Introduction to Random Matrix Theory for Analytic Number Theory

Paul-Olivier Dehaye
Merton College, University of Oxford

Rencontre GDR Géométrie non commutative
Aspet, July 4th 2008

Outline

I will try to present some ideas, theorems and conjectures from Random Matrix Theory as applied to Analytic Number Theory.

- General idea
- Position of zeroes (pair correlation)
- Modeling
  - Other statistics on position of zeroes
  - Moments (values)
- Remark on RMT computations

Pólya-Hilbert original idea

Find a self-adjoint operator H such that its set of eigenvalues $\{\gamma_i\} \subset \mathbb{C}$ corresponds to (nontrivial) zeroes of the Riemann zeta function:

$$\zeta\left(\frac{1}{2} + \mathrm{i}\gamma_i\right) = 0$$

The spectral theorem then corresponds to the Riemann Hypothesis.

The same concept would apply to a host of zeta functions, essentially covering the Generalized Riemann Hypothesis.

We started here with a self-adjoint operator. In general H could be taken to lie in a set S of operators, all satisfying some symmetry condition.

A step further

If we forget about the arithmetic origin, what properties distinguish H from others in the set S?

Inspired by statistical physics, we gamble that some properties of the eigenvalues of H are actually true accross S.

By averaging over S, we are then able to recover conjectural information about eigenvalues of H (=zeroes of ζ) by looking at eigenvalues of objects in S.

Which operators?

In order to compute the various relevant statistics, we need a set of operators, all satisfying some symmetry condition, and a measure on the set (se we can average).

We obtain this set and measure as limit of sets of matrices. There are two approaches to defining a set. To illustrate:

- $N \times N$ hermitian matrices
  - with entries filled using Gaussian distributions
  - with unique measure such that entries are independent and invariant under unitary conjugation
- $\mathrm{U}(N)$, with Haar measure

In the limit for N, the first gives the GUE, the second the CUE. There are many more (GOE, GSpE, $\mathrm{SO}(2N)$, $\mathrm{SO}(2N+1)$, $\mathrm{USp}(2N)$, $\cdots$) .

Montgomery-Odlyzko conjecture

Riemann: The density of zeroes is asymptotic to $\frac{\log T}{2\pi}$.

Conjecture ("Pair correlation"):

$$\lim_{T\to\infty} \frac{1}{N(T)} \sum_{\substack{\zeta(1/2+i\gamma)=0 \\ 0\le\gamma,\gamma'\le T \\ \frac{2\pi\alpha}{\log T}\le\gamma-\gamma'\le\frac{2\pi\beta}{\log T}}} 1 \quad = \quad \int_\alpha^\beta 1 - \left(\frac{\sin(\pi x)}{\pi x}\right)^2 \mathrm{d}x$$

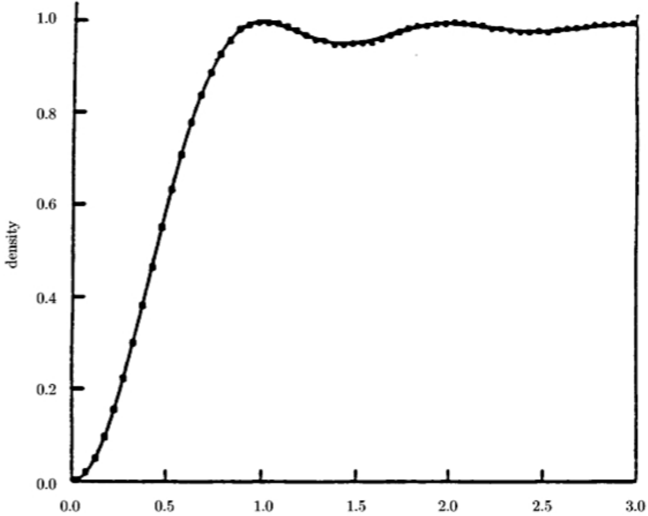

Figure: Pair correlation based on 8×10^6 zeroes near the 10^{20}th, vs. the function $1 - \left(\frac{\sin(\pi x)}{\pi x}\right)^2$.

Theorem (Montgomery): On RH, the maps

$$f \to \lim_{T\to\infty} \frac{2\pi}{T\log T} \sum_{0\le\gamma,\gamma'\le T} f\left(\tilde{\gamma} - \tilde{\gamma}'\right)$$

with $\tilde{\gamma} = \frac{1}{2\pi}\gamma\log(\gamma)$, and

$$f \to \int_0^\infty f(x) W_\zeta(x) \mathrm{d}x$$

with $W_\zeta(x) = 1 - \left(\frac{\sin(\pi x)}{\pi x}\right)^2$, are equal for functions with Fourier transform supported on the interval $[-1,1]$.

