1,\ \chi) = \frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{q-1} \overline{\chi}(a) \cdot \sum_{n=1}^{\infty} \frac{e^{\frac{2\pi i a n}{q}}}{n}$$

We had defined $\zeta = e^{\frac{2\pi i}{q}}$ and $F(z) = \sum_{n=1}^{\infty} \frac{z^n}{n} = \log\left(\frac{1}{1-z}\right)$ for $|z| \leq 1$, so that $L(1, \chi) = \frac{1}{\tau(\overline{\chi})} \sum \overline{\chi}(a) F(\zeta^{an})$. Take the branch where $\log(x)$ is real if $x > 0$, and $\log(e^{i\theta}) = i\theta \in (-\pi, +\pi]$. Take $0 < a < q$. Use trig:

$$1 - e^{\frac{2\pi i a}{q}} = e^{\frac{\pi i a}{q}} (e^{\frac{-\pi i a}{q}} - e^{\frac{+\pi i a}{q}}) = -2ie^{\frac{\pi i a}{q}} \sin\frac{\pi a}{q}$$
$$= e^{\pi i\left(\frac{a}{q} - \frac{1}{2}\right)} \cdot 2\sin\frac{\pi a}{q}$$
$$F(e^{\frac{2\pi i a n}{q}}) = \log \frac{1}{1 - e^{\frac{2\pi i a n}{q}}} = -\log(2\sin\frac{\pi a}{q}) - \pi i \left(\frac{a}{q} - \frac{1}{2}\right)$$
$$L(1,\ \chi) = \frac{-1}{\tau(\overline{\chi})} \underbrace{\sum \overline{\chi}(a) \log(2\sin\frac{\pi a}{q})}_{S(\chi)} - \frac{\pi i}{\tau(\overline{\chi}) q} \underbrace{\sum \overline{\chi}(a) \cdot a}_{T(\chi)}$$

Note that if $\chi(-1) = +1$ then (by symmetry with replacing $a \mapsto q - a$) we have $T(\chi) = 0$. More precisely,

$$\sum \overline{\chi}(a) a = \sum \overline{\chi}(-a)(q-a) = \sum \overline{\chi}(a) \cdot (q-a) = q \sum \overline{\chi}(a) - \sum \overline{\chi}(a) \cdot a$$

Similarly, if $\chi(-1) = -1$

$$\sum \overline{\chi}(a) \cdot \log\left(2\sin\frac{\pi a}{q}\right) = \sum \overline{\chi}(q-a)\log\left(2\sin\frac{\pi(q-a)}{q}\right)$$
$$= \sum \overline{\chi}(-a)\log(2\sin(\pi - \frac{\pi a}{q})) = -\sum \overline{\chi}(a)\log\left(2\sin\frac{\pi a}{q}\right)$$

So, we have two cases:

$$L(1,\ \chi) = \frac{-1}{\tau(\overline{\chi})}\sum \overline{\chi}(a)\log\left(2\sin\frac{\pi a}{q}\right) \qquad \chi \text{ even}$$

$$L(1,\ \chi) = -\frac{\pi i}{q\tau(\overline{\chi})}\sum_{a=1}^{q-1}\overline{\chi}(a)\cdot a \qquad \chi \text{ odd}$$

Let $\chi = \chi_K$ be a quadratic character (arising from a quadratic extension $K \to Q$). First assume that K is a real quadratic field.

$$L(1,\ \chi_K) = -\frac{1}{\tau(\overline{\chi})}\log\left(\prod\left(e^{\frac{\pi i a}{q}} - e^{\frac{-\pi i a}{q}}\right)^{\overline{\chi}(a)}\right)$$

(There should be an extra factor of i in the denominator, because the 2 in $2\sin$ cancels the 2 in the $2i$ denominator of the exponential version of sin... Prof. Mazur claims that it goes away when you examine terms – the terms with i in the denominator cancel the terms with it in the denominator?) Write this as

$$L(1,\ \chi) = -\frac{1}{\tau(\overline{\chi})}\cdot\log(\varepsilon_\chi)$$

Note that $\chi = \overline{\chi}$ since this is a quadratic character. Let $e^{\frac{2\pi i}{2q}} = \zeta$, a root of unity. So this is

$$\varepsilon_\chi = \prod\left(e^{\frac{\pi i a}{q}} - e^{\frac{-\pi i a}{q}}\right)^{\chi(a)} = \prod\underbrace{(\zeta^a - \zeta^{-a})}_{\zeta^{-a}(\zeta^{2a}-1)}{}^{\chi(a)}$$

$\zeta^a \in \mathbb{Z}[\zeta] \subset \mathbb{Q}(\zeta)$ (a $2q^{th}$ root of unity), and $\mathbb{Z}[\zeta^2] \subset \mathbb{Q}(\zeta^2)$ (q^{th} roots of unity). Let $\xi = \zeta^2$ be this q^{th} root of unity. The root of unity ζ^{-a} doesn't matter; we really only care about $\zeta^{2a} - 1 = \xi^a - 1$, for $(q, a) = 1$.

Suppose we have $(b, q) = 1$, so

$$\xi^b - 1 = (\xi - 1)(\xi^{b-1} + \xi^{b-2} + \cdots + 1)$$

Find b' such that $bb' = 1$. Then we can write $\xi - 1 = (\xi - b)^{b'} - 1$. So the above equation is also

$$\xi - 1 = (\xi^b - 1)((\xi^{b'})^{b-1} + \cdots + 1)$$

So the ratio of any $\frac{\zeta^b - 1}{\zeta^a - 1}$ is a unit (if $(a, q) = 1 = (b, q)$), which also means that ε_χ is a unit in $\mathbb{Z}[\xi]$, where ξ is a primitive q^{th} root of unity. It turns out that $\varepsilon_\chi \in K$.

Let A be the ring of units of K, and let $U = A^* \subset A \subset K$ be the group of units. Then $U = \{\pm 1\} \times \gamma^{\mathbb{Z}}$, where γ is the *fundamental unit*: the generator that has the property $\gamma > 1$ (i.e. it is real and positive) in the usual embeding. So $\varepsilon_\chi = \gamma^h$ (where h is now

just some arbitrary power...). (Note that it is not negative, because it was the log of something > 1.) It turns out that $|h|$ is the class number.

DIGRESSION 16.1. The class number is the obstruction for A to satisfy unique factorization. If it is 1, then the ring of integers A satisfies unique factorization. If A is a PID, then it has unique factorization. The class number is the obstruction to being a PID. Consider the multiplicative system of nonzero ideals; there is a sub-multiplicative system of principal ideals. There are no inverses; but impose the equivalence relation $I \sim J$ if there exist principal ideals $(n), (m)$ such that $(n)I = (m)J$. There is an induced multiplication, and you can show that this is a finite group. This is called the ideal class group, and the class number is its size. If it is trivial, then every ideal is principal.

So $L(1, \chi) = \frac{-1}{\tau(\chi)} = \log(\gamma^h) = h \log \gamma$, where $\log \gamma$ is called the *regulator* of the quadratic field. This is an example of an *analytic formula*.

16.1. The Dedekind zeta-function of a number field. Let $A \subset K$ be the ring of integers of a number field K.

$$\sum_{ideals} \frac{1}{(NI)^s} = \prod_{P\ prime} \frac{1}{1 - NP^{-s}} =: \zeta_K(s)$$

These enjoy some basic facts of life:

(1) There is an analytic continuation to $\mathbb{C}$ with a single, simple pole at $s = 1$. Unlike $\zeta(s)$, the residue of the pole has arithmetic information:

$$res = \frac{2^{r_1}(2\pi)^{r_2}(Class\ number)(Regulator)}{(\#roots\ of\ 1)\sqrt{|Discriminant|}}$$

If $K \to \mathbb{Q}$ is a degree-n extension, then there are r_1 embeddings into $\mathbb{R}$, and r_2 distinct embeddings into $\mathbb{C}$ (not including the trivial ones into $\mathbb{R}$), *up to conjugation*. So $n = r_1 + 2r_2$. (This information is easy to come by: take the minimal polynomial of a primitive element of K; ask how many real roots and how many pairs of complex roots.)

