The Zeros of Elliptic Curve L-functions: Analytic Algorithms with Explicit Time Complexity

Simon Spicer

A dissertation submitted in partial fulfillment
of the requirements for the degree of

Doctor of Philosophy

University of Washington

2015

Reading Committee:

William Stein, Chair

Ralph Greenberg

Neal Koblitz

Bernard Deconinck, GSR

Program Authorized to Offer Degree:
UW Mathematics

University of Washington

Abstract

The Zeros of Elliptic Curve L-functions:
Analytic Algorithms with Explicit Time Complexity

Simon Spicer

Chair of the Supervisory Committee:
Professor William Stein
Mathematics

Elliptic curves are central objects of study in modern-day algebraic number theory. The problem of how to determine the rank of a rational elliptic curve is a difficult one, and at the time of the writing of this thesis an unconditional general method for doing so is not known.

It has been known for decades that contingent on the Birch and Swinnerton-Dyer Conjecture, an algorithm to compute rank exists, but this algorithm has unknown time complexity. In the first part of this thesis we prove that, assuming standard conjectures, an *effective* algorithm exists to compute rank with time complexity that is polynomial in the curve's conductor. This method involves evaluating the L-function of the curve in question, and as such is practical for curves with conductors up to $\sim 10^{16}$ on current computer architecture.

The second part of this work addresses the question of what can be done when the conductor is too large for the above method to be practical. To this end we exhibit an analytic method to bound rank from above that doesn't rely on directly evaluating an elliptic curve's L-function, and as such can be used on curves with very large conductors. Because this method involves sums over the imaginary parts of the zeros of an elliptic curve L-function, we also include results concerning the locations thereof, and an exposition of related quantities.

PREFACE

I have attempted to emphasize accessibility and readability throughout this work. Specifically, no knowledge beyond standard graduate-level complex analysis and algebra is assumed, and advanced knowledge of number theoretic topics is *not* required. As such, I hope that the results in this dissertation are accessible to a wide audience, even those at the advanced undergraduate level. Chapter 1 was written specifically to be a gentle introduction to the subject matter of this thesis.

For the expert I recommend skipping straight to Chapter 2, wherein the main results are stated. Proofs for these results can be found in Chapters 4 and 5 (from 5.2 onwards).

Finally, a note on conjecture dependencies. Many of the results in this work are contingent on the validity of three of the major open conjectures in number theory: the Birch and Swinnerton-Dyer conjecture (BSD), the Generalized Riemann Hypothesis (GRH) and the ABC conjecture (ABC). For ease of exposition, instead of stating explicitly in a result which of the above conjectures are assumed, we will list the three-letter initial of each assumed conjecture after the heading of each result. For example, the following result:

Proposition 0.0.1 (BSD)**.** *A rational elliptic curve with odd parity has a point of infinite order.*

means that this proposition follows under the assumption that BSD is true.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

By no means did I produce this dissertation in a vacuum. Many individuals have provided critical contributions over the course of my studies, and we are thankful to all of them. However, some we must mention specifically. Sincere thanks must be given to my advisor William Stein, who for many years has provided the patient mentorship and guidance needed to make this dissertation a reality. I would also like to extend a heartfelt thanks to the University of Washington department of Mathematics as a whole, and to the graduate student coordinator Brooke Miller in particular, for supporting me throughout my studies at UW.

Beyond this, a number of mathematicians have given valuable advice. We are grateful for the correspondence with Barry Mazur on the explicit formula for elliptic curves, which was my entry point into the whole topic of elliptic curve L-functions; moreover we thank Peter Sarnak for his input on low-lying zeros of elliptic curve L-functions, and helping spur the formulation of the central idea of this thesis. John Cremona and Noam Elkies gave sage insight on the topics of the real period and regulator respectively. And we are grateful to John Voight, who used an early version of my rank estimation code and highlighted some significant bugs. And thanks must be given to Wei Ho, Jen Balakrishnan, Jamie Weigandt and Nathan Kaplan for putting up with my less-than-expert attempts to compute the ranks of large databases of elliptic curves.

And last but not least, a huge thank you to my wife Kimberly for her constant unwavering support throughout.

DEDICATION

To Kimberly and Bram, who comprise two thirds of the Spicer Theorem.

Chapter 1

INTRODUCTION

Let E be an elliptic curve over the rational numbers. We can think of E as the set of rational solutions (x, y) to a two-variable cubic equation in the form:

$$E : y^2 = x^3 + Ax + B \tag{1.0.1}$$

for some integers A and B, along with an extra "point at infinity". An important criterion is that the E be a smooth curve; this translates to the requirement that the discriminant D_E of the curve, given by $D_E = -16(4A^3 + 27B^2)$, is not zero.

One of the natural questions to ask when considering an elliptic curve is "how many rational solutions are there?" It turns out elliptic curves fall in that sweet spot where the answer could be zero, finitely many or infinitely many - and figuring out which is the case is a deeply non-trivial – and as yet still open – problem.

The rational solutions on E form an abelian group with a well-defined group operation that can be easily computed. By a theorem of Mordell, the group of rational points on an elliptic curve $E(\mathbb{Q})$ is finitely generated; we can therefore write

$$E(\mathbb{Q}) \approx E_{\text{Tor}}(\mathbb{Q}) \times \mathbb{Z}^r, \tag{1.0.2}$$

where $E_{\text{Tor}}(\mathbb{Q})$ is a finite group (called the torsion subgroup of E), and r is a non-negative integer, denoted the *algebraic rank* of E.

Determining the torsion subgroup of E is relatively straightforward. By a celebrated theorem of Mazur, rational elliptic curves have torsion subgroups that are (non-canonically) isomorphic to one of precisely fifteen possibilities: $\mathbb{Z}/n\mathbb{Z}$ for $n = 1$ through 10, or $\mathbb{Z}/12\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ for $n = 1$ though 4. However, computing the rank r – the number of independent rational points of infinite order on E – is hard, and no unconditional method to do

so currently exists. It is towards this end that the work in this dissertation hopes to contribute.

Perhaps surprisingly, we can translate the algebraic problem of finding the number of rational solutions on E to an analytic one – at least conjecturally. The method of doing so is via elliptic curve L-functions; these are complex-analytic entire functions that somehow encode a great deal of information about the elliptic curve they describe. Unfortunately, it takes a few steps to define them:

Definition 1.0.2. Let p be a prime number;

- Define $N_p(E)$ to be the number of points on the *reduced curve* E modulo p. That is (excepting the cases $p = 2$ or 3, for which the definition is slightly more complicated), if E has equation $y^2 = x^3 + Ax + B$, then

$$N_p(E) = 1 + \#\left\{(\overline{x}, \overline{y}) \in \mathbb{F}_p^2 : \ \ \overline{y} \equiv \overline{x}^3 + A\overline{x} + B \pmod{p}\right\}, \tag{1.0.3}$$

  where the 1 accounts for the aforementioned point at infinity on E not captured by the above equation.

- Let $a_p(E) = p + 1 - N_p(E)$.

Hasse's Theorem states that $a_p(E)$ is always less that $2\sqrt{p}$ in magnitude for any p, and the Sato-Tate conjecure (recently proven by Taylor et al.) states that for a fixed elliptic curve, the a_p values, once suitably normalized, are asymptotically distributed in a semi-circular distribution about zero. In other words, the number of solutions to an elliptic curve equation modulo p is always about p, and can never be very far from that value.

Definition 1.0.3. For prime p,

- Define the *local factor* $L_p(E, s)$ to be the function of the complex variable s as follows:

$$L_p(s) = \frac{1}{1 - a_p(E)p^{-s} + \epsilon(p)p^{-2s}}, \tag{1.0.4}$$

where $\epsilon(p)$ is 0 if p is a *prime of bad reduction*, and 1 otherwise. [For any elliptic curve E there are only a finite number of primes of bad reduction; they are precisely the primes that divide the discriminant D_E of a minimal model of E].

- The **(global) L-function $L(E,s)$ attached to** E is defined to be the product of all the local L-functions, namely

$$L(E,s) = \prod_p L_p(E,s). \tag{1.0.5}$$

The above representation of $L(E,s)$ is called the Euler product form of the L-function. If we multiply out the terms and use power series inversion we can also write $L_E(s)$ as a *Dirichlet series*:

$$L(E,s) = \sum_{n=1}^{\infty} a_n(E) n^{-s}, \tag{1.0.6}$$

where for non-prime n the coefficients a_n are defined to be exactly the integers you get when you multiply out the Euler expansion.

If you do some analysis using Hasse's bound on the size of the $a_p(E)$ and their distribution according to Sato-Tate, one can show that the above two series converge absolutely when the real part of s is greater than $\frac{3}{2}$ (see Lemma 5.1.7 and Corollary 5.1.8) and diverge when the real part of s is less than $\frac{1}{2}$. However, the modularity theorem of Breuil, Conrad, Diamond, Taylor and Wiles [8] [35] [36] states that these elliptic curve L-functions can actually be analytically continued to the entire complex plane. That is, for every elliptic curve L-function $L(E,s)$ as defined above, there is an entire function on $\mathbb{C}$ which agrees with the Euler product/Dirichlet series definition for $\mathrm{Re}(s) > \frac{3}{2}$, but is also defined – and explicitly computable – for all other complex values of s. This entire function is what we actually call the L-function attached to E.

The way we analytically continue $L(E,s)$ yields that the function is highly symmetric about the line $\mathrm{Re}(s) = 1$; moreover, because the function is defined by real coefficients $L_E(s)$ also obeys a reflection symmetry along the real axis. The point $s = 1$ is therefore in a very

real sense the *central point* for the L-function, and it is the behavior of $L(E, s)$ at the central point that conjecturally captures the rank information of E. This is established concretely in the Birch and Swinnerton-Dyer Conjecture, the first part of which we state below (the full conjecture is stated in Chapter 3):

Conjecture 1.0.4 (Birch, Swinnerton-Dyer, part (a))**.** *Let E be an elliptic curve over $\mathbb{Q}$, with attached L-series $L(E, s)$. Then the Taylor series expansion of $L_E(s)$ about the central point $s = 1$ is*

$$L(E, 1 + s) = Cs^r + O(s^{r+1}), \tag{1.0.7}$$

where $C \neq 0$ and r is the algebraic rank of E.

That is, the first part of the BSD conjecture asserts that the order of vanishing of $L(E, s)$ at the central point is precisely the algebraic rank of E.

[Aside: Brian Birch and Peter Swinnerton-Dyer formulated the eponymous conjecture in the 1960s based in part on numerical evidence generated by the EDSAC computer at the University of Cambridge; this makes it one of the first instances of computer-generated data being used to support a mathematical hypothesis. Given the vast amount of supporting computational evidence that has now been collected, the BSD conjecture is overwhelmingly believed to be true.]

We can therefore at least conjecturally determine the curve's algebraic rank by computing the order of vanishing of the elliptic curve's L-function at the central point. This converts an generally difficult algebraic problem into a perhaps more tractable analytic one.

The work in this thesis hopes to address the question of how to effectively compute the order of vanishing of $L(E, s)$ at $s = 1$, which is denoted r_{an}, the *analytic rank* of E. This, again, is a non-trivial task – for example, how do you numerically distinguish between the nth Taylor coefficient of $L(E, s)$ being identically zero, and it just being non-zero but so small in magnitude that it is indistinguishable from zero given your finite-precision computations?

The short answer is that, using a just a computer, you can't. We need theorems governing the magnitude of the Taylor coefficients – especially that leading coefficient C mentioned

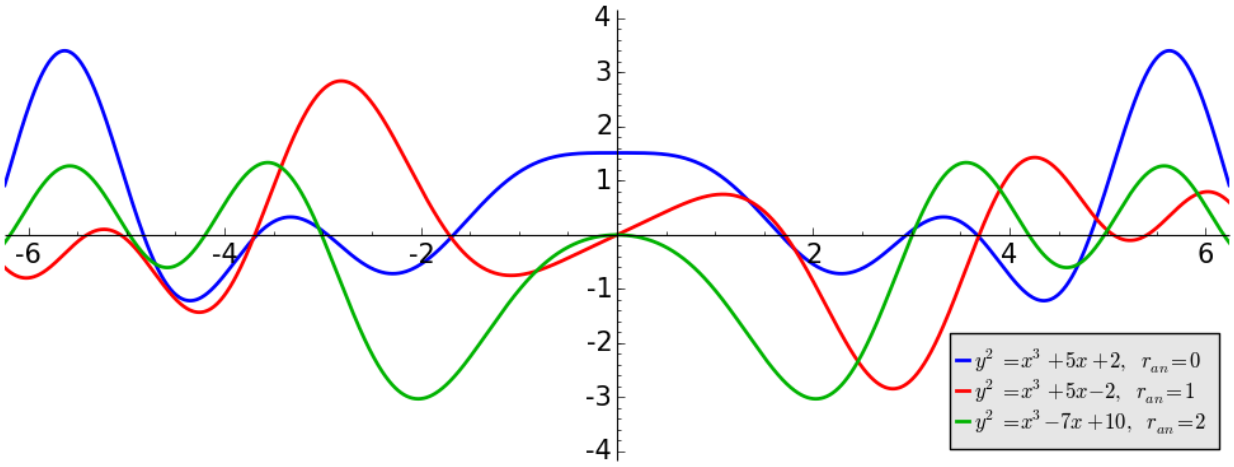

Figure 1.0.1: The values of three elliptic curve L-functions along the critical line $1 + it$ for $-6 \leq t \leq 6$, (transformed so that the functions are purely real to make the visualization a bit easier). Blue corresponds to a rank 0 curve, red is that of a rank 1 curve, and green is a rank 2 curve. Note that close to the origin the graphs look like non-zero constant function, a straight line and a parabola respectively.

above – in order to make analytic rank explicitly computable. This work establishes those results (assuming standard conjectures), telling us precisely how many digits of precision we need for an elliptic curve L-function to ascertain whether a given Taylor coefficient is or isn't zero. This in turn allows us to detail an algorithm to compute a curve's analytic rank with provable asymptotic time complexity . And thanks to the BSD conjecture, we therefore have a way to – at least conjecturally – compute the algebraic rank of E with a concrete handle on how long the computation will take.

The phrases "explicitly computable" and "provable asymptotic time complexity" are given precise definitions in the main body of this thesis, so read on for a more formal statement of the main problem and results.

The structure of this dissertation is as follows: Chapter 2 more formally lays out the problem tackled in this work and quotes the major results obtained in this work. Chapter 3 consists of an exposition of the mathematical background relevant to this thesis; while chapter 4 contains proofs of the main results. Chapter 5 consists of analytic methods and results that allow one, for example, to obtain estimates on analytic rank when evaluating a curve's L-function directly is computationally infeasible. Chapter 6 consists of remarks and ideas for future work. Supporting computational evidence is supplied where relevant, as opposed to being collected in its own chapter.

Chapter 2

PROBLEM OUTLINE AND MAJOR RESULTS

A natural question to ask in the field of computational number theory is: does an algorithm exist to compute the rank of an elliptic curve? Manin showed in [25] that, contingent on the Birch and Swinnerton-Dyer Conjecture being true, the answer to this question is yes. A rough outline of the method delineated by Manin is as follows: by day you search for points on a curve and thus obtain a lower bound on the algebraic rank of the curve; by night you evaluate central derivatives of the curve's L-function and thus obtain an upper bound on the analytic rank. If the Birch and Swinnerton-Dyer Conjecture is true, then eventually the two bounds will match up, and you will have computed the curve's rank.

However, although conjecturally guaranteed to terminate, the above method is ineffective from a time complexity perspective – there are no results establishing just how long it will take for the two bounds to match up. It is thus a somewhat less than satisfying answer to the question posed.

We therefore modify the question to the following: given a rational elliptic curve E, does an algorithm exist to compute the rank of E *that has provable big-Oh runtime in some measure of the arithmetic complexity of the curve*? In this work we answer this question in the affirmative – assuming standard conjectures.

The relevant measure of arithmetic complexity is the conductor N_E; below we provide an algorithm to compute rank and prove that it has polynomial runtime in N_E. However, to do so we must pay the price of having to assume not only the Birch and Swinnerton-Dyer Con-

jecture, but also the ABC Conjecture. The algorithm can be further sped up by assuming the Generalized Riemann Hypothesis. These will be abbreviated BSD, ABC and GRH respectively.

Specifically, we establish the following result:

Theorem 2.0.5 (BSD, ABC)**.** *Let $E/\mathbb{Q}$ have conductor N_E. There exists an algorithm to compute the algebraic rank r_E of E in $\tilde{O}\left(\sqrt{N_E}\right)$ time.*

The algorithm in question is as follows:

Algorithm 2.0.6 (Compute the rank of an elliptic curve)**.** Given a rational elliptic curve E represented by a global minimal Weierstrass equation $y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6$ with known conductor N_E:

1. Compute the real period Ω_E of E.
2. Set $k = \lceil 34 + 3.86 \log_2 N_E + \log_2(\Gamma(1.8 + 1.25 \log_2 N_E)) - \log_2 \Omega_E \rceil$, and set $m = 0$.
3. Evaluate $\frac{L_E^{(m)}(1)}{m!}$, the mth Taylor coefficient of the L-function of E at the central point, to k bits precision. If all k bits are zero, increment m by 1 and repeat this step.
4. Output $r_E = m$ and halt.

Here $\Gamma(s)$ is the usual Gamma function on $\mathbb{C}$.
Furthermore, if one also assumes GRH, step 2. can be replaced with:

2. Set $k = \lceil 22 + 2.47 \log_2 N_E + \log_2(\Gamma(1.25 + 0.87 \log_2 N_E)) - \log_2 \Omega_E \rceil$, and set $m = 0$.

This will reduce the runtime of Algorithm 2.0.6 by a constant factor.

This algorithm is not new – it is just a refinement on bounding the analytic rank of a curve with an explicitly chosen precision. What *is* new is the body of results in this dissertation proving that, assuming BSD and ABC (and optionally GRH), if the mth derivative of the L-series attached to E is zero to k bits precision, then it *is* identically zero. This allows us to

convert an algorithm that a priori only provides upper bounds on analytic rank, to one that computes rank exactly. Furthermore, we show that the algorithm is guaranteed to terminate in time polynomial in the curve's conductor.

Moreover, Algorithm 2.0.6 is in a sense optimal among analytic rank computation methods: since evaluating $L_E(s)$ takes $\tilde{O}(\sqrt{N_E})$ time, we cannot hope to get the rank out in time faster than this. [Of course other algebraic rank computation methods do exist that don't involve working with $L_E(s)$ directly. These, however, tend to be difficult to analyze from a complexity point of view. For example they scale with the size of the Tate-Shafarevich group of E, which isn't even known to be finite, let alone bounded by a power of the conductor.] The proof of Theorem 2.0.5 can be found in Section 4.1, but will require results established in preceding and following sections.

This work includes a number of related results; we quote below a selection which we believe are of particular interest:

Corollary 4.2.5. For $E/\mathbb{Q}$ with real period Ω_E and conductor N_E,

$$\Omega_E < 8.82921517\ldots \cdot (N_E)^{-\frac{1}{12}}, \tag{2.0.1}$$

That is, the real period goes to zero as the conductor of the curve goes to infinity. Moreover, this bound is optimal, in that the constant in the above inequality can be computed to any given precision, and a method exists to construct a curve E whose real period Ω_E is arbitrarily close to that constant times $(N_E)^{-\frac{1}{12}}$. This result is unconditional.

Theorem 5.2.3 (GRH)**.** Let γ 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 the imaginary parts of the nontrivial zeros of $L_E(s)$, where $\delta(x)$ is the usual Dirac delta function. That is, for any test function $f : \mathbb{R} \mapsto \mathbb{C}$ such that $\sum_\gamma f(\gamma)$ converges,

$$\langle f, \varphi_E \rangle = \int_{-\infty}^{\infty} f(x) \left(\sum_{\gamma \in S_E} \delta(x-\gamma) \right) dx = \sum_{\gamma \in S_E} f(\gamma). \tag{2.0.2}$$

Then as distributions,

$$\varphi_E = \sum_{\gamma} \delta(x-\gamma) = \frac{1}{\pi}\left[-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right) + \sum_{k=1}^{\infty} \frac{x^2}{k(k^2+x^2)} + \frac{1}{2}\sum_{n=1}^{\infty} c_n\left(n^{ix}+n^{-ix}\right)\right]. \tag{2.0.3}$$

where η is the Euler-Mascheroni constant $= 0.5772\ldots$, N_E is the conductor of E, and $c_n(E)$ is the nth Dirichlet coefficient of $\frac{L_E'}{L_E}(1+s)$.

Theorem 5.5.9 (GRH)**.** Let E have conductor N_E, and let $M_E(t)$ count the number of nontrivial zeros of $L_E(s)$ with imaginary part at most t in value. Then for $t \gg 0$ we have

$$M_E(t) = \frac{t}{\pi}\,\log\left(\frac{t\sqrt{N_E}}{2\pi e}\right) + \frac{1}{4} + O(\log t), \tag{2.0.4}$$

where the error term is positive as often as it negative and contributes no net bias asymptotically.

Corollary 5.5.11 (GRH)**.** Let $\gamma_n := \gamma_n(E)$ be the imaginary value of the nth nontrivial (and noncentral) zero in the upper half plane of $L_E(s)$ with analytic rank r_E. Moreover, let $W_0(s)$ be the Lambert W-function on $\mathbb{C}$ i.e. the principal branch of the functional inverse of the function $y = xe^x$. Then for $n \gg 1$ we have

$$\gamma_n = \frac{2\pi e}{\sqrt{N_E}} \cdot \exp\left(W_0\left[\left(\frac{r_E}{2}+n-\frac{3}{4}\right)\cdot\frac{\sqrt{N_E}}{2e}\right]\right) + O(\log n), \tag{2.0.5}$$

where the error term is positive as often as it negative and contributes no net bias asymptotically.

Define the *bite* of E to be $\beta_E = \sum_{\gamma\neq 0}\gamma^{-2}$, where γ ranges of the imaginary parts of the noncentral nontrivial zeros of $L_E(s)$.

Corollary 5.6.11 (GRH)**.** Let $E/\mathbb{Q}$ have analytic rank r_E, conductor N_E and bite β_E. Then r_E is the largest integer less than the quantity

$$\frac{1}{\sqrt{\beta_E}}\left[\left(-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right) + \frac{1}{2\sqrt{\beta_E}}\left(\frac{\pi^2}{6} - \mathrm{Li}_2\left(e^{-2\sqrt{\beta_E}}\right)\right) + \sum_{n<e^{2\sqrt{\beta_E}}} c_n(E)\cdot\left(1-\frac{\log n}{2\sqrt{\beta_E}}\right)\right]. \tag{2.0.6}$$

where η is the Euler-Mascheroni constant $= 0.5772\ldots$, $\mathrm{Li}_2(s)$ is the dilogarithm function on $\mathbb{C}$, and $c_n(E)$ is the nth Dirichlet coefficient of $\frac{L'_E}{L_E}(1+s)$.

Theorem 5.6.12 (GRH)**.** Let E have completed shifted L-function $\Lambda_E(1+s)$, analytic rank r_E and bite β_E. Then

$$r_E = \left\lfloor \frac{1}{\sqrt{\beta_E}} \cdot \frac{\Lambda'_E}{\Lambda_E}\left(1 + \frac{1}{\sqrt{\beta_E}}\right) \right\rfloor. \tag{2.0.7}$$

The next chapter provides definitions and background theory for the quantities mentioned in the results above; the the proofs can of course be found in the respective sections later in this work.

Chapter 3

NOTATION, DEFINITIONS AND BACKGROUND

3.1 Notation

For the rest of the body of this text we set the following notation:

- E is an elliptic curve over $\mathbb{Q}$ given by minimal Weierstrass equation

$$y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

  where $a_1, a_3 \in \{0, 1\}$, $a_2 \in \{-1, 0, 1\}$ and $a_4, a_6 \in \mathbb{Z}$.

- $D(E)$, $N(E)$ and $r_{al}(E)$ and $r_{an}(E)$ are the discriminant, conductor, algebraic rank and analytic rank of E respectively. For ease of exposition, the dependence on E will most often be indicated by a subscript E instead, and when there is no ambiguity it may be dropped entirely. Also, since much of this body of work assumes the validity of the the BSD conjecture, the algebraic and analytic rank of a curve will most often be assumed to be equal, in which case it will just be denoted r_E.

- p is a (rational) prime number and q is a prime power.

- s is the generic complex variable.

- $L(E, s)$ and $\Lambda(E, s)$ are the standard and completed L-functions attached to E respectively. Again, for ease of exposition we will in general subsume the E into a subscript and write $L_E(s)$ and $\Lambda_E(s)$.

- $C(E) = C_E$ is the leading nonzero coefficient of the Taylor series of $\Lambda_E(s)$ about $s = 1$; $C'(E) = C'_E$ is the leading nonzero coefficient of the Taylor series of $L_E(s)$ about $s = 1$.

- γ will always be used to denote the imaginary parts of nontrivial zeros of an L-function.
- $\beta(E) = \beta_E$ is the bite of E, defined as $\beta_E = \sum_{\gamma \neq 0} \gamma^{-2}$, where γ ranges over the noncentral nontrivial zeros of $L_E(s)$.
- η is the Euler-Mascheroni constant $= 0.5772156649\ldots$
- $\Gamma(s)$ is the standard Gamma function on $\mathbb{C}$, and the digamma function: $\digamma(s) = \frac{\Gamma'}{\Gamma}(s)$ is the logarithmic derivative of $\Gamma(s)$.

Furthermore, we define the following values associated to E (in all cases the dependence on E is understood):

- $b_2 = a_1^2 + 4a_2$
- $b_4 = a_1 a_3 + 2a_4$
- $b_6 = a_3^2 + 4a^6$
- $b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$
- $c_4 = b_2^2 - 24 b_4$
- $c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6$
- $D = D(E) = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9 b_2 b_4 b_6$; this is the definition of the discriminant of E
- $j = j(E) = \frac{c_4}{D}$ is the j-invariant of E

3.2 Definitions and Basic Results

The rest of this chapter covers the basic definitions of and results needed for the rest of this work (namely, big-Oh notation, elliptic curves and L-functions). Feel free to skip this if you are familiar with them.

3.2.1 Big-Oh Notation

Given that the running time of various algorithms will be discussed over the course of this work, we recall the definitions of big-Oh and soft-Oh notation, at least in the context of how they will be used here.

Definition 3.2.1. Let x be a positive input, and let $g(x)$ be some positive-valued reference function on x.

- We say a function $f(x) = O(g(x))$ (read "f is big-Oh of g"), if

$$\limsup_{x\to\infty} \left|\frac{f(x)}{g(x)}\right| < \infty. \tag{3.2.1}$$

  That is, $f(x) = O(g(x))$ if the asymptotic growth/decay rate of f is bounded by some multiple of that of g.

- We say a function $f(x) = \tilde{O}(g(x))$ (read "f is soft-Oh of g"), if there is some $m > 0$ such that

$$\limsup_{x\to\infty} \left|\frac{f(x)}{g(x)\left(\log g(x)\right)^m}\right| < \infty. \tag{3.2.2}$$

  That is, $f(x) = \tilde{O}(g(x))$ if the asymptotic growth/decay rate of f scales like that of g, up to the inclusion of log factors.

Note that $f(x) = \tilde{O}(g(x))$ implies that $f(x) = O(g(x)^{1+\epsilon})$ for any $\epsilon > 0$, but not vice versa; there are complexity classes strictly between the two. In this thesis we will work exclusively with soft O time complexities, so there is no need to elaborate on those classes here.

Definition 3.2.2. Let A be an algorithm which takes input of size k, where for simplicity we may think of k as a positive integer. Let $t_A(k)$ be the running time of A thought of as a function of the input size k.

- A is said to have *polynomial time complexity* if there is some $m > 0$ such that the running time of $t_A(k) = O(k^m)$, i.e. the asymptotic running time of the algorithm scales like some polynomial function of k.

- If $t_A(k) = O(k^\epsilon)$ for any $\epsilon > 0$, then A is said to have *sub-polynomial time complexity*. Note that if $t_A(k) = \tilde{O}(1)$, then A has sub-polynomial time complexity.

- If no $m > 0$ exists such that $t_A(k) = O(k^m)$, then A is said to have *super-polynomial time complexity*. If there is some $m > 1$ such that $t_A(k) = O(m^k)$, then A is said to have *exponential time complexity*.

Again, there are complexity classes strictly between polynomial and exponential complexity, but we won't consider them in this thesis. The same terminology can be applied to the space requirements of an algorithm, wherein we would replace the word 'time' with 'space'.

Note that in theoretical computer science the k is typically the number of bits needed to specify the input to the algorithm. However, in computational number theory the input itself is often a positive integer; many algorithms scale with some polynomial of the input magnitude as opposed to the number of bits defining the input. We therefore highlight the distinction between "polynomial time in the number of bits of the input" and "polynomial time in the magnitude of the input": the former is asymptotically much faster than the latter. When discussing time complexities we will always be clear to delineate what the measure of complexity k is.

