2009 Graduate Workshop on Zeta functions, L-functions and their Applications

Steven J. Miller

June 4, 2009

Contents

Abstract

These notes were TeXed in real-time by Steven J. Miller; all errors should be attributed to the typist.

1 Conrey: Random Matrix Theory and analytic number theory

1.1 Introduction to Random Matrix Theory I

`http://www.williams.edu/go/math/sjmiller/public_html/ntandrmt/talks/Random_matrix_theory_Conrey.ppt`

I'm giving four talks, the four R's of random matrix theory and analytic number theory: random matrix theory, recipe, ratios, ranks. It has to do with how random matrix theory has had an interface with the theory of L-functions in recent times. It's an indispensable tool that analytic number theorists need to know. When I was a student, we didn't need to know about modular forms, but at University of Michigan we just had one course on modular forms. That has changed, and for the better. It's great that it has spread out. Will give a perspective.

For the first talk there won't be any number theory, all just random matrix theory.

$U = (u_{jk})$, $U^t = (u_{kj})$ and $U^* = (\overline{u_{kj}})$. Will talk about $U(N)$, $SO(N)$ and $USp(2N)$, where for$USp(2N)$ we have all matrices $P \in U(2N)$ such that $PZP^t = Z$ with $Z = \begin{pmatrix} 0 & I_N \\ -I_N & 0 \end{pmatrix}$.

The eigenvalues split into even and odds for the orthogonal. All the matrices have their eigenvalues on the unit circle. For the unitary have angles between 0 and 2π; for others eigenangles symmetric so just look from 0 to π.

All of these compact groups have a Haar measure associated to them. For the purpose of integrating functions which are class functions (the function only depends on the eigenvalues of the matrix), we want to integrate over the groups. In these cases the Haar measure reduce to these Weyl formulas in the four cases.

We won't use the fact that these are Haar measures, and just think about these things and what we can do with them. Why are we doing this? Look at the eigenvalues of a randomly generated 96×96 unitary matrix versus 96 randomly chosen points on the circle, constructed by $\exp(2\pi ix)$ with x uniformly chosen on $[0, 1]$. Can see qualitatively a big difference between the two. The uniformly chosen points have clumps and gaps (Poisson), whereas the unitary one is more nicely spaced.

This comes about from the quadratic repulsion in the measures. For example, for the unitary case we have in teh density the factor $\prod_{j<k} |e^{i\theta_k} - e^{i\theta_j}|$.

Now look at the zeros of the Riemann zeta function $\zeta(s)$ at height 1200, take 96 zeros and wrap around the unit circle. (This was done by taking the distance from the first to the last and rescaling to make that equal 2π.) The distribution looks like the distribution from the unitary matrices, not like the Poisson.

The subject began with Montgomery and Dyson, but this picture is a great motivation for why we want to look at this. These really are, we believe, the measures that come up when we study L-functions.

Back to the Haar measure. What this means is that if we want to integrate $\int_{SO(2N)} f(O) dO_N$ then we can write this as

$$\frac{2^{(N-1)^2}}{\pi^N N!} \int_{[0,1]^N} f(\theta_1, \ldots, \theta_N) \prod_{j<k} (\cos\theta_k - \cos\theta_j)^2 d\theta_1 \cdots d\theta_N. \tag{1}$$

Everything we're goign to do today is at the level of undergraduate linear algebra, calculus of several variables, would be great for a really good undergraduate course. We're going to do really cool tricks with linear algebra, determinants, ..., and doing for a reason!

Will express everything in terms of Vandermonde determinants: $\Delta(x_1, \ldots, x_N) = \det_{N\times N}(x_k^{j-1})$. For example,

$$\begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{vmatrix}. \tag{2}$$

Note that $\Delta(x_!, \ldots, x_N) = \prod_{j<k}(x_k - x_j)$. Calculate the total degree of both sides, calculate order of vanishing, see it vanishes whenever any of the two are equal. This nails it down up to a constant, then look at the coefficient of $x_N^{N-1} x_{N-1}^{N-2} \cdots x_2$ is 1. (NOTE FROM TYPIST: to see the constant is non-zero, can we just look at $x_N \gg x_{N-1} \gg x_{N-2} \gg \cdots$ for $i \neq N$?) We see that the measures are related to Vandermonde determinants.

Where do we want to go? If Haar measure, then it has mass one over the group. We want to verify from first principles that the total mass of these measures is 1. In other words, if we integrate the function which is identically 1 we get 1, ie, we have probability measures. We use Andréief's identity. For functions ϕ_j and ψ_j

and any interval J we have

$$\frac{1}{N!}\int_{J^N} \det_{N\times N}(\phi_j(\theta_k)) \det_{N\times N}(\psi_j(\theta_k))d\theta_1\cdots d\theta_N \;=\; \det_{N\times N}\int_J \theta_j(\theta)\psi_k(\theta)d\theta. \quad (3)$$

Could use $\psi_k = \overline{\phi_j}$.

(Aside: In some ways the unitary case is the one you want to do the most / the one most connected to the zeta function, but doesn't fit in as well with the other case. Often have to argue slightly differently for unitary versus non-unitary, but all works out.)

For the unitary case $U(N)$, we take $\phi_j = e^{i(j-1)\theta}$ and $\psi_k = e^{-i(k-1)\theta}$. We get the integral vanishes unless $j = k$, in which case we find the total mass is 1.

We now turn to the orthogonal and symplectic cases. We will use some preparatory work to deal with the cosines. It is convenient to introduce orthogonal polynomials (Chebyshev polynomials). We let

$$\begin{aligned} T_n(\cos\theta) &= \cos(n\theta) \\ U_n(\cos\theta) &= \frac{\sin((n+1)\theta)}{\sin\theta} \\ V_n(\cos\theta) &= \frac{\sin((n+\frac{1}{2})\theta)}{\sin\frac{\theta}{2}}. \end{aligned} \quad (4)$$

These are orthogonal on $[0,\pi]$ with respect to various measures. $T_n^*(x) = \sqrt{2}T_n(x)$. The measures are $d\theta$ for T^*, $\sin^2\theta d\theta$ for U and $\sin^2\frac{\theta}{2}d\theta$ for V. Each vector has the same norm in these spaces.

We now rewrite the Vandermonde by using elementary row operations. For example,

$$\Delta(\cos\theta_1,\ldots,\cos\theta_N) \;=\; 2^{-N(N-1)/2}\det_{N\times N}(V_{j-1}(\cos\theta_k)) \quad (5)$$

(and similar formulas with T^* and U).

We rewrite all the measures as squares of determinants of things that are orthogonal.

For others use the Generalized Andréief, except now we have an extra function f:

$$\frac{1}{N!}\int_{J^N}\prod_{i=1}^{N} f(\theta_i)\det_{N\times N}(\phi_j(\theta_k))\det_{N\times N}(\psi_j(\theta_k))d\theta_1\cdots d\theta_N \;=\; \det_{N\times N}\int_J f(\theta)\theta_j(\theta)\psi_k(\theta)d\theta. \quad (6)$$

The proof of Andréief's identity proceeds by using the definition of the determinant, expanding it with the sign function (ie, we sum over all permutations). We now change variables, rearrange things, and eventually wind up with the answer. We first send $\tau \to \sigma\tau$ then $k \to \tau^{-1}k$. The key fact is that whatever σ is, when τ runs through all permutations so too does $\sigma\tau$. Several typos on the slides, but the idea is to just expand the determinants, change variables, ...

Goal of the talk: the first picture was of all the spacings. How do you calculate the neighbor spacing distribution in random matrix theory? How do we calculate the spacings of the 96 eigenvalues when we average over all unitary matrices of that size? This is where we're heading.

The following lemma (needs a name, call it the Transposing Lemma – it is a critical step): if you have a product of two determinants you can rewrite as a determinant of something else. The identity follows from the fact that the determinant of a matrix and its transpose are the same, and matrix multiplications:

$$\det_{N\times N}(\phi_{j-1}(x_k)) \det_{N\times N}(\psi_{j-1}(x_k)) \;=\; \det_{N\times N}\left(\sum_{n=1}^{N} \phi_{n-1}(x_j)\psi_{n-1}(x_k)\right). \qquad (7)$$

The ϕ's and ψ's are orthogonal polynomials – we multiply and sum, and this will lead to a simpler formula. It is essential that it is in this format. This will be useful in transforming the Haar measures, which are products of two determinants, into something more useful.

We do that and we now transpose the square determinants in the measures. We wind up with nice formulas for the various measures. For the unitary, we are now summing a geometric series, and there is a nice formula for that. For the Chebyshev polynomials, we get things like geometric series, involving things like sums of $\cos(n\theta_j)\cos(n\theta_k)$, in other words, things we know how to sum.

How do we add these up? There is a general theory in orthogonal polynomials on how to do this: Christoffel-Darboux. We don't need the general theory as we're adding trigonometric things. Everything is in terms of $S_N(\theta) = \sin(N\theta/2)\,/\sin(\theta/2)$. We thus get formulas for all of these expansions in terms of S_N. We give this names:

$$S_{U,N}(x,y) \;=\; S_N(y-x) \qquad (8)$$

and so on. We then find alternate formulas, such as

$$dU_N \;=\; \det_{N\times N}\left(S_{U,N}(\theta_j,\theta_k)\right)\frac{d\theta_1\cdots d\theta_N}{(2\pi)^N N!}. \qquad (9)$$

We're now ready for a big step, Gaudin's lemma. This will allow us to compute statistics for these groups. The set-up is as follows. We have a function f of two variables and some interval J. Suppose $\int_J f(x,\theta)f(\theta,y)d\theta = Cf(x,y)$ for all x, y and $C = C(J,f)$ is a constant, and $\int_J f(x,x)dx = D$. Then

$$\int_J \det_{M\times M}(f(\theta_j,\theta_k))d\theta_M = (D-(M-1)C) \det_{(M-1)\times(M-1)}(f(\theta_j,\theta_k)). \tag{10}$$

We use this repeatedly to integrate out eigenvalues. If we want information about one eigenvalue, we would apply $N-1$ times. We keep applying, this is the key step for everything. Some people call this the integrating out lemma, as we integrate out just the last variable, θ_M.

We now use Gaudin's lemma for O, O^- or USp. Say we care about n-level correlation. We apply this with $M = N$ and then $M = N-1$ all the way down to $M = n+1$. We find

$$\int_{[0,\pi]}^{N-n} \det_{N\times N} S_{G,N}(\theta_j,\theta_k)d\theta_{n+1}\cdots d\theta_N \ = \ \pi^{N-n}(N-n)! \det_{n\times n} S_{G,N}(\theta_j,\theta_k). \tag{11}$$

We need to prove the reproducing property of $S_{P,N}$.

We use Gaudin's lemma to compute the n-level density. We have a big $N\times N$ matrix, and we have a n (say 3, 4 or 10). We have a function f of these few variables. We want to sample f at every choice of n variables for each choice of matrix. Say we want to do 3-level density. We pick out each subset of three eigenvalues of N and evaluate f at those three variables (f is a symmetric function, so order does not matter). We add up over all subsets of 3 of N variables for one matrix, and then do for every matrix (ie, average using Haar measure). We have just proved that this equals integrating our function against a determinant, where the determinant only depends on n variables and not N variables.

We then get the 1-level density function for each group.

Won't return to random matrix theory in the rest of the lectures:

1.2 Introduction to Random Matrix Theory II: The Recipe

`http://www.williams.edu/go/math/sjmiller/public_html/ntandrmt/talks/The_recipe_A.ppt`

How do you make a conjecture for moments of L-functions? This has grown out of Random Matrix Theory. What we'll do has been numerically and theoretically tested and does very well. It's a great tool to teach the recipe.

1.2.1 Introduction

Started with the zeta function. In 1918 Hardy and Littlewood showed the mean square was $\log T$, and in 1926 Ingham showed the fourth moment was a constant time $\log^4 T$. The constant can be written in more enlightening ways, which fits with the pattern that Conrey and Ghosh found in 1992 for the sixth moment. No one had a conjecture for what these moments should look like; there was a sense for the power of $\log T$ in the problem, but not for the constant in front of it, even conjecturally. Everyone wanted to do (and still want to do!) the sixth moment. There would be numerous applications to zero density arguments, gaps between primes, but no one tried to figure out an asymptotic formula (or if they tried, weren't able to work it out).

What is the problem? We think of $\zeta(s)$ as having an approximate functional equation

$$\zeta(s) \;=\; \sum_{n\leq\sqrt{t/2\pi}} \frac{1}{n^s} + \chi(s) \sum_{n\leq\sqrt{t/2\pi}} \frac{1}{n^{1-s}} + \cdots . \tag{12}$$

We can do similar expansions for $\zeta(s)^2$ and $\zeta(s)^k$:

$$\begin{aligned}
\zeta(s)^2 \;&=\; \sum_{n\leq\sqrt{t/2\pi}} \frac{d(n)}{n^s} + \chi(s) \sum_{n\leq\sqrt{t/2\pi}} \frac{d(n)}{n^{1-s}} + \cdots \\
\zeta(s)^k \;&=\; \sum_{n\leq\sqrt{t/2\pi}} \frac{d_k(n)}{n^s} + \chi(s) \sum_{n\leq\sqrt{t/2\pi}} \frac{d_k(n)}{n^{1-s}} + \cdots ,
\end{aligned} \tag{13}$$

where $\zeta(s)^k = \sum_n d_k(n)/n^s$. What tools do we have? We have

$$\int_0^T \left| \sum_{n=1}^N a_n n^{it} \right|^2 dt \;=\; (T + O(N)) \sum_{n=1}^N |a_n|^2, \tag{14}$$

using

$$\int_0^T (m/n)^{it} dt \;=\; \begin{cases} T & \text{if } m = n \\ \frac{(m/n)^{iT}-1}{i\ln(m/n)} & \text{otherwise.} \end{cases} \tag{15}$$

The problem is we need to evaluate

$$\sum_{n=1}^N d_3(n) d_3(n+1) \tag{16}$$

for the moments. Using conjectures like these, one gets sixth and eight moments, but doesn't work for the tenth moment (ended up with a negative answer, which can't be right). The point is that we can interpret these as using the method of long polynomials with shifts up to T^2, but past there something new needs to be added.

Conrey and Ghosh (1985) said there should be an integer g_k such that the $2k^{\text{th}}$ moment should look like $(g_k a_k/k^2!)\log^{k^2} T$. What is the next term in the sequence of g_k's: $1, 2, 42, 24024, \dots$?

Berry and Keating were at the conference in Seattle. For some reason the number theorists weren't excited about his work on lower order fluctuations. Sarnak told Keating that to make a splash he should use random matrix theory to figure out the 42. So Keating went back to Bristol, assigned the problem to his current graduate student Nina Snaith. They worked it out. Assume zeros are behaving like eigenvalues of matrices, so perhaps the values of the zeta function behave like the values of characteristic polynomials. They then calculated the moments for characteristic polynomials. Amazingly enough, this calculation can be done exactly. They recover the sequence: $1, 2, 42, 24024, 701149020, \dots$.

If you have an $N \times N$ matrix such that the average spacing is $2\pi/N$, should match up the average spacing between eigenangles and zeros to be the same. So $N = \log T$ to get the zeros and eigenangles to have the same scale. We want a $k^2!$ in the denominator, and get an explicit form for the g_k's. It was conjectured that g_k should be an integer. Think of g_k as the number of Dirichlet polynomials of a given length that are needed for approximating, and thus it is reasonable to expect to get an integer. It turns out that g_k is an integer (Conrey-Farmer), but not easy to see this. For example, look at the expansion for g_{100}: several primes come in at the zeroth power after others had been larger, and thus almost was non-integer.

Selberg's integral formula is used for these computations:

$$\int_0^1 \cdots \int_0^1 |\Delta(x)|^{2\gamma} \prod_{j=1}^n x_j^{\alpha-1}(1-x_j)^{\beta-1} dx_1 \cdots dx_n$$

equals a product of Gamma functions. There are various forms of Selberg's integral. To evaluate their integrals, start with $|e^{i\alpha} - e^{i\beta}| = 2|\sin(\alpha/2 - \beta/2)|$, use trig identities involving $\sin(\alpha-\beta) = (\mathrm{ctan}\alpha - \mathrm{ctan}\beta)\sin\alpha\sin\beta$, and eventually get to a place where you can use Selberg's integral.

Can do this for other families of L-functions. How do you know what symmetry type to attach to a family of L-functions? The original theory grew up from Katz and Sarnak, who looked at function field examples. There one had monodromy groups, there was thus an obvious symmetry group (which was one of the classical compact groups). These families had analogues in the number field setting in many cases, and allowed one to figure out what group should be attached.

If you take any L-function in the Selberg class (functional equation, Euler product) and shift up the imaginary parameter and regard the family as parametrized by that parameter, one gets a unitary family: $L(s + i\alpha)$ with $\alpha \in \mathbb{R}$ varying. Another unitary family is the collection of Dirichlet characters: $L(s, \chi)$ with χ a Dirichlet character. For orthogonal examples, one has cuspidal newforms / elliptic curves, while for symplectic one can look at quadratic characters and symmetric squares of cuspidal newforms.

