COMPUTING CENTRAL VALUES FOR ELLIPTIC CURVE L-FUNCTIONS

An Undergraduate Research Scholars Thesis

by

MEGHAN SHANKS

Submitted to the Undergraduate Research Scholars program
Texas A&M University
in partial fulfillment of the requirements for the designation as an

UNDERGRADUATE RESEARCH SCHOLAR

Approved by Research Advisor: Dr. Matthew Young

May 2017

Major: Mathematics

ABSTRACT

Computing Central Values for Elliptic Curve L-Functions

Meghan Shanks
Department of Mathematics
Texas A&M University

Research Advisor: Dr. Matthew Young
Department of Mathematics
Texas A&M University

We give an experimental method for calculating the central values of elliptic curve L-functions. We begin by providing some theoretical analysis of the method, and show that, on average, with appropriate choice of parameters, it can be expected to work well. In addition, we provide some data on elliptic curve L-functions of large conductor that support this method.

TABLE OF CONTENTS

Page

LIST OF FIGURES

FIGURE Page

LIST OF TABLES

TABLE Page

1. INTRODUCTION

Elliptic curves are the object of some of the most challenging current problems in number theory. These problems range from applications in cryptography to the famous Birch and Swinnerton-Dyer conjecture. An elliptic curve can be defined as the set of solutions to the equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Over most fields, elliptic curves can be written in the form $y^2 = x^3 + ax + b$, known as Weierstrass Normal Form. For the purposes of this paper, we will consider this to be our definition of an elliptic curve.

Mathematicians are particularly interested in understanding the rational solutions to elliptic curves. The rational solutions to an elliptic curve, $E(\mathbb{Q})$, form a group. The identity of this group is an extra point known as the point at inifinity. Addition of two points, $P + Q$, is defined by drawing a line through P and Q. This line will generally intersect with a third point, R. Then we say that $P + Q = -R$, where $-R$ is the point R reflected over the x-axis. When $P = -Q$, the points lie on a vertical line and do not intersect a third point on the curve. In this case, we define $P+Q$ to be the point at infinity. Therefore reflection of a point over the x-axis does indeed produce its additive inverse.

In [Mor22], Mordell showed that $E(\mathbb{Q})$ is a finitely generated and therefore can be written

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E_{\text{tors}}. \tag{1.1}$$

The value of r, known as the *rank* of the elliptic curve, is indicative of the size of the group of rational solutions.

Since then, much work has been done towards determining the rank of elliptic curves. Much of this work is summarized in [RS02]. However, it is still not known, in general, how to find the rank of an elliptic curve. In fact it is not even known if the rank is uniformly bounded for all elliptic curves over $\mathbb{Q}$.

Elliptic curve L-functions can be used to study the rank of elliptic curves. An Elliptic curve L-fucntion, $L(s, E)$, is defined

$$L(s, E) = \prod_{p \nmid N_E} \left(1 - \frac{a_p}{p^{s+\frac{1}{2}}} + \frac{1}{p^{2s}}\right)^{-1} \prod_{p \mid N_E} \left(1 - \frac{a_p}{p^{s+\frac{1}{2}}}\right)^{-1}, \tag{1.2}$$

where N_E is the conductor of the elliptic curve and $a_p = p + 1 - |E(\mathbb{F}_p)|$ when $p \neq 2, 3$. When p is 2 or 3, a_p is defined slightly differently. Note that the definition for $L(s, E)$ above only converges when $Re(s) > 1$. In [Wil95] and [TW95], Wiles and Taylor showed that there is an analytic continuation of L to the complex plane along with a functional equation relating s to $1 - s$. It is conjectured by Birch and Swinnerton-Dyer that the rank of an elliptic curve is equal to its analytic rank, i.e. the order of vanishing of its L-function at the central point, $s = \frac{1}{2}$. Because of this conjecture, calculating the central value L-function and it's derivatives is of interest.

Using the functional equation, the central value of the L-function can be calculated using the infinite sum

$$L(1/2, E) = (1 + \omega_E) \sum_{n=1}^{\infty} \frac{\lambda_E(n)}{\sqrt{n}} \exp\left(\frac{-2\pi n}{\sqrt{N_E}}\right) \tag{1.3}$$

where ω_E is the root number of the elliptic curve, N_E is its conductor, and each $\lambda_E(n) = \frac{a_n}{\sqrt{n}}$. The root number, ω_E, has the value -1 when the analytic rank of the elliptic curve is odd and 1 when the analytic rank of the elliptic curve is even. We can easily see that when $\omega_E = -1$, $L(1/2, E) = 0$. Thus, for the interests of our investigation, we are only interested in elliptic curves where $\omega_E = 1$. The L-function of the elliptic curve, in this case, can be written as:

$$L(1/2, E) = 2 \sum_{n=1}^{\infty} \frac{\lambda_E(n)}{\sqrt{n}} \exp\left(\frac{-2\pi n}{\sqrt{N_E}}\right). \tag{1.4}$$

The other notable paramater in the central value computation is the function $\lambda_E(n)$. As previously mentioned, $\lambda_E(n) = \frac{a_n}{\sqrt{n}}$. In particular, when p is prime, $\lambda_E(p) = \frac{p+1-|E(\mathbb{F}_p)|}{\sqrt{p}}$. We define $\lambda(n)$ for non-prime value of n by equating the original defintion of the L-function at $s = 1/2$ with the series definition given above. We can determine that $\lambda(n)$ is multiplicative, and that $\lambda(p^j)$ is defined by a Cheybyshev polynomial. Because of this, $\lambda_E(p^k)$ must be periodic modulo p.

The obvious way to attempt to compute this value is to merely sum as many terms of the series as is necessary to achieve the desired precision, usually $O(\sqrt{N_E} \log N_E)$ terms. Hinkel and Young suggest in [HY15] that, assuming the Birch and Swinnerton-Dyer conjecture, we can an obtain a precise result by summing significantly fewer terms. For reference, the Birch and Swinnerton-Dyer conjecture states that, for a curve of rank r,

$$\frac{L^{(r)}(1/2, E)}{r!} = \frac{|\text{Ш}_E| \Omega_E R_E c_E}{|E_{\text{tors}}|^2} \tag{1.5}$$

where Ш_E, Ω_E, R_E, and c_E are respectively the Tate-Shafarevich group, the real period, the regulator, and the global Tamagawa number of the elliptic curve. All of the quantities on the right hand side of this equation can be efficiently calculated, except for $|\text{Ш}_E|$ and R_E. However, for curves of rank zero, $R_E = 1$. In addition, since $|\text{Ш}_E|$ is the order of a group, it must be an integer if it is finite. It is known that $|\text{Ш}_E|$ is finite for elliptic curves of analytic rank zero and one, and it is conjectured to be finite in general. Therefore, for curves of analytic rank zero, we only need to calculate $L(1/2, E)$ with enough precision to estimate $|\text{Ш}_E|$ to within 0.5 of its actual value. Then, by rounding to the nearest integer, we can determine the actual value of $|\text{Ш}_E|$ and use it to obtain $L(1/2, E)$.

Hinkel and Young suggest in [HY15] that, based on data, $\sqrt{N}$ terms is a sufficient initial approximation of $L(1/2, E)$ for $N_E \leq 10^{10}$. My work demonstrates that $\frac{1}{2}\sqrt{N}$ terms is enough, reducing total time needed to compute $L(1/2, E)$. In section 2, I provide theoretical support that this will work on average for small enough N using the framework provided in [You10], and discuss how this needs to grow for larger N. In section 3, I give empirical support for this claim and provide some analysis of the outliers for which this method does not work as well.