3.2.2 Elliptic curves

Definition 3.2.3. An elliptic curve E is a genus 1 smooth projective curve with a marked point $\mathcal{O}$. E is defined over a field K if E may be represented by the *Weierstrass equation* $y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6$, where $a1, \dots a_6 \in K$.

For elliptic curves defined over $\mathbb{Q}$, we may always find a model for E such that $a_1, a_3 \in \{0, 1\}$, $a_2 \in \{-1, 0, 1\}$ and $a_4, a_6 \in \mathbb{Z}$. Furthermore, there is the notion of *minimality* when it comes to models for elliptic curves. Without going into the definition thereof, unless stated otherwise we will assume that any given elliptic curve Weierstrass equation is specified by its global minimal model.

Definition 3.2.4. The set of K-rational points on E is denoted $E(K)$. $E(K)$ comprises an abelian group, with the "point at infinity" $\mathcal{O}$ acting as the group identity element.

It is often useful to view an elliptic curve E as the vanishing locus of the polynomial

$$f(x, y) = y^2 + a_1xy + a_3y^2 - x^3 - a_2x^2 - a_4x - a_6. \tag{3.2.3}$$

That is $E(K) = \{(x, y) \in K^2 : \ f(x, y) = 0\}$, along with the point at infinity $\mathcal{O}$.

For a rational elliptic curve $E/\mathbb{Q}$, we may consider the reduced curve $\tilde{E}/\mathbb{F}_p$ for any prime p. If $E/\mathbb{Q}$ is given by the global minimal model $y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6$, then the reduced curve is given by $y^2 + \overline{a_1}xy + \overline{a_3}y^2 = x^3 + \overline{a_2}x^2 + \overline{a_4}x + \overline{a_6}$, where $\overline{a_i}$ is a_i reduced modulo p. For $p = 2$ or 3 we may have to move to a different model for E first to avoid the reduced curve being automatically singular.

Definition 3.2.5. A prime p is called *good* if $\tilde{E}/\mathbb{F}_p$ is non-singular. The reduced curve is an elliptic curve over $\mathbb{F}_p$ (by definition) which we denote by $E/\mathbb{F}_p$; E is said to have *good reduction at p*. Otherwise, p is said to be *bad*, the reduced (singular) curve is denoted $\tilde{E}/\mathbb{F}_p$, and E is said to have *bad reduction at p*.

Theorem 3.2.6. *For any $E/\mathbb{Q}$, the set of bad primes is finite and non-empty.*

Singular reduced curves may be thought of as finite-field analogues of singular cubics over the rationals, for example those given by $y^2 = x^3$ and $y^2 = x^3 + x^2$ as seen below. Singular curves have a (unique) *singular point*, which is by definition where the partial derivatives $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ are both zero (here f is as given by equation 3.2.3).

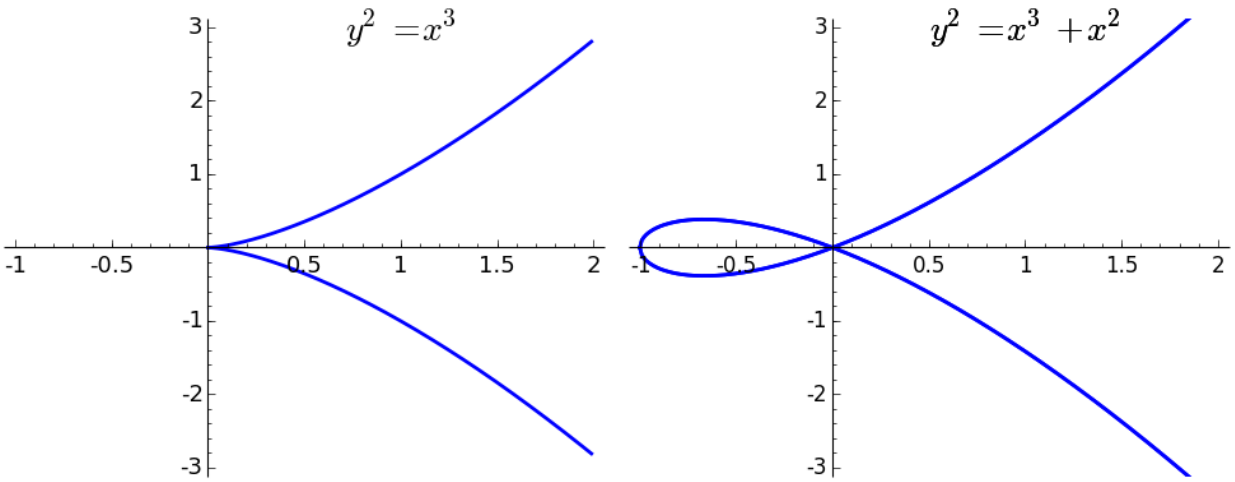

Figure 3.2.1: An example of two singular cubics over the rationals. The singular point for both curves is at the origin; for the the left curve the singular point is a *cusp*, and for the right curve it is a *node*.

In the finite field setting the notion of partial derivatives still makes sense, so one may define singular points accordingly. Bad reduction at a prime may be classified into one of three types according to the nature of the tangent space at the singular point on $\tilde{E}/\mathbb{F}_p$.

Definition 3.2.7. Let E have bad reduction at p; let P be the singular point on $\tilde{E}/\mathbb{F}_p$, and let $T_P(E)$ be the tangent space at P.

- If the $T_P(E)$ is one-dimensional, then P is a cusp, and E is said to have *additive reduction* at p.

- Otherwise $T_P(E)$ is two-dimensional, and P is then a node; E is then said to have

multiplicative reduction at p. Furthermore, multiplicative reduction can be decomposed into two cases:

- If $T_P(E)$ is defined over $\mathbb{F}_p$, then E is said to have *split multiplicative reduction* at p
- Otherwise $T_P(E)$ is defined over a quadratic extension of $\mathbb{F}_p$, and E is said to have *non-split multiplicative reduction* at p.

Primes of bad reduction are packaged together into an invariant called the *conductor* of E:

Definition 3.2.8. The conductor of E, denoted by N_E, is a positive integer given by

$$N_E = \prod_p p^{f_p(E)}, \tag{3.2.4}$$

where p ranges over all primes, and for $p \neq 2$ or 3,

$$f_p(E) = \begin{cases} 0, & E \text{ has good reduction at } p \\ 1, & E \text{ has multiplicative reduction at } p \\ 2, & E \text{ has additive reduction at } p. \end{cases} \tag{3.2.5}$$

For $p = 2$ and 3, the exponent $f_p(E)$ is still zero if p is good; however the exponent may be as large as 8 and 5 respectively if p is bad.

The "proper" definition of the conductor is Galois representation-theoretic and is defined in terms of the representation of the inertia group at p on the torsion subgroup of E; for $p \neq 2$ or 3 this reduces to the definition given above, but for 2 and 3 there may be nontrivial wild ramification which increases the exponent up to the stated amounts. A full technical definition of the conductor is given in [32, pp. 379-396]. In any case (including 2 and 3), the exponent $f_p(E)$ may be computed efficiently by Tate's algorithm, as detailed in the previous section of the same book [32, pp. 361-379].

3.2.3 Elliptic curve L-functions

We now move on to the definition of the L-function attached to an elliptic curve. For this we must define the numbers $a_p(E)$:

Definition 3.2.9.

- For good primes p (i.e. when $p \nmid N_E$), let

$$a_p(E) = p + 1 - \#\left\{E(\mathbb{F}_p)\right\}, \tag{3.2.6}$$

  where $\#\left\{E(\mathbb{F}_p)\right\}$ is the number of points on $E/\mathbb{F}_p$;

- For bad primes (when $p \mid N_E$), let

$$a_p(E) := \begin{cases} +1 & \text{if } E \text{ has split multiplicative reduction at } p \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p \\ 0 & \text{if } E \text{ has additive reduction at } p. \end{cases} \tag{3.2.7}$$

Hasse's theorem states that the number of points on E modulo p can never be too far from $p + 1$:

Theorem 3.2.10 (Hasse, 1936)**.** *For all elliptic curves $E/\mathbb{Q}$ and all primes p,*

$$|a_p(E)| \leq 2\sqrt{p}. \tag{3.2.8}$$

For ease of notation, when E is fixed we will let $a_p := a_p(E)$, letting the dependence on E be understood.

The Sato-Tate Conjecture, now a theorem thanks to Taylor, goes even further, giving an asymptotic distribution on the a_p:

Theorem 3.2.11 (Taylor, 2006-)**.** *For fixed $E/\mathbb{Q}$, the set of normalized a_p values $\left\{\frac{a_p}{2\sqrt{p}} : p \text{ prime}\right\}$ obey a semicircular distribution on the interval $[-1, 1]$. That is, for $1 \leq a \leq b \leq 1$, the*

asymptotic proportion of primes for which $a \leq \frac{a_p}{2\sqrt{p}} \leq b$ *is equal to the proportion of the area under the unit semicircle between* a *and* b.

Definition 3.2.12.

The L-function attached to E is a complex analytic function $L_E(s)$, defined initially on some right half-plane of the complex plane.

- The Euler product of the L-function attached to E is given by

$$L(E,s) = \prod_p \frac{1}{1 - a_p p^{-s} + \epsilon(p) p^{1-2s}}, \tag{3.2.9}$$

  where $\epsilon(p) = 0$ for bad p, and 1 for good p.

- The Dirichlet series for $L_E(s)$ is given by

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}. \tag{3.2.10}$$

  where for composite n, a_n is defined to be the integer coefficient of n^{-s} obtained by multiplying out the Euler product for $L(E,s)$.

Again, we will often write $L_E(s)$ or just $L(s)$ to simplify notation.

Corollary 3.2.13.

- *Hasse's Theorem implies that the Euler product and Dirichlet series for* $L_E(s)$ *converge absolutely for* $\mathrm{Re}(s) > \frac{3}{2}$.

- *Sato-Tate implies that the Euler product and Dirichlet series for* $L_E(s)$ *converge conditionally for* $\mathrm{Re}(s) > \frac{1}{2}$.

In this work we more often use the completed L-function attached to E:

Definition 3.2.14. The *completed L-function* attached to E is given by

$$\Lambda_E(s) = (N_E)^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L_E(s), \tag{3.2.11}$$

where N_E is the conductor of E and $\Gamma(s)$ the usual Gamma function on $\mathbb{C}$.

Thanks to the modularity theorem, we may in fact analytically continue $L_E(s)$ and $\Lambda_E(s)$ to be entire functions defined on all of $\mathbb{C}$.

Theorem 3.2.15 (Breuille, Conrad, Diamond, Taylor, Wiles et al., 1995,1999,2001)**.** *There exists an integral newform $f = \sum_n a_n q^n$ of of weight $k = 2$ and level N_E such that $L_E(s) = L_f(s)$.*

The modularity theorem above is essentially the converse of the theorem by Shimura in the 1960s: if f is a weight 2 newform of level N_E with rational Fourier coefficients, then there exists some elliptic curve $E/\mathbb{Q}$ of conductor N_E such that $L_f(s) = L_E(s)$. Hence any theorem about elliptic curve L-functions is thus really a theorem about L-functions of weight 2 newforms in disguise.

Corollary 3.2.16.

- $\Lambda_E(s)$ *extends to an entire function on* $\mathbb{C}$*. Specifically,* $\Lambda_E(s)$ *obeys the functional equation*

  $$\Lambda_E(s) = w_E\Lambda_E(2-s), \tag{3.2.12}$$

  where $w_E \in \{-1, 1\}$ *is the action of the Atkin-Lehner involution on the newform attached to* E*.*

- $L_E(s)$ *extends to an entire function on* $\mathbb{C}$ *via the definition of* $\Lambda_E(s)$ *and the functional equation above.*

We reproduce the analytic continuation for $\Lambda_E(s)$ explicitly below. Define the auxiliary function $\lambda_E(s)$ by

$$\lambda_E(s) = \left(\frac{\sqrt{N_E}}{2\pi}\right)^s \sum_{n=1}^{\infty} a_n n^{-s} \Gamma\left(s, \frac{2\pi n}{\sqrt{N_E}}\right), \tag{3.2.13}$$

where all the quantities are as defined previously, and $\Gamma(s,x)$ is the upper incomplete Gamma function on $\mathbb{C} \times \mathbb{R}_{>0}$. The sum converges absolutely for any s, so $\lambda_E(s)$ is entire. Then

$$\Lambda_E(s) = \lambda_E(s) + w_E \lambda_E(2-s). \tag{3.2.14}$$

Knapp goes through the proof of this formula in [21, pp. 270-271].

Definition 3.2.17. E is said to have *even parity* if $w_E = 1$, and *odd parity* if $w_E = -1$.

The functional equation for $\Lambda_E(s)$ shows that it is either symmetric or antisymmetric about the line $\mathrm{Re}(s) = 1$; moreover, since all the constituent parts for $\Lambda_E(s)$ are defined over the reals, $\Lambda_E(s)$ is also conjugate symmetric about the real axis. It follows that $\Lambda_E(s)$ is highly symmetric about the point $s = 1$. This is formalized in the following statement:

Proposition 3.2.18. *As a function of s, $\Lambda_E(1+s)$ is even if E has even parity, and odd if E has odd parity.*

This follows immediately from the functional equation.

Definition 3.2.19. For elliptic curve L-functions:

- The point $s = 1$ is called the *central point* or the *critical point*.
- The vertical line of symmetry $\mathrm{Re}(s) = 1$ is called the *critical line*.
- The vertical strip $0 \leq \mathrm{Re}(s) \leq 2$ is call the *critical strip*.

There is an oft-quoted anecdote that the way to differentiate analytic number theorists from algebraic number theorists is that for elliptic curve L-functions the former normalize so that the critical line lies at $\mathrm{Re}(s) = \frac{1}{2}$ (as is the case with $\zeta(s)$), while the latter keep the critical line at $\mathrm{Re}(s) = 1$. In this thesis we work mostly with $L_E(1+s)$ and $\Lambda_E(1+s)$ which shifts the critical line to the imaginary axis; a move which is bound to antagonize both parties equally!

A standard result with L-functions of Hecke eigenforms (of elliptic curve L-functions are a subset) is that "all the interesting stuff happens inside the critical strip":

Proposition 3.2.20. *For any $E/\mathbb{Q}$,*

$$\Lambda_E(1+s) \neq 0 \ \ \textit{when} \ \ |\mathrm{Re}(s)| > \frac{1}{2}. \tag{3.2.15}$$

This can be proven by showing that the logarithmic derivative of $\Lambda_E(1+s)$ converges absolutely for $\mathrm{Re}(s) > \frac{1}{2}$; see the corollary to Proposition 5.1.7 for a proof. The statement can with a bit more work be strengthened to asserting that all zeros are *strictly* inside the critical strip). In fact, the Generalized Riemann Hypothesis asserts that

$$\Lambda_E(1+s) \neq 0 \ \text{ when } \ \mathrm{Re}(s) \neq 0. \tag{3.2.16}$$

From the functional equation we get that $L_E(s)$ has simple zeros at the nonpositive integers; these are denoted the *trivial* zeros of $L_E(s)$. Zeros inside the critical strip are called *nontrivial*. The Generalized Riemann Hypothesis (formally stated in Section 3.3) asserts that all nontrivial zeros of $L_E(s)$ lie on the critical line $\mathrm{Re}(s) = 1$.

If $L_E(s)$ has a zero at the central point, it may or may not have multiplicity greater than 1.

Definition 3.2.21. Let E be an elliptic curve over $\mathbb{Q}$ and let $L_E(s)$ be its L-series. The *analytic rank* of E, denoted $r_{an}(E)$ or just r_{an} is the order of vanishing of $L_E(s)$ at the central point $s = 1$. That is, if the Taylor series of $L_E(s)$ about $s = 1$ is

$$L_E(1+s) = a_0 + a_1 s + a_2 s^2 + \cdots, \tag{3.2.17}$$

then $a_n = 0$ for $0 \leq n < r_{an}$ and $a_{r_{an}} \neq 0$.

We will work a lot with the leading coefficient of the L-seres at the central point, so it's worth giving it a name. To this end:

Definition 3.2.22.

- Let C'_E (or just C' when E is fixed) be the leading coefficient of $L_E(s)$ at the central point (the constant $a_{r_{an}}$ in the definition above).

- Let C_E (or just C when E is fixed) be the leading coefficient of $\Lambda_E(s)$ at the central point.

Observe that $C'_E = \frac{2\pi}{\sqrt{N_E}} \cdot C_E$. We will most often work with the latter, hence the notation.

We may use Equation 3.2.13 to produce formulae for the value of $\Lambda_E(s)$ and its higher derivatives at the central point:

Proposition 3.2.23.

1.

$$\Lambda_E(1) = \begin{cases} \frac{\sqrt{N_E}}{\pi} \sum_{n=1}^{\infty} \frac{a_n}{n} e^{-\frac{2\pi}{\sqrt{N_E}} \cdot n}, & w_E = 1 \\ 0, & w_E = -1 \end{cases}. \tag{3.2.18}$$

2. When m has the same parity as E, the mth derivative of $\Lambda_E(s)$ at the central point is given by

$$\Lambda_E^{(m)}(1) = 2 \sum_{n=1}^{\infty} a_n \int_1^{\infty} \left(\log \frac{t}{\sqrt{N_E}} \right)^m e^{-\frac{2\pi n}{\sqrt{N_E}} \cdot t} \, dt. \tag{3.2.19}$$

When m is opposite in parity to E, then $\Lambda_E^{(m)}(1) = 0$.

Proof. Observe that the series in equation 3.2.13 converges uniformly over the interval of integration; we may therefore swap the integral and summation signs. After a change of

variables we get

$$\lambda_E(1+s) = N_E^{\frac{1+s}{2}} \int_{\frac{1}{\sqrt{N_E}}}^{\infty} x^s f_E(it)\, dt = N_E^{\frac{1+s}{2}} \sum_{n=1}^{\infty} a_n \int_{\frac{1}{\sqrt{N_E}}}^{\infty} t^s e^{-2\pi nt}\, dt,$$

where f_E is the cusp form attached to E. Both $t^s e^{-2\pi nt}$ and its derivative w.r.t. s are continuous over the integration interval for any n, so by the Leibniz integration rule we may differentiate under the integral sign and evaluate at $s = 1$ to get

$$\lambda_E^{(m)}(1) = \sqrt{N_E} \cdot \sum_{n=1}^{\infty} a_n \int_{\frac{1}{\sqrt{N_E}}}^{\infty} (\log t)^m e^{-2\pi nt}\, dt. \tag{3.2.20}$$

Equation 3.2.19 follows by substituting $t \mapsto \sqrt{N_E} \cdot t$. For $m = 0$ the integrals may be evaluated directly: $\int_1^{\infty} e^{-\frac{2\pi nt}{\sqrt{N_E}}}\, dt = \frac{\sqrt{N_E}}{2\pi n} e^{-\frac{2\pi n}{\sqrt{N_E}}}$. □

Equation 3.2.19 allows us to establish bounds on the coefficients of the Taylor expansion of $\Lambda_E(s)$ about the central point. For this we will need the following technical lemma:

Lemma 3.2.24. *Let $N_E, n \in \mathbb{Z}_{>0}$, and suppose m is a positive integer such that $m < \frac{1}{2}\log N_E$. Then*

$$\left| \int_{\frac{1}{\sqrt{N_E}}}^{\infty} (\log t)^m e^{-2\pi nt}\, dt \right| < \frac{\left(\frac{1}{2}\log N_E\right)^m}{2\pi n} \left[e^{-\frac{2\pi n}{\sqrt{N_E}}} + \frac{e^{-2\pi n\sqrt{N_E}}}{2\pi n\sqrt{N_E}} \right]. \tag{3.2.21}$$

Proof. We split the integral in two, dealing with the intervals $\frac{1}{\sqrt{N_E}}$ to $\sqrt{N_E}$ and $\sqrt{N_E}$ to ∞ separately. Now $(\log t)^m$ is at most $(\frac{1}{2}\log N_E)^m$ in magnitude on $[\frac{1}{\sqrt{N_E}}, \sqrt{N_E}]$, so

$$\left| \int_{\frac{1}{\sqrt{N_E}}}^{\sqrt{N_E}} (\log t)^m e^{-2\pi nt}\, dt \right| < \left(\frac{1}{2}\log N_E\right)^m \int_{\frac{1}{\sqrt{N_E}}}^{\sqrt{N_E}} e^{-2\pi nt}\, dt < \frac{\left(\frac{1}{2}\log N_E\right)^m}{2\pi n} \left(e^{-\frac{2\pi n}{\sqrt{N_E}}} - e^{-2\pi n\sqrt{N_E}} \right).$$

For the integral on $[\sqrt{N_E}, \infty)$, we use integration by parts to get

$$\int_{\sqrt{N_E}}^{\infty} (\log t)^m\, e^{-2\pi nt}\, dt = \frac{\left(\frac{1}{2}\log N_E\right)^m}{2\pi n} \cdot e^{-2\pi n\sqrt{N_E}} + \frac{m}{2\pi n} \int_{\sqrt{N_E}}^{\infty} \frac{(\log t)^{m-1}}{t} e^{-2\pi nt}\, dt.$$

If $m < \frac{1}{2}\log N_E$, then $\frac{(\log t)^{m-1}}{t}$ is decreasing for $t > \sqrt{N_E}$, so we have

$$\frac{m}{2\pi n} \int_{\sqrt{N_E}}^{\infty} \frac{(\log t)^{m-1}}{t} e^{-2\pi nt}\, dt < \frac{m\left(\frac{1}{2}\log N_E\right)^{m-1}}{2\pi n\sqrt{N_E}} \int_{\sqrt{N_E}}^{\infty} e^{-2\pi nt}\, dt < \frac{\left(\frac{1}{2}\log N_E\right)^m}{(2\pi n)^2\sqrt{N_E}} \cdot e^{-2\pi n\sqrt{N_E}}.$$

Add up all the values and you get the established result. □

With the above lemma in hand, we establish an upper bound on the magnitude of the mth Taylor coefficient of $\Lambda_E(s)$ at the central point.

Proposition 3.2.25. *Let E have conductor N_E and completed L-function $\Lambda_E(s)$. Then so long as $m < \frac{1}{2}\log N_E$, the mth derivative of $\Lambda_E(s)$ at the central point is bounded explicitly in terms of N_E and m by*

$$\left|\Lambda_E^{(m)}(1)\right| < \frac{(\frac{1}{2}\log N_E)^m}{2\pi^2}\left(N_E + \frac{1}{e^{2\pi\sqrt{N_E}}-1}\right). \tag{3.2.22}$$

That is, for fixed m the mth Taylor coefficient of $\Lambda_E(s)$ is $O\left(N_E(\frac{1}{2}\log N_E)^m\right)$; the second term inside the final parentheses is negligible for $N_E \gg 1$.

Proof. From Lemma 3.2.24 and Equation 3.2.20 we have that

$$\left|\Lambda_E^{(m)}(1)\right| < 2\sqrt{N_E}\sum_{n=1}^{\infty}|a_n|\cdot\left[\frac{\left(\frac{1}{2}\log N_E\right)^m}{2\pi n}\left(e^{-\frac{2\pi n}{\sqrt{N_E}}} + \frac{e^{-2\pi n\sqrt{N_E}}}{2\pi n\sqrt{N}_E}\right)\right].$$

Using the bound $|a_n(E)| \leq n$ for any E, we get

$$\left|\Lambda_E^{(m)}(1)\right| < \frac{\sqrt{N_E}\left(\frac{1}{2}\log N_E\right)^m}{\pi}\sum_{n=1}^{\infty}e^{-\frac{2\pi n}{\sqrt{N_E}}} + \frac{\left(\frac{1}{2}\log N_E\right)^m}{2\pi^2}\sum_{n=1}^{\infty}\frac{e^{-2\pi n\sqrt{N_E}}}{n}.$$

Now

$$\sum_{n=1}^{\infty}e^{-\frac{2\pi n}{\sqrt{N_E}}} = \frac{1}{e^{\frac{2\pi n}{\sqrt{N_E}}}-1} < \frac{\sqrt{N_E}}{2\pi},$$

while $\sum_{n=1}^{\infty}\frac{e^{-2\pi n\sqrt{N_E}}}{n} \leq \sum_{n=1}^{\infty}e^{-2\pi n\sqrt{N_E}} = \frac{1}{e^{2\pi\sqrt{N_E}}-1}$. □

Note that for fixed N_E, if we allow $m \to \infty$, we actually have that the mth derivative can grow like $O\left(\frac{m!!}{(2\pi e)^{m/2}}\right)$, where $m!! = m(m-2)\cdots$ is the double factorial on m i.e. faster than exponentially in m. However, this behavior only starts to show when $m \gg \log N_E$ – hence our restriction on the magnitude of m. This will in practice never be an issue: we are primarily interested in the central derivatives in order to establish results about the analytic rank of E. Since maximum analytic rank grows more slowly than $\log N_E$ (c.f. Corollary 5.1.12), we will never need to consider $\Lambda_E^{(m)}(1)$ for $m > \frac{1}{2}\log N_E$.

Crucial to this thesis, $L_E(s)$ and its derivatives can be provably computed to a given precision in time that scales with the square root of the conductor of E:

Proposition 3.2.26. *When $m < \frac{1}{2}\log N_E$, the mth derivative of $L_E(s)$ at the central point can be provably computed to k bits precision in $\tilde{O}(k \cdot \sqrt{N_E})$ time, where N_E is the conductor of E.*

This is proven in full in the PhD thesis of Robert Bradshaw [7]. The basic argument is as follows:

1. Since the two differ by an exponential and a Gamma factor, computing $L_E^{(m)}(1)$ takes the same order of magnitude time as computing $\Lambda_E^{(m)}(1)$. This may be achieved, for example, by the formula given in Equation 3.2.19;

2. The integral $\int_1^\infty \left(\log \frac{t}{\sqrt{N_E}}\right)^m e^{-\frac{2\pi n}{\sqrt{N_E}}\cdot t}\, dx$ can be computed to k bits precision in time that scales proportional to k, is independant of n and subpolynomial in N_E;

3. The number of terms needed in the sum to achieve k bits precision is $O\left(\log(N_E)^m\sqrt{N_E}\right)$;

4. Computing a_n can be done in time polynomial in $\log n$;

5. Combining the above, computation time is dominated by evaluating $O(\log(N_E)^m\sqrt{N_E})$ integrals and a_n values. That is, the sum can be evaluated to k bits precision in time scaling with $k\sqrt{N_E}$ times some power of $\log N_E$.

We will use the result of Proposition 3.2.26 directly in the proof of Theorem 2.0.5. In fact, the $\tilde{O}(\sqrt{N_E})$ time needed to evaluate central derivatives of $L_E(s)$ is the computational bottleneck in algorithm 2.0.6; all other steps scale in time subpolynomial in N_E.

3.3 The Three Big Conjectures

The main results in this thesis are contingent on the Birch and Swinnerton-Dyer conjecture, The Generalized Riemann Hypothesis and the ABC conjecture. We reproduce the three conjectures in full below; citations for the papers in which they first appeared or are fully formulated are listed at the top of each conjecture.

The Birch and Swinnerton-Dyer conjecture (BSD) is needed to establish a way to compute and hence bound the magnitude of the leading coefficient of $L_E(s)$ at the central point.

Conjecture 3.3.1 (Birch, Swinnerton-Dyer)**.** *[5]*

1. *$r_{an} = r$; that is, the analytic rank of E is equal to its algebraic rank.*

2. *The leading coefficient at the central point in $L_E(s)$ is given by*

$$C'_E = \left(\frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#Ш(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{Tor}(\mathbb{Q}))^2} \right), \tag{3.3.1}$$

   where

   - *r is the algebraic rank of $E(\mathbb{Q})$,*
   - *Ω_E is the real period of (an optimal model of) E,*
   - *Reg_E is the regulator of E,*
   - *$\#Ш(E/\mathbb{Q})$ is the order of the Shafarevich-Tate group attached to $E/\mathbb{Q}$,*
   - *$\prod_p c_p$ is the product of the Tamagawa numbers of E, and*
   - *$\#E_{Tor}(\mathbb{Q})$ is the number of rational torsion points on E.*

For an excellent description of the conjecture and a breakdown of the arithmetic invariants mentioned above, see Andrew Wiles' official description of the BSD Conjecture on the Clay Math website [37].

The Generalized Riemann Hypothesis (GRH), as the name suggests, generalizes the famous conjecture first posed by Bernhard Riemann in 1859 [30]. The (standard) Riemann Hypothesis asserts that all nontrivial zeros of the Riemann zeta function $\zeta(s)$ occur on the vertical line $\mathrm{Re}(s) = \frac{1}{2}$. It is hard to track down where the Generalized Riemann Hypothesis was first formulated in its full generality (Conrey gives a good exposition in [10]), but it asserts that for a large class of suitably defined L-functions, the nontrivial nonreal zeros will occur on a single vertical line in the complex plane (where the exact lateral placement of said line depends on the class of L-function being considered). We use GRH as it applies to elliptic curve L-functions:

Conjecture 3.3.2 (Generalized Riemann Hypothesis for Elliptic Curves, version 1)**.** *[30] [10] Let E be an elliptic curve over $\mathbb{Q}$, and let $L_E(s)$ be its L-series. If ρ is a nontrivial zero of $L_E(s)$ with nonzero imaginary part, then* $\mathrm{Re}(\rho) = 1$.

