The Zeros of Elliptic Curve L-Functions

Simon Spicer

University of Washington

mlungu@uw.edu

July 8, 2013

Overview

- Motivated by a challenge question from Barry Mazur in the upcoming paper "How Explicit is the Explicit Formula?"
- Prove an explicit version of the explicit formula for elliptic curve L-functions, i.e. one with explicit error bounds for truncated sums over L-function zeros
- Applicable to work of Mazur, Sarnak et al
- This talk more about what to do with elliptic curve L-function zeros once you have them, as apposed to how to compute them in the first place

Motivating Example

- Let $\zeta(s)$ be the meromorphic continuation to $\mathbb{C}$ of $\sum_{n=1}^{\infty} n^{-s}$.

Motivating Example

- Let $\zeta(s)$ be the meromorphic continuation to $\mathbb{C}$ of $\sum_{n=1}^{\infty} n^{-s}$.
- Then $\zeta(s)$ has a single simple pole at $s = 1$, and simple zeros at $2\mathbb{Z}_{<0}$.

Motivating Example

- Let $\zeta(s)$ be the meromorphic continuation to $\mathbb{C}$ of $\sum_{n=1}^{\infty} n^{-s}$.
- Then $\zeta(s)$ has a single simple pole at $s = 1$, and simple zeros at $2\mathbb{Z}_{<0}$.
- All other zeros lie in the vertical strip $0 < \Re(s) < 1$, symmetric about the real axis.

Motivating Example

- Let $\zeta(s)$ be the meromorphic continuation to $\mathbb{C}$ of $\sum_{n=1}^{\infty} n^{-s}$.
- Then $\zeta(s)$ has a single simple pole at $s = 1$, and simple zeros at $2\mathbb{Z}_{<0}$.
- All other zeros lie in the vertical strip $0 < \Re(s) < 1$, symmetric about the real axis.

Conjecture (Riemann Hypothesis)

All nontrivial zeros of ζ are simple and lie on the line $\Re(s) = \frac{1}{2}$.

The Zeros of ζ

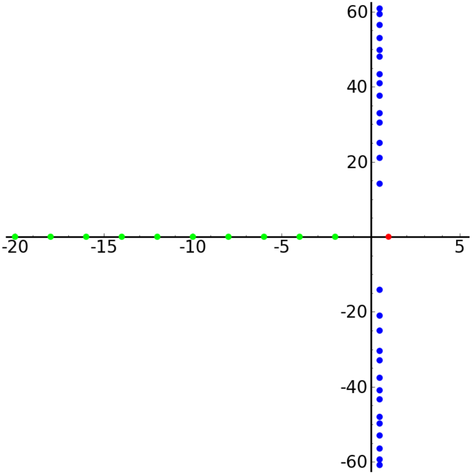
The imaginary parts of the first few zeros of $\zeta(s)$ in the upper half plane are

$$\begin{aligned}
&14.134725142\ldots\\
&21.022039639\ldots\\
&25.010857580\ldots\\
&30.424876126\ldots\\
&32.935061588\ldots\\
&37.586178159\ldots\\
&40.918719012\ldots\\
&43.327073281\ldots\\
&48.005150881\ldots\\
&49.773832478\ldots\\
&52.970321478\ldots\\
&56.446247697\ldots\\
&59.347044003\ldots\\
&60.831778525\ldots
\end{aligned}$$

The Zeros of ζ

The imaginary parts of the first few zeros of $\zeta(s)$ in the upper half plane are

14.134725142...
21.022039639...
25.010857580...
30.424876126...
32.935061588...
37.586178159...
40.918719012...
43.327073281...
48.005150881...
49.773832478...
52.970321478...
56.446247697...
59.347044003...
60.831778525...



The Explicit Formula for $\zeta(s)$

The Riemann zeta function $\zeta(s)$

Consider as a function of $x > 1$ the sum

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x} \left(\sum_{0<\gamma<T} \frac{2\sin(\gamma \log x)}{\gamma} \right)$$

contingent on RH, where γ runs over imaginary parts of nontrivial zeros.

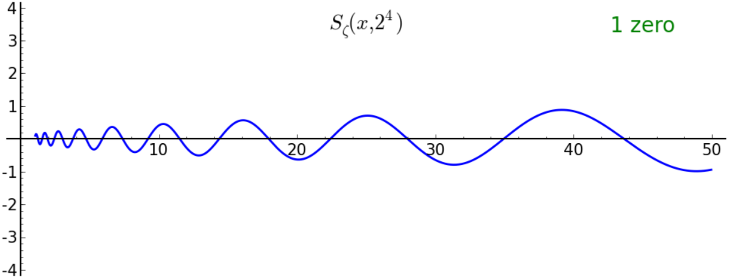
The Explicit Formula for $\zeta(s)$

The Riemann zeta function $\zeta(s)$

Consider as a function of $x > 1$ the sum

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x} \left(\sum_{0<\gamma<T} \frac{2\sin(\gamma \log x)}{\gamma} \right)$$

contingent on RH, where γ runs over imaginary parts of nontrivial zeros.



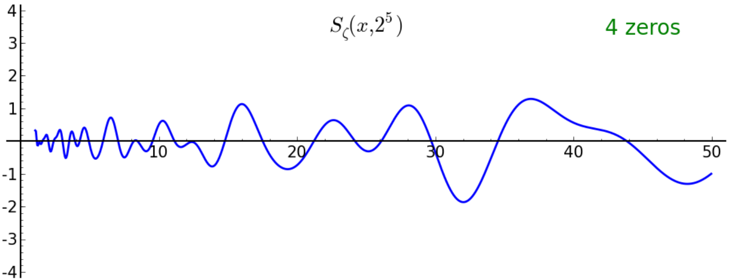
The Explicit Formula for $\zeta(s)$

The Riemann zeta function $\zeta(s)$

Consider as a function of $x > 1$ the sum

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{2\sin(\gamma \log x)}{\gamma}\right)$$

contingent on RH, where γ runs over imaginary parts of nontrivial zeros.



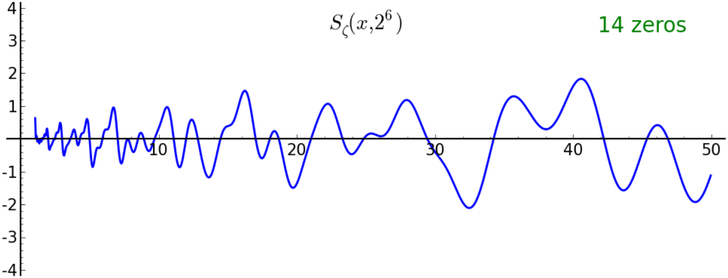
The Explicit Formula for $\zeta(s)$

The Riemann zeta function $\zeta(s)$

Consider as a function of $x > 1$ the sum

$$S_{\zeta}(x, T) = \sum_{|\rho|<T} \frac{x^{\rho}}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{2\sin(\gamma \log x)}{\gamma}\right)$$

contingent on RH, where γ runs over imaginary parts of nontrivial zeros.



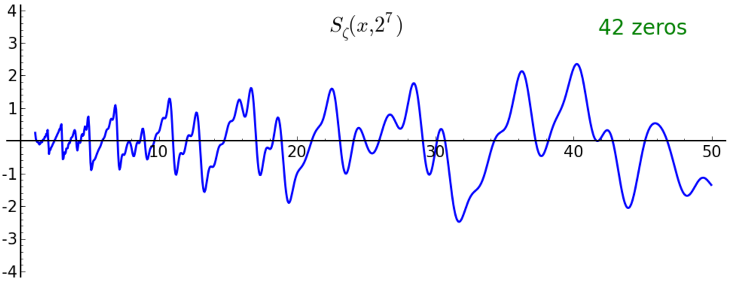
The Explicit Formula for $\zeta(s)$

The Riemann zeta function $\zeta(s)$

Consider as a function of $x > 1$ the sum

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{2\sin(\gamma \log x)}{\gamma}\right)$$

contingent on RH, where γ runs over imaginary parts of nontrivial zeros.



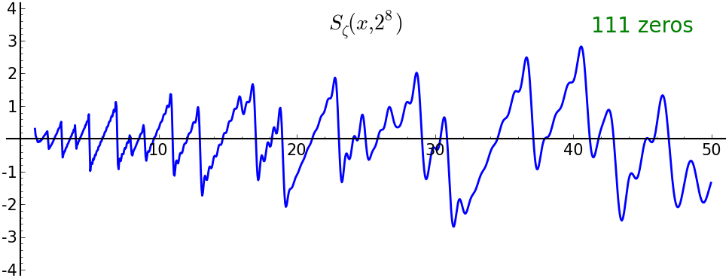
The Explicit Formula for $\zeta(s)$

The Riemann zeta function $\zeta(s)$

Consider as a function of $x > 1$ the sum

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{2\sin(\gamma \log x)}{\gamma}\right)$$

contingent on RH, where γ runs over imaginary parts of nontrivial zeros.



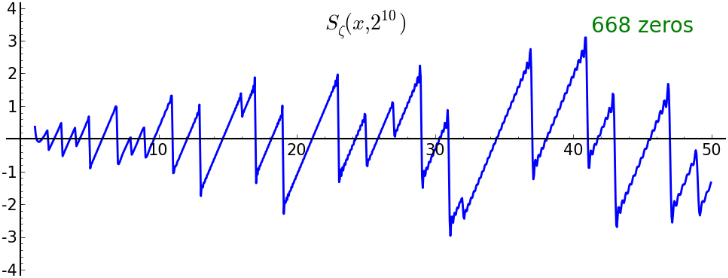
The Explicit Formula for $\zeta(s)$

The Riemann zeta function $\zeta(s)$

Consider as a function of $x > 1$ the sum

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{2\sin(\gamma \log x)}{\gamma}\right)$$

contingent on RH, where γ runs over imaginary parts of nontrivial zeros.



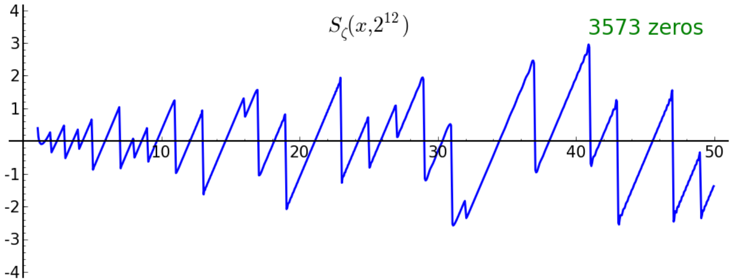
The Explicit Formula for $\zeta(s)$

The Riemann zeta function $\zeta(s)$

Consider as a function of $x > 1$ the sum

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{2\sin(\gamma \log x)}{\gamma}\right)$$

contingent on RH, where γ runs over imaginary parts of nontrivial zeros.



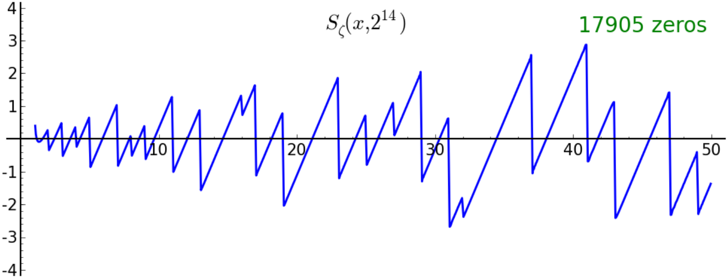
The Explicit Formula for $\zeta(s)$

The Riemann zeta function $\zeta(s)$

Consider as a function of $x > 1$ the sum

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{2\sin(\gamma \log x)}{\gamma}\right)$$

contingent on RH, where γ runs over imaginary parts of nontrivial zeros.



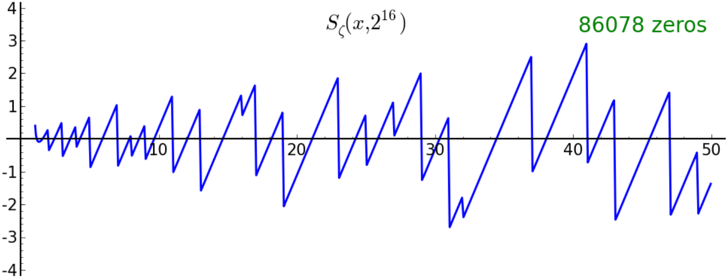
The Explicit Formula for $\zeta(s)$

The Riemann zeta function $\zeta(s)$

Consider as a function of $x > 1$ the sum

$$S_\zeta(x,T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{2\sin(\gamma \log x)}{\gamma}\right)$$

contingent on RH, where γ runs over imaginary parts of nontrivial zeros.



The Explicit Formula for $\zeta(s)$

What does this sum converge to?

The Explicit Formula for $\zeta(s)$

What does this sum converge to?

Theorem (Riemann 1858, von Mangoldt 1905)

$$\sum_{\rho} \frac{x^{\rho}}{\rho} = \lim_{T\to\infty} S_{\zeta}(x,T) = x - \frac{1}{2}\log\left(1 - 1/x^2\right) - \log(2\pi) - \psi_{\zeta}(x)$$

where $\psi_{\zeta}(x) = \sum_{p^e \leq x}' \log p$ *is the second Chebyshev function.*

The Explicit Formula for $\zeta(s)$

What does this sum converge to?

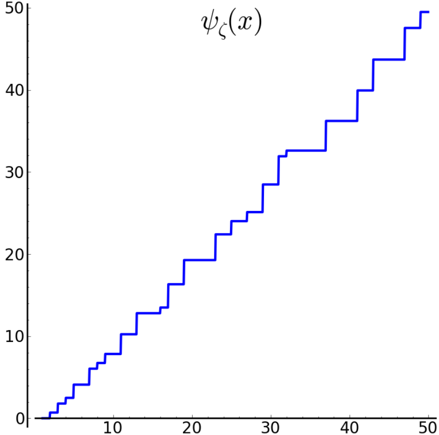
Theorem (Riemann 1858, von Mangoldt 1905)

$$\sum_{\rho} \frac{x^{\rho}}{\rho} = \lim_{T \to \infty} S_{\zeta}(x, T) = x - \frac{1}{2} \log\left(1 - 1/x^2\right) - \log(2\pi) - \psi_{\zeta}(x)$$

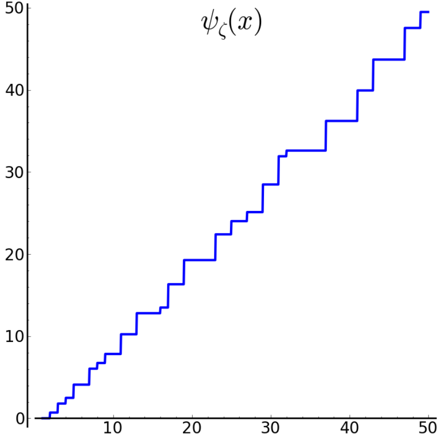
where $\psi_{\zeta}(x) = \sum_{p^e \leq x}' \log p$ *is the second Chebyshev function.*

This is known as (one formulation of) *the explicit formula* for $\zeta(s)$.

The Explicit Formula for $\zeta(s)$



The Explicit Formula for $\zeta(s)$



My Goal

Prove the explicit formula for elliptic curve L-functions, with error bounds for $S_E(x, T)$.

Elliptic Curves

Definition

An elliptic curve E is a smooth projective genus 1 algebraic curve with a marked point $\mathcal{O}$.

Elliptic Curves

Definition

An elliptic curve E is a smooth projective genus 1 algebraic curve with a marked point $\mathcal{O}$.

For This Talk:

$$E/\mathbb{Q}: \quad y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}$$

Elliptic Curves

Definition

An elliptic curve E is a smooth projective genus 1 algebraic curve with a marked point $\mathcal{O}$.

For This Talk:

$$E/\mathbb{Q}: \quad y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Z}$$

Example

$$E = 37a : y^2 = x^3 - 16x + 16$$

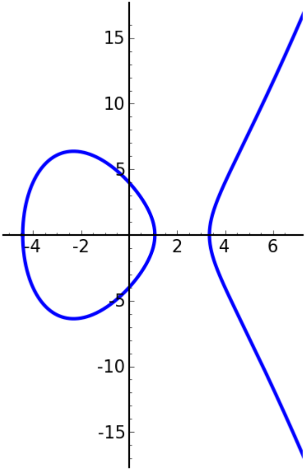


Figure: The Elliptic Curve $37a$

Elliptic Curves

Definition

An elliptic curve E is a smooth projective genus 1 algebraic curve with a marked point $\mathcal{O}$.

For This Talk:

$$E/\mathbb{Q}: \quad y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Z}$$

Example

$$E = 37a : y^2 = x^3 - 16x + 16$$

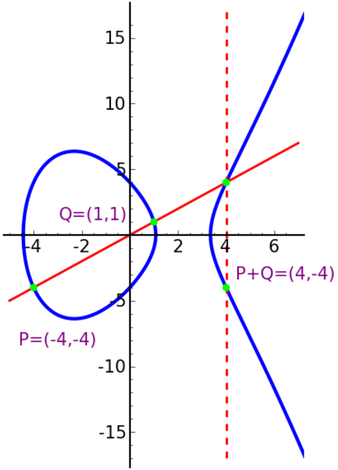


Figure: The Elliptic Curve $37a$

Theorem (Mordell 1922, Weil 1928)

$$E(\mathbb{Q}) \approx E(\mathbb{Q})_{TOR} \times \mathbb{Z}^r$$

where $E(\mathbb{Q})_{TOR}$ is a finite abelian group, and $r \in \mathbb{Z}_{\geq 0}$ is the algebraic rank of $E/\mathbb{Q}$.

Theorem (Mordell 1922, Weil 1928)

$$E(\mathbb{Q}) \approx E(\mathbb{Q})_{TOR} \times \mathbb{Z}^r$$

where $E(\mathbb{Q})_{TOR}$ is a finite abelian group, and $r \in \mathbb{Z}_{\geq 0}$ is the algebraic rank of $E/\mathbb{Q}$.

Example

For $E = 37a$, we have $E(\mathbb{Q}) \approx \mathbb{Z}^1$, generated by $P = (0, 4)$:

n	0	1	2	3	4	5	6
nP	$\mathcal{O}$	$(0,4)$	$(4,4)$	$(-4,-4)$	$(8,-20)$	$(1,-1)$	$(24,116)$

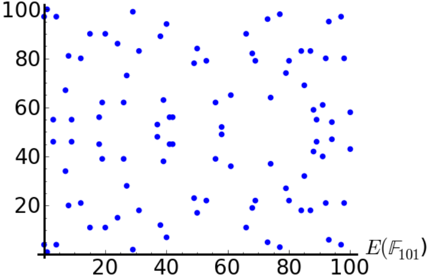
n	7	8	9
nP	$\left(-\frac{20}{9}, \frac{172}{27}\right)$	$\left(\frac{84}{25}, -\frac{52}{125}\right)$	$\left(-\frac{80}{49}, -\frac{2108}{343}\right)$

Elliptic Curves over finite fields

Example

$$E = 37a : y^2 = x^3 - 16x + 16$$

Consider its solutions (x, y) modulo 101, e.g. $(40, 7)$:

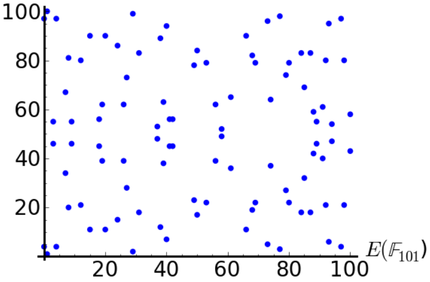


Elliptic Curves over finite fields

Example

$$E = 37a : y^2 = x^3 - 16x + 16$$

Consider its solutions (x, y) modulo 101, e.g. $(40, 7)$:



Definition

- For p prime with good reduction, $a_p(E) = a_p := p + 1 - \#E(\mathbb{F}_p)$
- For bad primes, $a_p := 0, 1$ or -1 depending on reduction type.

Elliptic Curves over finite fields

Theorem (Hasse, 1936)

$$|a_p| \leq 2\sqrt{p} \quad \textit{for all } p.$$

Elliptic Curves over finite fields

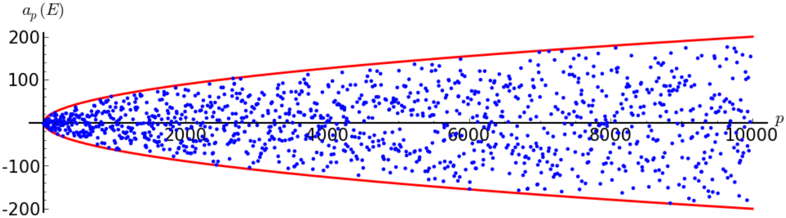
Theorem (Hasse, 1936)

$$|a_p| \leq 2\sqrt{p} \quad \textit{for all } p.$$

Example

For $E = 37a$,

p	2	3	5	7	11	13	17	19	23	29	31	37
a_p	-2	-3	-2	-1	-5	-2	0	0	2	6	-4	-1



The Conductor of a Curve

Definition

The conductor of E is $N = \prod_p p^{f_p(E)}$, where

$$f_p(E) = \begin{cases} 0, & p \text{ good} \\ 1, & \text{mult. reduction at } p \\ 2, & \text{add. reduction at } p, \end{cases}$$

for $p \neq 2, 3$ and possibly more for 2 and 3.

The Conductor of a Curve

Definition

The conductor of E is $N = \prod_p p^{f_p(E)}$, where

$$f_p(E) = \begin{cases} 0, & p \text{ good} \\ 1, & \text{mult. reduction at } p \\ 2, & \text{add. reduction at } p, \end{cases}$$

for $p \neq 2, 3$ and possibly more for 2 and 3.

Example

The conductor of $37a$ is $N = 37$, hence its name.

Elliptic Curve L-Functions

Definition

The L-function attached to E is

$$L_E(s) := \prod_{p|N} \frac{1}{1 - a_p p^{-s}} \prod_{p\nmid N} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{n=1}^{\infty} a_n n^{-s}$$

for $\Re(s) > \frac{3}{2}$.

The a_n are defined by multiplying out the Euler product.

Elliptic Curve L-Functions

Definition

The L-function attached to E is

$$L_E(s) := \prod_{p|N} \frac{1}{1 - a_p p^{-s}} \prod_{p\nmid N} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{n=1}^{\infty} a_n n^{-s}$$

for $\Re(s) > \frac{3}{2}$.

The a_n are defined by multiplying out the Euler product.

