# Fast Elliptic Curve Rank Computation in Sage

Simon Spicer

University of Washington

*mlungu@uw.edu*

October 6, 2014

# Problem Outline

Let $E/\mathbb{Q}$ be an elliptic curve.

# Problem Outline

Let $E/\mathbb{Q}$ be an elliptic curve. What is $\mathrm{rank}(E(\mathbb{Q}))$?

# Problem Outline

Let $E/\mathbb{Q}$ be an elliptic curve. What is $\text{rank}(E(\mathbb{Q}))$?

- Brute force point search.

# Problem Outline

Let $E/\mathbb{Q}$ be an elliptic curve. What is $\text{rank}(E(\mathbb{Q}))$?

- Brute force point search.
  - Only gives lower bounds to rank - when do you stop?

# Problem Outline

Let $E/\mathbb{Q}$ be an elliptic curve. What is $\text{rank}(E(\mathbb{Q}))$?

- Brute force point search.
  - Only gives lower bounds to rank - when do you stop?
  - Can be *very* inefficient:

# Problem Outline

Let $E/\mathbb{Q}$ be an elliptic curve. What is $\mathrm{rank}(E(\mathbb{Q}))$?

- Brute force point search.
  - Only gives lower bounds to rank - when do you stop?
  - Can be *very* inefficient:
  - $E : y^2 = x^3 - 157^2 x$ has "smallest" point

$$P = (x, y) = \left(-\frac{43565582610691407250551997}{609760250665615167250729}, \frac{56265361687773225244609387368307126580}{476144382506163554005382044222449067}\right)$$

# Problem Outline

Let $E/\mathbb{Q}$ be an elliptic curve. What is $\operatorname{rank}(E(\mathbb{Q}))$?

- Brute force point search.
  - Only gives lower bounds to rank - when do you stop?
  - Can be *very* inefficient:
  - $E : y^2 = x^3 - 157^2 x$ has "smallest" point

$$P = (x, y) = \left( -\frac{43565582610691407250551997}{609760250665615167250729}, \frac{562653616877773225244609387368307126580}{476144382506163554005382044222449067} \right)$$

- Other algebraic methods (e.g. $p$-descent)
  - Complicated to implement
  - Not guaranteed to succeed
  - Uneven
  - Can be very slow

# Problem Outline

Let $E/\mathbb{Q}$ be an elliptic curve. What is $\mathrm{rank}(E(\mathbb{Q}))$?

- Brute force point search.
  - Only gives lower bounds to rank - when do you stop?
  - Can be *very* inefficient:
  - $E : y^2 = x^3 - 157^2 x$ has "smallest" point

$$P = (x, y) = \left(-\frac{43565582610691407250551997}{609760250665615167250729}, \frac{56265361687777322524460938736830712658 0}{476144382506163554005382044222449067}\right)$$

- Other algebraic methods (e.g. $p$-descent)
  - Complicated to implement
  - Not guaranteed to succeed
  - Uneven
  - Can be very slow
- Analytic methods
  - Work with $L$-functions
  - Can be faster
  - Only give rank upper bounds

# Problem Outline

Underlying problem with these methods: how do they scale time-wise?

# Problem Outline

Underlying problem with these methods: how do they scale time-wise?

- What do they even scale with?

# 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)**

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

# Modularity & 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,

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

where $w = \pm 1$.

# Modularity & 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,

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

where $w = \pm 1$.

$\implies$ can compute $L_E(s)$ for any $s$.

# The BSD Conjecture

## Conjecture (Birch, Swinnerton-Dyer 1960s)

- $ord_{s=1} L_E(s) = rank(E(\mathbb{Q}))$ *"Analytic rank equals algebraic rank"*

# The BSD Conjecture

## Conjecture (Birch, Swinnerton-Dyer 1960s)

- *$ord_{s=1} L_E(s) = rank(E(\mathbb{Q}))$ "Analytic rank equals algebraic rank"*
- *There is a formula for the first nonzero Taylor coefficient for $L_E(s)$ at $s = 1$ in terms of invariants of $E$.*

# The BSD Conjecture

## Conjecture (Birch, Swinnerton-Dyer 1960s)

- $ord_{s=1} L_E(s) = rank(E(\mathbb{Q}))$ *"Analytic rank equals algebraic rank"*
- *There is a formula for the first nonzero Taylor coefficient for $L_E(s)$ at $s = 1$ in terms of invariants of $E$.*

Specifically, that coefficient is

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

where

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

# Analytic Methods to Compute Rank

Conjecturally: compute algebraic rank by computing analytic rank.

# Analytic Methods to Compute Rank

Conjecturally: compute algebraic rank by computing analytic rank.
Standard method: compute Taylor coefficients by evaluating $L_E(s)$.

