Rank of elliptic curves over number fields

Workshop on Matrix Ensembles and L-Functions, Isaac Newton Institute, July 2004

Chantal David, Concordia University, Montréal

Joint work with J. Fearnley and H. Kisilevsky

Elliptic curves over number fields

Let K be a number field, and let E be an elliptic curve over K.

$$E : y^2 = x^3 + ax + b, \quad a, b \in K.$$

Mordell-Weil Theorem

$E(K) \simeq \mathbb{Z}^r \oplus T$, where $r = \operatorname{rank}(E(K))$ and T is a torsion group.

L-function of E/K

$$L_E(s, K) = \prod_{\mathfrak{p} \nmid \Delta_E} \left(1 - \frac{a_{\mathfrak{p}}}{(\mathrm{N}\mathfrak{p})^s} + \frac{1}{\mathrm{N}\mathfrak{p}^{2s-1}}\right)^{-1} \prod_{\mathfrak{p} \mid \Delta_E} \left(1 - \frac{a_{\mathfrak{p}}}{(\mathrm{N}\mathfrak{p})^s}\right)^{-1}$$

where for each prime $\mathfrak{p}$ of $\mathcal{O}_K$ with good reduction

$$\mathrm{N}\mathfrak{p} = \#\left(\mathcal{O}_K/\mathfrak{p}\right) = p^f$$

$$\#E_{\mathfrak{p}}(\mathcal{O}_K/\mathfrak{p}) = \mathrm{N}\mathfrak{p} + 1 - a_{\mathfrak{p}}, \quad |a_{\mathfrak{p}}| \leq 2\left(\mathrm{N}\mathfrak{p}\right)^{1/2}.$$

Rank of elliptic curves over number fields

Let E be an elliptic curve over $\mathbb{Q}$. How does the rank vary over number fields K? When does E acquire new rank over K?

Birch and Swinnerton-Dyer conjecture
$\mathrm{ord}_{s=1} L_E(s, K) = \mathrm{rank}(E(K))$.

Quadratic extensions

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $K = \mathbb{Q}(\sqrt{d})$. Then

$$L_E(s, K) = L_E(s) L_{E_d}(s)$$

where $E_d/\mathbb{Q}$ is the elliptic curve

$$dy^2 = x^3 + Ax + B$$

called the quadratic twist of $E/\mathbb{Q}$.

$L_E(s) = \sum_{n\geq 1} a_n\, n^{-s}$ has analytic continuation and functional equation

$$\Lambda_E(s) = \left(\frac{\sqrt{N_E}}{2\pi}\right)^s \Gamma(s) L_E(s) = w_E \Lambda_E(2-s).$$

$L_{E_d}(s) = L_E(s, \chi_d) = \sum_{n\geq 1} \chi_d(n)\, a_n\, n^{-s}$, where $\chi_d(n) = \left(\frac{d}{n}\right)$, has analytic continuation and functional equation

$$\Lambda_E(s, \chi_d) = \left(\frac{|d|\sqrt{N_E}}{2\pi}\right)^s \Gamma(s) L_E(s, \chi_d) = w_E \chi_d(-N_E) \Lambda_E(2-s, \chi_d).$$

Conjecture (Goldfeld)

The average rank of E_d is $1/2$.

Random Matrix Theory and L-functions

Density Conjecture (Katz and Sarnak) $\Rightarrow$

The set of discriminants d such that the root number of E_d is $+1$, and $L_E(1, \chi_d) = 0$ has density 0.

The set of discriminants d such that the root number of E_d is -1, and $L_E(1, \chi_d)$ has a zero of order > 1 has density 0.

Conjecture (Conrey, Keating, Rubinstein and Snaith)

Let $E/\mathbb{Q}$ be an elliptic curve, and let $N_E(X)$ be the number of discriminants d with $|d| \leq X$ such that the root number is $+1$, and $L_E(1, \chi_d) = 0$. Then,

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

for some constants b_E and e_E depending on E.