Similarly, one can look at moments of quadratic L-functions. Jutila computed the first and second moments of $L(1/2, \chi_d)$, Soundararajan did the third and fourth moments (the fourth was conjectural). The corresponding powers of the logarithms are 1, 3, 6 and 10; one can get these numbers and values by averaging characteristic polynomials of symplectic matrices. Various people did similar computations for moments of weight 2 and prime level q cusp forms; now the powers are 0, 1, 3 and 6. One can again do a similar computation in random matrix theory, and again we are able to reproduce these numbers.

These conjectures are not numerically testable, unfortunately. If you tried the 42 on the sixth moment, in any reasonable range we can integrate we'll be off by large factors. The problem is that we're missing other 'main' terms; in other words, we should have a polynomial of degree k^2 in $\log T$ for the $2k^{\text{th}}$ moment of the zeta function. We knew this for the second (Ingham) and the fourth (Heath-Brown) moments of zeta. These polynomials can be determined, but what are their analogues?

This can be done. The trick is not to look directly at the mean square, but to put in shifts, see symmetries, and can make sense of it:

$$\begin{aligned} & \int_0^T \zeta(s+\alpha)\zeta(1-s+\beta)dt \\ = \quad & \int_0^T \left(\zeta(1+\alpha+\beta) + e^{-\ell(\alpha+\beta)}\zeta(1-\alpha-\beta)\right) dt + O(T^{1/2+\epsilon}) \end{aligned} \tag{17}$$

where $\ell = \log(t/2\pi)$. There is a random matrix analogue. Let $X = U(N)$ have eigenvalues $e^{i\theta_n}$ with characteristic polynomial $\Lambda_X(s) = \prod_{n=1}^N (1 - se^{-i\theta_n})$, and obtain a formula for integrating shifts over $U(N)$. Looks very similar. Can do something similar for the fourth moment. The poles cancel and get something regular. Get α, β on one side and γ, δ on the other, see how things are switched. We get a random matrix analogue for this.

Conrey, Farmer, Keating, Rubinstein and Snaith prove a theorem for

$$\int_{U(N)} \prod_{\alpha \in A} \prod_{\beta \in B} \Lambda_X(e^{-\alpha}) \Lambda_{X^*}(e^{-\beta}) dX. \tag{18}$$

Make an analogous conjecture for the zeta function, will try and make clear with the recipe in a minute. Leads to a conjecture for the $2k^{\text{th}}$ moment of the zeta function.

This leads to explicit formulas for the polynomial for the sixth moment. We get a polynomial of degree 9; unfortunately the 'main' term has a coefficient significantly smaller than the other computations. The conjecture is correct to about 5 digits, while if we just use the main term coming from 42 we're off by a factor of about 45.

1.2.2 The Recipe

There are three or four steps, each one is illegal, but it does produce the right answer in the end. It's a mystery as to why this gives the right answer in the end.

We have an integral of products of shifts of the zeta function. We use the approximate functional equation involving two sums. Note $\chi(s)$ is rapidly oscillating. Focus on only those terms with the same number of $\chi(s)$ and $\chi(1-s)$ terms. Leads to $\binom{2K}{K}$ terms. Take the first term, which has no χ terms. We only look at the diagonal term, when the product of the m's equals the product of the n's. Use $T^{-1}\int_0^T (m/n)^{it}$ tends to 1 if $m = n$ and 0 otherwise. It turns out to be multiplicative, and only need to figure out what happens at the primes. We get a product of zeta functions.

Say we have

$$\begin{aligned} &\sum_{m_1 m_2 = n_1 n_2} \frac{1}{m_1^{1/2+\alpha_1} m_2^{1/2+\alpha_2} n_1^{1/2+\beta_1} n_2^{1/2+\beta_2}} \\ &= \prod_p \sum_{m_1+m_2=n_1+n_2} \frac{1}{p^{(1/2+\alpha_1)m_1+(1/2+\alpha_2)m_2+(1/2+\beta_1)n_1+(1/2+\beta_2)n_2}}, \end{aligned} \tag{19}$$

where we sent $m_i \to p^{m_i}$ and similarly for the n's. We get

$$\prod_p \left(1 + \frac{1}{p^{(1/2+\alpha_1)+(1/2+\beta_1)}} + \frac{1}{p^{(1/2+\alpha_1)+(1/2+\beta_2)}} + \cdots\right) \tag{20}$$

and this leads to products of zeta functions evaluated at the α_i's and β_j's.

It isn't clear that what we have is analytic as all the shifts tend to zero, but we can re-write it in a nice integral form that makes this 'clear'. Writing it like this, using symmetric functions we can see that the poles cancel.

What would the recipe be for quadratic L-functions? It's basically the same, but with a different harmonic detector. We now have

$$\frac{1}{D^*}\sum_{d\leq D}\chi_D(n) \;=\; \begin{cases}\prod_{p|n}\frac{p}{p+1} & \text{if } n \text{ is a square}\\ 0 & \text{otherwise.}\end{cases} \tag{21}$$

We argue as before:

$$\begin{aligned}&\sum_{d\leq D}\sum_{m_1}\frac{\chi_d(m_1)}{m_1^{1/2+\alpha_1}}\cdots\sum_{m_K}\frac{\chi_d(m_K)}{m_K^{1/2+\alpha_K}}\\ =\;&\sum_{m_1,\dots,m_K}\frac{1}{m_1^{1/2+\alpha_1}\cdots m_K^{1/2+\alpha_K}}\sum_{d\leq D}\chi_d(m_1\cdots m_K).\end{aligned} \tag{22}$$

How do we get a square? We need $m_1\cdots m_K = \Box$. We change variables and set $m_j = p^{m_j}$. This leads to the requirement that $m_1+\cdots+m_K$ is even. We argue similarly as before. We need a combinatorial lemma involving a symmetric function of k variables that is regular near the origin and multiplied by a product of a function with a simple pole at $s=0$. This allows us to turn sums into integrals, and is the key step for making sure the resulting terms are regular.

Numerics give phenomenal agreement between conjecture and reality.

Have conjectures for averaging over all primitive Dirichlet characters modulo q. Conrey, Iwaniec and Soundararajan obtain an asymptotic formula with a power savings. There were more than 200 main terms, most of which cancel out. If we hadn't known what we were looking for, never would have sorted it out.

`http://www.williams.edu/go/math/sjmiller/public_html/ntandrmt/talks/The_recipe_A.ppt`

1.3 Ranks

Today we'll discuss an application to a very arithmetic situation. I really like this as there doesn't seem to be any other way to get a hold on this. The basic question is: twist a given elliptic curve and ask how often you get rank 2 as $d\leq D$. We can get some very nice answers using random matrix theory.

1.3.1 Numerics: Mathematica Program

For the different symmetry types of L-functions (unitary, symplectic or orthogonal), there are similarities in the products of the zeta factors and the products of the classical compact group – similar shape. We did integral values of k for moments, but Keating and Snaith did any moment, not just integral but actually complex as long as the real part of s is sufficiently large (so that the integral will converge).

Take L-function, go up to height 1000000, randomly sample in each interval of size 1 for awhile, sort, look at the bottom 10% say, see histogram plot. Want to work out how often we get rank 2. The values in families of L-functions are distributed the same as those of characteristic polynomials in random matrix families.

A Mathematica program is online at

```
http://www.williams.edu/go/math/sjmiller/public_html/
    ntandrmt/programs/ZetaValuesOnCriticalLine.nb
```

1.3.2 Number Theory Question

Which integers m are the sum of two rational cubes? Examples include 1729, 6, 346, ... If m is congruent to 4, 7, 8 or 9 then it is believed there is always a solution to $x^3+y^3 = m$; if m is 1, 2 or 5 modulo 9 than the solutions are believed to be rare. Random matrix theory conjectures that for these congruences, the number of $m \leq x$ with a solution and m square-free is about $Cx^{5/6}(\log x)^{\sqrt{3}/2-5/8}$. Might initially think equidistributed among the congruence classes, though Watkins found a lot more (about twice as many) that are 2 modulo 7 than 3 modulo 7.

Some number theory (from Gauss): if $p \equiv 1 \bmod 3$ then there are three solutions to $4p = a^2 + 3b^2$ with $a \equiv 2 \bmod 3$. Gauss gave a formula for the number of solutions: $p + 1 - a_{p,m}$, Watkins conjectures a formula involving $a_{p,b}$.

How to get this conjecture? Depends on elliptic curves, Birch and Swinnerton-Dyer conjecture, values of L-functions. An elliptic curve $E : y^2 = x^3 + Ax + B$ with A, B integers has an associated abelian group of rational solutions. The Birch and Swinnerton-Dyer conjecture states the order of this group equals the vanishing of the associated L-function at the central point.

How do you define the L-function? The way you define an L-function is by one prime at a time, where $a_p = p + 1 - N_p$ with N_p the number of points on E over the finite field of p elements. By Wiles et al, we know the L-function is entire and satisfies a functional equation with a root number $w_E = \pm 1$. Note there are two normalizations, with the central point either at 1 or 1/2.

Let d be a fundamental discriminant and $\chi_d(n)$ the Kronecker symbol. We can define the twisted L-function by

$$L_E(s) \ = \ \sum_{n=1}^{\infty} \frac{a_n \chi_d(n)}{n^s}, \tag{23}$$

which differs from the old L-function by the factor of $\chi_d(n)$; equivalently, the twisted elliptic curve is now $E_d : dy^2 = x^3 + Ax + B$. The root number is now $\chi_d(-Q)w_E$.

1.3.3 Vanishing

Goldfeld conjectured that half the time the rank is 0 and half the time the rank is 1 in these families of quadratic twists. By random matrix theory, we expect rank 2 curves to occur in these quadratic families for $d < x$ about $C_E x^{3/4} (\log x)^{b_E}$, where the exponent depends on the elliptic curve (how the elliptic curve factors).

Key point: how will we be able to pick out when it vanishes? There is a formula for the value at the central point. From lots of people, we know that for twists of E_{11} we have

$$L_E(1/2, \chi_d) \ = \ \kappa_{11} c_{11}(|d|)^2 \sqrt{d}, \tag{24}$$

with κ about 2.9176. We are going to create a random matrix model that models the values of these L-functions. We will ask what the probability of the value of the characteristic polynomial is smaller than $\kappa_{11}/\sqrt{d}$, as if it less than this it must be zero (as the $c_1 1(|d|)^2$ is an integer).

Quadratic twists form an orthogonal family, using even functional equations so want $\mathrm{SO}(2N)$. What is the probability that the value of a characteristic polynomial is at most α? The probability density is known, so just have to do the integral. (Get this from Perron's formula.) Use information about poles, Barnes G-function, get an $N^{3/8}$ which is why we have a $\log x$ to the 3/8 (comes from random matrix theory, not number theory).

So $L_E(1/2, \chi_d) = \kappa c_d^2/\sqrt{d}$ and if it is less than $\kappa/\sqrt{d}$ it is zero, so

$$\mathrm{Prob}(L_E(1/2, \chi_d) < \kappa/\sqrt{x}) \ \sim \ c a_{-1/2} (\log x)^{3/8} x^{-1/4}. \tag{25}$$

It is important that we can take moments to an arbitrary complex power; this allows us to recover the distribution of values. . We have a lot of data, theta functions worked out for over 2000 elliptic curves, taking hundreds of millions of quadratic twists for each. Looked at prime twists up to 10^8. Very flat. The problem is we don't know what C_E is. For half the residue classes get one answer, for another get a different answer. Take ratio, lots of stuff cancels out except for the arithmetic factor at the prime p where we are looking at the d's modulo that p. The advantage of these ratios is that all the unknown things cancel. Left with an answer on how rank 2 twists are distributed in arithmetic progressions.

Went and also calculated a lower order term to see if it would help. It's complicated and depends on the recipe from yesterday. We can compute things for integer k, get an analytic function of k, even though can't do arbitrary moments think can identify terms down, used this and see a very noticeable difference. Gets much better.

What about rank 3 in families of quadratic twists? We have a formula from the Birch and Swinnerton-Dyer conjecture, involving regulator, the order of the Tate-Shafarevich group, the order of the torsion group, ... Snaith calculated the derivative of the characteristic polynomial, but sadly when one plugs it in the resulting conjecture does not agree with data; however, the ratios experiment still works.

One Saturday Evening at the Newton Institute:

Conjecture 1.1 (Saturday Night Conjecture)**.** *There exists a $\theta \in (0, 1/2)$ such that for any elliptic curve over $\mathbb{Q}$ and fundamental discriminant d with $L_E(1/2, \chi_d) = 0$ and $L_E'(1/2, \chi_d) \neq 0$ it is the case that $L_E'(1/2, \chi_d) \gg d^{\theta - 1/2 - \epsilon}$. Maybe $\theta = 1/6$??*

Can do for weight 4 modular forms. Discretization changes. The central value should be $1/d^{(k-1)/2}$. The difference is when $k = 2$ we had something that summed to $x^{3/4}$, whereas now we'll get something that sums to $x^{1/4}$. When you put in $k = 6$ the series will converge, and thus only expect finitely many.

David, Fearnley and Kivilevsky obtain $x^{1/2-\epsilon}$ for twists of a weight 2 form by a cubic Dirichlet character; RMT predicts $x^{1/2}$ with some log factors.

1.4 Ratios

Note: I said on the first day that there is no good book on random matrix theory; I forgot Steve Miller's book. Chapter 15 of that book (an introduction to classical random matrix theory and applications to L-functions):

`http://press.princeton.edu/chapters/s15_8220.pdf`

Mean averages of products of quotients of characteristics polynomials or L-functions. Integral moments: did products of shifts of L-functions, now will have L-functions in the denominator. We have a conjecture that uses a recipe like the one from integral moments that allows us to conjecture; on the random matrix theory side can prove the answer. Great parallel. The integral moment is contained in the ratios (just take nothing in the denominator). Can do any statistic you want with the ratios. Think of statistics of zeros / spacings as local statistics, but when you do moments that is more subtle (global statistics), the random matrix theory we saw on the first day harder with shifts, didn't show how to do. Ratios branches between the two: can recover zero statistics. There are some fluctuations between data and the main term predictions; the ratios conjecture allows us to predict the lower order term. Another application is the mollifier example. Gonek talked about the first 2 pages of Levinson's 70 page paper (the rest is evaluating the integral). He didn't know ahead of time that the integral would work out and give such a good constant – he could have gotten at least -1/3 of the zeros! With ratios it gives a quick well to tell the answer to questions like this before doing 68 pages of computations!

Have

$$R_\zeta(\alpha,\beta,\gamma,\delta) \ = \ \int_0^T \frac{\zeta(s+\alpha)\zeta(1-s+\beta)}{\zeta(s+\gamma)\zeta(1-s+\delta)}dt. \tag{26}$$

Farmer conjectured for small $\alpha,\dots,\delta$ the answer.

1.4.1 Ratios Conjecture

At an MSRI conference in 1998 mentioned this and asked if anyone had seen something similar. Zirnbauer was in the audience, and knew how to do it for characteristic polynomials:

$$\int_{U(N)} \frac{\Lambda_A(e^\alpha)\Lambda_{A^*}(e^{-\beta})}{\Lambda_A^(e^{-\gamma})\Lambda_{A^*}(e^{-\delta})}dA. \tag{27}$$

Conjecture 1.2 (Ratios Conjecture: Conrey, Farmer and Zirnbauer)**.** *For* $\Re(\gamma),\Re(\delta) > 0$ *and imaginary parts of all* $\ll T^{1-\epsilon}$ *and* $s = 1/2+it$*, predict* $R_\zeta(\alpha,\beta,\gamma,\delta)$.

Sketch of steps:

- We use the approximate functional equation to expand the L-functions in the numerator. We don't worry about how far the sum should be as will extend later, and we will drop the error term in the approximate functional equation.

- Expand the denominator using the Mobius function
- We have four pieces: first piece is like

$$\sum_{m,n,h,k} \frac{\mu(h)\mu(k)}{m^{1/2+\alpha}n^{1/2+\beta}h^{1/2+\gamma}k^{1/2+\delta}} \int_0^T \left(\frac{mh}{nk}\right)^{it} dt; \tag{28}$$

take $mh = nk$ and the integral gives T. NO off diagonal terms, only keep the easy terms. We have a sum now that is multiplicative, and get

$$\begin{aligned} & T\prod_p \sum_{m+h=n+k} \frac{\mu(p^h)\mu(p^k)}{p^{(1/2+\alpha)m+(1/2+\beta)n+(1/2+\gamma)h+(1/2+\delta)k}} \\ = \; & T\prod_p \left(1+\frac{1}{p^{1+\alpha+\beta}}-\frac{1}{p^{1+\alpha+\delta}}-\frac{1}{p^{1+\beta+\gamma}}+\frac{1}{p^{1+\gamma+\delta}}+O\left(\frac{1}{p^2}\right)\right) \\ = \; & T\prod_p \left(1+\frac{1}{p^{1+\alpha+\beta}}\right)\left(1-\frac{1}{p^{1+\alpha+\gamma}}\right)\left(1-\frac{1}{p^{1+\beta+\gamma}}\right)\left(1+\frac{1}{p^{1+\gamma+\delta}}\right)\left(1+O\left(\frac{1}{p^2}\right)\right) \\ = \; & T\frac{\zeta(1+\alpha+\beta)\zeta(1+\gamma+\delta)}{\zeta(1+\alpha+\delta)\zeta(1+\beta+\gamma)}A_1(\alpha,\beta,\gamma,\delta) \end{aligned} \tag{29}$$

(recycling variables: $m \to p^m$ and so on). We then do the next three terms. The second is small as it has just one $\chi(s)$, as is the third term. The fourth term is large as it has a $\chi(s+\alpha)\chi(1-s+\beta)$ from the approximate functional equations.