(2) There is a functional equation as follows. Define

$$\Gamma_{\mathbb{R}}(s) = \pi^{\frac{-s}{2}} \Gamma\left(\frac{s}{2}\right)$$

(the Gamma-factor we've seen in the Riemann ζ-function), and

$$\Gamma_{\mathbb{C}}(s) = 2 \cdot (2\pi)^{-s} \Gamma(s)$$

In general,

$$\Gamma_K(s) = \Gamma_{\mathbb{R}}(s)^{r_1} \cdot \Gamma_{\mathbb{C}}(s)^{r_2}$$

If you define

$$\xi_K(s) = \Gamma_K(s) \cdot |Disc_K|^{\frac{s}{2}} \cdot \zeta_K(s)$$

then there is a functional equation

$$\xi_K(s) = \xi_K(1 - s)$$

REMARK 16.2. Read Ireland/ Rosen, or Davenport's *Higher Arithmetic*, for an elementary treatment of class numbers.

16.2. Analytic continuation of $L(s,\chi)$. Let χ be a primitive, modulus-q Dirichlet character. In the Riemann ζ case, recall the motivation for Hecke's theorem: we introduced Θ, used Poisson summation, got the functional equation for Θ, which gave analytic continuation and a functional equation for $\zeta(s)$. We will do the same in this case, by constructing Θ_χ, etc.

17. March 29

Let $z \in \mathbb{C}$ where $\mathrm{Re}(z) > 0$. Let χ be a primitive character of modulus q. Define

$$\kappa = \kappa(\chi) = \begin{cases} 0 & \chi \text{ even} \\ 1 & \chi \text{ odd} \end{cases}$$

$$\Theta_{even}(z,\ \chi) = \sum_{n=-\infty}^{\infty} \chi(n) e^{\frac{-\pi n^2 z}{q}} \qquad \chi \text{ even}$$

$$\Theta_{odd}(z,\ \chi) = \sum n\ \chi(n) e^{\frac{-\pi n^2 z}{q}} \qquad \chi \text{ odd}$$

Theorem 17.1. There are functional equations

$$\Theta_{even}(z,\ \chi) = \frac{\tau(\chi)}{q^{\frac{1}{2}}} z^{-\frac{1}{2}} \cdot \Theta_{even}\left(\frac{1}{z}, \overline{\chi}\right)$$

$$\Theta_{odd}(z,\ \chi) = \frac{\tau(\chi)}{i q^{\frac{1}{2}}} z^{-\frac{3}{2}} \cdot \Theta_{odd}\left(\frac{1}{z}, \overline{\chi}\right)$$

n in the sums above are only interesting as elements of congruence classes mod q. That is,

$$\Theta_{even}(z,\ \chi) = \sum_{a=1}^{q-1} \chi(a) \sum_{m=-\infty}^{\infty} e^{\frac{-\pi(mq+a)^2 z}{q}}$$

Change variables $A = \frac{a}{q}$, $Z = qz$.

Theorem 17.2. $\sum_{m=-\infty}^{\infty} e^{-\pi(m+A)^2 \cdot Z} = Z^{-\frac{1}{2}} \sum_{m=-\infty}^{\infty} e^{2\pi i k A} e^{\frac{-\pi k^2}{Z}}$

Use Poisson summation:

$$\sum_{m=-\infty}^{\infty} f(m) = \sum_{k=-\infty}^{\infty} \widehat{f}(k)$$

with $f(u) = e^{-\pi(u+A)^2 Z}$ and $\widehat{f}(t) = Z^{-\frac{1}{2}} e^{2\pi i A t} e^{\frac{-\pi t^2}{Z}}$. Now apply this:

$$\begin{aligned}\Theta_{even}(z,\ \chi) &= \sum_{a=1}^{q-1} \chi(a) \cdot \sum_{m=-\infty}^{\infty} e^{-\pi(m+\frac{a}{q})^2 qz} \\ &= \sum_{a=1}^{q-1} \sum_{m=-\infty}^{\infty} e^{-\pi(mq+a)^2 \frac{z}{q}} = z^{-\frac{1}{2}} \sum_{a=1}^{q-1} \chi(a) \sum_{m=-\infty}^{\infty} e^{2\pi i k \frac{a}{q}} e^{\frac{-\pi k^2}{qz}} \\ &= \sum_{k=-\infty}^{\infty} e^{\frac{-\pi k^2}{qz}} \underbrace{\sum_{a=1}^{q-1} \chi(a) e^{\frac{2\pi i k a}{q}}}_{Gauss\ sum} \\ &= \sum_{k=-\infty}^{\infty} e^{\frac{-\pi k^2}{qz}} \overline{\chi}(k) \cdot \tau(\ \chi)\end{aligned}$$

$$(qz)^{-\frac{1}{2}} \tau(\ \chi) \cdot \sum_{k=-\infty}^{\infty} \overline{\chi}(k) \cdot e^{\frac{-\pi k^2}{qz}} = \frac{\tau(\ \chi)}{q^{\frac{1}{2}}} \cdot z^{-\frac{1}{2}} \theta_{even}\left(\frac{1}{z}, \overline{\chi}\right)$$

Define the *epsilon factor*:

$$\varepsilon(\ \chi) = \frac{\tau(\ \chi)}{i^k q^{\frac{1}{2}}}$$

Now we can write the functional equation more concisely as

$$\Theta_\kappa(z,\ \chi) = \frac{\varepsilon}{z^{\frac{1}{2}+k}} \Theta_\kappa\left(\frac{1}{z}, \overline{\chi}\right)$$

17.1. Hecke's Theorem. The input is λ, k, ε and two functions

$$f(Z) = \sum a(n) e^{\frac{2\pi i n Z}{\lambda}}$$

$$g(Z) = \sum_{n=1}^{\infty} b(n) e^{\frac{2\pi i Z}{\lambda}}$$

such that

$$\varepsilon g\left(-\frac{1}{Z}\right) = \left(\frac{i}{Z}\right)^k f(Z)$$

Officially exclude the case $q = 1$; this is the Riemann zeta function, and we've done it.

Take $Z = iz$, $\lambda = 2q$, and $\varepsilon = \varepsilon(\ \chi)$.

$$f \mapsto \sum a(m) e^{\frac{-\pi m z}{q}} \qquad g \mapsto \sum b(m) e^{\frac{-\pi m z}{q}}$$

$$\varepsilon g\left(\frac{i}{z}\right) = z^{-k} f(iz)$$

Define

$$a(m) = \begin{cases} 0 & \text{if } m \text{ is non-square} \\ 2\,\chi(n) & \text{if } m = n^2 \end{cases}$$

$$b(m) = \begin{cases} 0 & \text{if } m \text{ is non-square} \\ 2\overline{\chi}(n) & \text{if } m = n^2 \end{cases}$$

Exercise: Finish this for HW; some stuff is probably wrong here...

17.2. Cyclotomic Fields. Consider the extension $\mathbb{Q}(e^{\frac{2\pi i}{N}}) \to \mathbb{Q}$ (that is, adjoining a primitive N^{th} root ζ of unity). This is Galois, where $G \cong (\mathbb{Z}/N\mathbb{Z})^*$. The conjugates of ζ are ζ^a (for $(a, N) = 1$). Let μ_N denote the group of all N^{th} roots of unity in $\mathbb{Q}(\zeta)$; the generators are the aforementioned ζ^a. An element in the Galois group is a map $\mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ that is the identity on $\mathbb{Q}$; so it is uniquely determined by assigning $\zeta^i \mapsto \zeta^{ai}$. If we call this automorphism σ_a, the isomorphism $(\mathbb{Z}/N\mathbb{Z})^* \to G$ is just $a \mapsto \sigma_a$.

