1

Zeta functions in arithmetic and their spectral statistics

Zeév Rudnick
Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel

1 Introduction

The Riemann zeta function $\zeta(s)$ serves as an important model in many investigations in the theory of Quantum Chaos. My aims in these lectures, which are directed at physicists, are to explain some of the basic properties of $\zeta(s)$, its importance in Number Theory, introduce generalizations of $\zeta(s)$ used by number theorists, and discuss the spectral statistics of their zeros in connection with Random Matrix Theory.

In section 2, I begin by discussing the theory of prime numbers and the connection with the Riemann zeta function and the significance of the Riemann Hypothesis to the distribution of primes. In section 3, I discuss Dirichlet's theorem on the existence of primes in arithmetic progression. For this purpose, I introduce Dirichlet L-functions, a generalization of Riemann zeta function, and survey their basic properties. In section 4, I give two examples of automorphic L-functions, those attached to the modular discriminant and to eigenfunctions of the Laplacian on the modular domain. In section 5, after a very brief overview of Random Matrix Theory, I discuss spectral statistics of the zeros of all these L-functions. It seems that all of them have GUE statistics. In section 6, I sketch the argument that the pair correlation of the zeros is that of GUE, in the range that it can be proved.

2 The Riemann zeta function

We begin by surveying the theory of primes and the basic properties of the Riemann zeta function. For background reading, see [3], [7].

2.1 Prime Numbers

A *prime* is a natural number $p > 1$ which has no factors (other than itself and 1). The sequence of primes is thus $p_1 = 2,\ p_2 = 3,\ p_3 = 5, \dots$. A basic fact concerning integer arithmetic is

Theorem 2.1. (Fundamental Theorem of Arithmetic) *Every natural number is uniquely decomposable into a product of prime powers.*

The primes are thus the building blocks of all the integers. We would like to study their distribution. The first observation is due to Euclid.

Theorem 2.2. (Euclid) *There are infinitely many primes.*

Proof Argue by *reductio ad absurdum*: If there were finitely many primes, say only M of them, then form the integer $Q = p_1 \cdot p_2 \cdot \ldots \cdot p_M + 1$. It is either a prime or decomposable. Since Q is greater than all the primes $p_1, \ldots, p_M$, it cannot be a prime. However, Q clearly leaves remainder 1 on division by each of the available primes p_i, and thus being divisible by no prime, cannot decompose into a product of primes! We thus arrive at a contradiction. $\square$

A strengthening of Euclid's theorem is due to Euler, who showed that the sum of reciprocals of primes diverges:

$$\sum_p \frac{1}{p} = \infty$$

2.2 The density of primes

After knowledge that there are infinitely many primes, one can try to assess their density. Gauss recounted that in 1792, as a boy of 15, he arrived at the conjecture that the density of primes near x is about $1/\log x$ and so if we denote by $\pi(x)$ the number of primes up to x

$$\pi(x) := \#\{n : p_n \leq x\}$$

then $\pi(x)$ is asymptotically equal to the logarithmic integral, given for $x > 2$ by

$$\mathrm{Li}(x) := \int_2^x \frac{dt}{\log t}$$

In turn, $\mathrm{Li}(x)$ has an asymptotic expansion

$$\mathrm{Li}(x) = \frac{x}{\log x} + \frac{x}{(\log x)^2} + \ldots + c_n \frac{x}{(\log x)^n} + O(\frac{x}{(\log x)^{n+1}})$$

To check the strength of $\mathrm{Li}(x)$ as an approximation to $\pi(x)$, we examine Table 1 (writing $[y] :=$ integer part of y). As is seen from this table, $\mathrm{Li}(x)$ is a remarkably good approximation to $\pi(x)$ in this range. As a measure of the quality of the approximation, note that the width of the third column is about a half of the width of the second one, that is to say that the remainder is approximately square root of the main term!

The statement that $\pi(x) \sim \mathrm{Li}(x)$ is known as the Prime Number Theorem. It was proved in 1896 by Hadamard and de la Vallée Poussin, by using the Riemann zeta function. The empirical statement made above from the data in Table 1 as to the magnitude of the remainder in this approximation is a form of the celebrated Riemann Hypothesis. The connection between $\zeta(s)$ and the distribution of primes will be explained in Section 2.5, after we review some of the properties of $\zeta(s)$.

Table 1 Comparison between $\pi(x)$ and $\mathrm{Li}(x)$.

x	$\pi(x)$	$[\mathrm{Li}(x)] - \pi(x)$
10^8	5,761,455	754
10^{10}	455,052,511	3,104
10^{12}	37,607,912,018	38,263
10^{14}	3,204,941,750,802	314,890
10^{16}	279,238,341,033,925	3,214,632

2.3 The product formula for $\zeta(s)$

The Riemann zeta function is defined for complex s with $\mathrm{Re}(s) > 1$ by the series

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

The first important fact we need to know is Euler's product formula, which introduces prime numbers into the study of $\zeta(s)$:

Theorem 2.3 *For* $\mathrm{Re}(s) > 1$, $\zeta(s)$ *can be represented by the convergent product over all primes:*

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

Proof The idea is to expand each of Euler's factors $(1 - p^{-s})^{-1}$ as a geometric series

$$\frac{1}{1 - p^{-s}} = \sum_{k=0}^{\infty} \frac{1}{p^{ks}}$$

and to multiply together the resulting series

$$\prod_p \frac{1}{1 - p^{-s}} = \sum \frac{1}{(p_1^{k_1} p_2^{k_2} \cdot \ldots \ldots \cdot p_r^{k_r})^s}$$

We can write this as a sum

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

where $a(n)$ is the number of ways of expressing the integer n as a product of prime powers. By the Fundamental Theorem of Arithmetic 2.1, this can be done in one and only one way, i.e. $a(n) = 1$, which proves the product formula, once we check that everything is absolutely convergent if $\mathrm{Re}(s) > 1$. □

As the above argument shows, the product formula is but a form of the Fundamental Theorem of Arithmetic.

Remark Since $\zeta(s)$ is given as a convergent product when $\mathrm{Re}(s) > 1$, it is never zero in this region.

2.4 Analytic continuation and functional equation of $\zeta(s)$

To further explore the connection between the theory of primes and $\zeta(s)$, we will analytically continue $\zeta(s)$ to all values of s. We use the Gamma function given for $\mathrm{Re}(s) > 0$ by the integral representation

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

to define the *completed zeta function* by

$$\zeta^*(s) := \pi^{-s/2} \Gamma(\frac{s}{2}) \zeta(s)$$

The basic fact about this variant of $\zeta(s)$ is

Theorem 2.4

(1) *The completed zeta function $\zeta^*(s)$ has a meromorphic continuation to the entire s-plane.*

(2) *$\zeta^*(s)$ is analytic except for simple poles at $s = 0, 1$.*

(3) *It satisfies the functional equation*

$$\zeta^*(s) = \zeta^*(1 - s)$$

As an immediate consequence of this fact, we observe that $\zeta^*(s)$ has no zeros outside the critical strip $0 \leq \mathrm{Re}(s) \leq 1$. This holds since $\Gamma(s)$ is never zero, and $\zeta(s)$ is analytic and nonzero in the region of convergence $\mathrm{Re}(s) > 1$, so that the completed zeta function $\zeta^*(s) \neq 0$ in $\mathrm{Re}(s) > 1$; by the functional equation, the same is true for the symmetric region $\mathrm{Re}(s) < 0$. Moreover, since $\Gamma(s)$ is analytic except for simple poles at $s = 0, -1, -2, \ldots$, $\zeta(s)$ is nonzero in $\mathrm{Re}(s) < 0$ except for simple zeros at the negative even integers $s = -2, -4, \ldots$ (to make up for the simple poles of $\Gamma(\frac{s}{2})$ at these points). These are called the *trivial zeros* of $\zeta(s)$; the nontrivial ones are the zeros of $\zeta^*(s)$ and as we have seen they all lie in the critical strip.

