L-functions and Random Matrix Theory

Chantal David
Concordia University
Montréal

MSRI, January 2011

Riemann Zeta function

The Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p} \left(1 - p^{-s}\right)^{-1}, \quad \mathrm{Re}(s) > 1$$

has meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1$.

Riemann Zeta function

The Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p} \left(1 - p^{-s}\right)^{-1}, \quad \mathrm{Re}(s) > 1$$

has meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1$. It satisfies the functional equation

$$\Lambda(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s) = \Lambda(1 - s),$$

where

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

Zeroes of $\zeta(s)$

The Prime Number Theorem

$$\pi(x) = \#\{p \leq x\} \sim \frac{x}{\log x} \sim \mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$$

can be reduced to the statement that $\zeta(s) \neq 0$ for $\mathrm{Re}(s) = 1$.

Zeroes of $\zeta(s)$

The Prime Number Theorem

$$\pi(x) = \#\{p \leq x\} \sim \frac{x}{\log x} \sim \mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$$

can be reduced to the statement that $\zeta(s) \neq 0$ for $\mathrm{Re}(s) = 1$. More explicitely,

$$\pi(x) = \mathrm{Li}(x) + O\left(x \exp(-\sqrt{\log x})\right)$$

corresponds to the zero-free region $\sigma \geq 1 - c/\log t$ for $s = \sigma + it$.

Zeroes of $\zeta(s)$

The Prime Number Theorem

$$\pi(x) = \#\{p \le x\} \sim \frac{x}{\log x} \sim \mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$$

can be reduced to the statement that $\zeta(s) \neq 0$ for $\mathrm{Re}(s) = 1$. More explicitely,

$$\pi(x) = \mathrm{Li}(x) + O\left(x \exp(-\sqrt{\log x})\right)$$

corresponds to the zero-free region $\sigma \ge 1 - c/\log t$ for $s = \sigma + it$. The Riemann Hypothesis states that for $0 < \mathrm{Re}(s) < 1$, $\zeta(s) = 0$ implies that $\mathrm{Re}(s) = 1/2$. It is equivalent to

$$\pi(x) = \mathrm{Li}(x) + O\left(x^{1/2} \log x\right).$$

Number of zeroes in the critical strip

The Riemann-Von Mangoldt formula states that

$$\begin{aligned} N(T) &= \{\rho = \sigma + i\gamma \; : \; \zeta(\rho) = 0, \; 0 \le \sigma \le 1, \; 0 < \gamma < T\} \\ &= \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T) \sim \frac{T \log T}{2\pi}. \end{aligned}$$

Number of zeroes in the critical strip

The Riemann-Von Mangoldt formula states that

$$\begin{aligned} N(T) &= \{\rho = \sigma + i\gamma \ : \ \zeta(\rho) = 0, \ 0 \le \sigma \le 1, \ 0 < \gamma < T\} \\ &= \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T) \sim \frac{T \log T}{2\pi}. \end{aligned}$$

The first few zeroes are:
$\rho_1 = 1/2 + 14.134725i$, $\rho_2 = 1/2 + 21.022040i$,
$\rho_3 = 1/2 + 25.010858i$, $\rho_2 = 1/2 + 21.022040i$,
$\rho_5 = 1/2 + 32.935062i$, $\rho_6 = 1/2 + 37.586178i$.

Distribution of the zeroes in the critical strip

How are the (imaginary parts of the) zeroes distributed? For example, do they look like $T \log T/2\pi$ random points on an interval of length T?

Distribution of the zeroes in the critical strip

How are the (imaginary parts of the) zeroes distributed? For example, do they look like $T \log T/2\pi$ random points on an interval of length T?

How many zeroes $\rho = \sigma + i\gamma$ are such that are such that

$$\frac{2\pi\alpha}{\log T} < \gamma_1 - \gamma_2 < \frac{2\pi\beta}{\log T} \iff \alpha < \frac{\gamma_1 \log T}{2\pi} - \frac{\gamma_2 \log T}{2\pi} < \beta?$$

We have normalised the zeroes such that there are now $\sim T$ zeroes on an interval of length T.