# Analytic Methods to Compute Rank

Conjecturally: compute algebraic rank by computing analytic rank.
Standard method: compute Taylor coefficients by evaluating $L_E(s)$.
Upsides:

# Analytic Methods to Compute Rank

Conjecturally: compute algebraic rank by computing analytic rank.
Standard method: compute Taylor coefficients by evaluating $L_E(s)$.
Upsides:

- Straightforward implementation

# Analytic Methods to Compute Rank

Conjecturally: compute algebraic rank by computing analytic rank.
Standard method: compute Taylor coefficients by evaluating $L_E(s)$.
Upsides:

- Straightforward implementation
- $\tilde{O}(\sqrt{N})$ runtime

# Analytic Methods to Compute Rank

Conjecturally: compute algebraic rank by computing analytic rank.
Standard method: compute Taylor coefficients by evaluating $L_E(s)$.
Upsides:

- Straightforward implementation
- $\tilde{O}(\sqrt{N})$ runtime
- Often faster than algebraic methods*

# Analytic Methods to Compute Rank

Conjecturally: compute algebraic rank by computing analytic rank.
Standard method: compute Taylor coefficients by evaluating $L_E(s)$.
Upsides:

- Straightforward implementation
- $\tilde{O}(\sqrt{N})$ runtime
- Often faster than algebraic methods*

Downsides:

# Analytic Methods to Compute Rank

Conjecturally: compute algebraic rank by computing analytic rank.
Standard method: compute Taylor coefficients by evaluating $L_E(s)$.
Upsides:

- Straightforward implementation
- $\tilde{O}(\sqrt{N})$ runtime
- Often faster than algebraic methods*

Downsides:

- Conjectural for $r_{an} \geq 2$

# Analytic Methods to Compute Rank

Conjecturally: compute algebraic rank by computing analytic rank.
Standard method: compute Taylor coefficients by evaluating $L_E(s)$.
Upsides:

- Straightforward implementation
- $\tilde{O}(\sqrt{N})$ runtime
- Often faster than algebraic methods*

Downsides:

- Conjectural for $r_{an} \geq 2$
- Infeasible for large conductor

# Analytic Methods to Compute Rank

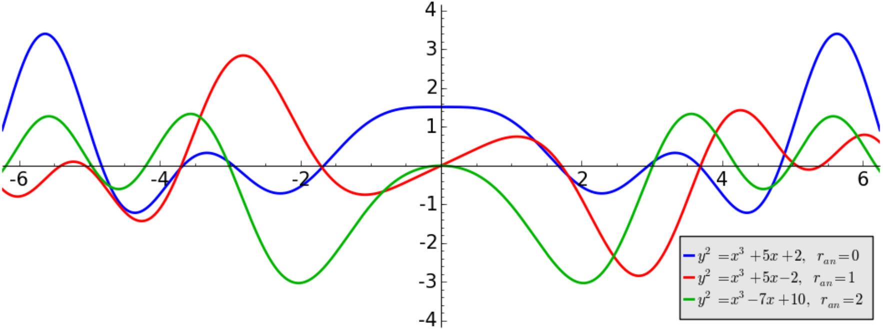
Conjecturally: compute algebraic rank by computing analytic rank.
Standard method: compute Taylor coefficients by evaluating $L_E(s)$.
Upsides:

- Straightforward implementation
- $\tilde{O}(\sqrt{N})$ runtime
- Often faster than algebraic methods*

Downsides:

- Conjectural for $r_{an} \geq 2$
- Infeasible for large conductor
- Finite precision $\implies$ can only ever compute upper bounds on rank

# The Central Zero



# Zero Sums

# Zero Sums

## Example

Let $\Delta$ be a positive constant and let $\mathrm{sinc}(x) = \frac{\sin(\pi x)}{\pi x}$, and consider the sum

$$\sum_{\gamma} \mathrm{sinc}^2(x)\Big|_{x=\Delta\gamma}$$

where $\gamma$ ranges over the imaginary parts of all the nontrivial zeros of the $L$-function of $E$.

# Zero Sums

## Example

Let $\Delta$ be a positive constant and let $\operatorname{sinc}(x) = \frac{\sin(\pi x)}{\pi x}$, and consider the sum

$$\sum_{\gamma} \operatorname{sinc}^2(x)\Big|_{x=\Delta\gamma}$$

where $\gamma$ ranges over the imaginary parts of all the nontrivial zeros of the $L$-function of $E$.

## Example

The curve $E : y^2 = x^3 - 18x + 51$ is a rank 1 curve, $N = 750384$.

