UNDERGRADUATE
RESEARCH
SCHOLAR

Computing Central Values for Elliptic Curve L-Functions

Meghan Shanks
Advised by Dr. Matthew Young

March 29, 2016

Introduction

Elliptic Curves

- Elliptic Curves are interesting objects in mathematics
  - Useful in cryptography
  - Related to two of the Clay Mathematics Millennium Prize Problems
- Elliptic curves are generally written in the form $E : y^2 = x^3 + ax^2 + b$
- We are particularly interested in the rational solutions of elliptic curves
  - It has been proven that these solutions form a group $E(\mathbb{Q})$
  - We know that $E(\mathbb{Q}) = E_{\text{tors}} \times \mathbb{Z}^r$ where E_{tors} is a finite group
  - The number of copies of $\mathbb{Z}$ contained in $E(\mathbb{Q})$, r, is called the rank of the elliptic curve

L-fucntions

- There are L-functions associated with elliptic curves
- We are primarily interested in the central values of these L-functions
- For a given elliptic curve E, the central value of the L-function is defined as

$$L(1/2, E) = (1 + \omega_E) \sum_{n=1}^{\infty} \frac{\lambda_E(n)}{\sqrt{n}} \exp\left(\frac{-2\pi n}{\sqrt{N_E}}\right)$$

- L-functions are useful for understanding other properties of elliptic curves
    - For example, Birch and Swinnerton-Dyer conjecture that the rank of an elliptic curve is equal to its analytic rank (the smallest value of r such that $L^{(r)}(1/2, E) \neq 0$
- Calculating central values allows us to determine whether an elliptic curve has rank 0
- Unfortunately, since $L(1/2, E)$ is defined with an infinite series, it is difficult to calculate efficiently

Methodology

- My research involves developing a more efficient method for calculating the central values of elliptic curves
  - Improves upon the methods presented in [HY15]
- Based upon the Birch and Swinnerton-Dyer conjecture which states that for an elliptic curve of rank 0,

$$L(1/2, E) = \frac{|Ш_E|\Omega_E c_E}{|E_{\text{tors}}|^2} \tag{1}$$

- Algorithm follows the following steps:
  1. Approximate the value of $L(1/2, E)$ by summing the first $\delta\sqrt{N_E}$ terms for some δ
  2. Use the Birch and Swinnerton-Dyer conjecture to calculate $|Ш_{E,\text{approx}}| = |\frac{L_{\text{approx}}(1/2,E)|E_{\text{tors}}|^2}{\Omega_E c_E}|$
  3. Since $|Ш_E|$ must be an integer, use the approximation $|Ш_{E,\text{approx}}|$ to recover the exact value of $|Ш_E|$
  4. Use new value of $|Ш_E|$ to calculate $L(1/2, E) = \frac{|Ш_E|\Omega_E c_E}{|E_{\text{tors}}|^2}$

Theoretical Support

Main Heuristic

Heuristic 2.1.

Let $\delta \geq \frac{1}{24\pi} \log N_E - C_2 \log\log N_E$ *for some constant* C_2 *such that* $4\pi C_2 < 1$*. On average, as the conductor approaches infinity, we expect* $||Ш_{approx,E}| - |Ш_E|| < 1/2$*.*

Reasoning:

- We would like to show $|Ш_{E,\text{tail}}| = ||Ш_{\text{approx},E}| - |Ш_E|| < \frac{1}{2}$
- Birch and Swinnerton-Dyer conjecture: $|Ш_E| = \frac{L(1/2,E)|E_{\text{tors}}|^2}{\Omega_E c_E}$
- By our definition: $|Ш_{\text{approx},E}| = \frac{L_{\text{approx}}(1/2,E)|E_{\text{tors}}|^2}{\Omega_E c_E}$
- Therefore we can write $|Ш_{E,\text{tail}}| = |\frac{L_{\text{tail}}(1/2,E)|E_{\text{tors}}|^2}{\Omega_E c_E}|$
- Need to understand L_{tail} before we continue

Understanding L_{tail}

- Recall that $L_{\text{tail}}(1/2, E) = 2 \sum_{n > \delta\sqrt{N_E}} \frac{\lambda_E(n)}{\sqrt{n}} e^{\frac{-2\pi n}{\sqrt{N_E}}}$
- L_{tail} is difficult to bound for a generic elliptic curve
  - This is partially due to erratic behavior $\lambda_E(n)$
- Because of this, we will instead consider the average behavior of $L_{\text{tail}}(1/2, E)$ over a family of elliptic curves
- In other words, we will examine $\frac{1}{4|A||B|} \sum_{\substack{|a| \le A \\ |b| \le B}} (L_{\text{tail}, E_{a,b}})^2$

Understanding L_{tail}

- In order to understand $\frac{1}{4|A||B|} \sum_{\substack{|a| \leq A \\ |b| \leq B}} (L_{\text{tail},E_{a,b}})^2$, we need to understand what will happen when we sum $\lambda_{E_{a,b}}(m)\lambda_{E_{a,b}}(n)$ over our family
- Using techniques from [You07] and simplifying assumptions and that are primarily modeled after those in [CFK$^+$02], we can show:

Heuristic 2.2.