1.4.2 Application: Levinson's integral

Let

$$M(s) \; = \; \sum_{n\le y} \frac{\mu(n)\frac{\log(y/n)}{\log y}}{n^s} \tag{30}$$

and consider the second moment of ζ mollified by M. We get something like

$$\int_0^T \zeta(s)\zeta(1-s)M(s)M(1-s)dt \tag{31}$$

and use the Ratios conjecture to get a prediction for this integral.

1.4.3 Classical Compact Group Theorems and $\zeta(s)$

Consider $\mathcal{R}(A, B; C, D)$, shifts of characteristic polynomials of unitary matrices and the corresponding integral of the ratio. Let $Z(A, B) = \prod_{\alpha \in A, \beta \in B} z(\alpha + \beta)$ with $z(x) = (1-e^{-x})^{-1}$. Set $Z(A, B; C, D) = Z(A, B)Z(C, D) \,/\, Z(A, D)Z(B, C)$. Then the ratios theorem relates $\mathcal{R}(A, B; C, D)$ to Z for unitary, orthogonal, symplectic.

We have similar formulas for ζ. Now set $Z_\zeta(A, B) = \prod_{\alpha \in A, \beta \in B} \zeta(1 + \alpha + \beta)$ and $Z_\zeta(A, B; C, D) = Z_\zeta(A, B)Z_\zeta(C, D) \,/\, Z_\zeta(A, D)Z_\zeta(B, C)$. Conjecturally formula is very similar, with $Z \to Z_\zeta$ and add an arithmetic factor.

1.4.4 Application to Pair Correlation

Can deduce all the lower order terms in pair correlation from this. We start with Montgomery's pair correlation formula, proved under RH if the support of $w(x) = 4/(4 + x^2)$. Odlyzko's data shows phenomenal agreement between the pair correlation of zeta zeros and the prediction high up; however, if you look at small zeros it is off by a bit. One thing to look at is the difference between the empirical and the expect, you see fluctuations. These lower order terms can be explained with the ratios conjecture. In the Bogomolny-Keating plot, you see a dip at the first zero of $\zeta(s)$ (both numerically and theoretically) (refined pair correlation conjecture of Bogomolny-Keating, Conrey-Snaith). In the lower order term see an integral against ζ'/ζ on the line $\Re(s) = 1$, but still see the dip from the zeta zeros.

How do you use the Ratios conjecture to produce this formula? Assume the ratios conjecture, get

$$\int_0^T \frac{\zeta'}{\zeta}(1/2 + it + \alpha)\frac{\zeta'}{\zeta}(1/2 - it + \beta)dt. \tag{32}$$

Want to evaluate

$$\sum_{\gamma, \gamma' < T} f(\gamma - \gamma'). \tag{33}$$

We can write this as an integral over contours $\mathcal{C}_1$ and $\mathcal{C}_2$ of the product of $(\zeta'/\zeta)(z)$ $(\zeta'/\zeta)(w)\, f(-i(z-w))$. Note we are differentiating the ratios conjecture – we can differentiate as it is supposed to be uniform in all the variables so differentiation is as legal as can be in a conjecture like this. To make this somewhat rigorous, assume test function has holomorphy properties and ratios conjecture holds for certain ranges of shifts, but expect final formula to hold in greater generality. Plot of what remains now looks random. The main term agrees with Montgomery's conjecture. Try to look at lower order terms in the pair correlation arguments of Montgomery starting on the other side.

Can do the same approach for pair correlation for RMT using the ratios theorem. This could be at the bottom of the combinatorics problems from Rudnick-Sarnak and Gao. How do we do this here? We sum a test function:

$$\int_{U(N)} \sum_{1\leq j,k\leq N} f(\theta_j,\theta_k) dU_N. \tag{34}$$

Use the ratios theorem to work things out, get a determinant

$$\begin{pmatrix} N & S_N(u-v) \\ S_N(v-u) & N \end{pmatrix}, \quad S_N(\theta) \ = \ \frac{\sin(N\theta/2)}{\sin(\theta/2)}. \tag{35}$$

If we scale by sending $\theta_i \to \theta_i N/2\pi$ and take the limit as $N \to \infty$ we recover the pair correlation function.

1.4.5 Other Applications

Can do triple correlations, 1-level density. Steve Miller and others have produced lower order terms (and agrees in some families up to square-root cancelation). Interesting plots by Mike Rubinstein (dot wherever there is a zero of an $L(s,\chi_d)$, see fascinating bands, ratios conjecture explains these patterns).

2 Murty:

2.1 Introduction to Artin L-functions

http://www.williams.edu/go/math/sjmiller/public_html/ntandrmt/talks/UtahWorkshopNotes.pdf

Let me begin some words about the Dedekind zeta function. Let k be an algebraic number field. Inside this number field we'll look at the ring of integers $\mathcal{O}_k$. It is a ring, and it is a Dedekind domain (a Dedekind domain is an integral domain where every ideal can be factored uniquely into a product of prime ideals). Every ideal $\mathfrak{a} = {\mathfrak{p}_1}^{a_1} \cdots {\mathfrak{p}_t}^{a_t}$, where the norm is given by $N\mathfrak{a} = [\mathcal{O}_k : \mathfrak{a}]$. We define the Dedekind zeta function by

$$\zeta_k(s) \ = \ \sum_{\mathfrak{a}} \frac{1}{(N\mathfrak{a})^s}, \tag{36}$$

which converges for $\Re(s) > 1$. As there is unique factorization, we have an Euler product

$$\zeta_k(s) \;=\; \prod_{\mathfrak{p}} \left(1 - \frac{1}{(N\mathfrak{p})^s}\right)^{-1}. \tag{37}$$

This is a generalization of the zeta function $\zeta(s) = \sum 1/n^s$, $\zeta_{\mathbb{Q}}(s)$.

In Riemann's paper he used the theory of theta functions to find the functional equation and analytic continuation, showing it has a simple pole of order 1 at 1:

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) \;=\; \pi^{(1-s)/s}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s). \tag{38}$$

As we'll talk about the Hurwitz zeta function later, it is worth mentioning it now:

$$\zeta(s,x) \;=\; \sum_{n=0}^{\infty} \frac{1}{(n+x)^s} \tag{39}$$

for $0 < x \leq 1$; note $\zeta(s,1) = \zeta(s)$. Hurwitz introduced this to study Dirichlet L-functions. These arise from a character $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ by

$$\begin{aligned} L(s,\chi) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \\ &= \sum_{a=1}^{q} \chi(a) \sum_{n \equiv a \bmod q} \frac{1}{n^s} \\ &= \sum_{a=1}^{q} q^{-s} \sum_{t=0}^{\infty} \frac{1}{(t+\frac{a}{q})^s}. \end{aligned} \tag{40}$$

We now discuss a theorem of Hecke. A good reference is my problems book in algebraic number theory. We first set some notation. Let d_k be the discriminant of k, with r_1 the number of real embeddings and r_2 the number of non-real (ie, complex) embeddings. We write

$$\xi_k(s) \;=\; s(1-s)\left(\frac{\sqrt{|d_k|}}{2^{r_2}\pi^{n/2}}\right)\Gamma\left(\frac{s}{2}\right)^{r_1}\Gamma(s)^{r_2}\zeta_k(s) \;=\; \xi_k(1-s). \tag{41}$$

It thus admits a functional equation and analytic continuation, and

$$\lim_{s\to 1}\zeta_k(s) \;=\; \frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{|d_k|}}. \tag{42}$$

What are h and R? We denote the class number of kj by h. On the collection of ideals, we say two are equivalent, written $\mathfrak{a} \sim \mathfrak{b}$, if and only if there exists $\alpha, \beta \in \mathcal{O}_k$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$; the ideal classes can be given a group structure, and we call this the ideal class group. It is a classical theorem (Dirichlet's unit theorem) that $\mathcal{O}_k^*$ is a finitely generated abelian group. It has a finite part and a free part, $W \oplus \mathbb{Z}^r$ with $r = r_1 + r_2 - 1$. The finite part has rank $w = |W|$, the number of roots of unity contained in k. H

We write the fundamental system of units by $\epsilon_1, \dots, \epsilon_r$. We have our embeddings $k \to k^{(i)}$ with $1 \le i \le r_1 + 2r_2$. We order the embeddings by writing the real embeddings first adn then write the complex embeddings and then write the conjugates of the complex embeddings. We look at the determinant of a matrix involving the units and call that the regulator:

$$R \;=\; \det\left(\log|\epsilon_i^{(j)}|\right)_{1\le i,j\le r}. \tag{43}$$

Until Hecke things were not well understood here. We wrote down Dirichlet L-functions in terms of the Hurwitz zeta functions. What is the analogue of the Dirichlet L-function in the number field context? The answer is not an easy one. What is the analogue of residue classes modulo q? The analogue turns out to involve the ideal class group.

Two answers were provided to generalizing $L(s,\chi)$, one by Hecke and one by Artin.

Hecke said take an ideal $\mathfrak{f}$ of $\mathcal{O}_k$, and define the $\mathfrak{f}$-ideal class group as follows: We say $\mathfrak{a} \sim_{\mathfrak{f}} \mathfrak{b}$ if there exists $\alpha, \beta \in ok$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$ and $\alpha \equiv \beta \bmod \mathfrak{f}$ and α/β is totally positive (all conjugates positive). This gives rise to a finite group, the $\mathfrak{f}$-ideal ray class group. We let $\mathcal{H}_{\mathfrak{f}}$ denote this group, and take a character $\chi : \mathcal{H}_{\mathfrak{f}} \to \mathbb{C}^*$ and set

$$L(s,\chi) \;=\; \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{(N\mathfrak{a})^s} \quad \text{(Hecke)}. \tag{44}$$

These series have analytic continuation, functional equations, and are entire if χ is not trivial. We still have the notion of primitive character....

We first state one of the main theorems from Class Field Theory (which came from the work of Hecke and others). Given any algebraic number field k and an ideal $\mathfrak{f}$ of $\mathcal{O}_k$, there exists a field $k_{\mathfrak{g}}/k$ whose Galois group is isomorphic to $\mathcal{H}_{\mathfrak{f}}$; moreover, any finite abelian extension of k is contained in some $k_{\mathfrak{f}}$ for some $\mathfrak{f}$. This is an extension of the Kronecker-Weber Theorem: every finite abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_q)$ (for some q?). Leads to answers of Hilbert's 12th problem in some cases.

Here is Artin's approach. Artin begins by looking at the Galois extension $\mathbb{Q}(\zeta_q)$ over $\mathbb{Q}$, with Galois group $(\mathbb{Z}/q\mathbb{Z})^*$. Artin's motivation is start with an algebraic number field k, look at a finite extension K with Galois group G, take a representation $\rho : G \to \mathrm{GL}(V)$, try to attach an L-function to the data: $L(s, \rho, K/k)$.

Let's review some basic algebraic number theory (from a Galois perspective). At the beginning of the talk we talked about unique factorization into prime ideals. We have K/k with Galois group G attached to the extension. We have the ring of integers downstairs $\mathcal{O}_k$ and upstairs $\mathcal{O}_K$ with $\mathcal{O}_k \subset \mathcal{O}_K$. Given $\mathfrak{p} \in \mathcal{O}_k$ we can write it upstairs: $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$. Apply a $\sigma \in G$. The left hand side stays the same, namely $\mathfrak{p}\mathcal{O}_K$, while the right hand side becomes $\sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_g)^{e_g}$. Thus G acts on $\{\mathfrak{P}_1, \dots, \mathfrak{P}_g\}$ transitively. We let $D_{\mathfrak{P}}$ denote the decomposition group at $\mathfrak{P}$, namely $\{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}$. We also have the inertia group

$$I_{\mathfrak{P}} \ = \ \{\sigma \in G : \sigma(x) \equiv x \bmod \mathfrak{P} \text{ for all } x \in \mathcal{O}_K\}. \tag{45}$$

We have $I_{\mathfrak{P}}$ is a normal subgroup of $D_{\mathfrak{P}}$: $I_{\mathfrak{P}} \lhd D_{\mathfrak{P}}$. We can study $(\mathcal{O}_K/\mathfrak{P})/(\mathcal{O}_k/\mathfrak{p})$. We get a canonical isomorphism:

$$D_{\mathfrak{P}}/I_{\mathfrak{P}} \ \equiv \ \mathrm{Gal}\left((\mathcal{O}_K/\mathfrak{P})/(\mathcal{O}_k/\mathfrak{p})\right). \tag{46}$$

It is cyclic: $x \mapsto x^{N\mathfrak{p}}$, $\sigma(x) \equiv x^{N\mathfrak{p}} \bmod \mathfrak{P}$. We have $\sigma_{\mathfrak{P}}$ is well-defined up to $I_{\mathfrak{P}}$. The Frobenius automorphism at $\mathfrak{P}$. The $\sigma_{\mathfrak{P}_i}$'s are all conjugate. Call $\sigma_{\mathfrak{p}}$ the conjugacy class of σ_{gP_i}, the Artin symbol at $\mathfrak{p}$. This should be thought of as a generalization of the Legendre symbol (or more precisely the Jacobi-Kronecker symbol).

It turns out that $I_{\mathfrak{P}} = 1$ for all but finitely many primes. We know exactly when it is not trivial. If $\mathfrak{P}$ is unramified in the extension then it is trivial. For all unramified $\mathfrak{p}$ we have $I_{\mathfrak{P}} = 1$ for all $\mathfrak{P}|\mathfrak{p}$.

Take a representation

$$\rho : \mathrm{Gal}(K/k) \ \to \ glv. \tag{47}$$

Define

$$L(s, \rho, K/k) \quad = \quad \prod_{\mathfrak{P}} \det\left(1 - \rho(\sigma_{\mathfrak{P}}) N\mathfrak{P}^{-s} | V^{I_{\mathfrak{P}}}\right)^{-1} \tag{48}$$

(as same for conjugate elements, doesn't matter which representation we pick and so the above is well-defined). The Euler product converges for $\Re(s) > 1$. Artin conjectured that if ρ is irreducible and not equal to 1 then $L(s, \rho, K/k)$ extends to an entire function and satisfies a functional equation. Need an analogue of the discriminant, an Artin conductor, Gamma factors determined by plus one and minus one eigenspaces, and finally we'll get the functional equation. This was all proved; without going into the details we'll just say there is a functional equation. Artin showed some power has a meromorphic continuation. He took that power and showed that that had the right functional equation, finessed with characters to get the functional equation. First rigorous one came later.

Two functorial properties of Artin L-series. An Artin L-function didn't talk about reducible or irreducible representations. Since the definition only depends on the trace, some people also write $L(s, \chi, K/k)$ for $L(s, \rho, K/k)$ where $\chi = \mathrm{Tr}(\rho)$. We then have

$$L(s, \chi_1 + \chi_2, K/k) \ = \ L(s, \chi_1)L(s, \chi_2). \tag{49}$$

Let us consider the chain $k - -K^H - -K$, with character ψ from $K^H - -K$ and Galois group H form K^H to K. We have

$$L(s, \psi, K/K^H) \ = \ L(s, \mathrm{Ind}_H^G \psi, K/k), \tag{50}$$

invariance under induction.

What do we know about the Artin conjecture? We have Artin's reciprocity law.

Theorem 2.1 (Artin's Reciprocity Law)**.** *If ρ is 1-dimensional then there exists an $\mathfrak{f} \in \mathcal{O}_k$ and a character χ of $\mathcal{H}_{\mathfrak{f}}$ such that*

$$L(s, \rho, K/k) \ = \ L(s, \chi), \tag{51}$$

where $L(s, \chi)$ is the Hecke L-series. Hecke generalized Riemann's results to abelian case, saves the day here. This proves Artin's conjecture in this case.

If you analyze what the above is saying in the special case of a quadratic extension ($k = \mathbb{Q}$ and K quadratic), get the quadratic reciprocity law.

Theorem 2.2 (Brauer's Induction Theorem)**.** *If you have any character χ of a finite group G, there exist nilpotent subgroups H_i and ψ_i one-dimensional characters of H_i such that*

$$\chi \ = \ \sum_i a_i \mathrm{Ind}_{H_i}^G \psi_i \tag{52}$$

with $a_i \in \mathbb{Z}$. Artin had a multiple could be written this way.