Definition

The *completed* L-function attached to E is

$$\Lambda_E(s) := N^{s/2}(2\pi)^{-s}\Gamma(s)L_E(s)$$

Modularity & Analytic Continuation of $L_E(s)$

Theorem (Breuille, Conrad, Diamond, Taylor, Wiles et al, 1999,2001)

There exists an integral newform $f \in S_2(\Gamma_0(N))$ s.t. $L_f(s) = L_E(s)$. That is, there exists a holomorphic function f on $\mathbb{H}$ with Fourier decomposition $f(z) = \sum_n a_n(f)e^{2\pi inz}$ such that $a_n(f) = a_n(E)$.

Modularity & Analytic Continuation of $L_E(s)$

Theorem (Breuille, Conrad, Diamond, Taylor, Wiles et al, 1999,2001)

There exists an integral newform $f \in S_2(\Gamma_0(N))$ *s.t.* $L_f(s) = L_E(s)$. *That is, there exists a holomorphic function* f *on* $\mathbb{H}$ *with Fourier decomposition* $f(z) = \sum_n a_n(f) e^{2\pi i n z}$ *such that* $a_n(f) = a_n(E)$.

Corollary

$L_E(s)$ *extends to an entire function on* $\mathbb{C}$. *Specifically,*

$$\Lambda(s) = w\Lambda(2-s),$$

where $w = \pm 1$.

The Zeros of $L_E(s)$

Three flavors:

- A simple zero at $0, -1, -2, -3, \ldots$
- A zero of order r_{an} at $s = 1$; r_{an} is called the *analytic rank* of E
- Countably infinite zeros in the strip $0 < \Re(s) < 2$, symmetric about $\Re(s) = 1$ and x-axis.

The Zeros of $L_E(s)$

Three flavors:

- A simple zero at $0, -1, -2, -3, \ldots$
- A zero of order r_{an} at $s = 1$; r_{an} is called the *analytic rank* of E
- Countably infinite zeros in the strip $0 < \Re(s) < 2$, symmetric about $\Re(s) = 1$ and x-axis.

Conjecture (Generalized Riemann Hypothesis for Elliptic Curves)

All nontrivial zeros of $L_E(s)$ are simple and lie on the line $\Re(s) = 1$.

The Zeros of $L_E(s)$

Three flavors:

- A simple zero at $0, -1, -2, -3, \ldots$
- A zero of order r_{an} at $s = 1$; r_{an} is called the *analytic rank* of E
- Countably infinite zeros in the strip $0 < \Re(s) < 2$, symmetric about $\Re(s) = 1$ and x-axis.

Conjecture (Generalized Riemann Hypothesis for Elliptic Curves)

All nontrivial zeros of $L_E(s)$ are simple and lie on the line $\Re(s) = 1$.

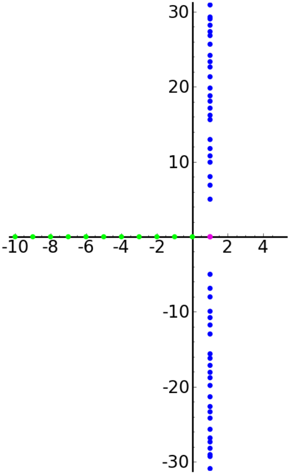


Figure: The zeros of $L_E(s)$ for $E = 37a$

The BSD Conjecture

Conjecture (Birch, Swinnerton-Dyer 1960s)

- $r_{an} = r$, *i.e. the order of vanishing of* $L_E(s)$ *at* $s = 1$ *equals the rank of the free part of* $E(\mathbb{Q})$

The BSD Conjecture

Conjecture (Birch, Swinnerton-Dyer 1960s)

- $r_{an} = r$, *i.e. the order of vanishing of* $L_E(s)$ *at* $s = 1$ *equals the rank of the free part of* $E(\mathbb{Q})$
- *The leading coefficient of* $L_E(s)$ *at* $s = 1$ *is*

$$\frac{\Omega_E \cdot Reg_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{Tor}(\mathbb{Q}))^2}$$

The BSD Conjecture

Conjecture (Birch, Swinnerton-Dyer 1960s)

- $r_{an} = r$, *i.e. the order of vanishing of* $L_E(s)$ *at* $s = 1$ *equals the rank of the free part of* $E(\mathbb{Q})$
- *The leading coefficient of* $L_E(s)$ *at* $s = 1$ *is*

$$\frac{\Omega_E \cdot Reg_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{Tor}(\mathbb{Q}))^2}$$

where

- Ω_E *is the real period of (an optimal model of)* E,
- Reg_E *is the regulator of* E,
- $\#\text{Ш}(E/\mathbb{Q})$ *is the order of the Shafarevich-Tate group attached to* $E/\mathbb{Q}$,
- $\prod_p c_p$ *is the product of the Tamagawa numbers of* E, *and*
- $\#E_{Tor}(\mathbb{Q})$ *is the number of rational torsion points on* E.

The Shifted Logarithmic Derivative

To state the explicit formula for elliptic curves, we will need to characterize $\frac{L_E'}{L_E}(s+1)$.

The Shifted Logarithmic Derivative

To state the explicit formula for elliptic curves, we will need to characterize $\frac{L_E'}{L_E}(s+1)$.

Lemma 1 (S.)

$\frac{L_E'}{L_E}(s+1) = \frac{d}{ds}\log(L_E)(s+1)$ has the Dirichlet series $\sum_n c_n(E)n^{-s}$ which converges absolutely for $\Re(s) > \frac{1}{2}$, where

$$c_n(E) := \begin{cases} -\left(p^e + 1 - \#\widetilde{E}(\mathbb{F}_{p^e})\right) \cdot \frac{\log(p)}{p^e}, & n = p^e \text{ a prime power,} \\ 0, & \text{otherwise} \end{cases}$$

and $\#\widetilde{E}(\mathbb{F}_{p^e})$ is the number of points on over $\mathbb{F}_{p^e}$ on the (possibly singular) projective curve obtained by reducing E modulo p.

The Shifted Logarithmic Derivative

Proof (Sketch).

- $L_E(s) := \prod_{p|N} \frac{1}{1-a_p p^{-s}} \prod_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}}$, so

The Shifted Logarithmic Derivative

Proof (Sketch).

- $L_E(s) := \prod_{p|N} \frac{1}{1-a_p p^{-s}} \prod_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}}$, so
  $\frac{L_E'}{L_E}(s) = -\sum_{p|N} \frac{a_p \log(p)\cdot p^{-s}}{1-a_p p^{-s}} - \sum_{p\nmid N} \frac{a_p \log(p)\cdot p^{-s} - 2p^{k-1}\log(p)\cdot p^{-2s}}{1-a_p p^{-s}+p^{k-1}\cdot p^{-2s}}$

The Shifted Logarithmic Derivative

Proof (Sketch).

- $L_E(s) := \prod_{p|N} \frac{1}{1-a_p p^{-s}} \prod_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}}$, so
  $\frac{L_E'}{L_E}(s) = -\sum_{p|N} \frac{a_p \log(p)\cdot p^{-s}}{1-a_p p^{-s}} - \sum_{p\nmid N} \frac{a_p \log(p)\cdot p^{-s} - 2p^{k-1}\log(p)\cdot p^{-2s}}{1-a_p p^{-s}+p^{k-1}\cdot p^{-2s}}$
- For good p, write $1 - a_p p^{-s} + p^{k-1} \cdot p^{-2s} = (1-\alpha_p p^{-s})(1-\beta_p p^{-s})$; invert each denominator as power series in p^{-s} and multiply out

The Shifted Logarithmic Derivative

Proof (Sketch).

