The derivative of $SO(2N+1)$ characteristic polynomials and rank 3 elliptic curves

N. C. Snaith
School of Mathematics,
University of Bristol,
Bristol BS8 1TW, UK

August 15, 2005

Abstract

Here we calculate the value distribution of the first derivative of characteristic polynomials of matrices from $SO(2N+1)$ at the point 1, the symmetry point on the unit circle of the eigenvalues of these matrices. The connection between the values of random matrix characteristic polynomials and values of the L-functions of families of elliptic curves implies that this calculation in random matrix theory is relevant to the problem of predicting the frequency of rank three curves within these families, since the Birch and Swinnerton-Dyer conjecture relates the value of an L-function and its derivatives to the rank of the associated elliptic curve. This article is based on a talk given at the Isaac Newton Institute for Mathematical Sciences during the "Clay Mathematics Institute Special Week on Ranks of Elliptic Curves and Random Matrix Theory".

1 Introduction

1.1 Random matrix theory and number theory

The connection between random matrix theory and number theory began with the work of Montgomery [26] when he conjectured that the distribution of the complex zeros of the Riemann zeta function follows the same statistics as the eigenvalues of a random matrix chosen from $U(N)$ generated uniformly with respect to Haar measure. This conjecture is supported by numerical evidence [27] and also by further work [15, 30, 2, 3] suggesting that the same conjecture is true for more general L-functions. For all these L-functions there is a Generalized Riemann Hypothesis that the non-trivial zeros lie on a vertical line in the complex plane. The conjectures mentioned above concern the statistics of the zeros high on this critical line.

The philosophy of Katz and Sarnak [18, 19] extended the connection with random matrix theory by proposing that rather than averaging over many zeros of a given L-function, if the zeros near to the point where the critical line crosses the real axis are averaged over a family of naturally connected L-functions, then they will be found to follow the statistics of the eigenvalues of one of the three classical compact groups of random matrices: $U(N)$, $O(N)$ or $USp(2N)$, where again the statistics are computed with respect to the probability measure given by Haar measure. There is numerical evidence for this conjecture as well [29], and strong support is given to it by the rigorous work of Katz and Sarnak [18] in the case of function field zeta functions.

For a review of applications of random matrix theory to questions in number theory see, for example, [5] or [22].

There has been a series of papers, starting with [21] and continuing with [6, 17, 16, 20, 8, 7], examining how random matrix theory can be used to predict the distribution of values of the Riemann zeta function and other L-functions, either averaged over an interval high on the critical line, or over a family at the critical point where the critical line crosses the real axis. For large values of the natural asymptotic parameter, for example the variable ordering the L-functions within the family, the moments of L-functions are conjectured to split into a product of an arithmetic contribution, determined by the family being averaged over, and a component derived from a random matrix calculation - the corresponding moment of the characteristic polynomial of the matrices in one of the three groups $U(N)$, $O(N)$ or $USp(2N)$. The asymptotic parameter on the random matrix side is the dimension of the matrix N and a natural equivalence can be made between the two.

In the following section we review the results of Conrey, Keating, Rubinstein and Snaith [9] which use the random matrix prediction for the leading order behaviour of moments of L-functions mentioned above to conjecture the frequency of zeros at the critical point among L-functions in a family corresponding to quadratic twists of an elliptic curve. With the Birch and Swinnerton-Dyer conjecture, this result predicts the frequency of curves of rank two or greater occurring in this family. This work makes use of a discretization formula [35, 31, 23] relating L-values at the critical point to Fourier coefficients of half-integral weight forms. See also David, Fearnley and Kisilevsky [12] for a similar use of random matrix theory to predict frequency of vanishing at the critical point amongst families of elliptic curve L-functions twisted by cubic characters.

The second half of this article presents the random matrix calculation of the distribution of values of the derivative of characteristic polynomials of matrices from $SO(2N+1)$ with Haar measure. We find, at equation (2.19), that moment of the derivative grows like

$$\mathcal{M}(N,s) := \int_{SO(2N+1)} |\Lambda_U'(1)|^s dU_{Haar} \sim (2\pi)^{s/2} 2^{-s^2/2} \frac{G(3/2)}{G(3/2+s)} N^{s^2/2+s/2}, \tag{1.1}$$

where $\Lambda_U(e^{i\theta})$ is the characteristic polynomial of $U \in SO(2N+1)$ and $G(z)$ is the Barnes double gamma function (see 2.10). We also show that the probability that $|\Lambda_U'(1)| < X$ over $U \in SO(2N+1)$ is, for small X, given by (see (2.8) and the sentence following)

$$\tfrac{2}{3} X^{\frac{3}{2}} f(N), \tag{1.2}$$

for the function f given at (2.9). With a discretization formula for the derivatives of elliptic curve L-functions at the critical point similar to that of the L-values themselves, (1.2) could be used to predict the frequency of curves of rank 3 or higher within a family of quadratic twists. Unfortunately such a formula for the derivative of L-functions at the critical point is not yet known, but is being investigated [11], where numerical support is also given to the validity of the model presented here.