2. THEORETICAL SUPPORT

In this section, we seek to provide theoretical support that our approximation method will work for reasonably sized conductors. Ideally, we would like to show that for a given elliptic curve E, $L_{\text{approx}}(1/2, E) = 2\sum_{n\leq\delta\sqrt{N_E}} \frac{\lambda_E(n)}{\sqrt{n}} e^{\frac{-2\pi n}{\sqrt{N_E}}}$ allows us to make a good enough approximation of the actual value of $L(1/2, E)$ to determine the exact value of Ш assuming the Birch and Swinnerton-Dyer conjecture. We determine this by using the Birch and Swinnerton-Dyer conjecture to set $|Ш_E| = \frac{L(1/2,E)|E_{\text{tors}}|^2}{\Omega_E c_E}$. We let $|Ш_{\text{approx},E}| = \frac{L(1/2,E)_{\text{approx}}|E_{\text{tors}}|^2}{\Omega_E c_E}$. If $||Ш_{\text{approx},E}| - |Ш_E|| < 1/2$, then, since $|Ш_E|$ must be an integer, we know that by rounding to the nearest integer we will obtain the exact value of $|Ш_E|$.

Unfortunately, $L_{\text{approx}}(1/2, E)$ is difficult to work with for a general elliptic curve. The conductor as well as λ_E behave somewhat erratically, and so bounding the difference between $L_{\text{approx}}(1/2, E)$ and $L(1/2, E)$ becomes problematic. Because of these problems, we will consider the average of this difference over a family of elliptic curves, and show that, for a large enough δ, we can expect our method to work on average. This is not sufficient to show that our method will always work, since the worst case may be much different than the average case, and may cause our method to fail. However, we expect that most elliptic curves will behave more like the average case than the worst case, and so our approximation should be sufficient for many elliptic curves.

In addition, some of the complications above necessitate simplifying assumptions. Many of our assumptions are similar to those made in [CFK$^+$05]. The assumptions generally involve ignoring error terms that are not entirely insignificant. While these assumptions cannot be rigorously justified, data seems to indicate that these assumptions work when taken together. That this works in our case is justified by our data in Section 3.

Our main result in this section is the following:

Heuristic 2.1. *Let $L_{approx}(1/2, E)$ and $|Ш_{approx,E}|$ be defined as above. 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 $||Ш_{approx,E}| - |Ш_E|| < 1/2$.*

In order to support Heuristic 2.1, we first estimate $\frac{1}{4|A||B|} \sum_{\substack{|a| \leq A \\ |b| \leq B}} \lambda_{E_{a,b}}(m)\lambda_{E_{a,b}}(n)$:

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.

Our support for this heuristic is as follows:

Assume $m = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \ldots {p_k}^{\alpha_k}$ and $n = {p_1}^{\beta_1}{p_2}^{\beta_2} \ldots {p_k}^{\beta_k}$. Then $\lambda_{E_{a,b}}(m) = \prod_i \lambda_{E_{a,b}}({p_i}^{\alpha_i})$, and similarly for $\lambda_{E_{a,b}}(n)$. Since $\lambda(p^k)$ is periodic over p, $\lambda_{E_{a,b}}(m)\lambda_{E_{a,b}}(n)$ is necessarily periodic over mn. Therefore, if $4AB$ is a multiple of mn, we can write:

$$\frac{1}{4|A||B|} \sum_{\substack{|a| \leq A \\ |b| \leq B}} \lambda_{E_{a,b}}(m)\lambda_{E_{a,b}}(n) = \frac{1}{(mn)^2} \sum_{a,b \bmod mn} \lambda_{E_{a,b}}(m)\lambda_{E_{a,b}}(n). \tag{2.1}$$

Our first simplifying assumption is that equation 2.1 is a good approximation in general. This is a reasonable approximation when AB is much larger than mn, as in this case anything remaining after the final full period will be small compared to the total sum. However when AB is small, and in particular is smaller than mn, it is likely that the remainder will be large compared to the total sum. As mentioned before, due to [CFK$^+$05], we do not expect this approximation error to affect our final result.

Using the Chinese remainder theorem and the previous assumption, we can determine that

$$\frac{1}{4|A||B|}\sum_{\substack{|a|\leq A\\|b|\leq B}}\lambda_{E_{a,b}}(m)\lambda_{E_{a,b}}(n)\approx\frac{1}{(mn)^2}\prod_{p_i}\sum_{a \bmod p_i^{\alpha_i+\beta_i}}\sum_{b \bmod p_i^{\alpha_i+\beta_i}}\lambda_{E_{a,b}}({p_i}^{\alpha_i})\lambda_{E_{a,b}}({p_i}^{\beta_i}). \tag{2.2}$$

We will next apply the Hecke relation, which states that $\lambda_{E_{a,b}}(p^m)\lambda_{E_{a,b}}(p)$ is equal to $\lambda_{E_{a,b}}(p^{m+1})+\lambda_{E_{a,b}}(p^{m-1})$ if p does not divide the discriminant of $E_{a,b}$, and $\lambda_{E_{a,b}}(p^{m+1})$ if p does divide the discriminant. Our second simplifying assumption will be to only consider the case where p does not divide the discriminant of $E_{a,b}$. A careful reading of equations 4.8-4.12 in [You10] suggest that this estimation will not have a large effect on our final result. In this case, $\lambda_{E_{a,b}}({p_i}^{\alpha_i})\lambda_{E_{a,b}}({p_i}^{\beta_i})=\sum_{0\leq d\leq \min(\alpha_i,\beta_i)}\lambda_{E_{a,b}}(p_i^{\alpha_i+\beta_i-2d})$, and we can write

$$\frac{1}{4|A||B|}\sum_{\substack{|a|\leq A\\|b|\leq B}}\lambda_{E_{a,b}}(m)\lambda_{E_{a,b}}(n)\approx\frac{1}{(mn)^2}\prod_{p_i}\sum_{a \bmod p_i^{\alpha_i+\beta_i}}\sum_{b \bmod p_i^{\alpha_i+\beta_i}}\sum_{d=0}^{\min(\alpha_i,\beta_i)}\lambda_{E_{a,b}}(p_i^{\alpha_i+\beta_i-2d}). \tag{2.3}$$

Since $\lambda_{E_{a,b}}(p_i^{\alpha_i+\beta_i-2d})$ is periodic modulo p, this can be rewritten as

$$\frac{1}{4|A||B|}\sum_{\substack{|a|\leq A\\|b|\leq B}}\lambda_{E_{a,b}}(m)\lambda_{E_{a,b}}(n)\approx\frac{1}{(mn)^2}\prod_{p_i}\sum_{0\leq d\leq \min(\alpha_i,\beta_i)}p_i^{2(\alpha_i+\beta_i-1)}\left(\sum_{a \bmod p_i}\sum_{b \bmod p_i}\lambda_{E_{a,b}}(p_i^{\alpha_i+\beta_i-2d})\right). \tag{2.4}$$

At this point, we will use our next simplifying assumption. By [You10], we know the following is true:

$$\sum_{a \text{ mod } p} \sum_{b \text{ mod } p} \lambda_{E_{a,b}}(p^j) = \begin{cases} 0, & \text{j odd} \\ p^2, & \text{j=0} \\ 0, & \text{j even and } 2 \leq j \leq 8 \\ x_{p,j}, & \text{j even and } \geq 10 \end{cases} \tag{2.5}$$

where $x_{p,j}$ is related to the trace of a Hecke operator. Since this last case occurs relatively rarely and makes $\lambda_{E_{a,b}}(p^j)$ difficult to work with, we approximate λ in the following manner:

$$\sum_{a \text{ mod } p} \sum_{b \text{ mod } p} \lambda_{E_{a,b}}(p^j) \approx \begin{cases} p^2, & \text{j=0} \\ 0, & \text{otherwise} \end{cases} \tag{2.6}$$

As stated before, we expect this approximation to have little effect on our final result for the reasons described in [CFK$^+$05].