- $L_E(s) := \prod_{p|N} \frac{1}{1-a_p p^{-s}} \prod_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}}$, so
  $\frac{L_E'}{L_E}(s) = -\sum_{p|N} \frac{a_p \log(p)\cdot p^{-s}}{1-a_p p^{-s}} - \sum_{p\nmid N} \frac{a_p \log(p)\cdot p^{-s} - 2p^{k-1}\log(p)\cdot p^{-2s}}{1-a_p p^{-s}+p^{k-1}\cdot p^{-2s}}$
- For good p, write $1 - a_p p^{-s} + p^{k-1} \cdot p^{-2s} = (1-\alpha_p p^{-s})(1-\beta_p p^{-s})$; invert each denominator as power series in p^{-s} and multiply out
- $\Rightarrow \frac{L_E'}{L_E}(s) = \sum_{p|N} \sum_{e\geq 1} -a_p^e \log(p)(p^e)^{-s}$
  $+ \sum_{p\nmid N} \sum_{e\geq 1} -(\alpha_p^e + \beta_p^e) \log(p)(p^e)^{-s}$

The Shifted Logarithmic Derivative

Proof (Sketch).

- $L_E(s) := \prod_{p|N} \frac{1}{1-a_p p^{-s}} \prod_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}}$, so
  $\frac{L_E'}{L_E}(s) = -\sum_{p|N} \frac{a_p \log(p)\cdot p^{-s}}{1-a_p p^{-s}} - \sum_{p\nmid N} \frac{a_p \log(p)\cdot p^{-s} - 2p^{k-1}\log(p)\cdot p^{-2s}}{1-a_p p^{-s}+p^{k-1}\cdot p^{-2s}}$
- For good p, write $1 - a_p p^{-s} + p^{k-1} \cdot p^{-2s} = (1-\alpha_p p^{-s})(1-\beta_p p^{-s})$; invert each denominator as power series in p^{-s} and multiply out
- $\Rightarrow \frac{L_E'}{L_E}(s) = \sum_{p|N}\sum_{e\geq 1} -a_p^e \log(p)(p^e)^{-s}$
  $+ \sum_{p\nmid N}\sum_{e\geq 1} -(\alpha_p^e + \beta_p^e)\log(p)(p^e)^{-s}$
- By Silverman etc.,
  $a_p^e = p^e + 1 - \#\widetilde{E}(\mathbb{F}_{p^e})$ for bad p, and
  $\alpha_p^e + \beta_p^e = p^e + 1 - \#E(\mathbb{F}_{p^e})$ for good p

The Shifted Logarithmic Derivative

Proof (Sketch).

- $L_E(s) := \prod_{p|N} \frac{1}{1-a_p p^{-s}} \prod_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}}$, so
  $\frac{L_E'}{L_E}(s) = -\sum_{p|N} \frac{a_p \log(p)\cdot p^{-s}}{1-a_p p^{-s}} - \sum_{p\nmid N} \frac{a_p \log(p)\cdot p^{-s} - 2p^{k-1}\log(p)\cdot p^{-2s}}{1-a_p p^{-s}+p^{k-1}\cdot p^{-2s}}$
- For good p, write $1 - a_p p^{-s} + p^{k-1}\cdot p^{-2s} = (1-\alpha_p p^{-s})(1-\beta_p p^{-s})$; invert each denominator as power series in p^{-s} and multiply out
- $\Rightarrow \frac{L_E'}{L_E}(s) = \sum_{p|N}\sum_{e\geq 1} -a_p^e \log(p)(p^e)^{-s}$
  $+ \sum_{p\nmid N}\sum_{e\geq 1} -(\alpha_p^e + \beta_p^e)\log(p)(p^e)^{-s}$
- By Silverman etc.,
  $a_p^e = p^e + 1 - \#\widetilde{E}(\mathbb{F}_{p^e})$ for bad p, and
  $\alpha_p^e + \beta_p^e = p^e + 1 - \#E(\mathbb{F}_{p^e})$ for good p
- Finally, shift left by 1 $\Rightarrow (p^e)^{-(s+1)} = \frac{1}{p^e}(p^e)^{-s}$ to pick up factor of $\frac{1}{p^e}$ in coefficients.

$\square$

Another Way to Express $\frac{L_E'}{L_E}(s+1)$

Lemma 2 (S.)

We may express $\frac{L_E'}{L_E}(s+1)$ as a sum over the zeros of $L_E(s)$. Specifically, assuming GRH then for any s not in the set of zeros of $L_E(s+1)$,

$$\frac{L_E'}{L_E}(s+1) = \left[\eta + \log\left(\frac{2\pi}{\sqrt{N}}\right)\right] - \sum_{k=1}^{\infty} \frac{s}{k(k+s)} + \sum_{\gamma} \frac{s}{s^2+\gamma^2}$$

where η is the Euler-Mascheroni constant $= 0.5772156649\ldots$
and γ ranges over the imaginary parts of all nontrivial zeros of L_E.

Another Way to Express $\frac{L_E'}{L_E}(s+1)$

Proof (Sketch).

Another Way to Express $\frac{L_E'}{L_E}(s+1)$

Proof (Sketch).

- By definition, $L_E(s) = \left(\frac{2\pi}{\sqrt{N}}\right)^s \Gamma(s)^{-1} \Lambda_E(s)$

Another Way to Express $\frac{L_E'}{L_E}(s+1)$

Proof (Sketch).

- By definition, $L_E(s) = \left(\frac{2\pi}{\sqrt{N}}\right)^s \Gamma(s)^{-1}\Lambda_E(s)$
- $\Rightarrow$ Shifted logarithmic derivative
  $\frac{L_E'}{L_E}(s+1) = \log\left(\frac{2\pi}{\sqrt{N}}\right) - \frac{\Gamma'}{\Gamma}(s+1) + \frac{\Lambda_E'}{\Lambda_E}(s+1)$

Another Way to Express $\frac{L_E'}{L_E}(s+1)$

Proof (Sketch).

- By definition, $L_E(s) = \left(\frac{2\pi}{\sqrt{N}}\right)^s \Gamma(s)^{-1}\Lambda_E(s)$
- $\Rightarrow$ Shifted logarithmic derivative
  $\frac{L_E'}{L_E}(s+1) = \log\left(\frac{2\pi}{\sqrt{N}}\right) - \frac{\Gamma'}{\Gamma}(s+1) + \frac{\Lambda_E'}{\Lambda_E}(s+1)$
- $\frac{\Gamma'}{\Gamma}(s+1) = -\eta + \sum_{k=1}^{\infty} \frac{s}{k(k+s)}$ outside negative integers

Another Way to Express $\frac{L_E'}{L_E}(s+1)$

Proof (Sketch).

- By definition, $L_E(s) = \left(\frac{2\pi}{\sqrt{N}}\right)^s \Gamma(s)^{-1} \Lambda_E(s)$
- $\Rightarrow$ Shifted logarithmic derivative
  $\frac{L_E'}{L_E}(s+1) = \log\left(\frac{2\pi}{\sqrt{N}}\right) - \frac{\Gamma'}{\Gamma}(s+1) + \frac{\Lambda_E'}{\Lambda_E}(s+1)$
- $\frac{\Gamma'}{\Gamma}(s+1) = -\eta + \sum_{k=1}^{\infty} \frac{s}{k(k+s)}$ outside negative integers
- $\frac{\Lambda_E'}{\Lambda_E}(s+1) = \sum_{\gamma} \frac{s}{s^2+\gamma^2}$, obtained by logarithmically differentiating Hadamard product of $\Lambda_E(s+1)$.