That is, $L_E(s)$ is never zero outside of the *critical line* $\mathrm{Re}(s) = 1$ and the nonpositive integers. There are numerous equivalent formulations of GRH; we will most often use the following pertaining to the shifted completed L-function:

Conjecture 3.3.3 (Generalized Riemann Hypothesis for Elliptic Curves, version 2)**.** *[30] [10] Let E be an elliptic curve over $\mathbb{Q}$, and let $\Lambda_E(s)$ be the completed L-function attached to E. Then*

1. $\Lambda_E(1+s) = 0 \Longrightarrow \mathrm{Re}(s) = 0$.

Finally, we will need strong form of the ABC conjecture of Masser and Oesterlé in order to establish lower bounds on the regulator and real period of E.

Conjecture 3.3.4 (Masser-Oesterlé)**.** *[26] [29]*
Let (a, b, c) be a triple of coprime positive integers such that $a + b = c$, and let $\mathrm{rad}(abc) = \prod_{p|abc} p$ *be the product of all primes dividing a, b and c. Then for any $\epsilon > 0$ there is a constant K_ϵ such that*

$$c < K_\epsilon \,\mathrm{rad}(abc)^{1+\epsilon}. \tag{3.3.2}$$

The ABC conjecture is famous for the large number of other results that it implies. Of these, we will need two that relate to elliptic curves. It is a relatively straightforward exercise to show that the conductor of an elliptic curve divides its minimal discriminant. Szpiro's conjecture, formulated in the 1980s, asserts that the latter cannot be too big in terms of the former:

Conjecture 3.3.5 (Szpiro)**.** *[34]*
Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E and minimal discriminant D_E. Then for any $\epsilon > 0$ there is a constant K_ϵ such that

$$|D_E| < K_\epsilon \cdot (N_E)^{6+\epsilon}. \tag{3.3.3}$$

We will also invoke a equivalent version of the above conjecture:

Conjecture 3.3.6 (Modified Szpiro)**.** *Let c_4 and c_6 be the c-invariants of a minimal model of $E/\mathbb{Q}$, as defined in Section 3.1. Then for any $\epsilon > 0$ there is a constant K_ϵ independent of E such that*

$$\max\left\{|c_4|^3, |c_6|^2\right\} \leq K_\epsilon \cdot (N_E)^{6+\epsilon}. \tag{3.3.4}$$

Lang's conjecture posits that the height of a point on a rational curve cannot be too small in terms of the discriminant:

Conjecture 3.3.7 (Lang)**.** *[24, pp. 73-74]*
There is a positive constant M_0 such that for any elliptic curve $E/\mathbb{Q}$ with minimal discriminant D_E, the Néron-Tate canonical height of any nontorsion point $P \in E(\mathbb{Q})$ obeys

$$\hat{h}(P) \geq M_0 \log |D_E|. \tag{3.3.5}$$

Chapter 4

AN ALGORITHM TO COMPUTE RANK

4.1 Proof of the Main Theorem

In this section we prove Theorem 2.0.5: specifically, that Algorithm 2.0.6 is guaranteed, assuming BSD and ABC and optionally GRH, to correctly output an elliptic curve's rank in time $\tilde{O}(\sqrt{N_E})$, where N_E is the conductor of the input curve. Note that the proof will quote certain results established later in this work.

The following precision theorem establishes how many bits precision are needed to provably determine if a given L-function Taylor coefficient is zero or not:

Theorem 4.1.1 (BSD, ABC, (GRH))**.** *Let E have L-function $L_E(s)$, conductor N_E and real period Ω_E, and let*

$$k = \lceil 34 + 3.86 \log_2 N_E + \log_2(\Gamma(1.8 + 1.25 \log_2 N_E)) - \log_2 \Omega_E \rceil . \tag{4.1.1}$$

Assuming BSD and ABC, we have the following:

1. *$k = O((\log N_E)^{1+\epsilon})$ for any $\epsilon > 0$.*
2. *If $L_E^{(m)}(1) = 0$ for all $0 \leq m < n$ and $\frac{L_E^{(n)}(1)}{n!}$ is zero to k bits precision, then $L_E^{(n)}(1)$ is identically zero.*

If one further assumes GRH, we may instead let

$$k = \lceil 22 + 2.47 \log_2 N_E + \log_2(\Gamma(1.25 + 0.87 \log_2 N_E)) - \log_2 \Omega_E \rceil \tag{4.1.2}$$

for the same results to hold.

Proof. The first statement follows from Theorem 4.2.11, which states that Ω_E is bounded away from zero by a negative power of N_E. Also note that $\Gamma(s) = O(e^{s \log s})$, so $\log_2(\Gamma(1.8 + 1.25 \log_2 N_E)) = O(\log N_E \log\log N_E)$, from which the result follows.

To prove the second statement, observe that by BSD the leading non-zero Taylor coefficient of $L_E(s)$ at the central point is given by Equation 3.3.1. We thus have that

$$C'_E \geq \frac{1}{256} \cdot \mathrm{Reg}_E \cdot \Omega_E, \tag{4.1.3}$$

since $\prod_p c_p \geq 1$, $\#Ш_E \geq 1$, and by Mazur's Theorem $\#E_{\mathrm{Tor}} \leq 16$. Thus

$$\log_2 C'_E \geq -16 + \log_2 \mathrm{Reg}_E + \log_2 \Omega_E. \tag{4.1.4}$$

Now by Theorem 4.3.8 we have that $\mathrm{Reg}_E \geq 4.36 \times 10^{-6} \cdot (N_E)^{-3.86} \cdot \Gamma(1.8 + 0.25 \log N_E)^{-1}$. Thus $\log_2 \mathrm{Reg}_E \geq -17.81 - 3.86 \log_2 N_E - \log_2(\Gamma(1.8 + 1.25 \log_2 N_E))$, where we have changed the log inside the Gamma factor to base to for consistency with the rest of the logs). We therefore have that

$$\log_2 C'_E \geq -33.81 - 3.86 \log_2 N_E - \log_2(\Gamma(1.8 + 1.25 \log_2 N_E)) + \log_2 \Omega_E > -k, \tag{4.1.5}$$

where k is as defined above. Hence if the nth taylor coefficient of $L_E(s)$ at the central point is zero to k bits precision and all preceding Taylor coefficients are zero, then it *cannot* be the leading BSD coefficient, and so must be identically zero.

If we assume GRH, we instead have $\mathrm{Reg}_E \geq 2.11 \times 10^{-2} \cdot (N_E)^{-2.47} \cdot \Gamma(1.25 + 0.16 \log N_E)^{-1}$. Repeat as before to obtain the required precision stated in Equation 4.1.2. □

In other words, when k is defined as above, the leading Taylor coefficient of $L_E(s)$ at $s = 1$ must be greater than 2^{-k} in magnitude. Note that the -16 appearing in the right hand side of the above inequalities comes from bounding the order of the torsion group of E; this constant can therefore be reduced or eliminated by computing the torsion order of E explicitly, which is quick to do. This is something that therefore should be done in any

optimized implementation of Algorithm 2.0.6.

We now prove **Theorem 2.0.5**: that, assuming BSD and ABC and optionally GRH, Algorithm 2.0.6 computes the rank of an elliptic curve in $\tilde{O}\left(\sqrt{N_E}\right)$ time.

Proof. Let k be as defined according to either Equation 4.1.1 or 4.1.2 depending on whether GRH is assumed or not. That the algorithm terminates with correct output is a direct corollary from Proposition 4.1.1: if $\frac{L_E^{(r)}}{r!}$ is computed to k bits precision and some of those bits are nonzero *and* all preceding Taylor coefficients have been shown to be zero, then r must be the rank of E; hence the output of rank$= r$ is correct.

In terms of time complexity, observe that k is $\tilde{O}(\log N_E)$ in magnitude, and by Corollary 4.2.9, can be computed in time $O((\log N_E)^m)$ for some m. By Corollary 5.3.4, we need to evaluate at most $\frac{1}{2}\log N_E + 1.6$ central Taylor coefficients of $L_E(s)$ to k bits precision; Proposition 3.2.26 states that each of these can be done in $\tilde{O}\left(k \cdot \sqrt{N_E}\right)$ time. Hence the algorithm is guaranteed to terminate in time at most

$$O((\log N_E)^m) + \left(\frac{1}{2}\log N_E + 1.6\right) \cdot \tilde{O}\left(k \cdot \sqrt{N_E}\right) = \tilde{O}\left(\sqrt{N_E}\right), \tag{4.1.6}$$

since k is sub-polynomial in N_E. The $\frac{1}{2}\log N_E + 1.6$ in the above statements may be replaced with $0.32 \log N_E + 0.5$ if GRH is assumed, but resulting time complexity remains $\tilde{O}\left(\sqrt{N_E}\right)$. □

For evidence supporting the validity of Theorem 2.0.5, I wrote a naïve implementation of Algorithm 2.0.6 in Sage and collected timings on SageMathCloud of the algorithm's runtime. 100 curves were drawn from the Cremona database according to a log-uniform distribution on their conductors; a log/log scatter plot of timings vs. conductors can be seen in Figure 4.1.1 (the algorithm produced the correct output in all cases).

The red line in the figure is the best fit straight line, which has slope 0.503; the predicted slope of 0.5 is well within the sample error of 0.016. This is therefore good computational

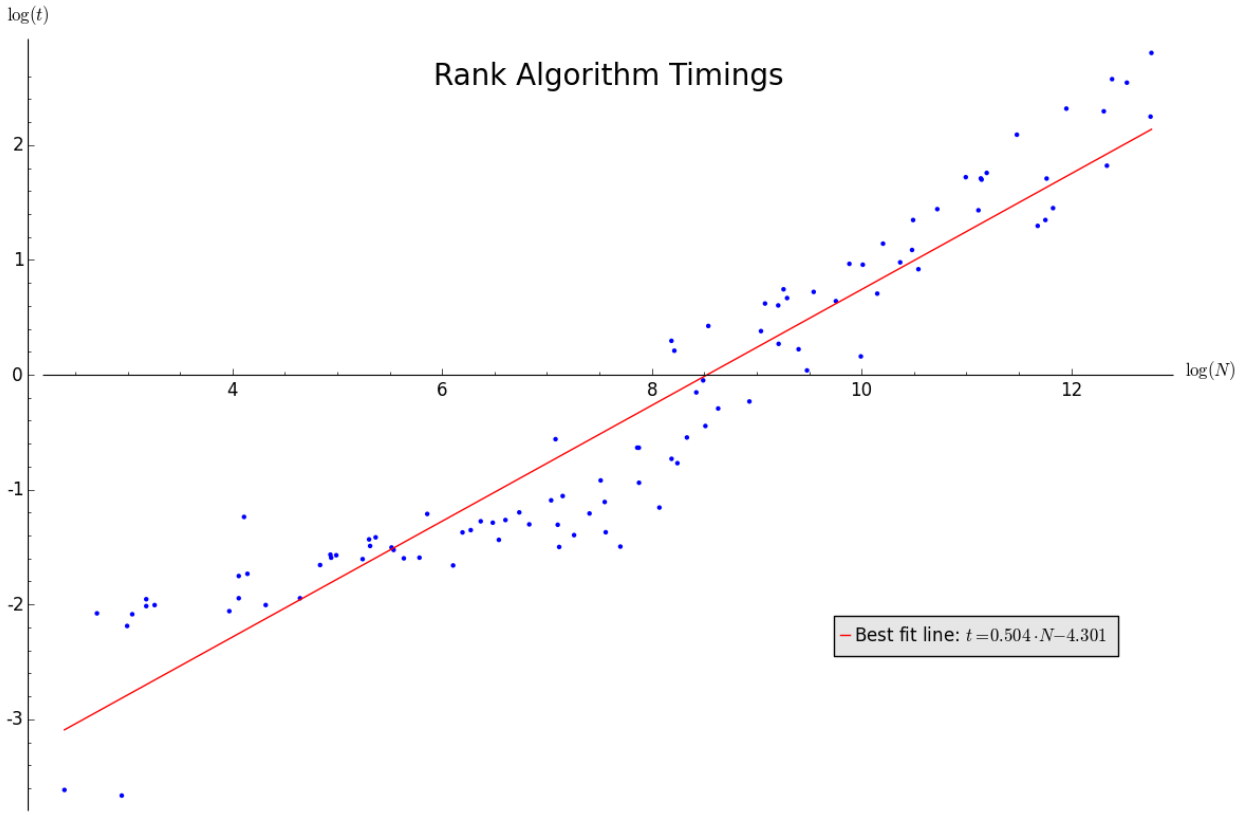

Figure 4.1.1: A scatter plot of the time in seconds taken to compute the rank of an elliptic curve using a Sage implementation of Algorithm 2.0.6 (without assuming GRH) vs. conductor, plotted on a log/log scale, for 100 curves drawn randomly from the Cremona database.

evidence that the runtime of the rank algorithm does indeed scale with $\sqrt{N_E}$.

Using this best fit line, we can make predictions as to how long the algorithm will take to run on curves of larger conductor. For example, the curve of largest known rank is a rank 28 curve found by Elkies (as discussed in [6]); it has conductor $\log N_E \sim 325.9$. For this curve we estimate Algorithm 2.0.6 to take roughly 1.1×10^{62} years, which is about 8×10^{51} times the age of the universe.

Clearly then, the $\tilde{O}(\sqrt{N_E})$ time complexity of Algorithm 2.0.6 limits its usefulness when it comes to curves of large rank. For a method that can be used on such curves, see Chapter 5.

4.2 The Real Period

The real period of a rational elliptic curve E is a measure of the "size" of the set of *real* points on E.

Recall that $E(\mathbb{C})$, the group of complex points on E, is isomorphic via the (inverse of the) Weierstrass $\wp$-function to $\mathbb{C}$ modulo a lattice under addition; that is, $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, and $\omega_1, \omega_2 \in \mathbb{C}$. If E is defined over the real numbers (as rational elliptic curves are), then we may always write ω_1 as being positive real. The second generator ω_2 can be written as being positive imaginary when E has positive discriminant, or in the upper half plane with real part $\frac{\omega_1}{2}$ when E has negative discriminant. [Note: some texts normalize ω_2 to have imaginary part equal to $-\frac{\omega_1}{2}$ when $D_E < 0$, as this sometimes makes the presentation more natural. However, for the work below we will always assume that $\mathrm{Re}(\frac{\omega_2}{\omega_1}) = 0$ or $\frac{1}{2}$.] See [31, Ch. VI] and [32, Ch. I] for a more detailed exposition of the complex theory of elliptic curves and elliptic and modular functions respectively.

Definition 4.2.1. Let $E/\mathbb{Q}$ have discriminant D_E, and $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ and $\omega_1 \in \mathbb{R}$. The *real period* of E is defined to be

$$\Omega_E = \begin{cases} 2\omega_1 & D_E > 0 \\ \omega_1 & D_E < 0 \end{cases}. \tag{4.2.1}$$

We are interested in answering the question: For a curve of a given discriminant, how big and how small can Ω_E be? Can the real period be arbitrarily small or large, or does it scale in some meaningful way with the discriminant? For our purposes, establishing a lower bound on Ω_E is what is needed to bound the central leading Taylor coefficient of $L_E(s)$ from below. However, we include the result giving an upper bound on Ω_E, as we find its implication – that Ω_E goes to zero as N_E goes to infinity – an interesting one.

First, an upper bound. To this end, we have the following result from the complex theory

of elliptic curves:

Proposition 4.2.2. *Let $\Delta(z)$ be the Ramanujan Delta function on the complex upper half plane, i.e.*

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}, \tag{4.2.2}$$

where $q = e^{2\pi iz}$. Let $E/\mathbb{C}$ have discriminant D_E and lattice basis (ω_1, ω_2) as defined above. Set $z = \frac{\omega_1}{\omega_2}$ (such that $\mathrm{Im}(z) > 0$). Then

$$D_E = \left(\frac{2\pi}{\omega_1}\right)^{12}\Delta(z). \tag{4.2.3}$$

A proof of the above can be found in Chapter I of [32]. Using this result we can readily establish an upper bound on Ω_E:

Proposition 4.2.3. *Let $E/\mathbb{Q}$ have discriminant D_E and real period Ω_E. Then*

$$\Omega_E < 8.82921517\ldots\cdot(D_E)^{-\frac{1}{12}}. \tag{4.2.4}$$

Proof. Equation 4.2.3 yields

$$\omega_1 = 2\pi|D_E|^{-\frac{1}{12}}\left|\Delta\left(\frac{\omega_2}{\omega_1}\right)\right|^{\frac{1}{12}}. \tag{4.2.5}$$

Recall that since E is defined over $\mathbb{Q}$, we may choose a lattice basis (ω_1, ω_2) such that $\omega_1 \in \mathbb{R}_+$ and the real part of ω_2 equals either 0 or $\frac{\omega_1}{2}$. Thus we may take $z = \frac{\omega_2}{\omega_1}$ to have real part either equal to 0 or $\frac{1}{2}$. Moreover, $\mathrm{Re}(s) = 0$ if $D_0 > 0$ and $\mathrm{Re}(z) = \frac{1}{2}$ if $D_E < 0$. See Chapter I of [32] for proofs of these statements.

Thus $D_E > 0$ corresponds to $q = e^{2\pi iz}$ being positive real lying in the open interval $q \in (0, 1)$, while $D_E < 0$ corresponds to $q \in (-1, 0)$. Now Δ is a cuspidal modular form on $\mathrm{SL}_2(\mathbb{Z})$, so as a function of q, $\Delta(q)$ is continuous on $(-1, 1)$, zero at the origin, and decaying to zero at $q = -1$ and $q = 1$. It must therefore achieve a maximum magnitude on both open intervals $q \in (-1, 0)$ and $q \in (0, 1)$.

The critical points of Δ have been studied in there own right – see for example [19] and [38]. We see that $\Delta(q)$ has precisely one critical point on each of the intervals $q \in (-1, 0)$ and $q \in (0, 1)$; these occur at $q = 0.03727681\ldots$ and $q = -0.43929305\ldots$ respectively (corresponding to $z = 0.52352170\ldots i$ and $z = \frac{1}{2} + 0.13091903\ldots i$ in the upper half plane respectively). At these two values we have $|\Delta(q)|^{\frac{1}{12}}$ equal to $0.70258935\ldots$ and $1.40521323\ldots$ respectively. We conclude that

$$\Omega_E \leq 2\pi \cdot 1.40521323\ldots \cdot |D_E|^{-\frac{1}{12}} = 8.82921517\ldots \cdot |D_E|^{-\frac{1}{12}}. \tag{4.2.6}$$

□

Note that the real period is *not* invariant under isomorphism over $\mathbb{Q}$. As the elliptic discriminant D_E varies by a twelfth power of an integer as one considers $\mathbb{Q}$-isomorphic models of E, the real period varies by the negative first power of that same integer. This is an immediate consequence of the following statement:

Lemma 4.2.4. *Let E be the global minimal model of a rational elliptic curve, and let D_E and Ω_E be its discriminant and real period respectively. Let E' be isomorphic to E over $\overline{\mathbb{Q}}$, and let $D_{E'}$ and $\Omega_{E'}$ be defined analogously. Then there exists a u such that $u^{12} \in \mathbb{Z}$, where $D_{E'} = u^{12} D_E$ and $\Omega_{E'} = \frac{1}{u}\Omega_E$.*

A proof of the result regarding the discriminant can be found on pages 48-49 of [31]; the result regarding the real period follows, for example, from Equation 4.2.3 by chasing through how D_E and Ω_E vary under $\mathbb{C}$-isomorphism.

Another consequence is that the bound given in Equation 4.2.4 is optimal, in the sense that the $\frac{1}{12}$ in the negative power of the the discriminant cannot be replaced with any larger value. As an explicit example, consider the family of CM elliptic curves given by Weierstrass equations

$$E^d : \quad y^2 = x^3 - d^2 x, \tag{4.2.7}$$

for $d \in \mathbb{Z}$ positive squarefree. This is just the family of curves related to the congruent number problem, one of the oldest open problems in mathematics (for an excellent treatment on congruent numbers and how they relate to elliptic curves, see [22]). Then E^d is just the quadratic twist by d (hence the notation) of the curve

$$E: \quad y^2 = x^3 - x, \tag{4.2.8}$$

which has discriminant 64 and conductor 32. For this family we may actually write down Ω_{E^d} in terms of a special value of the Gamma function:

$$\Omega_{E^d} = \frac{\Gamma(\frac{1}{4})^2}{\sqrt{2\pi d}}. \tag{4.2.9}$$

This follows from the fact that $\frac{\omega_2}{\omega_1} = i$ for any of the E^d, and that

$$\Delta(i) = \frac{\Gamma(\frac{1}{4})^{24}}{2^{24}\pi^{18}} \tag{4.2.10}$$

(first shown by Ramanujan in his second notebook – see [1]). Furthermore, E^d has discriminant $D_{E^d} = (2d)^6$. So using equation 4.2.3, for congruent number curves we obtain

$$\Omega_{E^d} = \frac{\Gamma(\frac{1}{4})^2}{\sqrt{\pi}} \cdot (D_{E^d})^{-\frac{1}{12}} = 7.416\ldots \cdot (D_{E^d})^{-\frac{1}{12}}. \tag{4.2.11}$$

Since $4\pi = 12.566\ldots$ this result conforms with the bound given in Equation 4.2.4. It should also be clear from the example above that any family of quadratic twists of a given curve will have the real period scale with the $-\frac{1}{12}$th power of the discriminant. Furthermore, since the j-invariant is surjective, we can find $E/\mathbb{Q}$ with $z = j^{-1}(E)$ arbitrarily close to $\frac{1}{2}+0.13091903\ldots i$, so the constant $8.82921517\ldots$ obtained in Proposition 4.2.3 is also optimal.

Corollary 4.2.5. *For $E/\mathbb{Q}$ with real period Ω_E and conductor N_E,*

$$\Omega_E < 8.82921517\ldots \cdot (N_E)^{-\frac{1}{12}}. \tag{4.2.12}$$

That is, the real period goes to zero as the conductor of the curve goes to infinity.

This follows immediately from Proposition 4.2.3, as the conductor of an elliptic curve always divides its discriminant. Again, by the same reasoning as before this bound should be optimal. Note that this result is unconditional.

Equation 4.2.3 gives us a way to compute the real period of E, but it is in general not the most efficient means of doing so (as $z = \frac{\omega_1}{\omega_2}$ must be found by, for example, inverting the j-invariant of E). Instead, ω_1 may be computed using the (real version of the) Gauss arithmetic-geometric mean. Recall the definition thereof: let $a, b \in \mathbb{R}_{\geq 0}$. Set $a_0 = a$ and $b_0 = b$, and for $n \geq 0$ let $a_{n+1} = \frac{1}{2}(a_n + b_n)$ and $b_{n+1} = \sqrt{a_n b_n}$. Then $\mathrm{AGM}(a, b)$ is defined to be the common limit of both the a_n and the b_n. Moreover, the convergence is quadratic – precision roughly doubles with every iteration – and is thus very quick. A deeper exposition of the AGM including a proof of convergence and convergence rate can be found in [11].

Proposition 4.2.6. *Let $E/\mathbb{Q}$ have minimal Weierstrass equation $y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6$. Write the equation in the form*

$$\left(y + \frac{a_1x + a_3}{2}\right)^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} = (x - e_1)(x - e_2)(x - e_3), \tag{4.2.13}$$

where e_1, e_2, e_3 are the 3 complex roots of the polynomial in x on the right hand side, and b_2, b_4 and b_6 are as defined in Section 3.1.

1. *If $D_E > 0$, then $e_1, e_2, e_3 \in \mathbb{R}$, so without loss of generality we may order them as $e_3 > e_2 > e_1$. Then*

$$\omega_1 = \frac{\pi}{AGM(\sqrt{e_3 - e_1}, \sqrt{e_3 - e_2})}. \tag{4.2.14}$$

2. *If $D_E < 0$, then the RHS polynomial has only one real root; we may write $e_3 \in \mathbb{R}$ and $e_1 = \overline{e_2}$. Let $z = \sqrt{e_3 - e_1} = s + it$; choose the root such that $s > 0$. Then*

$$\omega_1 = \frac{\pi}{AGM(|z|, s)}. \tag{4.2.15}$$

Proof. Cremona and Cremona-Thongjunthug give good explanations and derivations this formula in [12] and [13] respectively. □

To get a lower bound on Ω_E from the above definitions, we will need the following technical result.

Definition 4.2.7. For a given $E/\mathbb{Q}$, let

$$d(E) = \max\left\{|e_i - e_j| : \ e_i, e_j \text{ are roots of } 4x^3 + b_2x^2 + 2b_4x + b_6, i \neq j\right\} \tag{4.2.16}$$

be the maximum root separation of the cubic polynomial on the RHS of equation 4.2.13 (i.e. b_2, b_4 and b_6 are the b-invariants of E).

Observe that for both the positive and negative discriminant cases, the AGM in the denominators in equations 4.2.14 and 4.2.15 is at most $\sqrt{d(E)}$. It is useful therefore to have a bound on the magnitude of $d(E)$ in terms of the b-invariants:

Lemma 4.2.8. *Given the above setup,*

$$d(E) < 2 + \frac{1}{2}\max\left\{|b_2|, 2|b_4|, |b_6|\right\}. \tag{4.2.17}$$

Proof. We apply Rouche's Theorem on the polynomial $x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$. Observe that $|\frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}| < |x^3|$ when $|x| < 1 + \max\left\{\frac{|b_2|}{4}, \frac{|b_4|}{2}, \frac{|b_6|}{4}\right\}$, so by Rouche's Theorem we must have that any root e of the cubic obeys $|e| < 1 + \frac{1}{4}\max\left\{|b_2|, 2|b_4|, |b_6|\right\}$. The result follows. □

Corollary 4.2.9 (ABC)**.** *The real period of an elliptic curve can be computed to a specified precision in polynomial time and space in the number of bits of the curve's conductor.*

Proof. We see from Proposition 4.2.6 that Ω_0 can be computed by a) finding the roots of a cubic polynomial related to the Weierstrass equation for E, and then b) applying the AGM to a certain simple function of that cubic's roots.

Step a) can be achieved in polynomial time in log of the maximum magnitude of the a-invariants, which means it can be done in polynomial time in the c-invariants. By Modified Szpiro (Conjecture 3.3.6) the conductor of a curve is bounded in magnitude by a polynomial

in the c-invariants; chaining this all together gives us that step a) can be commuted in time polynomial in $\log N_E$, i.e. sub-polynomial in N_E.

In step b), Lemma 4.2.8 implies that the inputs to the AGM are bounded by a polynomial of the b-invariants of E, so again by Szpiro they are bounded by a power of N_E. The AGM converges quadratically when both the inputs are positive real; therefore it will converge to specified precision with time bounded by a polynomial of $\log N_E$. Thus altogether we see that the real period can be computed to a given precision with time polynomial in $\log N_E$, i.e. sub-polynomial in N_E itself. □

The take-away from the above result is that computing the real period is quick, and will never be the computational bottleneck when it comes to running Algorithm 2.0.6.

Corollary 4.2.10 (S.)**.** *Let $E/\mathbb{Q}$ have (not necessarily minimal) Weierstrass equation $y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6$ have real period Ω_E, and define b_2, b_4 and b_6 as at the beginning of section 3. Then*

$$\Omega_E > \frac{\alpha\pi}{\sqrt{1 + \frac{1}{4}\max\{|b_2|, 2|b_4|, |b_6|\}}}, \tag{4.2.18}$$

where $\alpha = 1$ if E has positive discriminant and $\frac{1}{2}$ if E has negative discriminant.

Proof. This follows immediately from the definition of Ω_E given in Proposition 4.2.6 and Lemma 4.2.8. □

Again, this bound is optimal in the sense that the square root sign in the denominator cannot be replaced with any smaller exponent. To see this, consider the family of elliptic curves

$$E_n : \quad y^2 = x^3 - (nx - 1)^2. \tag{4.2.19}$$

For a given n, E_n has b_2, b_4 and b_6 equal to $-4n^2, 4n$ and -4 respectively.

The polynomial $x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} = x^3 - n^2x^2 + 2nx - 1$ has a single root at $n^2 - O(\frac{1}{n})$ and two roots very close to the origin with magnitude $O(\frac{1}{n})$. Hence the real period for E_n is

$$\Omega_{E_n} = \frac{2\pi}{n} + O\left(\frac{1}{n}\right). \tag{4.2.20}$$

On the other hand, for a given n

$$1 + \frac{1}{4}\max\{|b_2|, 2|b_4|, |b_6|\} = 1 + n^2. \tag{4.2.21}$$

for $n \geq 2$. So for this family of curves the lower bound given by inequality 4.2.10 is $\frac{\pi}{\sqrt{1+n^2}}$. Since Ω_{E_n} asymptotes to twice this value, it is clear that the bound would be violated for sufficiently large n if the square root were replaced with a smaller power.