We believe that the model presented in Section 2 should apply to the L-functions selected from families of quadratic twists of elliptic curves for the property that they have a zero of at least order one at the critical point. However, there has been some very interesting theoretical work computing the one-level densities of zeros of families of L-functions selected in a different way (through parametric families of elliptic curves) that implies that in that case the zero at the critical point does not affect the position of nearby zeros (see [25] and [38]). This does not seem to be a contradiction with the model proposed here (where the zero at the critical point does repel the other close by zeros), as the zero statistics are examined over collections of L-functions selected in very different ways.

The result presented at (1.1) has already been applied by Delaunay in [13] in order to predict the moments of the orders of Tate-Shafarevich groups and regulators of elliptic curves with odd rank belonging to a family of quadratic twists.

This work has been extended [32] to considering subsets of matrices from $SO(N)$ that are constrained to have n eigenvalues equal to 1, and investigating the first non-zero derivative of the characteristic polynomial at that point. When $n = 1$ this specializes to the result in the present paper.

1.2 Random matrix theory and elliptic curves

We review here the results of [9] which apply random matrix theory to predicting the frequency of vanishing at the critical point of the L-functions in the family of elliptic curves described below; or equivalently, assuming the Birch and Swinnerton-Dyer conjecture, the frequency of rank 2 or higher curves occurring in the family of elliptic curves. The motivation for the random matrix calculations presented in Section 2 is that they may be used similarly to examine rank 3 curves, see [11].

We consider an L-function (defined by the Dirichlet series and Euler product below when Re $s > 3/2$)

$$L_E(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p \mathcal{L}_p(1/p^s) = \prod_{p|\Delta} \left(1 - a_p p^{-s}\right)^{-1} \prod_{p\nmid\Delta} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}, \qquad (1.3)$$

that is associated to an elliptic curve E over $\mathbb{Q}$

$$E: \; y^2 = x^3 + Ax + B. \qquad (1.4)$$

The coefficients a_p, for prime p, are determined by $a_p = p + 1 - \#E(\mathbb{F}_p)$, where $\#E(\mathbb{F}_p)$ counts the number of pairs x, y, with $0 \leq x, y \leq p - 1$, such that $y^2 \equiv x^3 + Ax + B \pmod{p}$, plus one for the point at infinity. Δ is the discriminant of the cubic $x^3 + Ax + B$. For an extremely clear introduction to elliptic curves in the context discussed here, see the review paper by Rubin and Silverberg [28].

A family of quadratic twists of this elliptic curve is formed by

$$E_d: \; dy^2 = x^3 + Ax + B \qquad (1.5)$$

for integer d that are fundamental discriminants, and the corresponding family of L-functions, ordered by $|d|$, are

$$L_E(s, \chi_d) = \sum_{n=1}^{\infty} \frac{a_n \chi_d(n)}{n^s}, \qquad (1.6)$$

where the characters $\chi_d(n)$ are the Kronecker symbol:

$$\chi_d(n) = \left(\frac{d}{n}\right). \qquad (1.7)$$

The original L-function, $L_E(s)$, and its twisted companions, $L_E(s,\chi_d)$, have an analytic continuation with the following functional equations [37, 33, 4]

$$\left(\frac{2\pi}{\sqrt{Q}}\right)^{-s}\Gamma(s)L_E(s) = w_E\left(\frac{2\pi}{\sqrt{Q}}\right)^{s-2}\Gamma(2-s)L_E(2-s) \tag{1.8}$$

(where Q is the conductor of the curve E and the sign of the functional equation, w_E, takes the value ±1) and, if $(d,Q)=1$,

$$\left(\frac{2\pi}{\sqrt{Q}|d|}\right)^{-s}\Gamma(s)L_E(s,\chi_d) = \chi_d(-Q)w_E\left(\frac{2\pi}{\sqrt{Q}|d|}\right)^{s-2}\Gamma(2-s)L_E(2-s,\chi_d). \tag{1.9}$$

See also [10] where there is a similar but more detailed discussion of these L-functions.

The sign of the functional equation for the twisted L-function $L_E(s,\chi_d)$ is $\chi_d(-Q)w_E$ and is either $+1$ or -1. We consider the family of L-functions

$$\mathcal{F}_{E^+} = \{L_E(s,\chi_d):\ \chi_d(-Q)w_E = +1\}. \tag{1.10}$$

By the philosophy of Katz and Sarnak it is expected that the zeros near the critical point of such a family have statistics like eigenvalues near 1 of matrices from $SO(2N)$ with Haar measure. These eigenvalues occur in complex conjugate pairs and an eigenvalue at one must have even multiplicity. The even functional equation of the L-functions forces the same symmetry on their zeros lying, by the Generalized Riemann Hypothesis, on the line $\mathrm{Re}\, s = 1$.

In contrast, the low-lying zeros of the L-functions in the family

$$\mathcal{F}_{E^-} = \{L_E(s,\chi_d):\ \chi_d(-Q)w_E = -1\}. \tag{1.11}$$

display the same statistics as $SO(2N+1)$ eigenvalues near one, since in this case there is always an eigenvalue at one and it has to have odd multiplicity.