$\square$

An Interesting Aside

Corollary 1

If $E/\mathbb{Q}$ has conductor N and analytic rank r then

$$N > 0.202e^{2r}$$

An Interesting Aside

Corollary 1

If $E/\mathbb{Q}$ has conductor N and analytic rank r then

$$N > 0.202e^{2r}$$

Better results (S.), although nowhere close to effective yet:

r	$N \geq$	Smallest Known Conductor
0	3	11
1	6	37
2	16	389
3	55	5077
4	232	234446
5	1192	19047851
6	6696	5187563742

An Interesting Aside

Contingent on GRH and BSD we have a complete description of the Taylor series of L_E about $s = 1$. Specifically:

An Interesting Aside

Contingent on GRH and BSD we have a complete description of the Taylor series of L_E about $s = 1$. Specifically:

Corollary 2

Let $L_E(s+1) = s^r \left(a + b \cdot s + c \cdot s^2 + O(s^3)\right)$,
where a is the leading coefficient described by BSD. Then

$$\frac{b}{a} = \eta + \log\left(\frac{2\pi}{\sqrt{N}}\right)$$

$$\frac{c}{a} = \frac{1}{2}\left[\eta + \log\left(\frac{2\pi}{\sqrt{N}}\right)\right]^2 - \frac{\pi^2}{12} + \sum_{\gamma>0} \gamma^{-2}$$

Recursive formulae exist for higher coefficients as well.

The Explicit Formula for Elliptic Curves

Definition

The Explicit Formula for Elliptic Curves

Definition

Let

- $$S_E(x, T) := \sum_{|\gamma|<T} \frac{x^{i\gamma}}{i\gamma} = \sum_{0<\gamma<T} \frac{2\sin(\gamma \log x)}{\gamma}$$

  where γ runs over imaginary parts of nontrivial zeros other than $s = 1$

The Explicit Formula for Elliptic Curves

Definition

Let

- $$S_E(x,T) := \sum_{|\gamma|<T} \frac{x^{i\gamma}}{i\gamma} = \sum_{0<\gamma<T} \frac{2\sin(\gamma \log x)}{\gamma}$$

  where γ runs over imaginary parts of nontrivial zeros other than $s = 1$

- $$\psi_E(x) := {\sum_{n\leq x}}' c_n(E)$$

  i.e. $\psi_E(x)$ is the cumulative sum function of the Dirichlet coefficients of $\frac{L_E'}{L_E}(s+1)$
  (Recall $c_n(E) = \left(p^e + 1 - \#\widetilde{E}(\mathbb{F}_{p^e})\right) \cdot \frac{\log(p)}{p^e}$ for $n = p^e$ and 0 otherwise)

The Explicit Formula for Elliptic Curves

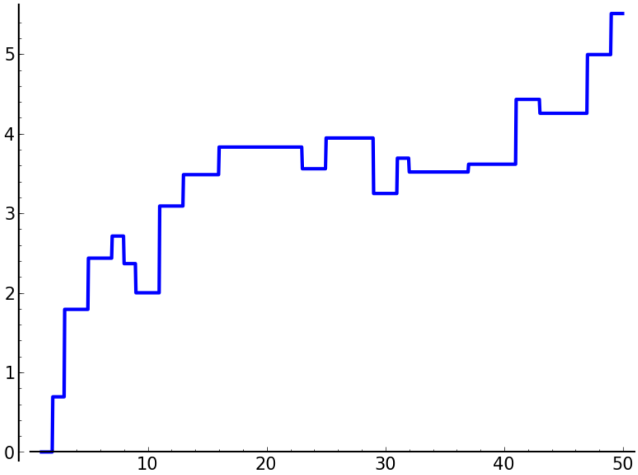


Figure: $\psi_E(x)$ for $E = 37a$

The Explicit Formula for Elliptic Curves

Theorem

For any any $E/\mathbb{Q}$ with conductor N and for any $x > 1$ the partial sum function $S_E(x, T)$ converges as $T \to \infty$. Specifically,

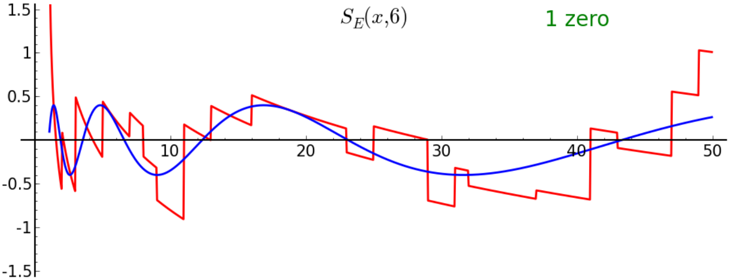
$$\begin{aligned}\lim_{T\to\infty} S_E(x, T) &= \sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} \\ &= -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1 - x^{-1}) + \psi_E(x)\end{aligned}$$

where η is the Euler-Mascheroni constant $= 0.5772156649\ldots$

The Explicit Formula for Elliptic Curves

Theorem

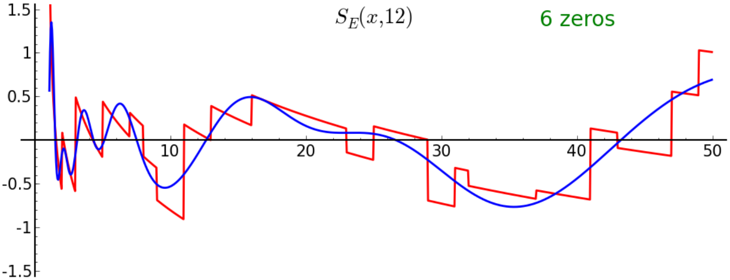
$$\sum_{\gamma>0} \frac{2\sin(\gamma\log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1-x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

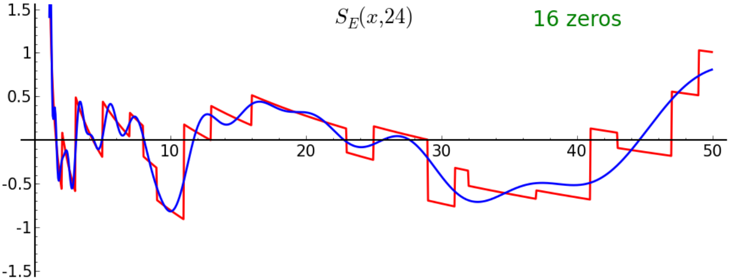
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1 - x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

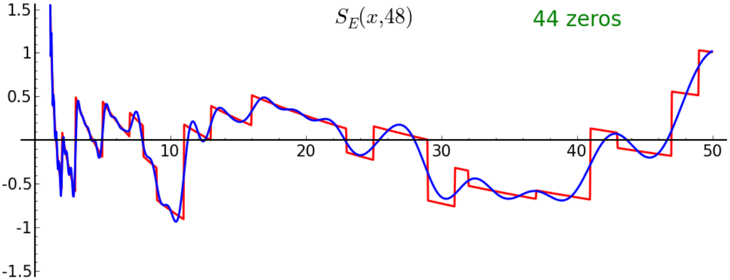
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1-x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

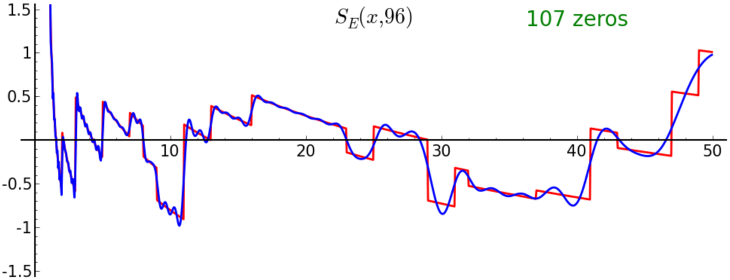
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1-x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

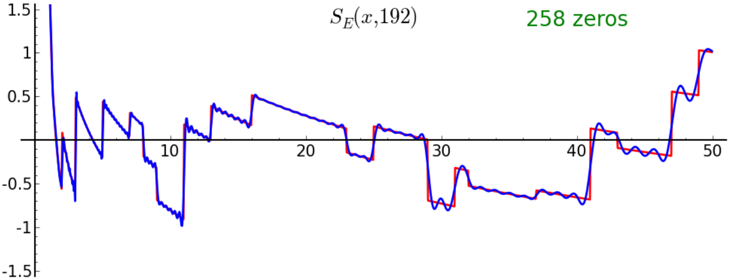
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1-x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