Finally, if we assume the Szpiro conjecture, Corollary 4.2.10 allows us to the real period of a minimal model of E from below in terms of that curve's conductor. We will invoke a slight reformulation of Modified Szpiro (Conjecture 3.3.6): Suppose the minimal short Weierstrass model of E is $y^2 = x^3 + Ax + B$, i.e. there does not exist any prime p such that $p^4|A$ and $p^6|B$. Then for any $\epsilon > 0$ there is a constant K_ϵ independent of E such that

$$\max\left\{|A|^3, |B|^2\right\} \leq K_\epsilon \cdot (N_E)^{6+\epsilon}. \tag{4.2.22}$$

(Since for a curve in short Weierstrass form $c_4 = -48A$ and $c_6 = -864B$, we see that the above statement and Modified Szpiro are equivalent). Using this, we obtain the following:

Theorem 4.2.11 (ABC)**.** *Let E have conductor N_E, and let Ω_E be the real period of a minimal model of E. Then, assuming ABC, for any $\epsilon > 0$ there is a constant K_ϵ independent of E such that*

$$\Omega_E > K_\epsilon \cdot (N_E)^{-\frac{3}{2}-\epsilon}. \tag{4.2.23}$$

Proof. Let E be given by its minimal short Weierstrass equation $y^2 = x^3 + Ax + B$. E then has b-invariants $b_2 = 0$, $b_4 = 2A$ and $b_6 = 4B$, so by Lemma 4.2.10 the real period of E obeys

$$\Omega_E > \frac{\pi}{2\sqrt{1 + \max\{|A|, |B|\}}}. \tag{4.2.24}$$

Now by the aforementioned version of Szpiro, for any $\epsilon > 0$ we have

$$\begin{aligned}
\sqrt{1 + \max\{|A|, |B|\}} &< 1 + \max\left\{|A|^2, |B|^2\right\}^{\frac{1}{4}} \\
&\leq 1 + \max\left\{|A|^3, |B|^2\right\}^{\frac{1}{4}} \qquad \text{since } A \in \mathbb{Z} \\
&\leq 1 + \left[K_\epsilon (N_E)^{6+\epsilon}\right]^{\frac{1}{4}} \\
\implies \sqrt{1 + \max\{|A|, |B|\}} &< K_\epsilon (N_E)^{\frac{3}{2}+\epsilon},
\end{aligned}$$

where to achieve the last line we absorb 1 into K and relabel as necessary to account for the $\frac{1}{4}$th power, and relabel $\frac{\epsilon}{2} \mapsto \epsilon$. Again, after absorbing the factor of $\frac{\pi}{2}$ into K in equation 4.2.24, the result follows. □

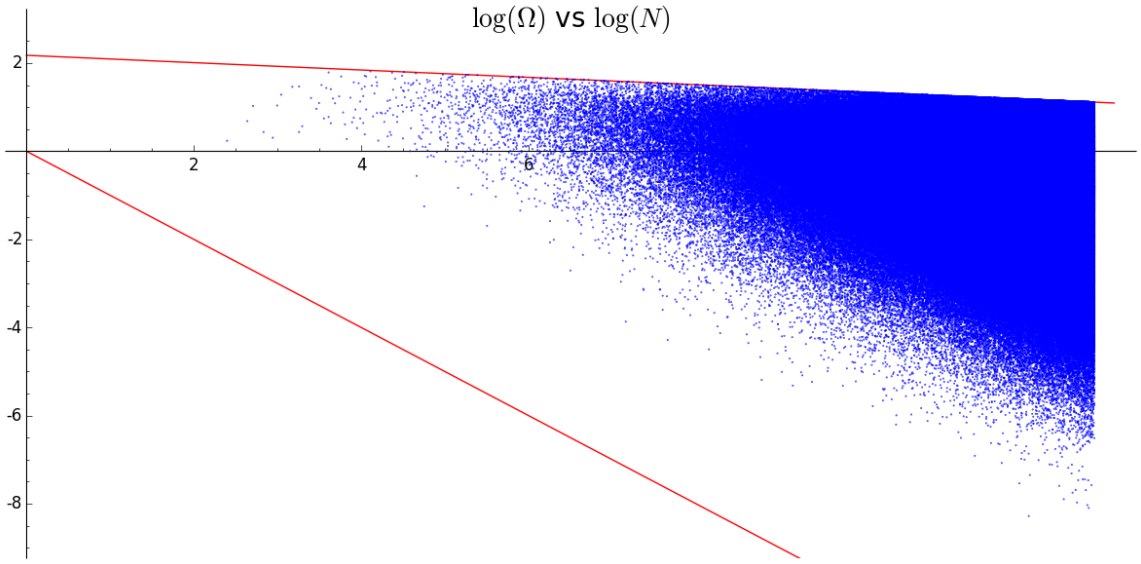

Figure 4.2.1: A scatter plot of $\log \Omega_E$ on the vertical axis vs. $\log N_E$ on the horizontal axis, for all curves up to conductor 350000. The upper red line is the proven upper bound $\Omega_E < 8.82921517\ldots \cdot (N_E)^{-\frac{1}{12}}$, which can be seen to be sharp. The lower red line corresponds to the bound $\Omega_E > (N_E)^{-1}$. Empirically this appears to hold easily, lending credence to the validity of the weaker assertion in Conjecture 4.2.12.

Thankfully, we do not need to assume a specific value of K_ϵ for a given ϵ for Theorem 2.0.5 to hold. However, expirical data suggests that for $\epsilon = \frac{1}{2}$ we can easily get away by choosing $K = 1$. We formalize this with the following conjecture:

Conjecture 4.2.12. *Let E have conductor N_E, and let Ω_E be the real period of a minimal model of E. Then*

$$\Omega_E > (N_E)^{-2}. \tag{4.2.25}$$

4.3 The Regulator

To define the regulator of a rational elliptic curve, we must first define the naïve logarithmic height, Néron-Tate canonical height and the Néron-Tate pairing on points on E.

Let E be an elliptic curve over $\mathbb{Q}$ and $P \in E(\mathbb{Q})$ a rational point on E. The *naïve logarithmic height* of P is a measure of the size' of the coordinates of P.

Definition 4.3.1. Define $h(\mathcal{O}) = 0$. For $P \neq \mathcal{O}$, we may write $P = (x, y) \in \mathbb{Q}^2$, with $x = \frac{a}{b}, a, b \in \mathbb{Z}$, $b > 0$ and $\gcd(a, b) = 1$. We then define the naïve height of P to be

$$h(P) := \max\{\log|a|, \log|b|\}. \tag{4.3.1}$$

If you compute the naïve heights of a number of points on an elliptic curve, you'll notice that the naïve height function is "almost a quadratic form" on E. That is $h(nP) \sim n^2 h(P)$ for integers n, up to some constant that doesn't depend on P. We can turn h into a true quadratic form as follows:

Definition 4.3.2. The *Néron-Tate height* height function $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ is defined as

$$\hat{h}(P) := \lim_{n\to\infty} \frac{h(2^n P)}{(2^n)^2}, \tag{4.3.2}$$

where h is the naïve logarithmic height defined above.

Theorem 4.3.3 (Néron-Tate)**.** *Néron-Tate defines a canonical quadratic form on $E(\mathbb{Q})$ modulo torsion. That is,*

1. *For all $P, Q \in E(\mathbb{Q})$,*

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\left[\hat{h}(P) + \hat{h}(Q)\right], \tag{4.3.3}$$

   i.e. $\hat{h}$ obeys the parallelogram law;

2. *For all $P \in E(\mathbb{Q})$ and $n \in \mathbb{Z}$,*

$$\hat{h}(nP) = n^2 \hat{h}(P). \tag{4.3.4}$$

3. *$\hat{h}$ is even, and the pairing $\langle\ ,\ \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}$ by*

$$\langle P, Q\rangle = \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right) \tag{4.3.5}$$

is bilinear;

4. *$\hat{h}(P) = 0$ iff P is torsion;*

5. *We may replace h with another height function on $E(\mathbb{Q})$ that is "almost quadratic" without changing $\hat{h}$.*

For a proof of this theorem and elaboration on the last point, see [31, pp. 227-232].

Definition 4.3.4. The *Néron-Tate pairing* on $E/\mathbb{Q}$ is the bilinear form $\langle\ ,\ \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}$ by

$$\langle P, Q\rangle = \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right). \tag{4.3.6}$$

Note that this definition may be extended to all pairs of points over $\overline{\mathbb{Q}}$, but the definition above suffices for our purposes.

If $E(\mathbb{Q})$ has rank r, then $E(\mathbb{Q})/E_{\text{tor}}(\mathbb{Q}) \hookrightarrow \mathbb{R}^r$ as a rank r lattice via the height pairing map. Specifically, if $\{P_1, \ldots, P_r\}$ is a basis for $E(\mathbb{Q})$ modulo torsion, then we send $Q \in E(\mathbb{Q})$ to the vector $(\langle Q, P_1\rangle, \ldots, \langle Q, P_r\rangle)$. Note that the image of a given point under this embedding obviously depends on the choice of basis. However, any two lattices comprising the image of $E(\mathbb{Q})$ using two different basis choices are isomorphic, and thus always have the same covolume.

Definition 4.3.5. The *regulator* Reg_E of $E/\mathbb{Q}$ is the covolume of the lattice that is the image of $E(\mathbb{Q})$ under the above pairing map. That is, if $\{P_1, \ldots, P_r\}$ generates $E(\mathbb{Q})$, then

$$\text{Reg}_E = \det\left(\langle P_i, P_j\rangle\right)_{1\le i,j\le r}, \tag{4.3.7}$$

where $\left(\langle P_i, P_j\rangle\right)_{1\le i,j\le r}$ is the matrix whose (i,j)th entry is the value of the pairing $\langle P_i, P_j\rangle$. If $E/\mathbb{Q}$ has rank zero, then Reg_E is defined to be 1.

Note that for any $P \in E(\mathbb{Q})$, $\langle P, P \rangle = \hat{h}(P)$. Thus the regulator of any rank 1 curve is just the smallest height of a non-torsion point on that curve.

Loosely, the regulator measures the "density" of rational points on E: positive rank elliptic curves with small regulators have many points with small coordinates, while those with large regulators have few such points.

There are conjectural bounds on how large a curve's regulator can be in terms of its conductor – see for example Conjecture 6.3 in Lang's Survey of Diophantine Geometry [24, p. 99]. This is a topic we hope to investigate more fully future work, but the question that is relevant to this thesis is not how large the regulator can be, but how small. Specifically, given $E/\mathbb{Q}$ with (minimal) discriminant D_E, what is the smallest Reg_E can be as a function of D_E?

This is an open question. However, recall Lang's Height Conjecture (Conjecture 1.4 in [24, pp. 73-74]):

Conjecture 3.3.7. Let $E/\mathbb{Q}$ have minimal discriminant D_E. There exists an absolute constant $M_0 > 0$ independent of E such that any non-torsion point $P \in E(\mathbb{Q})$ satisfies

$$\hat{h}(P) \geq M_0 \log |D_E|. \tag{4.3.8}$$

That is, the minimum height of a non-torsion point on E scales with the log of the absolute value of the curve's minimal discriminant. Hindry and Silverman in [18] show that the ABC conjecture implies Lang's height conjecture and, better yet, gives an explicit lower bound on M_0:

$$M_0 \geq 6 \times 10^{-11}. \tag{4.3.9}$$

The bound was further improved by Elkies (albeit still contingent on ABC) in the early 2000s [15] to

$$M_0 \geq 3.9479 \times 10^{-5}. \tag{4.3.10}$$

Note that Theorem 2.0.5 requires the assumption of ABC for results regarding the real period

of E; quoting the above result therefore requires no further unproven results.

There is general agreement in the literature is that the value of M_0 above is not optimal; however, there is no strong consensus as to how much larger M_0 could be. A survey by Elkies [16] reveals 54 known cases of points P on curves over $\mathbb{Q}$ where $\hat{h}(P) < \frac{1}{100}$, and the largest value of $\hat{h}/\log|D_E|$ is $\sim 8.46 \times 10^{-5}$, achieved by a point on a curve of conductor $N = 3476880330$. Given the evidence in this and other compiled data, it seems quite likely that there are as-yet undiscovered instances of points with low height driving the observed lower bound down closer to the value of 3.9479×10^{-5}.

One can therefor make the more conservative following observation:

Corollary 4.3.6 (ABC)**.** *There exists an absolute constant $M_1 > 0$ independent of E such that any non-torsion point P on any elliptic curve $E(\mathbb{Q})$ satisfies*

$$\hat{h}(P) \geq M_1. \tag{4.3.11}$$

The smallest absolute point height found in the aforementioned survey by Elkies is $\hat{h}(P) = 8.914 \times 10^{-3}$, achieved by the point $P = (7107, -602054)$ and its negative on the curve with Cremona label `3990v1`, given by the equation $E : y^2 + xy + y = x^3 + x^2 - 125615x + 61201397$. (note that the Elkies' table uses a slightly different definition of height, equal to half the value of the height as defined above). One can see in this table that the known points of smallest height all belong to curves with small conductor, so it is perhaps more believable that this is indeed the point of smallest height on any rational elliptic curve – for such a point is guaranteed to exist, assuming ABC.

Even though the Elkies bound above would seem so small as to be of limited use in practical applications, we can use it to bound a curve's regulator from below in terms of an inverse power of its conductor. For this we will need the following geometric lemma:

Lemma 4.3.7. *Let L be a lattice in $\mathbb{R}^r$ with covolume V_L. If h is the minimum nonzero vector length in L, then*

$$V_L \geq \left(\frac{\sqrt{\pi}}{2} \cdot h\right)^r \cdot \frac{1}{\Gamma(1+\frac{r}{2})}, \tag{4.3.12}$$

where $\Gamma(s)$ is the usual Gamma function on $\mathbb{C}$.

Proof. Recall Minkowski's Theorem: Let L be a lattice in $\mathbb{R}^r$ with covolume V_L, and let S be a convex symmetric subset of $\mathbb{R}^r$ with volume $\mathrm{Vol}(S)$. If $\mathrm{Vol}(S) > 2^r \cdot V_L$, then S contains a nonzero element of L – see [33, p. 80] for a proof.

So let $S = B(0, h)$, i.e. the open ball of radius h centered at the origin, where h is the minimum nonzero vector length in L. By construction S contains no nonzero lattice elements, so by Minkowski's theorem we must have that

$$\mathrm{Vol}(S) \leq 2^r V_L. \tag{4.3.13}$$

The volume of the r-sphere with radius L is given by

$$\mathrm{Vol}(S) = \frac{\pi^{\frac{r}{2}}}{\Gamma(1+\frac{r}{2})} \cdot h^r; \tag{4.3.14}$$

combining the above two statements and solving for V_L completes the result. □

With the above lemma we can then prove the following:

Theorem 4.3.8 (BSD, ABC, (GRH))**.** *Let $E/\mathbb{Q}$ have conductor N_E. Assuming BSD and ABC, we have that*

$$\mathrm{Reg}_E \geq 4.36 \times 10^{-6} \cdot (N_E)^{-3.86} \cdot \frac{1}{\Gamma(1.8 + 0.25 \log N_E)}. \tag{4.3.15}$$

If one further assumes GRH, then one has the improved bound

$$\mathrm{Reg}_E \geq 2.11 \times 10^{-2} \cdot (N_E)^{-2.47} \cdot \frac{1}{\Gamma(1.25 + 0.16 \log N_E)}. \tag{4.3.16}$$

Proof. For curves of conductor ≤ 350000, we consulted Cremona's tables and verified numerically that the above statements. Thus without loss of generality we may assume $D_E \geq N_E > 350000$. Hence for any point $P \in E(\mathbb{Q})$, by Conjecture 3.3.7 and the Elkies' bound in Equation 4.3.11 we have that

$$\hat{h}(P) \geq 3.9479 \times 10^{-5} \cdot \log |D_E| \geq 6 \times 10^{-11} \cdot \log(350000) = 5.0397 \times 10^{-4}. \tag{4.3.17}$$

Let $h = 5.0397 \times 10^{-4}$, and let L be the rank r lattice that is the image of $E(\mathbb{Q})$ under the height pairing map (for a given choice of basis of $E(\mathbb{Q})$), where r is the rank of E. It follows that any nonzero vector in L has length at least h. Thus by Lemma 4.3.7 we must then have that

$$\mathrm{Reg}_E \geq \left(\frac{\sqrt{\pi}}{2} \cdot h\right)^r \cdot \frac{1}{\Gamma(1 + \frac{r}{2})}.$$

By BSD, the algebraic and analytic rank are equal, so we have that

$$r < a \log N_E + b, \tag{4.3.18}$$

where by Corollary 5.1.12 we may take $a = 0.5, b = 1.6$ if we aren't assuming GRH, and by Corollary 5.3.4 $a = 0.32, b = 0.5$ if we are. Thus

$$\begin{aligned} \mathrm{Reg}_E &\geq \left(\frac{\sqrt{\pi}}{2} \cdot h\right)^{a \log N_E + b} \cdot \frac{1}{\Gamma\left(1 + \frac{a \log N_E + b}{2}\right)} \\ &= \left(\frac{\sqrt{\pi}}{2} \cdot h\right)^b \cdot (N_E)^{a \log\left(\frac{\sqrt{\pi}}{2} \cdot h\right)} \cdot \frac{1}{\Gamma\left((1 + \frac{b}{2}) + \frac{a}{2} \log N_E\right)}. \end{aligned}$$

[Note that replacing r with $a \log N_E + b$ inside the Gamma factor is only valid in the region where the Gamma function is monotonically increasing, i.e. for $a \log N_E + b \geq 1$. However, we are in this case in both the non-GRH and GRH versions of the proof, since we are assuming $N_E > 350000$.]

Substituting the respective values of a and b and simplifying produces the two inequalities stated in the theorem. □

There are a few things worth pointing out about this result. Firstly, the Gamma factor means that the proven lower bound on the regulator eventually decreases more rapidly than any negative power of the conductor. However, since $\Gamma(s) = O(e^{s \log s})$, we see that $\Gamma\left((1 + \frac{b}{2}) + \frac{a}{2} \log N\right) = O(N^{c \log \log N})$ for some constant c. That is, the exponent in the negative power of N_E coming from the Gamma factor grows, albeit very slowly.

Note that (without assuming GRH), the number of bits extra precision needed in Algorithm 2.0.6 required to compensate for the Gamma factor is $\log_2(\Gamma(1.8 + 0.25 \log N_E))$. Even though this quantity grows faster than $\log N_E$, the constant in front of $\log N_E$ inside the Gamma factor is small enough that for all practical purposes the number of bits precision needed to account for the Gamma factor grows linearly with log of the conductor over the range of conductors for which the rank algorithm is practical. For example, when $N_E = 350000$ the number of extra bits precision needed to accommodate for the Gamma factor is just 5 (even without assuming GRH). And even for $N_E = 10^{20}$ – which is about the upper limit for what is practical on modern architecture – the number of extra bits needed is 30. Either way, the number of bits needed to account for the regulator isn't an issue in any way since the computational bottleneck in the rank algorithm is the $\sqrt{N_E}$ dependence coming from evaluating $L_E(s)$, which grows faster than any power or $\log N_E$.

Also note that the first step in the proof – manual verification for all curves below conductor 35000 – isn't strictly necessary; it only improves the constants in the bounds by a small amount. However, it serves to highlight that the power of N_E in the two bounds can theoretically be improved further by exhaustively checking all curves up to a higher conductor bound. If, for example, we believe that 8.914×10^{-3} is a global minimum point height over all rational elliptic curves, then (assuming GRH) we would instead get

$$\mathrm{Reg}_E \geq 8.89 \times 10^{-2} \cdot (N_E)^{-1.55} \cdot \frac{1}{\Gamma(1.25 + 0.16 \log N_E)}. \tag{4.3.19}$$

Even so, we do *not* expect either bound to be anywhere close to optimal; almost certainly

more careful analysis could further reduce the negative exponent of N or increase the size of the constant in front of it – or better yet, eliminate the Gamma factor. In practice, we see the smallest regulators tend to *grow* with conductor, further highlighting that the above bound is rather crude. However, the statement in Theorem 4.3.8 is good enough for our purposes: it will help establish that the central leading coefficient of $L_E(s)$ cannot be exponentially small in N_E.

We invite the interested reader to improve upon this result, and thus ultimately speed up the runtime of Algorithm 2.0.6.

Chapter 5

ZERO SUMS

Algorithm 2.0.6 allows us to compute the rank of an elliptic curve in $\tilde{O}\left(\sqrt{N_E}\right)$ time by evaluating successive derivatives of $L_E(s)$ at the central point. However, there is an inescapable limitation of this algorithm: the $\sqrt{N_E}$ time dependence of evaluating $L_E(s)$ means that it becomes infeasible to run on modern computer hardware when the conductor is larger than about 10^{16}. Moreover, since there is no known way to evaluate elliptic curve L-functions in faster than square-root-conductor time, there is essentially nothing we can do to make such a rank computation algorithm asymptotically faster.

In this section we work toward presenting a method to bound analytic rank from above that does not require direct computation of a curve's L-function. The upside of such an algorithm is that it can be run on curves with much larger conductor, with the tightness of the bound scaling with how long one wants computation time to be. The downside is that we will have to sacrifice exactness: the method will only provide upper bounds on rank.

Because the aforementioned method relies on sums over the zeros of $L_E(s)$, for this entire section we will assume GRH unless explicitly stated otherwise.

5.1 Logarithmic Derivatives

Let $E/\mathbb{Q}$ have conductor N_E.

Definition 5.1.1. The *logarithmic derivative* of the L-function attached to E is

$$\frac{L_E'}{L_E}(s) := \frac{d}{ds}\log L_E(s) = \frac{L_E^{'}(s)}{L_E(s)}. \tag{5.1.1}$$

Logarithmic derivatives have some useful properties. Importantly, the logarithmic derivative of the product of meromorphic functions is the sum of the logarithmic derivatives thereof. To this end:

Proposition 5.1.2.

$$\frac{\Lambda_E'}{\Lambda_E}(s) = \log\left(\frac{\sqrt{N_E}}{2\pi}\right) + \digamma(s) + \frac{L_E'}{L_E}(s), \tag{5.1.2}$$

where $\digamma(s) = \frac{\Gamma'}{\Gamma}(s)$ *is the digamma function on* $\mathbb{C}$.

This follows immediately from the definition of $\Lambda_E(s) = (N_E)^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L_E(s)$.

Note that the digamma function is well-understood and easily computable. It has simple poles at the negative integers, and it has the following infinite sum expansion about $s = 1$:

$$\digamma(1+s) = -\eta + \sum_{k=1}^{\infty} \frac{s}{k(k+s)}. \tag{5.1.3}$$

This series converges absolutely for any s not equal to a negative integer, and uniformly on bounded sets (excluding the aforementioned negative integers).

What is perhaps surprising, however, is that $\frac{L_E'}{L_E}(s)$ can be represented by an elegant Dirichlet series. Recall that for $p \nmid N_E$, the characteristic polynomial of Frobenius w.r.t. f at p is $x^2 - a_p x + p^2$, where a_p is as given by Definition 3.2.9. Let this quadratic polynomial split as $(x - \alpha_p)(x - \beta_p)$ in $\mathbb{C}$, where for α_p and β_p the dependance on E is understood.

Definition 5.1.3. For $n \in \mathbb{N}$, let

$$b_n(E) := \begin{cases} -\left(\alpha_p^e + \beta_p^e\right) \cdot \log(p), & n = p^e \text{ a prime power } (e \geq 1), \text{ and } p \nmid N_E \\ -a_p^e \cdot \log(p), & n = p^e \text{ and } p \mid N_E \\ 0, & \text{otherwise.} \end{cases} \tag{5.1.4}$$

Lemma 5.1.4. *The Dirichlet series for $\frac{L_E'}{L_E}(s)$ is given by*

$$\frac{L_E'}{L_E}(s) = \sum_{n=1}^{\infty} b_n(E)\, n^{-s}, \tag{5.1.5}$$

where the coefficients $b_n(E)$ are defined as in Definition 5.1.3.

Proof. The proof is an exercise in taking the logarithmic derivative of the Euler product formula for $L_E(s)$ and simplifying. Note we may write the Euler product of $L_E(s)$ as

$$L_E(s) = \prod_{p \mid N_E} \left(1 - a_p p^{-s}\right)^{-1} \prod_{p \nmid N_E} \left(1 - \alpha_p p^{-s}\right)^{-1} \left(1 - \beta_p p^{-s}\right)^{-1}. \tag{5.1.6}$$

The result follows by taking the logarithmic derivative of each term individually and then summing the results. □

The Dirichlet coefficients for $\frac{L_E'}{L_E}(s)$ have a beautiful characterization in terms of the number of points on E over finite fields:

Proposition 5.1.5.

$$b_n(E) = \begin{cases} -\left(p^e + 1 - \#\widetilde{E}(\mathbb{F}_{p^e})\right) \cdot \log(p), & n = p^e \text{ a prime power,} \\ 0, & \text{otherwise.} \end{cases} \tag{5.1.7}$$

where $\#\widetilde{E}(\mathbb{F}_{p^e})$ is the number of points over $\mathbb{F}_{p^e}$ on the (possibly singular) curve obtained by reducing E modulo p.

Proof. It is a standard result that if $(x-\alpha_p)(x-\beta_p)$ is the characteristic polynomial for Frobenius on E for the prime of good reduction p, then

$$\#E(\mathbb{F}_{p^e}) = p^e + 1 - \alpha_p^e - \beta_p^e \tag{5.1.8}$$

(see [31, pp. 134-136] for a proof), from which the result at $p \nmid N_E$ follows.

For primes of bad reduction, recall

$$a_p(E) := \begin{cases} +1, & E \text{ has split multiplicative reduction at } p \\ -1, & E \text{ has non-split multiplicative reduction at } p \\ 0, & E \text{ has additive reduction at } p. \end{cases} \tag{5.1.9}$$

Let $E_{\text{ns}}(\mathbb{F}_{p^e})$ be the group of nonsingular points on $\widetilde{E}(\mathbb{F}_{p^e})$.

When E has additive reduction at p, $E_{\text{ns}}(\mathbb{F}_{p^e}) \simeq (\mathbb{F}_{p^e}, +)$, so together with the singular point $\#\widetilde{E}(\mathbb{F}_{p^e}) = p^e + 1$;

Hence $(p^e + 1 - \#\widetilde{E}(\mathbb{F}_{p^e}))\log(p) = 0 = a_p^e \log(p)$.

When E has split multiplicative reduction at p, $E_{\text{ns}}(\mathbb{F}_{p^e}) \simeq (\mathbb{F}_{p^e}^*, \times)$, so together with the singular point $\#\widetilde{E}(\mathbb{F}_{p^e}) = (p^e - 1) + 1 = p^e$; So $(p^e + 1 - \#\widetilde{E}(\mathbb{F}_{p^e}))\log(p) = 1 \cdot \log(p) = a_p^e \log(p)$.

When E has non-split multiplicative reduction at p, let $L/\mathbb{F}_{p^e}$ be the quadratic extension obtained by adjoining to $\mathbb{F}_{p^e}$ the slopes of the tangent lines at the singular point; then $E_{\text{ns}}(\mathbb{F}_{p^e}) \simeq \ker(\text{Norm}_{L/\mathbb{F}_{p^e}})$.

Some thought should convince you that there are $p^e - (-1)^e$ elements in L with norm 1, so together with the singular point $\#\widetilde{E}(\mathbb{F}_{p^e}) = p^e + 1 - (-1)^e$;

Hence $(p^e + 1 - \#\widetilde{E}(\mathbb{F}_{p^e}))\log(p) = (-1)^e \cdot \log(p) = a_p^e \log(p)$. See [31, pg. 180, Prop. 5.1] for the proofs of the above isomorphisms.

□

With elliptic curve L-functions it is often easier to work with the shifted logarithmic derivative $\frac{L_E'}{L_E}(1+s)$ as it places the critical point at the origin. We therefore define notation for the coefficients of the shifted Dirichlet series below:

Definition 5.1.6. The logarithmic derivative of the shifted L-function $L_E(1+s)$ is given by Dirichlet series

$$\frac{L'_E}{L_E}(1+s) := \sum_n c_n n^{-s} = \sum_n \frac{b_n}{n} n^{-s}, \tag{5.1.10}$$

i.e. $c_n = b_n/n$, where the b_n are as defined in Definition 5.1.3.

