L-Functions: A Crash Course

Simon Spicer

University of Washington
mlungu@uw.edu

July 2, 2013
Introduction: The Riemann Zeta Function

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

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

\[ \zeta(s) = \prod_{p} \frac{1}{1-p^{-s}} \] 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 \( \Re(s) > 1 \).
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”

\[ \sum_{n=1}^{\infty} n^{-s} = 1^{-s} + 2^{-s} + 3^{-s} + 4^{-s} + \ldots \\
= (1^{-s} + 2^{-s} + (2^2)^{-s} + \ldots) \left(1^{-s} + 3^{-s} + (3^2)^{-s} + \ldots\right) \ldots \\
= \left[(2^{-s})^0 + (2^{-s})^1 + (2^{-s})^2 \ldots\right] \left[(3^{-s})^0 + (3^{-s})^1 + (3^{-s})^2 \ldots\right] \ldots \\
= \left(\frac{1}{1 - 2^{-s}}\right) \left(\frac{1}{1 - 3^{-s}}\right) \left(\frac{1}{1 - 5^{-s}}\right) \ldots \]
Extending $\zeta(s)$ to a Larger Domain

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

Yes! Observe:

$$2 - s \zeta(s) = 2 - \sum_{n=1}^{\infty} n^{-s} = \sum_{n=1}^{\infty} (2n)^{-s} - s \zeta(s) = (1 - 2 \cdot 2^{-s} + 3 \cdot 3^{-s} - \ldots) - (2 \cdot 2^{-s} - 2 \cdot 4^{-s} + 2 \cdot 6^{-s} - \ldots) = 1 - s - 2^{-s} + 3^{-s} - 4^{-s} - \ldots.$$
Extending $\zeta(s)$ to a Larger Domain

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

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

$$= \sum_{n=1}^{\infty} (2n)^{-s}$$
Extending $\zeta(s)$ to a Larger Domain

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

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

$$= \sum_{n=1}^{\infty} (2n)^{-s}$$

So

$$(1 - 2 \cdot 2^{-s}) \zeta(s) = \zeta(s) - 2 \cdot 2^{-s} \zeta(s)$$

$$= (1^{-s} + 2^{-s} + 3^{-s} + \ldots) - (2 \cdot 2^{-s} + 2 \cdot 4^{-s} + 2 \cdot 6^{-s} + \ldots)$$

$$= 1^{-s} - 2^{-s} + 3^{-s} - 4^{-s} + \ldots$$

$$= \sum_{n=1}^{\infty} (-1)^{n+1} n^{-s}.$$
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.

$\zeta(s) = (1-2^{1-s})^{-1} \sum_{n=1}^{\infty}(-1)^{n+1}n^{-s}$
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 $s = 1$. 
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 \( \mathbb{C} \).
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 \( \mathbb{C} \).
ζ(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 $s = 1$. 

ζ(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 $\zeta$ are simple and lie on the line $\Re(s) = \frac{1}{2}$.***
The Zeros of $\zeta$

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 Zeros of $\zeta$

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...

[Graph showing the imaginary parts of the zeros]
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 $\rho$ 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 $\rho$ 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

$$\frac{x^\rho}{\rho} + \frac{x^{\overline{\rho}}}{\overline{\rho}} = \frac{x^{1/2+i\gamma}}{1/2 + i\gamma} + \frac{x^{1/2-i\gamma}}{1/2 - i\gamma}$$

$$= \frac{\sqrt{x}}{1/4 + \gamma^2} \left[ \cos(\gamma \log x) + 2\gamma \sin(\gamma \log x) \right]$$
The Explicit Formula for $\zeta(s)$

Contingent on the Riemann Hypothesis:

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

where $\gamma$ 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 $\gamma$ 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 $\gamma$ 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 $\gamma$ runs over imaginary parts of nontrivial zeros.

where $\gamma$ 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 $\gamma$ 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 $\gamma$ 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 $\gamma$ runs over imaginary parts of nontrivial zeros.

![Graph of $S_\zeta(x, 2^{10})$ with 668 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 $\gamma$ 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 $\gamma$ 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 $\gamma$ runs over imaginary parts of nontrivial zeros.
The Explicit Formula for $\zeta(s)$

What does this sum converge to?

$$\sum \rho = \lim_{T \to \infty} S(\zeta(x, T)) = x - \frac{1}{2} \log \left(1 - \frac{1}{x^2}\right) - \log(2\pi) - \psi(\zeta(x))$$

where $\psi(\zeta(x)) = \sum' p \leq x \log p$ is the second Chebyshev function.

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

What does this sum converge to?

**Theorem (Riemann 1858, von Mangoldt 1905)**

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

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)**

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

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

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

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

Simon Spicer (UW)
L-Functions and their Zeros
July 2, 2013 13 / 32
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 $\epsilon > 0$. 

Simon Spicer (UW)

L-Functions and their Zeros

July 2, 2013 13 / 32
\( \zeta(s) \) is the prototypical example of an \textit{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 \textit{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.
\( \zeta(s) \) is the prototypical example of an \textit{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 \textit{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 $\mathcal{O}$. 

For This Talk:

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

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

Figure: The Elliptic Curve 37
**Elliptic Curves**

**Definition**
An elliptic curve $E$ is a smooth projective genus 1 algebraic curve with a marked point $O$.

**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 $O$.

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

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 $O$.