Let $K \to L$ be any Galois extension, with Galois group G. There are rings of integers $B \subset L$ and $A \subset K$. By the primitive element theorem, write $L = K(\theta)$, where θ satisfies an irreducible polynomial $f(X) \in K[X]$ of degree equal to $[L : K]$. So $L = K[X]/(f(X))$. We are in a separable extension, so f is separable, i.e. all its roots $\theta_1, \cdots, \theta_n$ are distinct. The Galois group acts on the set $\{\theta_i\}$, and there is a single orbit.

We can always assume that f is monic. θ is an algebraic number, so it is in B; so $A[\theta] \subset B$. (It is not always the case that a ring of integers is generated by a single element; the inclusion here may be proper, and we don't care.)

The ground field doesn't matter, so assume $K = \mathbb{Q}$. Then $B = \mathbb{Z}[\theta]$. Reduce mod primes; $B \to \mathbb{Z}[\theta]/p\mathbb{Z}[\theta]$. There is a map

$$f(X) \in \mathbb{Z}[X] \longrightarrow \overline{f}(X) \in \mathbb{F}_p[X]$$

Roots θ_i get sent to roots $\overline{\theta}_i$ of $\overline{f}$. If $p \nmid Disc$, the $\overline{\theta}_i$ are distinct. But $\overline{f}$ might split as $\overline{f} = \overline{f}_1 \cdots \overline{f}_\nu$ (irreducibles). So $\mathbb{F}_p[X]/\overline{f}_i(X)$ are fields. So you can write $p\mathbb{Z}[\theta] = P_1 \cdots P_\nu$ where P_i is the kernel of $\mathbb{Z}[X]/(f(X)) \to \mathbb{F}_p[X]/(\overline{f}_i(X))$.

18. April 3

REMARK 18.1. There was a typo. The functional equation should have been

$$\varepsilon g\left(\frac{-1}{Z}\right) = \left(\frac{Z}{i}\right)^k f(Z)$$

Let $\zeta = e^{\frac{2\pi i}{N}}$ be a primitive N^{th} root of 1. Form $\mathbb{Z}[\zeta] = \mathbb{Z}[X]/(\Phi_N(x))$ where Φ_N is the cyclotomic polynomial $1 + X + \cdots + X^{N-1}$, whose roots are all the primitive N^{th} roots of unity. We had an extension $\mathbb{Q}(\zeta) \to \mathbb{Q}$, with an isomorphism $G \cong (\mathbb{Z}/N\mathbb{Z})^*$ (where G is the Galois group), identifying $a \in (\mathbb{Z}/N\mathbb{Z})^*$ with the automorphism $\zeta \mapsto \zeta^a$.

Now let $L \to K$ be any Galois extension. By the primitive element theorem, we can write $L = K[\theta] = K[X]/F(X)$, and suppose $\theta_1, \cdots, \theta_d$ are all the roots of F (that is,

$\theta = \theta_i$ for some i and θ_i is the full set of conjugates). If $A \subset K$ is the ring of integers, $B = A[\theta]$ is the ring of integers of L. [Oops! The Galois group doesn't necessarily fix the ring of integers... We should let $B = A[\theta_1, \cdots, \theta_n]$, but then this messes other stuff up. Fixed below.] Let $\pi \subset A$ be a prime ideal, not dividing $\operatorname{disc} F$. Let $k = A/\pi$. We can then factor $F_\pi(X) = \prod_{j=1}^{\nu} f_j(X) \in k[X]$. The ideal π lifts to $\pi B \subset B$, and $B/\pi B = k[X]/(F_\pi(X))$. Check that F_π is a separable polynomial. By the Chinese Remainder Theorem, $k[X]/(F_\pi(X)) = \prod_{j=1}^{\nu} k_j$ where $k_j = k[X]/(f_j)$. This gives a nice description of the prime decomposition of $\pi B \subset B$: if P_j is the kernel of $B \to k_j$, then $\pi B = \prod_{j=1}^{\nu} P_j$. The Galois group G of the extension operates transitively on $\{\theta_1, \cdots, \theta_d\}$ and on $\{P_1, \cdots, P_\nu\}$. Furthermore, given a fixed θ, the map $G \to \{\theta_1, \cdots, \theta_d\}$ given by $g \mapsto g\theta$ is a 1-1 correspondence. This is not the case for the P_j: let $G_j = \{g \in G : gP_j = P_j\}$ be the stabilizer. G_j acts on $k_j = B/P_j$, and hence represents an element of the Galois group. So now $\{G_1, \cdots, G_\nu\}$ is in 1-1 correspondence with $\{P_1, \cdots, P_\nu\}$, via the obvious map $G_j \mapsto P_j$ (G acts by conjugation on the left and multiplication on the right).

Consider the collection $\{G_j\}_{j=1,\cdots,\nu}$ as a collection of subgroups of G. This corresponds to a full orbit under the action of G.

G_j acts on B and stabilizes P_j, so it acts on $k_j = B/P_j$. This induces a mapping $G_j \to Gal(k_j/k)$, which turns out to be an isomorphism. All the G_j are cyclic, and there is a canonical generator: $\varphi_j : x \mapsto x^q$, where $q = |k|$ (this is a homomorphism on $k_j = B/P^j$). Call this "Frobenius at P_j". We have a collection $\{\varphi_j\}_{j=1,\cdots,\nu}$, which form a single conjugacy class in G. This depends only on the choice of π, so call it $C_\pi \subset G$.

It turns out that none of this depends on the choice of θ or B.

18.1. More general theory. We have an extension $L \to K$, with $A \subset K$ the ring of integers. Let $\pi \subset A$ be a prime ideal, and let $A_\pi = \varprojlim_m A/\pi m$ be the localization. Then let $B_\pi = B \otimes_A A_\pi$. Suppose that $\pi \nmid \operatorname{disc}(L/K)$ (where the discriminant is now an ideal). We have $\prod B_{P_j}$. As before, the G_j act on B_{P_j}. Let $k_j = B_{P_j}/P^j \cdot B_{P_j}$ be the residue field; we have a Galois group $Gal(k_j/k)$. Let the inertial group be the kernel of $G_j \twoheadrightarrow Gal(k_j/k)$. Assume that $\pi \nmid \operatorname{disc}(L/K)$, so there is a unique generator $\varphi_j : x \mapsto x^q$. For all π that are "good" (i.e. those that don't divide $\operatorname{disc}(L/K)$), we have identified a single conjugacy class $C_\pi \subset G$, called Frobenius at π.

For example, let $\mathbb{Q}(\zeta)/\mathbb{Q}$, and let $G \cong (\mathbb{Z}/N\mathbb{Z})^*$. This is an abelian group, so conjugacy classes are single elements. If p is good (i.e. $p \nmid N$), then C_p is the image of p in G (i.e. it's $p \pmod N$).

If $L \to K$ is a Galois extension, and $C \subset G = Gal(L/K)$ is a conjugacy class, let $\mathcal{P}_C = \{\pi \text{ "good" } : C_\pi = C\}$ be the *Chebotarev class*. In the previous example, the Chebotarev classes are the arithmetic progressions $p = a + Nt$, for given N.

18.2. Review of representation theory. A representation is a homomorphism $\rho : G \to GL_n(\mathbb{C}) \cong \mathrm{Aut}_{\mathbb{C}}(V)$ where V is an n-dimensional vector space. We will be considering representations up to conjugation. If G acts on V_1 and V_2, we say that the representations are equivalent if there is an isomorphism $h : V_1 \to V_2$ such that, for all $v \in V_1$, $g \in G$, we have $h(gv) = gh(v)$.