Both numerical and analytical evidence have been given already [9], and we review the argument here, that random matrix theory can be used to conjecture the frequency of L-functions vanishing at the critical point in a family such as $\mathcal{F}_{E^+}$. This is particularly important because of the Birch and Swinnerton-Dyer conjecture which asserts that the order of the zero of an elliptic curve L-function at the critical point is equal to the rank of the Mordell-Weil group of the elliptic curve. (See [28] for a discussion of ranks of elliptic curves and for a summary of what is known about the occurrence of ranks of various sizes amongst families of elliptic curves.)

To model values of L-functions from $\mathcal{F}_{E^+}$ near the point $s=1$, we use the characteristic polynomials of matrices from $SO(2N)$

$$\Lambda_U(e^{i\theta}) = \prod_{n=1}^{N}\left(1-e^{i(\theta_n-\theta)}\right)\left(1-e^{i(-\theta_n-\theta)}\right), \tag{1.12}$$

evaluated at the point $\theta=0$. Here $e^{\pm i\theta_1},\ldots,e^{\pm i\theta_N}$ are the eigenvalues of the matrix $U\in SO(2N)$.

The moments of $\Lambda_U(1) = \prod_{n=1}^{N}\left|1-e^{i\theta_n}\right|^2$ are easily calculated using Weyl's expression [36] for Haar measure on the conjugacy classes of $SO(2N)$ and a form of Selberg's integral to be [20]

$$
\begin{aligned}
&\int_{SO(2N)} \Lambda_U(1)^s dU_{Haar} \\
&\quad = 2^{2Ns} \prod_{j=1}^{N} \frac{\Gamma(N+j-1)\Gamma(s+j-1/2)}{\Gamma(j-1/2)\Gamma(s+j+N-1)} \qquad (1.13)\\
&\equiv M_O(N,s).
\end{aligned}
$$

The L-function moments are then conjectured to have the form [6, 20]

$$
\begin{aligned}
M_E(T,s) &\equiv \frac{1}{T^*} \sum_{\substack{|d|\leq T \\ L_E(s,\chi_d)\in\mathcal{F}_{E+}}} L_E(1,\chi_d)^s \\
&\sim a_s(E) M_O(N,s) \qquad (1.14)
\end{aligned}
$$

for large T. Here $N=\log T$ (from equating the density of zeros near the critical point with the density of the matrix eigenvalues), the sum is over fundamental discriminants d, T^* is the number of terms in the sum and $a_s(E)$ is an Euler product that contains arithmetic information specific to the elliptic curve E and the family of L-functions being averaged over. In practice, it is often a subset of $\mathcal{F}_{E^+}$ that is summed over. If, for example, we select those L-functions $L_E(s,\chi_d)$ in $\mathcal{F}_{E^+}$ with $d>0$ and further restricted by a condition on d mod Q, if Q is odd, and on $d \mod 4Q$, if Q is even, then the arithmetic factor would be

$$
\begin{aligned}
a_s(E) = &\prod_{p\nmid Q} \left(1-p^{-1}\right)^{s(s-1)/2} \left(\frac{p}{p+1}\right)\left(\frac{1}{p}+\frac{1}{2}\left(\mathcal{L}_p(1/p)^s+\mathcal{L}_p(-1/p)^s\right)\right) \\
\times &\prod_{p|Q} \left(1-p^{-1}\right)^{s(s-1)/2} \mathcal{L}_p(a_p/p)^s. \qquad (1.15)
\end{aligned}
$$

See [10] and [8], Section 4.4 for more examples.

Next we consider the distribution of the values of the characteristic polynomials of $SO(2N)$ matrices at the point 1. If $P_O(N,x)dx$ is the probability that the characteristic polynomial of a matrix chosen from $SO(2N)$ with Haar measure has a value between x and $x+dx$, then

$$
\begin{aligned}
P_O(N,x) &= \frac{1}{2\pi i x}\int_{(c)} M_O(N,s)x^{-s}ds \\
&\sim x^{-1/2}h(N) \qquad (1.16)
\end{aligned}
$$

for $x\to 0^+$, since for small x the behaviour is dominated by the pole of $M_O(N,s)$ at $s=-1/2$. Here (c) denotes a path of integration along the vertical line from $c-i\infty$ to $c+i\infty$.