Conjecture (Montgomery's Pair Correlation conjecture, 1974)

$$\frac{1}{T} \sum_{\substack{0<\hat{\gamma}_1,\hat{\gamma}_2\leq T \\ \alpha<\hat{\gamma}_1-\hat{\gamma}_2<\beta}} 1 \sim \int_{\alpha}^{\beta} 1 - \left(\frac{\sin \pi u}{\pi u}\right)^2 \, du$$

Conjecture (Montgomery's Pair Correlation conjecture, 1974)

$$\frac{1}{T} \sum_{\substack{0<\hat{\gamma}_1,\hat{\gamma}_2 \leq T \\ \alpha<\hat{\gamma}_1-\hat{\gamma}_2<\beta}} 1 \sim \int_{\alpha}^{\beta} 1 - \left(\frac{\sin \pi u}{\pi u} \right)^2 du$$

Theorem (Montgomery, 1974)

Let ϕ be a test function such that the support of the Fourier transform $\hat{\phi}(u)$ is contained in $(-1, 1)$. Then

$$\frac{1}{T} \sum_{0<\hat{\gamma}_1,\hat{\gamma}_2 \leq T} \phi(\hat{\gamma}_1 - \hat{\gamma}_2) \sim \int_{-\infty}^{\infty} \phi(u) \left(1 - \left(\frac{\sin \pi u}{\pi u} \right)^2 \right) du$$

Conjecture (Montgomery's Pair Correlation conjecture, 1974)

$$\frac{1}{T} \sum_{\substack{0<\hat{\gamma}_1,\hat{\gamma}_2\leq T \\ \alpha<\hat{\gamma}_1-\hat{\gamma}_2<\beta}} 1 \sim \int_{\alpha}^{\beta} 1 - \left(\frac{\sin \pi u}{\pi u}\right)^2 du$$

Theorem (Montgomery, 1974)

Let ϕ be a test function such that the support of the Fourier transform $\hat{\phi}(u)$ is contained in $(-1,1)$. Then

$$\frac{1}{T} \sum_{0<\hat{\gamma}_1,\hat{\gamma}_2\leq T} \phi(\hat{\gamma}_1 - \hat{\gamma}_2) \sim \int_{-\infty}^{\infty} \phi(u) \left(1 - \left(\frac{\sin \pi u}{\pi u}\right)^2\right) du$$

Dyson noticed that this gives the pair correlation between eigenvalues of large random unitary matrices.

Random Unitary Matrices

Let $U(N)$ be the set of $N \times N$ unitary matrices in $M_N(\mathbb{C})$, i.e.

$$A^* A = A\,A^* = I_N.$$

Random Unitary Matrices

Let $U(N)$ be the set of $N \times N$ unitary matrices in $M_N(\mathbb{C})$, i.e.

$$A^* A = A\, A^* = I_N.$$

Let $A \in U(N)$, and let $\lambda_k(A) = e^{i\theta_k(A)}$ be the eigenvalues, with $0 \le \theta_1(A) \le \theta_2(A) \cdots \le \theta_N(A) \le 2\pi$.

Random Unitary Matrices

Let $U(N)$ be the set of $N \times N$ unitary matrices in $M_N(\mathbb{C})$, i.e.

$$A^* A = A\,A^* = I_N.$$

Let $A \in U(N)$, and let $\lambda_k(A) = e^{i\theta_k(A)}$ be the eigenvalues, with $0 \le \theta_1(A) \le \theta_2(A) \cdots \le \theta_N(A) \le 2\pi$. Let

$$R(A)[\alpha, \beta] = \frac{1}{N} \# \left\{ j \neq k \; : \; \alpha \le \frac{N}{2\pi}(\theta_j - \theta_k) \le \beta \right\}.$$

Again, we have normalised the eigenangles in such a way that there are N angles on an interval of length N.

Random Unitary Matrices

Let

$$R(A)[\alpha, \beta] = \frac{1}{N} \# \left\{ j \neq k \ : \ \alpha \leq \frac{N}{2\pi}(\theta_j - \theta_k) \leq \beta \right\}.$$

Random Unitary Matrices

Let

$$R(A)[\alpha,\beta] = \frac{1}{N}\#\left\{ j \neq k \ : \ \alpha \leq \frac{N}{2\pi}(\theta_j - \theta_k) \leq \beta \right\}.$$

Then, with the appropriate measure on $U(N)$ (which is the translation invariant Haar measure)

$$\lim_{N\to\infty} \int_{U(N)} R(A)[\alpha,\beta]\, dA = \int_\alpha^\beta 1 - \left(\frac{sin\pi u}{\pi u}\right)^2 \, du.$$

GUE Conjecture

- Montgomery's Pair Correlation conjecture does not mean that the zeroes are distributed as the eigenvalues of large Hermitian matrix, but that the pair correlations are the same for the two sets.

GUE Conjecture

- Montgomery's Pair Correlation conjecture does not mean that the zeroes are distributed as the eigenvalues of large Hermitian matrix, but that the pair correlations are the same for the two sets.
- But Montgomery, and others, went on to conjecture that perhaps all the statistics, not just the pair correlation statistic, would match up for zeta-zeros and eigenvalues of random matrices. This conjecture is called the GUE conjecture.