We find

$$
\begin{aligned}
L(s, \chi, K/k) &= \prod L(s, \mathrm{Ind}_{H_i}^{G} \psi_i, K/k)^{a_i} \\
&= \prod_i L(s, \psi_i, K/K^{H_i})^{a_i} \\
&= \prod_i L(s, \phi_i)^{a_i} \quad \text{(Hecke character)}, \qquad (53)
\end{aligned}
$$

which gives a meromorphic continuation.

What do we know about higher dimensional characters?

Theorem 2.3 (Langlands-Tunnell Theorem)**.** *If ρ is 2-dimensional and odd with solvable image (that is, the image of ρ is a solvable group), then*

$$L(s, \rho, K/k) \; = \; L(s, \pi) \tag{54}$$

where π is an automorphic representation of $\mathrm{GL}_2(K)$.

The above was important in the proof of Fermat's last theorem.

2.2 The Chebotarev density theorem

```
http://www.williams.edu/go/math/sjmiller/public_html/
        ntandrmt/talks/UtahWorkshopNotes.pdf
```

2.2.1 Introduction

Last time we looked at K/k, a finite Galois extension of algebraic number fields. Let $G = \mathrm{Gal}(K/k)$. Given a prime ideal $\mathfrak{p} \in \mathcal{O}_k$ it has prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_g \in \mathcal{O}_K$ above. The Frobenius automorphism $\sigma_{\mathfrak{P}}$, and $\sigma_{\mathfrak{p}}$ is the conjugacy class of $\sigma_{\mathfrak{P}}$. All of this is well defined as long as $\mathfrak{p}$ is unramified in K. Thus we have an assignment $\mathfrak{p} \mapsto \sigma_{\mathfrak{p}}$, a conjugacy class in G. We call this the Artin symbol at $\mathfrak{p}$.

Example 2.4. *Let $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{D})$, $\mathrm{Gal}(K/k) \equiv \{\pm 1\}$. Here $p \mapsto \left(\frac{D}{p}\right)$ is the Legendre symbol.*

Example 2.5. *Let $k = \mathbb{Q}$ and now take $K = \mathbb{Q}(\zeta_q)$, a q^{th} root of unity. We have* $\mathrm{Gal}(K/k) \equiv (\mathbb{Z}/q\mathbb{Z})^*$. *For $(a, q) = 1$, $\tau_a(\zeta_q) = \zeta_q^a$, $p \mapsto \sigma_p = \tau_a$ ($p \equiv a \bmod q$).*

As we vary the prime ideals, what does the image of the map look like? Are there Artin symbols that hit a conjugacy class, and if so how often? That is really the Chebotarev density theorem.

2.2.2 Chebatorev Density Theorem

Theorem 2.6 (Chebatorev Density Theorem)**.** *Fix a conjugacy class C of G.*

$$\#\{\mathfrak{p} : N\mathfrak{p} \leq x : \sigma_{\mathfrak{p}} = C\} \ \sim\ \frac{|C|}{|G|}\,\pi(x) \tag{55}$$

as $x \to \infty$.

Recall

Theorem 2.7 (Prime Ideal Theorem)**.** *We have*

$$\#\{\mathfrak{p} : N\mathfrak{p} \leq x\} \ \sim\ \pi(x). \tag{56}$$

Thus the Chebatorev density theorem is generalizing the result of primes in arithmetic progressions.

There is one particular class of the class containing the identity element, $C = 1$. Here we have

$$\#\{\mathfrak{p} : N\mathfrak{p} \leq x, \sigma_{\mathfrak{p}} = 1\} \ \sim\ \frac{\pi(x)}{|G|}. \tag{57}$$

Recall $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_g$. What does it mean for the Artin symbol to be 1? Take a Galois automorphism, apply upstairs get distinct. This means the prime ideal when lift is splitting into the largest number of prime ideals that we can have, ie, $\mathfrak{p}$ splits completely.

Another way to look at this is through a classical theorem of Dedekind.

Theorem 2.8 (Dedekind)**.** *Let K be an algebraic number field, $K = \mathbb{Q}(\theta)$ with $f(x)$ the minimal polynomial of θ in $\mathbb{Z}[x]$. Suppose*

$$f(x) \ =\ f_1(x)^{e_1} \cdots f_g(x)^{e_g} \bmod p \tag{58}$$

where the $f_i(x)$ are irreducible modulo p. Then if $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$ we have

$$\mathfrak{P} \ =\ (p, f_i(\theta)) \quad \text{and} \quad N\mathfrak{P} \ =\ p^{\deg f_i}. \tag{59}$$

Suppose $K = \mathbb{Q}(\theta)$ is a Galois extension of $\mathbb{Q}$ with $f(x)$ a normal polynomial (if you adjoin one root you have them all; for example, a cyclotomic polynomial). To say p splits completely in K is the same as saying that $f(x)$ factors completely as a product of linear polynomials modulo p.

This looks very special, don't come across normal polynomials all the time. What happens if we have any old polynomial with integer coefficients: how often does $f(x)$ modulo p have a root? Look at K over $\mathbb{Q}$ with fields $K_1 = K(\theta_1)$, K_2, $\dots$, K_n between $\mathbb{Q}$ and K. Let G be the Galois group of K/k. If we go back to Dedekind's theorem and ask what it means for the polynomial to have a root, we see one of these polynomials must be linear, so there is a prime ideal upstairs of degree 1. Can translate this into group theoretic statements. We find $f(x) \bmod p$ has a root if and only if $\sigma_p \in \cup_{g\in G} g^{-1}Hg = X$. This implies

$$\#\{p \leq x : f(x) \bmod p \text{ has a root}\} \sim \frac{|X|}{|G|}\,\pi(x). \tag{60}$$

Here H is the Galois group fixing. A good exercise is to show that $|X| < |G|$ if $f(x)$ is irreducible of degree 2 or more.

Aside: Chebotarev had a difficult life, poor family trying to eke out existence in Russia. He worked this out without access to journals, wrote in 1926 or so before Artin had introduced his non-abelian L-series. You can now invoke the analytic machinery / Tauberian theorems and this pops out. But this is not the way it happened historically. He discovered this without using any of this by finessing through abelian sub-extensions. You can translate this theorem into group theory / extensions. This inspired Artin and led to the reciprocity law. The main tools that Artin developed for proving reciprocity came by studying Chebotarev's theorem

Is there an effective version of the Chebotarev? We want a theorem with a main and an error term.

There are three versions:

- An unconditional version;
- A version assuming GRH;
- A version assuming GRH and Artin's conjecture.

The first two are covered in a fundamental paper of Lagarias and Odlyzko (Effective versions of the Chebotarev density theorem. Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 409–464. Academic Press, London, 1977), the second by Murty, Murty and Saradha (which is online at

`http://www.williams.edu/go/math/sjmiller/public_html/ntandrmt/handouts/murty/Murty_ModularFormsChebotarevDensity.pdf`.

Theorem 2.9 (Version 1)**.** *We have*

$$\left|\#\{\mathfrak{p} : N\mathfrak{p} \le x : \sigma_{\mathfrak{p}} = C\} - \frac{|C|}{|G|}\,\pi(x)\right| \;\le\; \frac{|C|}{|G|}\,\mathrm{li} x^{\beta} + O\left(|c| x \exp\left(-c_1\sqrt{\frac{\log x}{[K:\mathbb{Q}]}}\right)\right) \tag{61}$$

provided that $\log x \ge c_2[K:\mathbb{Q}](\log|d_K|)^2$*, where* β *is a possible zero of* $\zeta_K(s)$ *in* $[1 - 1/\log|d_K|, 1]$.

Remark 2.10 (For the experts)**.** In the cyclotomic case it is far short of the Siegel-Walfisz case. In that case $[K : \mathbb{Q}]$ is like $\phi(q)$, and getting something like $\log^{1/3} x$. Gives a sense of how weak the unconditional version is.

Theorem 2.11 (Version 2, assuming GRH for Dedekind Zeta Function)**.** *Assume* $\zeta_K(s) \neq 0$ *for* $\Re(s) > 1/2$*. Then*

$$\left|\#\{\mathfrak{p} : N\mathfrak{p} \le x : \sigma_{\mathfrak{p}} = C\} - \frac{|C|}{|G|}\,\pi(x)\right| \;\le\; c_3|C|x^{1/2}(\log M(K/k) + [K:\mathbb{Q}]\log x), \tag{62}$$

where

$$M(K/k) \;=\; \sum_{p|d_K}\log p + \frac{\log|d_K|}{[K:\mathbb{Q}]} + \log[K:\mathbb{Q}]. \tag{63}$$

The above is Lagarias-Odlyzko cleaned up by Serre. Serre analyzed the ramification carefully, using a beautiful result of Hensel to get a significant savings. The main point is that the error term is like $x^{1/2}$ and that the dependence on the conjugacy class is as above.

Theorem 2.12 (Version 3, assuming GRH and Artin's Conjecture)**.** *We have*

$$\left|\#\{\mathfrak{p} : N\mathfrak{p} \le x : \sigma_{\mathfrak{p}} = C\} - \frac{|C|}{|G|}\,\pi(x)\right| \;\le\; c_4|C|^{1/2}x^{1/2}(\log M(K/k) + \log x). \tag{64}$$

All the constants above are effectively computable.

When the conjugacy classes are large, this matters.

2.2.3 Applications of the Chebotarev Density Theorem

- The first application was to Artin's primitive root conjecture: 2 is a primitive root modulo p infinitely often. (The story is that he was challenged to provide a concrete application of class field theory.) We have the following equivalences: $2^{(p-1)/q} \not\equiv 1 \bmod p$ $q|p-1$. Having p split completely in the cyclotomic field $\mathbb{Q}(\zeta_q)$ and $x^q \equiv 2 \bmod p$ has as solution in $\mathbb{Q}(\sqrt[q]{2})$ is equivalent to $2^{(p-1)/q} \equiv 1 \bmod p$ and $q \equiv 1 \bmod p$. Do a sieve, make sure it doesn't split completely, take away some primes, as do sieve go through a tower of fields, need good control of error terms when use Chebotarev.

- Applications to modular forms: Let f be a Hecke eigenform. Deligne showed that there exists an ℓ-adic representation $\rho_\ell : \mathrm{Gal}(\overline{Q}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ with the property that $\mathrm{tr}(\rho_\ell(\sigma_p)) \equiv \lambda_f(p) \bmod \ell$. The residue class is determined by the conjugacy class of the Artin symbol in the extension. It is now a question of how often is $\tau(p)$ divisible by ℓ? Same as saying a Galois extension whose ramification and degree can control and symbol belongs to given conjugacy class if and only if zero modulo ℓ. Size of error terms matter.

2.2.4 Interplay between Artin's conjecture and GRH

This is building on work of Heilbronn, Stark, K. and R. Murty. WE have a Galois extension K/k with Galois group G. Let

$$\zeta_K(s) \ = \ \prod_{\chi} L(s, \chi, K/k)^{\chi(1)} \tag{65}$$

where χ is an irreducible character of G and $\chi(1)$ is the degree of the character. Heilbronn introduced what we'll call the Heilbronn character. Fix an $s_0 \in \mathbb{C}$.

$$\theta_G(g) \ = \ \sum n(\chi, s_0)\chi(g); \tag{66}$$

this character is a linear combination of the characters χ, and

$$n(\chi, s_0) \ = \ \mathrm{ord}_{s=s_0} L(s, \chi, K/k). \tag{67}$$

This order is well defined, is a virtual character.

The key point is to know some very basic group theory.

Theorem 2.13 (Frobenius Reciprocity Theorem)**.** *Given a group G, let H be a subgroup. Suppose we have a character ψ of H, can look at the induced character on the big group,* $(\mathrm{Ind}_H^G \psi, \chi) \ = \ (\psi, X\Big|_H)$ *(the inner products are taken in two different spaces).*

Lemma 2.14 (Heilbronn's Lemma)**.** *Take a Galois extension K/k with Galois group G and let K^H be intermediate (with Galois group H from K^H to K). Then*

$$\theta_G\Big|_H \ = \ \theta_H. \tag{68}$$

Proof. Use Frobenius reciprocity. □

One should always use Parseval, and thus we should compute

$$(\theta_G, \theta_G) \ = \ \sum_\chi n(\chi, s_0)^2. \tag{69}$$

But what does the inner product mean? By definition, it is

$$(\theta_G, \theta_G) \ = \ \frac{1}{|G|} \sum_{g \in G} |\theta_G(g)|^2. \tag{70}$$

We have $\theta_G(g) = \theta_{<g>}(g)$, with

$$\theta_{<g>}(g) \ = \ \sum_\psi n(\psi, s_0)\psi(g). \tag{71}$$

We thus find

$$|\theta_{<g>}(g)| \ \le \ \sum n(\psi, s_0). \tag{72}$$

As have a situation where Artin's conjecture is known, don't need absolute values, things factor, and we find

$$|\theta_{<g>}(g)| \ \le \ \sum n(\psi, s_0) \ = \ \mathrm{ord}_{s=s_0}\zeta_K(s). \tag{73}$$

We thus find

$$\sum_\chi n(\chi, s_0)^2 \ \le \ \left(\mathrm{ord}_{s=s_0}\zeta_K(s)\right)^2. \tag{74}$$

If the Riemann Hypothesis is true, so Dedekind zeta function has no zero to the right of 1/2, the stuff on the right is zero, analyticity.... GRH implies that any pole of an Artin L-series has real part 1/2.

If $\zeta_K(s)$ has a simple zero at $s = s_0$, then either have zero or 1 on right hand side, only one term can introduce pole, look at factorization

$$\zeta_K(s) \ = \ \prod_\chi L(s, \chi, K/k)^{\chi(1)}, \tag{75}$$

must come from an abelian thing (already know entire), know any Artin L-series is analytic at $s = s_0$. This was so cute that R. Foote and K. Murty tried to squeeze out as much as possible out of this idea.

Theorem 2.15 (R. Foote and K. Murty). *If K/k is Galois of odd degree,* $\mathrm{ord}_{s=s_0}\zeta_K(s) \leq 3$*, then any Artin L-series is analytic at $s = s_0$.*

2.3 Special values of Artin L-series

`http://www.williams.edu/go/math/sjmiller/public_html/ntandrmt/talks/UtahWorkshopNotes.pdf`

Recall we have K/k Galois with Galois group G, $\rho : G \to \mathrm{GL}(V)$ and $L(s, \rho, K/k)$. Given an integer m, what can we say about $L(m, \rho, K/k)$?

The simplest case goes back to Euler. He proved using simple facts about the cotangent function that

$$\zeta(2m) \;\in\; \pi^{2m}\mathbb{Q}^*. \tag{76}$$

This is elementary. Euler's proof wasn't the best, as pointed out by Siegel. Siegel noticed that the method of deriving the formula for $\zeta(2m)$ using standard power series is probably a fluke case, and it is better to observe that if you take the Eisenstein series of weight $2m$,

$$E_{2m}(z) \;=\; \sum_{(a,b)\neq(0,0)} \frac{1}{(az+b)^{2m}} \tag{77}$$

is a modular form of weight $2m$, and one finds

$$E_{2m}(z) \;=\; 2\zeta(2m) + \cdots, \tag{78}$$

and the constant term is a $\mathbb{Q}$-linear combination of terms up to a certain point. The rest of this uses contangent expansions. The next term is like

$$\frac{(2\pi)^{2m}}{(2m)!} \sum \sigma_{2m-1}(q)q^n. \tag{79}$$

Serre revived this for p-adic interpretations. More or less this idea can be considered in the context of a number field.

Let K be a totally real field, and construct an Eisenstein series

$$\sum_{a,b\in\mathcal{O}_K} \frac{1}{N(az+b)^{2m}}, \tag{80}$$

with $[K;k] = d$ and the norm being $(a^{(1)}z_1 + b^{(1)})(a^{(2)}z_2 + b^{(2)})\cdots$, specialize, invoke constant term a linear combination of others, get $\zeta_K(2m) \in \pi^{2md}\mathbb{Q}$.

Theorem 2.16 (Siegel-Klingen Theorem)**.** *Take any algebraic number field K, let ψ be a Hecke character,*

$$L(1-m,\psi) \;\in\; \mathbb{Q}(\psi), \tag{81}$$

where $\mathbb{Q}(\psi)$ is the field generated by the values of ψ.

When is this zero, when is it non-zero? This is controlled by Gamma factors. Using the functional equation, we can evaluate $L(m,\psi)$ explicitly in some cases. What does this mean? We have to go back to the functional equation of the Artin L-series. $L(s,\rho,K/k)$ with $\chi = \mathrm{tr}(\rho)$. We have

$$\xi(s,\chi) \;=\; \left(|d_K| N\mathfrak{f} \pi^{-d\chi(1)}\right)^{s/2} \Gamma\left(\frac{s}{2}\right)^a \Gamma\left(\frac{s+1}{2}\right)^b L(s,\chi,K/k) \tag{82}$$

with $d = [K:k]$, $a = (\chi(1)+\chi(c))/2$ and $b = (\chi(1)-\chi(c))/2$. We write χ is totally real if $\chi(c) = \chi(1)$ and totally complex if $\chi(c) = \chi(1)$, where c is complex conjugation. Mixtures can happen; in the two extreme cases (all plus 1 or minus 1 eigenvalues), we can say something non-trivial about $L(m,\psi)$.