Using the above definition, we can determine that $\sum_{a \text{ mod } p_i} \sum_{b \text{ mod } p_i} \lambda_{E_{a,b}}(p_i^{\alpha_i+\beta_i-2d}) \approx 0$ unless $\alpha_i + \beta_i = 2d$, and

$$\frac{1}{4|A||B|} \sum_{\substack{|a| \leq A \\ |b| \leq B}} \lambda_{E_{a,b}}(m)\lambda_{E_{a,b}}(n) \approx \frac{1}{(mn)^2} \prod_{p_i} \sum_{\substack{0 \leq d \leq \min(\alpha_i,\beta_i) \\ \alpha_i+\beta_i=2d}} p_i^{2(\alpha_i+\beta_i)}. \tag{2.7}$$

But, since $d \leq \min(\alpha_i, \beta_i)$, $\alpha_i + \beta_i = 2d$ only when $d = \alpha_i = \beta_i$. Also, when $\alpha_i = \beta_i$ for all i, $m = n$. Thus, when $m \neq n$, we get 0, and when $m = n$, we can write

$$\frac{1}{4|A||B|} \sum_{\substack{|a| \leq A \\ |b| \leq B}} \lambda_{E_{a,b}}(m)\lambda_{E_{a,b}}(n) \approx \frac{1}{m^4} \prod_{p_i} p_i^{4\alpha_i} \approx \frac{1}{m^4} m^4 \approx 1 \tag{2.8}$$

which gives us Heuristic 2.2.

We will next use Heuristic 2.2 to estimate how $L_{tail}(1/2, E) = L(1/2, E) - L_{approx}(1/2, E) = 2\sum_{n \geq \delta\sqrt{N_E}} \frac{\lambda_E(n)}{\sqrt{n}} e^{\frac{-2\pi n}{\sqrt{N_E}}}$ grows as we take larger families. In order to do this, we need to make a fourth simplifying assumption. We will approximate L_{tail} with

$$L^*_{tail} = 2 \sum_{n \geq \delta\sqrt{X_{A,B}}} \frac{\lambda_E(n)}{\sqrt{n}} e^{\frac{-2\pi n}{\sqrt{X_{A,B}}}} \tag{2.9}$$

where $X_{A,B}$ is a value that is on the same order as the conductors of the elliptic curves in the family. We then get the following heuristic:

Heuristic 2.3.

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

We begin our discussion of support for this heuristic by noting that

$$(L^*_{tail,E_{a,b}})^2 = \left(2 \sum_{n \geq \delta\sqrt{X_{A,B}}} \frac{\lambda_E(n)}{\sqrt{n}} e^{\frac{-2\pi n}{\sqrt{X_{A,B}}}}\right)^2 \tag{2.10}$$

$$= 4 \sum_{n_1 \geq \delta\sqrt{X_{A,B}}} \sum_{n_2 \geq \delta\sqrt{X_{A,B}}} \frac{\lambda_E(n_1)\lambda_E(n_2)}{\sqrt{n_1 n_2}} e^{\frac{-2\pi(n_1+n_2)}{\sqrt{X_{A,B}}}}. \tag{2.11}$$

Therefore we get

$$\frac{1}{4|A||B|} \sum_{\substack{|a|\leq A \\ |b|\leq B}} (L^*_{tail,E_{a,b}})^2 = \frac{4}{4|A||B|} \sum_{\substack{|a|\leq A \\ |b|\leq B}} \sum_{n_1 \geq \delta\sqrt{X_{A,B}}} \sum_{n_2 \geq \delta\sqrt{X_{A,B}}} \frac{\lambda_{E_{a,b}}(n_1)\lambda_{E_{a,b}}(n_2)}{\sqrt{n_1 n_2}} e^{\frac{-2\pi(n_1+n_2)}{\sqrt{X_{A,B}}}} \tag{2.12}$$

$$= 4 \sum_{n_1 \geq \delta\sqrt{X_{A,B}}} \sum_{n_2 \geq \delta\sqrt{X_{A,B}}} e^{\frac{-2\pi(n_1+n_2)}{\sqrt{X_{A,B}}}} \frac{1}{4|A||B|} \sum_{\substack{|a|\leq A \\ |b|\leq B}} \frac{\lambda_{E_{a,b}}(n_1)\lambda_{E_{a,b}}(n_2)}{\sqrt{n_1 n_2}}. \tag{2.13}$$

However, by Heuristic 2.2, the innermost sum is approximately 0 unless $n_1 = n_2$, in which case it is 1. Therefore

$$\frac{1}{4|A||B|}\sum_{\substack{|a|\leq A\\|b|\leq B}}(L^*_{tail,E_{a,b}})^2 \approx 4\sum_{n\geq\delta\sqrt{X_{A,B}}}\frac{e^{\frac{-4\pi n}{\sqrt{X_{A,B}}}}}{n}. \tag{2.14}$$

Since $n \geq \delta\sqrt{X_{A,B}}$, we know that

$$4\sum_{n\geq\delta\sqrt{X_{A,B}}}\frac{e^{\frac{-4\pi n}{\sqrt{X_{A,B}}}}}{n} \leq \frac{4}{\delta\sqrt{X_{A,B}}}\sum_{n\geq\delta\sqrt{X_{A,B}}}e^{\frac{-4\pi n}{\sqrt{X_{A,B}}}}. \tag{2.15}$$

Approximating via integration yields that

$$\begin{aligned}\frac{4}{\delta\sqrt{X_{A,B}}}\sum_{n\geq\delta\sqrt{X_{A,B}}}e^{\frac{-4\pi n}{\sqrt{X_{A,B}}}} &\leq \frac{4e^{-4\pi\delta}}{\delta\sqrt{X_{A,B}}} + 4\int_{\delta\sqrt{X_{A,B}}}^{\infty}e^{\frac{-4\pi t}{\sqrt{X_{A,B}}}}\,dt &(2.16)\\ &= \frac{4e^{-4\pi\delta}}{\delta\sqrt{X_{A,B}}} + \frac{e^{-4\pi\delta}}{\pi\delta}. &(2.17)\end{aligned}$$

As A and B go to infinity, $X_{A,B}$ also goes to infinity. But as $X_{A,B}$ goes to infinity, the first term gets small compared to the second term. Thus we can write

$$\lim_{A,B\to\infty}\frac{1}{4|A||B|}\sum_{\substack{|a|\leq A\\|b|\leq B}}(L^*_{tail,E_{a,b}})^2 \leq \frac{e^{-4\pi\delta}}{\pi\delta}. \tag{2.18}$$

We are now ready to give our support for Heuristic 2.1. We would like to show that

$$|Ш_{E,\text{tail}}| = |Ш_{\text{approx},E} - Ш_E| < \frac{1}{2}. \tag{2.19}$$

We first note that, using the Birch and Swinnerton-Dyer conjecture, we can write

$$|Ш_{E,\text{tail}}| = |\frac{L_{\text{approx}}(1/2, E)|E_{\text{tors}}|^2}{\Omega_E c_E} - \frac{L(1/2, E)|E_{\text{tors}}|^2}{\Omega_E c_E}| \tag{2.20}$$

$$= |\frac{L_{\text{tail}}(1/2, E)|E_{\text{tors}}|^2}{\Omega_E c_E}|. \tag{2.21}$$

We will consider how this grows as the conductor gets large. By Heuristic 2.3, we expect that, on average for large conudctors, $L_{\text{tail}} \leq \sqrt{\frac{e^{-4\pi\delta}}{\pi\delta}}$. Mazur showed in [Maz77] that the order of the torison group, $|E_{\text{tors}}|$ is uniformly bounded by a constant. The Tamagawa number, c_E, is an integer, and therefore always at least 1. Finally, a heuristic by Watkins [Wat08] states that as the conductor N_E goes to infinity, $\Omega_E \asymp N_E^{-1/12}$.

Therefore, we can estimate that, on average for large conductors,

$$|Ш_{E,\text{tail}}| \leq \frac{\sqrt{\frac{e^{-4\pi\delta}}{\pi\delta}}|E_{\text{tors}}|^2}{N_E^{-1/12} c_E}. \tag{2.22}$$

We would like to consider how δ must grow so that

$$\frac{\sqrt{\frac{e^{-4\pi\delta}}{\pi\delta}}|E_{\text{tors}}|^2}{N_E^{-1/12} c_E} < \frac{1}{2} \tag{2.23}$$

as N_E gets large.

We first rewrite this as

$$\frac{{N_E}^{1/6} e^{-4\pi\delta}}{4\pi\delta} < \frac{c_E^2}{16|E_{\text{tors}}|^4}. \tag{2.24}$$

We note that this will definitely be true when

$$\frac{{N_E}^{1/6} e^{-4\pi\delta}}{4\pi\delta} < \frac{1}{16|E_{\text{tors}}|^4}, \tag{2.25}$$

since $c_E \geq 1$. In addition, this estimate will not cause us to significantly underestimate our bound for δ, since c_E is almost constant.