# Zero Sums

## Example

Let $\Delta$ be a positive constant and let $\text{sinc}(x) = \frac{\sin(\pi x)}{\pi x}$, and consider the sum

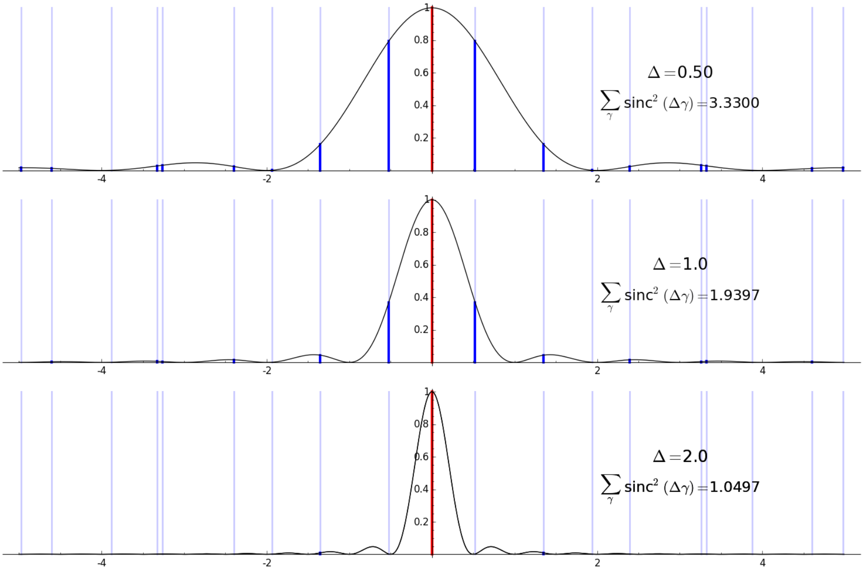
$$\sum_{\gamma} \text{sinc}^2(x)\Big|_{x=\Delta\gamma}$$

where $\gamma$ ranges over the imaginary parts of all the nontrivial zeros of the $L$-function of $E$.

## Example

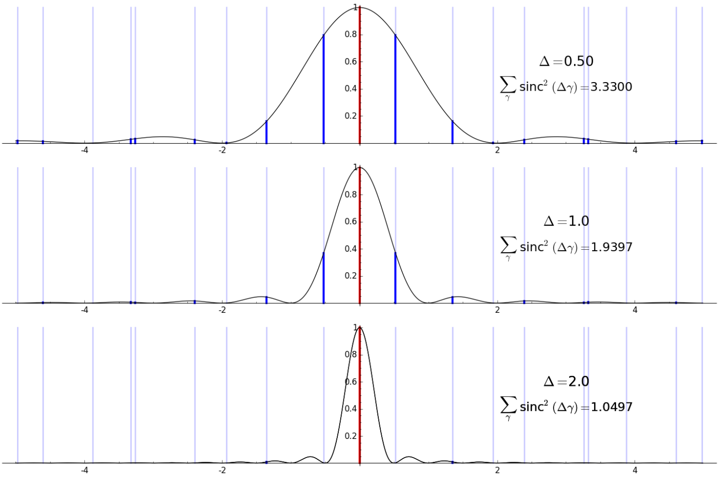
The curve $E : y^2 = x^3 - 18x + 51$ is a rank 1 curve, $N = 750384$.
Its first few zeros in the upper half plane have imaginary parts
$0, 0.522568720, 1.35341446, 1.93770878, 2.39321529, 3.25991966, 3.32420508, 3.87882138, 4.60372690, 4.97511170, \ldots$

# Zero Sums



$\Delta = 0.50$
$\sum_{\gamma} \text{sinc}^2(\Delta\gamma) = 3.3300$
$\Delta = 1.0$
$\sum_{\gamma} \text{sinc}^2(\Delta\gamma) = 1.9397$
$\Delta = 2.0$
$\sum_{\gamma} \text{sinc}^2(\Delta\gamma) = 1.0497$

# Zero Sums




Because $\mathrm{sinc}^2(0) = 1$ and $\mathrm{sinc}^2(\Delta\gamma) \to 0$ as $\Delta \to \infty$ for any nonzero $\gamma$, the zero sum limits to $r_{an}$ as $\Delta \to \infty$.

# Bounding Analytic Rank via Zero Sums/Explicit Formulae

Evaluate zero sum sum cleverly for large enough $\Delta \implies$ compute analytic rank.

# Bounding Analytic Rank via Zero Sums/Explicit Formulae

Evaluate zero sum sum cleverly for large enough $\Delta \implies$ compute analytic rank.

**Definition**

An *explicit formula* for an elliptic curve $L$-functions is one of a suite of formulae which relate sums over the nontrivial zeros of $L_E(s)$ to sums over the curve's $a_p$ values.

# Bounding Analytic Rank via Zero Sums/Explicit Formulae

Evaluate zero sum sum cleverly for large enough $\Delta \implies$ compute analytic rank.

**Definition**

An *explicit formula* for an elliptic curve $L$-functions is one of a suite of formulae which relate sums over the nontrivial zeros of $L_E(s)$ to sums over the curve's $a_p$ values.

Can compute zero sums *without* having to compute locations of the zeros themselves.

# Bounding Analytic Rank via Zero Sums/Explicit Formulae

Evaluate zero sum sum cleverly for large enough $\Delta \implies$ compute analytic rank.

**Definition**

An *explicit formula* for an elliptic curve $L$-functions is one of a suite of formulae which relate sums over the nontrivial zeros of $L_E(s)$ to sums over the curve's $a_p$ values.

Can compute zero sums *without* having to compute locations of the zeros themselves.

Good news: explicit formula exists for $\mathrm{sinc}^2$ zero sum!

