L-Functions: A Crash Course

Simon Spicer

University of Washington

mlungu@uw.edu

July 2, 2013

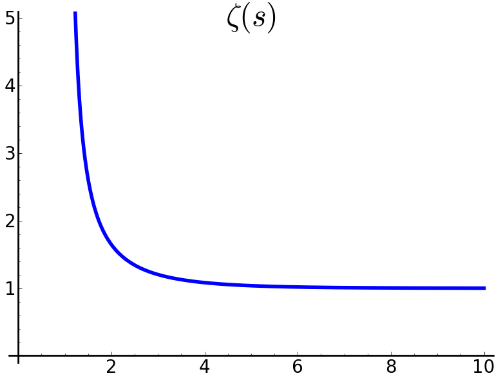
Introduction: The Riemann Zeta Function

Introduction: The Riemann Zeta Function

Let $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ be the Riemann zeta function.

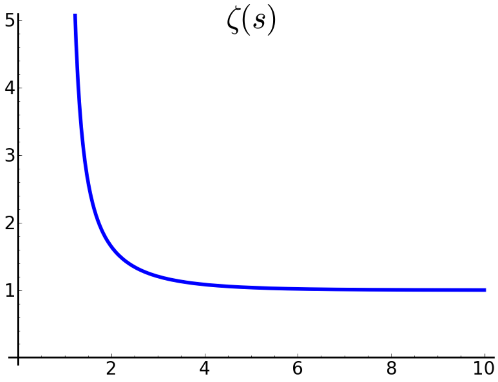
Introduction: The Riemann Zeta Function

Let $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ be the Riemann zeta function.



Introduction: The Riemann Zeta Function

Let $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ be the Riemann zeta function.



This Dirichlet series converges absolutely for any complex s with $\Re(s) > 1$

The Euler product

The Euler product

Theorem (Euler 1737)

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

where the product is taken over all primes, and the product converges absolutely for $\Re(s) > 1$.

The Euler product

Theorem (Euler 1737)

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

where the product is taken over all primes, and the product converges absolutely for $\Re(s) > 1$.

"Proof"

$$\begin{aligned}
\sum_{n=1}^{\infty} n^{-s} &= 1^{-s} + 2^{-s} + 3^{-s} + 4^{-s} + \dots \\
&= \left(1^{-s} + 2^{-s} + (2^2)^{-s} + \dots\right)\left(1^{-s} + 3^{-s} + (3^2)^{-s} + \dots\right)\cdots \\
&= \left[(2^{-s})^0 + (2^{-s})^1 + (2^{-s})^2 \dots\right]\left[(3^{-s})^0 + (3^{-s})^1 + (3^{-s})^2 \dots\right]\cdots \\
&= \left(\frac{1}{1-2^{-s}}\right)\left(\frac{1}{1-3^{-s}}\right)\left(\frac{1}{1-5^{-s}}\right)\cdots
\end{aligned}$$

Extending $\zeta(s)$ to a Larger Domain

Can we get better convergence for $\zeta(s)$?

Extending $\zeta(s)$ to a Larger Domain

Can we get better convergence for $\zeta(s)$? Yes! Observe:

$$\begin{aligned} 2^{-s}\zeta(s) &= 2^{-s}\sum_{n=1}^{\infty} n^{-s} \\ &= \sum_{n=1}^{\infty}(2n)^{-s} \end{aligned}$$

Extending $\zeta(s)$ to a Larger Domain

Can we get better convergence for $\zeta(s)$? Yes! Observe:

$$\begin{aligned} 2^{-s}\zeta(s) &= 2^{-s}\sum_{n=1}^{\infty} n^{-s} \\ &= \sum_{n=1}^{\infty}(2n)^{-s} \end{aligned}$$

So

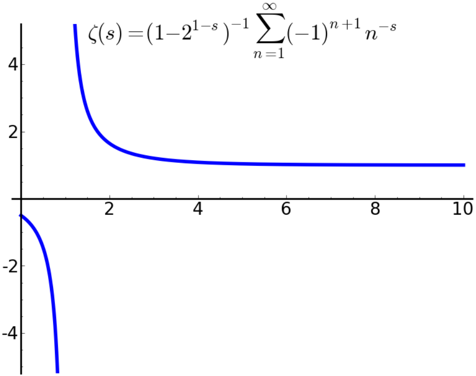
$$\begin{aligned} &(1-2\cdot 2^{-s})\zeta(s) = \zeta(s) - 2\cdot 2^{-s}\zeta(s) \\ &= \left(1^{-s}+2^{-s}+3^{-s}+\ldots\right) - \left(2\cdot 2^{-s}+2\cdot 4^{-s}+2\cdot 6^{-s}+\ldots\right) \\ &= 1^{-s}-2^{-s}+3^{-s}-4^{-s}+\ldots \\ &= \sum_{n=1}^{\infty}(-1)^{n+1}n^{-s}. \end{aligned}$$

Extending $\zeta(s)$ to a Larger Domain

$\sum_{n=1}^{\infty}(-1)^{n+1}n^{-s}$ converges (conditionally) on the strip $0 < \Re(s) \leq 1$, so we can use it to define $\zeta(s)$ on the entire right half plane.

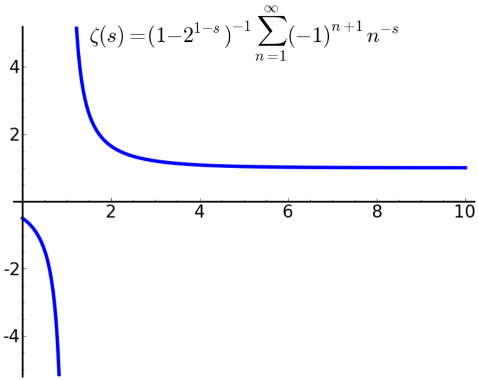
Extending $\zeta(s)$ to a Larger Domain

$\sum_{n=1}^{\infty}(-1)^{n+1}n^{-s}$ converges (conditionally) on the strip $0 < \Re(s) \leq 1$, so we can use it to define $\zeta(s)$ on the entire right half plane.