For large N, $h(N)\sim 2^{-7/8}G(1/2)\pi^{-1/4}N^{3/8}$ (G is the Barnes double gamma function, defined as [1, 34]:

$$
G(1+z) = (2\pi)^{z/2} e^{-[(1+\gamma)z^2+z]/2} \prod_{n=1}^{\infty}\left[(1+z/n)^n e^{-z+z^2/(2n)}\right], \qquad (1.17)
$$

where γ is Euler's constant. See also (2.10) for more properties of this function.) Since the probability that an element of $SO(2N)$ has a characteristic polynomial whose value at 1 is X or smaller is $\int_0^X P_O(N,x)dx$, we find that the the behaviour of this probability for small X and large N is

$$\lim_{N\to\infty} N^{-3/8} \lim_{X\to 0^+} \left(X^{-1/2}\int_0^X P_O(N,x)dx\right) = 2^{1/8}G(1/2)\pi^{-1/4}. \tag{1.18}$$

We see from equation (1.14) that for large d, moments of L-functions are conjectured to be just $a_s(E)$ (the prime product) times the random matrix moment $M_O(N,s)$. If this is true, then we define $P_E(T,x)dx$ as the probability, amongst members of $\mathcal{F}_{E^+}$, that $L_E(1,\chi_d)$, for $|d|$ around e^N, will take a value between x and $x+dx$, giving

$$P_E(T,x) \quad = \quad \frac{1}{2\pi i x}\int_{(c)} M_E(T,s)x^{-s}ds, \tag{1.19}$$

and an approximation for this probability for small x should be

$$P_E(T,x) \quad \sim \quad a_{-1/2}(E)x^{-1/2}h(N). \tag{1.20}$$

Here equating densities of zeros gives $N \sim \log T$.

But these L-functions are constrained to take only certain discretized values. The L-values have the form [35, 31, 23]:

$$L_E(1,\chi_d) = \kappa_E \frac{c_E(|d|)^2}{\sqrt{d}}, \tag{1.21}$$

where the $c_E(|d|)$ are integers, the Fourier coefficients of a half-integral weight form.

The argument now is to suppose that if

$$L_E(1,\chi_d) < \frac{\kappa_E}{\sqrt{d}} \tag{1.22}$$

then

$$L_E(1,\chi_d) = 0, \tag{1.23}$$

and so to integrate (1.20) as we did (1.16) and so predict that

$$\#\{|d| \le T : L_E(1,\chi_d) = 0, L_E(s,\chi_d) \in \mathcal{F}_{E^+}\} \sim \frac{8}{3}\sqrt{\kappa_E} a_{-1/2}\frac{T^*}{T^{1/4}}h(N). \tag{1.24}$$

with $N \sim \log T$. However, the $c(|d|)$ are divisible by some predetermined powers of 2 which change this discretization. To avoid this problem, the conjecture stated in [9] is restricted to prime discriminants.

Conjecture 1.1 *(Conrey, Keating, Rubinstein, Snaith):*

Let E be an elliptic curve defined over $\mathbb{Q}$. Then there is a constant $c_E \ge 0$ such that

$$\sum_{\substack{p \le T \\ L_E(1,\chi_p)=0 \\ L_E(s,\chi_p)\in\mathcal{F}_{E^+}}} 1 \sim c_E T^{3/4}(\log T)^{-5/8}$$

(The conjecture was originally stated in [9] with $c_E > 0$, but in fact numerics have revealed that the constant can be zero [10] for certain families. An explanation of such a case with $c_E = 0$ was given by Delaunay [14].)

With the Birch and Swinnerton-Dyer conjecture, this suggests that out of all the elliptic curves associated with L-functions in $\mathcal{F}_{E^+}$ with prime discriminant $p \leq T$ (there are of order $T/\log T$ of them), a number of order $T^{3/4}(\log T)^{-5/8}$ should have rank two or greater. The $T^{3/4}$ has been predicted previously by Sarnak using different arguments, but random matrix theory adds more detailed information in the form of the power on the logarithm. For numerical evidence supporting the conjecture, see [9].

In the next section we will calculate the distribution of values of the first derivative at the point 1 of the characteristic polynomials from $SO(2N+1)$ matrices (with Haar measure). The calculation is similar to that leading to (1.16). If a discretization of values of $L'_E(1,\chi_d)$ were known, in analogy to (1.21), then the following calculation could be used to probe questions of elliptic curves of rank three occurring in families of quadratic twists (the family described in (1.5)).

2 Random matrix calculations

In this section we will calculate the probability of the first derivative of a characteristic polynomial of a random (with respect to Haar measure) $SO(2N+1)$ matrix taking a value less than X at the point 1 on the unit circle. Since the zeros near the critical point of L-functions in the family $\mathcal{F}_{E^-}$ are predicted to have statistics like those of the eigenvalues near 1 of a random $SO(2N+1)$ matrix, it is expected that the probability density of values of the derivative of the characteristic polynomial will model that of the derivative at the critical point of L-functions in this family.