The *character* of a representation is $\chi_\rho : G \to \mathbb{C}$ that maps $g \mapsto Trace(\rho(g))$. This is well-defined up to equivalence: if you change a matrix up to conjugation, you don't change its trace.

Given a character $G \xrightarrow{\chi} \mathbb{C}$, this factors through the set $\mathcal{C}$ of all conjugacy classes; so there is an induced function $\mathcal{C} \to \mathbb{C}$, which we also call χ. Let $H_G = Maps(\mathcal{C}, \mathbb{C})$, which we make into a Hilbert space as follows:

$$(\varphi \mid \psi) = \frac{1}{|G|} \sum_{x \in G} \varphi(x)\overline{\psi}(x)$$

There is a natural basis. If $c \in \mathcal{C}$, then

$$\delta_c : \begin{cases} c' \mapsto 0 & \text{if } c' \neq c \\ c' \mapsto 1 & \text{if } c' = c \end{cases}$$

A representation ρ on V is irreducible if it cannot be decomposed as $\rho_1 + \rho_2$ on $V_1 \oplus V_2$. An *irreducible character* is one that comes from an irreducible representation.

Theorem 18.2 (Orthogonality relations)**.** $\{\chi\}_{\chi \text{ irreducible}} \subset H_G$ is an orthonormal basis.

So now we have two bases: the natural basis, and the "deeper" basis of irreducibles. We can relate these:

$$\delta_c = \frac{|c|}{|G|} \cdot \sum_{\chi \text{ irreducible}} \overline{\chi}(c)\ \chi$$

Also, the representation is determined uniquely by the irreducible characters, and it is expressible uniquely as a sum of irreducibles.

18.3. Artin L-functions. Let L/K be an extension with Galois groups G, and a representation $G \to GL_n(\mathbb{C})$. Choose a prime $\pi \nmid \mathrm{disc}(L/K)$. We have a conjugacy class C_π of elements. Choose $\varphi_\pi \in C_\pi$ and a positive integer m. φ_π^m is uniquely determined up to conjugacy, and so are $\rho(\varphi_\pi^m)$ and $Trace(\rho(\varphi_\pi^m)) =: \chi_\rho(\varphi_\pi^m)$. Call $\varphi = \varphi_\pi$ and $\chi_\rho(\varphi_\pi^m) = \chi(\pi^m)$. We will use this to produce a Dirichlet series, the "local at π Artin-Euler factor attached to ρ and L/K":

$$L_\pi(s; \rho, L/K) = \sum_{m=1}^{\infty} \frac{\chi(\pi^m)}{m(N\pi)^{ms}}$$

The numerators are bounded, so this makes sense for $\sigma > 1$.

Alternatively, let φ_π be Frobenius at π; $\rho(\varphi_\pi) \in GL_n(\mathbb{C}) \subset Mat_n(\mathbb{C})$. Let $\mathbb{1}$ denote the identity matrix here. Exercise: show that

$$L_\pi(s; \rho, L/K) : s \mapsto \frac{1}{\det(\mathbb{1} - \rho(\varphi_\pi) \cdot N\pi^{-s})}$$

for sufficiently large $Re(s)$. Let π be (possibly) ramified. The inertial group I_j is the normal subgroup given by the kernel of

$$G_j \twoheadrightarrow Gal(k_j/k)$$

We had a representation ρ acting on a vector space V; but G_j and I_j also act on V. Let

$$V^{I^j} = \{v \in V \,:\, \gamma v = v \ \forall \gamma \in I_j\}$$

This is designed to have an action of $G_j/I_j = Gal(k_j/k)$, which we call ρ_j. Frobenius is sitting in this latter Galois group, and it corresponds to some element $\psi_j \in G_j/I_j$. If V had dimension n, let n_j be the dimension of V^{I_j}. We have $1, \rho_j(\psi_j) \in GL_n(\mathbb{C}) \subset Mat_{n_j}(\mathbb{C})$. Then we have a function

$$s \mapsto 1 - \rho_j(\psi_j)(N\pi)^{-s} \in Mat_{n_j}(\mathbb{C})$$

Define

$$L(s, \rho, L/K) = \prod_\pi L_\pi(s, \rho; L/K)$$

where the product is taken over *all* π, ramified or not.

19. April 5

19.1. Zeros of L-functions (Akhil). We cared about $\sum_{n \equiv \ell (q)} \Lambda(n)$, and more generally $\psi(x, \chi) = \sum_{n \le x} \Lambda(n)\,\chi(n) = \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} \frac{-L'(s,\chi)}{L(s,\chi)} \frac{x^s}{s}\, \mathrm{d}s$. Recall that ζ had no zeros in the area $\sigma \ge 1 - \frac{c}{\log t}$ for some c.

Proposition 19.1. Let χ be nontrivial, with $\sigma \in (\delta, 2)$. Then

$$L(s,\ \chi) \ll (1 + \tau^{1-\sigma}) \min\{\frac{1}{\sigma - 1}, \log \tau\}$$

Proposition 19.2. If $\frac{5}{6} \le \sigma \le 2$, then

$$\frac{L'(s,\, \chi)}{L(s,\, \chi)} = \sum_{\rho \text{ close to } s} \frac{1}{s - \rho} + O(\log \tau)$$

where "close" means in the circle of radius $\frac{5}{6}$ around $\frac{3}{2} + it$.

This comes from a more general fact about analytic functions, and the proof is the same as in the ζ case.

OBSERVATION 19.3. If $\mathrm{Re}(s) > 1$ then $\mathrm{Re}\left(\frac{L'(s,\chi)}{L(s,\chi)}\right) \geq \mathrm{Re}\left(\frac{1}{s-\rho}\right) - C \cdot \log \tau$ for any root ρ close to s. In particular, if $\rho = \beta + i\gamma$, take $s = 1 + \eta + i\gamma$. Then

$$\mathrm{Re}\left(\frac{L'(s,\,\chi)}{L(s,\,\chi)}\right) \geq \frac{1}{1+\eta-\beta} - C \cdot \log \gamma$$

Proposition 19.4.

$$\mathrm{Re}\left(3\frac{L'(\sigma,\,\chi_0)}{L(s,\,\chi_0)} + 4\frac{L'(\sigma+it,\,\chi)}{L(\sigma+it,\,\chi)} + \frac{L'(\sigma+2it,\,\chi^2)}{L(\sigma+2it,\,\chi^2)}\right) \leq 0$$

This is the analogue of a similar inequality from earlier.

$$\frac{L'}{L}(\sigma,\ \chi_0) = \frac{-3}{\sigma-1} + c$$

$$\frac{L'}{L}(\sigma+2it,\ \chi^2) \geq -c \cdot \log \tau$$

$$\mathrm{Re}\left(\frac{L'}{L}\right)(s,\ \chi) \leq \frac{3}{4(\sigma-1)} + C \cdot \log \tau$$

$$\frac{1}{r+\eta} - c \cdot \log \gamma \leq \frac{3}{4\eta + c \cdot \log \gamma}$$

Let $D = \frac{\eta}{r}$, then

$$\frac{1}{(1+r)} \leq \frac{3}{4Dr} + c \cdot \log \gamma$$

$$\left(\frac{1}{D+1} - \frac{3}{4D}\right)\left(\frac{1}{r}\right) \leq c \cdot \log \gamma \implies r \gg (\log \gamma)^{-1}$$

Theorem 19.5.

$$\pi(x,q,a) = \frac{1}{\varphi(q)} \log x + O(xe^{-\delta\sqrt{\log x}})$$

19.2. Recall we had an extension $L \to K$ and a Frobenius element $\varphi_\pi \in G$, where π is a "good" prime of K. For example, in the case of the cyclotomic extension $\mathbb{Q}(\zeta_N) \to \mathbb{Q}$, a "good" prime is one such that $p \nmid N$. It determines an element in the Galois group $G = (\mathbb{Z}/N\mathbb{Z})^*$; this is φ_p.