Extending $\zeta(s)$ to a Larger Domain

$\sum_{n=1}^{\infty}(-1)^{n+1}n^{-s}$ converges (conditionally) on the strip $0 < \Re(s) \leq 1$, so we can use it to define $\zeta(s)$ on the entire right half plane.



We can see $\zeta(s)$ clearly has a pole at $s = 1$.

The Completed Zeta Function

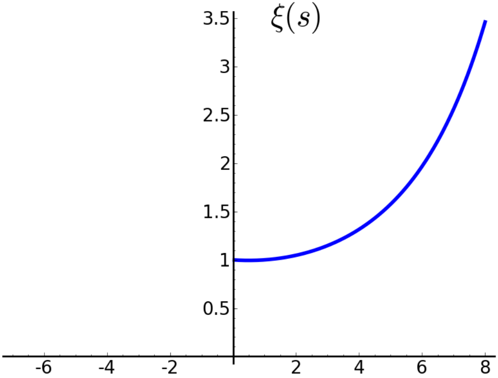
Define the *completed zeta function*

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

The Completed Zeta Function

Define the *completed zeta function*

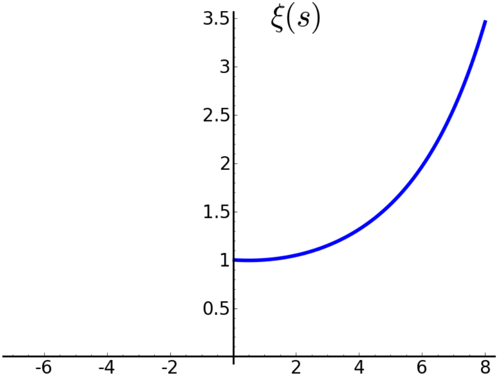
$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$



The Completed Zeta Function

Define the *completed zeta function*

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

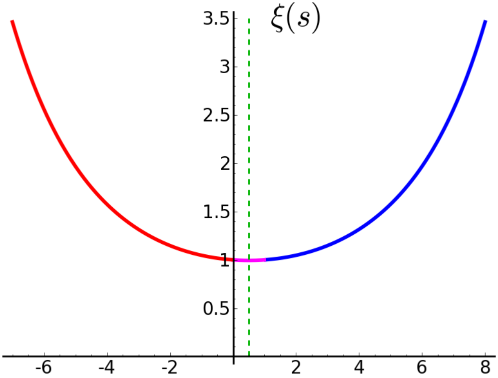


We can show that $\xi(s) = \xi(1-s)$ on the strip $0 < \Re(s) < 1$, so we use this to extend $\zeta(s)$ to all of $\mathbb{C}$.

The Completed Zeta Function

Define the *completed zeta function*

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$



We can show that $\xi(s) = \xi(1-s)$ on the strip $0 < \Re(s) < 1$, so we use this to extend $\zeta(s)$ to all of $\mathbb{C}$.

$\zeta(s)$ Analytically continued to $\mathbb{C}$

So we have

$$zeta(s) = \begin{cases} (1-2^{1-s})^{-1}\sum_{n=1}^{\infty}(-1)^{n+1}n^{-s} & \Re(s) > 0 \\ 2^s\pi^{s-1}\sin\left(\frac{\pi s}{2}\right)\Gamma(1-s)\zeta(1-s) & \Re(s) \le 0 \end{cases}$$

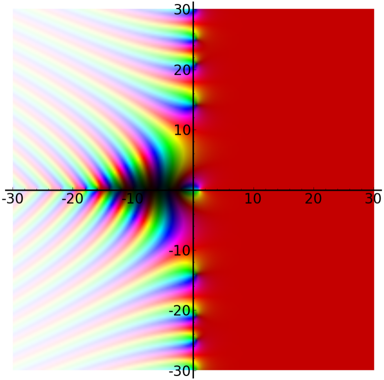
defined for all $s \in \mathbb{C}$ except $s = 1$.

$\zeta(s)$ Analytically continued to $\mathbb{C}$

So we have

$$zeta(s) = \begin{cases} (1-2^{1-s})^{-1}\sum_{n=1}^{\infty}(-1)^{n+1}n^{-s} & \Re(s) > 0 \\ 2^s\pi^{s-1}\sin\left(\frac{\pi s}{2}\right)\Gamma(1-s)\zeta(1-s) & \Re(s) \leq 0 \end{cases}$$

defined for all $s \in \mathbb{C}$ except $s = 1$.



The Poles and Zeros of $\zeta(s)$

We can show $\zeta(s)$ has:

- a single simple pole at $s = 1$ with residue 1, and no other poles on $\mathbb{C}$

The Poles and Zeros of $\zeta(s)$

We can show $\zeta(s)$ has:

- a single simple pole at $s = 1$ with residue 1, and no other poles on $\mathbb{C}$
- simple zeros at $-2, -4, -6, -8 \ldots$ coming from the $\Gamma(s/2)$ part of the functional equation, called the *trivial zeros*

The Poles and Zeros of $\zeta(s)$

We can show $\zeta(s)$ has:

- a single simple pole at $s = 1$ with residue 1, and no other poles on $\mathbb{C}$
- simple zeros at $-2, -4, -6, -8 \ldots$ coming from the $\Gamma(s/2)$ part of the functional equation, called the *trivial zeros*
- no other zeros outside the vertical strip $0 < \Re(s) < 1$