# The Explicit Formula for Elliptic curves

## Definition

For $n \in \mathbb{N}$, let $c_n = c_n(E)$ be the $n$th Dirichlet coefficient of $\frac{L_E'}{L_E}(1+s)$, i.e.

$$c_n(E) := \begin{cases} -\left(\alpha_p^e + \beta_p^e\right) \cdot \frac{\log(p)}{p^e}, & n = p^e \;\; e \geq 1, \;\; p \nmid N \\ -a_p^e \cdot \frac{\log(p)}{p^e}, & n = p^e \;\; p \mid N \\ 0, & \text{otherwise} \end{cases}$$

# The Explicit Formula for Elliptic curves

## Definition

For $n \in \mathbb{N}$, let $c_n = c_n(E)$ be the $n$th Dirichlet coefficient of $\frac{L_E'}{L_E}(1+s)$, i.e.

$$c_n(E) := \begin{cases} -\left(\alpha_p^e + \beta_p^e\right) \cdot \frac{\log(p)}{p^e}, & n = p^e \;\; e \geq 1, \;\; p \nmid N \\ -a_p^e \cdot \frac{\log(p)}{p^e}, & n = p^e \;\; p \mid N \\ 0, & \text{otherwise} \end{cases}$$

## Theorem (Explicit Formula, Distributional Version)

*Let $\gamma$ range over the imaginary parts of the zeros of $L_E(s)$ with multiplicity. Let $\varphi_E = \sum_\gamma \delta(x-\gamma)$ be the complex-valued distribution on $\mathbb{R}$ corresponding to summation over $\gamma$. Then as a distribution,*

$$\varphi_E = \frac{1}{\pi}\left[\log\left(\frac{\sqrt{N}}{2\pi}\right) + \frac{\Gamma'}{\Gamma}(1+ix) + \sum_{n=1}^{\infty} c_n \cos(x \log n)\right].$$

# The Explicit Formula for Elliptic curves

## Theorem (Explicit Formula, Fourier Version)

*Suppose that* $f(x): \mathbb{R} \to \mathbb{C}$ *is even, piecewise continuous and integrable. Suppose that the Fourier transform* $\hat{f}(y) = \int_{-\infty}^{\infty} e^{-ixy} f(x)\, dx$ *exists and is such that* $\sum_{n=1}^{\infty} c_n \hat{f}(\log n)$ *converges absolutely. Then*

$$\sum_{\gamma} f(\gamma) = \frac{1}{\pi}\left[\log\left(\frac{\sqrt{N}}{2\pi}\right)\hat{f}(0) + \int_{-\infty}^{\infty} \left(\Re F(1+it)\right) f(t)\, dt + \sum_{n=1}^{\infty} c_n \hat{f}(\log n)\right],$$

*where* $\gamma$ *runs over the imaginary parts of the zeros of* $L_E(s)$*.*

# The Explicit Formula for the $\operatorname{sinc}^2$ Sum

$$\sum_{\gamma} \operatorname{sinc}^2(\Delta\gamma) = \frac{1}{\pi\Delta}\left[-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right) + \frac{1}{2\pi\Delta}\left(\frac{\pi^2}{6} - \operatorname{Li}_2\left(e^{-2\pi\Delta}\right)\right)\right.$$
$$\left. - \sum_{\substack{p^n < e^{2\pi\Delta} \\ p \text{ prime}}} \frac{(\alpha_p^n + \beta_p^n)\log(p)}{p^n}\left(1 - \frac{n\log p}{2\pi\Delta}\right)\right]$$

# The Explicit Formula for the $\mathrm{sinc}^2$ Sum

$$\sum_{\gamma} \mathrm{sinc}^2(\Delta\gamma) = \frac{1}{\pi\Delta}\left[-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right) + \frac{1}{2\pi\Delta}\left(\frac{\pi^2}{6} - \mathrm{Li}_2\left(e^{-2\pi\Delta}\right)\right)\right.$$
$$\left. - \sum_{\substack{p^n < e^{2\pi\Delta} \\ p \text{ prime}}} \frac{(\alpha_p^n + \beta_p^n)\log(p)}{p^n}\left(1 - \frac{n\log p}{2\pi\Delta}\right)\right]$$

where

- $\gamma$ ranges over the nontrivial zeros of the $L$-function attached to $E$ and $\Delta$ is a positive parameter
- $\eta$ is the Euler-Mascheroni constant $= 0.5772\ldots$ and $N$ is the conductor of $E$
- $\mathrm{Li}_2(x)$ is the dilogarithm function, defined by $\mathrm{Li}_2(x) = \sum_{k=1}^{\infty} \frac{x^k}{k^2}$
- $\alpha_p$ and $\beta_p$ are the two complex roots of $x^2 - a_p x + p = 0$ (if $p$ has good reduction)

# Bounding Analytic Rank via Zero Sums/Explicit Formulae

$$\sum_{\gamma} \operatorname{sinc}^2(\Delta\gamma) = \frac{1}{\pi\Delta}\left[-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right) + \frac{1}{2\pi\Delta}\left(\frac{\pi^2}{6} - \operatorname{Li}_2\left(e^{-2\pi\Delta}\right)\right) - \sum_{\substack{p^n < e^{2\pi\Delta} \\ p \text{ prime}}} \frac{(\alpha_p^n + \beta_p^n)\log(p)}{p^n}\left(1 - \frac{n\log p}{2\pi\Delta}\right)\right]$$

- Everything on RHS is effectively (and efficiently) computable
- Prime power sum is *finite*, so no truncation error.