Let $A, B, m, n \in \mathbb{Z}$ such that $A, B, m, n > 0$. Then

$$\frac{1}{4|A||B|} \sum_{\substack{|a| \leq A \\ |b| \leq B}} \lambda_{E_{a,b}}(m)\lambda_{E_{a,b}}(n)$$

is approximately 1 when $m = n$ and 0 otherwise.

Understanding L_{tail}

- Since $L_{\text{tail}}(1/2, E) = 2 \sum_{n > \delta\sqrt{N_E}} \frac{\lambda_E(n)}{\sqrt{n}} e^{\frac{-2\pi n}{\sqrt{N_E}}}$, we can write

$$\frac{1}{4|A||B|} \sum_{\substack{|a| \leq A \\ |b| \leq B}} (L_{tail,E_{a,b}})^2 \approx 4 \sum_{n_1 \geq \delta\sqrt{X_{A,B}}} \sum_{n_2 \geq \delta\sqrt{X_{A,B}}} \frac{e^{-2\pi(n_1+n_2)/\sqrt{X_{A,B}}}}{\sqrt{n_1 n_2}} \frac{1}{4|A||B|} \sum_{\substack{|a| \leq A \\ |b| \leq B}} \lambda_{E_{a,b}}(n_1)\lambda_{E_{a,b}}(n_2)$$

  where $X_{A,B}$ is the average of N_E over the family
- Notice the inner sum can be rewritten using Heuristic 2.2

$$\frac{1}{4|A||B|} \sum_{\substack{|a| \leq A \\ |b| \leq B}} (L_{tail,E_{a,b}})^2 \approx 4 \sum_{n \geq \delta\sqrt{X_{A,B}}} \frac{e^{\frac{-4\pi n}{\sqrt{X_{A,B}}}}}{n}$$

- Since $n \geq \delta\sqrt{X_{A,B}}$,

$$4 \sum_{n \geq \delta\sqrt{X_{A,B}}} \frac{e^{\frac{-4\pi n}{\sqrt{X_{A,B}}}}}{n} \leq \frac{4}{\delta\sqrt{X_{A,B}}} \sum_{n \geq \delta\sqrt{X_{A,B}}} e^{\frac{-4\pi n}{\sqrt{X_{A,B}}}}$$

Understanding L_{tail}

- Approximating via integration gives us

$$\frac{4}{\delta\sqrt{X_{A,B}}}\sum_{n\geq\delta\sqrt{X_{A,B}}} e^{\frac{-4\pi n}{\sqrt{X_{A,B}}}} \leq \frac{4e^{-4\pi\delta}}{\delta\sqrt{X_{A,B}}} + 4\int_{\delta\sqrt{X_{A,B}}}^{\infty} e^{\frac{-4\pi t}{\sqrt{X_{A,B}}}}\,dt$$

$$= \frac{4e^{-4\pi\delta}}{\delta\sqrt{X_{A,B}}} + \frac{e^{-4\pi\delta}}{\pi\delta}$$

- For large $X_{A,B}$, the first term is small. Thus we get a second heuristic:

Heuristic 2.3.

$$\lim_{A,B\to\infty}\frac{1}{4|A||B|}\sum_{\substack{|a|\leq A\\|b|\leq B}}(L_{tail,E_{a,b}})^2 \leq \frac{e^{-4\pi\delta}}{\pi\delta}$$

Main Heuristic

Now that we understand L_{tail}, we can return to our main heuristic:

Heurisitic 2.1.

Let $\delta \geq \frac{1}{24\pi} \log N_E - C_2 \log\log N_E$ *for some constant* C_2 *such that* $4\pi C_2 < 1$. *On average, as the conductor approaches infinity, we expect* $||Ш_{approx,E}| - |Ш_E|| < 1/2$.