The Poles and Zeros of $\zeta(s)$

We can show $\zeta(s)$ has:

- a single simple pole at $s = 1$ with residue 1, and no other poles on $\mathbb{C}$
- simple zeros at $-2, -4, -6, -8\ldots$ coming from the $\Gamma(s/2)$ part of the functional equation, called the *trivial zeros*
- no other zeros outside the vertical strip $0 < \Re(s) < 1$
- an infinite number of zeros inside the strip $0 < \Re(s) < 1$, symmetric about the real axis and $\Re(s) = \frac{1}{2}$, called the *nontrivial zeros*

The Poles and Zeros of $\zeta(s)$

We can show $\zeta(s)$ has:

- a single simple pole at $s = 1$ with residue 1, and no other poles on $\mathbb{C}$
- simple zeros at $-2, -4, -6, -8\ldots$ coming from the $\Gamma(s/2)$ part of the functional equation, called the *trivial zeros*
- no other zeros outside the vertical strip $0 < \Re(s) < 1$
- an infinite number of zeros inside the strip $0 < \Re(s) < 1$, symmetric about the real axis and $\Re(s) = \frac{1}{2}$, called the *nontrivial zeros*

Conjecture (Riemann Hypothesis)

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

The Zeros of ζ

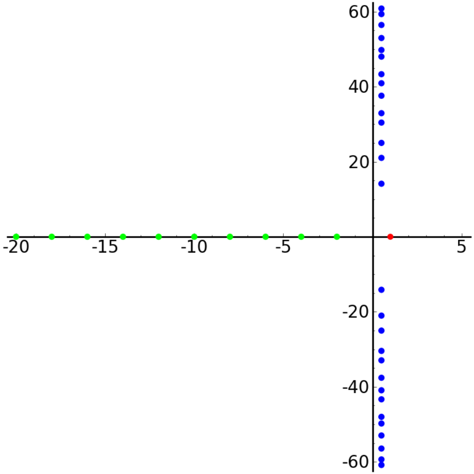
The imaginary parts of the first few zeros of $\zeta(s)$ in the upper half plane are

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

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 $\zeta(s)$

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

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho}$$

where ρ runs over nontrivial zeros of $\zeta(s)$.

The Explicit Formula for $\zeta(s)$

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

$$S_\zeta(x, T) = \sum_{|\rho| < T} \frac{x^\rho}{\rho}$$

where ρ runs over nontrivial zeros of $\zeta(s)$.
According to RH, nontrivial zeros come in pairs and have the form $\rho = \frac{1}{2} \pm i\gamma$, so in the above sum for a single zero pair we have

$$\begin{aligned}\frac{x^\rho}{\rho} + \frac{x^{\overline{\rho}}}{\overline{\rho}} &= \frac{x^{1/2+i\gamma}}{1/2 + i\gamma} + \frac{x^{1/2-i\gamma}}{1/2 - i\gamma} \\ &= \frac{\sqrt{x}}{1/4 + \gamma^2} \left[\cos(\gamma \log x) + 2\gamma \sin(\gamma \log x)\right]\end{aligned}$$

The Explicit Formula for $\zeta(s)$

Contingent on the Riemann Hypothesis:

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x} \left(\sum_{0<\gamma<T} \frac{\cos(\gamma \log x) + 2\gamma \sin(\gamma \log x)}{1/4 + \gamma^2} \right)$$

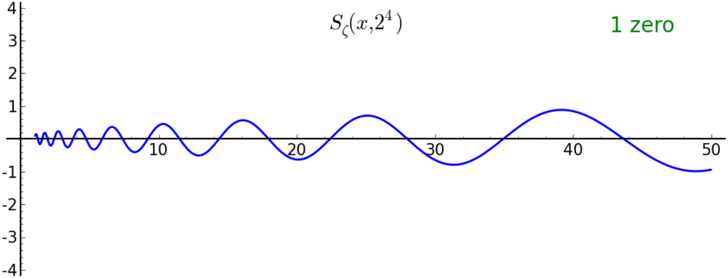
where γ runs over imaginary parts of nontrivial zeros.

The Explicit Formula for $\zeta(s)$

Contingent on the Riemann Hypothesis:

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{\cos(\gamma \log x) + 2\gamma \sin(\gamma \log x)}{1/4 + \gamma^2}\right)$$

where γ runs over imaginary parts of nontrivial zeros.

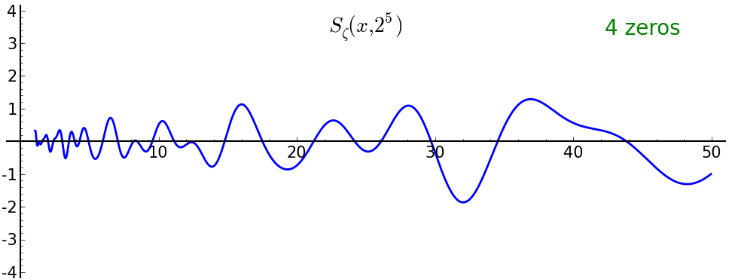


The Explicit Formula for $\zeta(s)$

Contingent on the Riemann Hypothesis:

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{\cos(\gamma \log x) + 2\gamma \sin(\gamma \log x)}{1/4 + \gamma^2}\right)$$

where γ runs over imaginary parts of nontrivial zeros.