We only know $\zeta(3)$ is irrational (Apéry); we don't know if $\zeta(3)/\pi^3 \notin \mathbb{Q}$.

Conjecture 2.17. *The numbers $\pi, \zeta(3), \zeta(5), \ldots$ are algebraically independent.*

Rivoal made a major breakthrough a few years ago when showed that infinitely many of these numbers are irrational. Improved by Ball, Rivoal and Zudlin to $\dim_{\mathbb{Q}} \mathrm{Span}(\zeta(3), \zeta(5), \ldots, \zeta(2a+1)) \geq c \log a$.

2.3.1 The classical case

Dirichlet's formula:

$$\tau(\chi) \;=\; \sum_{A} \chi(a)\zeta_q^a. \tag{83}$$

Send $a \to an$ with $(n,q)=1$. Then

$$\begin{aligned} \tau(\chi) &= \sum_a \chi(an)\zeta_q^{an} \\ \overline{\chi}(n)\tau(\chi) &= \sum_a \chi(a)\zeta_q^{an} \\ \chi(n)\tau(\overline{\chi}) &= \sum_a \overline{\chi}(a)\zeta_q^{an}. \end{aligned} \tag{84}$$

The last equation is valid for χ primitive for all n. We get

$$\begin{aligned}\tau(\overline{\chi}) \sum_{n} \frac{\chi(n)}{n} &= \sum_{a=1}^{q} \overline{\chi}(a) \sum_{n=1}^{\infty} \frac{\zeta_q^{an}}{n} \\ &= \sum_{a=1}^{q} \overline{\chi}(a) \log(1-\zeta_q^a). \qquad (85)\end{aligned}$$

For Dirichlet characters $\chi \bmod q$, $L(1,\chi)$ is a $\overline{\mathbb{Q}}$-linear combination of logarithms of algebraic numbers.

Theorem 2.18 (Baker)**.** *If $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}} - \{0\}$ and $\beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}}$ then*

$$\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n \qquad (86)$$

is either zero or transcendental. Thus $L(1,\chi)$ is transcendental.

What about $L(1,\chi,K/k)$ for a general Artin series?

2.3.2 Stark's Conjecture

Conjecture 2.19 (Stark's Conjecture: 1975)**.** *Let χ be irreducible and not equal to 1. Then*

$$L(1,\chi,K/k) \;=\; \frac{w(\overline{\chi})2^a\pi^b}{(|d_K|N\mathfrak{f})^{1/2}}\,\theta(\chi)R(\chi), \qquad (87)$$

where $\theta(\chi) \in \overline{\mathbb{Q}}$, $R(\chi)$ is the determinant of an $a \times a$ matrix $\overline{\mathbb{Q}}$-linear combination of logarithms of algebraic numbers, $a = (\chi(1)+\chi(c))/2$ and $b = (\chi(1)-\chi(c))/2$.

Stark proved this conjecture if χ is a rational character (ie, it takes on rational values).

Note there is a transcendental part (coming from the π) and another part. Can we say anything about the transcendence? Only if $a = 1$ and $b = 0$ can we say for sure about the transcendence of $L(1,\chi,K/k)$.

2.3.3 Schanuel's Conjecture

Conjecture 2.20 (Schanuel's Conjecture)**.** *Let $\alpha_1, \ldots, \alpha_n$ be complex numbers linearly independent over $\mathbb{Q}$. The transcendence degree of $\mathbb{Q}(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n})$ $\geq n$.*

To see how hard this is, take $\alpha_1 = 1$ and $\alpha_2 = \pi$, then we get that π and e are algebraically independent! This is unknown, though we do know that at least one of $\pi + e$ and πe is transcendental.

A 'weaker' conjecture is if $\log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over $\mathbb{Q}$ then they are algebraically independent. This is also unknown.

The weaker conjecture proves $L(1, \chi, K/k)$ is transcendental if χ is rational. So Stark's conjecture plus the weaker Schanuel imply that $L(1, \chi, K/k)$ is transcendental for any χ.

2.3.4 Other values

We have (at least conjecturally) knowledge when $s = 1$ (or $m = 1$). What about other values of m? Coates and Lichtenbaum showed that Siegel-Klingen implies $L(m, \chi, K/k) \in \pi^{m\chi(1)}\overline{\mathbb{Q}}$ provided that m is even and χ is totally real or m is odd and χ is totally complex.

2.3.5 Zagier's Conjecture

For general m, what is $\zeta_K(m)$? Define the polylogarithm function

$$\mathrm{Li}_m(z) \;=\; \sum_{\nu=1}^{\infty} \frac{z^\nu}{\nu^m}, \tag{88}$$

and note that when $m = 1$ we have $\mathrm{Li}_1(z) = -\log(1-z)$. We modify it as follows:

$$\mathcal{L}_m(z) \;=\; \begin{cases} \Re\left(\sum_{j=0}^{m} \frac{B_j}{j!}\, 2^j (\log|z|)^j \mathrm{Li}_m(z)\right) & \text{if } m \text{ even} \\ \mathrm{Im}\left(\sum_{j=0}^{m} \frac{B_j}{j!}\, 2^j (\log|z|)^j \mathrm{Li}_m(z)\right) & \text{if } m \text{ odd.} \end{cases} \tag{89}$$

Conjecture 2.21 (Zagier)**.** *There exist $y_1, \ldots, y_{d_m} \in K$ so that*

$$\zeta_K(m) \;=\; \pi^{(n-d_m)m} |d_K|^{-1/2} \det\left(\mathcal{L}_m(\sigma_j(y_i))\right), \tag{90}$$

where it is $d_m \times d_m$ determinant with $n = [K : k]$.

Similar conjectures for Artin L-functions. Zagier proved for $m = 2$, Goncharov for $m = 3$.

2.3.6 A question of Chowla

Chowla (1964) asked whether or not there exists a function $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Q}$ so that

$$\sum_{n=1}^{\infty} \frac{f(n)}{n} \;=\; 0 \tag{91}$$

(with f non-zero, of course) for q prime?

Theorem 2.22 (Baker, Birch and Wirsing)**.** *No such function exists (for any q such that $\mathbb{Q}(f(n))$ is disjoint from the qth cyclotomic field $\mathbb{Q}(\zeta_q)$).*

The proof uses linear forms.
What is the significance of this theorem?

Corollary 2.23. *For q prime, $L(1, \chi)$ with $\chi \bmod q$ are linearly independent over $\mathbb{Q}$.*

From an earlier lecture, we know we have an analytic continuation:

$$\sum \frac{f(n)}{n^s} \;=\; (??\text{factor}??) \sum_{a=1}^{q} f(a)\zeta(s, a/q). \tag{92}$$

Chowla and his daugher showed that q prime, $s = 2$: $\sum f(n)/n^2 = 0$ is true if and only if $f(1) = \cdots = f(q-1) = f(q)/(1-q^2)$.

Conjecture 2.24 (Chowla-Milnor)**.** *Fix m, the $\zeta(m, a/q)$ with $(a, q) = 1$ and $1 \le a < q$ are linearly independent over $\mathbb{Q}$.*

To appreciate how hard this conjecture is:

Theorem 2.25. *The Chowla-Milnor conjecture for $q = 4$ is equivalent to $\zeta(m)/\pi^m \notin \mathbb{Q}$ for m odd.*

Conjecture 2.26 ([The polylogarithm conjecture)**.** $\mathrm{Li}_m(\alpha_1), \ldots, \mathrm{Li}_m(\alpha_n)$ *are linearly independent over $\mathbb{Q}$ then they are linearly independent over $\overline{\mathbb{Q}}$.*

The polylogarithm conjecture implies the Chowla-Milnor conjecture.

2.4 L-series and transcendental numbers

http://www.williams.edu/go/math/sjmiller/public_html/ntandrmt/talks/UtahWorkshopNotes.pdf

Theorem 2.27 (Baker, Birch and Wirsing)**.** *Let $f : \mathbb{Z}/q\mathbb{Z} \to \overline{\mathbb{Q}}$ and suppose $f(a) = 0$ for $1 < (a, q) < q$. Suppose that the field $\mathbb{Q}(f(n))$ is disjoint from the qth cyclotomic field $\mathbb{Q}(\zeta_q)$ (clear if f is rational valued). Then*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n} \neq 0. \tag{93}$$

Look at the Dirichlet series we can attach to this f:

$$\begin{aligned} L(s, f) &= \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \\ &= \sum_{a=1}^{q} f(a) \sum_{n \equiv a \bmod q} \frac{1}{n^s} \\ & \quad q^{-s} \sum_{a=1}^{q} f(a) \zeta(s, a/q). \end{aligned} \tag{94}$$

Recall the Hurwitz zeta function $\zeta(s, x)$ is the perturbed Dirichlet series

$$\zeta(s, x) = \sum_{n=0}^{\infty} \frac{1}{(n + x)^s}. \tag{95}$$

We have that $\zeta(s, x)$ extends to all $s \in \mathbb{C}$ except for $s = 1$, and

$$\zeta(s, x) = \frac{1}{s - 1} - \psi(x) + O(s - 1), \quad \psi(x) = \frac{\Gamma'(x)}{\Gamma(x)}. \tag{96}$$

There will be a polar part, whose residue is $\sum_a f(a)$, so to have no pole requires this to vanish. In other words,

$$\sum \frac{f(n)}{n} < \infty \text{ if and only if } \sum_{a=1}^{q} f(a) = 0. \tag{97}$$

We find

$$L(1, f) = -\frac{1}{q} \sum_{a=1}^{q} f(a) \psi(a/q), \tag{98}$$

where ψ is the Digamma function.

Whenever you have a function defined on a group, gut instinct is to apply Fourier analysis:

$$\begin{aligned} f(n) &= \sum_{a=1}^{q} \widehat{f}(a)\zeta_q^{an} \\ \widehat{f}(n) &= \frac{1}{q}\sum_{a=1}^{q} f(a)\zeta_q^{-an}, \end{aligned} \tag{99}$$

with $\zeta_q = e^{2\pi i/q}$. We have

$$\sum_{a=1}^{q} f(a) \;=\; 0 \quad \text{if and only if} \quad \widehat{f}(q) \;=\; 0. \tag{100}$$

We have

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{f(n)}{n} &= \sum_{n=1}^{\infty} \frac{1}{n} \sum_{a=1}^{q-1} \widehat{f}(a)\zeta_q^{an} \\ &= -\sum_{a=1}^{q-1} \widehat{f}(a)\log(1-\zeta_q^{q}) \\ &= \overline{\mathbb{Q}} - \text{linear combination of logs of alg nos.} \end{aligned} \tag{101}$$

Thus Baker's result now implies that $L(1,f)$ is transcendental. We find

$$\sum_{a=1}^{q} f(a)\psi\left(\frac{a}{q}\right) \;=\; -\sum_{a=1}^{q-1} \widehat{f}(a)\log(1-\zeta_q^{a}). \tag{102}$$

The right hand side is transcendental, so immediately we deduce

Corollary 2.28. *The Digamma values $\psi(a/q)$ for $1 \le a \le q$ with $(a,q)=1$ or $a=q$ are such that there is at most one algebraic number in this list. Observe that $\psi(1) = -\gamma$ is Euler's constant, which could be the exception!*

Lehmer: Euler's constant is:

$$\gamma \;=\; \lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n} - \log x\right); \tag{103}$$

we can generalize to

$$\gamma(a,q) \;=\; \lim_{x\to\infty}\left(\sum_{\substack{n\le x\\ n\equiv a \bmod q}} \frac{1}{n} - \frac{\log x}{q}\right). \tag{104}$$

Theorem 2.29 (Murty-Saradha)**.** *Consider*

$$\gamma(a,q) \quad = \quad \frac{1}{q}\left(\psi\left(\frac{a}{q}\right) + \log q\right) \tag{105}$$

with $1 \le a < q$ and $g \ge 2$. Then there is at most one algebraic number in the list. Note $\gamma(2,4) \in \gamma\mathbb{Q}$.

What can be said about the number field context? What is the philosophy? Instead of narrowing attention to a zeta function or a Dirichlet L-function, one should study linear combinations of these. That seems to be the moral.

Consider an algebraic number field k with $\mathfrak{a}$ an ideal of $\mathcal{O}_k$. Recall the analogue of coprime residue classes modulo q are the ray classes. Let $\mathcal{H}(\mathfrak{a})$ be the q-ideal ray class group. We have $K_{\mathfrak{a}}/k$ with group $\mathcal{H}(\mathfrak{a})$. Let $f : \mathcal{H}(\mathfrak{a}) \to \overline{\mathbb{Q}}$ and

$$L(s,f) \;=\; \sum_{\mathfrak{a}} \frac{f(\mathfrak{a})}{N\mathfrak{a}^s}. \tag{106}$$

The natural question is when is $L(1,f) = 0$?

Hecke studied

$$L(s,f) \;=\; \sum_{C\in\mathcal{H}(\mathfrak{a})} f(c) \sum_{\mathfrak{a}\in C} \frac{1}{N\mathfrak{a}^s} \;=\; \sum_{C\in\mathcal{H}(\mathfrak{a})} f(c)\zeta(s,C). \tag{107}$$

We have $\zeta(s,C)$ extends for all $s \in \mathbb{C}$ not equal to 1. Thus we get an analytic continuation of $L(s,f)$. We have

$$L(1,f) \;=\; \sum \frac{f(\mathfrak{a})}{N\mathfrak{a}} \;<\; 0 \quad \text{if and only if} \quad \sum_{C\in\mathcal{H}(\mathfrak{a})} f(C) \;=\; 0. \tag{108}$$

Theorem 2.30. *Let k be an imaginary quadratic field, $\mathfrak{a} = 1$, let $f : \mathcal{H} \to \overline{\mathbb{Q}}$ with f not identically zero. Then $L(1,f) \neq 0$.*

In the imaginary quadratic case, more things going on that help us. What are they? First, $L(1,f)/\pi$ is a $\overline{\mathbb{Q}}$-linear form in logarithms of algebraic numbers.

We notice that the Hurwitz zeta function has analytic continuation, constant term given by Digamma function. What is the analogue here? Comes from the Kronecker limit formula. Set

$$\Delta(z) \quad = \quad q\prod_{n=1}^{\infty}(1-q^n)^{24} \tag{109}$$

with $q = e^{2\pi z}$. Take an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ with $\mathfrak{a} = [\beta_1, \beta_2]$, $\mathrm{Im}(\beta_2/\beta_1) > 0$,

$$g(\mathfrak{a}) \ = \ (2\pi)^{-12}(N\mathfrak{a})^6|\Delta(\beta_2/\beta_1)|, \tag{110}$$

g is really a function on the ideal classes. $g(C)$ with C an ideal class gives

$$\begin{aligned}\zeta(s,C) \quad &= \quad \frac{2\pi}{w\sqrt{|d_k|}}\Big(\frac{1}{s-1} + 2\gamma \\ &\qquad - \ \log|d_k| - \frac{1}{6}\log g(C^{-1})\Big) + O(s-1),\end{aligned} \tag{111}$$

and

$$L(1,f) \ = \ -\frac{\pi}{3w\sqrt{|d_k|}}\sum_{C\in\mathcal{H}} f(C)\log g(C^{-1}). \tag{112}$$

We have the following result from Class Field Theory:

Theorem 2.31. *For any two ideal classes C_1, C_2 we have $g(C_1)/g(C_2) \in K_{\mathcal{H}}$.*

What is the reason behind the 'at most one algebraic' theorem: it is measuring the transcendence degree of the field generated. There is really only one transcendental number being generated by the g's. With this added information, we can rewrite

$$L(1,f) \ = \ -\frac{\pi}{3w\sqrt{|d_k|}}\sum_{C} f(c)\log\frac{g(C)}{g(C_0)}. \tag{113}$$

We therefore see that either $L(1,f) = 0$ or $L(1,f)/\pi$ is transcendental.

How do you get non-vanishing? More class field theory! Again we have K_H/k with group $\mathcal{H}$ and $\sigma_{\mathfrak{p}}(g(C)/g(C_0)) = g(\mathfrak{p}^{-1}C)/g(\mathfrak{p}^{-1}C_0)$. Thus $L(1,f) = 0$ implies that $L(1,f^\sigma) = 0$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

LEt k be an imaginary quadratic field, $\mathcal{H}$ with ψ a Hecke character. $L(1,\psi)$ are linearly independent over $\overline{\mathbb{Q}}$: $\sum c_\psi L(1,\psi) = 0$ with $c_\psi \in \overline{\mathbb{Q}}$, $f = \sum c_\psi \psi$, $L(1,f) = 0$ implies $f \equiv 0$ implies $c_\psi = 0$ for all ψ.