# Bounding Analytic Rank via Zero Sums/Explicit Formulae

$$\sum_{\gamma} \operatorname{sinc}^2(\Delta\gamma) = \frac{1}{\pi\Delta}\left[-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right) + \frac{1}{2\pi\Delta}\left(\frac{\pi^2}{6} - \mathrm{Li}_2\left(e^{-2\pi\Delta}\right)\right) - \sum_{\substack{p^n < e^{2\pi\Delta} \\ p \text{ prime}}} \frac{(\alpha_p^n + \beta_p^n)\log(p)}{p^n}\left(1 - \frac{n\log p}{2\pi\Delta}\right)\right]$$

- Everything on RHS is effectively (and efficiently) computable
- Prime power sum is *finite*, so no truncation error.

Tactic:

# Bounding Analytic Rank via Zero Sums/Explicit Formulae

$$\sum_{\gamma} \operatorname{sinc}^2(\Delta\gamma) = \frac{1}{\pi\Delta}\left[-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right) + \frac{1}{2\pi\Delta}\left(\frac{\pi^2}{6} - \operatorname{Li}_2\left(e^{-2\pi\Delta}\right)\right) - \sum_{\substack{p^n < e^{2\pi\Delta} \\ p \text{ prime}}} \frac{(\alpha_p^n + \beta_p^n)\log(p)}{p^n}\left(1 - \frac{n\log p}{2\pi\Delta}\right)\right]$$

- Everything on RHS is effectively (and efficiently) computable
- Prime power sum is *finite*, so no truncation error.

Tactic:

- Pick a sufficiently large* value of $\Delta$

# Bounding Analytic Rank via Zero Sums/Explicit Formulae

$$\sum_{\gamma} \operatorname{sinc}^2(\Delta\gamma) = \frac{1}{\pi\Delta}\left[-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right) + \frac{1}{2\pi\Delta}\left(\frac{\pi^2}{6} - \mathrm{Li}_2\left(e^{-2\pi\Delta}\right)\right) - \sum_{\substack{p^n < e^{2\pi\Delta} \\ p \text{ prime}}} \frac{(\alpha_p^n + \beta_p^n)\log(p)}{p^n}\left(1 - \frac{n\log p}{2\pi\Delta}\right)\right]$$

- Everything on RHS is effectively (and efficiently) computable
- Prime power sum is *finite*, so no truncation error.

Tactic:

- Pick a sufficiently large* value of $\Delta$
- Compute everything on the RHS and add it all up

# Bounding Analytic Rank via Zero Sums/Explicit Formulae

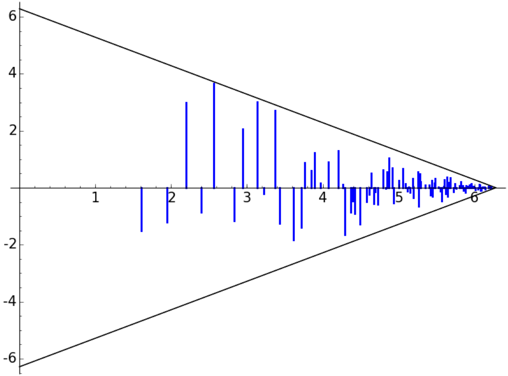
$$\sum_{\gamma} \operatorname{sinc}^2(\Delta\gamma) = \frac{1}{\pi\Delta}\left[-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right) + \frac{1}{2\pi\Delta}\left(\frac{\pi^2}{6} - \mathrm{Li}_2\left(e^{-2\pi\Delta}\right)\right) - \sum_{\substack{p^n < e^{2\pi\Delta} \\ p \text{ prime}}} \frac{(\alpha_p^n + \beta_p^n)\log(p)}{p^n}\left(1 - \frac{n\log p}{2\pi\Delta}\right)\right]$$

- Everything on RHS is effectively (and efficiently) computable
- Prime power sum is *finite*, so no truncation error.

Tactic:

- Pick a sufficiently large* value of $\Delta$
- Compute everything on the RHS and add it all up
- Resulting value is an upper bound for the analytic rank of $E$; hopefully close.

# The $c_n$ Sum for $E : y^2 = x^3 + 103x?51$, with $\Delta = 1$




- $\sum_{\log n < 2\pi\Delta} c_n \cdot (2\pi\Delta - \log n)$.
- The black lines are the triangular function $y = \pm(2\pi\Delta - x)$
- Blue line at $x = \log n$ has height $c_n \cdot (2\pi\Delta - \log n)$.
- Sum the signed lengths of the blue lines to get value of the sum over $n$
- Only 120 non-zero terms $\Longrightarrow$ quick to compute.