For a matrix $U \in SO(2N+1)$ the characteristic polynomial looks like

$$\Lambda_U(e^{i\theta}) = (1-e^{-i\theta})\prod_{n=1}^{N}(1-e^{i(\theta_n-\theta)})(1-e^{i(-\theta_n-\theta)}). \tag{2.1}$$

We will consider the derivative

$$\begin{aligned}\Lambda'_U(1) \quad &:= \quad \frac{d}{d\alpha}\left[(1-e^{-\alpha})\prod_{n=1}^{N}(1-e^{i\theta_n-\alpha})(1-e^{-i\theta_n-\alpha})\right]_{\alpha=0} \\ &= \quad \prod_{n=1}^{N}|1-e^{i\theta_n}|^2 \\ &= \quad 2^N\prod_{n=1}^{N}(1-\cos\theta_n). \end{aligned} \tag{2.2}$$

We will now calculate the moments and value distribution of $\Lambda'_U(1)$ averaged over $SO(2N+1)$ with respect to Haar measure. Since $\Lambda'_U(1)$ depends only on the eigenvalues of the matrix U, we use the expression

$$C\prod_{n=1}^{N}(1-\cos\theta_n)\prod_{1\leq j<k\leq N}(\cos\theta_j-\cos\theta_k)^2 \tag{2.3}$$

for the measure on conjugacy classes of matrices with the same set of eigenvalues [36]. The normalisation constant is $C = 2^{-N^2} \prod_{j=1}^{N} \Gamma(N+j)\ \left(\Gamma(j+1)\Gamma(1/2+j)\Gamma(j-1/2)\right)^{-1}$.

The sth moment of the derivative of the characteristic polynomial is given by

$$\begin{aligned}
\mathcal{M}(N,s) &:= C\int_0^{\pi}\cdots\int_0^{\pi} |\Lambda_U'(1)|^s \prod_{n=1}^{N}(1-\cos\theta_n) \prod_{1\le j<k\le N}(\cos\theta_j-\cos\theta_k)^2 d\theta_1\cdots d\theta_N \\
&= C\int_0^{\pi}\cdots\int_0^{\pi} 2^{Ns}\prod_{n=1}^{N}(1-\cos\theta_n)^{1+s} \prod_{1\le j<k\le N}(\cos\theta_j-\cos\theta_k)^2 d\theta_1\cdots d\theta_N \\
&= C2^{Ns}\int_{-1}^{1}\cdots\int_{-1}^{1}\prod_{n=1}^{N}\frac{(1-x_n)^{1/2+s}}{(1+x_n)^{1/2}} \prod_{1\le j<k\le N}(x_j-x_k)^2 dx_1\cdots dx_N. \qquad (2.4)
\end{aligned}$$

This can be evaluated using a form of Selberg's integral (for details see [24]):

$$\begin{aligned}
&\int_{-1}^{1}\cdots\int_{-1}^{1}\prod_{1\le j<l\le n}|(x_j-x_l)|^{2\gamma}\prod_{j=1}^{n}(1-x_j)^{\alpha-1}(1+x_j)^{\beta-1}dx_j \\
&= 2^{\gamma n(n-1)+n(\alpha+\beta-1)}\prod_{j=0}^{n-1}\frac{\Gamma(1+\gamma+j\gamma)\Gamma(\alpha+j\gamma)\Gamma(\beta+j\gamma)}{\Gamma(1+\gamma)\Gamma(\alpha+\beta+\gamma(n+j-1))}, \qquad (2.5)
\end{aligned}$$

if $\mathrm{Re}\alpha > 0$, $\mathrm{Re}\beta > 0$ and $\mathrm{Re}\gamma > -\min\left(\frac{1}{n}, \frac{\mathrm{Re}\alpha}{n-1}, \frac{\mathrm{Re}\beta}{n-1}\right)$.

We have $\gamma = 1$, $\alpha = 3/2+s$ and $\beta = 1/2$, so the integral in equation (2.4) is

$$\begin{aligned}
\mathcal{M}(N,s) &= C2^{2Ns+N^2}\prod_{j=1}^{N}\frac{\Gamma(j+1)\Gamma(1/2+s+j)\Gamma(j-1/2)}{\Gamma(s+N+j)} \\
&= 2^{2Ns}\prod_{j=1}^{N}\frac{\Gamma(1/2+s+j)\Gamma(N+j)}{\Gamma(1/2+j)\Gamma(s+N+j)}. \qquad (2.6)
\end{aligned}$$

If the probability that $|\Lambda_U'(1)|$ takes a value between x and $x+dx$ is given by $P(N,x)dx$, then from a standard result in probability (where the contour of integration is a vertical line with real part equal to c)

$$\begin{aligned}
P(N,x) &= \frac{1}{2\pi i x}\int_{(c)} x^{-s}\mathcal{M}(N,s)ds \\
&= \frac{1}{2\pi i x}\int_{(c)} x^{-s}2^{2Ns}\prod_{j=1}^{N}\frac{\Gamma(1/2+s+j)\Gamma(N+j)}{\Gamma(1/2+j)\Gamma(s+N+j)}ds \qquad (2.7)
\end{aligned}$$

We are particularly interested in the behaviour at small x, and this is dominated by the nearest pole to zero of the integrand: the pole at $s=-3/2$ of $\Gamma(1/2+s+j)$. Thus for small x

$$P(N,x) \sim x^{1/2}f(N). \qquad (2.8)$$

The probability that $|\Lambda_U'(1)| < X$ for U chosen from $SO(2N+1)$ with Haar measure is therefore $\sim \frac{2}{3}X^{\frac{3}{2}}f(N)$ for small X.