Kronecker discovered the following. $\mathcal{H}$, ψ as above, $\psi^2 = 1$ genus characters, D discriminant of k and factor as $D = D_1 D_2$ where D_i are discriminants, and define

$$\chi_{D_1 D_2}(\mathfrak{p}) \;=\; \begin{cases} \chi_{D_1}(N\mathfrak{p}) & \text{if } (\mathfrak{p}, D_1) = 1 \\ \chi_{D_2}(N\mathfrak{p}) & \text{if } (\mathfrak{p}, D_2) = 1, \end{cases} \tag{114}$$

with $\chi_D(p) = \left(\frac{D}{p}\right)$, the classical Legendre symbol (± 1). An immediate question that comes to mind: is this well-defined? Exercise: yes (Kronecker did this, have to check and make sure if satisfy both conditions then equal). The point is that

We have

$$L(s, \chi_{D_1 D_2}) \;=\; L(s\chi_{D_1}) L(s, \chi_{D_2}), \tag{115}$$

where the L-function on the left is the Hecke L-series and the two on the right are classical Dirichlet L-series. Think of this as a generalization of

$$\zeta_k(s) \;=\; \zeta(s) L(s, \chi_D). \tag{116}$$

As

$$\zeta_k(s) \;=\; \sum_C \zeta(s, C) \;=\; \zeta(s)(s, \chi_D). \tag{117}$$

Compare the constant terms of Laurent expansion of both sides. We find

$$\gamma L(1, \chi_D) + L'(1, \chi_D) \;=\; \frac{2\pi}{w\sqrt{|d_k|}} \sum_C (2\gamma - \log|d_k| - \frac{1}{6}\log g(C^{-1}) \tag{118}$$

which implies

$$\frac{L(1, \chi_D)}{L(1, \chi_D)} \;=\; \gamma - \log|d_k| - \frac{1}{6}\sum_C \log g(C). \tag{119}$$

We have

$$L(s, \chi_D) \;=\; D^{-s} \sum_{a=1}^{D} \chi_D(a) \zeta(s, a/D) \tag{120}$$

with the left hand side the classical $L(s, \chi)$. We have

$$\begin{aligned} \zeta(0, x) &= \frac{1}{2} - x \\ \zeta'(0, x) &= \log\left(\Gamma(x)/2\pi\right)) \;\; \text{(Lerch's formula)} \\ L(0, \chi_D) &= \sum_a \chi(a) \left(\frac{1}{2} - \frac{a}{D}\right) \\ L'(0, \chi_D) &= -(\log D) L(0, \chi_D) + \sum_a \chi(a) \log\Gamma\left(\frac{a}{D}\right). \end{aligned} \tag{121}$$

This gives a formula for $L'(1,\chi_D)/L(1,\chi_D)$ in terms of $\log\Gamma(a/D)$.

Theorem 2.32 (Chowla-Selberg formula). *We have*

$$\prod_C g(C)^6 \;=\; \left(\frac{1}{4\pi|d_k|}\right)^{|\mathcal{H}|}\prod_{a=1}^{D}\Gamma\left(\frac{a}{D}\right)^{w\chi_D(a)/2}. \tag{122}$$

The first product is transcendental and independent of π; this comes from facts about elliptic curves.

Theorem 2.33. *We have* π *and* $\exp\left(\frac{L'(1,\chi_D)}{L(1,\chi_D)}-\gamma\right)$ *are algebraically independent.*

Question 2.34. *Can we have* $L'(1,\chi_D)=0$ *for some* D*?*

This is unknown, but

Theorem 2.35 (K. Murty, Y. Ihara and M. Shimura). *This happens rarely. The number of* $\chi \bmod q$ *such that* $L'(1,\chi)=0$ *is bounded by* $\ll q^{\epsilon}$.

Recent results with Multiple Zeta Functions:

$$\zeta(s_1,\dots,s_\ell) \;=\; \sum_{n_1>n_2>\cdots>\geq 1}\frac{1}{n_1^{s_1}\cdots n_\ell^{s_\ell}} \tag{123}$$

with $s_1>1$ and $s_2,\dots,s_\ell\geq 1$. We say $s_1+\cdots s_\ell$ is the weight of ζ and ℓ is the length. We have

$$\begin{aligned}\zeta(s_1)\zeta(s_2) &= \sum_{n_1,n_2}\frac{1}{n_1^{s_1}n_2^{s_2}}\\ &= \sum_{n_1>n_2}+\sum_{n_2>n_1}+\sum_{n_1=n_2}\\ &= \zeta(s_1,s_2)+\zeta(s_2,s_1)+\zeta(s_1+s_2)\end{aligned} \tag{124}$$

with

$$\zeta(s) \;=\; \sum_{s_1+\cdots+s_\ell=s}\zeta(s_1,\dots,s_\ell). \tag{125}$$

Conjecture 2.36 (Zagier's MZV conjecture). *Let* V_k *be the* $\mathbb{Q}$*-span of* $\zeta(s_1,\dots,s_\ell)$ *with* $s_1+\cdots+s_\ell=k$*. Let* d_k *be the dimension of* V_k*. Define* $\delta_0=1$, $\delta_1=0$, $\delta_2=1$, $\delta_k=\delta_{k-2}+\delta_{k-3}$ *and* $\delta_k\sim e^{ck}$*. The conjecture is* $d_k=\delta_k$.

Terasoma and Goncharov, using a lot of algebraic geometry, showed that $d_k\leq\delta_k$. Gun-Murty-Rath showed that the Chowla-Milnor conjecture implies $d_k\geq 2$.

3 Gonek

3.1 The First 150 Years of the Riemann Zeta-Function

http://www.williams.edu/go/math/sjmiller/public_html/
ntandrmt/talks/Slides_Utah_09 Gonek1.pdf

We'll go through the paper and say what is in it, discuss the early history of the zeta function (mostly solving the problems Riemann left in his paper), and then talk about some of the major branches of the subject).

3.1.1 Riemann's paper

What does Riemann prove? He starts with Euler's formula $\sum_n n^{-s} = \prod_p (1 - p^{-s})^{-1}$. Riemann's first big step is to treat as a function of a complex variable $s = \sigma + it$. He gives two proofs of the analytic continuation of $\zeta(s)$, showing there is a simple pole at $s = 1$ and trivial zeros at the negative even integers. He proves the functional equation and then makes a number of claims:

- There are infinitely many non-trivial zeros of $\zeta(s)$ in the critical strip $0 \leq \Re(s) \leq 1$. There are clearly no zeros (from the Euler product) for $\Re(s) > 1$.
- If $N(t)$ is the number of non-trivial zeros $\rho = \beta + i\gamma$ with $\gamma \in [0, T]$ then as $T \to \infty$ we have $N(T) = \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T)$.
- The functional equation $\xi(s) = \frac{1}{2} s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s)$ is entire and has the product formula $\xi(s) = \xi(0) \prod_\rho (1 - s/\rho)$ (grouping ρ and $\overline{\rho}$ together).
- He claims an explicit formula relating primes to the zeta function:

$$\psi(x) \;=\; \sum_{n \leq x} \Lambda(n) \;=\; x - \sum_\rho \frac{x^\rho}{\rho} + \sum_{n=1}^{\infty} \frac{x^{-2n}}{2n} - \frac{\zeta'(0)}{\zeta(0)}. \tag{126}$$

  Riemann states this for $\pi(x) = \sum_{p \leq x} 1$ instead. From this we can see why the Prime Number Theorem might be true, namely $\psi(x) \sim x$.

Riemann knew all of this but couldn't prove it; the machinery had not caught up to his intuition. The last is

Conjecture 3.1 (The Riemann Hypothesis)**.** *All the non-trivial zeros have real part equal to 1/2.*

It took awhile to substantiate these claims. Hadamard in 1893 worked on the theory of entire funtions (Hadamard product formula) and proved

$$\xi(s) \;=\; \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s) \tag{127}$$

has the product

$$\xi(s) \;=\; \xi(0)\prod_{\Im(\rho)>0}\left(1-\frac{s+s^2}{\rho(1-\rho)}\right). \tag{128}$$

To do this he proved the estimate $N(t) \ll T\log T$; this is weaker than what Riemann claimed, but was sufficient for convergence.

In 1895 von Mangoldt proved Riemann's explicit formula for $\pi(x)$ and $\psi(x)$. The Prime Number Theorem still wasn't proven, but these assertions were.

In 1896 Hadamard and de la Vallée Poussin independently proved the Prime Number Theorem, namely that $\psi(x) \sim x$. The key ingredient was that $\zeta(1+it) \neq 0$ (ie, no zero on the line $\Re(s) = 1$). This is an asymptotic formula. A few years later de la Vallée Poussin proved the Prime Number Theorem with an error term, $\psi(x) = x + O(xe^{-\sqrt{c_1 \log x}})$. This required a zero-free region when $\sigma < 1 - \frac{c_0}{\log t}$ (ie, no zeros to the right of this).

In 1905 von Mangoldt proved Riemann's formula for $N(T)$. In the same year von Koch proved the Riemann Hypothesis means the error term in the prime number theorem is basically $\sqrt{x}$.

3.1.2 The order of $\zeta(s)$ in the critical strip

The critical strip is the most important region for $\zeta(s)$. How large can it be as we go up? Why do we want to know this? From the explicit formula we see the zeros are important in understanding the primes, and we can get some information about these from knowing the size of the function. It is a fact that the zeros of an analytic function and the growth of that function are related. Other arithmetic questions turn out to depend on this as well.

For example, we have Jensen's Formula. Let $f(z)$ be analytic for $|z| < R$ and $f(0) \neq 0$. If z_i are the zeros inside $|z| \leq R$ then

$$\log\left(\frac{R^n}{|z_1\cdots z_n|}\right) = \frac{1}{2\pi}\int_0^{2\pi}\log|f(Re^{i\theta})|d\theta - \log|f(0)|. \tag{129}$$

Another application involves sums of $d_k(n)$, where these sums are an explicit term plus an integral of $\zeta^k(s)$.

Let's focus on estimates at the edge of the strip. Upper bounds for $\zeta(s)$ near $\sigma = 1$ allow us to widen the zero-free region. This leads to improvements in the remainder term for the Prime Number Theorem. Littlewood improved these estimates in 1922, and widens the zero free region and gives a better error term: $O(xe^{-c\sqrt{\log x \log\log x}})$. The idea is to approximate

$$\zeta(\sigma + it) \approx \sum_{n=1}^{N} \frac{1}{n^{\sigma+it}} \tag{130}$$

and try to exploit cancellation. If one could use the cancellation of the n^{it} then one should be able to improve the bounds. Littlewood did this by using the theory of exponential sums developed by Weyl.

Many years later (1958) Vinogradov and Korobov independently got $\zeta(\sigma + it) \ll \log^{2/3} t$ and no zeros in $\sigma \geq 1 - \frac{c}{\log^{2/3} t}$, which gives a better error term again. Instead of using Weyl's method to estimate exponential sums, they use Vinogradov's method.

To summarize: bounds on the $\sigma = 1$ line lead to improvements in the error term. The result of Vinogradov-Korobov really hasn't been improved.

What should the truth be? One can show

$$(1 + o(1))e^{\gamma} \log\log t \leq_{i.o.} |\zeta(1 + it)| \leq_{RH} 2(1 + o(1))e^{\gamma} \log\log t; \tag{131}$$

there isn't much wiggle room between what is known and the RH.

What about inside the critical strip? In 1908 Lindelöf investigated this: For a fixed σ let $\mu(\sigma)$ denote the lower bound of numbers μ such that $\zeta(\sigma + it) \ll (1 + |t|)^{\mu}$.

- $\zeta(s)$ is bounded for $\sigma > 1$ so $\mu(\sigma) = 0$ for $\sigma > 1$.
- $|\zeta(s)| \sim (|t|/2\pi)^{1/2-\sigma}|\zeta(1-s)|$ which implikes $\mu(\sigma) = 1/2-\sigma+\mu(1-\sigma)$.
- In particular, $\mu(\sigma) = 1/2 - \sigma$ for $\sigma < 0$.

Lindelöf proved that $\mu(\sigma)$ is continuous, convex and non-increasing. It follows that $\mu(1/2) \leq 1/4$; this is called the convexity bound, breaking this is quite important. Hardy-Littlewood showed that $\zeta(1/2 + it) \ll |t|^{1/6+\epsilon}$. A long history of trying to improve this. The best results since have come from exponential sum methods. Huxley and Watt show that $\mu(1/2) < 9/56$ (for example).

Conjecture 3.2 (Lindelöf Conjecture (LH))**.** *We should have* $\mu(\sigma) = 0$ *for* $\sigma \geq 1/2$*; which then fills in the picture.*

The LH says that for large $|t|$, $\log |\zeta(1/2 + it)| \leq \epsilon \log |t|$.

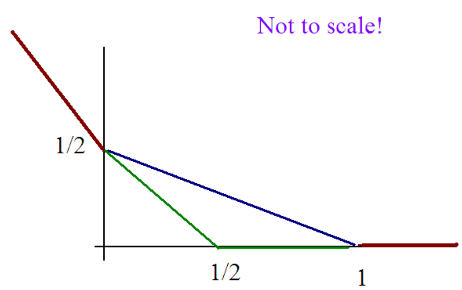

Figure 1: Plot of $\sigma(\mu)$

3.1.3 Mean value theorems

Averages such as

$$\int_0^T |\zeta(\sigma+it)|^{2k} dt \tag{132}$$

have been a focus for many years because

- Averages as well as pointwise upper bounds tell us about zeros and other applications;
- mean values are easier to prove than pointwise bounds;
-

In 1908 Landau proved the second moment:

$$\int_0^T |\zeta(\sigma+it)|^2 dt \;=\; \zeta(2\sigma)T \tag{133}$$

for $\sigma > 1/2$ fixed; in 1918 Hardy-Littlewood handled $\sigma = 1/2$ and found $T\log T$. To do this, they developed the approximate functional equation. In the same paper they prove a fourth moment, for $\sigma > 1/2$ fixed: $\zeta^4(2\sigma)T/\zeta(4\sigma)$. In 1926 Ingham gets the fourth moment on the half line, getting $(T/2\pi^2)\log^4 T$, by using an approximate functional equation for $\zeta(s)^2$. No one has proved a result for fourth or higher moments on the half-line. We have lower bounds (such as Ramachandra's) on the half-line: $T\log^{k^2} T$. This is believed to be the correct upper bound as well.

What constant should we put in front so that it is asymptotically correct? This suggests trying to find constants C_k such that

$$\int_0^T |\zeta(1/2+it)|^{2k} dt \ \sim \ C_k T \log^{k^2} T. \tag{134}$$

Conrey-Ghosh suggested that $C_k = a_k g_k / \Gamma(k^2+1)$ with g_k an integer. We know g_1 and g_2; Conrey-Ghosh conjectured that $g_3 = 42$ and Conrey-Ghosh-Gonek conjectured $g_4 = 24024$. Using random matrix theory, Keating and Snaith conjectured g_k for each k, and it agrees with the four previous values (the two known and the two conjectured). This was a huge development.

Recently Soundararajan has shown that under RH, we are close to the right order.

3.1.4 Zero density estimates

If you can't prove RH, can you at least show there aren't too many. There are lots of applications (such as gaps between prime numbers). Let $N(\sigma, T)$ denote the number of zeros in the critical strip with real part at least σ. Bohr and Landau showed in 1912 that $N(\sigma, T) \ll T$. Since $N(T) \sim (T/2\pi)\log T$, this says the proportion of zeros to the right of $\sigma > 1/2$ tends to 0 as $T \to \infty$. Equivalently, the zeros cluster near the half-line. If they are not all on the half-line, a huge amount are very near it. Bohr and Landau used Jensen's formula. Today we have much better zero-density estimates of the form $N(\sigma, T) \ll T^{\theta(\sigma)}$ with $\theta(\sigma) < 1$.

Conjecture 3.3 (Density Hypothesis)**.** $N(\sigma, T) \ll T^{2(1-\sigma)} \log T$.

Notice that when $\sigma = 1/2$ we do get $T \log T$. The LH implies $N(\sigma, T) \ll T^{2(1-\sigma)+\epsilon}$ (note RH implies LH).

3.1.5 The distribution of a-values of $\zeta(s)$

So far we've distributed when $\zeta(s) = 0$. What about when it equals a fixed number a? Bohr developed a lovely theory. First, the curve $f(t) = \zeta(\sigma + it)$ for some fixed $\sigma \in (1/2, 1]$. This curve is dense in $\mathbb{C}$, getting arbitrarily close to any complex number. The idea is to show that $\zeta(\sigma + it) \approx \prod_{p \le N}(1 - p^{-\sigma - it})^{-1}$ for most t, then use Kronecker's theorem to find a t so that the numbers p^{-it} point in such a way that $\prod_{p \le N}(1 - p^{-\sigma - it})^{-1} \approx a$. We have to hope that these t's are in the set where ζ can be approximated this way.

As a second result, let $N_a(\sigma_1, \sigma_2, T)$ be the number of solutions to $\zeta(s) = a$ for $\sigma_1 \le \sigma \le \sigma_2$ and $0 \le t \le T$. Using the same sort of ideas one gets this is asympototic to $c(\sigma_1, \sigma_2)T$. This is quite different from the case $a = 0$ (we are getting something of size T, not a power less).