Cyclic extensions

Let $k \geq 3$ be a prime, m a positive integer, and let $K/\mathbb{Q}$ a cyclic extension of degree k and conductor m. Let $\widehat{G}$ be the group of primitive characters of $G = \mathrm{Gal}(K/\mathbb{Q})$.

Each non-trivial character $\chi \in \widehat{G}$ is a multiplicative function

$$\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \langle \xi_k \rangle \subseteq \mathbb{C}^*.$$

The L-function of $E/\mathbb{Q}$ twisted by χ is

$$L_E(s,\chi) = \sum_{n \geq 1} a_n \, \chi(n) \, n^{-s},$$

and $L_E(s,\chi)$ has analytic continuation and functional equation

$$\Lambda_E(s,\chi) = \left(\frac{m\sqrt{N_E}}{2\pi}\right)^s \Gamma(s) \, L_E(s,\chi) = \frac{w_E \, \chi(N_E) \, \tau(\chi)^2}{m} \, \Lambda_E(2-s,\overline{\chi}).$$

L-functions over cyclic extensions

Let $K/\mathbb{Q}$ be a cyclic extension of degree k and conductor m, with Galois group G and character group $\widehat{G}$.

- $L_E(s, \chi_0) = L_E(s)$;
- $L_E(s, K) = \prod_{\chi \in \widehat{G}} L_E(s, \chi)$;
- For any non-trivial $\chi \in \widehat{G}$, $L_E(1, \chi) = 0$ if and only if $L_E(1, \chi) = 0$ for all non-trivial $\chi \in \widehat{G}$.

Then, under the Birch and Swinnerton-Dyer conjecture, E acquires new rank over K if and only if $L_E(1, \chi) = 0$ for some non-trivial character of $\widehat{G}$.

Let k be an odd prime, $E/\mathbb{Q}$ an elliptic curve, and let

$$\begin{aligned} N_{E,k}(X) &= \#\{K/\mathbb{Q} \text{ cyclic of degree } k,\ \mathrm{cond}(K) \le X,\ r_K(E) > r_{\mathbb{Q}}(E)\} \\ &= \frac{1}{k-1}\,\#\{\chi \neq \chi_0 \text{ of order } k,\ \mathrm{cond}(\chi) \le X,\ L_E(1,\chi) = 0\} \end{aligned}$$

under the Birch and Swinnerton-Dyer conjecture.

Conjecture

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

Random Matrix Theory

Let $U(N)$ be the group of N by N unitary matrices, which is a probability space with respect to the Haar measure. For each $A \in U(N)$, consider the characteristic polynomial

$$P_A(\lambda) = \det(\lambda I - A) = \prod_{n=1}^{N} \lambda - e^{i\theta_n}.$$

Keating and Snaith Model Statistics for the distribution of the special values $|L_E(1,\chi)|$, for Dirichlet characters of order k, are connected to the statistics for the distribution of the values $|P_A(1)|$ for $A \in U(N)$.

Keating and Snaith, *Random Matrix Theory and* $\zeta(1/2+it)$, 2000.

Discretisation

From the theory of modular symbols, we can write

$$\frac{2\,\tau(\chi)\,L_E(1,\chi)}{\Omega_E} = \sum_{a \bmod m} \overline{\chi}(a)\Lambda(a,m)$$

where Ω_E is a rational multiple of the real period, and $\tau(\chi)$ is the Gauss sum. The $\Lambda(a,m)$ are integers independent of χ.

Theorem

$$\frac{2\tau(\chi)L_E(1,\chi)}{\Omega_E} = \begin{cases} \chi(N_E)^{(k+1)/2}\; n_E(\chi) & \text{if } w_E = 1 \\ \\ \chi(N_E)^{(k+1)/2}\; (\xi_k - \xi_k^{-1})\; n_E(\chi) & \text{if } w_E = -1 \end{cases}$$

where $n_E(\chi)$ is an integer in $\mathbb{Q}(\xi_k) \cap \mathbb{R} = \mathbb{Q}(\xi_k)^+$.