GUE Conjecture

- Montgomery's Pair Correlation conjecture does not mean that the zeroes are distributed as the eigenvalues of large Hermitian matrix, but that the pair correlations are the same for the two sets.
- But Montgomery, and others, went on to conjecture that perhaps all the statistics, not just the pair correlation statistic, would match up for zeta-zeros and eigenvalues of random matrices. This conjecture is called the GUE conjecture.
- In the 1980s, Odlyzko began an intensive numerical study of the statistics of the zeros of $\zeta(s)$. He computed millions of zeros at heights around 10^{20} and spectacularly confirmed the GUE conjecture, which is also called the Montgomery-Odlyzko law.

The work of Katz and Sarnak

- For zeta functions of curves over finite fields, the zeroes are the reciprocal of eigenvalues of Frobenius acting on the first cohomology (with ℓ-adic coefficients) of the curve. This additional structure is used for example by Deligne in his proof of the Riemann Hypothesis for zeta functions of varieties over finite fields.

The work of Katz and Sarnak

- For zeta functions of curves over finite fields, the zeroes are the reciprocal of eigenvalues of Frobenius acting on the first cohomology (with ℓ-adic coefficients) of the curve. This additional structure is used for example by Deligne in his proof of the Riemann Hypothesis for zeta functions of varieties over finite fields.
- Katz and Sarnak used this spectral interpretation, and the equidistribution results due to Deligne, to prove that for the zeta functions of curves over finite fields satisfy the Montgomery-Odlyzko law (i.e. their pair-correlation is the pair correlation of random unitary matrices) when g and q tend to infinity (i.e. their result holds averaging over curves of genus g at the limit when q and g tends to infinity).

Deligne Equidistribution Theorem

Theorem (Deligne's Equidistribution Theorem)

Let $\mathcal{M}_g(\mathbb{F}_q)$ be the moduli space of curves of genus g over $\mathbb{F}_q$ (i.e. the set of $\mathbb{F}_q$-isomorphism classes of curves of genus g over $\mathbb{F}_q$). Let f be any continuous class function on $USp(2g)$. Then

$$\lim_{q\to\infty} \frac{\sum'_{C\in\mathcal{H}_g(\mathbb{F}_q)} f(\Theta_C)}{\sum'_{C\in\mathcal{H}_g(\mathbb{F}_q)} 1} = \int_{USp(2g)} f(A)dA.$$

where $\sum'$ means that each term is counted with the weights $1/\#Aut(C/\mathbb{F}_q)$.

Katz and Sarnak

The k-th consecutive spacings measure $\mu_k(A)$ on $U(N)$ is

$$\mu_k(A)[\alpha,\beta] = \frac{\#\left\{1 \leq j \leq N \ : \ \frac{N}{2\pi}(\theta_{j+k} - \theta_k) \in [\alpha,\beta]\right\}}{N}$$

Katz and Sarnak

The k-th consecutive spacings measure $\mu_k(A)$ on $U(N)$ is

$$\mu_k(A)[\alpha, \beta] = \frac{\#\left\{1 \leq j \leq N \ : \ \frac{N}{2\pi}(\theta_{j+k} - \theta_k) \in [\alpha, \beta]\right\}}{N}$$

Then, Katz and Sarnak showed that

$$\lim_{N \to \infty} \int_{U(N)} \mu_k(A)\, dA = \mu_k(\text{GUE}).$$

Katz and Sarnak

The k-th consecutive spacings measure $\mu_k(A)$ on $U(N)$ is

$$\mu_k(A)[\alpha, \beta] = \frac{\#\left\{1 \le j \le N \ : \ \frac{N}{2\pi}(\theta_{j+k} - \theta_k) \in [\alpha, \beta]\right\}}{N}$$

Then, Katz and Sarnak showed that

$$\lim_{N \to \infty} \int_{U(N)} \mu_k(A)\, dA = \mu_k(\mathrm{GUE}).$$

Moreover, let $\mu_k(C/\mathbb{F}_q)$ be the k-th consecutive spacings measure between the zeroes

$$\gamma_j = e^{i\theta_j}/\sqrt{q}, \quad j = 1, \ldots, 2g$$

of the zeta function of $C/\mathbb{F}_q$ ordered by size of θ_j.

Katz and Sarnak

Let the Kolmogoroff-Smirnov discrepancy between two measures μ and ν be

$$\mathrm{discrep}(\mu, \nu) = \sup \{ |\mu(I) - \nu(I)| \ : \ I \subseteq \mathbb{R} \} .$$

Theorem (Katz and Sarnak)

$$\lim_{g \to \infty} \lim_{q \to \infty} \frac{1}{|\mathcal{M}_g(\mathbb{F}_q)|} \sum_{C \in \mathcal{M}_g(\mathbb{F}_q)} \mathrm{discrep}(\mu_k(C/\mathbb{F}_q), \mu_k(GUE)) = 0.$$