Proof (Sketch) We start with the integral representation

$$\pi^{-s/2} \Gamma(\frac{s}{2}) \frac{1}{n^s} = \int_0^\infty e^{-\pi n^2 t} t^{s/2} \frac{dt}{t}$$

which shows that we have an integral representation of $\zeta^*(s)$ for $\mathrm{Re}(s) > 1$ as

$$\zeta^*(s) = \int_0^\infty \frac{\theta(t) - 1}{2} t^{s/2} \frac{dt}{t} \tag{2.1}$$

where the theta-function is given for $t > 0$ by

$$\theta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t}$$

By Poisson summation, $\theta(t)$ has a transformation formula

$$\theta(\frac{1}{t}) = \sqrt{t}\theta(t) \tag{2.2}$$

Breaking up the region of integration in the integral representation 2.1 to an integral over $(0,1)$ and one over $(1,\infty)$, we change variables $t \mapsto 1/t$ to to transform the integral over (0.1) to one over $(1,\infty)$. We then use the transformation formula 2.2 for $\theta(t)$ to find after some manipulation that

$$\zeta^*(s) = -\frac{1}{s} - \frac{1}{1-s} + \int_1^\infty \frac{\theta(t)-1}{2}\left(t^{s/2} + t^{(1-s)/2}\right)\frac{dt}{t} \tag{2.3}$$

Since $\theta(t) - 1 = O(e^{-\pi t})$ as $t \to \infty$, the integral is absolutely convergent for all s and is therefore an entire function of s. Thus from eqn 2.3 we get the meromorphic continuation, with the only poles being the simple ones at $s = 0, 1$. From the symmetry of eqn 2.3 with respect to $s \mapsto 1-s$ we get the functional equation. $\square$

2.5 Connecting the primes and the zeros of $\zeta(s)$

Riemann, in his seminal paper of 1858 [18], used $\zeta(s)$ to give a formula for $\pi(x)$ in terms of the zeros of $\zeta(s)$. His formula gives a clear understanding as to why $\mathrm{Li}(x)$ is the correct approximation to $\pi(x)$. Instead of a formula for $\pi(x)$, it is more convenient to give a formula for the weighted sum of prime *powers* $p^k \le x$, each prime power p^k weighted by the logarithm $\log p$ of the corresponding prime. One defines

$$\psi(x) := \sum_p \sum_{k:p^k \le x} \log p$$

The repetitions p^k for $k \ge 2$ give a contribution of the order of at most $\sqrt{x}$. The primes $(k=1)$ give a contribution which, if one believes Gauss' assertion that the density of primes near x is about $1/\log x$, is about x. Thus we expect (and the above argument is easily made rigorous) that the Prime Number Theorem is equivalent to the assertion that $\psi(x) \sim x$. This is made transparent by the formula (due to von Mangoldt)

$$\psi(x) = x - \sum \frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0) \tag{2.4}$$

where the sum is over all zeros ρ of $\zeta(s)$. Note that we cannot expect the formula to converge absolutely, since it would then define a *continuous* function of x, while $\psi(x)$ is a step function with jumps when $x = p^k$ is a prime power.

The contribution of the trivial zeros $\rho = -2, -4, -6, \dots$ is easily summed to equal $\frac{1}{2}\log(1-x^{-2})$ and is negligible. The constant term is $\zeta'/\zeta(0) = \log 2\pi$. The important part is the sum over the nontrivial zeros, which we expect to be of smaller order than x. It is thus crucial to understand the distribution of the zeros. We will turn to that, after a brief explanation of the origin of Riemann's formula.

2.6 The explicit formula

Riemann's formula and its variants such as eqn 2.4 are known as the *explicit formulae* of prime number theory. We give a smooth version which is absolutely convergent and is easily derived. For this we start with a compactly supported, smooth test function $g \in C_c^\infty(\mathbf{R})$, which we will usually assume is *even* ($g(-u) = g(u)$), and set

$$h(r) = \int_{-\infty}^{\infty} g(u) e^{-iru} du$$

which is an entire function of r, exponentially decaying for r real. For notational convenience we set $\Gamma_{\mathbf{R}}(s) = \pi^{-s/2}\Gamma(\frac{s}{2})$. We will denote the nontrivial zeros of ζ by $\rho_n = \frac{1}{2} + iE_n$.

Theorem 2.5 *For g, h as above we have*

$$\sum h(E_n) - 2h(\frac{i}{2}) = \frac{1}{2\pi}\int_{-\infty}^{\infty} h(r)\, 2\,\mathrm{Re}\frac{\Gamma'_{\mathbf{R}}}{\Gamma_{\mathbf{R}}}(\frac{1}{2}+ir)dr - 2\sum_p \sum_k \frac{\log p}{p^{k/2}} g(k\log p)$$

The general shape of this formula is as the formula for $\psi(x)$, the right hand side of it being a sum over prime powers weighted by their logarithm $\log p$, and the left hand side is a sum over the zeros. Much has been said of the formal similarity between such formulae and the trace formulae used in "quantum chaos" (see e.g. [1], [8]), and this is one of the main reasons for the interest in the zeta function among people working in this area.

Proof We set

$$H(s) = \int_{-\infty}^{\infty} g(u) e^{(s-\frac{1}{2})u} du$$

so that $h(r) = H(\frac{1}{2} + ir)$. Consider the integral

$$I(h) := \frac{1}{2\pi i}\int_{\mathrm{Re}(s)=2} H(s) \frac{\zeta^{*\prime}}{\zeta^*}(s) ds$$

We compute this integral in two ways. First we expand the logarithmic derivative of $\zeta^*(s)$ by using Euler's product $\zeta^*(s) = \Gamma_{\mathbf{R}}(s)\prod_p(1-p^{-s})^{-1}$, which gives

$$\frac{\zeta^{*\prime}}{\zeta^*}(s) = \frac{\Gamma'_{\mathbf{R}}}{\Gamma_{\mathbf{R}}}(s) - \sum_p \sum_{k\geq 1} \log p \cdot p^{-ks}$$

On shifting the contour of integration to $\mathrm{Re}(s) = 1/2$ and integrating term by term, we find

$$\begin{aligned} I(h) &= \frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\frac{1}{2}} H(s)\frac{\Gamma'_{\mathbf{R}}}{\Gamma_{\mathbf{R}}}(s)ds - \sum_p\sum_{k\geq 1}\log p \int_{\mathrm{Re}(s)=\frac{1}{2}} H(s) p^{-ks} ds \\ &= \frac{1}{2\pi}\int_{-\infty}^{\infty} h(r)\frac{\Gamma'_{\mathbf{R}}}{\Gamma_{\mathbf{R}}}(\frac{1}{2}+ir)dr - \sum_p\sum_{k\geq 1}\frac{\log p}{p^{k/2}} g(\log p^k) \end{aligned}$$

where we have used Fourier inversion in the last step.

On the other hand, by shifting the contour of integration to $\mathrm{Re}(s) = -1$ we pick up contributions from poles at $s = 0, 1$ and from the zeros ρ of $\zeta^*(s)$ in the critical strip $0 \le \mathrm{Re}(s) \le 1$:

$$I(h) = -H(1) - H(0) + \sum_\rho H(\rho) + \frac{1}{2\pi i}\int_{\mathrm{Re}(s)=-1} H(s)\frac{\zeta^{*\prime}}{\zeta^*}(s)ds$$

We transform the integral above by using the functional equation of $\zeta^*(s)$ in the form

$$\frac{\zeta^{*\prime}}{\zeta^*}(s) = -\frac{\zeta^{*\prime}}{\zeta^*}(1-s)$$

and change variables $s \mapsto 1-s$ to get

$$\frac{1}{2\pi i}\int_{\mathrm{Re}(s)=-1} H(s)\frac{\zeta^{*\prime}}{\zeta^*}(s)ds = -\frac{1}{2\pi i}\int_{\mathrm{Re}(s)=2} H(1-s)\frac{\zeta^{*\prime}}{\zeta^*}(s)ds = -I(\tilde{h})$$

where $\tilde{h}(r) = h(-r)$. Since g is even, $\tilde{h} = h$ and $H(0) = H(1) = h(i/2)$, and so we get the required formula. □

2.7 The Riemann Hypothesis

As noted in section 2.4, the nontrivial zeros of $\zeta(s)$ all lie in the critical strip $0 \le \mathrm{Re}(s) \le 1$. If ρ is a zero then by the functional equation $\zeta^*(s) = \zeta^*(1-s)$, so is $1-\rho$, and since $\zeta(\bar{s}) = \overline{\zeta(s)}$ ($\bar{z}$ denoting complex conjugation), we get zeros at $\bar{\rho}$ and $1-\bar{\rho}$ (the two symmetries $s \mapsto \bar{s}$ and $s \mapsto 1-s$ coincide on the "critical line" $\mathrm{Re}(s) = 1/2$).

The first few zeros were computed by Riemann himself, and all lie on the critical line $\mathrm{Re}(s) = 1/2$. They are $\rho_n = 1/2 + iE_n$ with $E_1 = 14.13\ldots, E_2 = 21.02\ldots, E_3 = 25.01\ldots$ etc. (by symmetry, we only need to consider positive E).

Riemann's Hypothesis (RH): *All nontrivial zeros of $\zeta(s)$ lie on the critical line* $\mathrm{Re}(s) = 1/2$.