If we let $\delta \geq \frac{1}{24\pi} \log N_E - C_2 \log\log N_E$ for some constant C_2, then

$$e^{-4\pi\delta} \leq e^{-4\pi(\frac{1}{24\pi}\log N_E - C_2 \log\log N_E)} \tag{2.26}$$

$$= e^{\frac{-1}{6}\log N_E + 4\pi C_2 \log\log N_E} \tag{2.27}$$

$$= N_E^{\frac{-1}{6}} e^{4\pi C_2 \log\log N_E} \tag{2.28}$$

$$= N_E^{\frac{-1}{6}} (\log N_E)^{4\pi C_2}. \tag{2.29}$$

Therefore, for large enough N_E,

$$\frac{{N_E}^{1/6} e^{-4\pi\delta}}{4\pi\delta} < \frac{(\log N_E)^{4\pi C_2}}{4\pi(\frac{1}{24\pi}\log N_E - C_2 \log\log N_E)} \tag{2.30}$$

$$= \frac{(\log N_E)^{4\pi C_2}}{\frac{1}{6}\log N_E - 4\pi C_2 \log\log N_E)}. \tag{2.31}$$

If we pick C_2 such that $4\pi C_2 < 1$ (for example, $C_2 = \frac{1}{8\pi}$), then for large N_E this will approach 0 as the denominator grows more quickly than the numerator. In other words, when $\delta \geq \frac{1}{24\pi}\log N_E - C_2 \log\log N_E$ and the conductor is large, $\frac{\sqrt{\frac{e^{-4\pi\delta}}{\pi\delta}}|E_{\text{tors}}|^2}{C_1 N_E^{-1/12} c_E} < \frac{1}{2}$. Since, as previously mentioned, $|\text{Ш}_{E,\text{tail}}|$ can be approximated, on average, by $\frac{\sqrt{\frac{e^{-4\pi\delta}}{\pi\delta}}|E_{\text{tors}}|^2}{C_1 N_E^{-1/12} c_E}$ when the conductor is large, we get Heuristic 2.1.

It is important to note that Heuristic 2.1 represents an average case result and not a worst case result. In other words, it is possible that even when we picked δ as described above, there may be outliers where this is not a good enough estimate to allow us to recover the actual value of $|\text{Ш}|$. Ideally, these points are relatively rare, and our method can be expected to work most of the time.

3. EMPIRICAL SUPPORT

In Section 2, we provided theoretic support that our method should work. In this section, we will examine our method empirically.

In order to gather data, we implemented the described algorithm in PARI/GP [PAR16]. The code itself can be found in appendix A. We decided to test our code primarily on families with maximum conductors on the order of 10^{10} and 10^{11}. In particular, we collected data for all elliptic curves $E : y^2 = x^3 + ax^2 + b$ where $630 \leq |a| \leq 900$, $10000 \leq |b| \leq 14000$, $\omega_E = 1$ and E is a global minimal model. These conductors are large enough that it has previously been difficult to compute the L-functions efficiently. However, they are still small enough that, with the method being discussed, they can be computed in a few seconds. This allows us to collect data for many elliptic curves.

The theoretical results from section 2 tell us that picking

$$\delta \geq \frac{1}{24\pi} \log N_E - C_2 \log\log N_E \tag{3.1}$$

with constant C_2 such that $4\pi C_2 < 1$ is necessary to approximate $L(1/2, E)$ precisely enough to accurately determine $|Ш|$, and thus $L(1/2, E)$. In particular, if we pick $C_2 = \frac{1}{8\pi}$ and $N_E = 10^{11}$, then

$$\begin{aligned} \delta &\geq \frac{1}{24\pi} \log 10^{11} - \frac{1}{8\pi} \log\log 10^{11} && (3.2) \\ &\approx 0.2 && (3.3) \end{aligned}$$

is at least necessary to determine $|Ш|$.

For our tests, we chose to use $\delta = 0.5$. In addition to recording the final central value (L) which we obtained for each elliptic curve, we also recorded the intermediate values

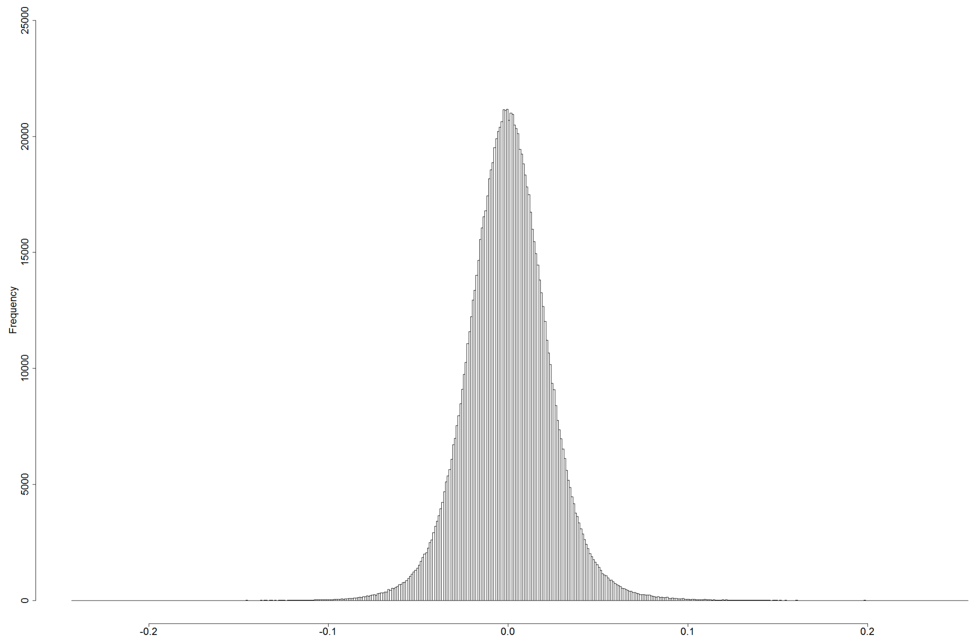

Figure 3.1: Distribution of L_{tail} Values for Given Elliptic Curves

L_{approx}, Ш, and Ш$_{\text{approx}}$ that were calculated during the process. In section 3.1, we will examine this collected data in relation to our average case results, while in section 3.2, we will consider the data points that differ significantly from our average case results.

3.1 Empirical Support for Average Case Results

We first give some empirical support that Heuristic 2.3 applies to the elliptic curves we are considering. This heuristic suggests that the average value of ${L_{\text{tail}}}^2$ over a family of elliptic curves similar to the one we are working over is expected ot be smaller than $\frac{e^{-4\pi\delta}}{\pi\delta}$. In particular, when $\delta = 0.5$, we expect that ${L_{\text{tail}}}^2 < 0.0012$ on average. Figure 3.1 shows the frequency with which different value of L_{tail} appear. We can see that most of the elliptic curves seem to have L_{tail} that is very close to zero. In fact, the average value of ${L_{\text{tail}}}^2$ over the given elliptic curves is $.00054$ (see figure 3.2). This is smaller than 0.0012, supporting our heuristic.