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

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

Figure: The Elliptic Curve 37a
Theorem (Mordell 1922, Weil 1928)

\[ E(\mathbb{Q}) \approx E(\mathbb{Q})_{\text{TOR}} \times \mathbb{Z}^r \]

where \( E(\mathbb{Q})_{\text{TOR}} \) 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)

\[ E(\mathbb{Q}) \approx E(\mathbb{Q})_{\text{TOR}} \times \mathbb{Z}^r \]

where \( E(\mathbb{Q})_{\text{TOR}} \) 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 \( P = (0, 4) \):

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n )</td>
<td>( nP )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>( \emptyset )</td>
<td>( (0, 4) )</td>
<td>( (4, 4) )</td>
<td>( (-4, -4) )</td>
<td>( (8, -20) )</td>
<td>( (1, -1) )</td>
<td>( (24, 116) )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n )</td>
<td>( nP )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>( (-\frac{20}{9}, \frac{172}{27}) )</td>
<td>( \frac{84}{25}, -\frac{52}{125} )</td>
<td>( -\frac{80}{49}, -\frac{2108}{343} )</td>
</tr>
</tbody>
</table>
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 $p$. 

![Graph showing points on an elliptic curve modulo 101]
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)

\[ p + 1 - 2\sqrt{p} \leq #E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p} \quad \text{for all } p. \]
Elliptic Curves over finite fields

Definition

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

Example

$E = \{37\}$

$a_p(E) = \{-2, -3, -2, -1, -5, 0, 2, -4, -1\}$
**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
$E = 37a$

<table>
<thead>
<tr>
<th>$p$</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_p$</td>
<td>-2</td>
<td>-3</td>
<td>-2</td>
<td>-1</td>
<td>-5</td>
<td>-2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>6</td>
<td>-4</td>
<td>-1</td>
</tr>
</tbody>
</table>

![Plot of $a_p(E)$ vs. $p$]
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

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

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 $L_E(s)$


$L_E(s)$ 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 $E = 37$
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

\[
\frac{\Omega_E \cdot \text{Reg}_E \cdot \#\Sha(E/\mathbb{Q}) \cdot \prod_p c_p}{\prod_p c_p (\#E_{\text{Tor}}(\mathbb{Q}))^2}
\]
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

$$\frac{\Omega_E \cdot \text{Reg}_E \cdot \#\Sha(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#\text{Tor}(E))^{2}}$$

where

- $\Omega_E$ is the real period of (an optimal model of) $E$,
- $\text{Reg}_E$ is the regulator of $E$,
- $\#\Sha(E/\mathbb{Q})$ 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
- $\#\text{Tor}(E)$ is the number of rational torsion points on $E$. 
Proposition

If \( E/Q \) has conductor \( N \) and analytic rank \( r \) then

\[ N > 15 e^{2r} \]

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

\[
\begin{align*}
N &\geq \text{Smallest Known Conductor} \\
0 &3 \\
1 &11 \\
2 &37 \\
3 &16389 \\
4 &555077 \\
5 &234446 \\
6 &19047851 \\
\end{align*}
\]
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:**

<table>
<thead>
<tr>
<th>$r$</th>
<th>$N \geq$</th>
<th>Smallest Known Conductor</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
<td>11</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>37</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
<td>389</td>
</tr>
<tr>
<td>3</td>
<td>55</td>
<td>5077</td>
</tr>
<tr>
<td>4</td>
<td>232</td>
<td>234446</td>
</tr>
<tr>
<td>5</td>
<td>1192</td>
<td>19047851</td>
</tr>
<tr>
<td>6</td>
<td>6696</td>
<td>5187563742</td>
</tr>
</tbody>
</table>
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

$$L_E(s + 1) = s^r (a + b \cdot s + c \cdot s^2 + O(s^3)),$$

where $a$ is the leading coefficient described by BSD. Then

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

where $\gamma$ 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.
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 $\gamma$ 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

Definition

Let $S_E(x, T) := \sum_{\gamma \text{ runs over imaginary parts of nontrivial zeros other than } s = 1} \psi_E(x) := \sum_{n \leq x} c_n(E) = -\left(\frac{p_e + 1 - \# \tilde{E} (F_p e)}{p} \log(p)\right) p^e$ for $n = p^e$ a perfect prime power, and 0 otherwise.
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 \( \gamma \) 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 \( \gamma \) runs over imaginary parts of nontrivial zeros other than \( s = 1 \)

\[ \psi(E)(x) := \sum_{n \leq x} c_n(E) \]

where \( c_n(E) = -\left( p^e + 1 - \#\hat{E}(\mathbb{F}_p^e) \right) \cdot \frac{\log(p)}{p^e} \) 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 $\eta$ 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**

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

\[S_E(x, 384) \quad 601 \text{ zeros}\]
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

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

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

\[
ap = \lim_{T \to \infty} \frac{-2\pi p}{\log p} \cdot \frac{1}{T} \sum_{0<\gamma<T} \frac{\cos(\gamma \log p)}{\gamma}
\]
Some Neat Corollaries

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

**Corollary (S.)**

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

\[p = 11, \quad a_p = -5\]

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.)**

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

\[\frac{p}{a_p} = 0\]

**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, \( \{ \text{nontrivial zeros of } L_E \} \sim \{ a_p(E) : p \text{ prime} \} \) 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 \( p \)
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 come from?

Take explicit formula:

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

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