The Riemann Hypothesis has been checked extensively and is widely believed to be true, though an explanation and proof are still missing to date. Its significance to the theory of primes is immense. For instance, we can use RH to explain the small size of the remainder term $\mathrm{Li}(x) - \pi(x)$ in Table 1. To see this, it suffices to show that $\psi(x) - x$ is small, and in fact we shall argue that it is of order at most $\sqrt{x}\log^2 x$. This is reasonable if we look at the formula for $\psi(x)$ in eqn 2.4, which we will write as

$$\psi(x) = x - \sum \frac{x^{1/2+iE_n}}{1/2+iE_n} + \ldots$$

where the sum is now only over the nontrivial zeros, the omitted terms being negligible. If we assume the E_n are *real*, so $|x^{1/2+iE_n}| = \sqrt{x}$, it is tempting to then use the triangle inequality to deduce

$$|\psi(x) - x| \leq \sqrt{x} \sum \frac{1}{|1/2 + iE_n|}$$

and so say that $\psi(x) - x$ is of order $\sqrt{x}$. The argument is not quite airtight, as it transpires that the sum of absolute values diverges: $\sum 1/|1/2 + iE_n| = \infty$. Nevertheless, this argument gives the essence of what is happening, and in fact taking more care and using the distribution of zeros described below, one can show that $\psi(x) - x \ll \sqrt{x} \log^2 x$. This gives $\pi(x) - \mathrm{Li}(x) \ll \sqrt{x} \log x$ and so explains the observation regarding the size of the third column in Table 1.

The Riemann Hypothesis is one of the most important unsolved problems in Number Theory, and its validity has numerous implications. For instance, there are algorithms for *primality testing* of integers which are proved to require polynomial time (that is, testing if n is prime or not requires a number of operations polynomial in $\log n$), provided we assume RH (and its generalization to Dirichlet L-functions described in the next section).

As to what was actually proved so far, the significant fact is that there are no zeros on the boundary of the critical strip: $\zeta(1 + it) \neq 0$, so $0 < \mathrm{Re}(\rho) < 1$ for all nontrivial zeros. This is enough to prove the Prime Number Theorem, as was done (independently) by Hadamard and de la Vallée Poussin in 1896. One has in fact a zero-free region near the boundary of the critical strip, whose width shrinks to zero as we go up. However, we do not have a proof that there is any strip of the form $\mathrm{Re}(s) > 1 - \delta$ in which there are no zeros, for any $\delta > 0$.

2.8 The distribution of zeros

There are infinitely many nontrivial zeros, in fact $\sum 1/|\rho| = \infty$ as is clear from the explicit formula 2.4, otherwise $\psi(x)$ would be continuous. We denote by $N(T)$ their number in the rectangle $R_T = \{0 \leq \mathrm{Re}(s) \leq 1, 0 \leq \mathrm{Im}(s) \leq T\}$. Riemann stated that $N(T)$ is asymptotic to $T/2\pi \log T/2\pi$ (rigorously proved by von Mangoldt in 1905). We make this more precise by separating out a smooth mean growth $\bar{N}(t)$ from a fluctuating part, in some form $N(t) = \bar{N}(t) + N_{\mathrm{osc}}(t)$, where $N_{\mathrm{osc}}(t)$ is of smaller order than the mean $\bar{N}(t)$ and oscillates around zero.

This can be done by noticing that $N(T)$ can be computed from the argument principle as the imaginary part of the integral of $\zeta^{*\prime}/\zeta^*(s)$ around a contour surrounding the boundary of the rectangle R_T. We denote by $\vartheta(t)$ the argument of the gamma factor $\Gamma_{\mathbf{R}}(1/2 + it)$ and take as the smooth part the contribution of this gamma factor to the winding number:

$$\bar{N}(t) = \frac{1}{\pi} \vartheta(t) + 1$$

By Stirling's formula,

$$\bar{N}(t) = \frac{t}{2\pi} \log \frac{t}{2\pi} - \frac{t}{2\pi} + \frac{7}{8} + O(\frac{1}{t})$$

The oscillatory part, traditionally denoted by $S(t)$, is given by the winding number of $\zeta(s)$. It is known to be of smaller order then $\bar{N}(t)$: $S(t) = O(\log t)$. Littlewood showed that it indeed has mean zero, in fact $\int_{t_0}^{T} S(t)dt \ll \log T$. Selberg proved that $S(t)/\sqrt{2\pi^2 \log\log t}$ has a normal value distribution.

3 Dirichlet L-functions and primes in arithmetic progressions

In this section we will describe a generalization of the Riemann zeta function used to capture a certain feature of primes: their distribution in arithmetic progression. A good reference for this material is Davenport's book [3].

3.1 Arithmetic progressions and modular arithmetic

An arithmetic progression is a subset of the integers of the form $\{a, a+q, a+2q, \dots\}$. We say that two integers a and b are *congruent modulo q* if their difference is divisible by q: $a - b = kq$, k an integer (not necessarily positive). We write this as $a \equiv b \bmod q$. The ordinary operations of integer arithmetic respect the congruence relation modulo a fixed integer q, that is if $a \equiv a' \bmod q$ and $b \equiv b' \bmod q$ then $a \pm b \equiv a' \pm b' \bmod q$, $a \cdot b \equiv a' \cdot b' \bmod q$ etc. We say that a is invertible modulo q if there is some integer b so that $ab \equiv 1 \bmod q$. This happens if and only if a and q have no common factors, that is their greatest common divisor is 1: $\gcd(a, q) = 1$. We denote the residue classes of integers modulo q by $\mathbf{Z}/q\mathbf{Z}$. As representatives we may take $\{0, 1, \dots, q-1\}$. The invertible residue classes are denoted by $(\mathbf{Z}/q\mathbf{Z})^*$, and the number of such residue classes is denoted $\phi(q)$ (Euler's phi-function).

3.2 Primes in arithmetic progressions

An important issue is the existence of primes in a given arithmetic progression: Given a and $q > 1$, to find a large prime p with $p \equiv a \bmod q$. Clearly, in some instances it cannot be done, say the progression $\{2, 4, 6, 8, \dots\}$ contains no large primes as all primes except 2 are odd. Likewise, if a and q have a common factor $d > 1$ then it divides every element of the progression $a, a+q, a+2q \dots$ and so there are no primes in it (excepting perhaps if $a = d$ is prime). We should thus restrict attention to the case that a and q are co-prime. It turns out that this is the only obstruction to the existence of primes in arithmetic progression, as was proved by Dirichlet in 1837. In fact there are arbitrarily large primes in every progression not excluded by such reasoning:

Theorem 3.1. (Dirichlet's Theorem) *For $q > 1$ and any a co-prime to q, there are infinitely many primes of the form $a + kq$.*

One can try to give an argument for this along the lines of Euclid's argument for the existence of infinitely many primes (Theorem 2.2). This works in a few cases of small q, and for some special progressions such as $p \equiv 1 \bmod q$, but this line of attack has not yielded Dirichlet's theorem in its full force. We will indicate the approach that demonstrates the existence of infinitely many primes in every allowable progression by using Dirichlet's L-functions, a generalization of $\zeta(s)$. This approach will also show that for fixed $q > 1$, every progression $a \bmod q$ has asymptotically the same density of primes.

3.3 Dirichlet characters

The method for pulling out primes (or arbitrary integers) in a progression uses "mod q harmonic analysis", where the fundamental harmonics are called *Dirichlet characters.*

Definition 3.2 *Given $q > 1$, a Dirichlet character modulo q is a function $\chi(n)$ on the integers satisfying*

(1) *χ is q-periodic: $\chi(n+q) = \chi(n)$.*
(2) *$\chi(n) = 0$ if n is not co-prime to q.*
(3) *Multiplicativity: $\chi(nm) = \chi(n)\chi(m)$.*
(4) *$\chi(1) = 1$.*

Example 3.3 The *trivial character* χ_o modulo q is given by $\chi_o(n) = 1$ if n is co-prime to q, and $\chi_o(n) = 0$ otherwise.

Before giving further examples, we note one property of Dirichlet characters, namely $\chi(-1) = \pm 1$. This is since by multiplicativity, $\chi(-1)^2 = \chi((-1)^2) = \chi(1) = 1$. We say χ is *even* (resp. *odd*) if $\chi(-1) = +1$ (resp. $\chi(-1) = -1$).

Example 3.4 We determine the characters modulo $q = 3$: The invertible residue classes are $(\mathbf{Z}/3\mathbf{Z})^* = \{1, -1\}$. Since always $\chi(1) = 1$, and $\chi(-1) = \pm 1$, we see that there are exactly two characters modulo 3, the trivial one χ_o, and the odd character determined by $\chi_1(-1) = -1$.