Reasoning:

- We already determined $|Ш_{E,\text{tail}}| = |\frac{L_{\text{tail}}(1/2, E)|E_{\text{tors}}|^2}{\Omega_E c_E}|$
  - $|E_{\text{tors}}|$ is bounded by a constant
  - $\Omega_E \asymp N_E^{-1/12}$ by [Wat08]
  - $L_{\text{tail}} \leq \sqrt{\frac{e^{-4\pi\delta}}{\pi\delta}}$ by 2.3
- Therefore we estimate that, for large conductor,

$$|Ш_{E,\text{tail}}| \leq \frac{\sqrt{\frac{e^{-4\pi\delta}}{\pi\delta}}|E_{\text{tors}}|^2}{N_E^{-1/12} c_E}$$

Main Heuristic

- Therefore we want to understand how δ must grow so that $\frac{\sqrt{\frac{e^{-4\pi\delta}}{\pi\delta}}|E_{\text{tors}}|^2}{N_E^{-1/12} c_E} < \frac{1}{2}$ for large conductors
- We rewrite this as $\frac{{N_E}^{1/6} e^{-4\pi\delta}}{4\pi\delta} < \frac{1}{16|E_{\text{tors}}|^4}$ (since $c_E \geq 1$)
- When $\delta \geq \frac{1}{24\pi} \log N_E - C_2 \log\log N_E$ for some constant C_2:

$$\begin{aligned} e^{-4\pi\delta} &\leq e^{-4\pi(\frac{1}{24\pi} \log N_E - C_2 \log\log N_E)} \\ &= N_E^{-1/6} (\log N_E)^{4\pi C_2} \end{aligned}$$

- Therefore for large N_E:

$$\frac{{N_E}^{1/6} e^{-4\pi\delta}}{4\pi\delta} < \frac{(\log N_E)^{4\pi C_2}}{\frac{1}{6} \log N_E - 4\pi C_2 \log\log N_E)}$$

- When $4\pi C_2 < 1$ then for large N_E this will approach 0, and thus be smaller than $\frac{1}{2}$ for large enough conductor.

Empirical Support

Empirical Support

- We can also provide empirical support that our method generally works
- In order to test our method, we implemented the algorithm in PARI/GP
- We tested the method on elliptic curves with maximum conductors on the order of 10^{10} and 10^{11}
  - In particular, we tested on all elliptic curves $E : y^2 = x^3 + ax^2 + b$ where $630 \leq |a| \leq 900$ and $10000 \leq |b| \leq 14000$ and E is a global minimal model
- Theoretic results tell us that we should pick

$$\begin{aligned}\delta &\geq \frac{1}{24\pi} \log N_E - C_2 \log \log N_E \\ &= \frac{1}{24\pi} \log 10^{11} - \frac{1}{8\pi} \log \log 10^{11} \\ &\approx 0.2\end{aligned}$$

  (where we chose $N = 10^{11}$ and $C_2 = \frac{1}{8\pi}$) to handle the average case
- We use $\delta = 0.5$ in order to hopefully account for both the average case and outliers

Empirical Support - Average Case Results - $|\text{Ш}_{\text{tail}}|$

- By Heuristic 2.1, since we took a large enough δ, we expect $|\text{Ш}_{\text{tail}}|$ to be well under $\frac{1}{2}$

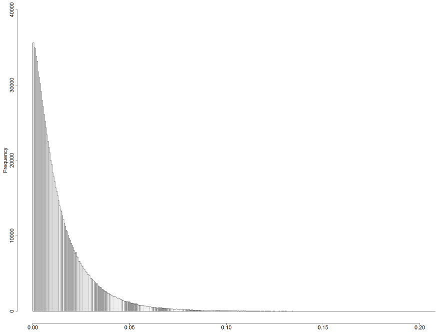

Figure 1: Distribution of $|\text{Ш}_{\text{tail}}|$ Values for Given Elliptic Curves

Empirical Support - Worst Case Results

- Since our theoretical results only discussed the average case, we also want to consider what happens in the worst case

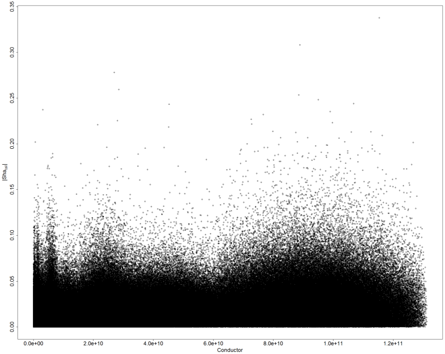

Figure 2: Conductor vs $|\text{Ш}_{\text{tail}}|$ for Given Elliptic Curves

Empirical Support - Analysis of Outliers

- We are interested in understanding what causes $|Ш_{\mathrm{tail}}|$ to be large so that we can correct for it when we expect $|Ш_{\mathrm{tail}}|$ to be much larger than the average case analysis indicates
- Since $|Ш_{E,\mathrm{tail}}| = |\frac{L_{\mathrm{tail}}(1/2,E)|E_{\mathrm{tors}}|^2}{\Omega_E c_E}|$, we expect that $|Ш_{E,\mathrm{tail}}|$ is large when either $|L_{\mathrm{tail}}|$ or $|E_{\mathrm{tors}}|$ is large, or when Ω_E or c_E is small
- Based on data, it appears that $|L_{\mathrm{tail}}|$ is the most significant factor

