VANISHING OF L-FUNCTIONS OF ELLIPTIC CURVES OVER NUMBER FIELDS

CHANTAL DAVID, JACK FEARNLEY, AND HERSHY KISILEVSKY

ABSTRACT. Let E be an elliptic curve over $\mathbb{Q}$, with L-function $L_E(s)$. For any primitive Dirichlet character χ, let $L_E(s,\chi)$ be the L-function of E twisted by χ. In this paper, we use random matrix theory to study vanishing of the twisted L-functions $L_E(s,\chi)$ at the central value $s=1$. In particular, random matrix theory predicts that there are infinitely many characters of order 3 and 5 such that $L_E(1,\chi)=0$, but that for any fixed prime $k\geq 7$, there are only finitely many character of order k such that $L_E(1,\chi)$ vanishes. With the Birch and Swinnerton-Dyer Conjecture, those conjectures can be restated to predict the number of cyclic extensions $K/\mathbb{Q}$ of prime degree such that E acquires new rank over K.

1. INTRODUCTION

Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N_E. For any number field $K/\mathbb{Q}$, let $E(K)$ be the group of points of E defined over K. By the Mordell-Weil Theorem, $E(K)$ is a finitely generated abelian group. Let $L_E(s,K)$ be the L-function of E over the field K.

Conjecture 1.1 (Birch and Swinnerton-Dyer conjecture over number fields)**.** *$L_E(s,K)$ has analytic continuation to the whole complex plane, and*

$$ord_{s=1}L_E(s,K) \;=\; r_K(E)$$

where $r_K(E)$ is the rank of $E(K)$.

In this paper, we fix E an elliptic curve over $\mathbb{Q}$, and we study how the rank varies over abelian fields $K/\mathbb{Q}$ of fixed prime degree. For example, are there infinitely many such number fields where E acquires new rank over K (i.e. $r_K(E) > r_{\mathbb{Q}}(E)$)? With the Birch and Swinnerton-Dyer conjecture, one can rephrase the question in terms of vanishing of the L-function $L_E(s,K)$ at $s=1$. Let K be an abelian extension of $\mathbb{Q}$ with

The first and third authors are partially supported by grants from NSERC and FCAR.

Galois group G and conductor m. Let $\hat{G}$ be the group of characters of G which can be identified with a set of Dirichlet characters

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

Let

$$L_E(s) = L_E(s, \mathbb{Q}) = \sum_{n \geq 1} \frac{a_n}{n^s}$$

be the L-function of E over $\mathbb{Q}$. For each primitive Dirichlet character χ, let

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

be the L-function of E over $\mathbb{Q}$ twisted by the character χ. By the work of [16, 15, 1], $L_E(s)$ and $L_E(s, \chi)$ have analytic continuation to the whole complex plane. It also follows from properties of number fields that

$$L_E(s, K) = \prod_{\chi \in \hat{G}} L_E(s, \chi), \tag{1}$$

and the vanishing of the twisted L-functions $L_E(s, \chi)$ at $s = 1$ is equivalent, via the Birch and Swinnerton-Dyer conjecture, to the existence of rational points of infinite order on $E(K)$.

In this paper, we use random matrix theory to study the vanishing of the twisted L-functions $L_E(s, \chi)$ at $s = 1$. It has been known since the work of Montgomery [13] that certain statistics on probability spaces of random matrices (as pair correlation between the eigenangles of the matrices) are similar to the same statistics on the zeroes of the Riemann zeta function. This intuition is supported by the extensive computations of Odlyzko [14] on the critical zeroes of the Riemann zeta function.

This was explored further in the work of Katz and Sarnak [8, 9], who extend the analogy between other probability spaces of matrices, and families of L-functions. Katz and Sarnak also studied the case of function fields, where they can actually prove some of those mysterious connections between random matrices and families of L-functions.

In order to study different statistics of number theoretic objects, Keating and Snaith [10, 11] introduced a new random variable on spaces of random matrices, the characteristic polynomial of the matrix evaluated at a given point. They computed the probability distribution of this new variable, which led to striking conjectures for the asymptotic behavior of the moments of the Riemann zeta function on the critical

line. The ideas of Keating and Snaith have been applied to study vanishing of L-functions in families [3, 5, 17]. Families of quadratic twists are studied in [3], where a conjectural asymptotic for the number of quadratic twists with even non-zero rank is presented. This refines a conjecture of Goldfeld [6] which predicts that quadratic twists with rank greater than one have density zero. In [5], the authors used the ideas of Keating and Snaith to obtain a conjectural asymptotic for the number of cubic Dirichlet characters χ such that $L_E(1,\chi)$ vanishes. We present in this paper the case of characters of order k, for k any odd prime. More precisely, the conjectures that we obtain from the random matrix model are (the case $k=3$ of [5] is included for completeness):

Conjecture 1.2. *Let k be an odd prime, let E be an elliptic curve defined over $\mathbb{Q}$, and let*

$$N_{E,k}(X) \;=\; \#\left\{\chi \text{ of order } k \;:\; cond(\chi) \leq X \text{ and } L_E(1,\chi)=0\right\}.$$

If $k=3$, then

$$\log N_{E,k}(X) \;\sim\; \frac{1}{2}\log X \quad \text{as } X\to\infty.$$

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 $k\geq 7$, then $N_{E,k}(X)$ is bounded.

In the light of (1), and under the Birch and Swinnerton-Dyer conjecture, one can rewrite $N_{E,k}(X)$ as

$$\begin{aligned} N_{E,k}(X) \;=\; & (k-1)\,\#\left\{K/\mathbb{Q} \text{ cyclic of degree } k \;:\right. \\ & \left. \operatorname{cond}(K)\leq X \text{ and } r_K(E) > r_{\mathbb{Q}}(E)\right\}. \end{aligned}$$

The structure of the paper is as follows. In the second section, we use modular symbols to rewrite the special values $L_E(1,\chi)$ as a product of terms depending only on E, and some algebraic integer $n_E(\chi)$ depending on the character. In the third section, we use the embedding of number fields as lattices in $\mathbb{C}$ to give a discretisation of the algebraic integers $n_E(\chi)$. In the fourth section, we use this discretisation and the work of Keating and Snaith to obtain conjectures on the asymptotic behavior of $N_{E,k}(X)$. Finally, the last section presents some experimental results.

2. Special values and modular symbols

The notation of this section follows the introduction of [12]. Let E be an elliptic curve over $\mathbb{Q}$. By the work of [16, 15, 1], E is modular and let $f(z)=\sum_{n\geq 1} a_n\, e^{2\pi i n z}$ be the Fourier expansion of the modular

form associated to E. Then, the the L-function $L_E(s)$ is the Mellin transform

$$L_E(s) = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty f(it) t^{s-1}\, dt. \tag{2}$$

$L_E(s)$ has analytic continuation to the whole complex plane, and satisfies the functional equation

$$\Lambda_E(s) = \left(\frac{\sqrt{N_E}}{2\pi}\right)^s \Gamma(s) L_E(s) = w_E \Lambda_E(2-s) \tag{3}$$

where $w_E = \pm 1$ is called the root number. From (2), we have that $L_E(1) = 2\pi \int_0^\infty f(it)\, dt$. For $a, m \in \mathbb{Q}, m > 0$, one defines the modular symbols

$$\lambda(a,m;E) \;=\; \lambda(a,m;f) = 2\pi \int_0^\infty f\left(it - \frac{a}{m}\right) dt. \tag{4}$$

Let χ be a primitive character of modulus m with Gauss sum

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

The twisted L-function $L_E(s,\chi)$ satisfies the functional equation

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

From the identity

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{a \bmod \mathrm{m}} \overline{\chi}(a) e^{2\pi i a n/m},$$

we have

$$\begin{aligned} f_\chi(z) &= \sum_{n \geq 1} \chi(n) a_n e^{2\pi i n z} \\ &= \frac{1}{\tau(\overline{\chi})} \sum_{a \bmod \mathrm{m}} \overline{\chi}(a) f\left(z + a/m\right) \end{aligned}$$

by rearranging the sums (Birch's lemma). It then follows that

$$L_E(1,\chi) \;=\; \frac{1}{\tau(\overline{\chi})} \sum_{a \bmod \mathrm{m}} \overline{\chi}(a) \lambda(a,m;E). \tag{5}$$

We define

$$\begin{aligned}\lambda^+(a,m;E) &= \lambda(a,m;E)+\lambda(-a,m;E)\\ &= 2\pi\int_0^\infty \sum_{n\geq 1} a_n\, e^{-2\pi nt}\,\left(e^{2\pi ian/m}+e^{-2\pi ian/m}\right)dt\\ &= 4\pi\sum_{n\geq 1} a_n\left(\mathrm{Re}\left\{e^{2\pi ian/m}\right\}\right)\int_0^\infty e^{-2\pi nt}dt\\ &= 2\sum_{n\geq 1}\frac{a_n}{n}\,\mathrm{Re}\left\{e^{2\pi ian/m}\right\}\end{aligned}$$

which is a real number as E is defined over $\mathbb{Q}$. As in [12], there is a rational multiple Ω_E of the real period such that all $\lambda^+(a,m;E)$ satisfy

$$\Lambda(a,m;E)=\frac{\lambda^+(a,m;E)}{\Omega_E}\in\mathbb{Z}.$$

In this paper, χ has prime order $k\geq 3$. Then, $\chi(-1)=1$, and we can rewrite (5) as

$$L_E(1,\chi) = \frac{\Omega_E}{2\tau(\overline{\chi})}\sum_{a \bmod m}\overline{\chi}(a)\Lambda(a,m;E) \tag{6}$$

where the integers $\Lambda(a,m;E)$ do not depend on the character χ, but only on the conductor m. Then, we see from (6) that

$$\frac{2\tau(\overline{\chi})L_E(1,\chi)}{\Omega_E}$$

is an algebraic integer in the field obtained by adding a kth root of unity. In fact, one can prove the stronger result which is critical to the discretisation of the next section. The particular case $k=3$ was proven in [5]. For any odd prime k, let $\mathbb{Q}(\xi_k)$ be the cyclotomic field obtained by adding a primitive kth root of unity ξ_k, and let $\mathbb{Q}(\xi_k)^+$ be the maximal real extension $\mathbb{Q}\subseteq\mathbb{Q}(\xi_k)^+\subseteq\mathbb{Q}(\xi_k)$ of degree $(k-1)/2$ over $\mathbb{Q}$. The ring of integers of $\mathbb{Q}(\xi_k)^+$ will be denoted by $\mathbb{Z}[\xi_k]^+$.

Theorem 2.1. *Let k be an odd prime, and let χ be a primitive character of order k. Then,*

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

where $n_E(\chi)\in\mathbb{Z}[\xi_k]\cap\mathbb{R}=\mathbb{Z}[\xi_k]^+$.

Proof: From the functional equation, we have

$$\begin{aligned} L_E^{alg}(1,\chi) &= \frac{2\tau(\overline{\chi})L_E(1,\chi)}{\Omega_E} = \frac{2\tau(\overline{\chi})w_E\chi(N_E)\tau(\chi)^2}{m\Omega_E}L_E(1,\overline{\chi}) \\ &= w_E\chi(N_E)\overline{\frac{2\tau(\overline{\chi})L_E(1,\chi)}{\Omega_E}} = w_E\chi(N_E)\overline{L_E^{alg}(1,\chi)} \end{aligned}$$

Let $z \in \mathbb{C}^*$ satisfying $z = w_E\chi(N_E)\overline{z}$. Then, $L_E^{alg}(1,\chi) = \alpha\overline{z}^{-1}$ with α real. If $w_E = 1$, we take $z = \chi(N_E)^{(k+1)/2}$, and $L_E^{alg}(1,\chi) = \alpha\overline{z}^{-1}$ with $\alpha \in \mathbb{R} \cap \mathbb{Z}[\xi_k] = \mathbb{Z}[\xi_k]^+$, which gives the result.
If $w_E = -1$, we take $z = \left(\xi_k - \xi_k^{-1}\right)\chi(N_E)^{(k+1)/2}$, and $L_E^{alg}(1,\chi) = \alpha\overline{z}^{-1}$ with $\alpha \in \mathbb{R} \cap \mathbb{Z}[\xi_k] = \mathbb{Z}[\xi_k]^+$, which gives the result. □

3. Discretisation

By Theorem 2.1, $n_E(\chi)$ is an algebraic integer in $\mathbb{Z}[\xi_k]^+$, and there is then a natural discretisation on the algebraic integer $n_E(\chi)$ given by the geometry of numbers. Let ϕ be the map

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

where $\mathrm{Gal}(\mathbb{Q}(\xi_k)^+/\mathbb{Q}) = \left\{\sigma_1 = 1, \sigma_2, \ldots, \sigma_{(k-1)/2}\right\}$. Let $\alpha_1, \ldots, \alpha_{(k-1)/2}$ be an integral basis for $\mathbb{Z}[\xi_k]^+$. 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 region

$$\begin{aligned} R = \big\{ & a_1\omega_1 + a_2\omega_2 + \cdots + a_{(k-1)/2}\omega_{(k-1)/2} : \\ & -1 < a_i < 1 \text{ for } 1 \le i \le (k-1)/2 \big\}. \end{aligned}$$

The discretisation given by the embedding of $\mathbb{Z}[\xi_k]^+$ in $\mathbb{R}^{(k-1)/2}$ is then

$$n_E(\chi) = 0 \iff \phi(n_E(\chi)) \in R. \tag{7}$$

Let χ 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 a character of conductor m and order k.

Lemma 3.1. *Let k be an odd prime, and χ a character of order k and conductor m. For any σ in $Gal(\mathbb{Q}(\xi_k)/\mathbb{Q})$, 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.

Proof: Using (6), we have

$$\begin{aligned} L_E^{alg}(1,\chi)^\sigma &= \left(\frac{2\tau(\overline{\chi})L_E(1,\chi)}{\Omega_E}\right)^\sigma \\ &= \sum_{a \bmod m} \overline{\chi}^\sigma(a)\Lambda(a,m;E) = L_E^{alg}(1,\chi^\sigma). \end{aligned}$$

Suppose first that $\omega_E = 1$. Then,

$$\begin{aligned} n_E(\chi)^\sigma &= L_E^{alg}(1,\chi)^\sigma \left(\chi(N_E)^{(k+1)/2}\right)^\sigma \\ &= \frac{2\tau(\overline{\chi}^\sigma)L_E(1,\chi^\sigma)}{\Omega_E}\left(\chi(N_E)^{(k+1)/2}\right)^\sigma, \end{aligned}$$

and taking absolute values we get the result with $c_{E,k} = \Omega_E/2$. The proof for $\omega_E = -1$ is similar, with a different explicit constant $c_{E,k}$. □

We first consider the case $k = 5$. We have that $\mathbb{Z}[\xi_5]^+ = \mathbb{Z}[\alpha]$ with $\alpha = (1+\sqrt{5})/2$, and $G_5 = \langle 1, \tau\rangle$, where the non-trivial automorphism τ sends $\sqrt{5}$ to $-\sqrt{5}$. Then, the lattice of $\mathbb{Z}[\alpha]$ in $\mathbb{R}^2$ is generated by $\omega_1 = (\alpha, \alpha^\tau)$ and $\omega_2 = (\alpha^\tau, \alpha)$. Let R be the region

$$R = \{a\omega_1 + b\omega_2 : -1 < a < 1, -1 < b < 1\}.$$

By (7), $n_E(\chi) = 0$ if and only if $\phi(n_E(\chi)) = (n_E(\chi), n_E(\chi)^\tau) \in R$. As the region R is not symmetric with respect to the absolute value, and we have a probability model for $|L_E(1,\chi)|$, we also consider the two regions of $\mathbb{R}^2$

$$\begin{aligned} R_1 &= \{(x,y) \;:\; -1 < x, y < 1\} \\ R_2 &= \left\{(x,y) \;:\; -\sqrt{5} < x, y < \sqrt{5}\right\} \end{aligned}$$

with the property that $R_1 \subseteq R \subseteq R_2$, and

$$(8) \qquad (n_E(\chi), n_E(\chi)^\tau) \in R_i \iff (|n_E(\chi)|, |n_E(\chi)^\tau|) \in |R_i|$$

where

$$|R_i| = \{(x,y) \in R_i \;:\; x, y \geq 0\}.$$

The following lemma is now immediate from (8) and Lemma 3.1

Lemma 3.2. *Let $\sigma \in Gal(\mathbb{Q}(\xi_5)/\mathbb{Q})$ be an automorphism which restricts to the non-trivial automorphism of $\mathbb{Q}(\sqrt{5})$. For $i = 1, 2$, we have*

$$(n_E(\chi), n_E(\chi)^\sigma) \in R_i \iff |L_E(1,\chi)|, |L_E(1,\chi^\sigma)| \leq \frac{c_i}{\sqrt{m}}$$

where c_1, c_2 are explicit constants depending only on E.

We now suppose that $k \geq 7$. Let B be the non-zero constant

$$B = \max_{1 \leq i \leq (k-1)/2} \sum_{j=1}^{(k-1)/2} |\sigma_i(\alpha_j)|,$$

and let $R \subseteq R' \subseteq \mathbb{R}^{(k-1)/2}$ be the region

$$R' = \left\{(x_1, \dots, x_{(k-1)/2}) \ : \ -B \leq x_i \leq B \text{ for } 1 \leq i \leq (k-1)/2.\right\}$$

Then, $n_E(\chi) = 0 \Rightarrow \phi(n_E(\chi)) \in R'$ by (7). The following lemma is now immediate from Lemma 3.1

Lemma 3.3. *Let $\sigma_1, \dots, \sigma_{(k-1)/2} \in Gal(\mathbb{Q}(\xi_k)/\mathbb{Q})$ be a set of representatives for $G_k = Gal(\mathbb{Q}(\xi_k)^+/\mathbb{Q})$. Then, $\phi(n_E(\chi)) \in R'$ if and only if*

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

where c_k is an explicit constant depending only E and k.

4. Unitary Random Matrices

Let $U(N)$ be the set of unitary $N \times N$ matrices with complex coefficients which forms a probability space with respect to the Haar measure. For each $A \in U(N)$, let

$$P_A(\lambda) = \det(A - \lambda I)$$

be the characteristic polynomial of A. For any $s \in \mathbb{C}$, let

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

be the moments for the distribution of $|P_A(1)|$ in $U(N)$ with respect to the Haar measure. In [10], Keating and Snaith proved that

$$M_U(s, N) = \prod_{j=1}^{N} \frac{\Gamma(j)\Gamma(j+s)}{\Gamma^2(j + s/2)}, \tag{9}$$

and then $M_U(s,N)$ is analytic for $\mathrm{Re}(s) > -1$, and has meromorphic continuation to the whole complex plane. By Fourier inversion, the probability density of $|P_A(1)|$ is

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

for some $c > -1$. Then, for any $I \subseteq \mathbb{R}$,

$$\mathrm{Prob}\left(|P_A(1)| \in I\right) = \int_I p(x)\, dx.$$

In our application to the vanishing of twisted L-functions, we will be interested only in small values of x where the value of $p(x)$ is determined by the first pole of $M_U(s,N)$ at $s=-1$. More precisely, for

$$x \leq N^{-1/2},$$

one can show that

$$p(x) \sim G^2(1/2)N^{1/4} \quad \text{as } N \to \infty,$$

where $G(z)$ is the Barnes G-function, with special value

$$G(1/2) = \exp\left(\frac{3}{2}\zeta'(-1) - \frac{1}{4}\log\pi + \frac{1}{24}\log 2\right)$$

(see [10, p. 81] or [7, p. 58] for more details).

We now consider the moments for the special values of L-functions in families of twists. Fix $k \geq 3$, and let

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

with an explicit constant b_k (see for example [2]). We then define for any $s \in \mathbb{C}$

$$M_E(s,X) = \frac{1}{N_k(X)}\sum_{\chi \in S_k(X)} |L_E(1,\chi)|^s \tag{10}$$

The family of twists of order k has unitary symmetry, as the values $|\zeta(1/2+it)|$ on the critical line. Then

Conjecture 4.1 (Keating and Snaith Conjecture for twists of order k)**.**

$$M_E(s,X) \sim a_E(s/2)M_U(s,N) \quad \textit{as } N = 2\log X \to \infty,$$

where $a_E(s/2)$ is an arithmetic factor depending only on the curve E.

In the conjecture, the relation between N and X is obtained by equating the mean density of eigenangles of matrices in the unitary group, and the mean density of non-trivial zeroes of the twisted L-functions $L_E(s,\chi)$ at a fixed height (see [5]). The arithmetic factor $a_E(s)$ can not be obtained from the random matrix theory, and has to be determined separately for each family from its arithmetic. This was done for the family of cubic twists in [5], and could be done for the family of twists of order k for each k. The arithmetic factor $a_E(s)$ would then be a meromorphic function for all $s \in \mathbb{C}$. As it will be seen below, the only influence of the arithmetic factor $a_E(s)$ in our application is that the special value $a_E(-1/2)$ will be part of the constant of the conjectural asymptotic of $N_{E,k}(X)$. This would not provide any further information to the cases $k \geq 5$ considered in this paper considered in this paper in view of Conjecture 1.2.

From Conjecture 4.1, the probability density $p_E(x)$ for the distribution of the special values $|L_E(1,\chi)|$ for characters of order k is

$$\begin{aligned} p_E(x) &= \frac{1}{2\pi i}\int_{(c)} M_E(s,X)\, x^{-s-1}\, ds \\ &\sim \frac{1}{2\pi i}\int_{(c)} a_E(s/2)\, M_U(s,N)\, x^{-s-1}\, ds \end{aligned} \tag{11}$$

as $N = 2\log X \to \infty$. As above, when $x \leq N^{-1/2}$, the value of $p_E(x)$ is determined by the residue of $M_U(s,N)$ at $s=-1$, and it follows from (11) that

$$p_E(x) \sim C_E \log^{1/4} X \tag{12}$$

for $x \leq (2\log X)^{-1/2}$, $X \to \infty$, and $C_E = 2^{1/4} a_E(-1/2) G^2(1/2)$.

Let χ be a character of order $k \geq 3$ and conductor m. We apply the above model to find the probability that $|L_E(1,\chi)| < cm^{-1/2}$, for some constant $c > 0$. For $x < cm^{-1/2} < (2\log m)^{-1/2}$ (for m large enough), we have $p_E(x) \sim C_E \log^{1/4} m$, and then

$$\begin{aligned} \text{Prob}\left(|L_E(1,\chi)| < cm^{-1/2}\right) &\sim \int_0^{cm^{-1/2}} C_E \log^{1/4} m\, dx \\ &= c\, C_E \frac{\log^{1/4} m}{m^{1/2}}. \end{aligned} \tag{13}$$