Characteristic polynomials of random matrices

zeroes of $\zeta(s)$ $\quad\leftrightarrow\quad$ eigenvalues of $A \in U(N)$

Characteristic polynomials of random matrices

$$\begin{aligned} \text{zeroes of } \zeta(s) &\quad\leftrightarrow\quad \text{eigenvalues of } A \in U(N) \\ \zeta(s) &\quad\leftrightarrow\quad \text{characteristic polynomial of } A \in U(N) \end{aligned}$$

Characteristic polynomials of random matrices

$$\begin{aligned} \text{zeroes of } \zeta(s) &\leftrightarrow \text{eigenvalues of } A \in U(N) \\ \zeta(s) &\leftrightarrow \text{characteristic polynomial of } A \in U(N) \end{aligned}$$

Let

$$P_A(\lambda) = \det(\lambda I - A) = \prod_{k=1}^{N} \left(\lambda - e^{i\theta_k(A)}\right)$$

where $\theta_1, \ldots, \theta_k$ are the eigenvalues of A.

Moments of $\zeta(s)$

Let

$$M_k(T) = \frac{1}{T} \int_0^T |\zeta(1/2 + it)|^{2k} \; dt.$$

We know that

Moments of $\zeta(s)$

Let

$$M_k(T) = \frac{1}{T}\int_0^T |\zeta(1/2+it)|^{2k}\ dt.$$

We know that

$$M_1(T) \quad \sim \quad \log T \quad \text{(Hardy and Littlewood, 1918)}$$

Moments of $\zeta(s)$

Let

$$M_k(T) = \frac{1}{T}\int_0^T |\zeta(1/2+it)|^{2k}\ dt.$$

We know that

$$\begin{aligned} M_1(T) &\sim \log T \quad \text{(Hardy and Littlewood, 1918)} \\ M_2(T) &\sim \frac{1}{2\pi^2}\log^4 T \quad \text{(Ingham, 1926)} \end{aligned}$$

Moments of $\zeta(s)$

Let

$$M_k(T) = \frac{1}{T}\int_0^T |\zeta(1/2+it)|^{2k}\ dt.$$

We know that

$$\begin{aligned} M_1(T) &\sim \log T \quad \text{(Hardy and Littlewood, 1918)} \\ M_2(T) &\sim \frac{1}{2\pi^2}\log^4 T \quad \text{(Ingham, 1926)} \end{aligned}$$

and it is conjectured that for any integer k

$$M_k(T) \sim c_k \log^{k^2} T.$$

Moments of $\zeta(s)$

It is conjectured that

$$M_k(T) \sim c_k \log^{k^2} T = \frac{g_k a_k}{\Gamma(1+k^2)} \log^{k^2} T.$$

where the arithmetic factor a_k is given by

$$a_k = \prod_p \left(1 - \frac{1}{p}\right)^{k^2} \sum_{j=0}^{\infty} \frac{d_k(p^j)^2}{p^j}.$$

Moments of $\zeta(s)$

It is conjectured that

$$M_k(T) \sim c_k \log^{k^2} T = \frac{g_k a_k}{\Gamma(1+k^2)} \log^{k^2} T.$$

where the arithmetic factor a_k is given by

$$a_k = \prod_p \left(1 - \frac{1}{p}\right)^{k^2} \sum_{j=0}^{\infty} \frac{d_k(p^j)^2}{p^j}.$$

We have that $g_1 = 1$ (Hardy and Littlewood, 1918), $g_2 = 2$ (Ingham, 1926) and it was conjectured that $g_3 = 42$ (Conrey and Ghosh, 1984) and $g_4 = 24024$ (Conrey and Gonek, 1998).

Moments of $\zeta(s)$

Conjecture (Keating and Snaith, 2000)

$$M_k(T) \sim c_k \log^{k^2} T = \frac{g_k a_k}{\Gamma(1+k^2)}$$

where the geometric factor g_k *is given by*

$$g_k = \prod_{j=0}^{k-1} \frac{j!}{(j+k)!}.$$

Moments of $\zeta(s)$

Conjecture (Keating and Snaith, 2000)

$$M_k(T) \sim c_k \log^{k^2} T = \frac{g_k a_k}{\Gamma(1+k^2)}$$

where the geometric factor g_k is given by

$$g_k = \prod_{j=0}^{k-1} \frac{j!}{(j+k)!}.$$

This comes from computing the moments of $P_A(\lambda)$.

