Ph.D Dissertation

Simon Spicer
University of Washington

February 3, 2015

Abstract

Something something elliptic curves and rank.

Contents

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:

$$E : y^2 = x^3 + Ax + B \tag{1.1}$$

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

$$E(\mathbb{Q}) \approx T \times \mathbb{Z}^r, \tag{1.2}$$

where T is a finite group (called the torsion subgroup of E), and r is 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 12; 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 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 1.1. 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

  $$N_p(E) = 1 + \#\left\{(\overline{x}, \overline{y}) \in \mathbb{F}_p^2 : \quad \overline{y} \equiv \overline{x}^3 + A\overline{x} + B \pmod{p}\right\}, \tag{1.3}$$

  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 (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 about p, and can never be very far from that value.

Definition 1.2. For prime p,

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

  $$L_p(s) = \left(1 - a_p(E)p^{-s} + \epsilon(p)p^{-2s}\right)^{-1}, \tag{1.4}$$

  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 $D(E)$ (again, sometimes including/excluding 2 or 3)].

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

$$L(E,s) = \prod_p L_p(E,s) \tag{1.5}$$

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*:

$$L(E,s) = \sum_{n=1}^{\infty} a_n(E) n^{-s}, \tag{1.6}$$

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 to representations only converge absolutely when the real part of s is greater than $\frac{3}{2}$, and conditionally for $\text{Re}(s) > \frac{1}{2}$. However, the modularity theorem of Breuil, Conrad, Diamond, Taylor and Wiles [BCDT01] [TW95] [Wil95] 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 $\text{Re}(s) > 1$, 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 $\text{Re}(s) = 1$; 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 2):

Conjecture 1.3 (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*

$$L(E, 1+s) = s^r \left[a + bs + O(s^2)\right], \tag{1.7}$$

where $a \neq 0$ 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. The BSD conjecture has now been verified for millions of elliptic curves without a single counterexample having been found; it is thus widely held 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 numerical 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 determine if the nth Taylor coefficient of $L(E,s)$ is identically zero, or non-zero but so small that it is indistinguishable from zero given your finite-precision computations?

The short answer is that, for a black box computer, you can't. We need theorems governing the magnitude of the Taylor coefficients – especially the leading coefficient C in the BSD conjecture – in order to make analytic rank explicitly computable. This work establishes those results, and details (assuming standard conjectures) an explicit algorithm with provable complexity to compute the analytic rank of a rational elliptic

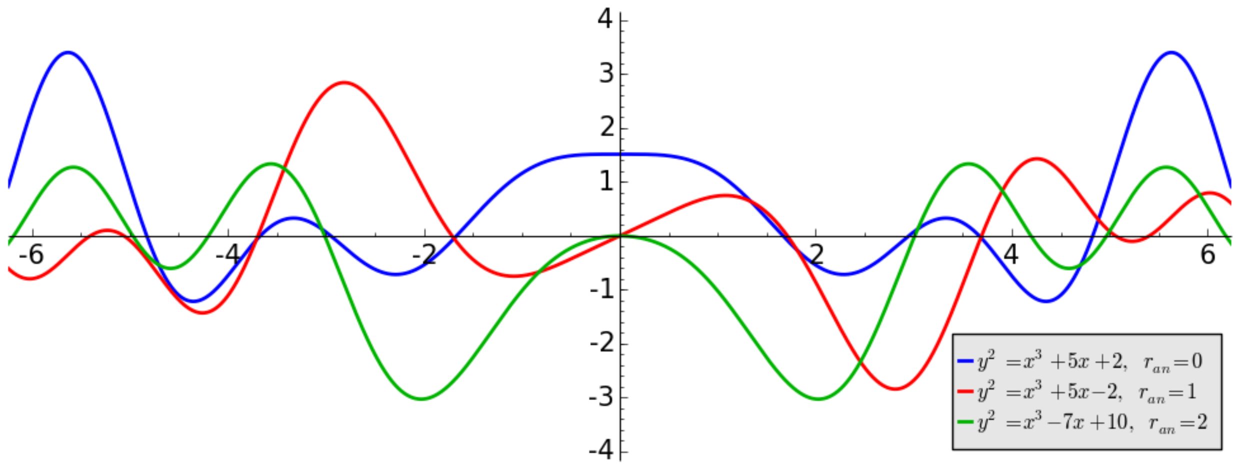

Figure 1.1: The values of three elliptic curve L-functions along the critical line $1 + it$ for $-6 \leq t \leq 6$. Blue corresponds to a rank 0 curve, red is that of a rank 1 curve, and green is a rank 2 curve. