Arithmetic Statistics and Mixed Moments of Elliptic Curve L-Functions over Function Fields

Jon Keating

School of Mathematics
University of Bristol

j.p.keating@bristol.ac.uk

July 11, 2019

Arithmetic Statistics

Arithmetic Statistics

Arithmetic statistics: Statistical properties of arithmetic functions, e.g. $\Lambda(n)$, $\mu(n)$, $d_k(n)$

Arithmetic Statistics

Arithmetic statistics: Statistical properties of arithmetic functions, e.g. $\Lambda(n)$, $\mu(n)$, $d_k(n)$

L-function statistics: Statistical properties of L-functions, e.g. zero-statistics, moments, etc

Arithmetic Statistics

Arithmetic statistics: Statistical properties of arithmetic functions, e.g. $\Lambda(n)$, $\mu(n)$, $d_k(n)$

L-function statistics: Statistical properties of L-functions, e.g. zero-statistics, moments, etc

Arithmetic and L-function statistics in function fields: Statistical properties of arithmetic functions and L-functions related to function fields defined over $\mathbb{F}_q$; e.g. $\Lambda(f)$, $\mu(f)$, $d_k(f)$ for f monic of degree k.

Arithmetic Statistics

Arithmetic statistics: Statistical properties of arithmetic functions, e.g. $\Lambda(n)$, $\mu(n)$, $d_k(n)$

L-function statistics: Statistical properties of L-functions, e.g. zero-statistics, moments, etc

Arithmetic and L-function statistics in function fields: Statistical properties of arithmetic functions and L-functions related to function fields defined over $\mathbb{F}_q$; e.g. $\Lambda(f)$, $\mu(f)$, $d_k(f)$ for f monic of degree k.

Limits: $k \to \infty$, or as the degree of the L-functions (considered as polynomials) grows, vs $q \to \infty$.

Primes in Short Intervals

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and integer } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

so that

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$$

Conjecture (Goldston & Montgomery, 1987; Montgomery & Soundararajan 2004)

For $X^\delta < H < X^{1-\delta}$, as $X \to \infty$

$$\frac{1}{X}\int_2^X \left| \sum_{n \in [x-\frac{H}{2}, x+\frac{H}{2}]} \Lambda(n) - H \right|^2 dx \sim H\Big(\log(X/H) - (\gamma_E + \log 2\pi)\Big)$$

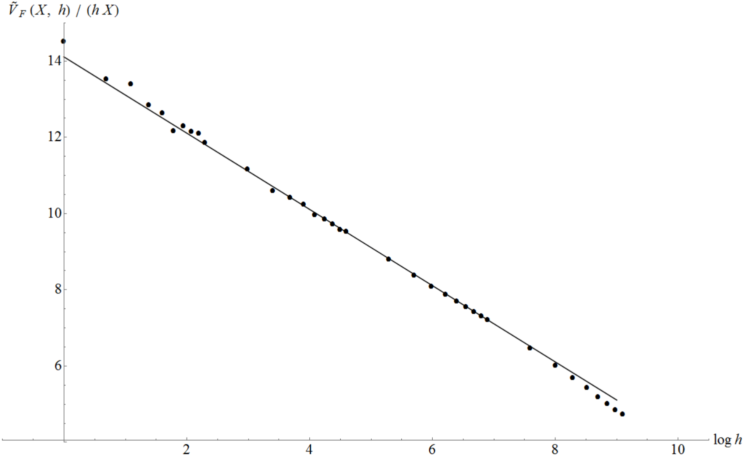

Figure 1. $\widetilde{V}_F(X,h)/(hX)$ plotted against $\log h$ when F is the Riemann zeta-function and $X = 15000000$ (•). The line is given by $y = -x + \log 15000000 - \gamma_0 - \log 2\pi$, which corresponds to $d_F = 1$ and $\mathfrak{q}_F = 1$.

Function Fields

Let $\mathbb{F}_q$ be a finite field of q elements and $\mathbb{F}_q[t]$ the ring of polynomials with coefficients in $\mathbb{F}_q$.

Function Fields

Let $\mathbb{F}_q$ be a finite field of q elements and $\mathbb{F}_q[t]$ the ring of polynomials with coefficients in $\mathbb{F}_q$.

Let $\mathcal{P}_n = \{f \in \mathbb{F}_q[t] : \deg f = n\}$ be the set of polynomials of degree n and $\mathcal{M}_n \subset \mathcal{P}_n$ the subset of monic polynomials.

Function Fields

Let $\mathbb{F}_q$ be a finite field of q elements and $\mathbb{F}_q[t]$ the ring of polynomials with coefficients in $\mathbb{F}_q$.

Let $\mathcal{P}_n = \{f \in \mathbb{F}_q[t] : \deg f = n\}$ be the set of polynomials of degree n and $\mathcal{M}_n \subset \mathcal{P}_n$ the subset of monic polynomials.

Define the norm of a polynomial $0 \neq f \in \mathbb{F}_q[t]$ to be

$$||f|| := q^{\deg f}$$

Function Fields

Let $\mathbb{F}_q$ be a finite field of q elements and $\mathbb{F}_q[t]$ the ring of polynomials with coefficients in $\mathbb{F}_q$.

Let $\mathcal{P}_n = \{f \in \mathbb{F}_q[t] : \deg f = n\}$ be the set of polynomials of degree n and $\mathcal{M}_n \subset \mathcal{P}_n$ the subset of monic polynomials.

Define the norm of a polynomial $0 \neq f \in \mathbb{F}_q[t]$ to be

$$||f|| := q^{\deg f}$$

Denote monic irreducible polynomials by P

Primes in Short Intervals: function field analogue

Define

$$\Lambda(f) = \begin{cases} \deg P & \text{if } f = P^k \text{ for some irreducible polynomial } P, \\ 0 & \text{otherwise.} \end{cases}$$

and

$$I(A;h) := \{f : ||f - A|| \leq q^h\} = A + \mathcal{P}_{\leq h}$$

Primes in Short Intervals: function field analogue

Define

$$\Lambda(f) = \begin{cases} \deg P & \text{if } f = P^k \text{ for some irreducible polynomial } P, \\ 0 & \text{otherwise.} \end{cases}$$

and

$$I(A;h) := \{f : ||f - A|| \leq q^h\} = A + \mathcal{P}_{\leq h}$$

Theorem (variance in intervals – JPK & Z. Rudnick, 2014)

Let $h < n - 3$. Then

$$\lim_{q\to\infty} \frac{1}{q^{h+1}} \mathrm{Var}_A\Big(\sum_{\substack{f\in I(A,h)\\ f(0)\neq 0}} \Lambda(f)\Big) = \int_{U(n-h-2)} |\mathrm{tr}\, U^n|^2 dU = n - h - 2$$

This is the exact analogue of the Goldston-Montgomery-Soundararajan formula.

Arithmetic progressions

In the same vein:

Theorem (variance in arithmetic progressions – JPK & Z. Rudnick, 2014)

Given a sequence of finite fields $\mathbb{F}_q$ and square-free polynomials $Q \in \mathbb{F}_q[t]$ with $2 \leq \deg(Q) \leq n+1$,

$$\sum_{\substack{A \bmod Q \\ \gcd(A,Q)=1}} \left| \sum_{\substack{f \in \mathcal{M}_n \\ f \equiv A \bmod Q}} \Lambda(f) - \frac{q^n}{\Phi(Q)} \right|^2 \sim q^n(\deg(Q)-1)$$

as $q \to \infty$.

This is the exact analogue of a formula in the number field setting conjectured by Hooley.

Ideas behind Proofs

- use characters to restrict sums over polynomials to subsets of $\mathcal{M}_n$ (intervals and arithmetic progressions)

Ideas behind Proofs

- use characters to restrict sums over polynomials to subsets of $\mathcal{M}_n$ (intervals and arithmetic progressions)
- this leads to expressions in terms of the associated L-functions

Ideas behind Proofs

- use characters to restrict sums over polynomials to subsets of $\mathcal{M}_n$ (intervals and arithmetic progressions)
- this leads to expressions in terms of the associated L-functions
- these L-functions can be expressed in terms of unitary matrices (Riemann Hypothesis)

Ideas behind Proofs

- use characters to restrict sums over polynomials to subsets of $\mathcal{M}_n$ (intervals and arithmetic progressions)
- this leads to expressions in terms of the associated L-functions
- these L-functions can be expressed in terms of unitary matrices (Riemann Hypothesis)
- in the limit as $q \to \infty$ use equidistribution (proved by N. Katz) to express the character sums as matrix integrals

Ideas behind Proofs

- use characters to restrict sums over polynomials to subsets of $\mathcal{M}_n$ (intervals and arithmetic progressions)
- this leads to expressions in terms of the associated L-functions
- these L-functions can be expressed in terms of unitary matrices (Riemann Hypothesis)
- in the limit as $q \to \infty$ use equidistribution (proved by N. Katz) to express the character sums as matrix integrals
- recognize/evaluate the integrals

Generalization of the Goldston-Montgomery-Soundararajan Formula (Bui, K & Smith, 2016)

Let $\mathcal{S}$ denote the Selberg class L-functions. For $F \in \mathcal{S}$ primitive,

$$F(s) = \sum_{n=1}^{\infty} \frac{a_F(n)}{n^s} = \prod_p \exp\left(\sum_{l=1}^{\infty} \frac{b_F(p^l)}{p^{ls}} \right).$$

satisfying the *functional equation*

$$\Phi(s) := Q^s \left(\prod_{j=1}^{r} \Gamma(\lambda_j s + \mu_j) \right) F(s) = \varepsilon_F \overline{\Phi}(1-s),$$

with some $Q > 0$, $\lambda_j > 0$, $\mathrm{Re}(\mu_j) \geq 0$ and $|\varepsilon_F| = 1$.
This determines the degree d_F and the conductor $\mathfrak{q}_F$:

$$d_F = 2\sum_{j=1}^{r} \lambda_j \qquad \text{and} \qquad \mathfrak{q}_F = (2\pi)^{d_F} Q^2 \prod_{j=1}^{r} \lambda_j^{2\lambda_j}.$$