3.1.6 Zeros on the critical line

Let $N_0(T)$ is the number of zeros up to T on the line. Hardy in 1914 showed there are infinitely many. Hardy-Littlewood in 1921 showed there are at least cT. This was improved by Selberg to a positive percent in 1942; Levinson got $1/3$ in 1974 and Conrey 2/5 in 1989. All of these use mean value estimates.

3.1.7 Calculating zeros on the line

In 1903 Gram showed that the first 15 zeros are on the line and are simple. Backlund improved this to the zeros up to 200 in 1912, long sequence of people improving this. Most recent is at least the first ten trillion. Also (Odlyzko) clumps of zeros around 10^{24} all on the line.

3.1.8 More recent developments

In the last 35 years there has been a lot of work trying to understand the zeros assuming RH, wanting to know how they are distributed. First big achievement due to Montgomery, where in 1974 he showed that under RH the zeros behave like eigenvalues of random Hermitian matrices. From 1980 onward Odlyzko has done extensive computations to support this conjecture.

There are also new mean value theorems (Gonek and Conrey, Gosh and Gonek). Assuming RH and sometimes GLH and GRH, Conrey, Ghosh and Gonek prove that there are large and small gaps between consecutive zeros, and simplicity.

Another new result is a hybrid formula. The random matrix formulas have no arithmetic in them; the g_k come from random matrix theory but the a_k come from arithmetic and must be inserted. Gonek, Hughes and Keating found an unconditional hybrid formula for $\zeta(s)$, writing it as a truncated product of primes times a truncated product of zeros (ie, an Euler-Hadamard combination). This gives the a_k and g_k both appearing naturally.

3.2 Mean Value Theorems and the Zeros of the Zeta Function

http://www.williams.edu/go/math/sjmiller/public_html/ntandrmt/talks/UtahWorkshopNotes.pdf

Themes from last time: Study of a-values, zeros, zeros on the line, simple zeros.... Mean value theorems play an important role in the field. Today we'll go more in depth on mean value theorems and give three applications to very important theorems. This will give an idea of how the tool of mean values is used in several different areas.

Outline:

- What is a mean value theorem?
- Mean values and zeros?
- A sample of important estimates.
- Application: A simple zero-density estimate.
- Application: Levinson's method.
- Application: number of simple zeros.

3.2.1 What is a mean value theorem?

If you have an analytic function f and integrate over a circle, that's an example from classical analysis. For our context, typically dealing with functions given by Dirichlet series, instead of integrating over a circle we integrate over vertical line segments: $\int_0^T |F(\sigma + it)|^2 dt$. Often want to do this integral on a line that is not in the half-plane of absolute convergence. While it is customary to divide by the length of the interval, frequently one doesn't.

Another time of mean value theorem is a discrete case: $\sum_{r=1}^{R} |F(\sigma_r + it_r)|^2$. For example, we could take $F(s) = \zeta(s)^k$. Another example is $F(s) = (\zeta'(s))^k$ and study $\sum_{\rho \in S} |\zeta'(\rho)|^{2k}$.

For another example, consider $F(s) = F_N(s) = \sum_{n=1}^{N} a_n n^{-s}$ a Dirichlet 'polynomial' of 'length' N. One can show its mean square (up to T) is $(T + O(N \log N)) \sum_{n=1}^{N} |a_n|^2 / n^{2\sigma}$; this is the classical result, and has been improved since by Montgomery and Vaughn.

3.2.2 Mean Value and zeros

We use Jensen's Formula. If an analytic function is small on a circle then you can't have too many zeros close to the center. This makes quantitative the intuitive notion that the density of zeros and the size of a function are connected.

Often not interested in mean on a circle but rather on a vertical line, we are not interested in Jensen's Formula on a circle but rather on a line. We have Littlewood's Lemma for an analytic function $f(s)$ which is non-zero on a rectangle $\mathcal{C}$. Littlewood's lemma expresses $2\pi \sum_{\rho \in \mathcal{C}} \mathrm{dist}(\rho)$ in terms of four integrals, two involving the logarithm of $|f|$ and two involving the argument of f; here the distance refers to the distance from the left edge of the rectangle $\mathcal{C}$. The main contribution will be $\int_0^T \log|f(\sigma_0 + it)|dt$; the other three terms are error terms.

This gives an expression involving the zeros in terms of one integral, which sadly is frequently hard to compute. We often use a trick to compute it. The trick is to put a one-half outside and square inside the logarithm; this doesn't change anything and is now talking about the average of the logarithm of the modulus squared; we use a convexity estimate to replace it with the logarithm of the integral:

$$\begin{aligned} \frac{1}{T}\int_0^T |f(\sigma_0+it)|dt &= \frac{1}{2T}\int_0^T \log|f(\sigma_0+it)|dt \\ &\leq \frac{1}{2}\log\left(\frac{1}{T}\int_0^T |f(\sigma_0+it)|^2 dt\right). \end{aligned} \tag{135}$$

3.2.3 A sample of important estimates

Recall that

$$I_k(\sigma, T) = \int_0^T |\zeta(\sigma+it)|^{2k} dt. \tag{136}$$

We have $I_1(\sigma, T) \sim c_1(\sigma)T$ as $T \to \infty$; if $\sigma = 1/2$ get $T \log T$, which implies $\zeta(s)$ is erratic on $\sigma = 1/2$.

Conrey and Ghosh conjectured formulas for these moments, which agree with the random matrix theory conjectures.

Another important mean is

$$\int_0^T |\zeta^{(j)}(\sigma+it)M_N(\sigma+it)|^2 dt, \tag{137}$$

where

$$M_N(s) \ = \ \sum_{n\le N} \frac{\mu(n)}{n^s}\left(1-\frac{\log n}{\log N}\right) \tag{138}$$

is a mollifer. Here $M_N(s)$ approximates $1/\zeta(s)$ when $\sigma > 1$ This continues for $\sigma \le 1$ in some sense. Hence $\zeta(s)M_N(s)$ should be tamer than $\zeta(s)$ on $\sigma = 1/2$ (can prove if RH is true if close to the half-line). General estimates for means like the above were proved by Conrey, Ghosh and Gonek with $N = T^\theta$ and $\theta < 1/2$. Later, Conrey used Kloosterman sums techniques to show these formulas also hold for $\theta < 4/7$.

One more example: Assuming the Riemann Hypothesis and the Generalized Lindelöf Hypothesis, Conrey, Ghosh and Gonek also proved the discrete version of this, including estimates for sums like

$$\sum_{\gamma<T} |\zeta'(\rho)M_N(\rho)|^2. \tag{139}$$

Here γ runs over the ordinates of the zeros of $\zeta(s)$ and $N = T^\theta$ with $\theta < 1/2$.

3.2.4 Application: A simple zero-density estimate

We fix a $\sigma > 1/2$ and want to know $N(\sigma, T)$, the number of zeros with $\Re(\rho) > \sigma$ and $\Im(\rho) < T$; we want an upper bound. We apply Littlewood's lemma for a rectangle $\mathcal{C}$ that is a little bit larger, with left boundary at $\Re(s) = \sigma_0$. We have

$$\sum_{\rho\in\mathcal{C}} \mathrm{dist}(\rho) \ \ge\ \sum_{\substack{\rho\in\mathcal{C}\\ \sigma\le\beta}} \mathrm{dist}(\rho) \ \ge\ (\sigma-\sigma_0)N(\sigma,T). \tag{140}$$

On the other hand, we can use Littlewood's lemma to replace the left hand side with an integral of the logarithm of the modulus of ζ, and then use our trick to replace that with $\le \frac{T}{4\pi}\log\left(\int_0^T |\zeta(\sigma_0+it)|^2 dt\right)$. The integral is $I_1(\sigma_0, T) \sim c_1(\sigma_0)T$. Therefore

$$(\sigma-\sigma_0)N(\sigma,T) \ \le\ \frac{T}{4\pi}\log c_1(\sigma_0) \tag{141}$$

and thus $N(\sigma, T) \ll T$. Since $N(T) \sim \frac{T}{2\pi}\log T$, we see

$$N(\sigma,T)/N(T) \ = \ O(1/\log T) \tag{142}$$

for any $\sigma > 1/2$, which implies an infinitesimal percentage of the zeros are off the line in the limit (in this sense).

We lose in the inequality in estimating the integral when we replace the integral of the logarithm with the logarithm of the integral; this replacement gets better the smoother the function is. If one puts in the right kind of mollifier, one can hope to do better.

3.2.5 Application: Levinson's method

Levinson proved that at least a third of the zeros are on the critical line. We let $N_0(T)$ denote the number of zeros on the critical line up to T. Hardy showed there were infinitely many, and then eventually Selberg showed that a positive percentage. The current record is do to Conrey, who showed that 40% of the zeros are on the line.

Levinson's method begins with a result of Speiser:

Theorem 3.4 (Speiser)**.** *RH is equivalent to* $\zeta'(s) \neq 0$ *for* $0 < \sigma < 1/2$.

In the 1970s a quantitative version was proved:

Theorem 3.5 (Levinson-Montgomery)**.** $\zeta(s)$ *and* $\zeta'(s)$ *have the same number of zeros inside* $\mathcal{C}$ *up to* $O(\log T)$*, where* $\mathcal{C}$ *is a rectangle from slightly to the left of 1/2 to -1.*

Proof. The change in the argument of $\zeta'(s)/\zeta(s)$ on the rectangle is $O(\log T)$, and the change in argument is 2π times the number of zeros of $\zeta'(s)$ in $\mathcal{C}$ minus the number of zeros of $\zeta(s)$ in $\mathcal{C}$. If the argument is bounded by $\log(T)$, then the number of zeros must be close. □

Sketch of the proof of Levinson's Theorem. We have $\zeta'(s)$ and $\zeta(s)$ essentially have the same number of zeros. The $\zeta(s)$ zeros are symmetric about the half line, so the ζ function has the same number of zeros on the other side. If we count the zeros in the box, it is $N(T) = N_0(T) + 2N'(T) + O(\log T)$ where $N'(T)$ is the number of zeros of $\zeta'(s)$ in the left box. Solving for $N_0(T)$ gives

$$N_0(T) \ = \ N(T) - 2N'(T) + O(\log T), \tag{143}$$

so an upper bound for $N'(T)$ gives a lower bound for $N_0(T)$.

By the functional equation for $\zeta(s)$, $\zeta'(s)$ has the same zeros in $1/2 < \sigma < 2$, $0 < t < T$ as

$$G(s) \ = \ \zeta(s) + \frac{\zeta'(s)}{L(s)}, \quad \text{where} \quad L(s) \ \sim \ \frac{1}{2\pi}\log s. \tag{144}$$

So we need an upper bound for the number of zeros of $G(s)$ in the rectangle in the right. We have a rectangle and an analytic function, use Littlewood's lemma:

$$\begin{aligned}\frac{1}{2\pi}\int_0^T \log|G(a+it)|dtM(a+it)+\mathcal{E} &= \sum_{\text{zeros of } G\in\mathcal{C}_a} \operatorname{dist}(\rho^*) \\ &\geq \sum_{\substack{\text{zeros of } G\in\mathcal{C}_a\\ \beta^*\geq 1/2}} \operatorname{dist}(\rho^*) \\ &\geq (1/2-a)N'(T); \qquad (145)\end{aligned}$$

here $a = \frac{1}{2} - \frac{c}{\log T}$ and $c > 0$ and $M_N(a+it)$ is our mollifier. The mollifier is

$$M(s) = \sum_{n\leq T^\theta} \frac{a_n}{n^s}, \quad a_n = \mu(n)n^{a-1/2}\left(1-\frac{\log n}{\log T^\theta}\right), \qquad (146)$$

which approximates $1/\zeta(s)$. Thus we need an estimate for the integral of G and M. Levinson showed one can take $\theta = 1/2-\epsilon$, Conrey showed one may take $\theta = 4/7-\epsilon$. Farmer conjectured that this remains true for θ arbitrarily large, which would give $N_0(T) \sim N(T)$, or 100% of the zeros are on the line. □

3.2.6 Application: number of simple zeros

We discuss how to show many zeros are simple. Let $N_s(T)$ be the number of zeros with imaginary part at most T and simple. We believe that $N(T) = N_0(T) = N_s(T)$. Montgomery (in his 1974 pair correlation paper) showed under RH that at least 2/3 of the zeros are simple. Using other methods, Conrey, Ghosh and Gonek proved that under RH and GLH that at least 19/27 of the zeros are simple.

Sketch of the method: We use a Cauchy-Schwartz inequality applied to

$$\left|\sum_{\gamma<T}\zeta'(1/2+i\gamma)\right|^2 \leq \left(\sum_{\substack{\gamma<T\\ 1/2+i\gamma \text{ simple}}} 1\right)\left(\sum_{\gamma<T}|\zeta'(1/2+i\gamma)|^2\right). \qquad (147)$$

Asymptotic estimates for the means provide a lower bound of $N_S(T) \geq cT$. We lose when using the Cauchy-Schwarz inequality, which suggests we should smooth ζ' and expect to lose less in the inequality. We use a mollifer involving $\mu(n)$, get a similar inequality but the means are more complicated to compute but doable. An elaboration of the method shows that under the same hypotheses 95% of the zeros are either simple or double.

3.3 Pair correlation of the zeros of the zeta function

http://www.williams.edu/go/math/sjmiller/public_html/ntandrmt/talks/UtahWorkshopNotes.pdf

Much of the subject began with Montgomery's pivotal paper on the pair correlation of the zeros of the zeta function. In Conrey's first talk he showed a lot of random matrix theory stuff to derive distributions for random matrix ensembles; won't recognize anything like that, doing everything on the number theory side.

3.3.1 Starts with an explicit formula

Take the logarithmic derivative of the zeta function: $\zeta'(s)/\zeta(s) = -\sum \Lambda(n)/n^s$. Key identity is the integral of $\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} y^w dw/w$, which is 1 if $y > 1$, $1/2$ if $y = 1$ and 0 if $y < 1$ (note $c > 0$). We use this as a basic building block, and find

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{\zeta'(s+w)}{\zeta(s+w)}\frac{x^w}{w}dw \;=\; -\sum_{n\le x}\frac{\Lambda(n)}{n^s}. \tag{148}$$

Can interchange integral and sum as everything is absolutely convergent. Should really do for a finite length integral and have error terms; called Perron's formula, take the limit as the truncation tends to infinity. We pull the contour to $-\infty$ and find the LHS equals

$$\sum_\rho \frac{x^{\rho-s}}{\rho-s} + \frac{x^{1-s}}{s-1} - \sum_{n=1}^{\infty}\frac{x^{-2n-s}}{2n+s} + \frac{\zeta'(s)}{\zeta(s)}. \tag{149}$$

We now equate these and get an explicit formula for $\sum \Lambda(n)/n^s$. If we take $s = 0$ we recover the standard explicit formula from the prime number theorem.

Assume RH and evaluate when $s = 3/2 + it$. Then take $s = -1/2 + it$ and evaluate, and we can replace the ζ'/ζ term with $-\log(|t| + 2) + O(1)$. We have expressions like $\pm x^{1/2}\sum_\gamma x^{i\gamma}/(1 \mp i(t-\gamma))$. We do some algebra and subtract, and find $-2x^{1/2}\sum_\gamma x^{i\gamma}/(1+(t-\gamma)^2)$. The right hand side is a continuous function in x as is the left hand side, so we don't have to worry about x being a prime power. We equate the simplifications of the left and right hand sides, trivially estimating some of the sums, and we find under RH that

$$-2x^{1/2}\sum_\gamma \frac{x^{i\gamma}}{1+(t-\gamma)^2)} \tag{150}$$

is equal to some simple terms and a Dirichlet series. We right this as $L(x,t) = R(x,t)$. Montgomery's pair correlation is proved by calculating both sides of $\int_0^T |L(x,t)|^2 dt$ and $\int_0^T |R(x,t)|^2 dt$.

Let's look at the left hand side term first. He truncates the sum and then extends the integral to $-\infty$ to ∞, introducing a small error. Square things out and do the integral via residue theory. The integral becomes $w(\gamma,\gamma') = 4/(4+(\gamma-\gamma')^2)$. Call the resulting expression $2\pi x F(x,T) + O(x\log^3 T)$, easily see $F(x,T)$ is non-negative. If we replace x with $1/x$ we get a complex conjugate and find $F(1/x,T) = F(x,T)$ for $x > 0$. Thus

$$\int_0^T |L(x,t)|^2 dt \;=\; 2\pi x F(x,T) + O(x\log^3 T). \tag{151}$$

We now have to compute the right hand side. We use the Montgomery-Vaughan mean value theorem to compute the mean value for the Dirichlet series piece, applying the prime number theorem. The other terms on the right hand side are handled in a straightforward manner. We write the RHS as a sum of $A_i(x,t)$ for $i = 1$ to 4. For a given x we let

$$M_i \;=\; \int_0^T |A_i(x,t)|^2 dt. \tag{152}$$

Order them so that $M_1 \geq \cdots \geq M_4$. By the Cauchy-Schwarz inequaltiy,

$$\int_0^R |R(x,t)|^2 dt \;=\; M_1 + O((M1M2)^{1/2}). \tag{153}$$

In different ranges, different ones of the A_i's are largest. We find the mean square of the right hand side is $\frac{T}{2\pi}(\log x + o(\log T)) + O(x\log x) + \frac{T}{2\pi x^2}\log^2 T(1+o(1)$. We set $x = T^\alpha$ and $F(\alpha) = F(\alpha,T) = \left(\frac{T}{2\pi}\log T\right)^{-1} F(T^\alpha,T)$.