Let ϕ be the map

$$\phi : \mathbb{Z}[\xi_k]^+ \to \mathbb{R}^{(k-1)/2}$$
$$\alpha \mapsto (\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_{(k-1)/2}(\alpha))$$

where $\mathrm{Gal}(\mathbb{Q}(\xi_k)^+/\mathbb{Q}) = \left\{\sigma_1 = 1, \sigma_2, \ldots, \sigma_{(k-1)/2}\right\}$.

Let $\alpha_1, \cdots, \alpha_N$ be an integral basis of $\mathbb{Z}[\xi_k]^+$. The image of $\mathbb{Z}[\xi_k]^+$ in $\mathbb{R}^{(k-1)/2}$ is the lattice generated by the linearly independent vectors

$$\omega_1 = \phi(\alpha_1), \ \ldots, \ \omega_{(k-1)/2} = \phi(\alpha_{(k-1)/2}).$$

Let $R \subseteq \mathbb{R}^{(k-1)/2}$ be the fundamental parallelogram

$$R = \left\{ \ a_1\omega_1 + \ldots + a_{(k-1)/2}\ \omega_{(k-1)/2} : \quad -1 < a_i < 1 \ \right\}.$$

Then,

$$L_E(1, \chi) = 0 \iff n_E(\chi) = 0 \iff \phi(n_E(\chi)) \in R.$$

Then,

$$n_E(\chi) = 0 \iff (n_E(\chi)^{\sigma_1}, \ldots, n_E(\chi)^{\sigma_{(k-1)/2}}) \in R.$$

Let $\chi \in \widehat{G}$ be any character of conductor m and order k. For any automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_k)/\mathbb{Q})$, let χ^σ be the character

$$\begin{aligned} \chi^\sigma : (\mathbb{Z}/m\mathbb{Z})^* &\to \langle \xi_k \rangle \subseteq \mathbb{C}^* \\ a &\mapsto \sigma\left(\chi(a)\right) \end{aligned}$$

Then, χ^σ is also an element of $\widehat{G}$.

Lemma Let k be an odd prime, and χ a character of order k and conductor m. For any σ in $\mathrm{Gal}(\mathbb{Q}(\xi_k)/\mathbb{Q})$, we have

$$|L_E(1, \chi^\sigma)| = \frac{c_{E,k}}{m^{1/2}} |n_E(\chi)^\sigma|$$

where $c_{E,k}$ is an explicit constant depending only on E and k.

Cubic characters

$n_E(\chi) \in \mathbb{Z}$, and $n_E(\chi) = 0$ if and only if

$$|n_E(\chi)| < 1 \iff |L_E(1,\chi)| < \frac{c}{\sqrt{m}}$$

Quintic characters

$n_E(\chi) \in \mathbb{Z}[\sqrt{5}]$, and $n_E(\chi) = 0$ if and only if

$$|L_E(1,\chi)| < \frac{c_1}{\sqrt{m}} \text{ and } |L_E(1,\chi^\sigma)| < \frac{c_2}{\sqrt{m}},$$

where σ is the non-trivial element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$.

General characters

$n_E(\chi) \in \mathbb{Z}[\xi_k]^+$, and $n_E(\chi) = 0$ if and only if

$$|L_E(1,\chi^{\sigma_i})| \le \frac{c_k}{m^{1/2}} \quad \text{for } 1 \le i \le (k-1)/2$$

where $\sigma_1, \ldots, \sigma_{(k-1)/2} \in \mathrm{Gal}(\mathbb{Q}(\xi_k)/\mathbb{Q})$ is a set of representatives for $\mathrm{Gal}(\mathbb{Q}(\xi_k)^+/\mathbb{Q})$.

Unitary Random Matrices

Let $U(N)$ be the set of unitary $N \times N$ matrices. For each $A \in U(N)$, let $P_A(\lambda) = \det(A - \lambda I)$ be the characteristic polynomial of A. Let

$$M_U(s, N) = \int_{U(N)} |P_A(1)|^s \, d\text{Haar}$$

be the moments of $|P_A(1)|$.