# How Big should $\Delta$ Be?

- The number of terms in the prime power sum is $O(e^{2\pi\Delta})$
  $\implies$ Time complexity of the method is exponential in $\Delta$

# How Big should $\Delta$ Be?

- The number of terms in the prime power sum is $O(e^{2\pi\Delta})$
  $\Longrightarrow$ Time complexity of the method is exponential in $\Delta$
  - $\Delta = 1 \Rightarrow$ O(milliseconds) runtime
  - $\Delta = 2 \Rightarrow$ O(seconds) runtime
  - $\Delta = 3 \Rightarrow$ O(hours) runtime

# How Big should $\Delta$ Be?

- The number of terms in the prime power sum is $O(e^{2\pi\Delta})$
  $\Longrightarrow$ Time complexity of the method is exponential in $\Delta$
  - $\Delta = 1 \Rightarrow$ O(milliseconds) runtime
  - $\Delta = 2 \Rightarrow$ O(seconds) runtime
  - $\Delta = 3 \Rightarrow$ O(hours) runtime
- Zero density is $O(\log N)$

# How Big should $\Delta$ Be?

- The number of terms in the prime power sum is $O(e^{2\pi\Delta})$
  $\implies$ Time complexity of the method is exponential in $\Delta$
  - $\Delta = 1 \Rightarrow$ O(milliseconds) runtime
  - $\Delta = 2 \Rightarrow$ O(seconds) runtime
  - $\Delta = 3 \Rightarrow$ O(hours) runtime
- Zero density is $O(\log N)$
- Choosing $\Delta(N) = \alpha \cdot \frac{1}{\pi}\left(-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right)$ for any constant $\alpha$
  $\implies$ bounds are tight a constant proportion of the time.

# How Big should $\Delta$ Be?

- The number of terms in the prime power sum is $O(e^{2\pi\Delta})$
  $\implies$ Time complexity of the method is exponential in $\Delta$
  - $\Delta = 1 \Rightarrow$ O(milliseconds) runtime
  - $\Delta = 2 \Rightarrow$ O(seconds) runtime
  - $\Delta = 3 \Rightarrow$ O(hours) runtime
- Zero density is $O(\log N)$
- Choosing $\Delta(N) = \alpha \cdot \frac{1}{\pi}\left(-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right)$ for any constant $\alpha$
  $\implies$ bounds are tight a constant proportion of the time.
- $\implies$ Time complexity is $O(N^{\alpha})$, but with small constants sitting in front.

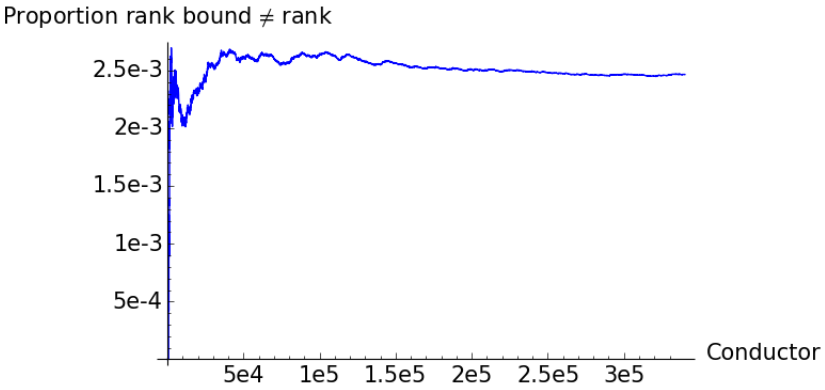
# How Big should $\Delta$ Be?

- The number of terms in the prime power sum is $O(e^{2\pi\Delta})$
  $\Longrightarrow$ Time complexity of the method is exponential in $\Delta$
  - $\Delta = 1 \Rightarrow$ O(milliseconds) runtime
  - $\Delta = 2 \Rightarrow$ O(seconds) runtime
  - $\Delta = 3 \Rightarrow$ O(hours) runtime
- Zero density is $O(\log N)$
- Choosing $\Delta(N) = \alpha \cdot \frac{1}{\pi}\left(-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right)$ for any constant $\alpha$
  $\Longrightarrow$ bounds are tight a constant proportion of the time.
- $\Longrightarrow$ Time complexity is $O(N^{\alpha})$, but with small constants sitting in front.
- For $\alpha = 1$, computed bound is actually the analytic rank 99.75% of the time.