Example 3.5 We take the case $q = 5$. Then $(\mathbf{Z}/5\mathbf{Z})^* = \{1, 2, 3, 4\}$. To determine all possible characters, we start by noticing that all invertible residues are powers of 2 mod 5: $-1 \equiv 4 \equiv 2^2 \bmod 5$, $3 \equiv 2^3 \bmod 5$. Since χ is multiplicative, this means $\chi(4) = \chi(2)^2$, $\chi(3) = \chi(2)^3$. Thus χ is determined by the number $\chi(2)$, which is a 4-th root of unity since $\chi(2)^4 = \chi(2^4) = \chi(1) = 1$. Therefore $\chi(2) = \pm 1, \pm i$ and each of these four possibilities gives rise to a Dirichlet character modulo 5.

In general, there are exactly $\phi(q)$ Dirichlet characters modulo q. They satisfy the fundamental Orthogonality Relations, crucial in their use to sieve out elements of progressions modulo q:

Lemma 3.6. (Orthogonality Relations)

(1) *For any nontrivial character $\chi \neq \chi_o$ modulo q*

$$\sum_{n \bmod q} \chi(n) = 0$$

(2) *For any $a \in (\mathbf{Z}/q\mathbf{Z})^*$ and $n \in \mathbf{Z}/q\mathbf{Z}$, ,*

$$\frac{1}{\phi(q)} \sum_{\chi \bmod q} \chi(a)^{-1}\chi(n) = \begin{cases} 1 & n \equiv a \bmod q \\ 0 & \textit{otherwise} \end{cases}$$

(the sum over all characters modulo q).

3.4 Dirichlet L-functions

Fix $q > 1$, which for simplicity I will assume is prime, and a nontrivial character χ modulo q. The corresponding L-function is defined for $\mathrm{Re}(s) > 1$ as

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

The sum converges conditionally in the region $\mathrm{Re}(s) > 0$. This is because the first part of the Orthogonality Relations implies the mean value of $\chi(n)$ is $O(1/n)$. In particular, $L(s,\chi)$ is analytic in $\mathrm{Re}(s) > 0$.

By using unique factorization for primes and multiplicativity of χ, one shows (as in the case of $\zeta(s)$) that there is an Euler product factorization

$$L(s,\chi) = \prod_p (1 - \frac{\chi(p)}{p^s})^{-1}$$

There is a functional equation, which for brevity we only give in the case that χ is even ($\chi(-1) = 1$): The completed L-function

$$L^*(s,\chi) := \pi^{-s/2}\Gamma(\frac{s}{2})L(s,\chi)$$

is entire, and we have a functional equation connecting $L(s,\chi)$ and $L(s,\chi^{-1})$:

$$L^*(s,\chi) = \tau(\chi)q^{-s}L^*(1-s,\chi^{-1})$$

Here the pre-factor $\tau(\chi)$ is a "Gauss sum"

$$\tau(\chi) := \sum_{m=1}^{q} \chi(m)e^{2\pi i m/q}$$

We will only need to know its magnitude, which is $|\tau(\chi)| = \sqrt{q}$. Note that the functional equation is not symmetric, as it relates $L(s,\chi)$ with $L(s,\chi^{-1})$, the L-function associated to the inverse character to χ.

The L-function associated to nontrivial χ has an analytic continuation, with no poles, and all its nontrivial zeros (that is, the zeros of the completed L function $L^*(s,\chi)$) are in the critical strip $0 \le \mathrm{Re}(s) \le 1$. The generalization of the Riemann Hypothesis is that all nontrivial zeros lie on the critical line $\mathrm{Re}(s) = 1/2$. This has been tested numerically but as in the case of $\zeta(s)$, an argument for it is lacking.

As for Riemann' ζ-function, for a nontrivial character χ modulo q there is an "explicit formula" relating the oscillatory sums

$$\psi(x,\chi) := \sum_{p^k \le x} \chi(p)\log p$$

with the nontrivial zeros ρ_χ of $L(s,\chi)$, which is

$$\psi(x,\chi) = -\sum_{\rho_\chi} \frac{x^{\rho_\chi}}{\rho_\chi} + \dots$$

Note the absence of the "main term" x which occurs if $\chi = \chi_o$ is the trivial character, and is due to the presence of the pole at $s=1$ in that case.

In smooth form, analogous to Theorem 2.5, the explicit formula for $L(s,\chi)$ is given by

$$\begin{aligned} \sum_n h(E_{n,\chi}) &= \frac{1}{2\pi}\int_{-\infty}^{\infty} h(r)\left(\log q + \frac{\Gamma'_{\mathbf{R}}}{\Gamma_{\mathbf{R}}}(\frac{1}{2}+ir) + \frac{\Gamma'_{\mathbf{R}}}{\Gamma_{\mathbf{R}}}(\frac{1}{2}-ir)\right) dr \\ &\quad - \sum_p \sum_k \frac{\log p}{p^{k/2}} \left(\chi(p^k) g(k\log p) + \chi^{-1}(p^k) g(-k\log p)\right) \end{aligned}$$

where $g \in C_c^\infty(\mathbf{R})$ is a compactly supported, smooth test function, $h(r) = \int_{-\infty}^{\infty} g(u) e^{-iru} du$ and the nontrivial zeros of $L(s,\chi)$ are denoted by $1/2 + iE_{n,\chi}$.

The density of zeros is given as for $\zeta(s)$ by

$$N(T) \sim \frac{T}{2\pi}\log\frac{T}{2\pi}$$

3.5 Application to primes in progressions

To see how to use the Orthogonality Relations, we fix $a \in (\mathbf{Z}/q\mathbf{Z})^*$ and count prime powers congruent to a modulo q, weighted with the logarithm of the corresponding prime:

$$\psi(x;a,q) := \sum_{p,k\geq 1} \sum_{p^k \equiv a \bmod q} \log p$$

Then using the second orthogonality relation, we can express this in terms of $\psi(x,\chi) = \sum_p \sum_{k\geq 1} \chi(p) \log p$:

$$\begin{aligned} \psi(x;a,q) &= \frac{1}{\phi(q)} \sum_{\chi \bmod q} \chi(a)^{-1} \psi(x,\chi) \\ &= \frac{1}{\phi(q)} \psi(x,\chi_o) + \frac{1}{\phi(q)} \sum_{\chi\neq\chi_o} \chi(a)^{-1}\psi(x,\chi) \end{aligned}$$

The trivial character's contribution to this sum is

$$\psi(x,\chi_o) = \frac{1}{\phi(q)}(\psi(x) + O(1)) \sim \frac{x}{\phi(q)}$$

by the Prime Number Theorem. To prove Dirichlet's Theorem, we need to show that the oscillatory sums $\psi(x,\chi)$ arising from nontrivial characters give lower order terms. This will establish that

$$\psi(x;a,q) \sim \frac{x}{\phi(q)}$$

and we thus get Dirichlet's theorem, with the extra information that every admissible progression to the fixed modulus q contains asymptotically the same number of primes.

Assuming RH for $L(s,\chi)$ for all characters modulo q gives that in fact $\psi(x)-x$ and each $\psi(x,\chi)$ for $\chi\neq\chi_o$ is not much bigger than square root of x. This shows that the number of primes $p\equiv a \bmod q$ of size $\leq x$ is $\mathrm{Li}(x)/\phi(q)$ (q fixed, $x\to\infty$) up to an error of size about square root of the main term.

Remark The above argument shows that there are infinitely many primes in the progression $p\equiv a \bmod q$ provided we know that $\psi(x)-x$ and each $\psi(x,\chi)$ for $\chi\neq\chi_o$ is of lower order than x, or that there are no zeros with $\mathrm{Re}(\rho)=1$. This is something of an overkill and is not the path that Dirichlet took. What he did was to argue that it suffices to show that there is never a zero at the point $s=1$, and he then gave proof for this fact. His reduction to the non-vanishing of $L(1,\chi)$ is to argue that the sum of reciprocals of the primes in this progression diverges (so there are certainly infinitely many of them!):

$$\sum_{p\equiv a \bmod q}\frac{1}{p}=\infty$$

By the orthogonality relation,

$$\sum_{p\equiv a \bmod q}\frac{1}{p}=\frac{1}{\phi(q)}\sum_{p}\frac{1}{p}+\frac{1}{\phi(q)}\sum_{\chi\neq\chi_o}\chi(a)^{-1}\sum_{p}\frac{\chi(p)}{p}$$

One uses Euler's argument that $\sum_p 1/p=\infty$, and then notices that by the Euler product for $L(s,\chi)$,

$$\log L(1,\chi)=\sum_{p}\frac{\chi(p)}{p}+O(1)$$

Since $L(s,\chi)$ is analytic at $s=1$ for $\chi\neq\chi_o$, if we know in addition that $L(1,\chi)\neq 0$ then $\sum_p\chi(p)/p$ is finite and so the sum $\sum_{p\equiv a \bmod q}1/p$ diverges with $\sum_p 1/p$.