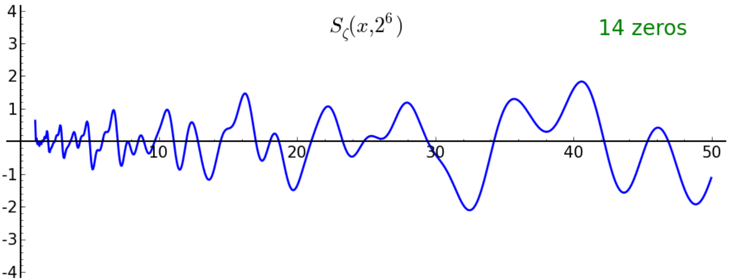


The Explicit Formula for $\zeta(s)$

Contingent on the Riemann Hypothesis:

$$S_\zeta(x,T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{\cos(\gamma \log x) + 2\gamma \sin(\gamma \log x)}{1/4+\gamma^2}\right)$$

where γ runs over imaginary parts of nontrivial zeros.

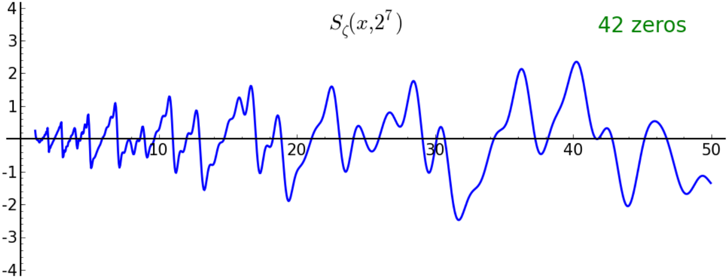


The Explicit Formula for $\zeta(s)$

Contingent on the Riemann Hypothesis:

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{\cos(\gamma \log x) + 2\gamma \sin(\gamma \log x)}{1/4 + \gamma^2}\right)$$

where γ runs over imaginary parts of nontrivial zeros.

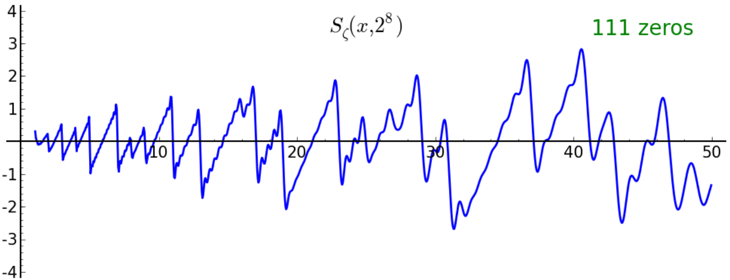


The Explicit Formula for $\zeta(s)$

Contingent on the Riemann Hypothesis:

$$S_\zeta(x,T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{\cos(\gamma \log x) + 2\gamma \sin(\gamma \log x)}{1/4+\gamma^2}\right)$$

where γ runs over imaginary parts of nontrivial zeros.

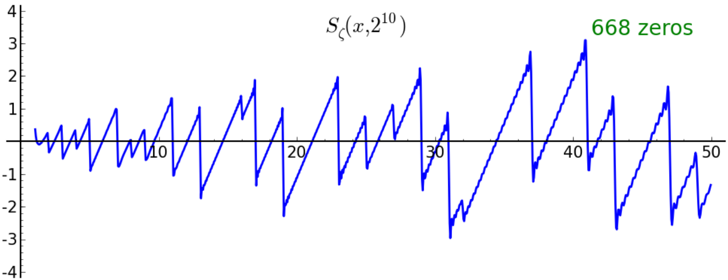


The Explicit Formula for $\zeta(s)$

Contingent on the Riemann Hypothesis:

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{\cos(\gamma\log x) + 2\gamma\sin(\gamma\log x)}{1/4+\gamma^2}\right)$$

where γ runs over imaginary parts of nontrivial zeros.

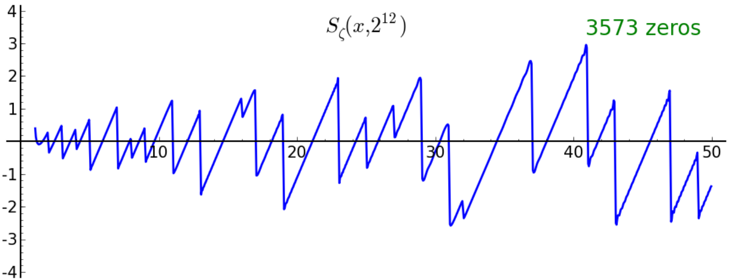


The Explicit Formula for $\zeta(s)$

Contingent on the Riemann Hypothesis:

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{\cos(\gamma \log x) + 2\gamma \sin(\gamma \log x)}{1/4 + \gamma^2}\right)$$

where γ runs over imaginary parts of nontrivial zeros.

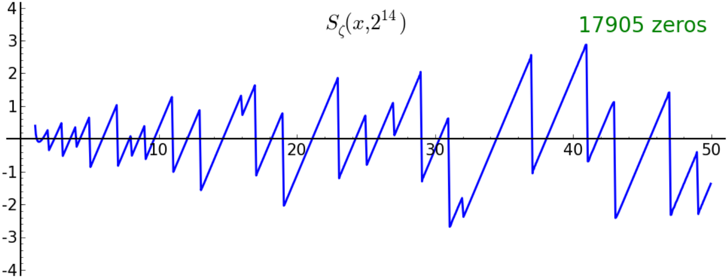


The Explicit Formula for $\zeta(s)$

Contingent on the Riemann Hypothesis:

$$S_\zeta(x, T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{\cos(\gamma \log x) + 2\gamma \sin(\gamma \log x)}{1/4 + \gamma^2}\right)$$

where γ runs over imaginary parts of nontrivial zeros.