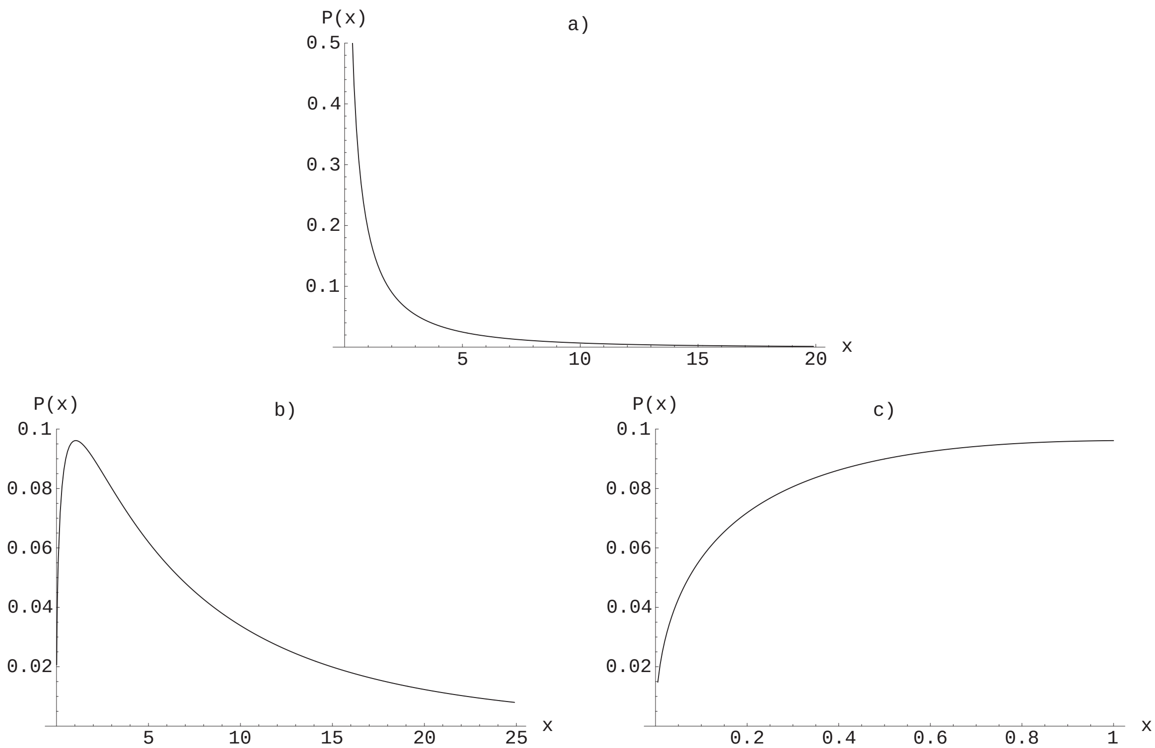

Figure 1: Figure a) shows the distribution of values of the characteristic polynomial at the point one of $SO(2N)$ matrices ($P_O(N,x)$ from (1.16)) when $N=5$. In comparison, figure b) is the value distribution of the derivative of the characteristic polynomial for $SO(2N+1)$ matrices, that is $P(N,x)$ from (2.7), at the point one when $N=5$. Figure c) shows in more detail the behaviour at the origin of figure b) (see equation (2.8)).

The function $f(N)$, derived from (2.7) by a residue calculation, is given by

$$f(N) = 2^{-3N} \frac{1}{\Gamma(N)} \prod_{j=1}^{N} \frac{\Gamma(j)\Gamma(N+j)}{\Gamma(1/2+j)\Gamma(N+j-3/2)}. \tag{2.9}$$

For large N the behaviour of $f(N)$ can be determined using the Barnes G-function [1, 34]:

$$G(1+z) = (2\pi)^{z/2} e^{-[(1+\gamma)z^2+z]/2} \prod_{n=1}^{\infty} \left[(1+z/n)^n e^{-z+z^2/(2n)} \right], \tag{2.10}$$

which has zeros at the negative integers, $-n$, with multiplicity n ($n = 1, 2, 3 \ldots$). Other properties useful to us are that

$$\begin{aligned} G(1) &= 1, \\ G(z+1) &= \Gamma(z)\, G(z), \end{aligned} \tag{2.11}$$

and furthermore, for large $|z|$

$$\log G(z+1) \sim z^2(\tfrac{1}{2}\log z - \tfrac{3}{4}) + \tfrac{1}{2} z \log(2\pi) - \tfrac{1}{12}\log z + \zeta'(-1) + O(\tfrac{1}{z}). \tag{2.12}$$