Dyson's remark

GUE

$$\lim_{N\to\infty} \frac{1}{N} \left\langle \sum_{\substack{\alpha,\alpha' \\ \text{eigenvalues}}} f(\tilde{\alpha} - \tilde{\alpha}') \right\rangle_{GUE(N)} = \int_0^\infty f(x) W_{GUE}(x) \mathrm{d}x$$

CUE/U(N)

$$\lim_{N\to\infty} \frac{1}{N} \int_{\mathrm{U}(N)} \sum_{\substack{e^{\mathrm{i}\theta}, e^{\mathrm{i}\theta'} \\ \text{e.v. of } U}} f\left(\frac{N}{2\pi}(\theta - \theta')\right) \mathrm{d}U = \int_0^\infty f(x) W_{\mathrm{U}}(x) \mathrm{d}x$$

$$\text{with } W_\zeta(x) = W_{\mathrm{U}}(x) = W_{GUE}(x) = 1 - \left(\frac{\sin(\pi x)}{\pi x}\right)^2$$

Dyson remarked to Montgomery that all those kernels are the same.

Rudnick-Sarnak

Rudnick and Sarnak extended this to functions of n pairwise differences (n-correlation) of the renormalized γ_is and again showed they behaved as eigenvalues from GUE or large unitary matrices.

They still have a restriction on the support of the Fourier transform of their test functions, but don't assume RH.

They then extended this to all arithmetic L-functions (of elliptic curves, algebraic varieties, Dirichlet characters, Galois representations, etc).

In some sense, these kernels for n-correlation are universal to all arithmetic L-functions and statistics of random matrices. We need other statistics to distinguish between the different cases.

Katz-Sarnak

Katz and Sarnak then looked at L-functions over function fields, i.e. L-functions constructed counting solutions over $\mathbb{F}_{q^n}$ for fixed q and $n \in \mathbb{N}_0$. In that setting, they have full and precise theorems that lead to conjectures and partial results for the number field case.

Modeling with families

The main idea in modeling L-functions is to use families, i.e. merely a set of L-functions indexed by a parameter called generally the conductor.

A family is modeled by associating to it a classical compact matrix group (in the case of fn fields, this is proved).The size of the matrices (N) scales with the conductor.

To leading order, the rescaled local zero statistics (n-correlation, n-level, nearest neighbor,...) are the same as the rescaled local eigenvalue statistics of the group. To leading order, the critical moments of the family equals the critical moments of the characteristic polynomials, up to a multiplicative arithmetic constant.

For the family we average over the L-functions with conductor less than X and then let $X \to \infty$. For the matrix groups the averages are taken with respect to Haar measure and we let $N \to \infty$.

Families

Some approximate examples of families:

- $\{L(E,\chi_d) : d \text{ discriminants}\}$: quadratic twists of L-functions of elliptic curves, indexed by d
- $\{L(E,s)\}$: elliptic curve L-functions, indexed by
  - conductor of the curve
  - size of the coefficients in the Weiertstrass equation of the curve (in various ways)
- $\{L(s,\chi) : \chi \text{ Dirichlet characters}\}$: Dirichlet L-functions, indexed by conductors of χ
- $\{L(f,s)\}$: f modular form of fixed weight k, indexed by level N
- ...
- $\left\{\zeta\Big((1/2+\mathrm{i}t_0)+\mathrm{i}t\Big)\right\}$, with $0 \le t_0 \le T$, indexed by T
- $\left\{L\Big((\sigma_0+\mathrm{i}t_0)+\mathrm{i}t\Big)\right\}$, with $0 \le t_0 \le T$, indexed by T

Statistics (to be renormalized)

- pair correlation:

$$f \rightarrow \lim_{T\to\infty} \frac{2\pi}{T\log T} \sum_{0\le\gamma,\gamma'\le T} f\left(\tilde{\gamma}-\tilde{\gamma}'\right)$$

- n^{th}-correlation: Take f such that $f(x_1,\cdots,x_n)=f(x_1+r,\cdots,x_n+r)$,

$$f \rightarrow \sum_{\{i_1,\cdots,i_n\}\subset\mathbb{N}} f\left(\tilde{\gamma}_{i_1},\cdots,\tilde{\gamma}_{i_n}\right)$$

- k^{th}-nearest neighbour: $f \rightarrow \sum_i f(\tilde{\gamma}_{i+k}-\tilde{\gamma}_i)$
- n-level statistics:

$$f \rightarrow \sum_{\{i_1,\cdots,i_n\}\subset\mathbb{N}} f\left(\tilde{\gamma}_{i_1},\cdots,\tilde{\gamma}_{i_n}\right)$$

- ...