Define

$$\frac{F'}{F}(s) = -\sum_{n=1}^{\infty} \frac{\Lambda_F(n)}{n^s} \qquad (\mathrm{Re}(s) > 1).$$

Then for $X^{1-1/d_F} < H < X^{1-\delta}$, as $X \to \infty$

$$\frac{1}{X}\int_2^X \left| \sum_{n\in[x-\frac{H}{2},x+\frac{H}{2}]} \Lambda_F(n) \right|^2 dx \sim H\Big(\log(X/H) + \log \mathfrak{q}_F - (\gamma_E - \log 2\pi) d_F \Big)$$

Define

$$\frac{F'}{F}(s) = -\sum_{n=1}^{\infty} \frac{\Lambda_F(n)}{n^s} \qquad (\mathrm{Re}(s) > 1).$$

Then for $X^{1-1/d_F} < H < X^{1-\delta}$, as $X \to \infty$

$$\frac{1}{X}\int_2^X \left| \sum_{n\in[x-\frac{H}{2},x+\frac{H}{2}]} \Lambda_F(n) \right|^2 dx \sim H\Big(\log(X/H) + \log \mathfrak{q}_F - (\gamma_E - \log 2\pi) d_F \Big)$$

and for $X^{\delta} < H < X^{1-1/d_F}$, as $X \to \infty$

$$\frac{1}{X}\int_2^X \left| \sum_{n\in[x-\frac{H}{2},x+\frac{H}{2}]} \Lambda_F(n) \right|^2 dx \sim \frac{1}{6} H\Big(6\log X - (3 + 8\log 2) \Big)$$

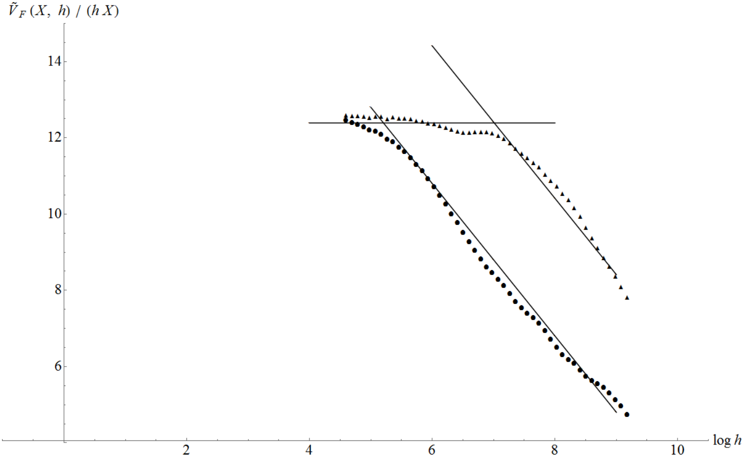

Figure 2. $\widetilde{V}_F(X,h)/(hX)$ plotted against $\log h$ when F is associated with the Ramanujan τ-function (●) and with an elliptic curve of conductor 37 (▲). Here $X = 1000000$. The horizontal line is given by $y = \log 1000000 - \frac{(3+8\log 2)}{6}$. The slanted lines are given by $y = -2x + 2(\log 1000000 - \gamma_0 - \log 2\pi)$, which corresponds to the case $d_F = 2$ and $\mathfrak{q}_F = 1$ for the Ramanujan τ-function, and $y = -2x + 2(\log 1000000 - \gamma_0 - \log 2\pi) + \log 37$, which corresponds to the case $d_F = 2$ and $\mathfrak{q}_F = 37$ for the elliptic curve.

Example: Elliptic Curve L-functions

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N defined over $\mathbb{Q}$ with L-function

$$L(s,E) = \prod_{p|N}(1 - a_p p^{-s-1/2})^{-1} \prod_{p\nmid N}(1 - a_p p^{-s-1/2} + p^{-2s})^{-1}$$

where $a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p)$. When $p \mid N$, then a_p is either 1, -1, or 0. In general, $|a_p| < 2\sqrt{p}$. Hence can write

$$\frac{a_p}{p^{1/2}} = 2\cos(\theta_p) = \alpha_p + \beta_p$$

where, for $p \nmid N$, one has $\alpha_p = e^{i\theta_p}$ and $\beta_p = e^{-i\theta_p}$ with $\theta_p \in [0, \pi]$ and for $p \mid N$, one has $\alpha_p = a_p$, and $\beta_p = 0$.

Define Λ_E by

$$\frac{L(s,E)'}{L(s,E)} = -\sum_{n=1}^{\infty} \Lambda_E(n) n^{-s},$$

so that for $e \geq 1$

$$\Lambda_E(n) = \begin{cases} \log p \cdot (\alpha_p^e + \beta_p^e) & \text{if } n = p^e \text{ with } p \text{ prime} \\ 0 & \text{otherwise.} \end{cases}$$

Denote the variance of the sum of Λ_E in arithmetic progressions, for example, by

$$S_{x,c,E}(A) := \sum_{\substack{n \leq x \\ n = A \bmod c}} \Lambda_E(n).$$

Define Λ_E by

$$\frac{L(s,E)'}{L(s,E)} = -\sum_{n=1}^{\infty} \Lambda_E(n) n^{-s},$$

so that for $e \geq 1$

$$\Lambda_E(n) = \begin{cases} \log p \cdot (\alpha_p^e + \beta_p^e) & \text{if } n = p^e \text{ with } p \text{ prime} \\ 0 & \text{otherwise.} \end{cases}$$