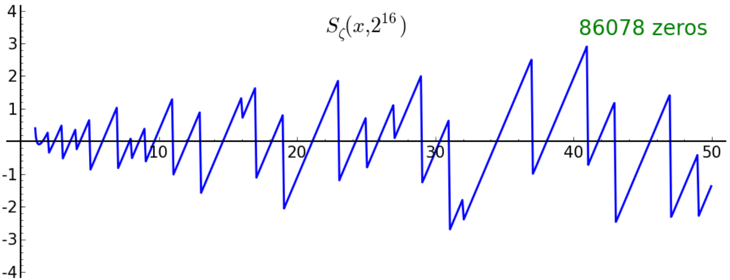


The Explicit Formula for $\zeta(s)$

Contingent on the Riemann Hypothesis:

$$S_\zeta(x,T) = \sum_{|\rho|<T} \frac{x^\rho}{\rho} = \sqrt{x}\left(\sum_{0<\gamma<T} \frac{\cos(\gamma\log x) + 2\gamma\sin(\gamma\log x)}{1/4+\gamma^2}\right)$$

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?

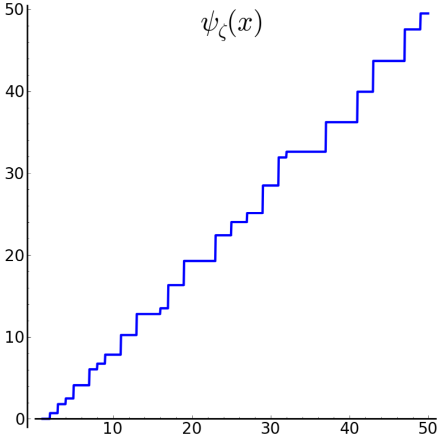
Theorem (Riemann 1858, von Mangoldt 1905)

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

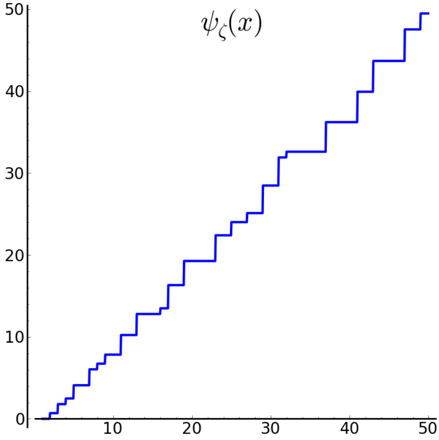
where $\psi_{\zeta}(x) = \sum_{p^e \leq x}' \log p$ *is the second Chebyshev function.*

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

The Explicit Formula for $\zeta(s)$



The Explicit Formula for $\zeta(s)$



Equivalent Formulation of the Riemann Hypothesis

The above function $\psi_\zeta(x) = x + O(x^{1/2+\epsilon})$ for arbitrarily small $\epsilon > 0$.

L-Functions

- $\zeta(s)$ is the prototypical example of an *L-function*: a meromorphic function on $\mathbb{C}$ that encode various arithmetic data about a particular algebraic object.

L-Functions

- $\zeta(s)$ is the prototypical example of an *L-function*: a meromorphic function on $\mathbb{C}$ that encode various arithmetic data about a particular algebraic object.
- For example, the explicit formula for $\zeta(s)$ shows that it encodes the locations of the prime numbers.

L-Functions

- $\zeta(s)$ is the prototypical example of an *L-function*: a meromorphic function on $\mathbb{C}$ that encode various arithmetic data about a particular algebraic object.
- For example, the explicit formula for $\zeta(s)$ shows that it encodes the locations of the prime numbers.
- Can define analogous L-functions attached to other number-theoretic objects:
  - Number fields
  - Modular forms
  - Elliptic curves
  - And many more

L-Functions

- $\zeta(s)$ is the prototypical example of an *L-function*: a meromorphic function on $\mathbb{C}$ that encode various arithmetic data about a particular algebraic object.
- For example, the explicit formula for $\zeta(s)$ shows that it encodes the locations of the prime numbers.
- Can define analogous L-functions attached to other number-theoretic objects:
  - Number fields
  - Modular forms
  - Elliptic curves
  - And many more

I will show what you can do with elliptic curve L-functions.

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

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

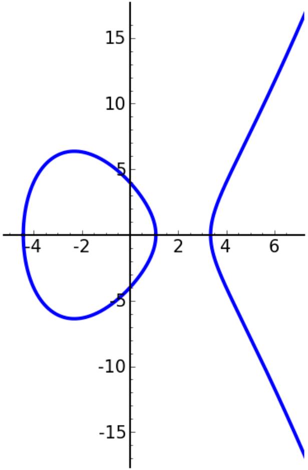


Figure: The Elliptic Curve 37*a*

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

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

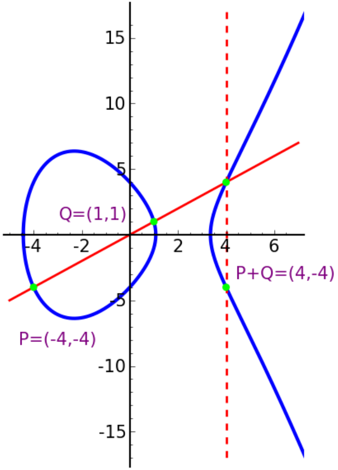


Figure: The Elliptic Curve 37a

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

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

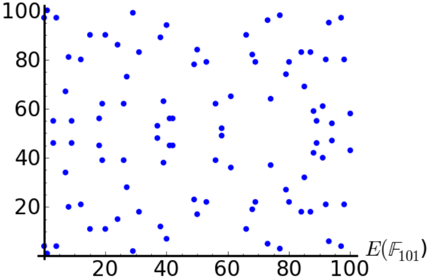
Consider its solutions (x, y) modulo 101, e.g. $(40, 7)$:

Elliptic Curves over finite fields

Example

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

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

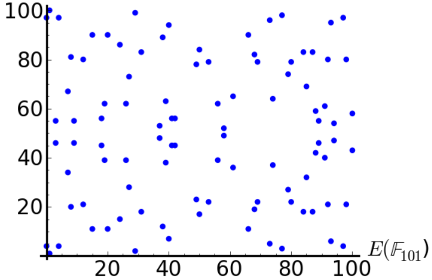


Elliptic Curves over finite fields

Example

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

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



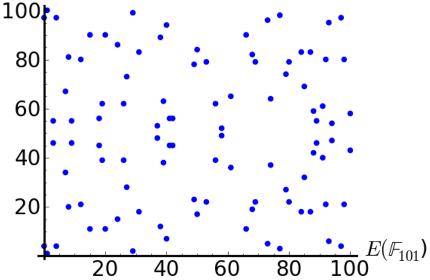
Let $\#E(\mathbb{F}_p)$ be the number of points on E modulo the prime p.

Elliptic Curves over finite fields

Example

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

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



Let $\#E(\mathbb{F}_p)$ be the number of points on E modulo the prime p.

Theorem (Hasse, 1936)

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p} \quad \textit{for all } p.$$

Elliptic Curves over finite fields

Definition

For prime p , let $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$.

Elliptic Curves over finite fields

Definition

For prime p , let $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$.

So an alternate statement of Hasse's Theorem is that $|a_p| \leq 2\sqrt{p}$ always.

Elliptic Curves over finite fields

Definition

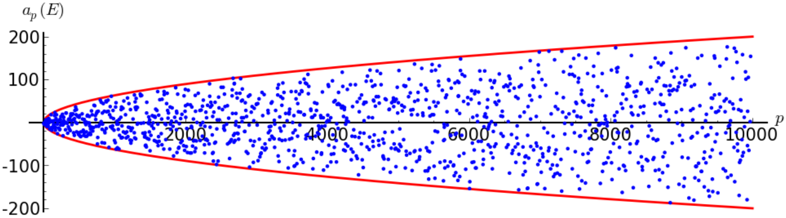
For prime p , let $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$.

So an alternate statement of Hasse's Theorem is that $|a_p| \leq 2\sqrt{p}$ always.

Example

$E = 37a$

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 N of an elliptic curve E is a positive integer that encapsulates primes of bad reduction for E, i.e. primes for which when we look at the set of points on E modulo p, *bad stuff** happens.

The Conductor of a Curve

Definition

The conductor N of an elliptic curve E is a positive integer that encapsulates primes of bad reduction for E, i.e. primes for which when we look at the set of points on E modulo p, *bad stuff** happens.

Example

The conductor of $37a$ is $N = 37$, hence its name. That is, bad stuff only happens for this elliptic curve at $p = 37$.

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

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

Analytic Continuation of $L_E(s)$

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

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

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

where $w = 1$ or -1 depending on the elliptic curve.

Analytic Continuation of $L_E(s)$

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

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

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

where $w = 1$ or -1 depending on the elliptic curve.

Notably, unlike $\zeta(s)$, $L_E(s)$ has no poles on $\mathbb{C}$ for any given elliptic curve E.

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 $\Re(s) = 1$.

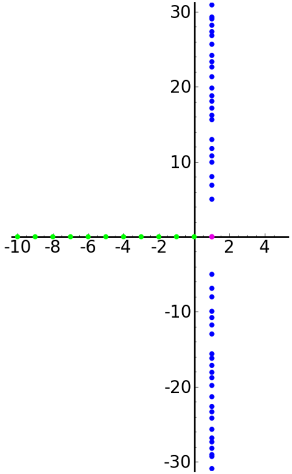


Figure: The zeros of $L_E(s)$ for $E = 37a$

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*

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

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*

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

where

- *Ω_E is the real period of (an optimal model of) E,*
- *Reg_E is the regulator of E,*
- *$\#Ш(E/\mathbb{Q})$ 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.*

Things You Can Do With EC L-functions

Things You Can Do With EC L-functions

Proposition

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

$$N > \frac{1}{5}e^{2r}$$

Things You Can Do With EC L-functions

Proposition

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

$$N > \frac{1}{5}e^{2r}$$

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

Things You Can Do With EC L-functions

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

Things You Can Do With EC L-functions

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

Proposition

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

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

where γ runs over the imaginary parts of the nontrivial zeros of $L_E(s)$ (excluding $s = 1$), and $\eta = 0.57721566\ldots$ is the Euler-Mascheroni constant.

Recursive formulae exist for higher coefficients as well.

The Explicit Formula for Elliptic Curves

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 $s = 1$

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

  where $c_n(E) = -\left(p^e + 1 - \#\widetilde{E}(\mathbb{F}_{p^e})\right) \cdot \frac{\log(p)}{p^e}$ for $n = p^e$ a perfect prime power, and 0 otherwise.

The Explicit Formula for Elliptic Curves

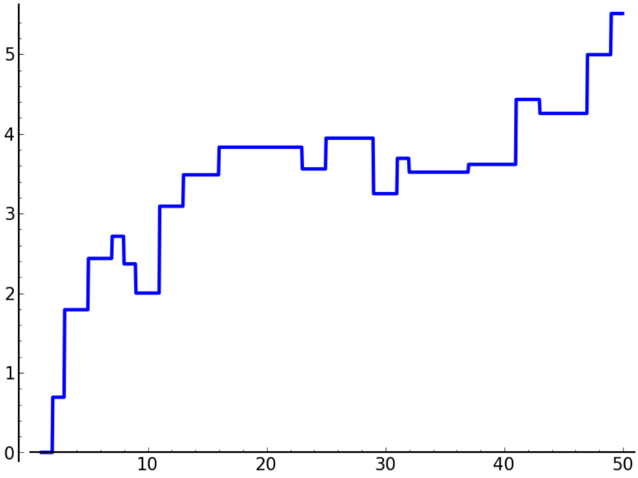


Figure: $\psi_E(x)$ for $E = 37a$

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,

$$\lim_{T\to\infty} S_E(x, T) = \sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma}$$