Because of its transparent Dirichlet series, we can bound the magnitude of $\frac{L'_E}{L_E}(1+s)$ for $\mathrm{Re}(s) > \frac{1}{2}$. Let $\frac{\zeta'}{\zeta}$ be the logarithmic derivative of the Riemann zeta function. Then $\frac{\zeta'}{\zeta}(s) = \sum -\Psi(n)n^{-s}$ for $\mathrm{Re}(s) > 1$, where $\Psi(n)$ is the von Mangoldt function, given by

$$\Psi(n) = \begin{cases} \log p & n = p^e \text{ a perfect prime power,} \\ 0 & \text{otherwise.} \end{cases} \tag{5.1.11}$$

(The von Mangoldt function is typically denoted $\Lambda(n)$ in the literature, but we have already reserved Λ for the competed L-function of an elliptic curve). Observe that $-\frac{\zeta'}{\zeta}(s)$ is strictly positive for $s > 1$ real, and decays to zero exponentially as $s \to \infty$.

Away from the critical strip the behaviors of both $L_E(s)$ and $\frac{L'_E}{L_E}(s)$ are tightly constrained.

Lemma 5.1.7. *Let $L_E(s)$ be the L-function of E. For any $s \in \mathbb{C}$ with $\sigma := \mathrm{Re}(s) > \frac{3}{2}$, we have the following:*

1.

$$\frac{\zeta(2\sigma-1)^2}{\zeta(\sigma-\frac{1}{2})^2} < |L_E(s)| < \zeta\left(\sigma - \frac{1}{2}\right)^2. \tag{5.1.12}$$

2.

$$2\frac{\zeta'}{\zeta}\left(\sigma - \frac{1}{2}\right) < \left|\frac{L'_E}{L_E}(s)\right| < -2\frac{\zeta'}{\zeta}\left(\sigma - \frac{1}{2}\right). \tag{5.1.13}$$

where $\zeta(s)$ is the Riemann Zeta function.

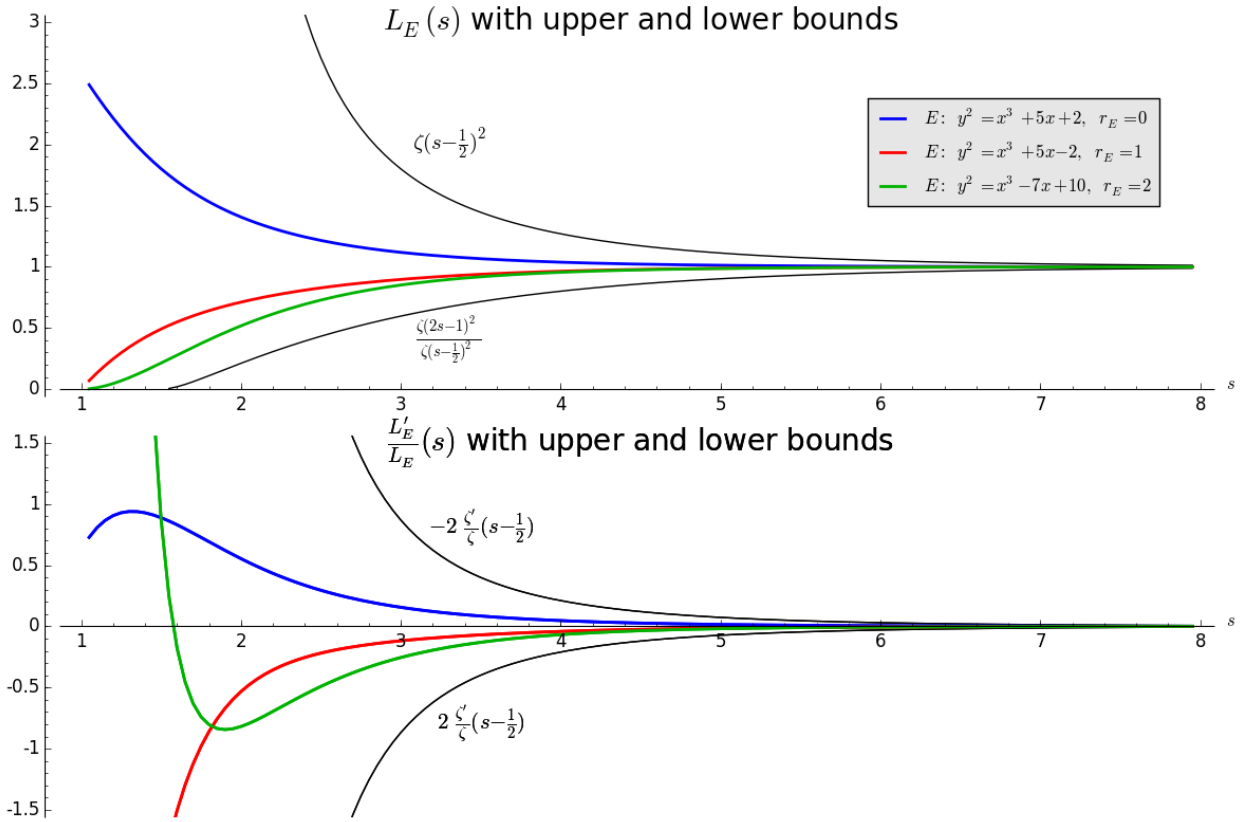

Figure 5.1.1: Plots of $L_E(s)$ and $\frac{L'_E}{L_E}(s)$ for $1 < s < 8$ for 3 elliptic curves – one each of rank 0, 1 and 2 – with the global bounds given in Lemma 5.1.7 drawn in.

Proof. For the bound on $L_E(s)$, note that we may write the Euler product representation of $L_E(s)$ as

$$L_E(s) = \prod_{p|N_E} \left(\frac{1}{1 - a_p p^{-s}}\right) \cdot \prod_{n\nmid N_E} \left(\frac{1}{1 - \alpha_p p^{-s}}\right)\left(\frac{1}{1 - \beta_p p^{-s}}\right), \tag{5.1.14}$$

where for good p, α_p and β_p are the two complex conjugate roots of the characteristic equation of Frobenius at p for E. Hasse's Theorem has that these are both precisely $\sqrt{p}$ in magnitude; since $|a_p| \leq 1$ for bad p we thus derive the inequality

$$\prod_p \left(\frac{1}{1 + \sqrt{p} \cdot p^{-s}}\right)^2 < |L_E(s)| < \prod_p \left(\frac{1}{1 - \sqrt{p} \cdot p^{-s}}\right)^2. \tag{5.1.15}$$

We then note that

$$\prod_p \left(\frac{1}{1-\sqrt{p}\cdot p^{-s}}\right)^2 = \left(\prod_p \frac{1}{1-p^{-s+\frac{1}{2}}}\right)^2 = \zeta(s-\frac{1}{2})^2,$$

while

$$\prod_p \left(\frac{1}{1+\sqrt{p}\cdot p^{-s}}\right)^2 = \left(\prod_p \frac{1-p^{-s+\frac{1}{2}}}{1-p^{-2s+1}}\right)^2 = \frac{\zeta(2s-1)^2}{\zeta(s-\frac{1}{2})^2}$$

to complete the result.

For the bound on $\frac{L_E'}{L_E}(s)$, observe that Hasse's Theorem implies that $|q+1-\#\widetilde{E}(\mathbb{F}_q)| \leq 2\sqrt{q}$ for any prime *power* q. Hence

$$\left|\frac{L_E'}{L_E}(s)\right| \leq \sum_n |b_n|\cdot n^\sigma < \sum_n 2\sqrt{n}\cdot\lambda(n)n^{-\sigma} = -2\frac{\zeta'}{\zeta}\left(\sigma-\frac{1}{2}\right).$$

The left inequality is proved in the same way with the signs reversed. The resulting inequalities are indeed strict, as Hasse's bound is guaranteed not to be tight when, say, $p=2$. □

Note that these bounds are global: they do not depend on the elliptic curve E in any way.

Corollary 5.1.8. *The Dirichlet series and Euler product for $L_E(s)$ converges absolutely for* $\mathrm{Re}(s) > \frac{3}{2}$.

This follows immediately from the fact that $L_E(s)$ is bounded in magnitude by the ζ function shifted a half unit to the left, and the Dirichlet series for $\zeta(s)$ converges for $\mathrm{Re}(s) > 1$.

Corollary 5.1.9. *$\Lambda_E(1+s)$ has no zeros outside the critical strip* $|\mathrm{Re}(s)| \leq \frac{1}{2}$.

Proof. This may be proven via either set of inequalities in the above proposition; we will use the latter. Recall that if f is meromorphic on $\mathbb{C}$, then $\frac{f'}{f}$ has a pole at $s=s_0$ iff f has a zero or pole at s_0; moreover poles of $\frac{f'}{f}$ are simple and have residue equal to the multiplicity of the corresponding zero/pole of f. But by the above $\frac{L_E'}{L_E}(1+s)$ converges absolutely for $\mathrm{Re}(s) > \frac{1}{2}$, so $\frac{\Lambda_E'}{\Lambda_E}(1+s)$ is well-defined and bounded for $\mathrm{Re}(s) > \frac{1}{2}$, and hence cannot have any poles in this region. By symmetry the same is true for $\mathrm{Re}(s) < -\frac{1}{2}$. Hence $\Lambda_E(1+s)$ cannot have any zeros for $|\mathrm{Re}(s)| > \frac{1}{2}$. □

If one assumes GRH, $\Lambda_E(1+s)$ has a particularly simple representation as a product over its zeros, from which we get a representation of $\frac{\Lambda_E'}{\Lambda_E}(1+s)$ as a sum over its zeros.

Proposition 5.1.10 (GRH)**.** *We have*

1.

$$\Lambda_E(1+s) = C_E \cdot s^{r_E} \cdot \prod_{\gamma>0} \left(1 + \frac{s^2}{\gamma^2}\right), \tag{5.1.16}$$

where C_E is the leading coefficient of $L_E(s)$ at the central point (i.e. that defined in Conjecture 3.3.1), and the product is taken over the imaginary parts of all nontrivial zeros of $\Lambda_E(1+s)$ in the upper half plane. The product converges absolutely for any s, and uniformly on any bounded set.

2.

$$\frac{\Lambda_E'}{\Lambda_E}(1+s) = \sum_{\gamma} \frac{s}{s^2+\gamma^2}, \tag{5.1.17}$$

where the sum is taken over the imaginary parts of **all** *nontrivial zeros of $\Lambda_E(1+s)$, including central zeros with multiplicity. The sum converges absolutely for any s outside the set of nontrivial zeros for $L_E(1+s)$, and uniformly on any bounded set outside of the set of zeros.*

Note that by GRH, γ^2 is always a nonnegative real number in any of the above expansions. Furthermore, since noncentral nontrivial zeros occur in conjugate pairs, each term for $\gamma \neq 0$ in Equation 5.1.17 appears exactly twice. It is therefore sometimes useful to rewrite it as

$$\frac{\Lambda_E'}{\Lambda_E}(1+s) = \frac{r_E}{s} + 2\sum_{\gamma>0} \frac{s}{s^2+\gamma^2}, \tag{5.1.18}$$

where r_E is the (analytic) rank of E.

Proof. $\Lambda_E(1+s)$ has a zero of order r_E at the origin, and by GRH all other zeros of $\Lambda_E(1+s)$ are simple, lie on the imaginary axis, and are symmetric about the origin.

Now since $\Lambda_E(1+s)$ is an entire function of finite order, we may express it as a Hadamard product over its zeros. As with the Hadamard product for the completed Riemann Zeta function, the symmetry of $\Lambda_E(1+s)$ simplifies this product to

$$\Lambda_E(1+s) = C_E \cdot s^{r_E} \cdot \prod_{\gamma \neq 0} \left(1 - \frac{s}{i\gamma}\right), \tag{5.1.19}$$

where C_E is the leading nonzero coefficient of the Taylor series for $\Lambda_E(1+s)$ at the central point; and for convergence the product should be taken over conjugate pairs of zeros. Combining conjugate pair terms yields Equation 5.1.16; logarithmic differentiation then yields Equation 5.1.18, which can be simplified to Equation 5.1.17. □

Corollary 5.1.11. $\frac{\Lambda_E'}{\Lambda_E}(1+s)$ *is an odd function.*

Note this result holds independent of GRH.

Lemma 5.1.7 and Equation 5.1.17 may be used to provide a crude bound on the analytic rank of E with respect to its conductor:

Corollary 5.1.12. *Let E have analytic rank $r_{an}(E)$ and conductor N_E. Then*

$$r_{an}(E) < 1.6 + \frac{1}{2}\log N_E. \tag{5.1.20}$$

Moreover, this bound is unconditional; it does not require GRH to hold.

Proof. We begin by assuming GRH. From Equation 5.1.17 we have the point estimate

$$r_{an} < \sum_{\gamma} \frac{1}{1+\gamma^2} = \frac{\Lambda_E'}{\Lambda_E}(2), \tag{5.1.21}$$

while from Lemma 5.1.7 we get

$$\frac{\Lambda_E'}{\Lambda_E}(2) = \log\left(\frac{\sqrt{N_E}}{2\pi}\right) + \digamma(2) + \frac{L_E'}{L_E}(2) < \frac{1}{2}\log N_E - \log 2\pi + 1 - \eta - 2\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right), \tag{5.1.22}$$

where $\digamma(s)$ is the digamma function on $\mathbb{C}$ and η is the Euler-Mascheroni constant $= 0.5772156649\ldots$. Collect constant terms and round up to get the stated bound.

If one does not assume GRH, then we must use a less simplified representation for the logarithmic derivative:

$$\frac{\Lambda_E'}{\Lambda_E}(1+s) = \sum_\rho \frac{1}{2}\left(\frac{1}{s-\rho} + \frac{1}{s-\bar{\rho}}\right), \tag{5.1.23}$$

where ρ ranges over the nontrivial zeros of $L_E(1+s)$. However, everything else proceeds as before, and the point estimate given in Equation 5.1.21 still holds. □

We will later use a related technique to show firstly that the factor in front of $\log N_E$ can be made arbitrarily small, at the expense of having to assume GRH and having to increase the added constant.

The following corollary of Proposition 5.1.10 will be of import in obtaining explicit bounds on the number of zeros of $L_E(s)$ in a given interval on the critical strip:

Corollary 5.1.13 (GRH)**.** *Let* $\mathrm{Re}(s) > 0$*, and write* $s = \sigma + i\tau$*, i.e.* $\sigma > 0$*. Then*

$$\sum_\gamma \frac{\sigma}{\sigma^2 + (\gamma-\tau)^2} = \mathrm{Re}\left(\frac{\Lambda_E'}{\Lambda_E}(1+s)\right), \tag{5.1.24}$$

where again the sum is taken over all nontrivial zeros of $L_E(s)$*. The sum converges absolutely for any* $\tau \in \mathbb{R}$ *and* $\sigma > 0$*.*

Proof. By equation 5.1.17 we have

$$\begin{aligned}
\mathrm{Re}\left(\frac{\Lambda_E'}{\Lambda_E}(1+s)\right) &= \mathrm{Re}\left(\sum_\gamma \frac{s}{s^2+\gamma^2}\right) \\
&= \frac{1}{2}\sum_\gamma \mathrm{Re}\left(\frac{1}{s-i\gamma} + \frac{1}{s+i\gamma}\right) \\
&= \frac{1}{2}\sum_\gamma \frac{\sigma}{\sigma^2+(\gamma-\tau)^2} + \frac{\sigma}{\sigma^2+(\gamma+\tau)^2}.
\end{aligned}$$

However, absolute convergence for $\sum_\gamma \frac{s}{s^2+\gamma^2}$ for any s in the right half plane implies absolute

convergence for the individual sums $\sum_\gamma \frac{\sigma}{\sigma^2+(\gamma-\tau)^2}$ and $\sum_\gamma \frac{\sigma}{\sigma^2+(\gamma+\tau)^2}$. We may thus write

$$\begin{aligned}\mathrm{Re}\left(\frac{\Lambda_E'}{\Lambda_E}(1+s)\right) &= \frac{1}{2}\sum_\gamma \frac{\sigma}{\sigma^2+(\gamma-\tau)^2} + \frac{1}{2}\sum_\gamma \frac{\sigma}{\sigma^2+(\gamma+\tau)^2} \\ &= \sum_\gamma \frac{\sigma}{\sigma^2+(\gamma-\tau)^2} \quad \text{by symmetry.}\end{aligned}$$

□

Observe that GRH implies that $\mathrm{Re}(\frac{\Lambda_E'}{\Lambda_E}(1+s)) > 0$ for $\mathrm{Re}(s) > 0$, since then each of the terms in the above sum are strictly positive. By oddness of $\frac{\Lambda_E'}{\Lambda_E}(1+s)$ we also then have that $\mathrm{Re}(\frac{\Lambda_E'}{\Lambda_E}(1+s)) < 0$ for all $\mathrm{Re}(s) < 0$, and $\mathrm{Re}(\frac{\Lambda_E'}{\Lambda_E}(1+s)) = 0 \Rightarrow \mathrm{Re}(s) = 0$.

5.2 The Explicit Formula for Elliptic Curves

Combining equations 5.1.2, 5.1.3 and 5.1.17 we get the following equality:

Proposition 5.2.1 (GRH). *Let $E/\mathbb{Q}$ have conductor N_E. Let γ range over all nontrivial zeros of $L_E(s)$ with multiplicity, let η be the Euler-Mascheroni constant, and let the $c_n = c_n(E)$ be as given by definitions 5.1.3 and 5.1.6. Then*

$$\sum_{\gamma} \frac{s}{s^2+\gamma^2} = \left[-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right] + \sum_{k=1}^{\infty} \frac{s}{k(s+k)} + \sum_{n=1}^{\infty} c_n n^{-s}. \tag{5.2.1}$$

This is the prototypical *explicit formula* for elliptic curves: an equation relating a sum over the nontrivial zeros of $L_E(s)$ to a sum over the logarithmic derivative coefficients of $L_E(s)$, plus some easily smooth part that only depends on the curve's conductor.

In general, the phrase "explicit formula" is not applied to a specific equation, but rather to a suite of equalities that resemble the above in some way. We reproduce Lemma 2.1 from [6], which is a more general version of the explicit formula, akin to the Weil formulation of the Riemann-von Mangoldt explicit formula for $\zeta(s)$.

Lemma 5.2.2 (GRH). *Suppose that $f(z)$ is an entire function s.t. there exists a $\delta > 0$ such that $f(x+iy) = O(x^{-(1+\delta)})$ for $|y| < 1+\epsilon$ for some $\epsilon > 0$. Suppose that the Fourier transform of f*

$$\hat{f}(y) = \int_{-\infty}^{\infty} e^{-ixy} f(x)\, dx \tag{5.2.2}$$

exists and is such that $\sum_{n=1}^{\infty} c_n \hat{f}\,(\log n)$ converges absolutely. Then

$$\sum_{\gamma} f(\gamma) = \frac{1}{\pi}\left[\log\left(\frac{\sqrt{N_E}}{2\pi}\right)\hat{f}(0) + \mathrm{Re}\int_{-\infty}^{\infty} \digamma(1+it) f(t)\, dt + \frac{1}{2}\sum_{n=1}^{\infty} c_n \left(\hat{f}\,(\log n) + \hat{f}\,(-\log n)\right)\right]. \tag{5.2.3}$$

A proof can be found in [20, Theorem 5.12]. Note that Equation 5.2.1 can be recovered by setting f to be the Poisson kernel $f_s(x) = \frac{s}{s^2+x^2}$; then $\hat{f}_s(y) = e^{-s|y|}$, so $\hat{f}_s(\log n) = n^{-s}$.

We give a distribution-theoretic reformulation of Lemma 5.2.2. While the subject of explicit formulae for L-functions of Hecke eigenforms is treated by a number of sources, the following doesn't seem to have been explicitly written down in the literature anywhere:

Proposition 5.2.3 (GRH)**.** *Let γ 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 the zeros of $L_E(s)$, where $\delta(x)$ is the usual Dirac delta function. That is, for any test function $f : \mathbb{R} \mapsto \mathbb{C}$ such that $\sum_\gamma f(\gamma)$ converges,*

$$\langle f, \varphi_E \rangle = \int_{-\infty}^{\infty} f(x) \left(\sum_{\gamma \in S_E} \delta(x-\gamma) \right) dx = \sum_{\gamma \in S_E} f(\gamma). \tag{5.2.4}$$

Then as distributions,

$$\varphi_E = \sum_\gamma \delta(x-\gamma) = \frac{1}{\pi} \left[-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi} \right) + \sum_{k=1}^{\infty} \frac{x^2}{k(k^2+x^2)} + \frac{1}{2} \sum_{n=1}^{\infty} c_n \left(n^{ix} + n^{-ix} \right) \right]. \tag{5.2.5}$$

In the above language, $\frac{\Lambda_E'}{\Lambda_E}(1+s) = \left\langle \frac{s}{s^2+x^2}, \varphi_E \right\rangle$ for $\mathrm{Re}(s) > 0$. Note that convergence on the right hand side is absolute for $\mathrm{Re}(s) > 1$, and conditional (provably so thanks to Sato-Tate) for $0 < \mathrm{Re}(s) \leq 1$.

5.3 Estimating Analytic Rank with the sinc^2 Sum

The Explicit Formula may be used to provide computationally effective upper bounds on the analytic rank of an elliptic curve. The method appears to have first been formulated by Mestre in [28], and used by Brumer in [9] to prove that, conditional on GRH, the average rank of elliptic curves was at most 2.3. This upper bound was improved to 2 by Heath-Brown in [17].

[Aside: one of the most groundbreaking developments in number theory in recent years is a series of results by Manjul Bhargava and Arul Shankar [2] [3] [4] proving that the average rank of elliptic curves is at most 0.885. These results are *unconditional*; the first such unconditional bound on average rank. For his work Bhargava received a Fields Medal in 2014.]

The analytic method stems from invoking the explicit formula as stated in Lemma 5.2.2 on a function f of a specific form:

Lemma 5.3.1 (GRH)**.** *Let γ range over the nontrivial zeros of $L_E(s)$. Let f be a non-negative even real-valued function on $\mathbb{R}$ such that $f(0) = 1$. Suppose further that the Fourier transform $\hat{f}$ of f has compact support, i.e. $\hat{f}(y) = 0$ for $|y| > R$ for some $R > 0$. Then for any $\Delta > 0$, we have*

$$\sum_{\gamma} f(\Delta\gamma) = \frac{1}{\Delta\pi}\log\left(\frac{\sqrt{N_E}}{2\pi}\right) + \mathrm{Re}\int_{-\infty}^{\infty} \Gamma(1+it) f(\Delta t)\, dt + \frac{1}{\Delta\pi}\sum_{n<e^{\Delta R}} c_n \hat{f}\left(\frac{\log n}{\Delta}\right). \quad (5.3.1)$$

Moreover, the value of the sum bounds from above the analytic rank of E for any given value of Δ, and sum converges to $r_{\mathrm{an}}(E)$ as $\Delta \to \infty$.

Proof. The formula as stated above is just an application of the explicit formula in Lemma 5.2.2, noting that the Fourier transform of $f(\Delta x)$ is $\frac{1}{\Delta}\hat{f}\left(\frac{\xi}{\Delta}\right)$. Since f is 1 at the origin, $\sum_\gamma f(\Delta\gamma) = r_E + \sum_{\gamma\neq 0} f(\Delta\gamma)$. Furthermore, f is non-negative and integrable, so the sum over noncentral zeros is nonnegative and decreases to zero as Δ increases. □

While in theory any f with the properties mentioned above work for bounding analytic

rank, the function

$$f(x) = \operatorname{sinc}^2(x) = \left(\frac{\sin(\pi x)}{\pi x}\right)^2 \tag{5.3.2}$$

is what is used by Mestre, Brumer, Heath-Brown in the publications above, and by Bober in [6]. This is due to its Fourier transform being compactly supported, namely is the triangular function:

$$\hat{f}(y) = \int_{-\infty}^{\infty} e^{-ixy} f(x)\, dx = \begin{cases} 1 - \frac{|y|}{2\pi}, & |y| \le 2\pi \\ 0, & |y| > 2\pi. \end{cases} \tag{5.3.3}$$

Moreover, if $f(x) = \operatorname{sinc}^2(x)$, the integral $\operatorname{Re} \int_{-\infty}^{\infty} \digamma(1+it) f(\Delta t)\, dt$ can be computed explicitly in terms of known constants and special functions:

$$\operatorname{Re} \int_{-\infty}^{\infty} \digamma(1+it) f(\Delta t)\, dt = -\frac{\eta}{\pi\Delta} + \frac{1}{2\pi^2\Delta^2}\left(\frac{\pi^2}{6} - \operatorname{Li}_2\left(e^{-2\pi\Delta}\right)\right), \tag{5.3.4}$$

where η is the Euler-Mascheroni constant $= 0.5772\ldots$ and $\operatorname{Li}_2(x)$ is the dilogarithm function, defined as $\operatorname{Li}_2(x) = \sum_{k=1}^{\infty} \frac{x^k}{k^2}$ for $|x| \le 1$.

Combining the above, we get a specialization of Lemma 5.3.1:

Corollary 5.3.2 (GRH)**.** *Let γ range over the nontrivial zeros of $L_E(s)$, and let $\Delta > 0$. Then*

$$\begin{aligned} \sum_{\gamma} \operatorname{sinc}^2(\Delta\gamma) = \quad & \frac{1}{\Delta\pi}\left[\left(-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right) + \frac{1}{2\pi\Delta}\left(\frac{\pi^2}{6} - \operatorname{Li}_2\left(e^{-2\pi\Delta}\right)\right)\right. \\ & \left. + \sum_{n < e^{2\pi\Delta}} c_n \cdot \left(1 - \frac{\log n}{2\pi\Delta}\right)\right]. \end{aligned} \tag{5.3.5}$$

What's notable about the above formula is that evaluation of the right hand side is a finite computation, and only requires knowledge of the elliptic curve's conductor and its a_p values up to some bound. Thus the zero sum is eminently computable, and results in a value that bounds from above the analytic rank of E.

The sinc^2 zero sum rank estimation method has been implemented in Sage (see Appendix A), and used to successfully estimate ranks on a database of 18 million elliptic curves with

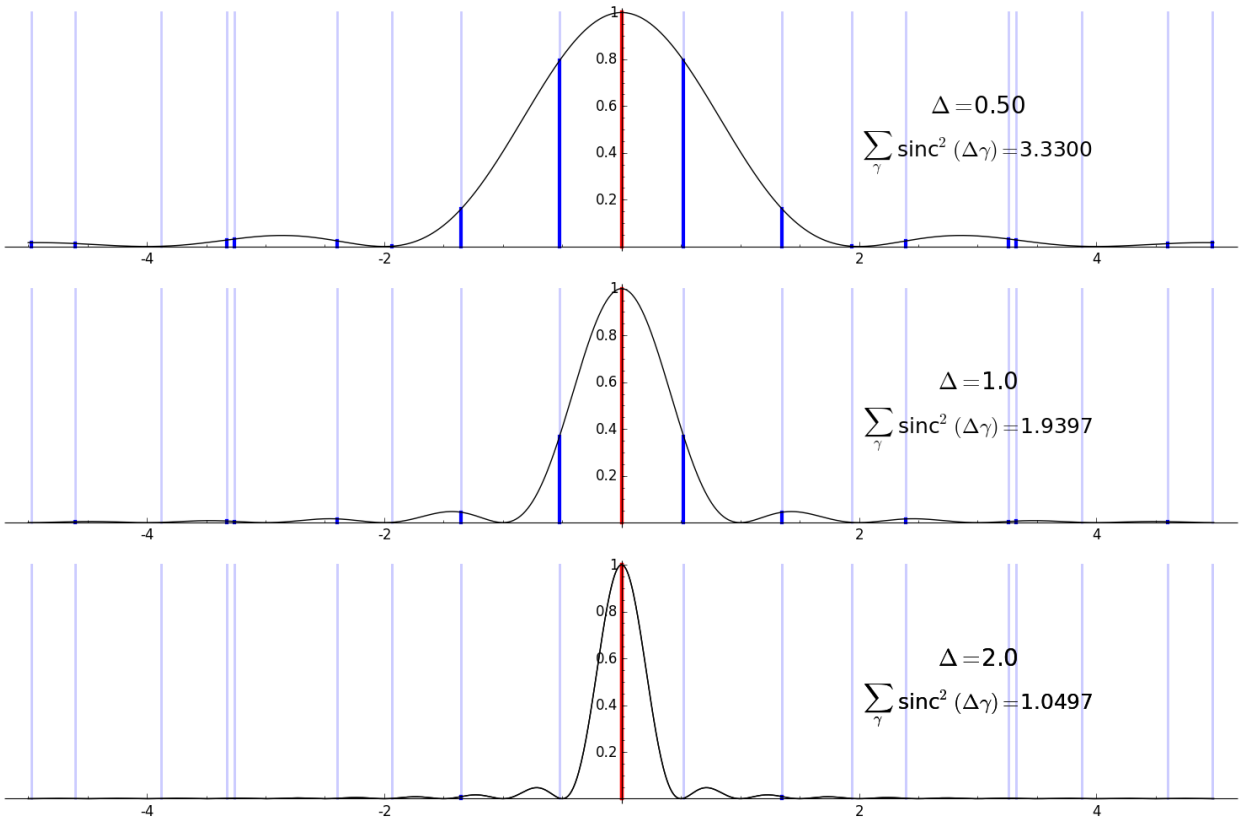

Figure 5.3.1: A graphic representation of the sinc^2 sum for the elliptic curve $E : y^2 = x^3 - 18x + 51$, a rank 1 curve with conductor $N_E = 750384$, for three increasing values of the parameter Δ. Vertical lines have been plotted at $x = \gamma$ whenever $L_E(1 + i\gamma) = 0$ – red for the single central zero, and blue for noncentral zeros; the height of the darkened portion of each line is given by the black curve $\text{sinc}^2(\Delta x)$. Summing up the lengths of the dark vertical lines thus gives the value of the sinc^2 sum. We see that as Δ increases, the contribution from the blue lines – corresponding to noncentral zeros – goes to zero, while the contribution from the central zero in red remains at 1. Thus the sum must limit to 1 as Δ increases.

conductor at most $\sim 10^{11}$. A range of Δ values was used, from $\Delta = 1.0$ (for which average time per curve was $\sim 10^{-5}$ s), to $\Delta = 2.0$ (average time per curve $\sim 10^{-1}$ s). See an upcoming paper by Ho, Balakrishnan, Kaplan, Stein, Weigandt, and S. for details on the computations.