4 Automorphic L-functions

Riemann's ζ-function and Dirichlet L-functions all belong to a wide class of number theoretic objects known as *automorphic L-functions*. It is outside the scope of these notes to give a general definition of these; instead, I will present two examples: The L-functions attached to the modular discriminant and those attached to eigenfunctions of the Laplacian on the modular domain.

4.1 The modular discriminant

The modular discriminant can be defined through the infinite product

$$\Delta(z):=q\prod_{n=1}^{\infty}(1-q^n)^{24},\quad q=e^{2\pi iz}$$

Table 2 The Ramanujan tau-function.

n	1	2	3	4	5	6	7
$\tau(n)$	1	-24	252	-1472	4830	-6048	-16744

where $z = x + iy$ has positive imaginary part $y = \mathrm{Im} z > 0$, so that $|q| < 1$. The infinite product can be expanded in a power series in q:

$$\Delta(z) = q + \tau(2)q^2 + \ldots + \tau(n)q^n + \ldots$$

for suitable integers $\tau(n)$. The first few are displayed in Table 2.

Using the coefficients $\tau(n)$, we form a Dirichlet series

$$L(s, \Delta) = \sum_{n=1}^{\infty} \frac{\tau^*(n)}{n^s}$$

where $\tau^*(n)$ are the normalized coefficients

$$\tau^*(n) := \frac{\tau(n)}{n^{11/2}}$$

This series is absolutely convergent for $\mathrm{Re}(s) > 1$, and has an analytic continuation to the entire complex plane. It satisfies the following functional equation: The completed L-function

$$L^*(s, \Delta) := \Gamma_{\mathbf{C}}(s + \frac{11}{2})L(s, \Delta), \qquad \Gamma_{\mathbf{C}}(s) := (2\pi)^{-s}\Gamma(s)$$

is entire and satisfies

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

Remark As a function of z, the modular discriminant has the fundamental transformation rule [23]

$$\Delta(-\frac{1}{z}) = z^{12}\Delta(z)$$

The analytic continuation and functional equation of $L(s, \Delta)$ follow from this rule and the integral representation

$$L^*(s, \Delta) = \int_0^{\infty} \Delta(iy)y^{s+11/2}\frac{dy}{y}$$

The coefficients $\tau(n)$ have many interesting properties. For instance, they have the multiplicativity property: for m, n co-prime,

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

while for p prime,

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

These relations were conjectured by Ramanujan, and proved by Mordell in the 1940's. As a consequence of the multiplicativity of $\tau(n)$, there is an Euler product expansion:

$$L(s,\Delta) = \prod_p \frac{1}{1-\tau^*(p)p^{-s}+p^{-2s}}$$

An important feature of $\tau(n)$ is that there is an asymptotic behavior of their mean square (Rankin and Selberg [22]):

$$\sum_{n\leq X} \tau^*(n)^2 \sim cX, \qquad X\to\infty, \qquad c>0 \tag{4.1}$$

As for the size of $\tau(n)$, it is dictated (via the multiplicative relations) by their size at prime arguments. Ramanujan conjectured that

$$|\tau(p)| \leq 2p^{11/2} \tag{4.2}$$

which was proved by Deligne in the 1970's [4], [5].

The sign of the coefficients $\tau(p)$ is conjectured to be distributed according to the "Sato–Tate law": The sequence $\{\tau^*(p)/2\}$ (p prime) is equidistributed in the interval $[-1,1]$ with respect to the semi-circle distribution

$$d\mu(x) = \frac{2}{\pi}\sqrt{1-x^2}dx$$

This was discovered numerically in the 1960's but is as yet not proven.

It will be convenient to write $\tau^*(p)$ as $\tau^*(p) = \operatorname{tr} U_p$ – the trace of a 2×2 matrix $U_p = \begin{pmatrix} \alpha_p & 0 \\ 0 & \alpha_p^{-1}\end{pmatrix}$. Then the Ramanujan conjecture 4.2 is equivalent to the matrix U_p being unitary, and the Sato–Tate law is equivalent to the equidistribution of the conjugacy classes $\{U_p\}$ in the special unitary group SU(2) with respect to Haar measure.

The L-function $L(s,\Delta)$ has "trivial" zeros, due to the poles of the Gamma factor $\Gamma_{\mathbf{C}}(s+\frac{11}{2}) := (2\pi)^{-(s+11/2)}\Gamma(s+\frac{11}{2})$, at $s+11/2 = 0,-1,-2,\dots$. The nontrivial zeros $\rho_n = 1/2+iE_n$ are known to be located inside the critical strip $0<\operatorname{Re}(s)<1$ and it is conjectured that they all lie on the critical line $\operatorname{Re}(s)=1/2$. This is the "Riemann Hypothesis" for $L(s,\Delta)$. Their density inside the critical strip is *twice* that of the Riemann ζ-function:

$$N(T) := \#\{\rho_n : 0<\operatorname{Im}(\rho_n)<T\} \sim 2\cdot\frac{T}{2\pi}\log\frac{T}{2\pi}, \qquad T\to\infty \tag{4.3}$$

The analogue of the Explicit formula (Theorem 2.5) is

$$\sum h(E_n) = \frac{1}{2\pi}\int_{-\infty}^{\infty} h(r)\, 2\operatorname{Re}\frac{\Gamma_{\mathbf{C}}'}{\Gamma_{\mathbf{C}}}(\frac{11}{2}+\frac{1}{2}+ir)dr - 2\sum_p\sum_k \frac{\log p}{p^{k/2}}\operatorname{tr}(U_p^k)\, g(k\log p) \tag{4.4}$$

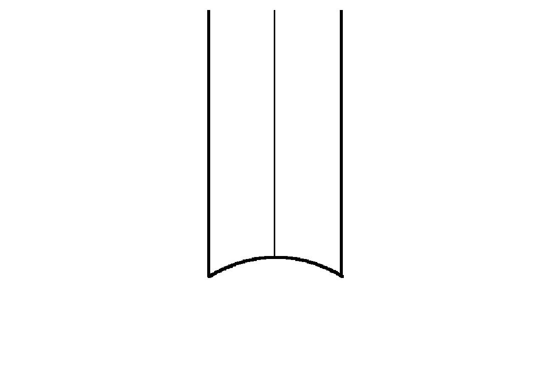

FIG. 1. The fundamental domain $\mathcal{F}$ for the modular group

4.2 Maass waveforms

Our second example of automorphic L-functions are those attached to "Maass waveforms". We begin with a brief survey of the spectral theory of the modular surface. For more details, see H. Iwaniec's book [10].

The upper half plane model $\mathbf{H}$ of the pseudo-sphere is the set of complex numbers $z = x + iy$ with positive imaginary part $y > 0$. The metric on $\mathbf{H}$ given by the line element $ds^2 = (dx^2 + dy^2)/y^2$ has constant negative curvature $K = -1$. Geodesics are circles/lines in $\mathbf{H}$ which are orthogonal to the real axis. The orientation-preserving isometries of the metric are the linear fractional maps $z \mapsto (az + b)/(cz + d)$ with $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ a real 2×2 matrix of determinant 1. The volume element of the metric is given by $dxdy/y^2$. The Laplace–Beltrami operator associated to the metric is $\Delta = y^2(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2})$.

The modular group $\Gamma = SL(2, \mathbf{Z})$ is the group of all such matrices with a, b, c, d integers. The modular surface $\Gamma \backslash \mathbf{H}$ is the Riemann surface obtained by identifying points of $\mathbf{H}$ which are translates of each other by elements of Γ. A fundamental domain for Γ is given by the set (Figure 1)

$$\mathcal{F} = \{z = x + iy \in \mathbf{H} : |z| \geq 1, \frac{1}{2} < \mathrm{Re}(z) \leq \frac{1}{2}\}$$

Every point of $\mathbf{H}$ is a translate of some point in $\mathcal{F}$ by an element of Γ, and no two distinct points of the interior of $\mathcal{F}$ are translates of each other. The volume of the fundamental domain (with respect to the invariant measure $dxdy/y^2$) is $\pi/3$. The fundamental domain admits a symmetry $T_{-1} : z \mapsto -\bar{z}$, which is an orientation reversing reflection in the imaginary axis $\mathrm{Im}(z) = 0$. The volume of the desymmetrized fundamental domain is $\pi/6$.