Values of ζ on the critical line

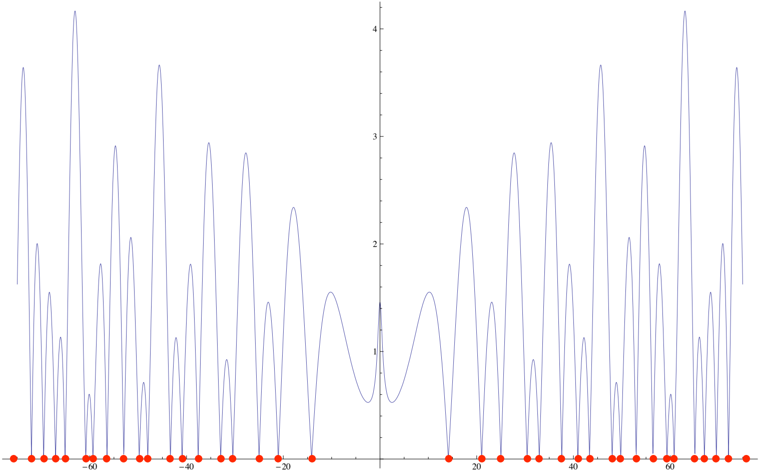

Figure: Graph of $|\zeta(1/2+\imath t)|$ for $t \in [-75, 75]$.

Keating-Snaith

Keating and Snaith suggested (and backed) that this should all be pushed further:

- Eigenvalues of random matrices model zeroes of zeta functions
- Zeroes of characteristic polynomials of random matrices model zeroes of zeta functions
- Characteristic polynomials of random matrices model zeta functions

For NCGters:
"There is information in the matrices beyond their spectrum"

This will show in two ways:

- Value at the critical point
- Moments

Values of ζ on the critical line

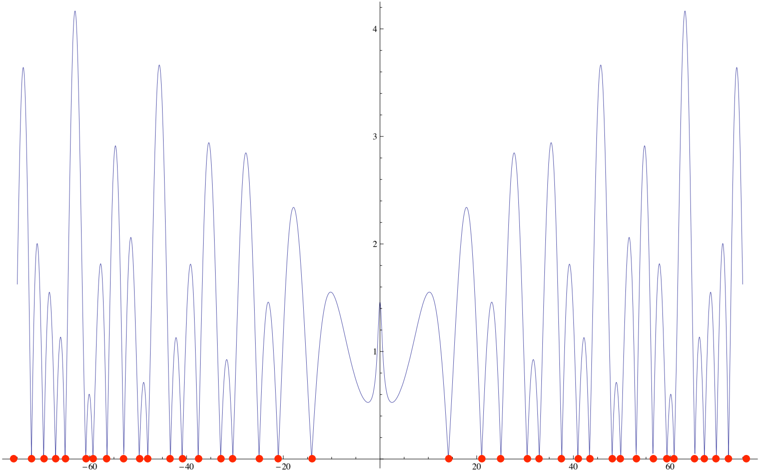

Figure: Graph of $|\zeta(1/2 + \mathrm{i}t)|$ for $t \in [-75, 75]$.

Moments

Theorem ($k = 1$: Hardy-Littlewood, $k = 2$: Ingham):

$$\lim_{T\to\infty} \frac{1}{T(\log T)^{k^2}} \int_0^T |\zeta(1/2 + \mathrm{i}t)|^{2k} \mathrm{d}t = f(k)a(k),$$

where $a(k)$ is a known product over primes, $f(1) = 1$, $f(2) = 1/12$.

Can we at least conjecture the other values for f?

Conrey and Gosh: $f(3) = 42/9!$
Conrey and Gonek: $f(4) = 24024/16!$

Keating and Snaith: $f(k) = \lim_{N\to\infty} \frac{1}{N^{k^2}} \int_{\mathrm{U}(N)} |\Lambda_U(1)|^{2k} \mathrm{d}U$, where

$$\int_{\mathrm{U}(N)} |\Lambda_U|^s \mathrm{d}U = \prod_{j=1}^{N} \frac{\Gamma(j)\Gamma(j+s)}{(\Gamma(j+s/2))^2}.$$

"The ζ-function is (conjecturally) modeled in leading order by averages over characteristic polynomials".

Modeling with families

The main idea in modeling L-functions is to use families, i.e. merely a set of L-functions indexed by a parameter called generally the conductor.