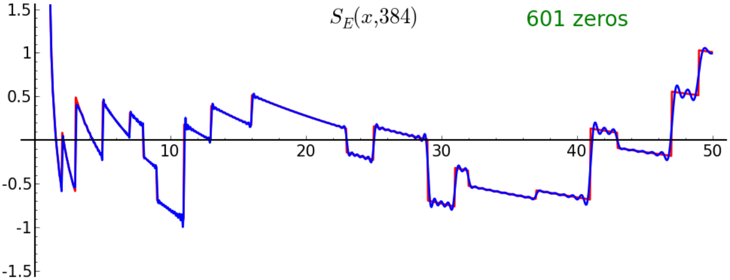
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1 - x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

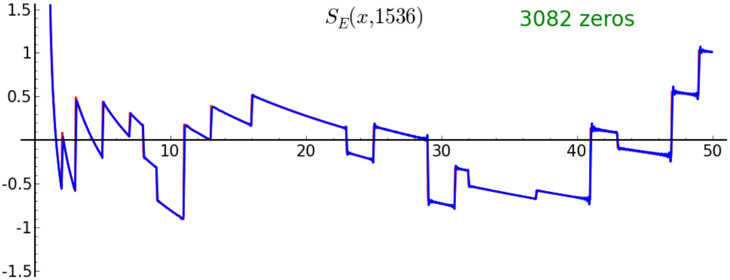
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1-x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

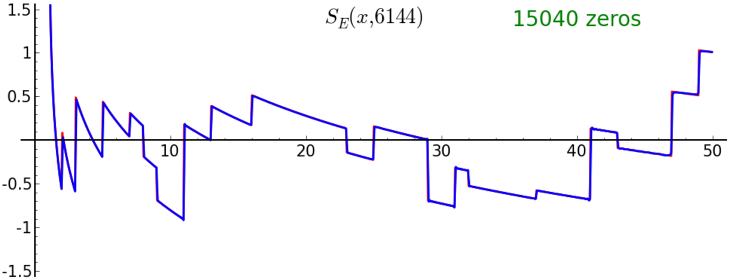
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1-x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1-x^{-1}) + \psi_E(x)$$



Proving the Explicit Formula

How do we go about proving this?:

Proving the Explicit Formula

How do we go about proving this?:

- Let $\sigma > \frac{1}{2}$ and consider the integral $\frac{-1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT} \frac{L_E'}{L_E}(s+1)\,\frac{x^s}{s}\;ds$

Proving the Explicit Formula

How do we go about proving this?:

- Let $\sigma > \frac{1}{2}$ and consider the integral $\frac{-1}{2\pi i} \int_{\sigma-iT}^{\sigma+iT} \frac{L_E'}{L_E}(s+1) \frac{x^s}{s} \, ds$
- Replace $\frac{L_E'}{L_E}(s+1)$ with two different series representations and distribute
- Replace each integral with contour integral on $\mathbb{C}$ plus residues
- Contour integrals $\to 0$ as $T \to \infty$.

Using the Cauchy Residue Theorem

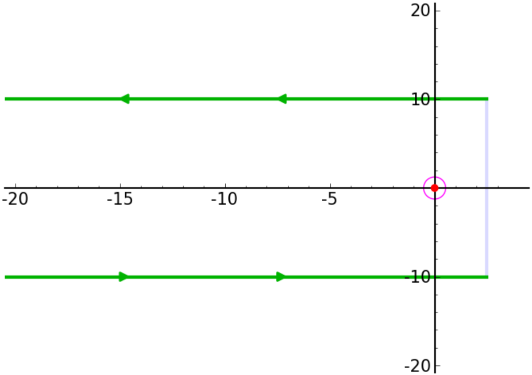
Example

$$\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT}\frac{x^s}{s}\,ds = 1+\frac{1}{2\pi i}\left(\int_{-\infty+iT}^{\sigma+iT}-\int_{-\infty-iT}^{\sigma-iT}\right)\frac{x^s}{s}\,ds$$

Using the Cauchy Residue Theorem

Example

$$\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT}\frac{x^s}{s}\,ds = 1+\frac{1}{2\pi i}\left(\int_{-\infty+iT}^{\sigma+iT}-\int_{-\infty-iT}^{\sigma-iT}\right)\frac{x^s}{s}\,ds$$



Improving the Explicit Formula

Current proofs (e.g. Iwaniec & Kowalski, Montgomery & Vaughn) only give asymptotic arguments for proofs.

Improving the Explicit Formula

Current proofs (e.g. Iwaniec & Kowalski, Montgomery & Vaughn) only give asymptotic arguments for proofs.

My Work:

Rework Proofs to include explicit constants on error terms.

Improving the Explicit Formula

Current proofs (e.g. Iwaniec & Kowalski, Montgomery & Vaughn) only give asymptotic arguments for proofs.

My Work:

Rework Proofs to include explicit constants on error terms.

Conjecture (S.)

Let $\epsilon(x, T) = S_E(x, T) + \eta + \log\left(\frac{2\pi}{\sqrt{N}}\right) + r_{an}\log x + \log(1 - x^{-1}) - \psi_E(x)$*. Then* $\exists$ *a positive constant* M *such that*

$$\epsilon(T, x) < M \cdot \frac{\log^2 T}{T} \cdot \frac{x + 1/x}{\log x}\left(1 + \sum_{n \neq x}\left|\frac{c_n}{n\log(\frac{x}{n})}\right|\right)$$

for $T >> 1$.

The Gibbs Phenomenon

Conjecture (S.)

$$\epsilon(T,x) < M \cdot \frac{\log^2 T}{T} \cdot \frac{x+1/x}{\log x}\left(1+\sum_{n\neq x}\left|\frac{c_n}{n\log(\frac{x}{n})}\right|\right) \text{ for } T >> 1.$$

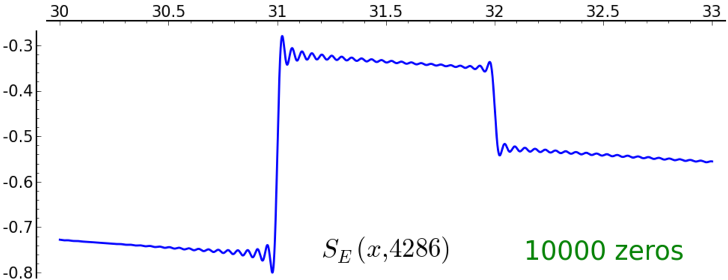


Figure: The Gibbs Phenomenon clearly visible at jump discontinuities for 37*a*.

The Hard Part

Why is this hard?

- Explicit proof requires us to bound integral of $\frac{\Lambda_E'}{\Lambda_E}(s+1)\frac{x^s}{s}$ across critical strip
- $\Rightarrow$ require explicit bounds on zero density along critical strip for EC L-functions.