We now use the probability density of the random matrix model with the discretisation of Section 3 to obtain conjectures for the vanishing of the L-values $L_E(1,\chi)$. We first suppose that $k=5$, and as in the previous section, let $\sigma \in \text{Gal}(\mathbb{Q}(\xi_5)/\mathbb{Q})$ which restricts to the non-trivial automorphism of $\mathbb{Q}(\sqrt{5})$. We saw in the previous two sections

that

$$L_E(1,\chi) = 0 \quad \Longleftrightarrow \quad \phi(n_E(\chi)) = (n_E(\chi), n_E(\chi)^\sigma) \in R.$$

As $R_1 \subseteq R \subseteq R_2$, and using Lemma 3.2, the probability that $L_E(1,\chi)$ is zero is bounded below by

$$\text{Prob}\left(|L_E(1,\chi)| < \frac{c_1}{\sqrt{m}}\right) \text{Prob}\left(|L_E(1,\chi^\sigma)| < \frac{c_1}{\sqrt{m}}\right)$$

and bounded above by

$$\text{Prob}\left(|L_E(1,\chi)| < \frac{c_2}{\sqrt{m}}\right) \text{Prob}\left(|L_E(1,\chi^\sigma)| < \frac{c_2}{\sqrt{m}}\right).$$

Assuming that $|L_E(1,\chi)|$ and $|L_E(1,\chi^\sigma)|$ are independent identically distributed random variables, and using (13), we get that the probability that $L_E(1,\chi)$ is zero is about

$$\frac{\log^{1/2} m}{m},$$

neglecting all constants which are not significant here. The sum of the probabilities is

$$\sum_{\chi \in S_3(X)} \frac{\log^{1/2} m}{m} \quad \sim \quad \frac{2b_3}{3} \log^{3/2} X. \tag{14}$$

As discussed in [5], the exact power of $\log X$ that is obtained with the random matrix approach depends subtly on the discretisation, and is difficult to predict. For examples, rational torsion of order three on the elliptic curve seemed to cause extra vanishing of the twisted L-values $L_E(1,\chi)$ for cubic characters, and changed the power of logarithm in the conjectural asymptotic for $N_{E,k}(X)$ of [5]. For $k = 5$, the sum of the probabilities is just on the border between convergence and divergence, and the random matrix model seems to indicate that the number of quintic twists such that $L_E(1,\chi)$ vanishes is infinite, but that $N_{E,k}(X) \ll X^\epsilon$ for any $\epsilon > 0$. This agrees with the empirical evidence of Section 5.

We now suppose that $k \geq 7$. Let $\sigma_1 = 1, \ldots, \sigma_{(k-1)/2}$ be elements of the Galois group of $\mathbb{Q}(\xi_k)/\mathbb{Q}$ which form a set of representatives for the Galois group of $\mathbb{Q}(\xi_k)^+/\mathbb{Q}$. As we saw in the two previous sections,

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

As $R \subseteq R'$, and using Lemma 3.3, the probability that $L_E(1,\chi)$ is zero is bounded by

$$\mathrm{Prob}\left(|L_E(1,\chi^{\sigma_1})| < \frac{c_k}{\sqrt{m}}\right), \ldots, \mathrm{Prob}\left(|L_E(1,\chi^{\sigma_{(k-1)/2}})| < \frac{c_k}{\sqrt{m}}\right).$$

Assuming that $|L_E(1,\chi^{\sigma_i})|$ are independent identically distributed random variables for $1 \leq i \leq (k-1)/2$, and using (13), we get that the probability that $L_E(1,\chi)$ is zero is

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

neglecting all constants which are not significant here. Summing the probabilities, this gives for $k \geq 7$

$$\sum_{\chi \in S_3(X)} \frac{\log^{(k-1)/8} m}{m^{(k-1)/4}} \quad = \quad O(1). \tag{15}$$

From the random matrix model, we then conjecture that the number of twists of order $k \geq 7$ such that $L_E(1,\chi)$ vanishes is bounded. This also agrees with the empirical evidence of Section 5.