We had Dirichlet L-functions, which involved a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$, and Artin L-functions, which involved a Galois character $\chi : G \to \mathbb{C}^*$. When $L = \mathbb{Q}(\zeta_N)$ and $K = \mathbb{Q}$, then there is a canonical identification between these two. In general, if you have an abelian extension (i.e. the Galois group is abelian), then there is an analogue that is a Dirichlet character. The relationship between them is basically class-field theory. (What's interesting is that the Dirichlet character has nothing to do with L, only K; but the whole point of Artin characters is that they depend on L.)

Ideals form a monoid. We can make it into an abelian group by adding in fractional ideals; call this I. Consider the characters $\chi : I \to \mathbb{C}^*$. Given an extension $L \to K$ that is Galois and abelian, for all good primes you get an element $\varphi_\pi \in G$. You a get a map from most of I to G (i.e., sending $\pi \mapsto \varphi_\pi$), just by multiplicativity. So a character $\chi : I \to \mathbb{C}^*$ factors through $G\ldots$

It took quadratic reciprocity to guarantee that the χ_K we defined before is actually defined on $(\mathbb{Z}/N\mathbb{Z})^*$

19.3. More algebraic number theory. Given an extension $L \to K$ with Galois group G, and a prime $\pi \subset K$ that lifts to P, we can form the decomposition group $D_P \subset G$, the subgroup stabilizing P. We defined the inertial group I_P as the kernel of $D_P \to Gal(k_P/k)$ (recall $k_P = B/P$, where B is the group of integers). From last time,

$$L_\pi(s, \rho, L/K) = \frac{1}{\det(1 - \rho^P(\varphi_\pi) \cdot N\pi^{-s})}$$

where $\rho^p : D_P/I_P \to Aut(V^{I^P})$. Then the global Artin L-function is

$$L(s, \rho, L/K) = \prod_\pi L_\pi(s, \rho, L/K)$$

You can show that this actually converges for $\sigma > 1$; in the cyclotomic case, if ρ is a 1-dimensional character, then this is the Dirichlet L-function.

Let $M \to L \to K$ be a Galois tower: there is a Galois group $G(M/K)$, and hence an induced Galois group $G(M/L)$ (we don't care whether $L \to K$ is Galois). By composition, given $\rho^L : G(L/K) \to GL_n(\mathbb{C})$, we get $\rho^M : G(M/K) \to G(L/K) \to GL_n(\mathbb{C})$. We have $L(s, \rho^L, L/K) = L(s, \rho^M, M/K)$, because if $\{\varphi_\pi^\ell\}$ are the Frobenius elements in the first extension, and $\{\varphi_\pi^M\}$ are the Frobenius elements in the second, the φ_π^M map onto φ_π^ℓ. Taking $1 : G \to \{1\}$, then $L(s, 1, L/K) = \zeta_K(s)$ is an incomplete Dedekind ζ-function.

19.4. Induced representations. Let $H \subset G$ be a subgroup, and suppose you have a representation $\rho : H \to GL_n(\mathbb{C})$. Then I claim you get an induced representation $Ind_H^G(\rho) : G \to GL_m(\mathbb{C})$, where $m = [G : H] \cdot n$, such that for every tower of fields $M \to L \to K$ (where $M \to K$ has Galois group G, and $L \to K$ has Galois group H), then

$$L(s, \rho, M/L) = L(s, Ind_H^G \rho, M/K)$$

This is basically linear algebra. Let W be a finite-dimensional $\mathbb{C}$ vector space with H acting $\mathbb{C}$-linearly. Define $\mathbb{C}[H] = \bigoplus_{h \in H} \mathbb{C} \cdot h$, an associative $\mathbb{C}$-algebra. By facts about representation theory, this is a direct sum of total matrix algebras, one for every irreducible character of H. You get a tensor product

$$\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W$$

20. April 10

April 24: Second $1\frac{1}{2}$ hour exam

Last time we introduced the group ring $\mathbb{C}[G]$; I mentioned that a G-representation V is the same as a left $\mathbb{C}[G]$-module. G acts on $\mathbb{C}[G]$ by left multiplication, so $\mathbb{C}[G]$ is a left (and right) G-module; this is called the regular representation, and it has degree $|G|$. When G was abelian, $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$. In general, we let $\widehat{G}$ be the set of irreducible G-representations. These are completely determined by their characters. The number of these is = the number of conjugacy classes in G. Suppose $\chi_1, \cdots, \chi_s$ are the irreducible characters, which have degree $d_1, \cdots, d_s$. Recall

$$\mathbb{C}[G] \cong \bigoplus_{i=1}^{s} End(V_i)$$

which gives that $|G| = \sum_{i=1}^{s} d_i^2$.

Let $H \subset G$ be finite groups. We have a character $\psi : H \to \mathbb{C}$, which belongs to a representation W. We want an induced representation

$$V = Ind_H^G W = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} W$$

of G, with character $\chi = Ind_H^G \psi$. Let $\mathscr{R} = \{\gamma\}_{\gamma \in \mathbb{G} \pmod H}$ be a set of representatives from each coset G/H. For all $g \in G$ there exists $h_{g/\gamma} \in H$ such that $g \cdot \gamma = \gamma' \cdot h_{g,\gamma}$. So G acts on $\bigoplus_{\gamma \in R} \gamma \cdot W$, where $\gamma W \to \gamma' W$ sends $w \mapsto h_{g,\gamma} w$. Recall ψ was the character of the H-representation, and $\chi = Ind_H^G \psi$ is the character of the induced G-representation. This can be defined as

$$\chi(u) = \sum_{\substack{r \in \mathscr{R} \\ r^{-1}ur = h_u, r \in H}} \psi(r^{-1}ur) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}ux \in H}} \psi(x^{-1}ux)$$

Alternatively, we could just write this as $\sum_{r \in \mathscr{R}} \psi(r^{-1}ur)$ where ψ is extended to G by $\psi_{G-H} = 0$.

Let $M \to L \to K$ be a sequence of fields, where $M \to K$ is Galois with Galois group G, and $M \to L$ is Galois with Galois group H. There is some prime π of K that splits as a series of P_i in L, and a series of Q_i in M. We have Artin L-functions $L(s, \psi; M/L)$ and $L(s, \chi, M/K)$.

Theorem 20.1.

$$L(s, \psi; M/L) = L(s, \chi, M/K)$$

This is not that deep. We know that $L(s, \chi, M/K) = \prod_\pi L_\pi(s, \chi; M/K)$. Define $L_\pi(s, \psi, M/L) = \prod_{P|\pi} L_P(s, \psi, M/L)$ (where ramified primes are *not* counted with multiplicity). We will actually avoid ramified primes; they make the notation worse. So it suffices to prove

Proposition 20.2.

$$L_\pi(s, \psi, M/L) = L_\pi(s,\ \chi; M/K)$$

Before proving this, we will do a special case.

EXAMPLE 20.3 (S_3-example). $M \to K$ has Galois group S_3, and $M \to L$ is degree 2. So $L \to K$ is a non-Galois cubic extension. Write $H = \{1, t\}$ and $G = \{1, t, r, rt, r^2, r^2t\}$. Let $\mathscr{R} = \{1, r, r^2\}$ be a representative system for G/H. Let π be a prime. Either it remains prime, it splits into two primes, or it splits into three primes. If it remains prime then the residue field extension is degree 3. In the second case, one degree is 1 and the other is 2; in the third case, all extensions are degree 1. In the first case, P can't stay prime, because the group isn't cyclic. So P splits into Q and $\overline{Q}$. In the second case, the combined residue extensions have to be the same. So P_1 lifts to Q_1 (degree 1) and P_2 splits into Q_2 and Q_3, each extensions of degree 1. In the third case, you can't have each P_i lift through a degree-2 extension to some Q_i: the decomposition group has to be contained in H; but they are all Galois conjugate. So each P_i splits into Q_i and $\overline{Q}_i$. So, determining the splitting of π in L determines the splitting in M.