Denote the variance of the sum of Λ_E in arithmetic progressions, for example, by

$$S_{x,c,E}(A) := \sum_{\substack{n \leq x \\ n = A \bmod c}} \Lambda_E(n).$$

Then for $x^\epsilon < c < x^{1-\epsilon}$, $\epsilon > 0$ the prediction is

$$\mathrm{Var}_A(S_{x,c,E}) \sim \frac{x}{\phi(c)} \min\{\log x, 2\log c\}.$$

Function Field Analogues

The corresponding formulae for the variance of the sum of $\Lambda_E(n)$ over arithmetic progressions (Hall, K & Roditty-Gershon) and short intervals (Sawin) hold (unconditionally) when $q \to \infty$ for the function field analogues of elliptic curve L-functions.

Explicit Example

Suppose q is an odd prime power, and let $E_{\mathrm{Leg}}/\mathbb{F}_q(t)$ be the Legendre curve, that is, the elliptic curve with affine model

$$y^2 = x(x-1)(x-t).$$

Over the ring $\mathbb{F}_q[t]$, this curve has conductor $s = t(t-1)$. The corresponding L-function is given by the Euler product

$$L(T, E_{\mathrm{Leg}}/\mathbb{F}_q(t)) = \prod_P L(T^{\deg(P)}, E_{\mathrm{Leg}}/\mathbb{F}_P)^{-1}$$

where $\mathbb{F}_P$ is the residue field $\mathbb{F}_q[t]/P\mathbb{F}_q[t]$.
Each Euler factor is the reciprocal of a polynomial and satisfies

$$T\frac{d}{dT}\log L(T, E_{\mathrm{Leg}}/\mathbb{F}_P)^{-1} = \sum_{m=1}^{\infty} a_{P,m} T^m \in \mathbb{Z}[[T]].$$

Define $\Lambda_{\mathrm{Leg}}(f)$ by

$$\Lambda_{\mathrm{Leg}}(f) = \begin{cases} \deg(P) \cdot a_{P,m} & \text{if } f = P^m \\ 0 & \text{otherwise,} \end{cases}$$

then the L-function satisfies

$$T \frac{d}{dT} \log(L(T, E_{\mathrm{Leg}}/\mathbb{F}_q(t))) = \sum_{n=1}^{\infty} \left(\sum_{f \in \mathcal{M}_n} \Lambda_{\mathrm{Leg}}(f) \right) T^n.$$

Let $Q \in \mathbb{F}_q[t]$ be monic and square-free. For each $n \geq 1$ and each A in $\Gamma(Q) = (\mathbb{F}_q[t]/Q\mathbb{F}_q[t])^\times$, consider the sum

$$S_{n,Q}(A) \; := \sum_{\substack{f \in \mathcal{M}_n \\ f \equiv A \bmod Q}} \Lambda_{\mathrm{Leg}}(f).$$

Let A vary uniformly over $\Gamma(Q)$.

Theorem (C. Hall, JPK, E. Roditty-Gershon)

If $\gcd(Q, s) = t$ *and if* $\deg(Q)$ *is sufficiently large, then*

$$\lim_{q\to\infty} \frac{|\Gamma(Q)|}{q^{2n}} \cdot \mathrm{Var}_A[S_{n,Q}(A)] = \min\{n, 2\deg(Q) - 1\}.$$

Let A vary uniformly over $\Gamma(Q)$.

Theorem (C. Hall, JPK, E. Roditty-Gershon)

If $\gcd(Q, s) = t$ *and if* $\deg(Q)$ *is sufficiently large, then*

$$\lim_{q\to\infty} \frac{|\Gamma(Q)|}{q^{2n}} \cdot \mathrm{Var}_A[S_{n,Q}(A)] = \min\{n, 2\deg(Q) - 1\}.$$

- The fact that the expression for the variance depends on $2\deg(Q)$ is a direct consequence of the fact that the associated L-functions have degree two. (For an L-function of degree r, one will get a leading term of $r\deg(Q)$ instead.) This then leads to there being two ranges.

Let A vary uniformly over $\Gamma(Q)$.

Theorem (C. Hall, JPK, E. Roditty-Gershon)

If $\gcd(Q, s) = t$ *and if* $\deg(Q)$ *is sufficiently large, then*

$$\lim_{q\to\infty} \frac{|\Gamma(Q)|}{q^{2n}} \cdot \mathrm{Var}_A[S_{n,Q}(A)] = \min\{n, 2\deg(Q) - 1\}.$$

- The fact that the expression for the variance depends on $2\deg(Q)$ is a direct consequence of the fact that the associated L-functions have degree two. (For an L-function of degree r, one will get a leading term of $r\deg(Q)$ instead.) This then leads to there being two ranges.
- This two-range phenomenon has subsequently been found to be important in, e.g., the distribution of angles of Gaussian primes by Rudnick & Waxman.

Let A vary uniformly over $\Gamma(Q)$.