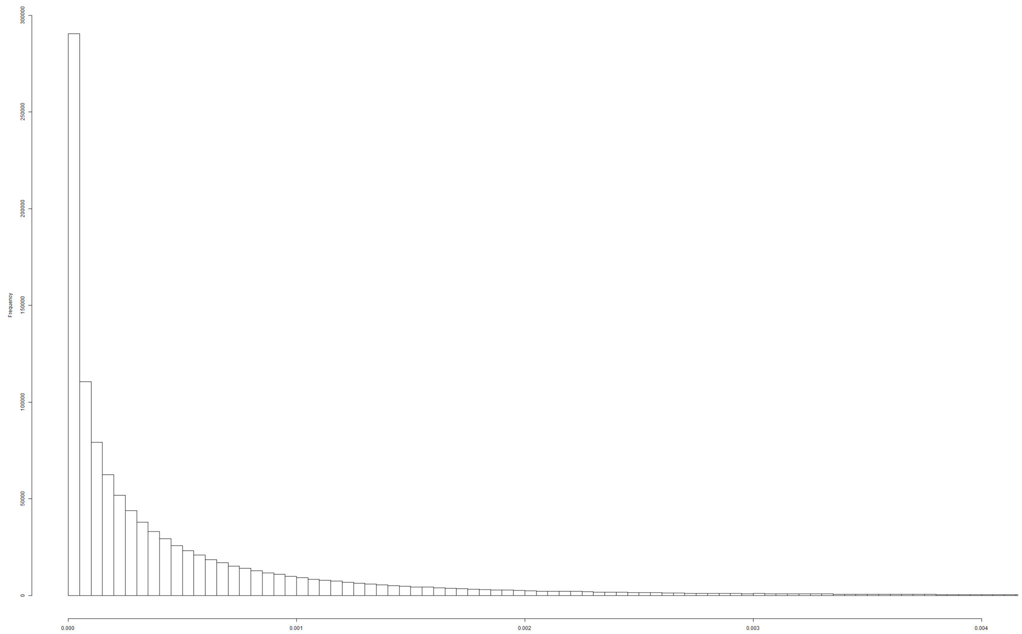

Figure 3.2: Distribution of ${L_{\text{tail}}}^2$ Values for Given Elliptic Curves (${L_{\text{tail}}}^2 > 0.004$ not shown)

However, it is important to note that we only expect the heurisitc to hold on average, not in general. One can see in figure 3.1 that there are some elliptic curves for which $|L_{\text{tail}}|$ is larger than expected. Figure 3.3 gives an idea of what these outliers look like. We can see that the values of $|L_{\text{tail}}|$ are, for the most part, very close to 0. However, there are occasionally elliptic curves with $|L_{\text{tail}}|$ of up to almost 0.3. This disparity between the average case and worst case will be discussed in further detail in section 3.2.

We next use our collected data to examine Heuristic 2.1. As noted previously, our choice of $\delta = 0.5$ is well above the $\delta = 0.2$ that Hueristic 2.1 suggests is necessary to handle elliptic curves with conductors on the order of 10^{10} and 10^{11}. Because of this, we would expect to see value of $|\text{Ш}_{\text{tail}}| = ||\text{Ш}| - \text{Ш}_{\text{approx}}|$ that are much smaller than $\frac{1}{2}$. Figure 3.4 shows the frequency with which different values of $|\text{Ш}_{\text{tail}}|$ appear over the elliptic curves for which we collected data. We can see that for the most part, $|\text{Ш}_{\text{tail}}|$ was

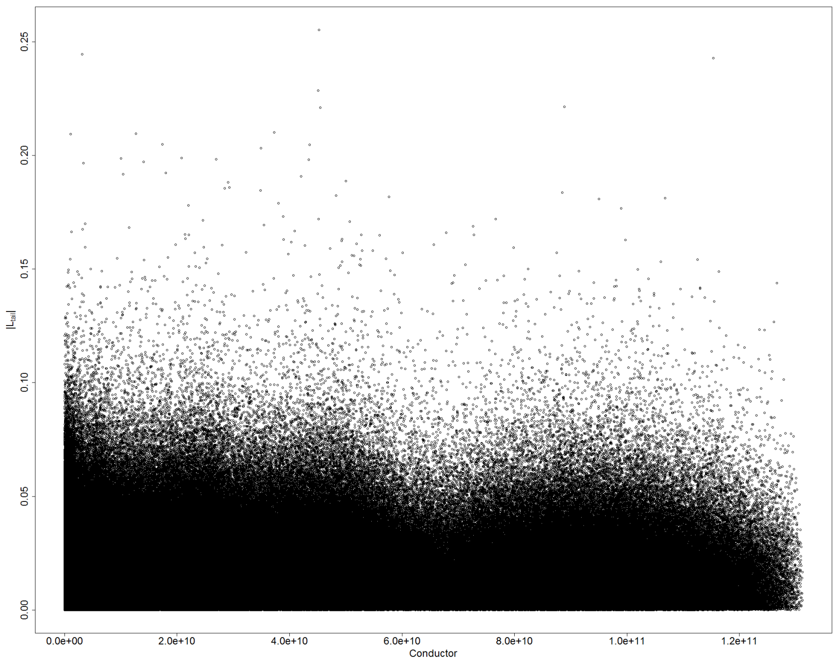

Figure 3.3: Conductor vs $|L_{\text{tail}}|$ for Given Elliptic Curves

smaller than 0.1, which is well below the 0.5 we expected.

Figure 3.5 also shows that most of the elliptic curves have small values of $|\text{Ш}_{\text{tail}}|$. However, this figure more clearly shows the outliers. It should be noted that since $|\text{Ш}|$ was obtained by rounding $|\text{Ш}_{\text{approx}}|$ to the nearest integer, it is impossible to obtain a value of $|\text{Ш}_{\text{tail}}|$ larger than 0.5. If $|\text{Ш}_{\text{tail}}|$ should be larger than 0.5, our algorithm will return the incorrect value of $|\text{Ш}|$ and $1-|\text{Ш}_{\text{tail}}|$. However, since all of our values are well below 0.5, it is likely that rounding gave us the correct value for $|\text{Ш}|$. In addition, as noted earlier, it is conjecture that $|\text{Ш}|$ will always be a perfect square. Therefore the accuracy of our method is further supported by the fact that, in all of our data, the value we obtained for $|\text{Ш}|$ is a perfect square.

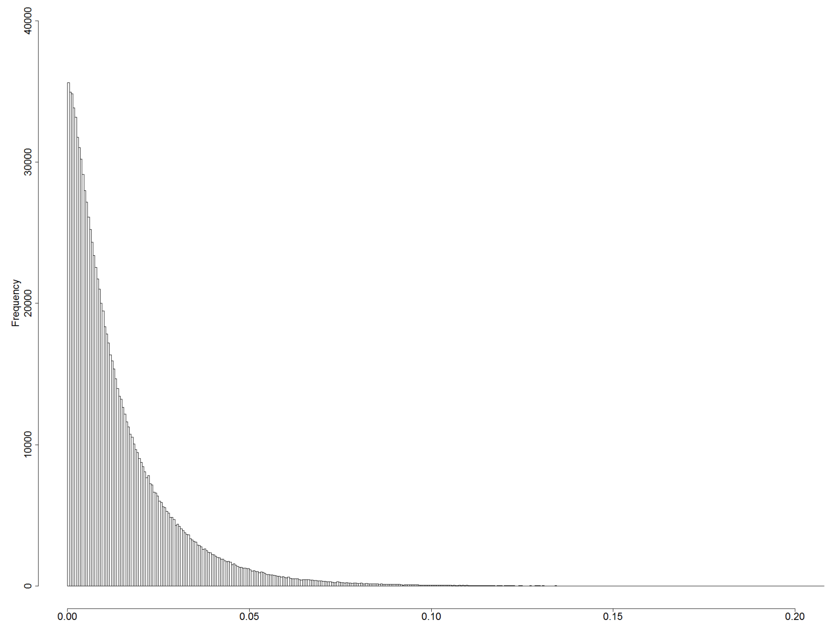

Figure 3.4: Distribution of $|Ш_{\text{tail}}|$ Values for Given Elliptic Curves

3.2 Analysis of Outliers

We previously showed that our data supports our average case results. However, our average case results tell us nothing about what happens in the worst case. It is possible that, even if we chose δ as desribed in Heuristic 2.1, $|Ш_{\text{tail}}|$ will be greater than 0.5, making it difficult to correctly obtain $|Ш|$. Therefore, if we can determine for which elliptic curves $|Ш_{\text{tail}}|$ is likely to be large, we can use larger δ or a different method to ensure we calculate the central value correctly.