A neat conclusion that can immediately be drawn from the finiteness of the sinc^2 explicit formula sum, is that maximum analytic rank grows more slowly than $\log N_E$:

Corollary 5.3.3 (GRH)**.** *For any $\epsilon > 0$ there is a constant $K_\epsilon > 0$ such that for any $E/\mathbb{Q}$ with conductor N_E, we have*

$$r_E < \epsilon \log N_E + K_\epsilon. \tag{5.3.6}$$

Proof. We note that for any given $\Delta > 0$, the sum $\sum_{n<e^{2\pi\Delta}} c_n \cdot \left(1 - \frac{\log n}{2\pi\Delta}\right)$ is bounded by a constant that is independent of the choice of elliptic curve, as the c_n values are bounded globally. Thus the right hand side of Equation 5.3.5 is equal to $\frac{1}{2\pi\Delta} \log N_E$ plus a number whose supremum magnitude depends only on Δ and not on E. Since the sum bounds analytic rank, taking $\epsilon = \frac{1}{2\pi\Delta}$ and letting $\epsilon \to 0$ proves the statement. □

[Aside: This statement is already known in the literature, so nothing new has been proven here. In fact, it's conjectured that maximum analytic rank grows more like $\sqrt{\log N_E}$ (existing numerical evidence would seem to support this), but this is still very much an open problem.]

The above allows us to provide bounds on analytic rank via point estimates by choosing particular values of ϵ. For example, if we choose $\epsilon = \frac{1}{\log 23} \sim 0.3189\ldots$ and collect and bound all the conductor-independent terms in equation 5.3.5, we can improve the result in Corollary 5.1.12 to the following:

Corollary 5.3.4 (GRH)**.** *Let E have analytic rank r_E and conductor N_E. Then*

$$r_E < 0.32 \log N_E + 0.5. \tag{5.3.7}$$

We leave the details of the proof to the reader as a fun analysis exercise.

Finally, it's worth noting is that when $\Delta \leq \frac{\log 2}{2\pi}$, the c_n sum in Equation 5.3.5 is empty. Thus we have the following:

Corollary 5.3.5 (GRH)**.** *Let $E/\mathbb{Q}$ have conductor N_E. Let η be the Euler-Mascheroni constant $= 0.5772\ldots$, and let γ range over the nontrivial zeros of $L_E(s)$. Then*

$$\sum_{\gamma} \operatorname{sinc}^2\left(\frac{\log 2}{2\pi} \cdot \gamma\right) = \frac{\log N_E}{\log 2} + K, \tag{5.3.8}$$

where $K = \frac{\pi^2}{6(\log 2)^2} - \frac{2\eta}{\log 2} - 2\frac{\log \pi}{\log 2} - 1 = -2.54476987\ldots$ is a global constant that is independent of E.

Proof. Evaluate Equation 5.3.5 at $\Delta = \frac{\log 2}{2\pi}$ and simplify, noting that $\operatorname{Li}_2\left(\frac{1}{2}\right) = \frac{\pi^2}{6} - \frac{(\log 2)^2}{2}$. □

5.4 Rank Estimation Fidelity and Choosing how to Scale Δ

Observe that for a fixed choice of Δ, evaluating Equation 5.3.5 has runtime that is almost independent of the conductor of E (it should scale with some power of $\log N_E$ due to the complexity of basic arithmetic operations). However, as conductor increases the tightness of the provided bound decreases – we can see this from the first term, which adds a positive bias to the sum proportion to $\log N_E$, which is not seen in the average ranks of curves as conductor increases.

Definition 5.4.1. The *fidelity* of a sinc^2 sum rank estimation with a given choice of Δ, is the average tightness of the rank bound as a function of conductor of the curve in question. Specifically, we may define

$$\text{fid}(\Delta, N) = \text{mean}\left\{ \left(\sum_{\Lambda_E(1+i\gamma)=0} \text{sinc}^2(\gamma\Delta) \right) - r_E : \quad N_E = N \right\}, \tag{5.4.1}$$

where E ranges over all rational elliptic curves with conductor N. Loosely, we may think of the fidelity of a given choice of Δ and N to be the expected accuracy of the rank estimate, or the chance that the sum is tight (e.g. within 2 of the true rank, since we are always assuming parity is known) for a curve of conductor $N_E = N$.

In other words, for fixed curves fidelity increases as Δ increases, but for fixed Δ fidelity *decreases* as the conductor of the curve in question increases. It follows that Δ should scale with N_E in order to obtain an estimates of constant fidelity. The natural question to ask then, given the statement of Equation 5.3.5, is: how large does Δ need to be such that $\sum_{\Lambda_E(1+i\gamma)=0} \text{sinc}^2(\gamma\Delta) < r_E + 2$?

Evaluating the sum will be dominated by the final sum over the c_n coefficients, whose runtime in turn is exponential in Δ, so we must be judicious in the choice of Δ. Experimentally, we found that choosing $\Delta(E) = \alpha \cdot \log N_E$ for any constant value of α produces

estimates of asymptotically constant fidelity. Such a choice makes the contribution from the first two terms in Equation 5.3.5 – $\frac{1}{\Delta\pi}\left(-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right) + \frac{1}{2\pi^2\Delta^2}\left(\frac{\pi^2}{6} - \mathrm{Li}_2\left(e^{-2\pi\Delta}\right)\right)$ – asymptotically constant, so net bias in the sum does not increase as N_E increases.

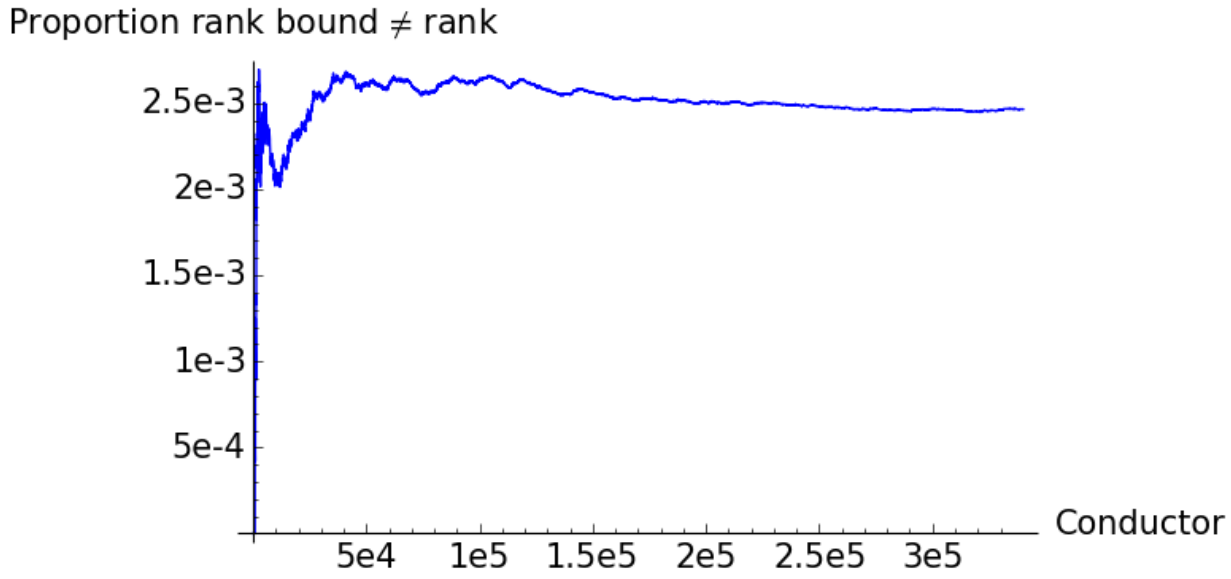

Figure 5.4.1: The cumulative proportion of curves in the Cremona database for which the sinc^2 rank bound was not within 2 of the true rank of the curve, using the scaling $\Delta(E) = \frac{1}{\pi}\left(-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right)$.

To generate Figure 5.4.1, we used the scaling $\Delta(E) = \frac{1}{\pi}\left(-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right)$, and computed rank bounds on the entire Cremona database of all rational elliptic curves up to conductor 350000; this scaling was chosen so that the bias coming from the first term in the sinc^2 sum was always exactly 1. It was found that the resulting bounds were within 2 of the true rank in 99.75% of cases. The 4000 or so curves for which the bound exceeded $r_E + 2$ all possess anomalously low-lying zeros that 'look like central zeros' when small values of Δ are used.

Since the number of terms in the c_n sum in Equation 5.3.5 is $e^{2\pi\Delta}$, choosing $\Delta(E) =$

$\alpha \cdot \log N_E$ means that the evaluating the sum will have $\tilde{O}\left((N_E)^{2\pi\alpha}\right)$ runtime. That is, the scaling choice used to generate Figure 5.4.1 yielded an $\tilde{O}(N_E)$ computation time. In general, runtime can be made to be $\tilde{O}\left((N_E)^{\epsilon}\right)$ for any $\epsilon > 0$, at the expense of lowering the fidelity of the bound.

It is worth noting explicitly that the accuracy of the sinc^2 sum rank estimate is sensitive to low-lying zeros. Thus if it known a priori that the L-function of a particular curve does not have any low-lying zeros, a smaller value of Δ can be used. This fact is exploited in [6], where Bober uses the method on curves of very large rank. There is a well-known phenomenon of zero repulsion in L-functions – zeros tend not to fall as close to each other as could be expected if they were distributed purely randomly on the critical line – and as such curves with large rank tend to have lowest zeros significantly higher up in the upper half plane than would be expected otherwise.

This, for example, allowed Bober to use a Δ value of only 3.2 to show that a curve with 28 independent points had analytic rank at most 30. The conductor of the curve in question is roughly 3.4×10^{141}, so using the scaling $\Delta(E) = \frac{1}{\pi}\left(-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right)$ would require a Δ value of about 51.1.

A related question we can of course ask is: how large does Δ have to be for the sinc^2 sum rank bound to have perfect fidelity, i.e. guaranteed to be less than 1 more than the rank of E? We will answer this question at the end of section 5.6, though in a way that requires knowledge of an extra invariant attached to E, namely the bite β_E.

5.5 The Distribution of Nontrivial Zeros

Though not necessary to prove Equation 5.3.5, we may also use zero sums to provide bounds on the density and estimates on the distribution and expected location of the nontrivial zeros of $L_E(s)$ as a function of the curve's conductor.

5.5.1 Explicit Bounds on Zero Density on the Critical Line

We start by investigating the density of zeros on the critical line. We will see that zero density scales with $\log N_E$; because the explicit formula is used extensively in this section, all results are of course taken to be contingent on GRH.

To this end, we define the *zero counting function*, which counts the number of zeros on the critical line up to a given bound:

Definition 5.5.1. For non-negative t, let $M_E(t)$ be the modified non-trivial zero counting function for $L_E(s)$, i.e.

$$M_E(t) := \sum_{|\gamma| \leq t}{}' \frac{1}{2}, \tag{5.5.1}$$

where γ runs over the imaginary parts of nontrivial zeros of $L_E(s)$, and the prime indicates that the final γ is taken with half weight if $\gamma = t$. The central zero is taken with with multiplicity r_E, where r_E is the analytic rank of E.

Note that $M_E(0) = \frac{r_E}{2}$, and the function jumps by 1 across the locations of nontrivial zeros, since noncentral zeros come in conjugate pairs and (by GRH) are always simple.

We may obtain bounds on $M_E(t)$ via the shifted completed logarithmic derivative $\frac{\Lambda_E'}{\Lambda_E}(1+s)$. Our workhorse theorem places tight constraints on the sum $\sum_\gamma \frac{\sigma}{\sigma^2+(\gamma-\tau)^2}$ for positive σ and real τ. This is a shifted Cauchy distribution-type sum, giving us information on the density of zeros with imaginary part near τ.

Theorem 5.5.2 (GRH)**.** *Let E be an elliptic curve with conductor N_E and L-function $L_E(s)$. Let $\sigma > \frac{1}{2}$ and $\tau \in \mathbb{R}$, and let γ range over the imaginary parts of the nontrivial zeros of $L_E(s)$. Then*

$$\left| \sum_{\gamma} \frac{\sigma}{\sigma^2 + (\gamma - \tau)^2} - \left[\log\left(\frac{\sqrt{N_E}}{2\pi} \right) + \operatorname{Re}\left(\digamma(1 + \sigma + i\tau) \right) \right] \right| < -2\frac{\zeta'}{\zeta}\left(\frac{1}{2} + \sigma \right). \tag{5.5.2}$$

Proof. Let $s = \sigma + i\tau$. By equations 5.1.2 and 5.1.13 we have

$$\begin{aligned} \sum_{\gamma} \frac{\sigma}{\sigma^2 + (\gamma - \tau)^2} &= \operatorname{Re}\left(\frac{\Lambda_E'}{\Lambda_E}(1 + s) \right) \\ &= \log\left(\frac{\sqrt{N_E}}{2\pi} \right) + \operatorname{Re}\left(\digamma(1 + \sigma + i\tau) \right) + \operatorname{Re}\left(\sum_n c_n n^{-s} \right). \end{aligned}$$

But by lemma 5.1.7

$$\left| \operatorname{Re}\left(\sum_n c_n n^{-s} \right) \right| \leq \left| \frac{L_E'}{L_E}(1 + s) \right| < -2\frac{\zeta'}{\zeta}\left(\frac{1}{2} + \sigma \right),$$

so

$$\left| \sum_{\gamma} \frac{\sigma}{\sigma^2 + (\gamma - \tau)^2} - \log\left(\frac{\sqrt{N_E}}{2\pi} \right) - \operatorname{Re}\left(\digamma(1 + \sigma + i\tau) \right) \right| < -2\frac{\zeta'}{\zeta}\left(\frac{1}{2} + \sigma \right).$$

□

Note that $\frac{\zeta'}{\zeta}$ decays rapidly with increasing σ, i.e. we have

$$\sum_{\gamma} \frac{\sigma}{\sigma^2 + (\gamma - \tau)^2} - \left[\log\left(\frac{\sqrt{N_E}}{2\pi} \right) + \operatorname{Re}\left(\digamma(1 + \sigma + i\tau) \right) \right] = O(\sigma^{-c})$$

for any $c > 0$.

Corollary 5.5.3 (GRH)**.** *Let $M_E(t)$ be the zero counting function as given in Definition 5.5.1. Then for $t \geq 1$ we have*

$$M_E(t) \leq t \log N_E + 2t \log(t + 1). \tag{5.5.3}$$

If we restrict to $t > 1.32$ we may further simplify this to

$$M_E(t) \leq t \log N_E + 2t \log t. \tag{5.5.4}$$

Proof. Take the right inequality in Theorem 5.5.2 with $\sigma = t$ and $\tau = 0$, yielding

$$\sum_{\gamma} \frac{t}{t^2+\gamma^2} \leq \frac{1}{2}\log N_E - \log 2\pi + \Re\digamma(1+t) - 2\frac{\zeta'}{\zeta}\left(\frac{1}{2}+t\right),$$

since the digamma function is real on the real axis.

Note that for $t \geq 1$ we have $-\frac{\zeta'}{\zeta}\left(\frac{1}{2}+t\right) < -\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right) = 1.50523\ldots$, since $-\frac{\zeta'}{\zeta}$ is decreasing with increasing t. Observe that this does not exceed $\log 2\pi = 1.83787\ldots$

Now $\Re\digamma(1+t) < \log(1+t)$ for $t \geq 0$. For the second inequality in the theorem, note that $-\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right) - \log 2\pi = 0.33264\ldots$, and $\Re\digamma(1+t) \leq \log(t) + 0.33264\ldots$ when $t \geq 1.32255\ldots$

Finally, we have that $\sum_{\gamma} \frac{t}{t^2+\gamma^2} \geq \frac{1}{2t} M_E(t)$, since all zeros in the interval $[-t,t]$ are counted with weight at least $\frac{1}{2t}$. Combining the above observations and collecting constants completes the proof. □

It is also useful to have an upper bound on the number of zeros in a given unit interval on the critical line.

Corollary 5.5.4 (GRH)**.** *For $t \geq 1$, $M_E(t+1) - M_E(t)$ gives the number of zeros γ with $t < |\operatorname{Im}(\gamma)| \leq t+1$. We have*

$$M_E(t+1) - M_E(t) < \frac{5}{4}\log(N_E) + \frac{5}{2}\log(t+1). \tag{5.5.5}$$

Proof. Proceed as before, but now taking the right inequality in theorem 5.5.2 with $\sigma = 1$ and $\tau = t + \frac{1}{2}$. Observe that

$$\sum_{\gamma} \frac{1}{1+\left(\gamma - t - \frac{1}{2}\right)^2} \geq \frac{4}{5} \cdot \frac{(M_E(t+1) - M_E(t))}{2},$$

since we are only counting zeros in the upper half plane. Also note that similar to before, $\Re\digamma\left(\frac{3}{2} + i\left(t+\frac{1}{2}\right)\right) - \log 2\pi - 2\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right) < \log(t+1)$ for $t \geq 1$. □

In a similar manner we derive for $t \geq 1$ that

$$\#\{\gamma : |\gamma - t| \leq 1\} < \log(N_E) + 2\log(t+1) \tag{5.5.6}$$

(note that unlike equation 5.5.5, the above only considers zeros with non-negative imaginary part).

Finally, recall the definition of the bite of E: $\beta_E = \sum_{\gamma \neq 0} \frac{1}{\gamma^2}$. We may use 5.5.2 to place an explicit bound on the tail end of the inverse square sum via the following:

Corollary 5.5.5 (GRH)**.** *For $\sigma \geq 1$ and $\tau \in \mathbb{R}$ we have*

$$\sum_{|\gamma - \tau| > \sigma} \frac{1}{(\gamma - \tau)^2} \leq \frac{\log(N_E) + 2\log(|\tau| + 1)}{\sigma}. \tag{5.5.7}$$

Specifically, when $\tau = 0$ we have

$$\sum_{|\gamma| > \sigma} \frac{1}{\gamma^2} \leq \frac{\log(N_E)}{\sigma}. \tag{5.5.8}$$

Proof. Observe that

$$\frac{\sigma}{2} \cdot \sum_{|\gamma - \tau| > \sigma} \frac{1}{(\gamma - \tau)^2} \leq \sum_{|\gamma - \tau| > \sigma} \frac{\sigma}{\sigma^2 + (\gamma - \tau)^2} \leq \sum_{\gamma} \frac{\sigma}{\sigma^2 + (\gamma - \tau)^2},$$

and the rightmost sum is bounded by $\frac{1}{2}\log N_E + \log(|\tau| + 1)$ as in the work above.

□

Equation 5.5.2 may also used to put lower bounds on the above quantities in some cases, which we hope to pursue in future work.

5.5.2 The Expected Number of Zeros up to t

Corollary 5.5.3 gives us explicit bounds on zero density, but the bound of $t \log N_E$ is not tight: empirically we see $M_E(t)$ grow more like $\frac{t}{2} \log N_E$; i.e. a factor of 2 slower. We may again use the explicit formula to come up with a more accurate expansion for the zero counting function, at the expense of have a more nebulous error term that resists attempts to put explicit bounds on it.

Proposition 5.5.6 (GRH)**.** *We have*

$$M_E(t) = \frac{1}{\pi}\left[\left(-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right)t + \sum_{k=1}^{\infty}\left(\frac{t}{k} - \arctan\left(\frac{t}{k}\right)\right) + \sum_{n=1}^{\infty}\frac{c_n}{\log n}\cdot\sin(t\log n)\right]. \tag{5.5.9}$$

Convergence on the RHS is pointwise with respect to t for both sums; for fixed t convergence for the sums over k and n is absolute and conditional respectively (and extremely slow for the latter).

Proof. Observe we may write $M_E(t) = \sum_\gamma f_t(\gamma)$, where

$$f_t(x) = \begin{cases} \frac{1}{2}, & |x| < t \\ \frac{1}{4}, & |x| = t \\ 0 & |x| > t. \end{cases} \tag{5.5.10}$$

Informally, we obtain the above formula by integrating both sides of Equation 5.2.5 against $f = f_t(x)$, noting that $\hat{f}_t(y) = \frac{\sin(ty)}{y}$. The integrals in the sum over k give us no issue and we may swap the order of the integral and summation signs, since convergence there is absolute. However, some care must be taken when it comes to the sum over n, since here convergence is only conditional.

Formally, we must write $M_E(t)$ as a path integral of $\frac{\Lambda_E'}{\Lambda_E}(1+s)$ on the path

$$\epsilon - it \mapsto \epsilon + it \mapsto -\epsilon + it \mapsto -\epsilon - it \mapsto \epsilon - it$$

for some $\epsilon > 0$, and invoke the Cauchy Residue Theorem. We may then shrink ϵ to zero (assuming GRH) to obtain that the RHS of 5.5.9 converges point wise to $M_E(t)$ as m and $n \to \infty$. □

Equation 5.5.9 may be though of having two components. The first two terms comprise a smooth part that gives the "expected number of zeros" up to t; and the trigonometric sum over n comprises the discretization information that yields the zeros' exact values relative to their general expected location. We expect the trigonometric sum to be zero infinitely often, and asymptotically it should be positive as often as it is negative. As such the sum should average out to zero and shouldn't contribute any asymptotic bias to the density of zeros on the critical line. We can therefore talk in a real sense of the expected number of zeros up to t, which is given by

$$\frac{1}{\pi}\left[\left(-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right)t + \sum_{k=1}^{\infty}\left(\frac{t}{k} - \arctan\left(\frac{t}{k}\right)\right)\right]. \tag{5.5.11}$$

Moreover, the trigonometric sum should grow very slowly with t. Put more formally, we have the following:

Conjecture 5.5.7 (GRH)**.** *GRH implies that*

$$\sum_{n=1}^{\infty}\frac{c_n}{\log n}\cdot\sin(t\log n) = O(\log t). \tag{5.5.12}$$

We won't say much more about bounding the error term in this thesis (or attempt to prove anything about its magnitude), since it requires more advanced analytical tools not mentioned or developed here.

Lemma 5.5.8. *For $t \gg 0$,*

$$\sum_{k=1}^{\infty}\left(\frac{t}{k} - \arctan\left(\frac{t}{k}\right)\right) = t\log t + (\eta - 1)t + \frac{\pi}{4} + O\left(\frac{1}{t}\right), \tag{5.5.13}$$

where $\eta = 0.5772\ldots$ is the Euler-Mascheroni constant.

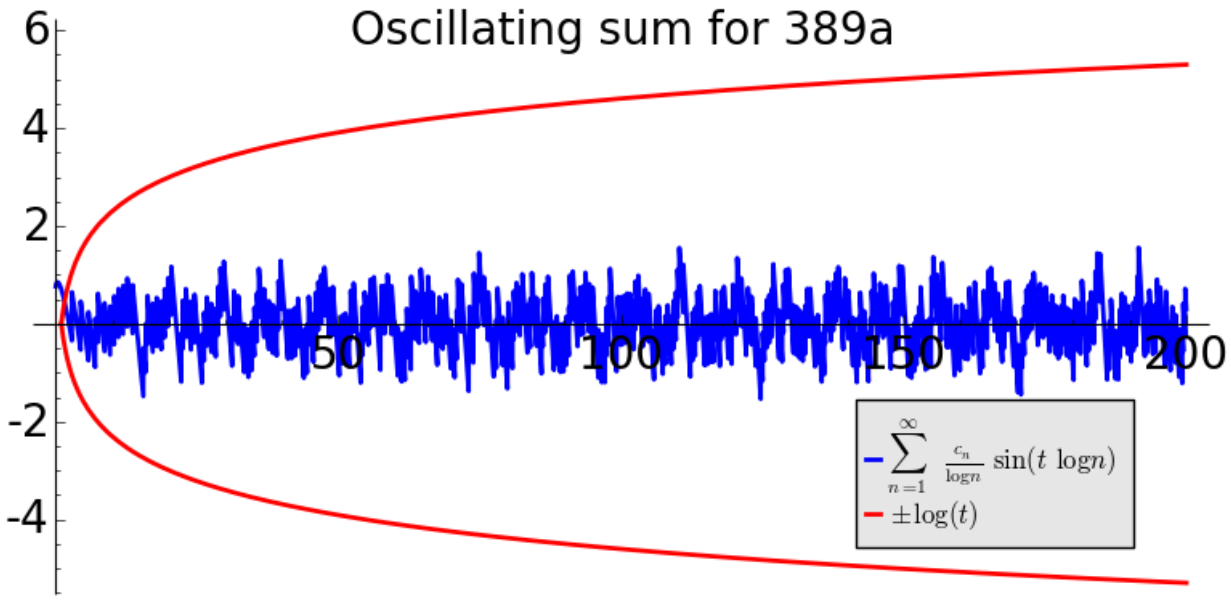

Figure 5.5.1: The oscillating sum $\sum_{n=1}^{\infty} \frac{c_n}{\log n} \cdot \sin(t \log n)$ for the curve with Cremona label $389a$ (with equation $y^2 + y = x^3 + x^2 - 2x$) versus $\pm \log(t)$ for $0 \leq t \leq 200$. Numerically we actually see the maximum value of the sum grow slower than $\log(t)$ - possibly $\log(t)^{\alpha}$ for some $0 < \alpha < 1$, or even $\log \log(t)$.

Proof. We have

$$\sum_{k=1}^{\infty} \left(\frac{t}{k} - \arctan\left(\frac{t}{k}\right) \right) = \int_0^t \sum_{k=1}^{\infty} \frac{x^2}{k(k^2+x^2)} \, dx = \int_0^t \mathrm{Re}\left(\digamma(1+ix) + \eta\right) \, dx,$$

where $\digamma(z)$ is the digamma function on $\mathbb{C}$. Now along the critical line we have the following asymptotic expansion for the real part of the digamma function:

$$\mathrm{Re}\left(\digamma(1+ix)\right) = \log x + \frac{1}{12} x^{-2} + O(x^{-4}) \tag{5.5.14}$$

Hence $\int_0^t \mathrm{Re}\left(\digamma(1+ix)\right) \, dx = t(\log t - 1) + O(1)$. The constant term of $\frac{\pi}{4}$ comes from integrating the difference between $\mathrm{Re}\left(\digamma(1+ix)\right)$ and $\log x$ between 0 and ∞:

$$\int_0^{\infty} \left[\mathrm{Re}\left(\digamma(1+ix)\right) - \log x\right] \, dx = \frac{\pi}{4}.$$

The result follows. □

Conjecture 5.5.7 and lemma 5.5.8 combine to give us a precise asymptotic statement on the distribution of zeros up to t, in the same vein as von Mangoldt's asymptotic formula for the number of zeros up to t for ζ:

Theorem 5.5.9 (GRH). *Let E have conductor N_E. Then for $t \gg 0$ we have*

$$M_E(t) = \frac{t}{\pi} \log\left(\frac{t\sqrt{N_E}}{2\pi e}\right) + \frac{1}{4} + O(\log t), \tag{5.5.15}$$

where the error term is positive as often as it negative and contributes no net bias.