Moments of characteristic polynomials of random matrices

Theorem (Keating and Snaith, 2000)

For any λ *such that* $|\lambda| = 1$, *and for any complex number* k,

$$M_k(N) = \int_{U(N)} |P_A(\lambda)|^{2k} \, dA = \prod_{j=1}^{N} \frac{\Gamma(j)\Gamma(j+2k)}{\Gamma(j+k)^2}.$$

Moments of characteristic polynomials of random matrices

Theorem (Keating and Snaith, 2000)

For any λ such that $|\lambda| = 1$, and for any complex number k,

$$M_k(N) = \int_{U(N)} |P_A(\lambda)|^{2k} \, dA = \prod_{j=1}^{N} \frac{\Gamma(j)\Gamma(j+2k)}{\Gamma(j+k)^2}.$$

Furthermore, when k is an integer

$$\lim_{N\to\infty} \frac{M_k(N)}{N^{k^2}} = \frac{G(1+k)^2}{G(1+2k)} = \prod_{j=0}^{k-1} \frac{j!}{(j+k)!},$$

where $G(k)$ is Barnes' double Gamma-function satisfying $G(1) = 1$ and $G(z+1) = \Gamma(z)G(z)$.

Further work

- One can compute more statistics on the zeroes of $\zeta(s)$ and check that they match the statistics for eigenvalues of random matrices;

Further work

• One can compute more statistics on the zeroes of $\zeta(s)$ and check that they match the statistics for eigenvalues of random matrices;

• An interesting statistics is the distribution of low-lying zeroes, which leads to the Density Conjecture of Katz and Sarnak;

Further work

- One can compute more statistics on the zeroes of $\zeta(s)$ and check that they match the statistics for eigenvalues of random matrices;
- An interesting statistics is the distribution of low-lying zeroes, which leads to the Density Conjecture of Katz and Sarnak;
- One can consider more general L-functions and compare their statistics with statistics of random matrices, maybe for other groups as $O(N)$ or $\mathrm{Sp}(N)$;

Further work

- One can compute more statistics on the zeroes of $\zeta(s)$ and check that they match the statistics for eigenvalues of random matrices;
- An interesting statistics is the distribution of low-lying zeroes, which leads to the Density Conjecture of Katz and Sarnak;
- One can consider more general L-functions and compare their statistics with statistics of random matrices, maybe for other groups as $O(N)$ or $\mathrm{Sp}(N)$;
- One consider L-functions in families, and consider statistics when the L-functions vary in the family (inspired by the work of Katz and Sarnak).

Families of L-functions

Moments of $\zeta(1/2 + it) \leftrightarrow$ average over $t \in \mathbb{R}$

Families of L-functions

Moments of $\zeta(1/2+it)$ $\leftrightarrow$ average over $t \in \mathbb{R}$
Moments of $L(1/2, f)$ $\leftrightarrow$ average over $f \in \mathcal{F}$

Families of L-functions

Moments of $\zeta(1/2 + it)$ $\leftrightarrow$ average over $t \in \mathbb{R}$
Moments of $L(1/2, f)$ $\leftrightarrow$ average over $f \in \mathcal{F}$

If we know the moments of $L(1/2, f)$ as $f \in \mathcal{F}$ varies, we know

- the distribution of the values of $L(1/2, f)$ as $f \in \mathcal{F}$ varies;

Families of L-functions

Moments of $\zeta(1/2 + it) \leftrightarrow$ average over $t \in \mathbb{R}$
Moments of $L(1/2, f) \quad \leftrightarrow$ average over $f \in \mathcal{F}$

If we know the moments of $L(1/2, f)$ as $f \in \mathcal{F}$ varies, we know

- the distribution of the values of $L(1/2, f)$ as $f \in \mathcal{F}$ varies;
- the vanishing of $L(1/2, f)$ as $f \in \mathcal{F}$ varies, using some discretisation coming from the arithmetic.

Families of L-functions

Moments of $\zeta(1/2+it)$ $\leftrightarrow$ average over $t \in \mathbb{R}$
Moments of $L(1/2, f)$ $\leftrightarrow$ average over $f \in \mathcal{F}$

If we know the moments of $L(1/2, f)$ as $f \in \mathcal{F}$ varies, we know

- the distribution of the values of $L(1/2, f)$ as $f \in \mathcal{F}$ varies;
- the vanishing of $L(1/2, f)$ as $f \in \mathcal{F}$ varies, using some discretisation coming from the arithmetic.

Let

$$\mathcal{F}(T) = \{f \in \mathcal{F} \ : \ c(f) \leq T\}$$

where $c(f)$ is the conductor of f.

Families of L-functions

The probability density function for the distribution of the special values $L(1/2, f)$ for $f \in \mathcal{F}(T)$ is given by

$$P(x, T) \quad = \quad \frac{1}{2\pi i} \int_{(c)} M_s(T) x^{-s-1} \, ds$$

where for any $s \in \mathbb{C}$, $M_s(T)$ are the moments

$$M_s(T) = \frac{1}{\#\mathcal{F}(T)} \sum_{c(f) \leq T} |L(1/2, f)|^s \, .$$

Families of L-functions

The probability density function for the distribution of the special values $L(1/2, f)$ for $f \in \mathcal{F}(T)$ is given by

$$P(x, T) \quad = \quad \frac{1}{2\pi i} \int_{(c)} M_s(T) x^{-s-1} \, ds$$

where for any $s \in \mathbb{C}$, $M_s(T)$ are the moments

$$M_s(T) = \frac{1}{\#\mathcal{F}(T)} \sum_{c(f) \leq T} |L(1/2, f)|^s \, .$$

One can use the Random Matrix model to replace the moments $M_s(T)$ by the moments $M_s(N)$ for a group of random matrices. The appropriate scaling is $N = \log c(f)$.