As noted in section 2,

$$|Ш_{\text{tail}}| = \left| \frac{L_{\text{tail}}(1/2, E)|E_{\text{tors}}|^2}{\Omega_E c_E} \right|. \tag{3.4}$$

In other words, $|Ш_{\text{tail}}|$ is likely to be large when either $|L_{\text{tail}}|$ or $|E_{\text{tors}}|$ is large, or when

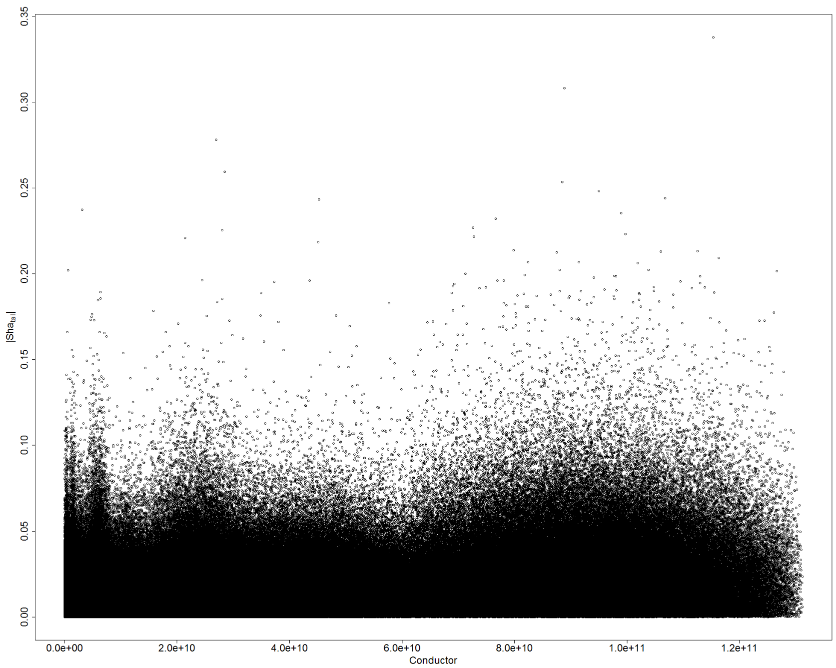

Figure 3.5: Conductor vs $|Ш_{\text{tail}}|$ for Given Elliptic Curves

Ω_E or c_E is small. Examining all of the elliptic curves with $|Ш_{\text{tail}}| > 0.2$ suggests that the most important factor is a large $|L_{\text{tail}}|$, since all of these elliptic curves have $|L_{\text{tail}}|$ larger than 0.1 (see appendix B). Plotting $|L_{\text{tail}}|$ against $|Ш_{\text{tail}}|$ (Figure 3.6) shows that this is mostly true. As can be seen in the graph, the data organizes itself in bands, where each band is characterized by the ratio $\frac{|Ш_{\text{tail}}|}{L_{\text{tail}}}$. This is explained by the fact $\frac{|Ш_{\text{tail}}|}{L_{\text{tail}}}$ is determined by Ω_E, c_E, and $|E_{\text{tors}}|$. 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 must represent a different value of $\frac{|E_{\text{tors}}|}{c_E}$

Understanding that $|Ш_{\text{tail}}|$ is determined primarily by the value of L_{tail} leads us to the question “What makes L_{tail} large?" Figure 3.3 suggests that the value of the conductor is not a significant factor, since there are examples of both elliptic curves of small conductor and elliptic curves of large conductor that have a large value for L_{tail}. In order to see if

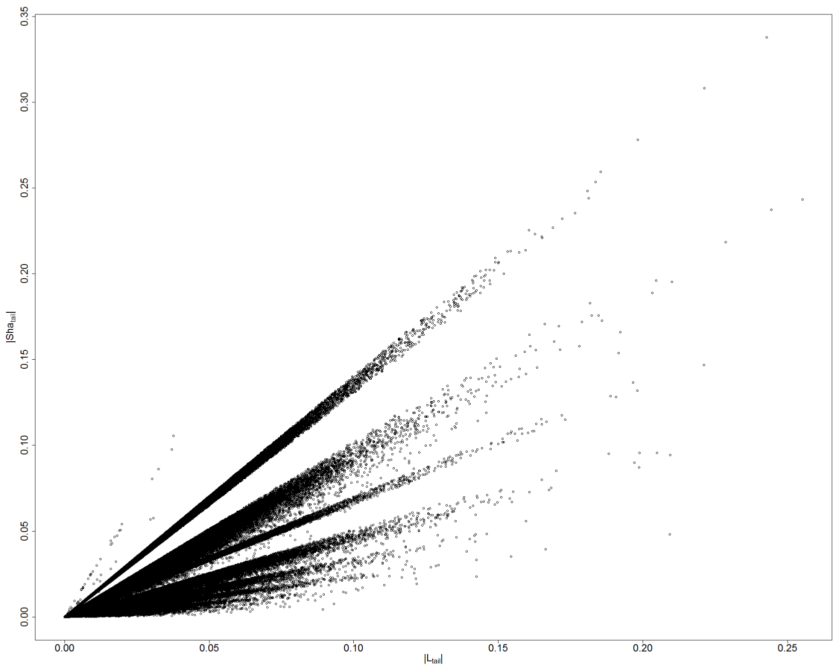

Figure 3.6: $|L_{\text{tail}|}$ vs $|Ш_{\text{tail}}|$ for Given Elliptic Curves

there was any easily identifiable property of an elliptic curve that correlated to a large value of L_{tail}, we plotted the value of L_{tail} against several different values associated with elliptic curves. The resulting graphs can be seen in appendix C. Examining these, it appears that elliptic curves with a small real period, tamagawa number, or torsion group are more likely to have a large value of L_{tail}. However, this is not very telling, since most of the elliptic curves in our family have a small real period, tamagawa number, and torsion group. Thus any given elliptic curve, including a particular elliptic curve with a large value of L_{tail}, is most likely going to have a small real period, tamagawa number, and torsion group. Therefore this observation tells us little about how to predict whether an elliptic curve will have an unusally large value for L_{tail}.

The other elliptic curve property that appears to correlate with the value of L_{tail} is the central value itself. As we can see in Figure 3.7, most of the elliptic curves with a large

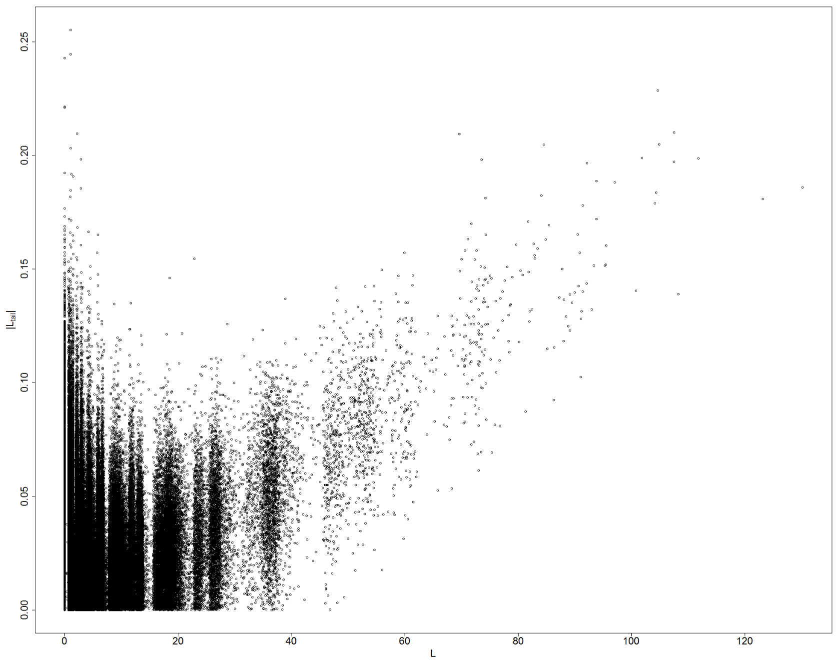

Figure 3.7: L vs $|L_{\text{tail}}|$ for Given Elliptic Curves

central value also had a large value of L_{tail}. However, it is important to also note that many elliptic curves with a central value very close to 0 also have a larger value of L_{tail}. In other words, an elliptic curve with large central value is very likely to also have a large value of L_{tail}, but there are additional elliptic curves with very small central values that also have large values of L_{tail}.