# How Big should $\Delta$ Be?

- The number of terms in the prime power sum is $O(e^{2\pi\Delta})$
  $\Longrightarrow$ Time complexity of the method is exponential in $\Delta$
  - $\Delta = 1 \Rightarrow$ O(milliseconds) runtime
  - $\Delta = 2 \Rightarrow$ O(seconds) runtime
  - $\Delta = 3 \Rightarrow$ O(hours) runtime
- Zero density is $O(\log N)$
- Choosing $\Delta(N) = \alpha \cdot \frac{1}{\pi}\left(-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right)$ for any constant $\alpha$
  $\Longrightarrow$ bounds are tight a constant proportion of the time.
- $\Longrightarrow$ Time complexity is $O(N^{\alpha})$, but with small constants sitting in front.
- For $\alpha = 1$, computed bound is actually the analytic rank 99.75% of the time.
- $\alpha = 1 \Rightarrow \Delta(N \approx 10^9) \sim 2.5$, so practical for curves with conductor not too large.

# How Big should $\Delta$ Be?




- Proportion of all curves up to conductor $N$ for which rank bound $\neq$ true rank.
- For entire Cremona db, only 0.25% had rank bound $\neq$ rank.
- Sampling at higher conductors yields similar fidelity.

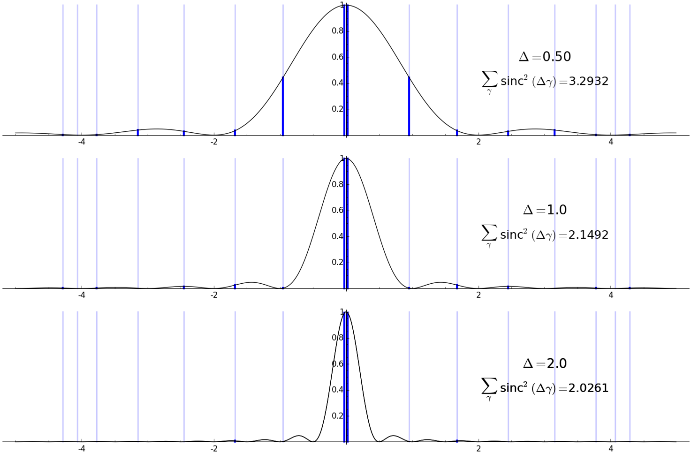
# When the Method Doesn't Work

# When the Method Doesn't Work

Method fails for curves with anomalously low-lying zeros.

# When the Method Doesn't Work

Method fails for curves with anomalously low-lying zeros.



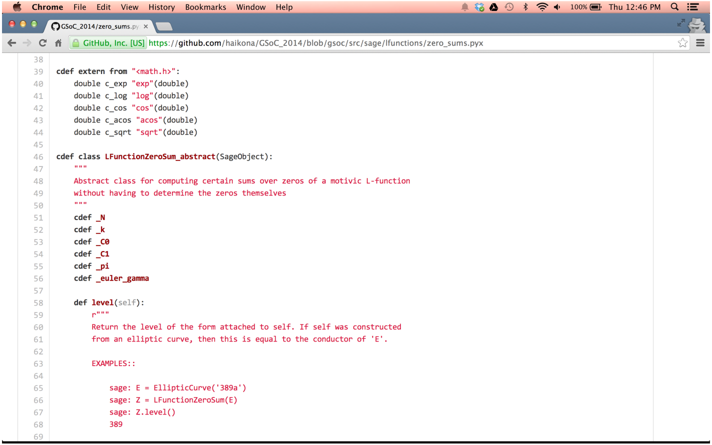
# Implementation

# Implementation

- The zero sum rank estimation method has been implemented for Sage in Python and Cython as part of my Google Summer of Code 2014 project.

# Implementation

- The zero sum rank estimation method has been implemented for Sage in Python and Cython as part of my Google Summer of Code 2014 project.
- Can be found at `https://github.com/haikona/GSoC_2014`:




```
cdef extern from "<math.h>":
    double c_exp "exp"(double)
    double c_log "log"(double)
    double c_cos "cos"(double)
    double c_acos "acos"(double)
    double c_sqrt "sqrt"(double)

cdef class LFunctionZeroSum_abstract(SageObject):
    """
    Abstract class for computing certain sums over zeros of a motivic L-function
    without having to determine the zeros themselves
    """
    cdef _N
    cdef _k
    cdef _C0
    cdef _C1
    cdef _pi
    cdef _euler_gamma

    def level(self):
        r"""
        Return the level of the form attached to self. If self was constructed
        from an elliptic curve, then this is equal to the conductor of 'E'.

        EXAMPLES::

            sage: E = EllipticCurve('389a')
            sage: Z = LFunctionZeroSum(E)
            sage: Z.level()
            389

```

# Implementation

- Usually much faster than traditional analytic rank methods.