L-functions attached to elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve with conductor N_E and L-function

$$\begin{aligned} L(s,E) &= \sum_{n=1}^{\infty} \frac{a_E(n)}{n^s} \\ &= \prod_{p \nmid N_E} \left(1 - \frac{a_E(p)}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1} \prod_{p \mid N_E} \left(1 - \frac{a_E(p)}{p^s}\right)^{-1} \\ &= \prod_{p \nmid N_E} \left(1 - \frac{\alpha_E(p)}{p^s}\right)^{-1} \left(1 - \frac{\overline{\alpha_E(p)}}{p^s}\right)^{-1} \prod_{p \mid N_E} \left(1 - \frac{a_E(p)}{p^s}\right)^{-1} \end{aligned}$$

where

$$\#E(\mathbb{F}_p) = p + 1 - a_E(p).$$

L-functions attached to elliptic curves

The L-function $L(s, E)$ converges absolutely for $\mathrm{Re}(s) > 2$, and has analytic continuation and functional equation

$$\Lambda(2 - s, E) = (2\pi)^{-s} N_E^{s/2} \Gamma(s) L(s, E) = w(E) \Lambda(2 - s, E),$$

where the sign of the functional equation $w(E)$ can be ± 1.

L-functions attached to elliptic curves

The L-function $L(s, E)$ converges absolutely for $\mathrm{Re}(s) > 2$, and has analytic continuation and functional equation

$$\Lambda(2-s, E) = (2\pi)^{-s} N_E^{s/2} \Gamma(s) L(s, E) = w(E) \Lambda(2-s, E),$$

where the sign of the functional equation $w(E)$ can be ± 1.

Conjecture (Birch and Swinnerton-Dyer)

$$ord_{s=1} L(s, E) = rank(E(\mathbb{Q})) .$$

Family of Quadratic Twists

Let E be the elliptic curve

$$y^2 = x^3 + ax + b.$$

Then the quadratic twist of E^D is the curve

$$Dy^2 = x^3 + ax + b.$$

Family of Quadratic Twists

Let E be the elliptic curve

$$y^2 = x^3 + ax + b.$$

Then the quadratic twist of E^D is the curve

$$Dy^2 = x^3 + ax + b.$$

It is not difficult to see that

$$L(s, E^D) = L(s, E, \chi_D) = \sum_{n=1}^{\infty} \frac{a_E(n)\chi_D(n)}{n^s}$$

where $\chi_D(n)$ is the quadratic character

$$\chi_D(n) = \left(\frac{D}{n}\right).$$

Family of Quadratic Twists

The twisted L-function

$$L(s, E, \chi_D) = \sum_{n \geq 1} \frac{a_E(n)\chi_D(n)}{n^s}$$

has analytic continuation and functional equation

$$\begin{aligned} \Lambda(s, E, \chi_D) &= \left(\frac{D\sqrt{N_E}}{2\pi}\right)^s \Gamma(s) L(s, E, \chi_D) \\ &= w(E, \chi_D)\Lambda(2 - s, E, \chi_D) \end{aligned}$$

where

$$w(E, \chi_D) = w(E)\chi_D(-N_E).$$

Family of Quadratic Twists

When the sign of the functional equation

$$w(E, \chi_D) = w(E)\chi_D(-N_E) = -1,$$

using $s = 1$ in the functional equation

$$\Lambda(s, E, \chi_D) \quad = \quad w(E, \chi_D)\Lambda(2 - s, E, \chi_D),$$

Family of Quadratic Twists

When the sign of the functional equation

$$w(E, \chi_D) = w(E)\chi_D(-N_E) = -1,$$

using $s = 1$ in the functional equation

$$\Lambda(s, E, \chi_D) \quad = \quad w(E, \chi_D)\Lambda(2 - s, E, \chi_D),$$

we have that

$$\Lambda(1, E, \chi_D) = -\Lambda(1, E, \chi_D) \Longrightarrow \Lambda(1, E, \chi_D) = 0 \Longrightarrow L(1, E, \chi_D) = 0.$$

Family of Quadratic Twists

When the sign of the functional equation

$$w(E, \chi_D) = w(E)\chi_D(-N_E) = -1,$$

using $s = 1$ in the functional equation

$$\Lambda(s, E, \chi_D) \quad = \quad w(E, \chi_D)\Lambda(2 - s, E, \chi_D),$$

we have that

$$\Lambda(1, E, \chi_D) = -\Lambda(1, E, \chi_D) \Longrightarrow \Lambda(1, E, \chi_D) = 0 \Longrightarrow L(1, E, \chi_D) = 0.$$

Since $w(E, \chi_D) = w(E)\chi_D(-N_E)$, $w(E, \chi_D) = -1$ for half of the discriminants D.