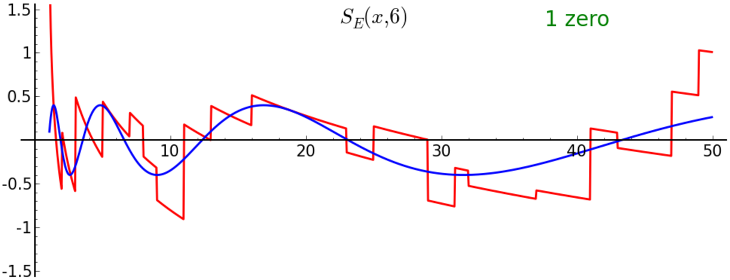
$$= -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1 - x^{-1}) + \psi_E(x)$$

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

The Explicit Formula for Elliptic Curves

Theorem

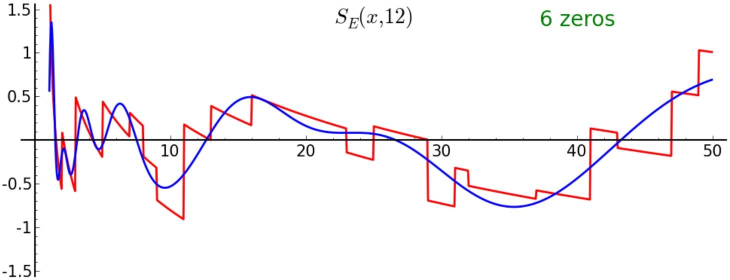
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an} \log x - \log(1 - x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

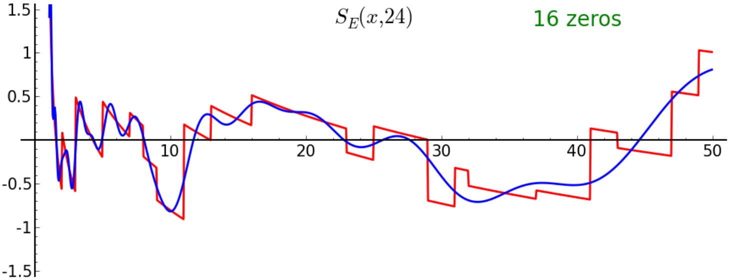
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1-x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

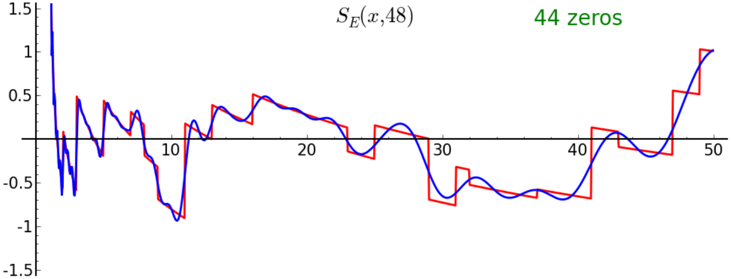
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an} \log x - \log(1 - x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

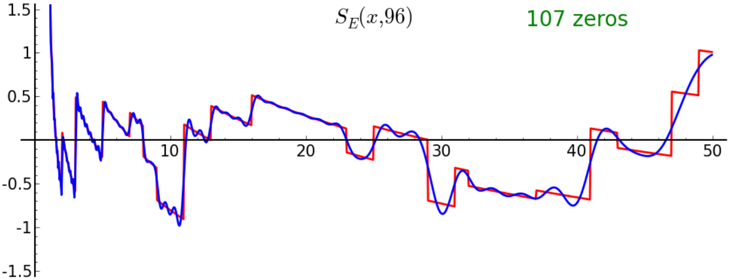
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an} \log x - \log(1 - x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

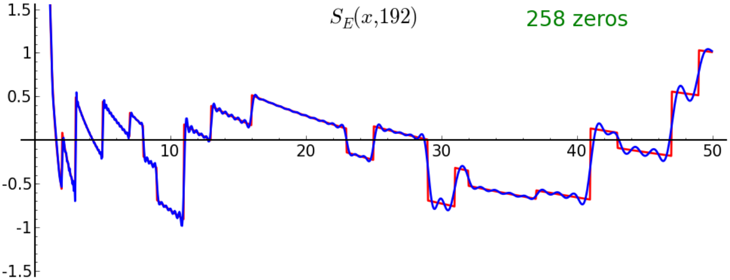
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1 - x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

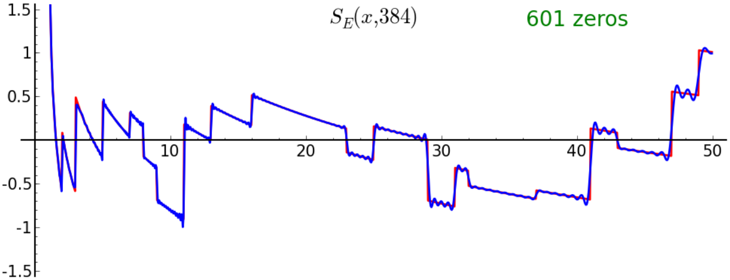
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1 - x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