The spectrum of Δ on the space of odd functions on $\Gamma\backslash\mathbf{H}$ is purely discrete, but on the even space there is continuous spectrum (the continuous spectrum is the interval $[1/4,\infty)$), and, what is less obvious, also discrete spectrum. *Maass waveforms*[1] are nonconstant Γ-periodic eigenfunctions of the Laplacian Δ, which are square-integrable on $\mathcal{F}$:

$$\begin{aligned} \psi(\gamma z) = \psi(z), &\qquad \gamma \in \Gamma, z \in \mathbf{H} \\ \Delta\psi + E\psi = 0, &\qquad E = \frac{1}{4} + t^2 > 0 \\ ||\psi||^2 := \int_{\mathcal{F}} |\psi(z)|^2 \frac{dxdy}{y^2} < \infty \end{aligned}$$

The space of such forms splits up into odd/even forms under the symmetry $z \mapsto -\bar{z}$:

$$\psi(-\bar{z}) = \pm\psi(z)$$

It is known that the discrete spectrum of the modular group is embedded in the continuous spectrum, so that the eigenvalues satisfy $E = 1/4 + t^2 > 1/4$.

Since the translations $z \mapsto z+1$ are in the modular group, an odd/even Maass form $\psi(z)$ has a Fourier expansion $\psi(z) = \sum_n W_n(y)e^{2\pi i n x}$. Taking into account the eigenfunction condition $\Delta\psi + (1/4 + t^2)\psi = 0$ and the square-integrability implies a more explicit form of this expansion:

$$\psi(z) = \sum_{n\neq 0} a_\psi(n) y^{1/2} K_{it}(2\pi|n|y)e^{2\pi i n x}$$

where $K_{it}(y)$ are modified Bessel functions; as $y \to \infty$, $K_{it}(y) \ll e^{-2\pi y}$. The coefficients $a_\psi(n)$ are the *Fourier coefficients* of $\psi(z)$. For even forms, $a_\psi(-n) = a_\psi(n)$, while for odd ones $a_\psi(-n) = -a_\psi(n)$.

There are additional symmetries to the space of functions on the modular domain – the *Hecke operators*. These are defined for $n > 0$ as

$$T_n\psi(z) := \frac{1}{\sqrt{n}} \sum_{\substack{ad = n \\ b \bmod d}} \psi(\frac{az+b}{d})$$

the sum going over all positive integers a, d with $ad = n$, and b with $0 \leq b < d$. The Hecke operators $\{T_n\}$ are a commutative family of Hermitian operators on $L^2(\Gamma\backslash\mathbf{H})$, which in addition commute with the Laplacian and with the reflection symmetry $T_{-1} : z \mapsto -\bar{z}$. They thus preserve the even/odd eigenspaces of Δ, and each eigenspace has a basis consisting of simultaneous eigenfunctions of all the Hecke operators. Such eigenfunctions are called even/odd Maass–Hecke eigenforms. Give such an eigenfunction ψ, with $T_n\psi = \lambda(n)\psi$, its Fourier

[1] named after H. Maass.

coefficients are given by

$$a_\psi(n) = a_\psi(1)\lambda(n), \qquad n > 0$$

Thus we can normalize the first Fourier coefficient $a_\psi(1) = 1$, and then the n-th coefficient is the Hecke eigenvalue $\lambda(n)$ (recall that for negative n, $a_\psi(n) = \pm a_\psi(|n|)$ according to the form ψ being even/odd).

The Hecke eigenvalues are multiplicative:

$$\begin{aligned} \lambda(mn) &= \lambda(m)\lambda(n), \qquad m, n \text{ co-prime} \\ \lambda(p^k)\lambda(p) &= \lambda(p^{k+1}) + \lambda(p^{k-1}), \qquad p \text{ prime} \end{aligned}$$

¿From the boundedness of ψ in the fundamental domain, one can infer that for any Maass form, $a_\psi(n) \ll n^{1/2}$. For Hecke eigenforms, it is conjectured that the Fourier coefficients are essentially bounded, more precisely that for prime p, $|\lambda(p)| \le 2$, and consequently $|\lambda(n)| \ll n^\epsilon$ for any $\epsilon > 0$. This is the "Ramanujan conjecture" for Maass forms, and is still open. The best result to-date in this direction is $|\lambda(p)| \le 2p^{5/28}$ [2]. As for the modular discriminant, one knows that in the mean-square, the Fourier coefficients are bounded:

$$\sum_{n \le X} |a_\psi(n)|^2 \sim c_\psi X, \qquad X \to \infty, \qquad c_\psi = \frac{||\psi||^2}{\pi/3}$$

Furthermore, it is believed that the signs of $\lambda(p)/\sqrt{p}$ are distributed according to the Sato–Tate law.

The L-function attached to a normalized Maass–Hecke eigenform ψ with Fourier coefficients $a(n) = \lambda(n)$, $a(1) = 1$, is defined by

$$L(s, \psi) = \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s}$$

The series is absolutely convergent for $\mathrm{Re}(s) > 1$. Due to the multiplicativity of the Hecke eigenvalues $\lambda(n)$, we have an Euler product expansion

$$L(s, \psi) = \prod_p \frac{1}{1 - \lambda(p)p^{-s} + p^{-2s}}, \qquad \mathrm{Re}(s) > 1$$

The L-function has an analytic continuation and functional equation similar to that of the modular discriminant. For simplicity, we describe only the case of *even* forms. In this case, if $E = 1/4 + t^2$ is the Laplace eigenvalue of ψ, then the completed L-function

$$L^*(s, \psi) := \Gamma_{\mathbf{R}}(s + it)\Gamma_{\mathbf{R}}(s - it)L(s, \psi)$$

is analytic in the entire complex plane, and the functional equation is simply

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

There are trivial zeros of $L(s,\psi)$ at $s = \pm it + k$, $k = 0, -1, -2, \ldots$. It is known that for the modular group all the Laplace eigenvalues lie above $1/4$, so t is real and so there are no trivial zeros in the interior of the critical strip. All nontrivial zeros $\rho_n = 1/2 + iE_n$ lie inside the critical strip $0 < \mathrm{Re}(s) < 1$, and the analogue of the Riemann Hypothesis is that they all lie on the critical line $\mathrm{Re}(s) = 1/2$. As for the modular discriminant, the density of the zeros in the critical strip is twice that of the Riemann ζ-function (eqn 4.3), and there is an Explicit Formula similar to eqn 4.4.

5 Spectral statistics of the zeros

We start with a sequence of numbers $x_1 \le x_2 \le \ldots \le x_n \le \ldots$, normalized so that $x_n \sim n$ as $n \to \infty$. The goal is to understand the fluctuations of the levels x_n from their mean. For instance, the nearest-neighbor level spacings are $s_n := x_{n+1} - x_n$, whose mean is unity. The level spacing distribution $P(s)$ measures the distribution of the spacings s_n:

$$P(s) = \lim_{N\to\infty} \frac{1}{N} \sum_{n \le N} \delta(s - s_n)$$

that is we want that for any test function $f \in C_c(0,\infty)$,

$$\frac{1}{N} \sum_{n\le N} f(s_n) \to \int_0^\infty f(s)P(s)ds, \qquad \text{as } N \to \infty$$

Our example of such a sequence of levels is to take the zeros $\rho_n = 1/2 + iE_n$ of one of the L-functions described in the previous sections, with the imaginary parts E_n (here we assume the relevant RH) lying in an interval $[E, 2E]$, $E \gg 1$. The number of "levels" E_n in this interval is asymptotic to $Ed \log E/2\pi$ as $E \to \infty$, where $d = 1$ in the case of $\zeta(s)$ and Dirichlet L-functions, and $d = 2$ for the L-functions attached to the modular discriminant or Maass wave-forms. Thus setting

$$x_n := \frac{d \log E}{2\pi} E_n$$

we get a sequence of normalized levels $x_n \sim n$ (this process is sometime referred to as "unfolding" the levels).

One model for such a sequence is to take the x_n as random (uncorrelated) numbers. In this case the level spacing distribution is $P_{\mathrm{rand}}(s) = e^{-s}$. Other models, more relevant for our purpose, are the ones arising in Random Matrix Theory [14]. For instance, we can take the eigenvalues $\lambda_1 \le \lambda_2 \le \ldots \le \lambda_N$ of an $N \times N$ hermitian matrix H chosen from the Gaussian Unitary Ensemble, that is the implied probability measure is $d\mu(H) = c_N e^{-\mathrm{tr}(H^2)} dH$. The expected level spacing distribution of the unfolded eigenvalues $x_n := \frac{\sqrt{2N}}{\pi}\lambda_n$ is given as $N \to \infty$ in terms of a Fredholm determinant:

$$P_{\mathrm{GUE}}(s) = \frac{d^2}{ds^2} \det(I - Q_s)$$

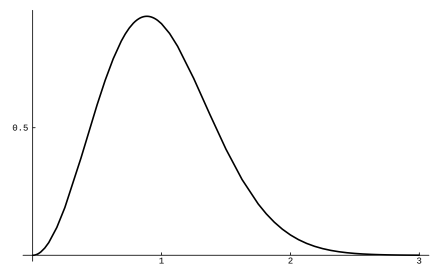

FIG. 2. The GUE level spacing distribution $P_{\mathrm{GUE}}(s)$.

where Q_s is the operator on $L^2(-1,1)$ given by the kernel

$$Q_s(x,y) = \frac{\sin \pi(x-y)s/2}{\pi(x-y)}$$

For small s, $P_{\mathrm{GUE}}(s) \sim \frac{\pi^2}{3}s^2$ (see Figure 2).