Conjecture (Goldfeld, 1979)

Let r_D *be the order of vanishing of* $L(s, E, \chi_D)$ *at* $s = 1$*. Then*

$$\lim_{T \to \infty} \frac{1}{\#\{|D| \le T\}} \sum_{|D| \le T} r_D = \frac{1}{2}.$$

Conjecture (Goldfeld, 1979)

Let r_D be the order of vanishing of $L(s,E,\chi_D)$ at $s=1$. Then

$$\lim_{T\to\infty} \frac{1}{\#\{|D|\le T\}} \sum_{|D|\le T} r_D = \frac{1}{2}.$$

Then, if we restrict the family $\mathcal{F}$ to

$$\mathcal{F}^+ = \{L(s,E,\chi_D) \ : \ w(E,\chi_D)=1\},$$

we expect that "most" $L(s,E,\chi_D)$ would not vanish at $s=1$.

Conjecture (Goldfeld, 1979)

Let r_D be the order of vanishing of $L(s, E, \chi_D)$ at $s = 1$. Then

$$\lim_{T\to\infty} \frac{1}{\#\{|D| \le T\}} \sum_{|D|\le T} r_D = \frac{1}{2}.$$

Then, if we restrict the family $\mathcal{F}$ to

$$\mathcal{F}^+ = \{L(s, E, \chi_D) \ : \ w(E, \chi_D) = 1\},$$

we expect that "most" $L(s, E, \chi_D)$ would not vanish at $s = 1$.

Using the Random Matrix Theory model, the distribution of the values of $L(1, E, \chi_D)$ is related to the distribution of the values of $P_A(\lambda)$ where A varies over the set of $2N \times 2N$ orthogonal matrices (symmetry type O^+).

Vanishing of quadratic twists

Conjecture (Conrey, Keating, Rubinstein and Snaith, 2000)

Let $N_E(T)$ *be the number of discriminants* D *with* $|D| \leq T$ *such that* $w(E, \chi_D) = 1$*, and* $L(1, E, \chi_D) = 0$*. Then,*

$$N_E(T) \sim b_E T^{3/4} \log^{e_E} T$$

for some constants b_E *and* e_E *depending on* E*.*

Vanishing of quadratic twists

Conjecture (Conrey, Keating, Rubinstein and Snaith, 2000)

Let $N_E(T)$ be the number of discriminants D with $|D| \leq T$ such that $w(E, \chi_D) = 1$, and $L(1, E, \chi_D) = 0$. Then,

$$N_E(T) \sim b_E T^{3/4} \log^{e_E} T$$

for some constants b_E and e_E depending on E.

Hypothesis: The moments

$$M_k(T) = \frac{1}{\#\mathcal{F}^+(T)} \sum_{\substack{L(s,E,\chi_D) \in \mathcal{F}^+ \\ |D| \leq T}} |L(1, E, \chi_D)|^k$$

behave like the moments of the characteristic polynomials of matrices in $SO(2N)$ where $N \sim \log T$.

Higher Order characters

Let $k \geq 3$ be a prime.
We study vanishing in the family of the twisted L-functions $L(s, E, \chi)$ where χ is a primitive Dirichlet characters of order k. In particular, χ is a multiplicative function

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

such that $\chi(a)^k = 1$ for all $a \in (\mathbb{Z}/q\mathbb{Z})^*$.

Higher Order characters

Let $k \geq 3$ be a prime.
We study vanishing in the family of the twisted L-functions $L(s, E, \chi)$ where χ is a primitive Dirichlet characters of order k. In particular, χ is a multiplicative function

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

such that $\chi(a)^k = 1$ for all $a \in (\mathbb{Z}/q\mathbb{Z})^*$.
Let $\tau(\chi)$ be the Gauss sum

$$\tau(\chi) = \sum_{a \bmod q} \chi(a) e^{2\pi i a/q}.$$

Then, $|\tau(\chi)|^2 = q$.

Higher Order characters

The twisted L-function

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

satisfies the functional equation

$$\begin{aligned} \Lambda(s,E,\chi) &= \left(\frac{q\sqrt{N_E}}{2\pi}\right)^s \Gamma(s)L(s,E,\chi) \\ &= w(E,\chi)\Lambda(2-s,E,\overline{\chi}). \end{aligned}$$

where $w(E,\chi) = \dfrac{w_E\chi(N_E)\tau(\chi)^2}{q}$.