Empirical Support - Analysis of Outliers

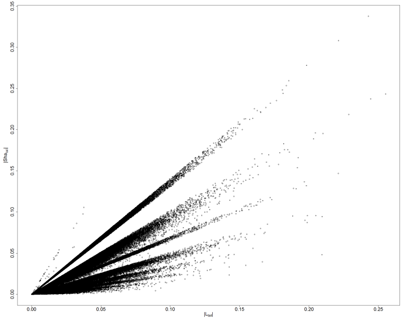

Figure 3: L_{tail} vs $|Ш_{\text{tail}}|$ for Given Elliptic Curves

- $|Ш_{E,\text{tail}}|$ increases as $|L_{\text{tail}}|$ increases
- Since Ω_E remains relatively constant over the family of Elliptic curves and both c_E and $|E_{\text{tors}}|$ take on discrete values, each band represents a different value of $\frac{|E_{\text{tors}}|}{c_E}$

Empirical Support - Analysis of Outliers

- Leads to question of whether we can predict when an elliptic curve will have large value of $|L_{\text{tail}}|$

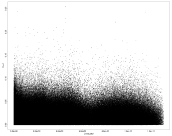

Figure 4: Conductor vs $|L_{\text{tail}}|$

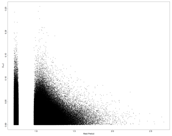

Figure 5: Real Period vs $|L_{\text{tail}}|$

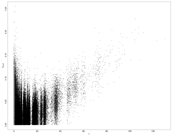

Figure 6: L vs $|L_{\text{tail}}|$

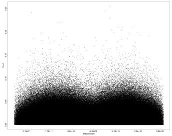

Figure 7: Discriminant vs $|L_{\text{tail}}|$

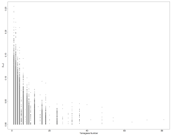

Figure 8: Tamagawa Number vs $|L_{\text{tail}}|$

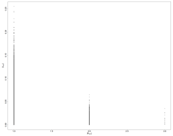

Figure 9: Torsion Group Size vs $|L_{\text{tail}}|$

Empirical Support - Analysis of Outliers

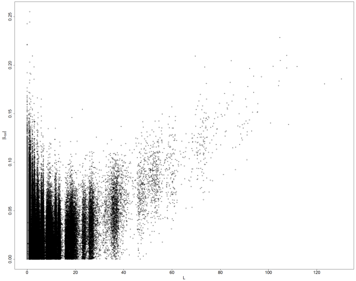

Figure 10: L vs $|L_{\text{tail}}|$ for Given Elliptic Curves

- High values of L seem to correlate with large $|L_{\text{tail}}|$
  - To account for this, we can adjust our method to use larger δ if our initial approximation of L is unusually large
- Unfortunately, there are also a few outliers when L is close to 0.
- Since most elliptic curves have L close to 0, this is an unhelpful characterization

Conclusion

- Our method of calculating central values appears to work both theoretically and empirically
- Using $\delta = 0.5$ seems to work well for elliptic curves with conductors on the order of 10^{10} and 10^{11}
  - This halves the amount of time it would take to compute using the method presented in [HY15].
- In addition, we have calculated central values for elliptic curves of large conductor that were previously uncalculated
  - This data can be used to explore other facets elliptic curves
- Future work could focus on understanding when an elliptic curve can be expected to have a large $|L_{\text{tail}}|$
- It would also be useful to extend this to larger derivatives of the L-function so that we can distinguish between elliptic curves of larger rank

References

[CFK+02] J. B. Conrey, D. W. Farmer, J. P. Keating, M. O. Rubinstein, and N. C. Snaith.
Integral moments of L-functions.
arXiv preprint math/0206018, 2002.

[HY15] Dustin Hinkel and Matthew P. Young.
The distribution of central values of elliptic curve L-functions.
Journal of Number Theory, 156:15–20, November 2015.

[Wat08] Mark Watkins.
Some heuristics about elliptic curves.
Experimental Mathematics, 17(1):105–125, 2008.

[You07] Matthew P. Young.
Moments of the critical values of families of elliptic curves, with applications.
arXiv preprint arXiv:0708.4042, 2007.