Theorem (C. Hall, JPK, E. Roditty-Gershon)

If $\gcd(Q,s) = t$ *and if* $\deg(Q)$ *is sufficiently large, then*

$$\lim_{q\to\infty} \frac{|\Gamma(Q)|}{q^{2n}} \cdot \mathrm{Var}_A[S_{n,Q}(A)] = \min\{n, 2\deg(Q) - 1\}.$$

- The fact that the expression for the variance depends on $2\deg(Q)$ is a direct consequence of the fact that the associated L-functions have degree two. (For an L-function of degree r, one will get a leading term of $r\deg(Q)$ instead.) This then leads to there being two ranges.
- This two-range phenomenon has subsequently been found to be important in, e.g., the distribution of angles of Gaussian primes by Rudnick & Waxman.
- (NB the same multiple-range behaviour arises in sufficiently high moments of the zeta function (c.f. Brian Conrey's talk))

Derivatives of Elliptic Curve L-functions and Applications to Rank Correlations

Derivatives of Elliptic Curve L-functions and Applications to Rank Correlations

- The first moment of the family of derivatives of L–functions of quadratic twists of a fixed modular form was computed by Bump-Friedberg & Hoffstein, Iwaniec, and Murty & Murty in 1990, with applications to non-vanishing;

Derivatives of Elliptic Curve L-functions and Applications to Rank Correlations

- The first moment of the family of derivatives of L–functions of quadratic twists of a fixed modular form was computed by Bump-Friedberg & Hoffstein, Iwaniec, and Murty & Murty in 1990, with applications to non-vanishing;
- e.g. for a fixed elliptic curve with root number equal to 1 there are infinitely many fundamental discriminants $d < 0$ such that its twist by d has analytic rank equal to 1.

Derivatives of Elliptic Curve L-functions and Applications to Rank Correlations

- The first moment of the family of derivatives of L–functions of quadratic twists of a fixed modular form was computed by Bump-Friedberg & Hoffstein, Iwaniec, and Murty & Murty in 1990, with applications to non-vanishing;
- e.g. for a fixed elliptic curve with root number equal to 1 there are infinitely many fundamental discriminants $d < 0$ such that its twist by d has analytic rank equal to 1.
- The second moment of this family was considered by Soundararajan & Young in 2010.

Derivatives of Elliptic Curve L-functions and Applications to Rank Correlations

- The first moment of the family of derivatives of L–functions of quadratic twists of a fixed modular form was computed by Bump-Friedberg & Hoffstein, Iwaniec, and Murty & Murty in 1990, with applications to non-vanishing;
- e.g. for a fixed elliptic curve with root number equal to 1 there are infinitely many fundamental discriminants $d < 0$ such that its twist by d has analytic rank equal to 1.
- The second moment of this family was considered by Soundararajan & Young in 2010.
- Petrow recently obtained several asymptotic formulas for moments of derivatives of these $GL(2)$ L–functions when the sign of the functional equation is -1 (on GRH).

In Function Fields (H. Bui, A. Florea, JPK & E. Roditty-Gershon)

Fix a prime power q with $(q, 6) = 1$ and $q \equiv 1 \pmod 4$. Let $K = \mathbb{F}_q(t)$ be the rational function field and $\mathcal{O}_K = \mathbb{F}_q[t]$. Let E/K be an elliptic curve defined by $y^2 = x^3 + ax + b$, with $a, b \in \mathcal{O}_K$ and discriminant $\Delta = 4a^3 + 27b^2$ such that $\deg_t(\Delta)$ is minimal among models of E/K of this form.

In Function Fields (H. Bui, A. Florea, JPK & E. Roditty-Gershon)

Fix a prime power q with $(q,6)=1$ and $q \equiv 1 \pmod 4$. Let $K=\mathbb{F}_q(t)$ be the rational function field and $\mathcal{O}_K=\mathbb{F}_q[t]$. Let E/K be an elliptic curve defined by $y^2=x^3+ax+b$, with $a,b\in\mathcal{O}_K$ and discriminant $\Delta=4a^3+27b^2$ such that $\deg_t(\Delta)$ is minimal among models of E/K of this form.
The associated L–function may be written (for $\Re(s)>1$),

$$\begin{aligned} L(E,s) := \mathcal{L}(E,u) &= \sum_{f\in\mathcal{M}} \lambda(f)u^{\deg(f)} \\ &= \prod_{P\mid\Delta}\left(1-\lambda(P)u^{\deg(P)}\right)^{-1}\prod_{P\nmid\Delta}\left(1-\lambda(P)u^{\deg(P)}+u^{2\deg(P)}\right)^{-1}, \end{aligned}$$

where we set $u:=q^{-s}$, and $\mathcal{M}$ denotes the set of monic polynomials over $\mathbb{F}_q[t]$.

The L–function is a polynomial in u with integer coefficients of degree

$$\mathfrak{n} := \deg\left(\mathcal{L}(E,u)\right) = \deg(M) + 2\deg(A) - 4,$$

where we denote by M the product of the finite primes where E has multiplicative reduction and by A the product of the finite primes where E has additive reduction.