Thus

$$\prod_{j=1}^{N} \Gamma(j) = G(N+1), \tag{2.13}$$

$$\prod_{j=1}^{N} \Gamma(N+j) = \frac{\prod_{j=1}^{2N}\Gamma(j)}{\prod_{j=1}^{N}\Gamma(j)} = \frac{G(2N+1)}{G(N+1)}, \tag{2.14}$$

$$\prod_{j=1}^{N} \Gamma(j+1/2) = \frac{G(3/2+N)}{G(3/2)} \tag{2.15}$$

and

$$\prod_{j=1}^{N} \Gamma(N+j-3/2) = \frac{G(2N-1/2)}{G(N-1/2)}. \tag{2.16}$$

So we can write

$$f(N) = 2^{-3N} \frac{G(N)G(2N+1)G(3/2)G(N-1/2)}{G(N+1)G(N+3/2)G(2N-1/2)} \tag{2.17}$$

and expanding the G-functions for large N gives

$$f(N) \quad \sim \quad G(3/2) N^{\frac{3}{8}} 2^{-\frac{15}{8}} \pi^{-\frac{3}{4}}. \tag{2.18}$$

Note that $G(3/2) = \Gamma(1/2)G(1/2)$ and $\Gamma(1/2) = \pi^{1/2}$ and [1] $G(1/2) = A^{-3/2}\pi^{-1/4}e^{1/8}2^{1/24}$ with $A = 1.28242713$.

Note also that we can use (2.12) to revisit the moment $\mathcal{M}(N,s)$ and examine that asymptotically for large N. This gives us the large N behaviour of the moments at the point one of the derivative of characteristic polynomials of $SO(2N+1)$ matrices. We have

$$\begin{aligned} \mathcal{M}(N,s) &= 2^{2Ns} \frac{G(3/2+s+N)}{G(3/2+s)} \frac{G(3/2)}{G(3/2+N)} \frac{G(2N+1)}{G(N+1)} \frac{G(s+N+1)}{G(s+2N+1)} \\ &\sim (2\pi)^{s/2} 2^{-s^2/2} \frac{G(3/2)}{G(3/2+s)} N^{s^2/2+s/2}. \end{aligned} \tag{2.19}$$

3 Discussion

We have shown that the probability that $|\Lambda'_U(0)| < X$ over $U \in SO(2N+1)$ with Haar measure is, for small X, given by $\frac{2}{3}X^{\frac{3}{2}}f(N)$. With a better understanding of the values taken by the derivative of L-functions associated to a family of quadratic twists of an elliptic curve this could be used to predict the frequency of rank three curves occurring amongst the members of such a family that have an odd functional equation. Some preliminary numerics have been done to investigate these derivative values, and further work is ongoing [11].

The result (2.19) was applied by Delaunay in [13] to predict moments of the orders of Tate-Shafarevich groups and the regulators of elliptic curves belonging to a family of quadratic twists - a family of type $\mathcal{F}_{E^-}$. The Birch and Swinnerton-Dyer conjecture provides a formula for the first non-zero derivative of an L-function in terms of various quantities related to the associated elliptic curve. One of these quantities is the order of the Tate-Shafarevich group, and another, in the case of the first derivative of L-functions with odd functional equation, is the regulator. For families of L-functions with even functional equation the result (1.14) is used by Delaunay to predict the asymptotic form of moments of the order of the Tate-Shafarevich group for the associated family of elliptic curves, and for families with odd functional equation (2.19) was used to conjecture the form of moments of the regulator.

4 Acknowledgments

Thanks to Brian Conrey for his number theoretical insight in recognizing the potential importance of these calculations from the start, to the Royal Society and EPSRC for supporting this research and to the Isaac Newton Institute for Mathematical Sciences for their hospitality during the programme "Random Matrix Approaches in Number Theory" during which this paper was prepared.

References

[1] E.W. Barnes, The theory of the G-function, *Q. J. Math.*, **31**:264–314, 1900.

[2] E.B. Bogomolny and J.P. Keating, Random matrix theory and the Riemann zeros I: three- and four-point correlations, *Nonlinearity*, **8**:1115–1131, 1995.

[3] E.B. Bogomolny and J.P. Keating, Random matrix theory and the Riemann zeros II:n-point correlations, *Nonlinearity*, **9**:911–935, 1996.

[4] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises, *J. Amer. Math. Soc.*, **14**(4):843–939, 2001.

[5] J.B. Conrey, L-functions and random matrices, In *Mathematics Unlimited 2001 and Beyond*; editors, B. Enquist and W. Schmid, pages 331–352. Springer-Verlag, Berlin, 2001, arXiv:math.nt/0005300.

[6] J.B. Conrey and D.W. Farmer, Mean values of L-functions and symmetry, *Int. Math. Res. Notices*, **17**:883–908, 2000, arXiv:math.nt/9912107.

[7] J.B. Conrey, D.W. Farmer, J.P. Keating, M.O. Rubinstein, and N.C. Snaith, Autocorrelation of random matrix polynomials, *Commun. Math. Phys.*, **237**(3):365–395, 2003, arXiv:math-ph/0208007.

[8] J.B. Conrey, D.W. Farmer, J.P. Keating, M.O. Rubinstein, and N.C. Snaith, Integral moments of L-functions, *Proc. Lond. Math. Soc.*, **91**(1):33–104, 2005, arXiv:math.nt/0206018.