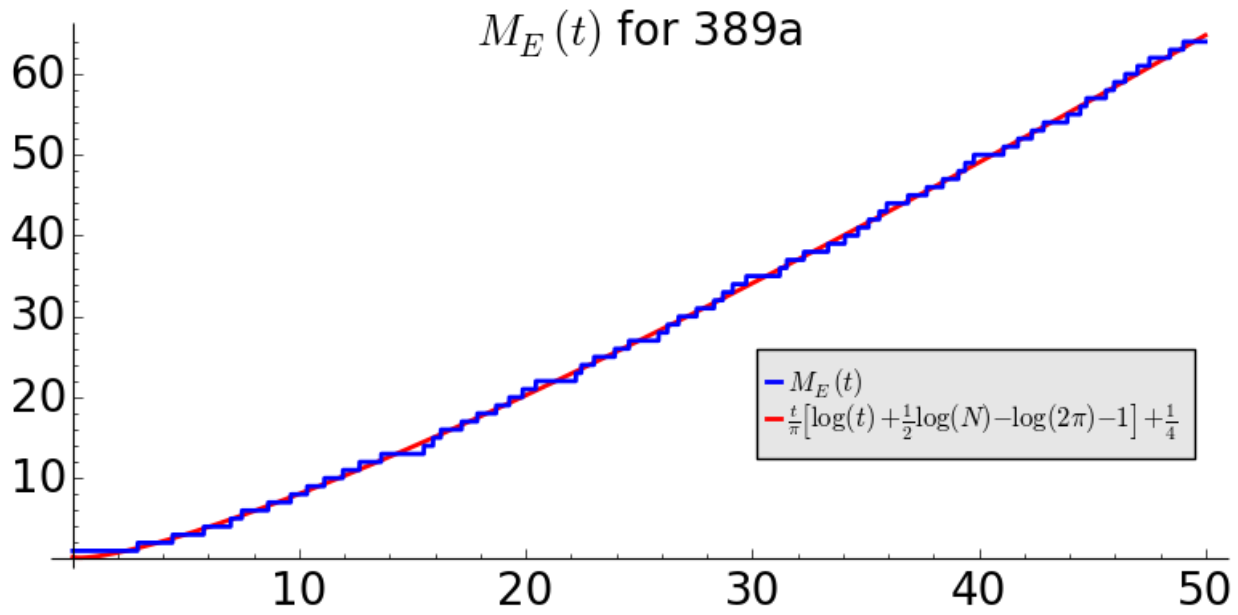

Figure 5.5.2: The number of zeros up to t versus $\frac{t}{\pi}\left[\log\left(\frac{t\sqrt{N_E}}{2\pi}\right) - 1\right] + \frac{1}{4}$ for the Cremona curve $389a$. The match up is extremely good.

Corollary 5.5.10 (GRH). *For $t \gg 0$, the number of zeros on the critical line in a unit interval*

$$M_E(t) - M_E(t-1) = \frac{1}{\pi} \log\left(\frac{t\sqrt{N_E}}{2\pi}\right) + O(\log t), \tag{5.5.16}$$

where again the error term contributes no net bias.

That is, zero density on the critical line grows like $\frac{1}{2}\log N_E + \log t$, where N_E is the conductor of E and t the distance from the real axis.

Neglecting the oscilating error term in Equation 5.5.15, we may solve for t in terms of the Lambert W-function to obtain an explicit formula for the expected value of the imaginary part of the nth zero on the critical line. Recall the definition of the Lambert W-function: if $y = xe^x$, then $x = W(y)$. W is a multiple-valued function; we make use of the principle branch W_0 below:

Corollary 5.5.11 (GRH)**.** *Let $\gamma_n := \gamma_n(E)$ be the imaginary value of the nth nontrivial (and noncentral) zero in the upper half plane of $L_E(s)$ with analytic rank r_E. Then*

$$\gamma_n \sim \frac{2\pi e}{\sqrt{N_E}} \cdot \exp\left(W_0\left[\left(\frac{r_E}{2} + n - \frac{3}{4}\right) \cdot \frac{\sqrt{N_E}}{2e}\right]\right), \tag{5.5.17}$$

in the sense that for a given curve, the difference between the above value and the true value of γ_n will on average be zero as $n \to \infty$.

Proof. Observe that the nth nontrivial noncentral zero has imaginary part t when $M_E(t) = \frac{r}{2} + n - \frac{1}{2}$ (since the final zero is counted with half weight). Hence using Equation 5.5.15 sans the oscillating error term, we solve for t in

$$\frac{t}{\pi}\log\left(\frac{t\sqrt{N_E}}{2\pi e}\right) + \frac{1}{4} = \frac{r_E}{2} + n - \frac{1}{2}.$$

□

[Aside: The principle branch of the Lambert W-function has the asymptotic expansion $W_0(x) = \log x - \log\log x + o(1)$, for $n \gg 0$ we recover the known asymptotic for the location of the nth nontrivial zero: $\gamma_n = O\left(\frac{n}{\log n}\right)$. Better yet, after some manipulation the asymptotic expansion gives us the proportionality constant explicitly:

$$\lim_{n\to\infty} \frac{\gamma_n}{\frac{n}{\log n}} = \pi. \tag{5.5.18}$$

Note, however, that the convergence rate is slow: $O(\frac{1}{\log n})$, and the constant in front scales with the log of the conductor of E.]

A natural question to ask, given that we now have an expected value for γ_n, is: how much does the imaginary part of the nth zero deviate from its expected location? To this end we define the *dispersion* of the nth zero:

Definition 5.5.12. The dispersion $\delta_n(E) := \delta_n$ of the imaginary part of the nth nontrivial zero in the upper half plane is the difference between the true and predicted values of γ_n, i.e.

$$\delta_n = \gamma_n - \frac{2\pi e}{\sqrt{N_E}} \cdot \exp\left(W_0\left[\left(\frac{r_E}{2} + n - \frac{3}{4}\right) \cdot \frac{\sqrt{N_E}}{2e}\right]\right). \tag{5.5.19}$$

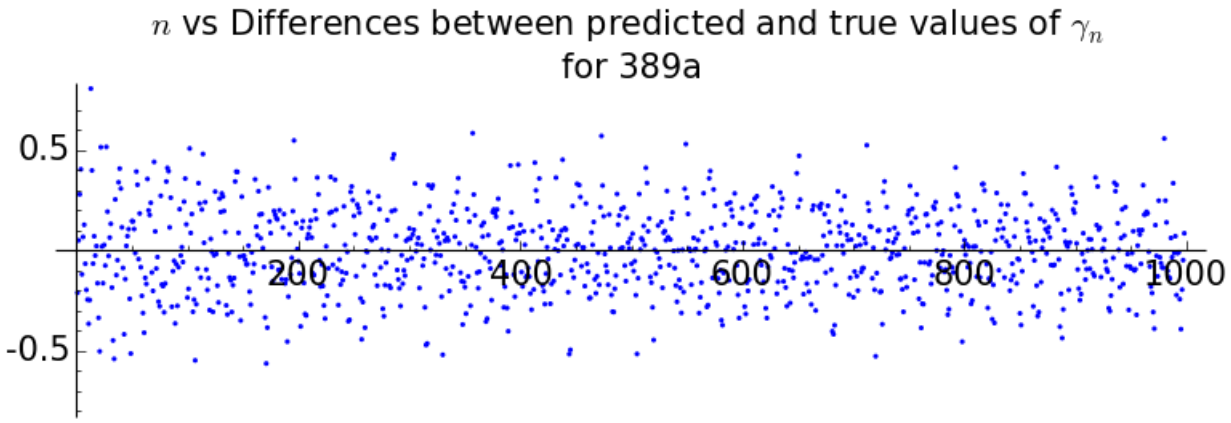

Figure 5.5.3: A scatter plot of zero dispersions for the first 1000 nontrivial zeros of the Cremona curve 389a, the rank 3 curve with smallest conductor. The values are seldom more than $\frac{1}{2}$.

Even though the above graph demonstrates that the zero dispersions are clearly not random, when viewed as a i.i.d. time series, the dispersions appear be normally distributed.

For the data set used the graph above, the mean was 3.16×10^{-5} (a good indicator that the expected value formula contains no systematic bias), standard deviation 0.1566.

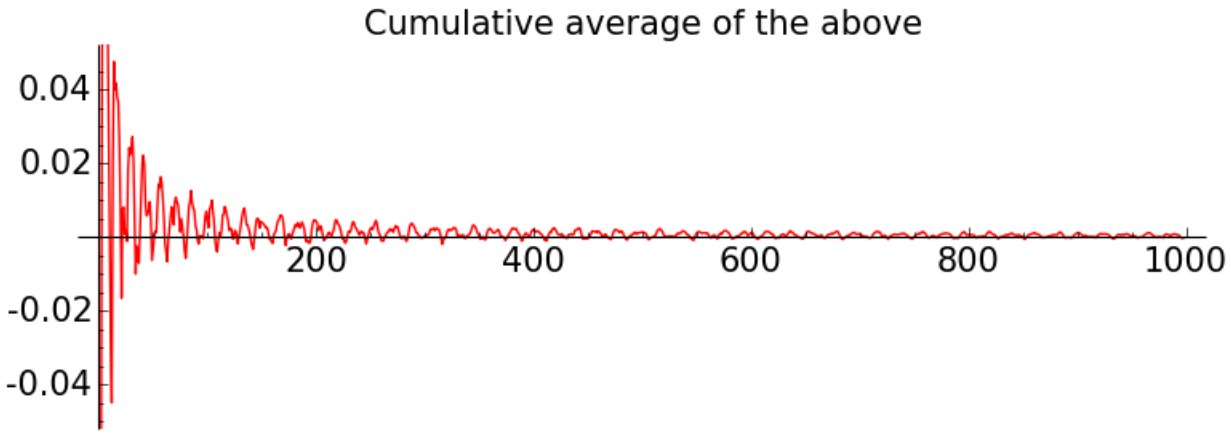

Figure 5.5.4: A cumulative average plot of the above, showing clearly that asymptotically, the average difference between the predicted and true values of γ_n is zero. The positive bias at the beginning comes from the $O(1/t)$ term in Lemma 5.5.8. Interestingly, although the deviations might a priori appear completely random, there is a clear oscillating structure in the average, and the line about which the oscillation occurs appears to decrease to zero from above.

The standard deviation appears to decrease with increasing n: we applied the Shapiro-Wilk normality test on batches of 1000 consecutive zero dispersions, and got p-values in excess of 0.2 (and most of the time in excess of 0.5) in all cases. Moreover, the computed standard deviations decreased uniformly from 0.1745 for the $n = 1000$ to 2000 dispersion set, to 0.1464 in the $n = 10000$ to 11000 set. We hope to pursue this investigation in future work.

Finally, we may also go in the other direction and use Equation 5.5.9 to make a guess as to the expected imaginary part of the *lowest* noncentral nontrivial zero of $L_E(s)$ as a function of increasing conductor N_E:

Proposition 5.5.13 (GRH)**.** *For a curve E with large conductor N_E and analytic rank r_E, the best guess for the imaginary part of the first nontrivial noncentral zero γ_0 of $L_E(s)$ in the*

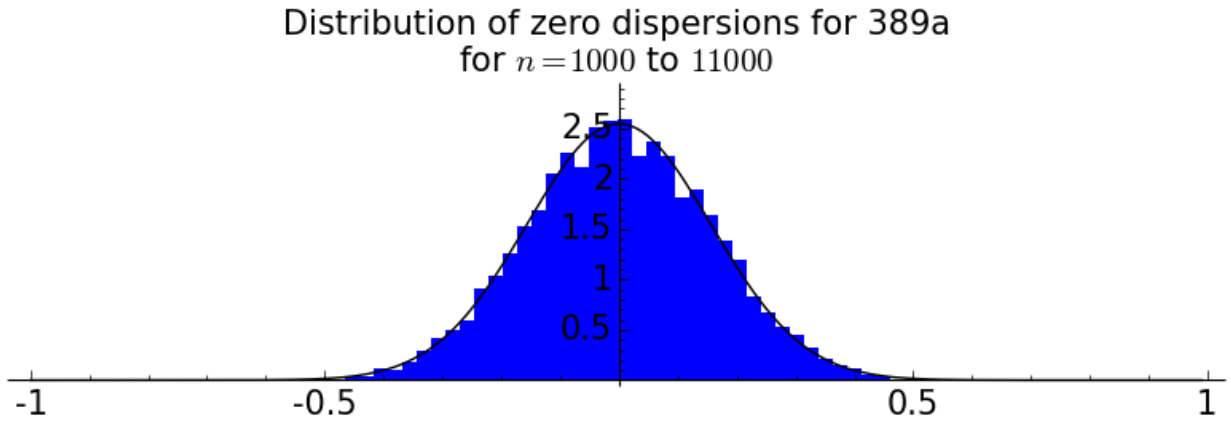

Figure 5.5.5: A histogram of zero dispersions for the curve 389 for the 1000th through 11000th zeros (we discard the first 1000 zeros to avoid the small-height bias observable in the cumulative average plot above).

upper half plane is

$$\gamma_0 = \frac{(r_E+1)\pi}{\log(N_E) - 2\log(2\pi) - 2\eta}. \tag{5.5.20}$$

The derivation is similar to before. The location of the first nontrivial noncentral zero is given by the value of t for which $M_E(t)$ jumps from $r_E/2$ to $r_E/2+1$; at that point $M_E(t) = r_E/2 + 1/2 = \frac{r_E+1}{2}$, so the expected value of γ_1 is given by setting equation 5.5.9 equal to $\frac{r_E+1}{2}$ and solving for t.

Now, however, $\frac{1}{\pi}\sum_{k=1}^{\infty}\left[\frac{t}{k} - \arctan\left(\frac{t}{k}\right)\right]$ is $O(t^3)$ for small t, so the quantity expressed in equation 5.5.11 is dominated by the $\frac{1}{\pi}\left(-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right)t$ term when N_E is large. Solving for t yields the desired value.

5.6 The Bite

Mazur and Stein in [27] define the *bite* of an elliptic curve:

Definition 5.6.1. The *bite* of $L_E(s)$ is

$$\beta(E) := \sum_{\gamma \neq 0} \gamma^{-2}, \tag{5.6.1}$$

where the sum runs over the imaginary parts of all *noncentral* nontrivial zeros of $L_E(s)$.

This quantity is of interest for a variety of reasons: it controls the rate of convergence in many explicit formula-type sums for $L_E(s)$, and is intimately linked with the analytic rank and leading central Taylor coefficient for the L-series of E. Again, the explicit dependence on E may be left as understood if the choice of E is unambiguous, or we may subsume the dependance on E into a subscript and write β_E. In this final section we establish some bounds involving the bite, show how one can compute it efficiently without having to compute the locations of the zeros of $L_E(s)$ explicitly, and give some zero sum examples relevant to this thesis where the bite comes into play.

Since sums of inverse higher powers of zeros also crop up, we generalize the notion of bite as follows:

Definition 5.6.2. For positive integer n, the *higher order bite* of order n for $L_E(s)$ is

$$\beta_n(E) := \sum_{\gamma \neq 0} \gamma^{-n}. \tag{5.6.2}$$

Thus $\beta_2(E) = \beta_E$ as defined previously. Note also that $\beta_n = 0$ for any odd n, since zeros come in conjugate pairs.

Equation 5.1.17 gives us a description of the Laurent expansion of $\frac{\Lambda_E'}{\Lambda_E}(1+s)$ about zero:

Proposition 5.6.3 (GRH). *The Laurent expansion of* $\frac{\Lambda_E'}{\Lambda_E}(1+s)$ *about zero is given by*

$$\frac{\Lambda_E'}{\Lambda_E}(1+s) = \frac{r_E}{s} + \beta_2 \cdot s - \beta_4 \cdot s^3 + \beta_6 \cdot s^5 - \dots \tag{5.6.3}$$

$$= \frac{r_E}{s} + \sum_{k=1}^{\infty} (-1)^{k-1} \beta_{2k} \cdot s^{2k-1}, \tag{5.6.4}$$

and this converges for $|s| < \gamma_0$, *where* γ_0 *is the imaginary part of the lowest noncentral nontrivial zero of* $L_E(s)$ *in the upper half plane.*

The proof of this follows immediately by expanding the sum in Equation 5.1.17 and collecting terms.

Corollary 5.6.4 (GRH). *Let* $E/\mathbb{Q}$ *have conductor* N_E, *L-function* $L_E(s)$ *with bite* $\beta_E = \beta_2(E)$ *and central leading coefficient* C_E'. *Let the Taylor series expansion of* L_E *about the central point be*

$$L_E(1+s) = C_E' \, s^{r_E} \left[1 + a \cdot s + b \cdot s^2 + O(s^3)\right] \tag{5.6.5}$$

Then

$$a = -\left[-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right] \tag{5.6.6}$$

$$2b = \left[-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right]^2 - \frac{\pi^2}{6} + \beta_E, \tag{5.6.7}$$

where η *is the Euler-Mascheroni constant* $= 0.5772\ldots$.

Proof. We note that the digamma function has the following Taylor expansion about $s = 1$:

$$\digamma(1+s) = -\eta - \sum_{k=1}^{\infty} (-1)^k \zeta(k+1) s^k, \tag{5.6.8}$$

where η is the Euler-Mascheroni constant, and $\zeta(s)$ is the Riemann zeta function.
Thus by equation 5.1.2 and Proposition 5.6.3 we have that

$$\frac{L_E'}{L_E}(1+s) = \frac{r_E}{s} - \left[-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right] + \left[-\zeta(2) + \sum_{\gamma \neq 0} \gamma^{-2}\right] \cdot s + O(s^2).$$

But if $L_E(1+s) = C'_E\, s^{r_E}\,[1 + a \cdot s + b \cdot s^2 + O(s^3)]$, then careful logarithmic differentiation yields

$$\frac{L'_E}{L_E}\,(1+s) = \frac{r_E}{s} + a + \left(-a^2 + 2b\right) \cdot s + O(s^2).$$

Comparing terms and solving for the relevant quantities produces the desired formulae. □

We may continue in the same vein to produce formulae for higher order coefficients of $L_E(s)$. As can be seen from above, these can in general be written in terms of sums of powers of the quantity $\left[-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right]$ (which is the constant term in the Laurent series of $\frac{\Lambda'_E}{\Lambda_E}\,(1+s)$), inverse sums of even powers of the nontrivial zeros, and $\zeta(n)$ for n a positive integer.

In other words, β_E and higher-order bites encode information about higher order terms in the Taylor expansion of $L_E(1+s)$; moreover, the Taylor series thereof contains no new information about the curve's attached invariants beyond that which can be found in the first nonzero coefficient and the bites $\beta_{2n}(E)$. Whether the bites do indeed have any arithmetic significance, however, is an open question.

As can be seen from the above, the bite of a curve is of interest is due to it being intimately linked with the leading central Taylor coefficient C_E of $\Lambda_E(1+s)$ and the (analytic) rank r_E. We may link the three quantities explicitly with a suite of inequalities derived from point estimates on the L-function of E and the logarithmic derivative thereof. First, we will need the following technical lemma:

Lemma 5.6.5 (GRH)**.** *Let $\sigma > \frac{1}{2}$. The bite β_E and analytic rank r_E of a curve E obey*

$$\sigma \cdot \beta_E + \frac{r_E}{\sigma} > \frac{1}{2}\log N_E + \digamma(1+\sigma) - \log(2\pi) - 2\frac{\zeta'}{\zeta}\left(\frac{1}{2} + \sigma\right), \tag{5.6.9}$$

where $\digamma(s) = \frac{\Gamma'}{\Gamma}(s)$ is the digamma function on $\mathbb{C}$, $\zeta(s)$ is the Riemann zeta function and N_E is the conductor of E.

Proof. From Equation 5.5.2, letting $\tau = 0$, we get

$$\sum_{\gamma} \frac{\sigma}{\sigma^2 + \gamma^2} > \log\left(\frac{\sqrt{N_E}}{2\pi}\right) + F(1+\sigma) - 2\frac{\zeta'}{\zeta}\left(\frac{1}{2} + \sigma\right). \tag{5.6.10}$$

But

$$\begin{aligned}\sum_{\gamma} \frac{\sigma}{\sigma^2 + \gamma^2} &= \frac{1}{\sigma}\sum_{\gamma} \frac{1}{1 + \left(\frac{\gamma}{\sigma}\right)^2} \\ &< \frac{1}{\sigma}\left(r_E + \sum_{\gamma \neq 0} \frac{1}{\left(\frac{\gamma}{\sigma}\right)^2}\right) \\ &= \frac{r_E}{\sigma} + \sigma \cdot \beta_E.\end{aligned}$$

Combining inequalities completes the proof. □

We then have the following:

Proposition 5.6.6 (GRH)**.** *Let β_E, C_E, r_E and N_E be the bite, completed L-function leading central Taylor coefficient, analytic rank and conductor of E respectively. Then*

$$(1 + \beta_E) \cdot C_E < 0.173 \cdot N_E, \tag{5.6.11}$$

$$\beta_E + \log C_E > \frac{1}{2}\log N_E - 5.229, \tag{5.6.12}$$

$$\beta_E + r_E > \frac{1}{2}\log N_E - 4.426. \tag{5.6.13}$$

Proof. The third inequality is a specialization of Lemma 5.6.5 with $\sigma = 1$, with the conductor-independent terms lumped together into one numerical value. The first two inequalities come from the Hadamard product of the completed L-function (Equation 5.1.16) evaluated one unit to the right of the central point:

$$\Lambda_E(2) = C_E \cdot \prod_{\gamma \neq 0}\left(1 + \frac{1}{\gamma^2}\right), \tag{5.6.14}$$

noting that $1 + \beta_E < \prod_{\gamma \neq 0}\left(1 + \frac{1}{\gamma^2}\right) < e^{\beta_E}$. On the other hand from the definition of the completed L-function we have $\Lambda_E(2) = N_E \cdot (2\pi)^{-2} \cdot L_E(2)$. Inequality 5.1.12 has that $\frac{\zeta(3)^2}{\zeta(\frac{3}{2})^2} < L_E(2) < \zeta\left(\frac{3}{2}\right)^2$; combining inequalities and collecting constant terms in the respective inequalities completes the two results. □

The take-away from Proposition 5.6.6 is that the bite and the leading Taylor coefficient C_E cannot both be very large or very small simultaneously relative to the conductor. Similarly, the larger the rank of a curve, the smaller β_E can be relative to N_E.

We can go even further and establish a lower bound on β_E in terms of N_E independent of C_E and r_E, at the expense of introducing a non-explicit constant. As asymptotic zero density on the critical line grows proportional to $\log N_E$ (see Theorem 5.5.9), we expect the bite to grow at least like $\log N_E$ too, regardless of the limiting behavior of zeros near the central point. This is indeed the case:

Proposition 5.6.7 (GRH)**.** *For all $\epsilon > 0$ there is a constant $K_\epsilon > 0$ such that for all elliptic curves E, the bite of E obeys*

$$\beta_E = \sum_{\gamma \neq 0} \frac{1}{\gamma^2} > \frac{1}{1+\epsilon} \log N_E - K_\epsilon. \tag{5.6.15}$$

where N_E is the conductor of E.

Proof. We again invoke Lemma 5.6.5 to observe that

$$\beta_E > \frac{1}{2\sigma} \log N_E - \frac{r_E}{\sigma^2} + \frac{1}{\sigma} \left[\digamma(1+\sigma) - \log(2\pi) + 2\frac{\zeta'}{\zeta}\left(\frac{1}{2}+\sigma\right) \right], \tag{5.6.16}$$

where the term in the square brackets is independent of N_E and is finite for any $\sigma > \frac{1}{2}$. By Corollary 5.3.3, the rank r_E grows slower than any multiple of $\log N_E$. Hence for $\epsilon > 0$ we may, for example, take $r_E < \epsilon^2 \log N_E + K'(\epsilon^2)$ for some constant K' dependent on ϵ^2, and then let $\sigma = \frac{1}{2} + \frac{1}{2}\epsilon$. This allows the constant in front of the collected $\log N_E$ term to be made arbitrarily close to 1 from below, while all other terms sum to a finite value independent of E. □

In reality we expect the bite to grow faster than $\log N_E$ – as zero density scales with $\log N_E$, the sum of the inverse squares thereof should naïvely be expected to grow with $(\log N_E)^2$. However, this is discounting any unusual behaviour of zeros near the central point.

Sarnak has mentioned in private correspondence that it's believed that the lowest noncentral zero γ_0 actually approaches a constant limiting distribution as conductor goes to infinity, which would in turn decrease any lower bound that can be placed on the bite.

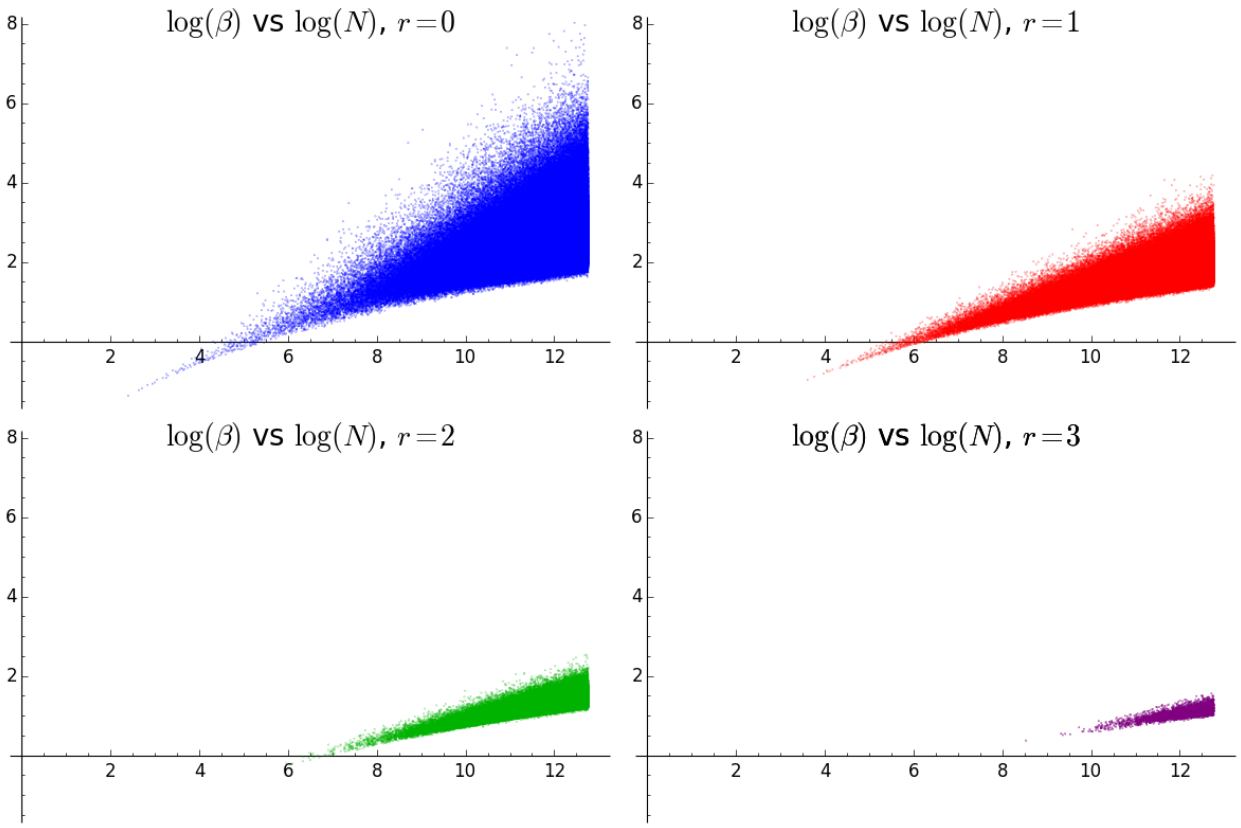

Figure 5.6.1: The bites of all curves in the Cremona tables were computed using the above method. Above is a scatterplot of $\log \beta_E$ vs. $\log N_E$ for curves of rank 0, 1, 2 and 3 respectively.

One can see from Figure 5.6.2 that the bite obeys a sharp lower bound with respect to the conductor, but the upper bound is somewhat less tight. More interesting is the fact that the lower bound appears the same regardless of rank, while curves with anomalously large bites are predominantly rank 0. This makes sense: large bites correspond to very low-lying zeros, and because of the well-documented zero repulsion effect, this usually only happens

when there are no zeros at the central point.

How does one go about computing the bite of an elliptic curve? The naïve way would be to compute the location of the n zeros up to some bound and then add up their inverse squares to get an approximation of β_E. This can indeed be done, for example via Rubinstein's `lcalc` package. However it is slow and inefficient, and one will always introduce some truncation error via this method.

Instead, the following result allows us to relate the bite directly to the leading Taylor coefficient C_E and higher derivatives of $\Lambda_E(s)$ at the central point:

Proposition 5.6.8 (GRH)**.** *Let E have completed L-function $\Lambda_E(s)$ and analytic rank r_E. Then*

$$\beta_E \cdot C_E = \frac{\Lambda_E^{(r_E+2)}(1)}{(r_E+2)!}, \tag{5.6.17}$$

where β_E is the bite of E, and C_E is the leading coefficient of $\Lambda_E(s)$ at the central point.