The L–function is a polynomial in u with integer coefficients of degree

$$\mathfrak{n} := \deg\big(\mathcal{L}(E,u)\big) = \deg(M) + 2\deg(A) - 4,$$

where we denote by M the product of the finite primes where E has multiplicative reduction and by A the product of the finite primes where E has additive reduction. The L–function satisfies the functional equation

$$\mathcal{L}(E,u) = \epsilon(E)(\sqrt{q}u)^{\mathfrak{n}}\mathcal{L}\Big(E, \frac{1}{qu}\Big)$$

where $\epsilon(E) \in \{\pm 1\}$.

The L–function is a polynomial in u with integer coefficients of degree

$$\mathfrak{n} := \deg\left(\mathcal{L}(E,u)\right) = \deg(M) + 2\deg(A) - 4,$$

where we denote by M the product of the finite primes where E has multiplicative reduction and by A the product of the finite primes where E has additive reduction. The L–function satisfies the functional equation

$$\mathcal{L}(E,u) = \epsilon(E)(\sqrt{q}u)^{\mathfrak{n}}\mathcal{L}\Big(E, \frac{1}{qu}\Big)$$

where $\epsilon(E) \in \{\pm 1\}$.

For $D \in \mathcal{O}_K$ with D square-free, monic of odd degree and $(D,\Delta) = 1$, consider the twisted elliptic curve $E \otimes \chi_D/K$ with the affine model $y^2 = x^3 + D^2ax + D^3b$.

The L–function is a polynomial in u with integer coefficients of degree

$$\mathfrak{n} := \deg\left(\mathcal{L}(E,u)\right) = \deg(M) + 2\deg(A) - 4,$$

where we denote by M the product of the finite primes where E has multiplicative reduction and by A the product of the finite primes where E has additive reduction. The L–function satisfies the functional equation

$$\mathcal{L}(E,u) = \epsilon(E)(\sqrt{q}u)^{\mathfrak{n}}\mathcal{L}\Big(E, \frac{1}{qu}\Big)$$

where $\epsilon(E) \in \{\pm 1\}$.

For $D \in \mathcal{O}_K$ with D square-free, monic of odd degree and $(D, \Delta) = 1$, consider the twisted elliptic curve $E \otimes \chi_D/K$ with the affine model $y^2 = x^3 + D^2ax + D^3b$. The L–function corresponding to the twisted elliptic curve $\mathcal{L}(E \otimes \chi_D, u)$ has the Dirichlet series and Euler product

$$\sum_{f \in \mathcal{M}} \lambda(f)\chi_D(f)u^{\deg(f)} =$$

$$\prod_{P|\Delta}\left(1 - \lambda(P)\chi_D(P)u^{\deg(P)}\right)^{-1} \prod_{P \nmid \Delta D}\left(1 - \lambda(P)\chi_D(P)u^{\deg(P)} + u^{2\deg(P)}\right)^{-1}$$

The new L–function is a polynomial of degree $(\mathfrak{n} + 2\deg(D))$ and satisfies the functional equation

$$\mathcal{L}(E \otimes \chi_D, u) = \epsilon\,(\sqrt{q}u)^{\mathfrak{n}+2\deg(D)}\mathcal{L}\Big(E \otimes \chi_D, \frac{1}{qu}\Big),$$

where

$$\epsilon = \epsilon(E \otimes \chi_D) = \epsilon_{\deg(D)}\epsilon(E)\chi_D(M),$$

with $\epsilon_{\deg(D)} \in \{\pm 1\}$ is an integer which only depends on the degree of D.

The new L–function is a polynomial of degree $\left(\mathfrak{n}+2\deg(D)\right)$ and satisfies the functional equation

$$\mathcal{L}(E\otimes\chi_D,u)=\epsilon\,(\sqrt{q}u)^{\mathfrak{n}+2\deg(D)}\mathcal{L}\Big(E\otimes\chi_D,\frac{1}{qu}\Big),$$

where

$$\epsilon=\epsilon(E\otimes\chi_D)=\epsilon_{\deg(D)}\epsilon(E)\chi_D(M),$$

with $\epsilon_{\deg(D)}\in\{\pm1\}$ is an integer which only depends on the degree of D.

Let $\mathcal{H}^*_{2g+1}$ denote the set of monic, square free polynomials of degree $(2g+1)$ coprime to Δ. Our first two theorems concern the first moments of $L(E\otimes\chi_D,1/2)$ and $L'(E\otimes\chi_D,1/2)$.

Theorem (Bui, Florea, JPK, Roditty-Gershon)

Unless $\epsilon_{2g+1}\epsilon(E) = -1$ *and* $M = 1$,

$$\frac{1}{|\mathcal{H}^*_{2g+1}|} \sum_{D \in \mathcal{H}^*_{2g+1}} L(E \otimes \chi_D, \tfrac{1}{2}) = c_1(M) + O_\varepsilon\left(q^{-g+\epsilon g}\right),$$

with $c_1(M) \neq 0$.

Theorem (Bui, Florea, JPK, Roditty-Gershon)

Unless $\epsilon_{2g+1}\epsilon(E) = -1$ *and* $M = 1$,

$$\frac{1}{|\mathcal{H}^*_{2g+1}|} \sum_{D \in \mathcal{H}^*_{2g+1}} L(E \otimes \chi_D, \tfrac{1}{2}) = c_1(M) + O_\varepsilon\big(q^{-g+\epsilon g}\big),$$

with $c_1(M) \neq 0$.