A family is modeled by associating to it a classical compact matrix group (in the case of fn fields, this is proved). The size of the matrices (N) scales with the conductor.

To leading order, the rescaled local zero statistics (n-correlation, n-level, nearest neighbor,...) are the same as the rescaled local eigenvalue statistics of the group. To leading order, the critical moments of the family equals the critical moments of the characteristic polynomials, up to a multiplicative arithmetic constant.

For the family we average over the L-functions with conductor less than X and then let $X \to \infty$. For the matrix groups the averages are taken with respect to Haar measure and we let $N \to \infty$.

“To leading order”

All the results or conjectures presented here give results at the leading order. Unfortunately, the leading order dominates only for extremely high $\log T$. Therefore, in order to test the conjectures numerically, it is best to include lower order terms as well.

Fortunately, a set of recipes to apply to explicit Dirichlet series has been developed in order to extract these lower order terms, and that allows to deal with the (subtle) arithmetic interaction (CFKRS).

Examples:

- For the moments, terms of lower order than $(\log T)^{k^2}$
- For the pair correlation, there are dips in the kernel that disappear for $T \to \infty$.

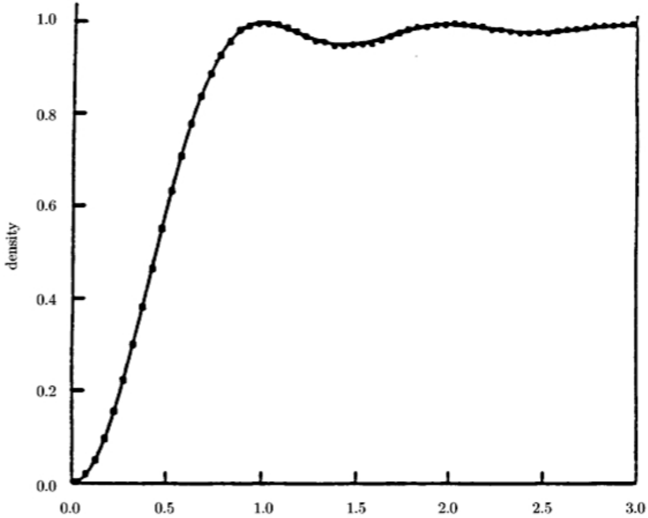

Figure: Pair correlation based on 8×10^6 zeroes near the 10^{20}th, vs. the function $1 - \left(\frac{\sin(\pi x)}{\pi x}\right)^2$.

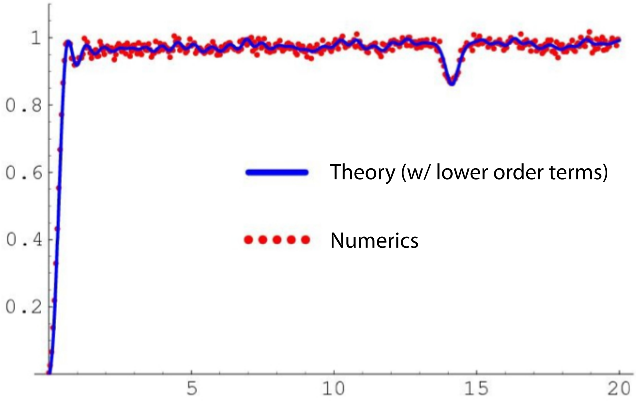

Figure: The same pair correlation for $\zeta(s)$, but based on 100000 zeroes and $T = 75000$ (image N.C. Snaith illustrating Bogomolny-Keating).

RMT methods (for moments)

$$\begin{aligned} a(k)f(k) &= \lim_{T\to\infty} \frac{1}{T(\log T)^{k^2}} \int_0^T |\zeta(1/2+\mathrm{i}t)|^{2k}\mathrm{d}t \\ f(k) &= \lim_{N\to\infty} \frac{1}{N^{k^2}} \int_{\mathrm{U}(N)} |\Lambda_U(1)|^{2k}\mathrm{d}U \end{aligned}$$

In general, the results in Random Matrix Theory are obtained by computing quantities at $k \in \mathbb{N}$, and then extending those to $k \in \mathbb{C}$ via Carlson's Theorem (uniqueness of analytic functions of low exponential type with given value at integers).

Some of these RMT statistics are relatively easy to compute, some are hard. So far, we only have a good handle on moments for multiplicative functions of eigenvalues. For instance, we can do $\prod_j \frac{\left|\Lambda\left(e^{\mathrm{i}\alpha_j}\right)\right|}{\left|\Lambda\left(e^{\mathrm{i}\beta_j}\right)\right|}$, but not really $|\Lambda'(1)|$.