Let $\psi : H \to \mathbb{C}^*$ be the nontrivial character. We know what ψ is on H: it sends $t \mapsto -1$.

$$\chi(u) = \sum_{0,1,2} \psi(r^{-i} u r^i)$$

$\chi(1) = 3$ because that's the degree of the induced representation ($[G : H] = 3$).

conj. class	1	t	r
χ	3	-1	0

Let 1 denote the trivial representation, ε denote the sign representation, and τ be the 2-dimensional representation (action of S_3 on its vertices).

	1	t	r
1	1	1	1
ε	1	-1	1
τ	2	0	-1

So $\chi = \varepsilon + \tau$. In this example, $L_\pi(s, \psi, M/L) = L_\pi(s, \varepsilon; M/K) \cdot L_\pi(s, \tau; M/K)$. Evaluating local factors gets

$$\left(\frac{1}{1 - \pi^{-s}}\right)^3$$

for the first case, $\left(\frac{1}{1+\pi^{-s}}\right)\left(\frac{1}{1-\pi^{-2s}}\right)$ for the second case, and $\left(\frac{1}{1-p^{-3s}}\right)$ for the third case.

Given the previous computation,

$$\underbrace{L(s, \psi; M/L)}_{\textit{degree } 1} = \underbrace{L(s, \varepsilon, M/K)}_{\textit{degree } 1} \cdot \underbrace{L(s, \tau; M/K)}_{\textit{degree } 2}$$

If we have a general theory of analytic continuation and functional equations for degree 1 and Artin L-functions, then we have that $L(s, \tau; M/K)$ would be the ratio of two analytic functions, i.e. a meromorphic function. If you have a zero-free region for Artin L-functions (which we do), then you get a zero-free region for $L(s, \tau, M/K)$ (modulo a few poles, maybe). This is actually useful: you don't need entire-ness to get good estimates.

Theorem 20.4 (Brauer)**.** Any character can be written $\chi = \sum_{finite} n_j Ind_{H_j}^G \psi_j$ such that each $\psi_j : H_j \to \mathbb{C}^*$ has degree 1, and $n_j \in \mathbb{Z}$.

Thus $L(s, \chi; M/K) = \prod L(s, \psi_j, M/L_j)^{n_j}$. Combining this with the "general theory", you have nice control over Artin L-functions: you can write them as the product / quotient of degree-1 L-functions, which are analytic.

PROOF OF PROPOSITION. π splits into primes $P_1, \cdots, P_\nu$ in L. For each of these, choose some Q_i above P_i in M. For each j choose $\eta_j \in G$ such that $\eta_j Q_1 = Q_j$. Each Q_j has a decomposition group G_j (this is the Galois group of $Q_j \to K$). These conjugate the way the Q_i's do: $\eta_j G_1 \eta_j^{-1} = G_j$. Each G_j contains Frobenius, which we call φ_j; and $\eta_j \varphi_1 \eta_j^{-1} = \varphi_j$. Let $f_j' : Q_j \to P_j$ be the degree of the residue field extension for $M \to L$, and let $f_j : P_j \to \pi$ be the other residue field extension degree. Let $f = f_j f_j'$ (the same for all j – it's the residue field extension degree of any of the Q_j over π).

(1) $|G_j| = f$
(2) $|G_j \cap H| = f_j'$
(3) $|G_j/(G_j \cap H)| = f_j$
(4) $\{\gamma_{j,1}, \gamma_{j,2}, \cdots, \gamma_{j,f_j}\}$ is a representative system for G_j modulo $G_j \cap H$.

Lemma 20.5.

$$\mathbf{L} : \{\gamma_{j,k} \cdot \eta_j \ : \ k = 1, .., f_j \ \ j = 1, \cdots, \nu\}$$

is a representative system for G/H.

PROOF. Homework. □

$$\chi(u) = \sum_{j,k} \psi(\gamma_{j,k} \eta_j u \eta_j^{-1} \gamma_{j,k}^{-1})$$

(Make use of the convention that $\varphi(X) = 0$ if $X \notin H$.) Take the Frobenius element φ_1, and let $u = \varphi_1^m$ be an arbitrary element of $G_1 = Gal(Q_1/k\pi)$. Write this as the *Artin symbol* $(Q_i, M/K)$. So $\varphi_j^{f_j} = (Q_j; M/L) \in H$, and $\varphi_j^m \in H$ iff $f_j \mid m$.

$$\chi(\varphi_1^m) = \sum \psi(\gamma_{jj,k} \underbrace{\eta_j \varphi_1^m \eta_j^{-1}} \gamma_{jk}^{-1})$$

$$= \sum \psi(\gamma_{jk}\varphi_j^m\gamma_{jk}^{-1})$$
$$= \sum_{j=1}^{\nu} f_j\psi(\varphi_j^m) \qquad \text{in an abelian group}$$

$$\begin{aligned}
\log L_\pi(s,\ \chi; M/K) &= \sum \frac{\chi(\pi^m)}{m\cdot N\pi^{ms}} \\
&= \sum \frac{\chi((Q_j, M/K)^m)}{m\cdot N\pi^{ms}} \\
&= \sum_{m=1}^{\infty}\sum_{j=1}^{\gamma} \frac{f_j\psi(\varphi_j^m)}{m\cdot N\pi^{ms}} \\
&= \sum_{n=1}^{\infty}\sum \frac{f_j\psi((\varphi_j^{f_j})^n)}{f_jn\cdot (N\pi)^{f_jns}} \qquad \text{only some of the above terms count} \\
&= L_\pi(s,\psi, M/L) \qquad \text{by definition}
\end{aligned}$$

□

21. April 12

21.1. Artin L-functions and Dedekind ζ-functions. Let $L \to K$ to be Galois with Galois group G, and choose $H \subset G$ as the trivial group. Then $L(s,\psi, L/L) = \zeta_L(s)$ by definition; but we just proved this is equal to $L(s, Ind_{\{1\}}^G\psi, L/K)$. Write $\mathbb{C}$ as a $\mathbb{C}[H]$ module, where every element of H acts trivially on $\mathbb{C}$. The induced representation χ is $\mathbb{C}[G]\otimes_{\mathbb{C}[H]}\mathbb{C}^1 = \mathbb{C}[G]$. So the induced character is the regular representation of G acting on $\mathbb{C}[G] \cong \bigoplus_{\chi_i\ irred} End_{\mathbb{C}}(V_i)$; if each representation V_i has dimension d_i, then $End_{\mathbb{C}}(V_i) = \bigoplus^{d_i} V_i$.

$$L(s, Ind_{\{1\}}^G\psi, L/K) = \prod_{\chi_i\ irred} L(s,\ \chi_i; L/K)^{d_i} = \zeta_L(s)$$

(Clarification: we're thinking of $\mathbb{C}[G]$ acting on $\mathbb{C}[G] = Reg$; also $|G| = \dim_{\mathbb{C}}(Reg)$. By more representation theory, write $Reg = \bigoplus End_{\mathbb{C}}(V_i) = \bigoplus M_{d_i\times d_i}(\mathbb{C})$. This is canonical. But $End_{\mathbb{C}}(V_i) = \bigoplus^{d_i} V_i$ depends on choice of basis.)