The same level spacing distribution arises if we take the eigenphases of an $N \times N$ unitary matrix, chosen at random with respect to Haar measure on the unitary group $\mathrm{U}(N)$ – this is Dyson's Circular Unitary Ensemble. Similarly if we take any of the families of compact classical groups, such as the unitary symplectic group $\mathrm{USp}(2N)$. In these compact examples it was proved by Katz and Sarnak [11] that it is not only the ensemble averages that converge to $P_{\mathrm{GUE}}(s)$ but this in fact holds for almost all matrices.

It is usually difficult to directly study the level spacing distribution. Instead of studying spacing between adjacent levels, one looks at correlations between all n-tuples of levels – these are the n-level correlation functions [14]. These determine all local statistics such as the level spacing distribution. For instance, the pair correlation function ($n=2$) of the unfolded sequence $\{x_n\}$ is defined as

$$R_2(f,N) = \frac{1}{N} \sum_{j \neq k \leq N} f(x_j - x_k)$$

for an even test function f. We want to study the limit as $N \to \infty$, expecting a

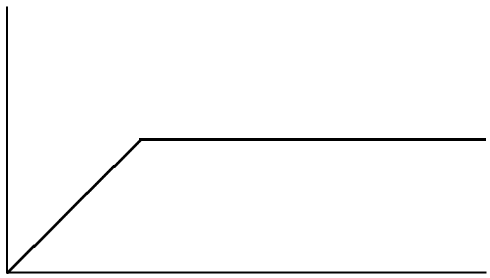

FIG. 3. $K_{\mathrm{GUE}}(\tau)$.

limiting behavior

$$R_2(f,N) \to \int_{-\infty}^{\infty} f(x)R_2(x)dx$$

For uncorrelated levels, we clearly have $R_2^{\mathrm{rand}}(x) = 1$. For the GUE case, F. Dyson [6] found that $R_2^{\mathrm{GUE}}(x) = 1 - (\sin \pi x/\pi x)^2$, that is in terms of the Fourier transform of f,

$$\frac{1}{N} \sum_{j,k \le N} f(x_j - x_k) \to \hat{f}(0) + \int_{-\infty}^{\infty} \hat{f}(\tau) K_{\mathrm{GUE}}(\tau) d\tau$$

where the "form-factor" $K_{\mathrm{GUE}}(\tau)$ is given by (Figure 3)

$$K_{\mathrm{GUE}}(\tau) = \begin{cases} |\tau| & |\tau| < 1 \\ 1 & |\tau| \ge 1 \end{cases}$$

In the early 1970's, H. Montgomery studied the clustering properties of the zeros of $\zeta(s)$ in connection with the class-number problem for quadratic fields [15]. He found that the pair correlation function of the zeros is given by $R_2^{\mathrm{GUE}}(x)$ at least for test functions whose Fourier transform is supported in the interval $(-1, 1)$. Once the connection with Random Matrix Theory was made, it was conjectured that the level spacing distribution of the zeros of $\zeta(s)$ are indeed those of GUE. This has been tested numerically by A. Odlyzko [16], [17], who found excellent agreement with the GUE predictions. The n-level correlation functions were also found to be in agreement with GUE for suitable restricted test functions, by Hejhal [9] for $n = 3$ and by Rudnick and Sarnak [20] for all n.

In the same manner, one can study the spectral statistics of the zeros of any of the L-functions described above. Indeed, it was shown by Rudnick and Sarnak [21] that the n-level correlation functions for the zeros of L-functions for any cuspidal automorphic form, such as the modular discriminant or a Maass wave-form, agree with GUE at least for a restricted class of test-functions. Thus we believe that the spectral statistics of the zeros of any of these L-functions are those of GUE. For the modular discriminant, this was also tested numerically – see [13], [19]. In the next section, I will sketch a derivation of the pair correlation function of one of these L-functions.

6 Computing the pair correlation function of the zeros

We consider the zeros $\rho_n = 1/2 + iE_n$ with E_n lying in a window such as $[E, 2E]$, and for these zeros we set

$$x_n = \frac{d\log E}{2\pi} E_n$$

to be the "unfolded" levels, where $d = 1$ for $\zeta(s)$ or Dirichlet L-functions, and $d = 2$ in the case of the modular discriminant or Maass wave-forms. Thus the mean spacing of the sequence x_n is unity as $E \to \infty$.

We need to compute the limit as $E \to \infty$ of the quantity

$$R_2(f, E) = \frac{1}{n(E)} \sum_{j \neq k} w_E(x_j) w_E(x_k) f(x_j - x_k)$$

where f is a suitable even function, the sum is over all pairs of zeros, $w_E(x)$ is a "window function" which picks out the ones in our window $[E, 2E]$, and $n(E)$ is the number of zeros in the window.

It is technically convenient to express this in the smoothed form

$$R_2(f, E) = \frac{1}{E d \log E / 2\pi} \sum_{j \neq k} h(\frac{E_j}{E}) h(\frac{E_k}{E}) f(\frac{d\log E}{2\pi}(E_j - E_k))$$

where we choose as the window function $w_E(x_n) := h(E_n/E)$, with $h(r) = \int_{-\infty}^{\infty} g(u) e^{iru} dr$ the Fourier transform of a compactly supported, even function $g(u)$. We will further choose f to be even and such that its Fourier transform $\hat{f}$ is compactly supported.

If we add in the contribution $f(0)$ of the diagonal terms $j = k$, this becomes

$$R_2(f, E) \sim -f(0) + \frac{2\pi}{E d\log E} \int_{-\infty}^{\infty} \left| \sum_n h(\frac{E_n}{E}) e^{i\tau d \log E \cdot E_n} \right|^2 \hat{f}(\tau) d\tau \qquad (6.1)$$

Next we use the Explicit Formula with the test function

$$h_{E,\tau}(r) := h(\frac{r}{E}) e^{i\tau d \log E \cdot r}$$

to express the sum over zeros as a sum over prime powers. For definiteness we concentrate on the case of a Maass wave-form ψ with Laplace eigenvalue $1/4 + t^2$, which is a normalized Hecke eigen-form. The explicit formula than gives

$$\sum_n h(\frac{E_n}{E}) e^{i\tau d \log E \cdot E_n} =$$

$$\frac{1}{2\pi}\int_{-\infty}^{\infty} h_{E,\tau}(r)\left(\frac{\Gamma'_{\mathbf{R}}}{\Gamma_{\mathbf{R}}}(\frac{1}{2}+it+ir)+\frac{\Gamma'_{\mathbf{R}}}{\Gamma_{\mathbf{R}}}(\frac{1}{2}-it+ir)\right)dr$$
$$-\sum_{p,k} A_{p,k}E\left(g(E(\tau d\log E+\log p^k))+g(E(\tau d\log E-\log p^k))\right)$$

where

$$A_{p,k}=\frac{\log p}{p^{k/2}}\operatorname{tr}U_p^k$$

and the Fourier coefficients of the Maass wave-form ψ are given by $\lambda(p)=\operatorname{tr}U_p$ for p prime. Substituting into eqn 6.1, one gets an expression for $R_2(f,E)$ as a sum of several terms, the important one being the one coming from the sums over primes in the explicit formula, namely

$$K(f,E)= \tag{6.2}$$
$$\sum_{p,k}\sum_{q,l}A_{p,k}A_{q,l}\int_{-\infty}^{\infty}E^2g(E(\tau d\log E\pm\log p^k))g(E(\tau d\log E\pm\log q^l))\hat{f}(\tau)d\tau$$

and the sum is over all 4 possible choices of signs $\pm\log p^k$, $\pm\log q^l$ (this is called the "semi-classical form-factor" in the Quantum Chaos literature).

In order to recover the GUE result, we need to show that as $E\to\infty$,

$$\frac{K(f,E)}{dE\log E/2\pi}\to\kappa(h)\int_{-\infty}^{\infty}K_{\mathrm{GUE}}(\tau)\hat{f}(\tau)d\tau$$

where $\kappa(h)\sim 1$ when we let h_E approximate a sharp window function for the interval $[E,2E]$, and the "form-factor" for GUE is given by

$$K_{\mathrm{GUE}}(\tau)=\begin{cases}|\tau| & |\tau|<1\\ 1 & |\tau|\geq 1\end{cases}$$

(Figure 3).