Some Neat Corollaries

Loosely, $\{\text{nontrivial zeros of } L_E\} \sim \{a_p(E) : p \text{ prime}\}$ in an information theoretic sense. For example,

Some Neat Corollaries

Loosely, $\{$nontrivial zeros of $L_E\} \sim \{a_p(E) : p$ prime$\}$ in an information theoretic sense. For example,

Corollary (S.)

$$a_p = \lim_{T\to\infty} \frac{-2\pi p}{\log p} \cdot \frac{1}{T} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$$

Some Neat Corollaries

Loosely, {nontrivial zeros of L_E} $\sim$ {$a_p(E)$: p prime} in an information theoretic sense. For example,

Corollary (S.)

$$a_p = \lim_{T\to\infty} \frac{-2\pi p}{\log p} \cdot \frac{1}{T} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$$

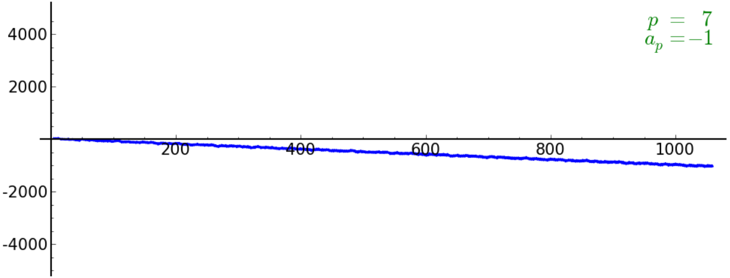


Figure: $\frac{-2\pi p}{\log p} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$ as a function of T for various small p

Some Neat Corollaries

Loosely, {nontrivial zeros of L_E} $\sim$ $\{a_p(E) : p \text{ prime}\}$ in an information theoretic sense. For example,

Corollary (S.)

$$a_p = \lim_{T\to\infty} \frac{-2\pi p}{\log p} \cdot \frac{1}{T} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$$

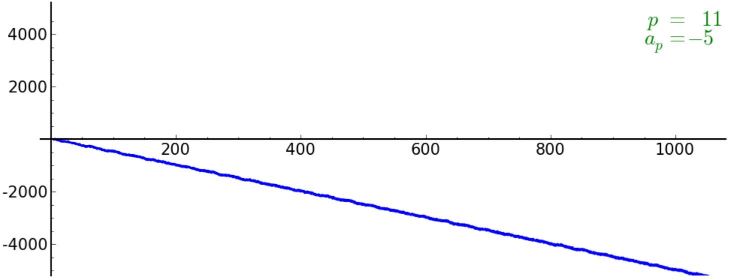


Figure: $\frac{-2\pi p}{\log p} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$ as a function of T for various small p

Some Neat Corollaries

Loosely, {nontrivial zeros of L_E} $\sim$ $\{a_p(E) : p \text{ prime}\}$ in an information theoretic sense. For example,

Corollary (S.)

$$a_p = \lim_{T\to\infty} \frac{-2\pi p}{\log p} \cdot \frac{1}{T} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$$

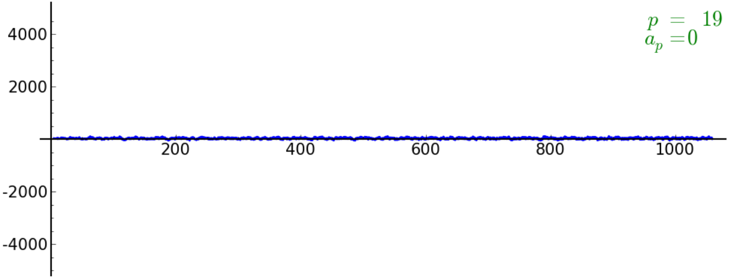


Figure: $\frac{-2\pi p}{\log p} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$ as a function of T for various small p

Some Neat Corollaries

Loosely, $\{\text{nontrivial zeros of } L_E\} \sim \{a_p(E) : p \text{ prime}\}$ in an information theoretic sense. For example,

Corollary (S.)

$$a_p = \lim_{T\to\infty} \frac{-2\pi p}{\log p} \cdot \frac{1}{T} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$$

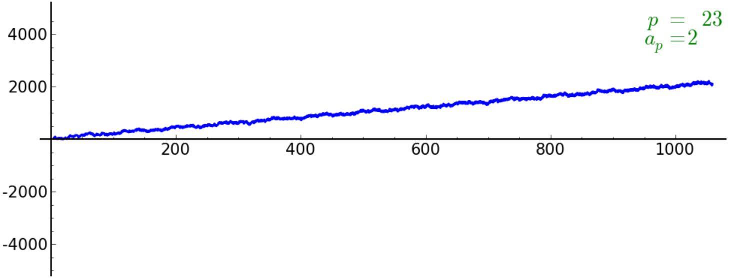


Figure: $\frac{-2\pi p}{\log p} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$ as a function of T for various small p

Some Neat Corollaries

Loosely, {nontrivial zeros of L_E} $\sim$ $\{a_p(E) : p \text{ prime}\}$ in an information theoretic sense. For example,

Corollary (S.)

$$a_p = \lim_{T\to\infty} \frac{-2\pi p}{\log p} \cdot \frac{1}{T} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$$

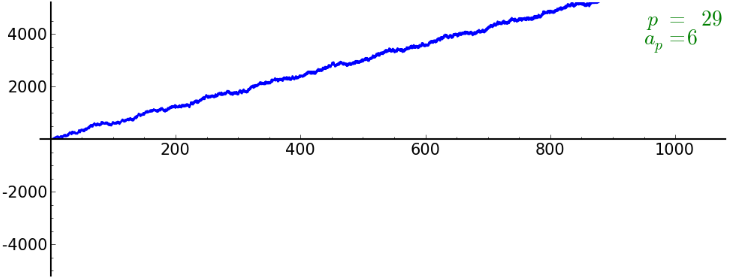


Figure: $\frac{-2\pi p}{\log p} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$ as a function of T for various small p

Some Neat Corollaries

Conjecture - Alternate BSD (Sarnak, Mazur)

For any given $E/\mathbb{Q}$,

$$\lim_{x\to\infty} \frac{1}{\log(x)} \sum_{p\leq x} \frac{-a_p \log(p)}{p} = r$$

Some Neat Corollaries

Conjecture - Alternate BSD (Sarnak, Mazur)

For any given $E/\mathbb{Q}$,

$$\lim_{x\to\infty} \frac{1}{\log(x)} \sum_{p\leq x} \frac{-a_p \log(p)}{p} = r$$

Where does this comes from?

Take explicit formula:

$$\sum_{\gamma} \frac{\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r\log x - \log(1 - 1/x) + \psi_E(x)$$

Divide both sides by $\log(x)$ and take limits*.

Future Work

Future Work

- Generalize to modular L-functions of arbitrary weight $+$ twist

Future Work

- Generalize to modular L-functions of arbitrary weight + twist
- Computing zeros more efficiently
  - Current best algorithms are polynomial in N
  - Would be great to get methods that are polynomial in $\log(N)$, or insensitive to N entirely

Future Work

- Generalize to modular L-functions of arbitrary weight $+$ twist
- Computing zeros more efficiently
  - Current best algorithms are polynomial in N
  - Would be great to get methods that are polynomial in $\log(N)$, or insensitive to N entirely
- Bounding rank analytically in an efficient way for given curves
  - Improve work of Bober et al

Future Work

- Generalize to modular L-functions of arbitrary weight + twist
- Computing zeros more efficiently
  - Current best algorithms are polynomial in N
  - Would be great to get methods that are polynomial in $\log(N)$, or insensitive to N entirely
- Bounding rank analytically in an efficient way for given curves
  - Improve work of Bober et al
- Location of the first nontrivial zero
  - No theorems currently exist giving bounds on the location of the first nontrivial zero in terms of N, r etc.

Future Work

- Generalize to modular L-functions of arbitrary weight + twist
- Computing zeros more efficiently
  - Current best algorithms are polynomial in N
  - Would be great to get methods that are polynomial in $\log(N)$, or insensitive to N entirely
- Bounding rank analytically in an efficient way for given curves
  - Improve work of Bober et al
- Location of the first nontrivial zero
  - No theorems currently exist giving bounds on the location of the first nontrivial zero in terms of N, r etc.
- Computing conductor efficiently via analytic methods?

Ngiyabonga Kakhulu

Ngiyabonga Kakhulu

Hamba Kahle!