Since we have determined that elliptic curves with large central value are likely to have large values of L_{tail}, we can take extra measures while working with these elliptic curves to ensure that we get an approximation that allows us to accurately determine Ш. However, there are still many elliptic curves with large L_{tail} that are not accounted for. These appear to generally have central values very close to 0. Since, as seen in Figure 3.8, almost all of the elliptic curves have central values very close to 0, this gives us little information to work with. It would be useful to, in the future, determine a method to differentiate between

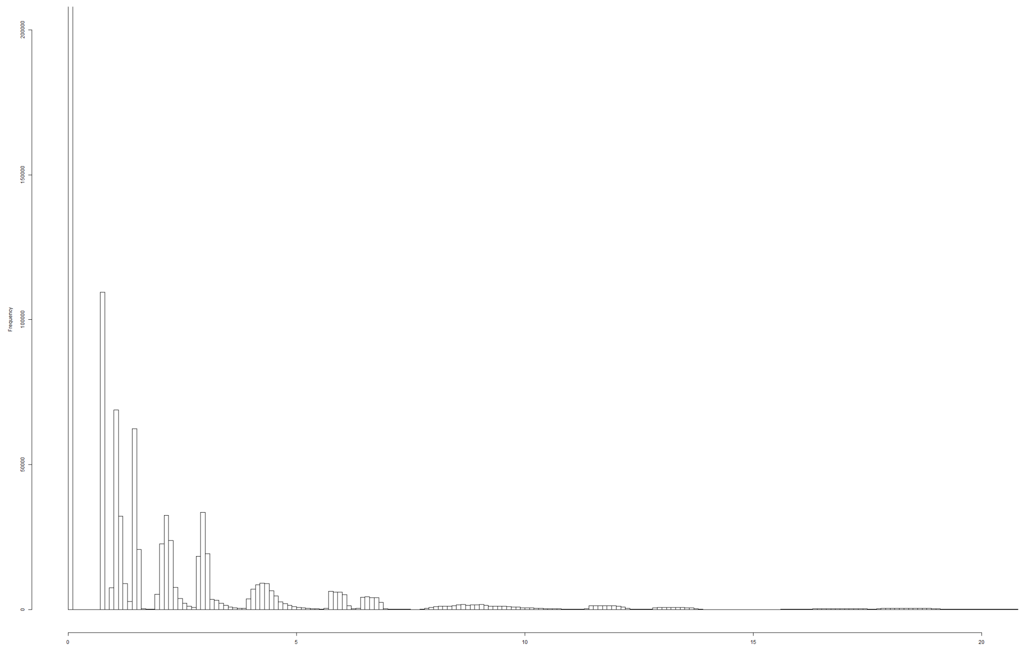

Figure 3.8: Frequency of Central Values for Given Elliptic Curves ($L(1/2, E) > 20$ not shown)

those elliptic curves with small central value and small L_{tail} from those with small central value and large L_{tail}.

REFERENCES

[CFK$^+$05] J. B. Conrey, D. W. Farmer, J. P. Keating, M. O. Rubinstein, and N. C. Snaith. Integral moments of l-functions. *Proceedings of the London Mathematical Society*, 91(1):33–104, 2005.

[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.

[Maz77] Barry Mazur. Modular curves and the eisenstein ideal. *Publications MathÃl'matiques de l'IHÃĽS*, 47:33–186, 1977.

[Mor22] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Cambridge Philos. Soc.*, 21:179–192, 1922.

[PAR16] PARI Group, Univ. Bordeaux. *PARI/GP version* `2.9.0`, 2016. available from `http://pari.math.u-bordeaux.fr/`.

[RS02] K. Rubin and A. Silverberg. Ranks of elliptic curves. *Bulletin of the American Mathematical Society*, 39(4):455–474, 2002.

[TW95] Richard Taylor and Andrew Wiles. Modular elliptic curves and fermatâĂŹs last theorem. *Ann. of Math.*, 141(2):443–551, 1995.

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

[Wil95] Andrew Wiles. Ring-theoretic properties of certain hecke algebras. *Ann. of Math.*, 141(2):553–572, 1995.

[You10] Matthew P. Young. Moments of the critical values of families of elliptic curves, with applications. *Canad. J. Math.*, 62:1155–1181, 2010.

APPENDIX A. FUNCTIONS USED IN CALCULATIONS

The following function is the primary function used to calculate and record elliptic curves along with their central values:

```
get_values(a1,a2,b1,b2,o_filename) = {

    local(E, root_no, L, t_approx, T, diff, time, L_1d,
        o_filename2, tors, tama, period, L_tail, L_appr);

    o_filename = concat(o_filename, ".csv");

    write(o_filename, "delta, a, b, N, root_no, L_approx,
        sha_approx, sha, diff, L, time (s), tors, tama,
        rlperiod, L_tail, disc");

    for(a=a1,a2,
    for(b=b1, b2,

        E = ellinit([a, b]);
        root_no = ellrootno(E);

        if(check_min(E),
        if(root_no==1,

        gettime();
        write1(o_filename, .5);
        write1(o_filename, ", ");
        write1(o_filename, a);
        write1(o_filename, ", ");
        write1(o_filename, b);
        write1(o_filename, ", ");
        write1(o_filename, ellglobalred(E)[1]);
        write1(o_filename, ",");
        write1(o_filename, root_no);
        write1(o_filename, ", ");
        L_appr = L_approx(E, .5);
        write1(o_filename, L_appr);
        write1(o_filename, ", ");
        t_approx = tsg(E, L_appr);
        write1(o_filename, t_approx);
```

```
        write1(o_filename, ", ");
        T = round(t_approx);
        write1(o_filename, T);
        write1(o_filename, ", ");
        diff = abs(T - t_approx);
        write1(o_filename, diff);
        write1(o_filename, ", ");
        L = L_act(E, T);
        write1(o_filename, L);
        write1(o_filename, ", ");
        time = gettime();
        write1(o_filename, round(time/1000));
        tors = elltors(E)[1];
        tama = ellglobalred(E)[3];
        period = get_real_period(E);
        write1(o_filename, ",");
        write1(o_filename, tors);
        write1(o_filename, ", ");
        write1(o_filename, tama);
        write1(o_filename, ", ");
        write1(o_filename, period);
        write1(o_filename, ", ");
        L_tail = abs(L-L_appr);
        write1(o_filename, L_tail);
        write1(o_filename, ", ");
        write(o_filename, E.disc););

    )));
    write("~/Documents/research/summer_data/0_log.csv", ",1");
    return(1);
};
```

The following is the set of helper functions called by the main funciton above:

```
get_real_period(E) = {
    local(real_period);
    real_period = E.omega[1];
    if((E.disc>0),
        real_period = real_period*2;
    );
    return(real_period);
```

```
}

L_approx(E, delta = 1) = {
    local(ans, root_no, an, cond);
    root_no = ellrootno(E);
    cond = ellglobalred(E)[1];
    ans = 0;
    all_ak = ellan(E, truncate(sqrt(cond))+1);
    if(root_no!=-1,
        for(i=1, delta*sqrt(cond),
            an = all_ak[i];
            ans = ans + an/i*exp(-2*Pi*i/sqrt(cond)););
        ans = ans*(root_no+1);
    );
    return(ans)
};

tsg(E, L) = {
    local(tors, period, tama, final);
    tors = elltors(E)[1];
    tama = ellglobalred(E)[3];
    period = get_real_period(E);

    final = L*sqr(tors)/period/tama;
    return(final)
};

check_min(E) = {
    local(temp);
    temp = ellglobalred(E)[2];
    if(temp == [1,0,0,0], return(1), return(0))
};

L_act(E, T) = {
    local(rp, tama, tors, final);
    tors = elltors(E)[1];
    tama = ellglobalred(E)[3];
    rp = get_real_period(E);
    final = rp*T*tama/tors/tors;
    return(final);
};
```