Theorem (Bui, Florea, JPK, Roditty-Gershon)

Unless $\epsilon_{2g+1}\epsilon(E) = 1$ *and* $M = 1$,

$$\frac{1}{|\mathcal{H}^*_{2g+1}|} \sum_{D \in \mathcal{H}^*_{2g+1}} \epsilon^- L'(E \otimes \chi_D, \tfrac{1}{2}) = c_2(M) L\big(\mathrm{Sym}^2 \mathrm{E}, 1\big)\mathrm{g} + \mathrm{c}_3(\mathrm{M}) + O_\varepsilon\big(q^{-g+\epsilon g}\big),$$

where $c_2(M) \neq 0$.

Similarly

Theorem (Bui, Florea, JPK, Roditty-Gershon)

Unless $\epsilon_{2g+1}\epsilon(E) = -1$ *and* $M = 1$,

$$\frac{1}{|\mathcal{H}^*_{2g+1}|} \sum_{D \in \mathcal{H}^*_{2g+1}} L(E \otimes \chi_D, \tfrac{1}{2})^2 = c_4(M) L\big(\mathrm{Sym}^2\mathrm{E}, 1\big)^3 \, \mathrm{g} + \mathrm{O}_\varepsilon\big(\mathrm{g}^{1/2+\varepsilon}\big),$$

where $c_4(M) \neq 0$.

Similarly

Theorem (Bui, Florea, JPK, Roditty-Gershon)

Unless $\epsilon_{2g+1}\epsilon(E) = -1$ *and* $M = 1$,

$$\frac{1}{|\mathcal{H}^*_{2g+1}|} \sum_{D \in \mathcal{H}^*_{2g+1}} L(E \otimes \chi_D, \tfrac{1}{2})^2 = c_4(M) L\big(\mathrm{Sym}^2\mathrm{E}, 1\big)^3 \mathrm{g} + \mathrm{O}_\varepsilon\big(\mathrm{g}^{1/2+\varepsilon}\big),$$

where $c_4(M) \neq 0$.

Theorem (Bui, Florea, JPK, Roditty-Gershon)

Unless $\epsilon_{2g+1}\epsilon(E) = 1$ *and* $M = 1$,

$$\frac{1}{|\mathcal{H}^*_{2g+1}|} \sum_{D \in \mathcal{H}^*_{2g+1}} \epsilon^- L'(E \otimes \chi_D, \tfrac{1}{2})^2 = c_5(M) L\big(\mathrm{Sym}^2\mathrm{E}, 1\big)^3 \mathrm{g}^3 + \mathrm{O}_\varepsilon(\mathrm{g}^{2+\epsilon}),$$

where $c_5(M) \neq 0$.

Let E_1 and E_2 be two elliptic curves over K. Let $\Delta = \Delta_1\Delta_2$, where, for $i = 1, 2$, Δ_i denotes the discriminant of E_i. Let M_i denote the product of the finite primes where E_i has multiplicative reduction and $\epsilon_i = \epsilon_{\deg(D)}\epsilon(E_i)\chi_D(M_i)$. Define

$$\epsilon_i^+ := \frac{1+\epsilon_i}{2} \qquad \text{and} \qquad \epsilon_i^- := \frac{1-\epsilon_i}{2}.$$

Let E_1 and E_2 be two elliptic curves over K. Let $\Delta = \Delta_1\Delta_2$, where, for $i = 1, 2$, Δ_i denotes the discriminant of E_i. Let M_i denote the product of the finite primes where E_i has multiplicative reduction and $\epsilon_i = \epsilon_{\deg(D)}\epsilon(E_i)\chi_D(M_i)$. Define

$$\epsilon_i^+ := \frac{1+\epsilon_i}{2} \qquad \text{and} \qquad \epsilon_i^- := \frac{1-\epsilon_i}{2}.$$

Theorem (Bui, Florea, JPK, Roditty-Gershon)

Unless $\epsilon_{2g+1}\epsilon(E_1) = -1$ and $M_1 = 1$, or $\epsilon_{2g+1}\epsilon(E_2) = 1$ and $M_2 = 1$, or $\epsilon(E_1) = \epsilon(E_2)$ and $M_1 = M_2$, we have

$$\frac{1}{|\mathcal{H}^*_{2g+1}|} \sum_{D\in\mathcal{H}^*_{2g+1}} \epsilon_2^- \, L(E_1\otimes\chi_D, \tfrac{1}{2})L'(E_2\otimes\chi_D, \tfrac{1}{2})$$
$$= c_6(M_1, M_2)L\big(\mathrm{Sym}^2\mathrm{E}_1, 1\big)\mathrm{L}\big(\mathrm{Sym}^2\mathrm{E}_2, 1\big)\mathrm{L}\big(\mathrm{E}_1\otimes\mathrm{E}_2, 1\big)\,\mathrm{g} + O_\varepsilon\big(g^{1/2+\varepsilon}\big),$$

where $c_6(M_1, M_2) \neq 0$.