Theorem 3.6 (Montgomery)**.** *Assuming RH,*

$$F(\alpha) \;=\; \left(\frac{T}{2\pi}\log T\right)^{-1} \sum_{0<\gamma,\gamma'\leq T} w(\gamma-\gamma')T^{i\alpha(\gamma-\gamma')} \tag{154}$$

equals

$$(1+o(1))T^{-2\alpha}\log T + \alpha + o(1) \tag{155}$$

uniformly for $|\alpha| \leq 1-\epsilon$ *as* $T \to \infty$.

3.3.2 Application

We integrate $F(\alpha)$ against a test function $\widehat{f}(\alpha)$. Knowing $F(\alpha)$, we can then get information about pairs of zeros:

$$\left(\frac{T}{2\pi}\log T\right)\int_{-\infty}^{\infty} F(\alpha)\widehat{r}(\alpha)d\alpha \;=\; \sum_{0<\gamma,\gamma'<T} w(\gamma-\gamma')r\left((\gamma-\gamma')\frac{T}{2\pi}\right). \quad (156)$$

Note we can only use this formula when $\widehat{r}$ is supported in $(-1,1)$.

One application is to counting simple zeros, taking $r(u)=(\sin(\pi\lambda u)/\pi\lambda u)^2$, so $\widehat{r}(\alpha)=\lambda^{-1}\max(1-|\alpha|/\lambda,0)$ for $\lambda>0$. Thus we need to take $\lambda<1$. Observe that if $\rho=1/2+i\gamma$ is a zero of multiplicity $m(\rho)$, then we end up with

$$\sum_{0<\gamma<T} m(\rho) \;\le\; \left(\frac{4}{3}+o(1)\right)\frac{T}{2\pi}\;\log T. \quad (157)$$

We have

$$\sum_{\substack{0<\gamma<T\\ \text{zero simple}}} 1 \ge \sum_{0<\gamma<T}(2-m(\rho)). \quad (158)$$

This leads to, under RH, that 2/3rds of the zeros are simple.

3.3.3 Montgomery's Conjecture

We proved his theorem for $F(\alpha)$ with $|\alpha|<1$ by computing the mean square of both sides. The hang-up is that we used the Montgomery-Vaughan theorem to compute the mean of the Dirichlet series. We can only do these computations for certain lengths of these Dirichlet series. What happens for larger α? The only required estimates for 'diagonal' terms involving $\sum_{n\le x}\Lambda(n)^2$ is satisfactory for $x=o(T)$. If $\alpha\ge 1$ then $x\ge T$ and 'off-diagonal terms contribute to the mean square. These require estimates of sums of $\Lambda(n)\Lambda(n+h)$ uniformly in h (this is equivalent to twin prime conjectures and so on).

Conjecture 3.7 (Montgomery)**.** $F(\alpha,T)=1+o(1)$ *uniformly for* $1\le\alpha\le A$ *for any fixed* A *as* $T\to\infty$*.*

This allows us to use more general $\widehat{r}$, and led him to

Conjecture 3.8 (Montgomery's Pair Correlation Conjecture)**.** *For any fixed* $\beta > 0$ *we have*

$$\sum_{\substack{0<\gamma,\gamma'<T \\ 0<\gamma'-\gamma<2\pi\beta/\log T}} 1 \sim \left(\int_0^\beta \left[1 - \left(\frac{\sin \pi x}{\pi x}\right)^2\right] dx\right) \frac{T}{2\pi} \log T \tag{159}$$

at $T \to \infty$.

One quick deduction is $\lim\inf(\gamma_{n+1} - \gamma_n)(\log \gamma_n)/2\pi = 0$. Another application is that almost all zeros are simple.

3.3.4 Recent developments

In the 1980s Goldston and Montgomery showed the Pair Correlation Conjecture is equivalent to a certaine stimate of teh variance of the number of primes in short intervals. Later Goldston, Gonek and Montgomery showed it is also equivalent to a mean value estimate for the second moment of $\zeta'(\sigma + it)/\zeta(\sigma + it)$ for σ near 1/2.

We do know (Goldston, Gonek, Özlük and Snyder) that $F(\alpha, T) \geq 3/2 - \alpha + o(1)$ on $(1, 3/2)$ under GRH.

3.4 Finite Euler Products and the Riemann Hypothesis

`http://www.williams.edu/go/math/sjmiller/public_html/ntandrmt/talks/UtahWorkshopNotes.pdf`

Why are all the zeros on the line? Why are they simple? What produces this? If you work in this subject, after a short while you realize that to prove the Riemann Hypothesis you'll have to use both the functional equation and the Euler product? Why? We have examples of functions that satisfy one but not the other (both ways) where the Riemann Hypothesis fails. So both are necessary, but this isn't an explanation.

- Approximations of $\zeta(s)$.
- A function related to $\zeta(s)$n and its zeros.
- The relation between $\zeta(s)$ and $\zeta_X(s)$.

3.4.1 Approximations of $\zeta(s)$

Let s be away from 1, write as $\sigma + it$, in the half-plane $\sigma > 1$ we have

$$\zeta(s) \; = \; \sum_{n=1}^{X} \frac{1}{n^s} + O\left(\frac{X^{1-\sigma}}{\sigma - 1}\right), \tag{160}$$

which is small if we are away from the pole at 1. The moral of this is that $\zeta(s)$ is approximately this partial sum when we are in the right half plane, and it doesn't really matter how small X is. Things improve as X grows, but can get away with a small X.

What happens when we get into the critical strip? Suffices to study the right half of the critical strip. A crude form extends:

$$\zeta(s) \; = \; \sum_{n=1}^{X} \frac{1}{n^s} + O\left(\frac{X^{1-\sigma}}{\sigma - 1}\right) + O(X^{-\sigma}), \tag{161}$$

but we need $X \gg t$. If we take $X = t$ we get

$$\zeta(s) \; = \; \sum_{n \leq t} \frac{1}{n^s} + O(t^{-\sigma}). \tag{162}$$

Moral: inside the critical strip you can't do better than this as far as unconditional estimates go. If you want to approximate the zeta function by a truncation in a critical strip, the length of the approximation must be of size t.

If you assume LH, namely $\zeta(1/2 + it) \ll (|t| + 2)^{\epsilon}$, then you get

$$\zeta(s) \; = \; \sum_{n \leq X} \frac{1}{n^s} + O(X^{1/2-\sigma}|t|^{\epsilon}), \tag{163}$$

which is fine for $1/2 \leq \sigma \ll$ and $X \leq t^2$.

What about to the left of $1/2$? We can't use short sums when $\sigma < 1/2$. Suppose ζ was a short sum of length X. Use Montgomery-Vaughan to get the mean square (integrating from T to $2T$) is of size $T \cdot X^{1-2\sigma}$, but the mean square of the zeta function integral is $T \cdot T^{1-2\sigma}$, which thus won't work with X short.

What if we try to examine approximations of the Euler product? Truncate the product: trivially estimate the tail of the product (no zeros when $\sigma > 1$), use logarithms, then exponentiate at the end. We find

$$\zeta(s) \; = \; \prod_{p \; leX} \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 + O\left(\frac{X^{1-\sigma}}{(1-\sigma)\log X}\right)\right). \tag{164}$$

What about approximations in the strip? We work with a weighted Euler product.

$$\prod_{p\le X^2}\left(1-\frac{1}{p^s}\right)^{-1} \;=\; \exp\left(\sum_{p\le X^2}\sum_{k=1}^{\infty}\frac{1}{kp^{ks}}\right). \tag{165}$$

We set

$$P_X(s) \;=\; \exp\left(\sum_{n\le X^2}\frac{\Lambda_X(n)}{n^s\log n}\right). \tag{166}$$

Also have to introduce a function $Q_X(s)$ which arises from zeros of $\zeta(s)$. There are three exponential sum pieces, one summing $F_2(z)$ over non-trivial zeros, one over the trivial zeros, and one over the pole. If z large then $F_2(z)$ small, and for z near zero we have $F_2(z)\sim\log(cz)$. The main contribution is from zeros close to s. It follows that

$$Q(s) \;\approx\; \prod_{|\rho-s|\le 1/\log X}\left(c(s-\rho)\log X\right). \tag{167}$$

Have P_X a finite Euler product of length X^2, Q_X a finite Hadamard product, then

Theorem 3.9 (Gonek-Hughes-Keating)**.** *For $\sigma\ge 0$ and $X\ge 2$,*

$$\zeta(s) \;=\; P_X(s)\cdot Q_X(s). \tag{168}$$

The more primes you take, the fewer zeros you need, and vice versa. Call this a hybrid formula. Writing this out with the approximations you see it's primes up to X^2 and zeros at most $1/\log X$ from s. If RH is true, the product is empty in the critical strip away from $s=1$ and get the finite Euler product. In fact, if $\sigma>1/2$ we have $\zeta(s)\approx P_X(s)$ (and can quantify this).

To the right of 1, we can approximate $\zeta(s)$ well with short sums, to the right of 1/2 it is if we assume LH, ... Does this continue to the left of 1/2? The answer is no again, no matter how long we take X. Instead of computing mean squares of ζ we'll do mean squares of $\log|\zeta(\sigma+it)|$, and again see the powers don't match. One consequence of this estimate is that if $\sigma<1/2$ then infinitely often in t we have $P_X(s)\gg\exp\left(X^{1-2\sigma}/\sqrt{\log X}\right)$, so P_X is big to the left of 1/2.

On LH (and so on RH) we have ζ is a short sum for $1/2 < \sigma \leq 1$ fixed, even if X is small. But on $\sigma = 1/2$ we need more terms:

$$\zeta(s) \;=\; \sum_{n \leq X} \frac{1}{n^s} + \sum_{X < n \leq t} \frac{1}{n^s} + o(1). \tag{169}$$

If you compare this to the approximate functional equation, we find

$$\sum_{X < n \leq t} \frac{1}{n^s} \;\sim\; \chi(s) \sum_{n \leq t/2\pi X} \frac{1}{n^{1-s}}. \tag{170}$$

If take $X = \sqrt{t/2\pi}$, the approximate functional equation has the same length in each term. On the critical line zeta can be approximated by something shorter if add another piece of similar complexity.

How much is the Euler product approximation off by as σ approaches $1/2$? A tempting guess is that for some range of X we have

$$\zeta(s) \;\approx\; P_X(s) + \chi(s) P_X(1-s). \tag{171}$$

But this is far too large if X is a power of t when $\sigma > 1/2$.

3.4.2 A function related to $\zeta(s)$n and its zeros

What if look at

$$\zeta_X(s) \;=\; P_X(s) + \chi(s) P_X(\overline{s}). \tag{172}$$

Notice these are identical on the critical line and

$$\zeta(s), \zeta_X(s) \;=\; P_X(s)(1 + o(1)) \tag{173}$$

when $\sigma > 1/2$ is fixed. So both ζ and ζ_X are approximately P_X when $\sigma > 1/2$.

Lemma 3.10. *If $0 \leq \sigma \leq 1$, $|t| \geq 10$, $|\chi(s)| = 1$ if and only if $\sigma = 1/2$. Further, we have a very good estimate for $\chi(s)$ (ie, its phase).*

Theorem 3.11. *All the zeros of $\zeta_X(s)$ with $|t| \geq 10$ lie on $\sigma = 1/2$.*

Proof. WE have

$$\zeta_X(s) \;=\; P_X(s) + \chi(s) P_X(\overline{s}). \tag{174}$$

We factor out $P_X(s)$, which never vanishes. Thus we need $\chi(s) P_X(\overline{s})/P_X(s) = -1$, so the modulus is 1. Note P_X is never 0, and by the lemma we need χ to be evaluated on the critical line to be of modulus 1. □

We have a function which is a skeleton of $\zeta(s)$, but easier to work with and satisfies the Riemann Hypothesis. Let's study it. What can we say about the number of zeros up to height T? For the regular zeta function the number of zeros can be written as the standard $(T/2\pi)\log(T/2\pi) - (T/2\pi) + 7/8 + S(T) + O(1/T)$, as well as being written as a sum of two arguments plus 1. We can now look at $\zeta_X(1/2 + it)$, pull out a $P_X(1/2 + it)$ and write the remaining piece involving arguments. It vanishes only when the exponential is -1, which requires the difference of the arguments to be 1/2 modulo 1. Call this function $F_X(t)$ (minus the above). Then on the half-line the zeros of $\zeta_X(1/2+it)$ are the solutions to $F_X(t) \equiv 1/2 \bmod 1$.

We can find a lower bound for the number of zeros. The function $F_X(t)$ is congruent to 1/2 modulo 1 happens at least $F_X(T)$ (as it is continuous). If you know a little about the zeta function, if we had equality in slide 23 is interesting as the sum is like an approximation for $S(T)$. How could we have more zeros? If $F_X(T)$ wiggles and is not monotonically increasing, we could have more zeros. It comes down to trying to figure out how large the sum can be. Call the size of that sum $\Phi(t)$, which infinitely often is big. In fact,

$$\Phi(tx) \ = \ \Omega\left(\sqrt{\log t/\log\log t}\right). \tag{175}$$

Farmer-Gonek-Hughes conjecture on what the right size is. Under RH, the sum we have is also bounded by $\Phi(t) + O(\log t/\log X)$.

How big does X have to be? Need $X \geq \exp(c\log t/\Phi(t))$.

Extra solutions: if $F_X(t)$ is not monotonically increasing, there could be extra solutions. Look at its derivative, and under RH the sum that arises is bounded by $\ll \Phi(t)\log X$. So for X not too large the derivative will be positive and thus there is a constant C such that if $X < \exp(C\log t/\Phi(t))$ then $F_X(t)$ is monotone and $N_X(t)$ is equal to (and not just $\leq$); this result assumes RH.

What about simple zeros? What can we say about simple zeros of $\zeta_X(s)$? Taking the derivative leads to $F_X'(t)$ must vanish. But we know that if X isn't too large that $F_X'(t)$ is positive. Thus

Theorem 3.12. *Under RH, there is a C such that for $X < \exp(C\log t/\Phi(t)$ all the zeros with imaginary part greater than 10 are simple.*

Unconditionally we can get 100% of the zeros are simple.

I find this very intriguing. We have a family of functions that has a Riemann hypothesis, can see what RH is true, can see why the zeros are simple.

What about large X? We really want to take X a power of t, but can only do $X < \exp(C \log t/\Phi(t))$. But even when X is large, the odds that $F'_X(\gamma) = 0$ are quite small. The likelihood of this happening without some hidden structure (there is some structure), the likelihood that where it crosses the line is where we have the derivative zero as well is improbable. Expect even for large X that most of the zeros will be simple.

3.4.3 Relation between $\zeta(s)$ and $\zeta_X(s)$

The plots show that even when we don't take too many primes, there is remarkable agreement between values of $|\zeta(s)|$ and $|\zeta_X(s)|$. Here is a heuristic reason. We saw that $P_X(s)$ approximates ζ to the right of $\sigma > 1/2$. Since $\chi(s)$ is small in this region, $\zeta_X(s) = P_X(s) + \chi(s)P_X(\overline{s})$, so this approximates $\zeta(s) + \chi(s)\zeta(\overline{s})$. On $\sigma = 1/2$, using the functional equation get $2\zeta(1/2 + it)$. This is why $|\zeta_X|$ is close to twice $|\zeta|$ on the half-line.

Why are the zeros close? Look at the expansion for $F_X(t)$. We get $N(t) - 1$ minus a sum over the imaginary part of F_2 evaluated at a function of the zeros. We only care about the values modulo 1, so can ignore the $N(t) - 1$. The sum is essentially bounded by $\log^{-2} X \sum_\gamma (t-\gamma)^{-2} \to 0$ as $X \to \infty$. Thus for large X, this sum is close to zero, so no way we can get a zero. Thus the zeros need to cluster near the zeros of the zeta function.

Theorem 3.13. *Under RH, if I is a closed interval between two consecutive zeros of $\zeta(s)$ and $t \in I$ then*

- $\zeta_X(1/2 + it) \to 2\zeta(1/2 + it)$ *as* $X \to \infty$*;*
- $\zeta_X(1/2 + it)$ *has no zeros in I for X sufficiently large.*

What is the moral of the story? Here is something that is almost transparent (at least if X isn't big). It's been part of the zeta function theory to find approximations. Polya came up with an approximation through an integral, and that seemed to be pretty amazing as the thing had the right number of zeros but uniformly distributed (like a picket fence), not capturing the complexity. This thing is....