APPENDIX B. ELLIPTIC CURVES WITH LARGE VALUES OF $|Ш_{\textbf{TAIL}}|$

In order to determine which elliptic curves are likely to have larege $|Ш_{\text{tail}}|$, we examined all elliptic curves with $|Ш_{\text{tail}}| \geq 0.2$. The results are shown below.

a	b	$\lvert Ш_{\text{tail}}\rvert$	L_{tail}	$\lvert E_{\text{tors}}\rvert$	c_E	Ω_E
665	11017	0.200	0.152	1	1	0.760
728	11302	0.214	0.159	1	1	0.746
743	10375	0.222	0.165	1	1	0.745
749	10288	0.227	0.169	1	1	0.744
752	11810	0.212	0.157	1	1	0.740
758	10627	0.232	0.172	1	1	0.742
794	10387	0.202	0.148	1	1	0.735
812	11855	0.248	0.181	1	1	0.729
827	10955	0.202	0.147	1	1	0.727
839	10163	0.207	0.150	1	1	0.726
842	10790	0.253	0.184	1	1	0.725
863	10795	0.207	0.149	1	1	0.720
875	10315	0.308	0.221	1	1	0.718
896	11941	0.278	0.198	1	1	0.713
665	13621	0.235	0.177	1	1	0.751
707	12065	0.221	0.165	1	1	0.748
707	13955	0.244	0.181	1	1	0.742
-787	13690	0.237	0.244	1	1	1.030
803	12415	0.223	0.163	1	1	0.729
818	12443	0.206	0.150	1	1	0.727
827	13295	0.213	0.154	1	1	0.723
854	13222	0.338	0.243	1	1	0.719
857	12125	0.202	0.146	1	1	0.720
860	12298	0.213	0.153	1	1	0.719
881	13852	0.202	0.144	1	1	0.713
884	12685	0.260	0.185	1	1	0.715
896	12373	0.225	0.161	1	1	0.713
899	12715	0.209	0.149	1	1	0.712
-847	13957	0.243	0.255	1	1	1.049
-826	13703	0.218	0.229	1	1	1.047

Table B.1: Relevant Data for Elliptic Curves with Large $|Ш_{\text{tail}}|$

APPENDIX C. ADDITIONAL GRAPHS

In order to determine what factors cause $|L_{\text{tail}}|$ to be unusually large, we investigated how $|L_{\text{tail}}|$ correlates with other elliptic curve data. The results of this investigation are shown below.

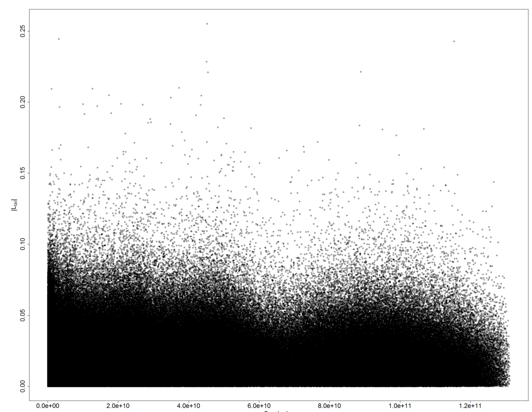

Figure C.1: Conductor vs $|L_{\text{tail}}|$ for Given Elliptic Curves

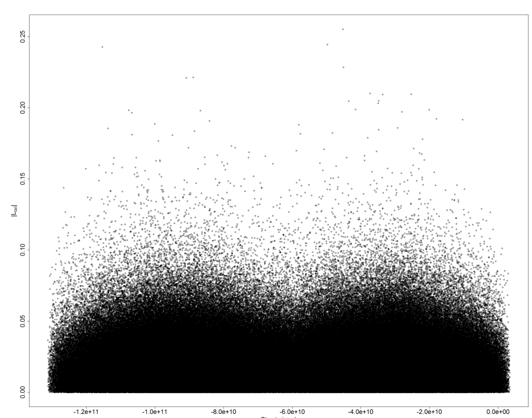

Figure C.2: Discriminant vs $|L_{\text{tail}}|$ for Given Elliptic Curves

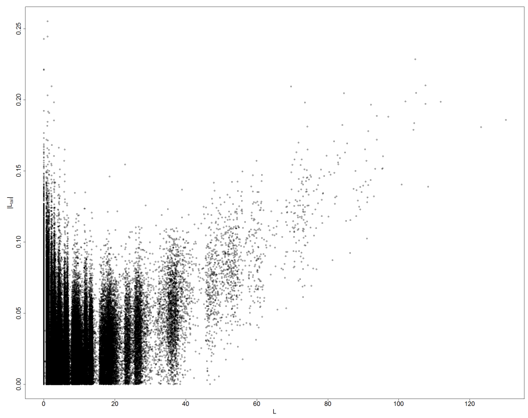

Figure C.3: $L(1/2, E)$ vs $|L_{\text{tail}}|$ for Given Elliptic Curves

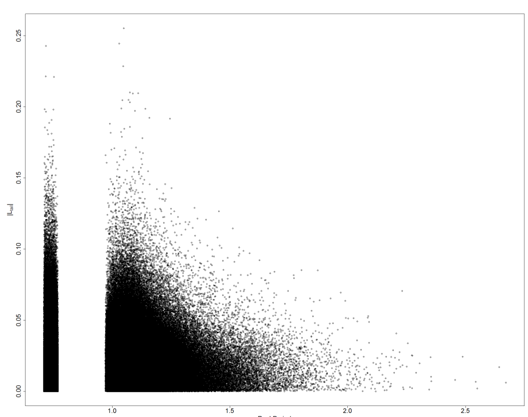

Figure C.4: Real Period vs $|L_{\text{tail}}|$ for Given Elliptic Curves

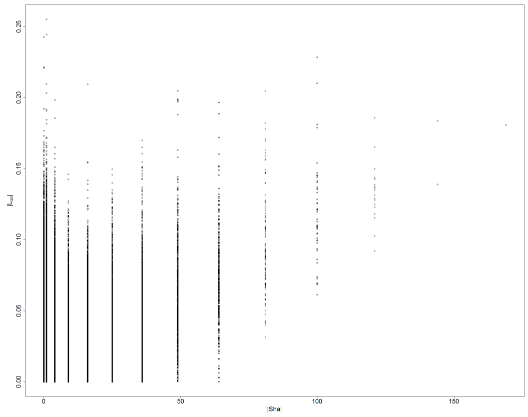

Figure C.5: $|Ш|$ vs $|L_{\text{tail}}|$ for Given Elliptic Curves

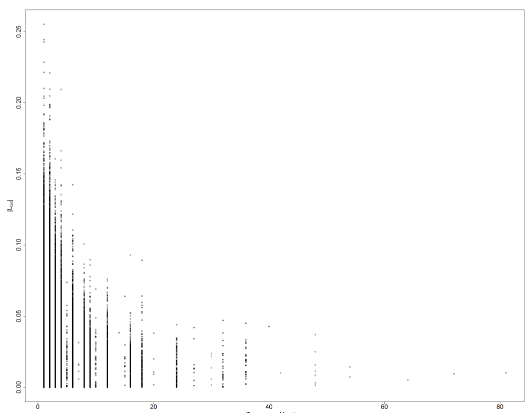

Figure C.6: Tamagawa Number vs $|L_{\text{tail}}|$ for Given Elliptic Curves

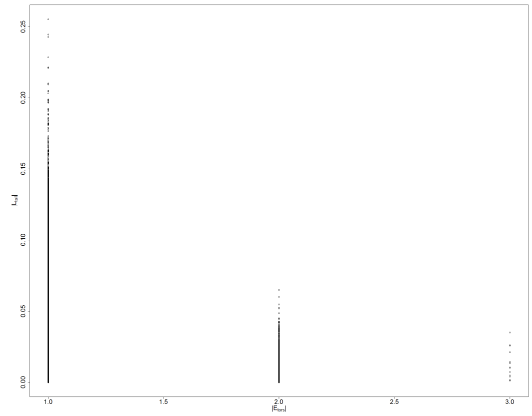

Figure C.7: $|E_{\text{tors}}|$ vs $|L_{\text{tail}}|$ for Given Elliptic Curves