5. Numerical Evidence

The following table shows the observed number of vanishing twists $L_E(1,\chi)$ for characters of orders three, five and seven, and for the first three elliptic curves in the Cremona catalogue [4]. For each elliptic curve E, the characters with conductor prime to N_E and less than two million were considered. Any two characters of conductor m and order k generating the same cyclic subgroup of the character group are conjugate, and hence the special values $L_E(1,\chi)$ vanish simultaneously by Lemma 3.1. The number in the table records one of each class of conjugate characters for which the special value vanishes, which is $1/(k-1)$ of the number of characters with vanishing special value. The twists of order eleven in the same range for the curve $E14$ were also computed, and no vanishing were found.

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

The results for cubic twists have been analyzed in [5] and support Conjecture 1.2. The results for quintic and septic twists are too sparse

to either support or refute Conjecture 1.2, but they nevertheless illustrate the extreme scarcity of vanishing in higher order twists which is predicted by the conjecture.

Acknowledgments This paper was first presented at the "Ranks of Elliptic Curves and Random Matrix Theory" workshop held at the Isaac Newton Institute in February 2004. The first and second authors would like to thank the organizers of the workshop and the Isaac Newton Institute for their hospitality and financial support. The first author would also like to thank B. Birch, B. Conrey and C. Hughes for helpful discussions.

References

[1] 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** (2001), 843–939 (electronic).

[2] H. Cohen, F. Diaz y Diaz and M. Olivier, A survey of discriminant counting, Algorithmic number theory (Sydney, 2002), 80–94, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002.

[3] J.B. Conrey, J.P. Keating, M. Rubinstein, N.C. Snaith, On the frequency of vanishing of quadratic twists of modular L-functions, Number theory for the Milennium I, 301–315, Editors: M. A. Bennett, B. C. Berndt, N. Boston NH. G. , Diamond, A. J. Hildebrand, W. Philipp, A. K. Peters Ltd, Natick, 2002.

[4] J. Cremona, Algorithms for modular elliptic curves, Cambridge University Press, Cambridge, UK, 1992.

[5] C. David, J. Fearnley and H. Kisilevsky, On the Vanishing of Twisted L-Functions of Elliptic Curves, *Experimental Mathematics*, 13 (2004), 185–198.

[6] D. Goldfeld, Conjectures on elliptic curves over quadratic fields, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), pp. 108–118, Lecture Notes in Math. **751**, Springer, Berlin, 1979.

[7] C. P. Hughes, On the characteristic polynomial of random unitary matrix and the Riemann zeta function, Ph.D. thesis, University of Bristol, England, 2001.

[8] N. M. Katz and P. Sarnak, Zeroes of zeta functions and symmetry, *Bull. Amer. Math. Soc. (N.S.)* **36** (1999), 1–26.

[9] N. M. Katz and P. Sarnak, Random matrices, Frobenius eigenvalues, and monodromy, American Mathematical Society Colloquium Publications **45**, American Mathematical Society, Providence, RI, 1999.

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

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

[12] B. Mazur, J. Tate and J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Invent. Math.* **84** (1986), 1–48.

[13] H. Montgomery, The pair correlation of zeroes of the zeta function, *Proc. Sym. Pure Math.* **24** (1973), 181–193.

[14] A. Odlyzko, The 10^{20}-th zero of the Riemann zeta function and 70 millions of his neighbors, preprint, A.T.T., 1989.
[15] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math. (2)* **141**, 553-572.
[16] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math. (2)* **141**, 443-551.
[17] M. Watkins, Rank distribution in a family of cubic twists, this volume.

Department of Mathematics and Statistics, Concordia University, 1455 de Maisonneuve Blvd. West, Montréal (Québec), Canada H3G 1M8

E-mail address, David: cdavid@mathstat.concordia.ca

E-mail address, Fearnley: jack@mathstat.concordia.ca

E-mail address, Kisilevsky: kisilev@mathstat.concordia.ca