The double sum in eqn 6.2 is over pairs of prime powers p^k, q^l satisfying

$$|\tau d\log E\pm\log p^k|,\qquad |\tau d\log E\pm\log q^l|\ll\frac{1}{E}$$

for τ in the support of $\hat{f}$ (since g is of compact support). This forces $\log p^k,\log q^l\sim|\tau|d\log E$. Further, g forces the sign of $\log p^k$ and of $\log q^l$ to be equal: It is $-$ if $\tau>0$ and $+$ if $\tau<0$. After changing variables $u=E(\tau d\log E-\log p^k)$ and approximating $\hat{f}(\tau)\sim\hat{f}(\frac{\log p^k}{d\log E})$, we obtain

$$K(f,E)\sim 2\frac{E}{d\log E}\sum_{p,k}\sum_{q,l}A_{p,k}A_{q,l}\hat{f}(\frac{\log p^k}{d\log E})g^{*2}(E(\log p^k-\log q^l))$$

where $g^{*2}(x)$ is the convolution

$$g^{*2}(x) := \int_{-\infty}^{\infty} g(u)g(x-u)du$$

We express $K(f,E)$ as a sum of two terms $K_{\rm diag}(f,E)$ and $K_{\rm off}(f,E)$, where $K_{\rm diag}(f,E)$ is the contribution of the diagonal terms $p^k = q^l$:

$$K_{\rm diag}(f,E) = 2\frac{E}{d\log E}\sum_{p,k} A_{p,k}^2 \cdot \hat{f}(\frac{\log p^k}{d\log E}) \cdot \int_{-\infty}^{\infty} g(u)^2 du \tag{6.3}$$

The diagonal contribution: To evaluate the diagonal contribution, we use

$$\sum_{p^k \le x} A_{p,k}^2 \sim \frac{1}{2}(\log x)^2$$

In the case $d=1$ this is a consequence of the Prime Number Theorem, while in the case $d=2$ it follows from "Rankin–Selberg theory" [22], [21]. Thus replacing $A_{p,k}^2$ in eqn 6.3 by its mean value (summation by parts) we find

$$\sum_{p,k} A_{p,k}^2 \hat{f}(\frac{\log p^k}{d\log E}) \sim \int_1^{\infty} \hat{f}(\frac{\log t}{d\log E}) d(\frac{1}{2}\log^2 t) = (d\log E)^2 \int_0^{\infty} \hat{f}(\tau)\tau d\tau$$

If we further use $\int_{-\infty}^{\infty} g(u)^2 du = \frac{1}{2\pi}\int_{-\infty}^{\infty} h(r)^2 dr$, we then find

$$\frac{K_{\rm diag}(f,E)}{Ed\log E/2\pi} \to \kappa(h)\int_{-\infty}^{\infty} \hat{f}(\tau)|\tau| d\tau$$

with $\kappa(h) = \int_{-\infty}^{\infty} h(r)^2 dr$.

Eliminating the off-diagonal terms: Suppose now that $\hat{f}$ is supported in the interval $[-1/d+\delta, 1/d-\delta] \subset (-1/d, 1/d)$, for some $\delta > 0$. Recall that $d=1$ for $\zeta(s)$ and Dirichlet L-functions, $d=2$ for L-functions attached to Maass wave-forms or the modular discriminant. We claim then that the off-diagonal term

$$K_{\rm off}(f,E) = \frac{E}{(d\log E)^2}\sum_{p^k \ne q^l} A_{p,k}A_{q,l}\hat{f}(\frac{\log p^k}{d\log E}) g^{*2}(E(\log p^k - \log q^l))$$

vanishes because all summands are identically zero. This is because in order that a term appear in this sum, we need both $|\log p^k - \log q^l| \ll 1/E$ as well as $\log p^k/d\log E < (1-\delta)/d$. Since both p^k and q^l are integers these two condition cannot be simultaneously satisfied for $E \gg 1$. Thus for $\hat{f}$ supported inside $(-1/d, 1/d)$ We find that

$$K(f,E) \sim K_{\rm diag}(f,E) \sim E\frac{d\log E}{2\pi}\kappa(h) \cdot \int_{-\infty}^{\infty} \hat{f}(\tau) K_{\rm GUE}(\tau) d\tau$$

Remark: The restriction $\mathrm{Supp}(\hat{f}) \subset (-1/d, 1/d)$ is made to ensure that the off-diagonal terms are trivially zero. In the case $d = 1$, the GUE form-factor $K_{\mathrm{GUE}}(\tau)$ changes its behavior right at the edge of this region (figure 3). In the range $|\tau| > 1$, $K_{\mathrm{diag}} \neq K_{\mathrm{GUE}}$ and we need to understand the contribution of the off-diagonal terms, which are of the same size as the diagonal ones. This involves understanding some aspect of the "twin-prime conjectures", which are beyond our reach at present (see [12] for a discussion and heuristics). In the case $d = 2$, the region $1/2 < |\tau| < 1$ is where we still expect the diagonal terms to dominate, but at present this too is beyond our reach.

Bibliography

1. M.V. Berry *Riemann's zeta function: A model for Quantum Chaos?* in *Quantum Chaos and Statistical Nuclear Physics*, Lecture Notes in Physics **263**, eds. T.H. Seligman and H. Nishioka, Springer-Verlag, Berlin (1986), 1–17.
2. D. Bump, W. Duke, J. Hoffstein and H. Iwaniec *An estimate for the Hecke eigenvalues of Maass forms*, Inter. Math. Res. Notices **4** (1992), 75–81.
3. H. Davenport *Multiplicative Number Theory*, second edition, Springer-Verlag 1980.
4. P. Deligne *Formes modulaires et représentations ℓ-adiques*, Séminaire Bourbaki 355 (1968/69), Lecture Notes in Mathematics **179**, Springer-Verlag, Berlin (1971), 139–172.
5. P. Deligne *La conjecture de Weil I*, Publ. Math. I.H.E.S. **43** (1974), 273–307.
6. F.J. Dyson *Statistical Theory of the Energy Levels of Complex Systems*, III, J. Math. Phys. **3** (1962), 166–175.
7. H.M. Edwards *Riemann's Zeta Function*, Academic Press 1974.
8. D.A. Hejhal *The Selberg Trace Formula and the Riemann Zeta Function*, Duke Jour. of Math. **43** (1976), 441–482.
9. D.A. Hejhal *On the Triple Correlation of Zeros of the Zeta Function*, Inter. Math. Res. Notices **7** (1994), 293–302.
10. H. Iwaniec *Introduction to the Spectral Theory of Automorphic Forms*, Bibl. Rev. Mat. Iberoamericana, Madrid 1995.
11. N. Katz and P. Sarnak *The Spacing Distributions Between Zeros of Zeta Functions*, manuscript, 1996.
12. J. Keating *The Riemann Zeta-Function and Quantum Chaology*, in: Proceedings of the Int. School of Physics *"Enrico Fermi"*, Course CXIX, eds: G. Casati, I. Guarneri and U. Smilansky, North-Holland (1993), 145–185.
13. J. B. Keiper *On the zeros of the Ramanujan τ-Dirichlet series in the critical strip*, Math. Comp. **65** (1996), 1613–1619.
14. M.L. Mehta *Random Matrices*, Second Edition, Academic Press 1991.
15. H.L. Montgomery *The Pair Correlation of Zeros of the Zeta Function*, Proc. Symp. Pure Math. **24**, 181–193, American Math. Soc., Providence 1973.

16. A.M. Odlyzko *On the Distribution of Spacings Between Zeros of Zeta Functions*, Math. of Comp. **48** (1987), 273–308.
17. A.M. Odlyzko *The* 10^{20} *Zero of the Riemann Zeta Function and* 70 *Million of its neighbors*, A.T. & T. preprint, 1989.
18. B. Riemann *Über die Anzahl der Primzahlen unter einer gegebenen Größe*, Montasb. der Berliner Akad. (1858/60) 671–680, in *Gessamelte Mathematische Werke* 2nd edition, Teubner, Leipzig 1982 no. VII.
19. M. Rubinstein, Ph.D. Thesis, Princeton 1997.
20. Z. Rudnick and P. Sarnak *The n-level correlations of zeros of the zeta function*, C.R. Acad. Sci. Paris **319** Série I (1994), 1027–1032 .
21. Z. Rudnick and P. Sarnak *Zeros of principal L-functions and random matrix theory*, Duke Jour. of Math. **81** (1996), 269–322.
22. A. Selberg *On the estimation of Fourier coefficients of modular forms*, Proc. Symp. Pure Math. **8**, Amer. Math. Soc., Providence (1965), 1–15.
23. J.-P. Serre *A Course in Arithmetic*, Springer Graduate Texts in Mathematics **7**, Springer-Verlag, New York 1973.