Theorem (Bui, Florea, JPK, Roditty-Gershon)

Unless $\epsilon_{2g+1}\epsilon(E_1) = 1$ *and* $M_1 = 1$, *or* $\epsilon_{2g+1}\epsilon(E_2) = 1$ *and* $M_2 = 1$, *or* $\epsilon(E_1) = -\epsilon(E_2)$ *and* $M_1 = M_2$, *we have*

$$\frac{1}{|\mathcal{H}^*_{2g+1}|} \sum_{D \in \mathcal{H}^*_{2g+1}} \epsilon_1^- \epsilon_2^- L'(E_1 \otimes \chi_D, \tfrac{1}{2}) L'(E_2 \otimes \chi_D, \tfrac{1}{2})$$

$$= c_7(M_1, M_2) L\left(\mathrm{Sym}^2 \mathrm{E}_1, 1\right) \mathrm{L}\left(\mathrm{Sym}^2 \mathrm{E}_2, 1\right) \mathrm{L}\left(\mathrm{E}_1 \otimes \mathrm{E}_2, 1\right) \mathrm{g}^2$$

$$+ O_\varepsilon\left(g^{1+\varepsilon}\right),$$

where $c_7(M_1, M_2) \neq 0$.

Define the analytic rank of a quadratic twist of an elliptic curve L-function $L(E \otimes \chi_D, s)$ by

$$r_{E\otimes\chi_D} := \mathrm{ord}_{s=1/2} L(E \otimes \chi_D, s).$$

Define the analytic rank of a quadratic twist of an elliptic curve L-function $L(E \otimes \chi_D, s)$ by

$$r_{E\otimes\chi_D} := \mathrm{ord}_{s=1/2} L(E \otimes \chi_D, s).$$

Corollary

Unless $\epsilon_{2g+1}\epsilon(E_1) = -1$ *and* $M_1 = 1$*, or* $\epsilon_{2g+1}\epsilon(E_2) = 1$ *and* $M_2 = 1$*, or* $\epsilon(E_1) = \epsilon(E_2)$ *and* $M_1 = M_2$*, we have*

$$\#\left\{D \in \mathcal{H}^*_{2g+1} : r_{E_1\otimes\chi_D} = 0, r_{E_2\otimes\chi_D} = 1\right\} \gg_\varepsilon \frac{q^{2g}}{g^{6+\varepsilon}}$$

as $g \to \infty$*. Also, unless* $\epsilon_{2g+1}\epsilon(E_1) = 1$ *and* $M_1 = 1$*, or* $\epsilon_{2g+1}\epsilon(E_2) = 1$ *and* $M_2 = 1$*, or* $\epsilon(E_1) = -\epsilon(E_2)$ *and* $M_1 = M_2$*, we have*

$$\#\left\{D \in \mathcal{H}^*_{2g+1} : r_{E_1\otimes\chi_D} = r_{E_2\otimes\chi_D} = 1\right\} \gg_\varepsilon \frac{q^{2g}}{g^{6+\varepsilon}}$$

as $g \to \infty$*.*

As far as we are aware, this is the first result in literature where explicit lower bounds concerning the correlations between the ranks of two twisted elliptic curves are obtained.

As far as we are aware, this is the first result in literature where explicit lower bounds concerning the correlations between the ranks of two twisted elliptic curves are obtained.

Following Harper's argument for the upper bounds for moments of L-functions, one may remove the exponents ε.

As far as we are aware, this is the first result in literature where explicit lower bounds concerning the correlations between the ranks of two twisted elliptic curves are obtained.

Following Harper's argument for the upper bounds for moments of L-functions, one may remove the exponents ε.

We fail to obtain positive proportions in the above results because we are not able to use a mollifier.

Mixed Moments and RMT

- Computing mixed moments is a key theme of recent developments in Random Matrix Theory.

Mixed Moments and RMT

- Computing mixed moments is a key theme of recent developments in Random Matrix Theory.
- There are interesting connections with the theory of Painlevé equations, conformal block expansions etc

Mixed Moments and RMT

- Computing mixed moments is a key theme of recent developments in Random Matrix Theory.
- There are interesting connections with the theory of Painlevé equations, conformal block expansions etc
- see *A representation of joint moments of CUE characteristic polynomials in terms of Painlevé functions*, Estelle Basor, Pavel Bleher, Robert Buckingham, Tamara Grava, Alexander Its, Elizabeth Its, & Jonathan P. Keating, arXiv:1811.00064

Mixed Moments and RMT

- Computing mixed moments is a key theme of recent developments in Random Matrix Theory.
- There are interesting connections with the theory of Painlevé equations, conformal block expansions etc
- see *A representation of joint moments of CUE characteristic polynomials in terms of Painlevé functions*, Estelle Basor, Pavel Bleher, Robert Buckingham, Tamara Grava, Alexander Its, Elizabeth Its, & Jonathan P. Keating, arXiv:1811.00064
- and *Mixed moments of characteristic polynomials of random unitary matrices*, Emma C. Bailey, Sandro Bettin, Gordon Blower, J. Brian Conrey, Andrei Prokhorov, Michael O. Rubinstein, & Nina C. Snaith, arXiv:1901.07479.