# Implementation

- Usually much faster than traditional analytic rank methods.

```
┌──────────────────────────────────────────────────────────────────────
│ Sage Version 6.2, Release Date: 2014-05-06                          │
│ Type "notebook()" for the browser-based notebook interface.         │
│ Type "help()" for help.                                             │
└──────────────────────────────────────────────────────────────────────
sage: E = EllipticCurve([-2934,19238]); E
Elliptic Curve defined by y^2 = x^3 - 2934*x + 19238 over Rational Field
sage: %time E.analytic_rank(algorithm='rubinstein')
CPU times: user 2.79 ms, sys: 6.08 ms, total: 8.87 ms
Wall time: 1min 12s
1
sage: %time E.analytic_rank(algorithm='zero_sum')
CPU times: user 23.8 ms, sys: 2.45 ms, total: 26.3 ms
Wall time: 41.9 ms
1
```

# Implementation

- Usually much faster than traditional analytic rank methods.

```
┌──────────────────────────────────────────────────────────────────────
│ Sage Version 6.2, Release Date: 2014-05-06                          │
│ Type "notebook()" for the browser-based notebook interface.         │
│ Type "help()" for help.                                             │
└──────────────────────────────────────────────────────────────────────
sage: E = EllipticCurve([-2934,19238]); E
Elliptic Curve defined by y^2 = x^3 - 2934*x + 19238 over Rational Field
sage: %time E.analytic_rank(algorithm='rubinstein')
CPU times: user 2.79 ms, sys: 6.08 ms, total: 8.87 ms
Wall time: 1min 12s
1
sage: %time E.analytic_rank(algorithm='zero_sum')
CPU times: user 23.8 ms, sys: 2.45 ms, total: 26.3 ms
Wall time: 41.9 ms
1
```

- Actually works better on curves of larger rank.

# Current Work

# Current Work

- This method is sensitive to the lowest nontrivial non central zero
  - Curve with large lowest first zero $\Longrightarrow$ method computes rank quickly
  - Curve with small lowest first zero $\Longrightarrow$ method computes slowly/fails to provide tight bound

# Current Work

- This method is sensitive to the lowest nontrivial non central zero
  - Curve with large lowest first zero $\Longrightarrow$ method computes rank quickly
  - Curve with small lowest first zero $\Longrightarrow$ method computes slowly/fails to provide tight bound
- Lowest zero location is intimately related to size of leading coefficient (that predicted by BSD conjecture):

# Current Work

- This method is sensitive to the lowest nontrivial non central zero
  - Curve with large lowest first zero $\Longrightarrow$ method computes rank quickly
  - Curve with small lowest first zero $\Longrightarrow$ method computes slowly/fails to provide tight bound
- Lowest zero location is intimately related to size of leading coefficient (that predicted by BSD conjecture):
- Bound leading coefficient from below $\Longleftrightarrow$ bound lowest zero away from central point

# Current Work

- This method is sensitive to the lowest nontrivial non central zero
  - Curve with large lowest first zero $\Longrightarrow$ method computes rank quickly
  - Curve with small lowest first zero $\Longrightarrow$ method computes slowly/fails to provide tight bound
- Lowest zero location is intimately related to size of leading coefficient (that predicted by BSD conjecture):
- Bound leading coefficient from below $\Longleftrightarrow$ bound lowest zero away from central point
- My thesis work: assume full BSD, GRH and ABC;
  $\Longrightarrow$ Effective method to compute rank with known time complexity.

# Current Work

- This method is sensitive to the lowest nontrivial non central zero
  - Curve with large lowest first zero $\Longrightarrow$ method computes rank quickly
  - Curve with small lowest first zero $\Longrightarrow$ method computes slowly/fails to provide tight bound
- Lowest zero location is intimately related to size of leading coefficient (that predicted by BSD conjecture):
- Bound leading coefficient from below $\Longleftrightarrow$ bound lowest zero away from central point
- My thesis work: assume full BSD, GRH and ABC;
  $\Longrightarrow$ Effective method to compute rank with known time complexity.

# Two Big Questions

$$\frac{L_E^{(r)}(1)}{r!} = \frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{\mathrm{Tor}}(\mathbb{Q}))^2}$$

# Two Big Questions

$$\frac{L_E^{(r)}(1)}{r!} = \frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\# E_{\mathrm{Tor}}(\mathbb{Q}))^2}$$

- How small can $\mathrm{Reg}_E$ be in terms of $N$?

# Two Big Questions

$$\frac{L_E^{(r)}(1)}{r!} = \frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\# E_{\mathrm{Tor}}(\mathbb{Q}))^2}$$

- How small can $\mathrm{Reg}_E$ be in terms of $N$?
- How small can $\Omega_E$ be in terms of $N$?:

# Two Big Questions

$$\frac{L_E^{(r)}(1)}{r!} = \frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#Ш(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{\mathrm{Tor}}(\mathbb{Q}))^2}$$

- How small can $\mathrm{Reg}_E$ be in terms of $N$?
- How small can $\Omega_E$ be in terms of $N$?:

Long and short: rank should be in $\tilde{O}(N^\beta)$ time for some $\beta >> 1$.

# Two Big Questions

$$\frac{L_E^{(r)}(1)}{r!} = \frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{\mathrm{Tor}}(\mathbb{Q}))^2}$$

- How small can $\mathrm{Reg}_E$ be in terms of $N$?
- How small can $\Omega_E$ be in terms of $N$?:

Long and short: rank should be in $\tilde{O}(N^\beta)$ time for some $\beta >> 1$.
Most likely not practical, but first such result.

Thank You