Theorem (Keating and Snaith)

$$M_U(s, N) = \prod_{j=1}^{N} \frac{\Gamma(j)\Gamma(j+s)}{\Gamma^2(j+s/2)}.$$

Then, the probability density of $|P_A(1)|$ is

$$p(x) = \frac{1}{2\pi i} \int_{(c)} M_U(s, N) x^{-s-1} ds \sim G^2(1/2) N^{1/4}$$

when $x \leq N^{-1/2}$, where $G(z)$ is the Barnes G-function.

Fix $k \geq 3$, and let

$$S_k(X) = \{\chi \text{ of order } k \text{ and conductor} \leq X\}$$
$$N_k(X) = \#S_k(X) \sim b_k X$$

with an explicit constant b_k.

Let

$$M_E(s, X) = \frac{1}{N_k(X)} \sum_{\chi \in S_k(X)} |L_E(1, \chi)|^s$$

be the moments of $|L_E(1, \chi)|$. The family of twists of order k has unitary symmetries.

Keating and Snaith Conjecture

$$M_E(s, X) \sim a_E(s/2) M_U(s, N)$$

when $N = 2 \log X \to \infty$, where $a_E(s/2)$ is an arithmetic factor depending only on the curve E.

Then, the probability distribution for the values $|L_E(1,\chi)|$ is

$$\begin{aligned} p_E(x) &= \frac{1}{2\pi i}\int_{(c)} M_E(s,X)\, x^{-s-1}\, ds \\ &\sim \frac{1}{2\pi i}\int_{(c)} a_E(s/2)\, M_U(s,N)\, x^{-s-1}\, ds \\ &\sim C_E \log^{1/4} X \end{aligned}$$

for $x \le (2\log X)^{-1/2}$, $X \to \infty$.

Let χ be a character of order $k \ge 3$ and conductor m. The probability that $L_E(1,\chi)$ vanishes is

$$\begin{aligned} \text{Prob}\left(|L_E(1,\chi)| < cm^{-1/2}\right) &\sim \int_0^{cm^{-1/2}} C_E \log^{1/4} m\, dx \\ &= c\, C_E \frac{\log^{1/4} m}{m^{1/2}} \end{aligned}$$

when $m \to \infty$.

Assuming that $|L_E(1, \chi^{\sigma_i})|$ are independent identically distributed random variables, the probability that $L_E(1, \chi)$ is zero is proportional to

$$\frac{\log^{(k-1)/8} m}{m^{(k-1)/4}}$$

for χ a primitive character of order k and conductor m.

Summing the probabilities, we have

$$\sum_{\chi \in S_3(X)} \frac{\log^{1/4} m}{m^{1/2}} \sim c_3 X^{1/2} \log^{1/4} X$$

$$\sum_{\chi \in S_5(X)} \frac{\log^{1/2} m}{m} \sim c_5 \log^{3/2} X$$

$$\sum_{\chi \in S_7(X)} \frac{\log^{3/4} m}{m^{3/2}} \ll 1$$

Numerical Evidence

For each elliptic curve E, the characters with conductor prime to N_E and less than two million were considered.

Curve	Cubic vanishing	Quintic vanishing	Septic vanishing
E11	1152	15	2
E14	4347	10	0
E15	2050	11	0

More on the discretisation

In the case of cubic twists, one can look at a more precise conjecture of the type

$$N_{E,3}(X) \sim b_E X^{1/2} \log^{e_E} X$$

where b_E and e_E are constants depending only on E.

The model described above indicates $e_E = 1/4$. If E has rational 3-torsion, then the conjectural divisibility

$$3^{\nu(m)-1} \mid n_E(\chi)$$

gives a probability of vanishing for $L_E(1, \chi)$

$$3^{\nu(m)-1} \frac{\log^{1/4} m}{m^{1/2}}.$$

Adding this additional information to our model will give $e_E = 9/4$ when E has rational 3-torsion.

Contents