[9] J.B. Conrey, J.P. Keating, M.O. Rubinstein, and N.C. Snaith, On the frequency of vanishing of quadratic twists of modular L-functions, In *Number Theory for the Millennium I: Proceedings of the Millennial Conference on Number Theory*; editor, M.A. Bennett et al., pages 301–315. A K Peters, Ltd, Natick, 2002, arXiv:math.nt/0012043.

[10] J.B. Conrey, J.P. Keating, M.O. Rubinstein, and N.C. Snaith, Random matrix theory and the Fourier coefficients of half-integral weight forms, *preprint*, 2004, arXiv:math.nt/0412083.

[11] J.B. Conrey, M.O. Rubinstein, N.C. Snaith, and M. Watkins, Discretisation for odd quadratic twists, *in Proceedings of the Clay Mathematics Institute Special Week on Ranks of Elliptic Curves and Random Matrix Theory.*

[12] C. David, J. Fearnley, and H. Kisilevsky, On the vanishing of twisted L-functions of elliptic curves, *Experimental Mathematics*, **13**(2):185–98, 2004.

[13] C. Delaunay, Moments of the orders of Tate-Shafarevich groups, *preprint.*

[14] C. Delaunay, Note on the frequency of vanishing of L-functions of elliptic curves in a family of quadratic twists, *preprint.*

[15] D.A. Hejhal, On the triple correlation of zeros of the zeta function, *Inter. Math. Res. Notices*, **7**:293–302, 1994.

[16] C.P. Hughes, Random matrix theory and discrete moments of the Riemann zeta function, *J. Phys. A-Math. Gen.*, **36**(12):2907–2917, 2003, arXiv:math.nt/0207236.

[17] C.P. Hughes, J.P. Keating, and N. O'Connell, Random matrix theory and the derivative of the Riemann zeta function, *Proc. R. Soc. Lond. A*, **456**:2611–2627, 2000.

[18] N.M. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues and Monodromy*, American Mathematical Society Colloquium Publications, 45. American Mathematical Society, Providence, Rhode Island, 1999.

[19] N.M. Katz and P. Sarnak, Zeros of zeta functions and symmetry, *Bull. Amer. Math. Soc.*, **36**:1–26, 1999.

[20] J.P. Keating and N.C. Snaith, Random matrix theory and L-functions at $s = 1/2$, *Commun. Math. Phys*, **214**:91–110, 2000.

[21] J.P. Keating and N.C. Snaith, Random matrix theory and $\zeta(1/2+it)$, *Commun. Math. Phys.*, **214**:57–89, 2000.

[22] J.P. Keating and N.C. Snaith, Random matrices and L-functions, *J. Phys. A*, **36**(12):2859–81, 2003.

[23] W. Kohnen and D. Zagier, Values of L-series of modular forms at the center of the critical strip, *Invent. Math.*, **64**:175–198, 1981.

[24] M.L. Mehta, *Random Matrices*, Elsevier, Amsterdam, third edition, 2004.

[25] S.J. Miller, One- and two-level densities for rational families of elliptic curves: evidence for the underlying group symmetries, *Compos. Math.*, **140**(4):952–992, 2004.

[26] H.L. Montgomery, The pair correlation of the zeta function, *Proc. Symp. Pure Math*, **24**:181–93, 1973.

[27] A.M. Odlyzko, The 10^{20}th zero of the Riemann zeta function and 70 million of its neighbors, *Preprint*, 1989, http://www.dtc.umn.edu/ odlyzko/unpublished/index.html.

[28] K. Rubin and A. Silverberg, Ranks of elliptic curves, *Bulletin of the American Mathematical Society*, **39**(4):455–74, 2002.

[29] M. Rubinstein, *Evidence for a Spectral Interpretation of Zeros of L-functions*, PhD thesis, Princeton University, 1998.

[30] Z. Rudnick and P. Sarnak, Zeros of principal L-functions and random matrix theory, *Duke Mathematical Journal*, **81**(2):269–322, 1996.

[31] G. Shimura, On modular forms of half integral weight, *Ann. Math.*, **97**(2):440–481, 1973.

[32] N.C. Snaith, Derivatives of random matrix characteristic polynomials with applications to elliptic curves, *preprint*, arXiv:math.nt/0508256.

[33] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.*, **141**(3):553–572, 1995.

[34] A. Voros, Spectral functions, special functions and the Selberg zeta function, *Commun. Math. Phys.*, **110**:439–465, 1987.

[35] J.-L. Waldspurger, Sur les coefficients de Fourier des formes modulaires de poids demi-entier, *J. Math. Pures Appl.*, **60**(9):375–484, 1981.

[36] H. Weyl, *Classical Groups*, Princeton University Press, 1946.

[37] A. Wiles, Modular elliptic curves and fermat's last theorem, *Ann. of Math.*, **141**(3):443–551, 1995.

[38] M.P. Young, Lower-order terms of the L-level density of families of elliptic curves, *Int. Math. Res. Notices*, **10**:587–633, 2005.