Higher Order characters

The twisted L-function

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

satisfies the functional equation

$$\begin{aligned} \Lambda(s, E, \chi) &= \left(\frac{q\sqrt{N_E}}{2\pi}\right)^s \Gamma(s) L(s, E, \chi) \\ &= w(E, \chi)\Lambda(2 - s, E, \overline{\chi}). \end{aligned}$$

where $w(E, \chi) = \dfrac{w_E \chi(N_E)\tau(\chi)^2}{q}$.
As the functional equation does not relate $L(s, E, \chi)$ to itself, $w(E, \chi) \neq 1$ does not imply that $L(1, E, \chi) = 0$.

Higher Order characters

Let

$$N_{E,k}(T) = \#\{\chi \text{ of order } k,\ \text{cond}(\chi) \leq T,\ L(1, E, \chi) = 0\}.$$

Higher Order characters

Let

$$N_{E,k}(T) = \#\left\{\chi \text{ of order } k,\ \text{cond}(\chi) \leq T,\ L(1, E, \chi) = 0\right\}.$$

The Density Conjecture of Katz and Sarnak predicts that

$$N_{E,k}(T) = \underline{o}\left(\#\left\{\chi \text{ order } k\ :\ \mathrm{cond}(\chi) \leq \mathrm{T}\right\}\right) = \underline{o}(T).$$

Higher Order characters

Let

$$N_{E,k}(T) = \#\left\{\chi \text{ of order } k,\ \text{cond}(\chi) \le T,\ L(1,E,\chi) = 0\right\}.$$

The Density Conjecture of Katz and Sarnak predicts that

$$N_{E,k}(T) = \underline{o}\left(\#\left\{\chi \text{ order } k \ :\ \mathrm{cond}(\chi) \le \mathrm{T}\right\}\right) = \underline{o}(T).$$

If $K/\mathbb{Q}$ is a cyclic extension of degree k and conductor q with Galois group G and character group $\widehat{G}$, then

$$L(s, E/K) = \prod_{\chi \in \widehat{G}} L(s, E, \chi).$$

Then, under the Birch and Swinnerton-Dyer conjecture, $N_{E,k}(T)$ is $(k-1)$ times the number of cyclic extensions $K/\mathbb{Q}$ of degree k and conductor $\le T$ with $\text{rank}(E/K) > \text{rank}(E/\mathbb{Q})$.

Conjectural asymptotics for $N_{E,k}(T)$

Conjecture (David-Fearnley-Kisilevsky, 2006)

- *If $k = 3$, then $N_{E,k}(T) \sim b_E T^{1/2} \log^{e_E} T$ as $T \to \infty$.*

Conjectural asymptotics for $N_{E,k}(T)$

Conjecture (David-Fearnley-Kisilevsky, 2006)

- *If* $k = 3$, *then* $N_{E,k}(T) \sim b_E T^{1/2} \log^{e_E} T$ *as* $T \to \infty$.
- *If* $k = 5$, *then* $N_{E,k}(T)$ *is unbounded, but* $N_{E,k}(T) \ll T^{\epsilon}$ *for any* $\epsilon > 0$ *as* $X \to \infty$.

Conjectural asymptotics for $N_{E,k}(T)$

Conjecture (David-Fearnley-Kisilevsky, 2006)

- *If* $k = 3$, *then* $N_{E,k}(T) \sim b_E T^{1/2} \log^{e_E} T$ *as* $T \to \infty$.
- *If* $k = 5$, *then* $N_{E,k}(T)$ *is unbounded, but* $N_{E,k}(T) \ll T^{\epsilon}$ *for any* $\epsilon > 0$ *as* $X \to \infty$.
- *If* $k \geq 7$, *then* $N_{E,k}(T)$ *is bounded.*

Conjectural asymptotics for $N_{E,k}(T)$

Conjecture (David-Fearnley-Kisilevsky, 2006)

- *If* $k = 3$, *then* $N_{E,k}(T) \sim b_E T^{1/2} \log^{e_E} T$ *as* $T \to \infty$.
- *If* $k = 5$, *then* $N_{E,k}(T)$ *is unbounded, but* $N_{E,k}(T) \ll T^{\epsilon}$ *for any* $\epsilon > 0$ *as* $X \to \infty$.
- *If* $k \geq 7$, *then* $N_{E,k}(T)$ *is bounded.*

Hypothesis: The moments

$$M_k(T) = \frac{1}{\#\mathcal{F}(T)} \sum_{\substack{L(s,E,\chi)\in\mathcal{F} \\ c(\chi)\leq T}} |L(1,E,\chi)|^k$$

behave like the moments of the characteristic polynomials of matrices in $U(N)$ where $N \sim \log T$.