Proof. From equation 5.1.16 we have that

$$\Lambda_E(1+s) = C_E\left(s^{r_E} + \beta_E s^{r_E+2} + O(s^{r_E+4})\right). \tag{5.6.18}$$

Differentiating $r_E + 2$ times and evaluating at $s = 0$ achieves the desired result. □

It is worth noting explicitly that one cannot hope to be able to compute the bite of a curve without knowing its analytic rank – we have to know how many zeros are precisely at the central point and not just ϵ away from the central point, otherwise β_E could be arbitrarily large. This obstruction notwithstanding, Proposition 5.6.8 gives us a straightforward way to compute the bite of E from the r_Eth and (r_E+2)th Taylor coefficients of $L_E(1+s)$:

Corollary 5.6.9 (GRH)**.**

$$\beta_E = \frac{1}{(r_E+1)(r_E+2)} \cdot \frac{\Lambda_E^{(r_E+2)}(1)}{\Lambda_E^{(r_E)}(1)} \tag{5.6.19}$$

$$= \frac{2}{(r_E+1)(r_E+2)} \cdot \frac{L_E^{(r_E+2)}(1)}{L_E^{(r_E)}(1)} - \left(-\eta + \log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right)^2 + \frac{\pi^2}{6}. \tag{5.6.20}$$

Proof. The first line follows immediately from Proposition 5.6.8 and the fact that $C_E = \frac{\Lambda^{(r_E)}(1)}{r_E!}$. The second line comes from the formula for the (r_E+2)th Taylor coefficient of L_E at the central point derived in Corollary 5.6.4. □

We can therefore compute the bite of a curve *without* having to compute the locations of the zeros themselves. Moreover, Theorem 2.0.5 implies that the bite can be provably computed to k bits precision in $\tilde{O}(k \cdot \sqrt{N_E})$ time (assuming standard conjectures). This may be done, for example, via Tim Dokchitser's `computel` PARI code, which can compute the Taylor series expansion of a motivic L-function at a given point. [Important side-note: the aforementioned package uses approximations that have not (yet) been shown to be provably correct; however, one could certainly write code to compute in square root time the central Taylor expansion of $L_E(s)$ via the work of Bradshaw in [7], which *does* produce provably correct L-function values.]

We finish off this section with a result giving an indication of one other area in which the bite of a curve comes into play: controlling convergence rates in explicit formula type sums. This is a topic worthy of its own paper, so we shall just present two examples relevant to the work in this thesis.

Theorem 5.6.10 (GRH)**.** *Let* $\sum_\gamma \mathrm{sinc}^2(\Delta\gamma)$ *be the* sinc^2 *sum for* E *with parameter* Δ*, as detailed in Equation 5.3.5. If we let* $\Delta = \frac{1}{\pi} \cdot \sqrt{\frac{\beta_E}{n}}$*, then the sum will evaluate to a value less than than* $r_E + n$*, where* r_E *is the analytic rank of* E*.*

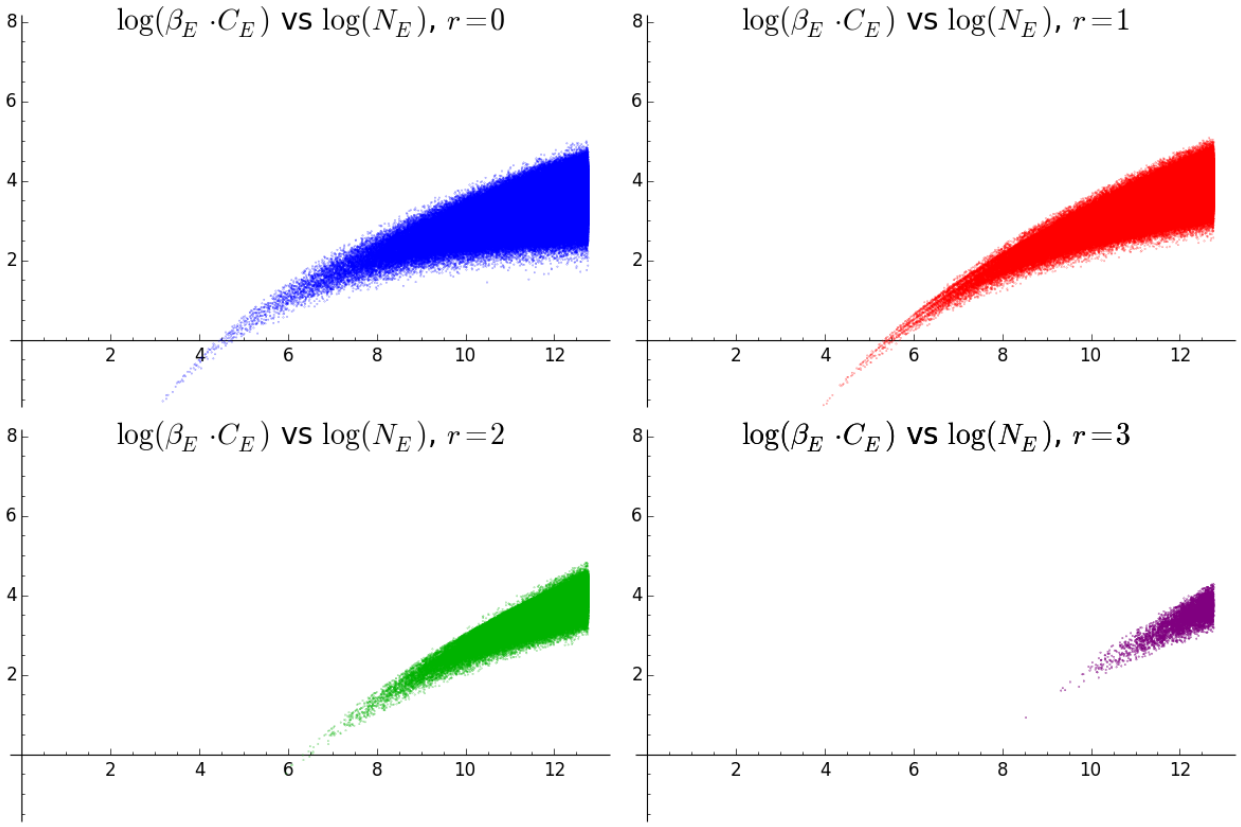

Figure 5.6.2: A scatter plot of $\log(\beta_E \cdot C_E)$ vs. $\log N_E$ for all curves up to conductor 350000, differentiated by rank. The constrained nature of the quantity $\beta_E \cdot C_E$ is readily apparent.

Corollary 5.6.11 (GRH)**.** *The analytic rank of E is the largest integer less than*

$$\frac{1}{\sqrt{\beta_E}}\left[\left(-\eta+\log\left(\frac{\sqrt{N_E}}{2\pi}\right)\right)+\frac{1}{2\sqrt{\beta_E}}\left(\frac{\pi^2}{6}-\mathrm{Li}_2\left(e^{-2\sqrt{\beta_E}}\right)\right)+\sum_{\log n<2\sqrt{\beta_E}} c_n\cdot\left(1-\frac{\log n}{2\sqrt{\beta_E}}\right)\right]. \tag{5.6.21}$$

Proof. We note that

$$\sum_{\gamma}\mathrm{sinc}^2(\Delta\gamma)=r_E+\sum_{\gamma\neq 0}\mathrm{sinc}^2(\Delta\gamma)<r_E+\sum_{\gamma\neq 0}\frac{1}{(\pi\Delta\gamma)^2}=r_E+\frac{1}{\pi^2\Delta^2}\cdot\beta_E. \tag{5.6.22}$$

So choosing $\Delta=\frac{1}{\pi}\cdot\sqrt{\frac{\beta_E}{n}}$ bounds the sum value from above by r_E+n. The corollary follows immediately from Equation 5.3.5 the case with $n=1$. □

This formula comes with one giant caveat that renders it of little use practically – it requires knowing the bite of a curve, which of course in itself requires knowing the curve's analytic rank a priori. Nevertheless, the above serves to underscore that determining the bite and determining the analytic rank of a curve are computationally equivalent: we can compute the bite knowing the rank via Equations 5.6.19 or 5.6.20, and we can compute the rank knowing the bite via Formula 5.6.21.

Using the bite we have an even simpler way to compute the analytic rank of an elliptic curve:

Theorem 5.6.12 (GRH)**.**

$$r_E = \left\lfloor \frac{1}{\sqrt{\beta_E}} \cdot \frac{\Lambda_E'}{\Lambda_E} \left(1 + \frac{1}{\sqrt{\beta_E}}\right) \right\rfloor. \tag{5.6.23}$$

Proof. By Equation 5.1.17, the Hadamard product expansion of $\frac{\Lambda_E'}{\Lambda_E}(1+s)$ gives us

$$s \cdot \frac{\Lambda_E'}{\Lambda_E}(1+s) = s \cdot \prod_{\gamma} \frac{s}{s^2+\gamma^2} = r_E + \prod_{\gamma \neq 0} \frac{1}{1+(\frac{\gamma}{s})^2} < r_E + s^2 \cdot \beta_E. \tag{5.6.24}$$

So, analogous to the method used in the proof of Theorem 5.6.10, evaluating at $s = \sqrt{\frac{n}{\beta_E}}$ gives a real value bounded by $r_E + n$. □

Again, there are subtle issues present with this formula. Apart from again having to know the bite of a curve, even though we can evaluate $\Lambda_E(s)$ and its derivative to any given precision in $\tilde{O}(\sqrt{N_E})$ time, the same is not true for the logarithmic derivative. Namely, we may encounter destructive precision loss near the central point if r_E has high analytic rank and/or low-lying zeros. We therefore caution against using this method to determine analytic rank willy-nilly, as in our mind it does *not* constitute a method to compute rank provably without doing more work.

Chapter 6
REMARKS AND FUTURE WORK

This dissertation pulls in results from a number of disparate topics related to elliptic curves, with the general approach being "do enough to establish results that are sufficient to support the main theorems, then move on". As such, many of the bounds and statements obtained of the course of this work are very far from optimal, and the ultimate running time of, say, Algorithm 2.0.6 could be considerably improved if these bounds were tightened. Beyond this there are natural generalizations to the results in this work that should be considered, We list below the areas where results could be improved upon or generalized, and in so doing detail directions for possible future work.

6.0.1 Implementing and optimizing the rank algorithm

I coded up a naïve implementation of Algorithm 2.0.6 in Sage to collect supporting data for inclusion in this dissertation, but the algorithm is calling out for a dedicated optimized implementation for general use. Much of the hard work has already been done – for example, Bradshaw provided a Sage implementation of provable motivic L-function evaluation in [7], and Sage already includes functionality to compute the real period of an elliptic curve.

There are several optimizations that should be included in any implementation. Three which immediately spring to mind are as follows:

- One should check for torsion on E, which is quick to do. Doing so results in up to 16 less bits of precision needed when evaluating $L_E(s)$.

- It might be advantageous to compute the Tamagawa product $\prod_p c_p$ if it can be quickly

done. Again, this results in a larger lower bound on the leading Taylor coefficient of C_E, and thus less precision needed when evaluating $L_E(s)$.

- The $r_{an}(E) < a \log N_E + b$ bounds used for analytic rank are in practice far too crude; in reality the vast majority of curves (if you believe the folklore conjecture, asymptotically 100%) have rank 0 or 1, and maximum observed rank goes more like $\sqrt{\log N_E}$. It therefore makes sense to obtain a better upper bound on the rank of a given curve up front; this then gives a better lower bound on the regulator and thus further reduces the required precision when provably evaluating $L_E(s)$. One could, for example, run the sinc^2 sum algorithm exhibited in Section 5.3 with some small choice of Δ, which doesn't require direct evaluation of $L_E(s)$.

6.0.2 Generalizing results to modular L-functions of arbitrary weight and level

The results in this thesis revolve around working with the L-function attached to a given elliptic curve. By the modularity theorem [8], each of these is actually the L-function attached to a certain weight 2 integral cuspidal eigenform of level N_E, where N_E is the conductor of the curve in question.

In general we can attach an L-function to a cuspidal eigenform of arbitrary weight and level. Many of the results in this dissertation should carry over naturally, allowing us to address the issue of computing the analytic rank of higher-weight modular L-functions. Specifically, given an analogue of BSD we should be able to show that an algorithm exists to compute the analytic rank of a modular L-function that is polynomial-time in the level of that form. An immediate question would then be: how does such a method scale with the *weight* of the form?

Moreover, the sinc^2 zero sum method to bound analytic rank from above should transfer directly to higher weight forms. We hope in future to extend the functionality of the Sage code to accommodate for this – in fact, we designed the code layout with this extensibility

explicitly in mind.

6.0.3 CM curves and families of quadratic twists

Two related questions that we can ask are:

- Can we get better bounds and results if we restrict ourselves to considering CM curves?
- Do there exist optimizations for Algorithm 2.0.6 and other results if we consider the family of quadratic twists of a given elliptic curve? How does complexity scale with the twisting parameter d?

In both cases, we should ask the question: how do the BSD invariants (especially the regulator and real period) vary within a given family? At the very least the real periods within a family of twists is very rigidly controlled, so we should for be able to write down the required precision in Algorithm 2.0.6 as a function of conductor without needing to compute the real period for each curve.

Some work has already gone into considering the case of quadratic twists of a given curve – see [14]. It would be interesting to see if these ideas could be incorporated to improve the results in this thesis.

6.0.4 Bounding analytic rank from above in terms of conductor

To establish a lower bound on the regulator of an elliptic curve in terms of its conductor we require an upper bound on the analytic rank. To this end we invoke Corollaries 5.1.12 and 5.3.4, stating that maximum analytic rank is bounded by a constant times $\log N_E$ plus another explicit constant.

However, Corollary 5.3.3 asserts that, contingent on GRH, the maximum analytic rank of a curve with conductor at most N in fact grows slower than any multiple of $\log N$. We

would like to use this result more effectively, but the issue lies in making the constant K_ϵ explicit in terms of the ϵ chosen. This translates to bounding the c_n sum

$$\sum_{n<e^{2\pi\Delta}} c_n \cdot \left(1 - \frac{\log n}{2\pi\Delta}\right) \tag{6.0.1}$$

in terms of the parameter Δ.

A natural question we can ask, and hopefully answer, is "can this be done effectively"? One can readily obtain a naive explicit bound on the c_n sum that is exponential in Δ, but this is clearly of limited practical use. Empirically, even when Δ is large the c_n sum is seldom more than one or two units in magnitude (because as $\Delta \to \infty$ the c_n sum $\to$ the rank of E). The obstruction is that the sum is carried out over prime powers and large amounts of cancellation occurs due to the changing signs of the c_n coefficients, so this this term is tricky to control without more advanced analytic tools.

Nevertheless, if one could show that the sum grows in magnitude at most polynomial in Δ (regardless of E) and obtain explicit constants, then we should be able to show that the lower bound on the regulator of E would go to zero more slowly than any negative power of N, as appears to be the case in practice.

6.0.5 The regulator

The lower bound on Reg_E could potentially be improved in multiple ways. Firstly, the result relies on the Hindry-Silverman/Elkies' result [15] that, contingent on ABC, for any rational point P on curve E with discriminant D_E obeys

$$\hat{h}(P) > M_0 \log(D_E), \tag{6.0.2}$$

where $M_E \geq 3.94 \times 10^{-5}$. This result is in all probability not optimal. An improvement in the lower bound on point height would result in a direct improvement on the constants involved

in the lower bound on the regulator, and thus the precision required in the evaluation of $L_E(s)$ in Algorithm 2.0.6. Again, this is a deep topic, so new insight here won't come easily.

What is perhaps a bit more tractable is to continue in the same vein as in the beginning of the proof of Theorem 4.3.8: artificially increase the size of the constant, and check computationally that it holds for all curves up to a given conductor bound. We chose a bound of $N = 350000$ simply because that is where Cremona's tables currently go to, but there is no theoretical reason one has to stop there. This option of course pays the price of being computationally much more tedious.

Finally, the lower bound on Reg_E contains a reciprocal Gamma factor, which means that the lower bound decays faster than any power of $\log N_E$. This factor arises from the lower bound on the minimum covolume of a lattice in $\mathbb{R}^r$ with a fixed minimum vector length (Lemma 4.3.7), which is most likely not optimal. If a better lower bound could be exhibited on Lattice covolume as a function of dimension, it is conceivable that we could eliminate the Gamma factor entirely. This is desirable, as we would then have that Reg_E is bounded below by a negative power of the conductor.

The real period

The lower bound on the real period of an elliptic curve could potentially be improved further. Specifically, in we would like to make the constant in Theorem 4.2.11 completely explicit as a function of ϵ, which would remove the need to compute Ω_E in order to determine the precision.

Secondly, the bound of $\mathrm{Reg}_E > K_\epsilon \cdot (N_E)^{-1.5-\epsilon}$ does not seem to be very tight; empirically it would appear that minimum real period goes more like $(N_E)^{-1}$. It would be useful to see if the proofs in Section 4.2 could be reworked to make the results conform more closely with the observed data.

6.0.6 *Convergence rate and and convexity statements on the sinc^2 rank bounding sum*

Equation 5.3.5 gives the analytic rank of E as a limit:

$$r_E = \lim_{\Delta\to\infty} \frac{1}{\Delta\pi}\left[\left(-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right) + \frac{1}{2\pi\Delta}\left(\frac{\pi^2}{6} - \mathrm{Li}_2\left(e^{-2\pi\Delta}\right)\right) + \sum_{n<e^{2\pi\Delta}} c_n \cdot \left(1 - \frac{\log n}{2\pi\Delta}\right)\right]. \tag{6.0.3}$$

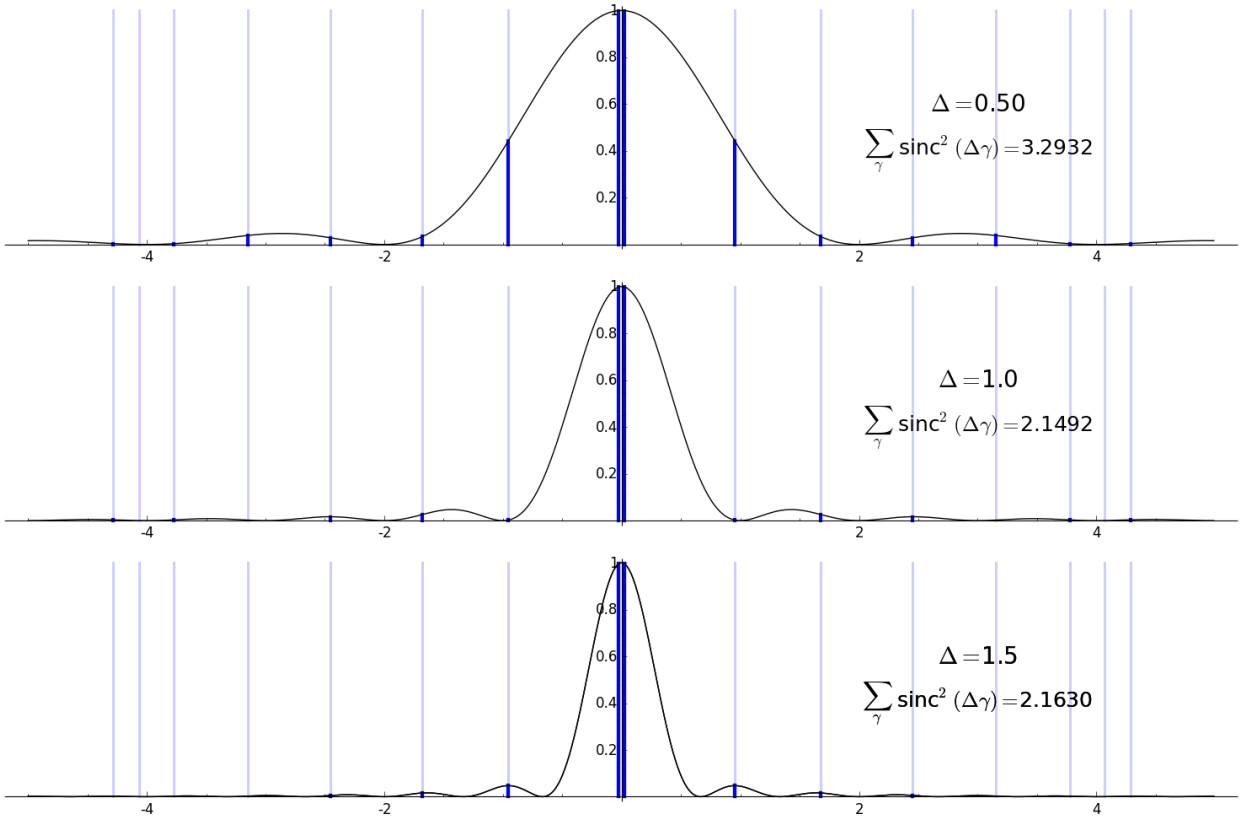

Figure 6.0.1: A graphic representation of the sinc^2 sum for the Cremona curve `256944c1` , a rank 0 curve with conductor $N_E = 256944$, for $\Delta = 0.5$, 1.0 and 1.5.

However, more work needs to be done regarding the rate of convergence of this sum. We give a result regarding convergence rate of the sinc^2 sum in terms of the bite β_E of a curve in

Theorem 5.6.10. However, this is more of a step sideways, as the bite remains a mysterious quantity in its own right.

Consider the example in Figure 6.0.1: the Cremona curve `256944c1`, a rank 0 curve, has a pathologically low-lying zero at $\gamma_0 = 0.02560\ldots$. For small values of Δ, it therefore appears that this curve has analytic rank 2, not zero. In fact, only for $\Delta >\sim 2.815$ does the sum evaluate to a value less than 2 (which, after invoking parity, gives us that it is rank 0). This highlights the fact that some curves – specifically those with low-lying zeros – require Δ to be large for the sum to be within, say, 2 of the true rank of the curve.

Furthermore, Figure 6.0.1 shows that the convergence from above is unfortunately *not* even necessarily monotone: as Δ is increased the small outlying bumps of the sinc^2 function can travel over zeros and temporarily increase the value of the sum.

Even though this is the case, we should be able to make some sort of a convexity statement regarding the convergence of the sinc^2 sum. This should allow us to use point estimates in the rank estimation code to decide which Δ values to use on a given curve, and in so doing make the code more efficient. This has the potential to significantly increase the effectiveness of the rank estimation code.

6.0.7 Better bounds on the bite

Section 5.6 discusses at the topic of the bite of an elliptic curve, namely the quantity

$$\beta_E = \sum_{\gamma \neq 0} \frac{1}{\gamma^2}. \tag{6.0.4}$$

It would be useful to have better bounds in either direction for this quantity. In terms of bounding from below, we are reasonably confident that the constant K_ϵ in Equation 5.6.15 can be made explicit in terms of ϵ, given more diligent controlling of the various zero sum-based inequalities. Better yet, it would seem that the bite must grow faster than any multiple of

$\log N_E$, and we would like to show that this is the case. It is conceivable that this could also be achieved using the methods detailed in this work.

On the other hand, placing an upper bound on the bite is equivalent to bounding the lowest noncentral zero away from the central point. This is a much deeper and more difficult endeavour, equivalent to placing a lower bound on the leading central Taylor coefficient of $L_E(s)$. The latter is done in Chapter 4, and in fact a direct corollary of this is that the lowest noncentral zero γ_0 is bounded below by $(N_E)^{-\alpha}$ for some $\alpha > 0$. However, in the leading Taylor coefficient bound a constant introduced from the bound on the real period is never made explicit; while this is good enough to get a polynomial-time rank algorithm out, it *isn't* good enough to make the lower bound on γ_0 explicit. Again, we hope that this issue can be resolved in future work, perhaps by making all constants in bounds on the real period completely explicit.

BIBLIOGRAPHY

[1] Berndt, B., and Zhang, L.-C. Ramanujan's identities for eta-functions. *Mathematische Annalen 292*, 1 (1992), 561–573.

[2] Bhargava, M., and Shankar, A. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *arXiv preprint arXiv:1006.1002* (2010).

[3] Bhargava, M., and Shankar, A. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *arXiv preprint arXiv:1007.0052* (2010).

[4] Bhargava, M., and Shankar, A. The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1. *arXiv preprint arXiv:1312.7859* (2013).

[5] Birch, B., and Swinnerton-Dyer, P. Notes on elliptic curves, ii. *J. reine angew. Math 218* (1965), 79–108.

[6] Bober, J. W. Conditionally bounding analytic ranks of elliptic curves. *The arXiv* (2011), 1–9.

[7] Bradshaw, R. W. *Provable Computation of Motivic L-functions*. PhD thesis, University of Washington, 2010.

[8] Breuil, C., Conrad, B., Diamond, F., and Taylor, R. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc. 14*, 4 (2001), 843–939 (electronic).

[9] Brumer, A. The average rank of elliptic curves i. *Inventiones mathematicae 109*, 1 (1992), 445–472.

[10] Conrey, J. B. The Riemann hypothesis. *Notices of the AMS 50*, 3 (2003), 341–353.

[11] Cox, D. A. The arithmetic-geometric mean of Gauss. In *Pi: A Source Book*. Springer New York, 2000, pp. 481–536.

[12] Cremona, J. E. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 1997.

[13] Cremona, J. E., and Thongjunthug, T. The complex agm, periods of elliptic curves over and complex elliptic logarithms. *Journal of Number Theory 133*, 8 (2013), 2813 – 2841.

[14] Delaunay, C., and Roblot, X.-F. Regulators of rank one quadratic twists. *ArXiv e-prints* (July 2007).

[15] Elkies, N. D. Points of low height on elliptic curves and surfaces i: Elliptic surfaces over $\mathbb{P}^1$ with small d. In *Algorithmic Number Theory*. Springer, 2006, pp. 287–301.

[16] Elkies, N. D., and Stein, W. A. Nontorsion points of low height on elliptic curves over $\mathbb{Q}$, 2002.

[17] Heath-Brown, D. R. The average analytic rank of elliptic curves. *Duke Mathematical Journal 122*, 3 (04 2004), 591–623.

[18] Hindry, M., and Silverman, J. The canonical height and integral points on elliptic curves. *Inventiones mathematicae 93*, 2 (1988), 419–450.

[19] Imamoglu, Ö., Jermann, J., and Tóth, Á. Estimates on the zeros of E_2. *ArXiv e-prints* (Dec. 2013), 1–12.

[20] Iwaniec, H., and Kowalski, E. *Analytic Number Theory*. No. v. 53 in American Mathematical Society colloquium publications. American Mathematical Society, 2004.

[21] Knapp, A. W. *Elliptic Curves*. Mathematical Notes - Princeton University Press. Princeton University Press, 1992.

[22] Koblitz, N. I. *Introduction to Elliptic Curves and Modular Forms*. Graduate Texts in Mathematics. Springer New York, 2012.

[23] Lang, S. *Fundamentals of Diophantine geometry*. Springer Science & Business Media, 1983.

[24] Lang, S. *Survey of diophantine geometry*, corr. 2nd printing ed. Berlin: Springer, 1997.

[25] Manin, Y. I. Cyclotomic fields and modular curves. *Russian Mathematical Surveys 26*, 6 (1971), 7.

[26] Masser, D. W. Open problems. In *Proceedings Symposium Analytic Number Theory, herausgegeben von WWL Chen, London. Imperial College* (1985).

[27] Mazur, B., and Stein, W. How explicit is the explicit formula?, 2013.

[28] Mestre, J.-F. Formules explicites et minorations de conducteurs de varits algbriques. *Compositio Mathematica 58*, 2 (1986), 209–232.

[29] Oesterlé, J. Nouvelles approches du "théorème" de Fermat. *Séminaire Bourbaki 30* (1988), 165–186.

[30] Riemann, B. On the number of primes less than a given magnitude. *Monthly Reports of the Berlin Academy* (1859).

[31] Silverman, J. H. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, Dec 1985.

[32] Silverman, J. H. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 1994.

[33] Stein, W. A. Algebraic number theory: a computational approach, 2012.

[34] Szpiro, L. Présentation de la théorie d'Arakelov. *Current Trends in Arithmetical Algebraic Geometry?, Contemporary Mathematics 67* (1987), 279–293.

[35] Taylor, R., and Wiles, A. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2) 141*, 3 (1995), 553–572.

[36] Wiles, A. Modular elliptic curves and Fermat's Last Theorem. *Ann. of Math. (2) 141*, 3 (1995), 443–551.

[37] Wiles, A. The Birch and Swinnerton-Dyer conjecture, 2014.

[38] Wood, R., and Young, M. P. Zeros of the weight two Eisenstein Series. *ArXiv e-prints* (Dec. 2013), 1–12.

Appendix A

CODE REPO AND BLOG POSTS

The analytic rank estimation code mentioned in this thesis is hosted on GitHub, and is accessible to all free of charge under the GNU General Public License.

- The repo can be found at

  `https://github.com/haikona/GSoC_2014`

  The relevant Sage Trac ticket is

  `http://trac.sagemath.org/ticket/16773`

- Moreover, as it was being written the code was blogged about extensively; the posts on various aspects of the code's functionality can be found at

  `http://mathandhats.blogspot.com/`

VITA

Simon Spicer was born and raised in Johannesburg, South Africa, but has spent the past six years in Seattle pursuing his mathematics PhD at the University of Washington. At the time of completing this thesis he and his wife Kimberly have just welcomed their first child, Bramwell, into the world. In his spare time Simon enjoys writing code, piloting airplanes and attempting to teach his family Afrikaans.