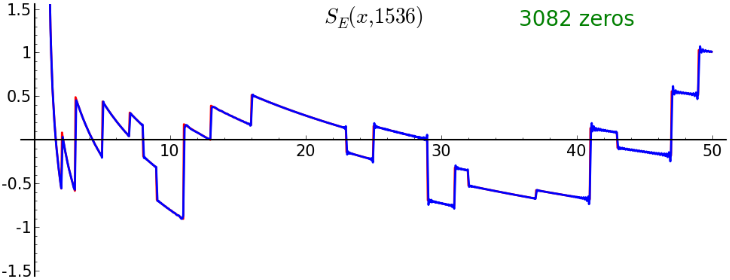
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an} \log x - \log(1 - x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

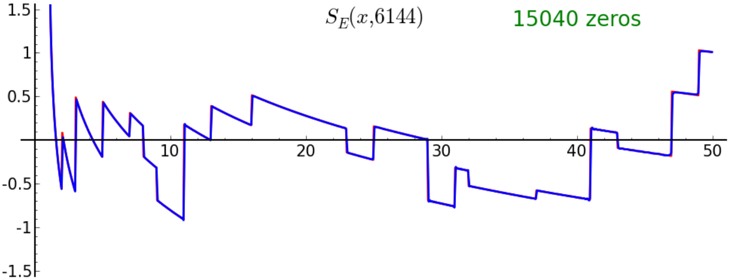
$$\sum_{\gamma>0} \frac{2\sin(\gamma \log x)}{\gamma} = -\eta - \log\left(\frac{2\pi}{\sqrt{N}}\right) - r_{an}\log x - \log(1-x^{-1}) + \psi_E(x)$$



The Explicit Formula for Elliptic Curves

Theorem

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



Some Neat Corollaries

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

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.)

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

Some Neat Corollaries

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

Corollary (S.)

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

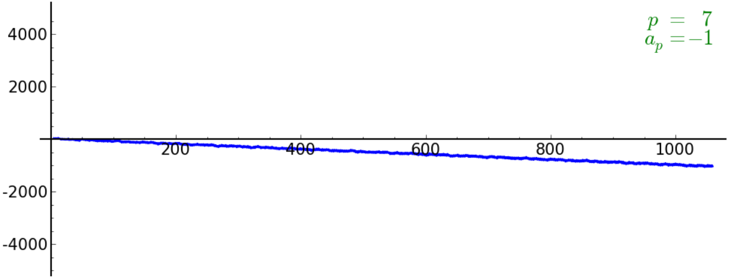


Figure: $\frac{-2\pi p}{\log p} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$ as a function of T for various small p

Some Neat Corollaries

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

Corollary (S.)

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

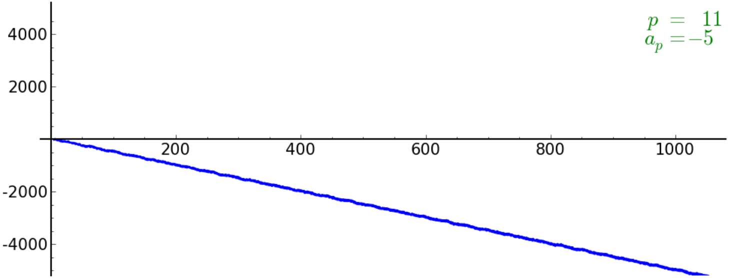


Figure: $\frac{-2\pi p}{\log p} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$ as a function of T for various small p

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.)

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

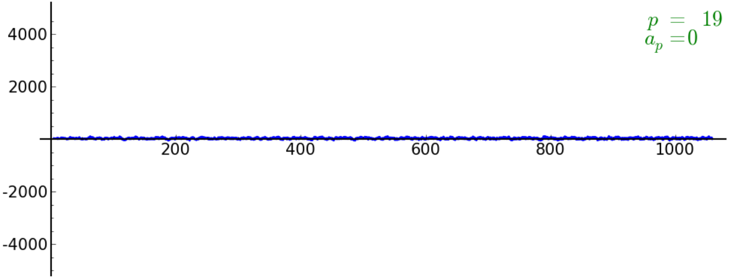


Figure: $\frac{-2\pi p}{\log p} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$ as a function of T for various small p

Some Neat Corollaries

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

Corollary (S.)

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

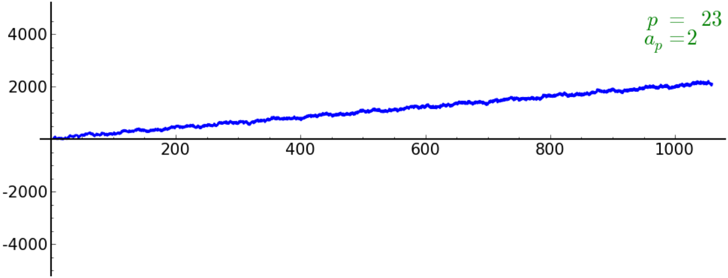


Figure: $\frac{-2\pi p}{\log p} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$ as a function of T for various small p

Some Neat Corollaries

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

Corollary (S.)

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

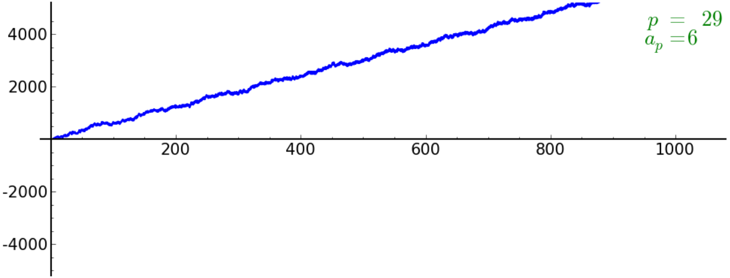


Figure: $\frac{-2\pi p}{\log p} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}$ as a function of T for various small p

Some Neat Corollaries

Conjecture - Alternate BSD Part 1 (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 Part 1 (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*.

Ngiyabonga Kakhulu

Ngiyabonga Kakhulu

Hamba Kahle!