21.2. Signed divisors and D-ideal class groups. (Notation is made up by Mazur.) We have a number field $K \to \mathbb{Q}$, with ring of integers A. A *signed divisor* is a pair (D, S_∞) (usually referred to as D), where D is an ideal, and S_∞ is a set of distinct real embeddings of $K \hookrightarrow \mathbb{R}$. Define I_D to be the group of fractional ideals of A relatively prime to D: the "denominators" do not include primes of D. Let Pr_D be the set of principal D-ideals: the subgroup of nonzero elements $a \in K^*$ such that

(1) for all $P \mid D$, $a \in A_P$ (A localized at P)
(2) $a \equiv 1 \pmod{D_P}$; so $D_P = D \cdot A_P$ for all $P \mid D$; alternatively, $a - 1$ has no copies of p in the denominator
(3) a has positive image under any embedding $K \hookrightarrow \mathbb{R}$

DEFINITION 21.1. $Cl_D(K) = I_D/Pr_D$ is the *ideal class group.*

If α is an ideal, write $[\alpha]$ to represent the corresponding element in the ideal class group.

Let κ_D be the set of ideals prime to D, and let $\kappa_D(c) = \{\alpha \in \kappa_D \,:\, [\alpha] = c\}$. Also define

$$\kappa_D(c, X) = \{\alpha \in \kappa_D(c) \,:\, \left|N_{K/\mathbb{Q}}\alpha\right| \leq X\}$$

Theorem 21.2. There exists $\rho = \rho_D(K) > 0$ depending upon K and D, but not c, such that

$$|\kappa_D(c, X)| = \rho \cdot X + O\left(X^{1-\frac{1}{[K:\mathbb{Q}]}}\right)$$

It turns out that

$$\rho = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot Regulator}{|roots\ of\ 1| \cdot \sqrt{Discriminant}}$$

but it doesn't really matter what ρ is, and it simplifies the proof if you don't specify ρ. We'll prove this... later? maybe not at all.

If $K = \mathbb{Q}$, then $\rho = 1$. If $K = \mathbb{Q}(i)$, ideals are points in the first quadrant of the radius-x circle.

Define

$$\zeta_K^c(s) = \sum_{\substack{\alpha \in \kappa_D \\ [\alpha] = c}} (N\alpha)^{-s}$$

Also define

$$\zeta_K^{\{D\}}(s) = \sum_{\alpha \in \kappa_D} (N\alpha)^{-s} = \sum_{c \in Cl_D(K)} \zeta_K^c(s)$$

Also, write $\zeta_{\mathbb{Q}}$ for the Riemann ζ function.

$A(x)$ of the Dirichlet series $\zeta_K^c(s) - \rho \cdot \zeta_{\mathbb{Q}}(s)$ is $O(X^{1-\frac{1}{[K:\mathbb{Q}]}})$. Going back to the old lim sup discussion, we can show that the abscissa of convergence is $\leq 1 - \frac{1}{[K:\mathbb{Q}]}$.

Corollary 21.3. ζ_K^c has meromorphic continuation to at least $\sigma = 1 - \frac{1}{[K:\mathbb{Q}]}$, and has a pole at $s = 1$ with residue $= \rho$.

Corollary 21.4. The incomplete ζ-function $\zeta_K^{\{D\}}(s)$ has the same meromorphic continuation with residue $h_D(K) \cdot \rho$, where $h_D(K) = |Cl_D(K)|$.

21.3. Ideal class L-functions. Let D be a signed divisor. A D-ideal class character (of degree 1) is a homomorphism

$$I_D/Pr_D \xrightarrow{\chi} \mathbb{C}^*$$

Also view these as characters (also notated ζ) of I_D.

$$L^{\{D\}}(s,\ \chi) = \sum_{c \in Cl_D(\kappa)} \zeta^c(s) = \sum_{\alpha \in \kappa_D} \frac{\chi(\alpha)}{(N\alpha)^s} = \prod_{P \in \kappa_D} \frac{1}{1 - \frac{\chi(P)}{NP^s}}$$

(the last expression is by unique factorization, just like the Riemann ζ case).

Corollary 21.5. If χ is any nontrivial character, then $L^{\{D\}}(s, \chi)$ extends *as an analytic function* to the right-half plane bounded by $\sigma = 1 - \frac{1}{[K:\mathbb{Q}]}$.

Why? $\zeta^c(s)$ has a pole of exactly the same residue R at $s = 1$. So the residue of $L^{\{D\}}(s, \chi)$ is $\sum_{c \in Cl_D(K)} \chi(c) \cdot R$.

You can also prove (but we won't) that $L^{\{D\}}(s, \chi)$ doesn't vanish on $\sigma = 1$. We also have the weaker result that $L^{\{D\}}(1, \chi) \neq 0$.

21.4. Logs of Ideal class L-functions. The difference between ζ-functions and L-functions is that L-functions have to have Euler products, but ζ-functions may not. When we have a product, we want to take the log.

Say that $f \sim g$ if $f - g$ is analytic around $s = 1$.

$$\log L^{\{D\}}(s,\ \chi) = \sum_{m=1}^{\infty} \sum_{P \in \kappa_D} \frac{\chi(P)^m}{m \cdot (NP)^{ms}} = \sum \frac{\chi(P)}{(NP)^s} + Rest \sim \sum_{P \in \kappa_D} \frac{\chi(P)}{NP^s} \sim \sum_{\substack{P \in \kappa_D \\ \deg(P)=1}} \frac{\chi(P)}{NP^s}$$

($L^{\{D\}}(s, \chi)$ has an analytic continuation around $s = 1$.)

Let K be a field, $\mathscr{P}$ a collection of primes. Take

$$\frac{\sum_{P \in \mathscr{P}} \frac{1}{NP^s}}{\sum_{P \text{ prime}} \frac{1}{NP^s}}$$

, and the denominator is $\sim \log \frac{1}{s-1}$. Then the limit of this as $s \to 1$ is the *Dirichlet density*.

21.5. Relationship between D-ideal class L-functions and abelian Artin L-functions.

Theorem 21.6. Let L/K be abelian, with Galois group G. There exists a signed divisor D over K and a unique surjective homomorphism $Cl_D(L) \overset{Artin}{\twoheadrightarrow} G$ that is completely described by the following: if $P \in I_D(K)$ is prime, and $[P]$ is its image in the class group, then $Artin([P]) = \varphi_P \in G$ (the Frobenius element).

Corollary 21.7. If $\chi : G \to \mathbb{C}^*$ is a character, then

$$L^D(s,\ \chi \circ Artin) = L^{incomplete}(s,\ \chi, L/K)$$

where the incompleteness is because we've ignored ramified primes on the left.

22. April 17

22.1. Density. The Dedekind zeta function has a simple pole at $s = 1$, and is analytic elsewhere.

$$\zeta_K(s) = \sum_{P \in \mathscr{P}_K} (NP)^{-s} = 1 \cdot \log \frac{1}{s-1} + h(s)$$

where $h(s)$ is analytic. (This comes from breaking up ζ_K as a sum over primes to various powers, and realizing that powers > 1 don't change much.) Then we took $A \subset \mathscr{P}_K$, and asked about $\sum_{P \in A} NP^{-s}$. We say that A has *strong analytic density* if

$$\sum_{P \in A} (NP)^{-s} = a \cdot \log \frac{1}{s-1} + h(s)$$

where h is another function that is holomorphic around $s = 1$. Impose the relation $f(s) \sim g(s)$ if $f(s) = g(s) + h(s)$ where $h(s)$ is analytic around $s = 1$.

A has *natural density* a if

$$a = \lim_{X \to \infty} \frac{\#\{P \in A\ :\ NP \leq X\}}{\#\{P \in \mathscr{P}_K\ :\ NP \leq X\}}$$

A has *Dirichlet density* (or *analytic density*) a if

$$a = \lim_{s \to 1^+} \left(\frac{\sum_{P \in A} NP^{-s}}{\log \frac{1}{s-1}} \right)$$

Let K be a field, P a prime over $p \in \mathbb{Q}$. Say that P *has degree 1* if $N_{K/\mathbb{Q}} P = p$.

Proposition 22.1. Let $A = \mathscr{P}_K^{(1)} \subset \mathscr{P}$ be the set of primes of K of degree 1. Then the strong analytic density of A is 1.

$$\sum \frac{1}{NP^s} = \underbrace{\sum_p \sum_{Ps.tNP=p} \frac{1}{p^s}}_{degree\ 1} + (higher\ degree) \leq \sum \sum \frac{1}{p^s} + [K : \mathbb{Q}] \sum_{k \geq 2} \frac{1}{p^{ks}}$$

So, $A^{(1)} \subset A$ have the same densities. Similarly, the stuff of degree 1 over some other field F has the same density.

22.2. The Artin Map. We did not prove:

Theorem 22.2. Let L/K be an Abelian extension with Galois group G. There exists a signed divisor D of K and a surjective homomorphism called the Artin map

$$Cl_D(K) = \frac{I_D(K)}{Pr_D(K)} \overset{Artin}{\longrightarrow} G$$

such that the composition

$$P \mapsto \underbrace{[P]}_{\in Cl_D(K)} \overset{Artin}{\to} (P; L/K) = Frob_P$$

produces the Frobenius element.

In particular, consider the composition $I_D \overset{Artin}{\to} G \overset{\chi}{\to} \mathbb{C}^*$; clearly

$$L(s.\ \chi_D, L/K) = L^{D-incomplete}(s,\ \chi, L/K)$$

Proposition 22.3 (Regularity)**.** Let $\chi = \chi_D$ (i.e. a D-ideal class character) that is not principal. Then $L(1, \chi_D, K)$ is regular: that is, it is neither zero nor a pole.

This implies the same for abelian Artin L-functions. But we also get it for non-abelian Artin L-functions! We proved that Brauer's theorem implies the following: if χ is any non-abelian character, then $\chi = \sum_{\chi_i\ irred} n_i Ind_{H_i}^G \chi_i$ where $n_i \in \mathbb{Z}$. So

$$L(s,\ \chi, L/K) = \prod (L(s,\ \chi_i, L/K_i))^{n_i}$$

where K_i is the fixed field of H_i.

Theorem 22.4. Let L/K be an abelian extension. Let $c \in Gal(L/K)$, and define

$$A_c = \{P \text{ prime of } K\ :\ Frob_P = c\}$$

$$\text{Strong analytic density of } A_c = \frac{1}{[L:K]}$$

Theorem 22.5 (General Chebotarev)**.** If L/K is any Galois extension, and $C \subset G$ a conjugacy class. Let $A_C = \{P\ :\ Frob_P = C\}$. Then

$$\text{Strong analytic density of } A_C = \frac{|C|}{[L:K]}$$

Lemma 22.6. G is a finite group, C a single conjugacy class. Let δ_C be the characteristic function of C: $\delta_C(x) = \begin{cases} 1 & x \in C \\ 0 & x \notin C \end{cases}$. Then

$$\delta_C = \frac{|C|}{|G|} \sum_{\chi\ irred} \overline{\chi}(c)\ \chi$$

ABELIAN IDEAL CLASS L-FUNCTION THEOREM $\to$ GENERAL. $\delta_C = \sum_{\chi\ irred} a(\chi)\cdot\chi$. By orthonormality,

$$\frac{1}{|G|}\sum_{x\in G}\delta_C(x)\overline{\chi}(x) = a(\chi)$$

$$a(\chi) = \frac{1}{|G|}\sum_{x\in C}\overline{\chi}(x) = \frac{|C|}{|G|}\overline{\chi}(x)$$

Let $Frob_P$ denote the conjugacy class of $Frob$ at P in G.

$$\sum_{P\in A_c} NP^{-s} = \sum_{P\in\mathscr{P}_K}\delta_C(Frob_P)\cdot NP^{-s} = \frac{|C|}{|G|}\sum NP^{-s} + \frac{\mathbb{C}|}{|G|}\sum_{\chi\ irred\ \neq 1}\overline{\chi}(c)\sum_P \chi(Frob_P)\cdot NP^{-s}$$

because the principal character applied to $Frob_P$ is just 1.

We want to show that the second term has no effect (is analytic), and in particular, that $\sum_P \chi(Frob_P)\cdot NP^{-s} \sim 0$ for fixed χ nonprincipal. This comes from the regularity theorem for nonabelian characters. □

ARTIN ABELIAN THEOREM $\to$ ARTIN GENERAL THEOREM. We had a Galois extension L/K with Galois group G. Let $C\subset G$ be a conjugacy class, and let $g\in C$ (choice shouldn't matter!). Let M be the fixed field under g; so L/M has Galois group cyclic, generated by g. Let p denote a prime in $\mathbb{Q}$, π a prime in K, P a prime in M, and Q a prime in L. As before, norm always means norm down to $\mathbb{Q}$. L/M is an abelian extension. Suppose we want $Frob_P = g$. That implies that P is inert in L/M. So there exists a unique Q lying over P. Let $G_Q\subset G$ be the stabilizer of Q in G. If $Frob_P = g$ then $G_Q = \langle g\rangle$. So the notation $G_Q = G_P$ makes sense.

When we compute analytic density, we only care about the degree-1 primes π. If P lies over π then it is also degree 1: its decomposition group is just G_Q.

We're trying to compute A_C in $\mathscr{P}_K$: the primes of K whose Frobenius live in C. We want:

$$\sum_{\substack{\deg\pi=1\\ \exists Q, Frob_Q = g}} (N\pi)^{-s} \sim \frac{|C|}{|G|}\log\frac{1}{s-1}$$

The LHS is $\sum p^{-s}\cdot\#\{\pi\to p,\ \exists Q\to\pi, Frob_Q = g\}$. For every Q, there is a corresponding P. So this is

$$\sum_p p^{-s}\cdot\#\{\pi\to p\ :\ \exists P\to\pi, Frob_P = g\} =: f(s)$$

We want to compare this with the RHS

$$g(s) := \sum p^{-s}\#\{P\ :\ \deg P = 1, Frob_P = g\} = \sum_{\substack{\deg P=1, Frob_P = g\\ P\to p}} (NP)^{-s}$$

By the abelian theorem (or, even the cyclic theorem), this is

$$\sim \frac{1}{|\langle g \rangle|} \cdot \log \frac{1}{s-1}$$

Lemma 22.7.

$$\# := \#\{P \to \pi, \deg P = 1, Frob_P = g\} = \frac{|G|}{|\langle g \rangle| \cdot |C|}$$

This is the number of primes over π that has the same Frobenius element as g. (We're assuming that $\# > 0 \ldots$ this should end up in the theorem hypotheses...)

Note that if there is some Q over P with $Frob_Q = g$, then that Q is unique. So $\# = \#\{P \to \pi, \deg P = 1,\ \exists Q \to P, Frob_Q = g\}$. Let $\{Q, Q_1, \cdots, Q_?\}$ be the other primes over π. Every Q_i is given by a conjugacy class of G/G_Q. $Frob_{xQ} = xgx^{-1}$. The number = the number of x that commute with g; this is the commutator in G of g. Anything in G_Q doesn't change anything; so we divide by G_Q:

$$\# = \frac{Centralizer_G(g)}{G_Q}$$

I claim that $Cent_G(g) = \frac{|G|}{\#\text{elts. conjugate to } g} = \frac{|G|}{|C|}$. So

$$f(s) \sim \frac{|C|}{|G|} \log \frac{1}{s-1}$$

□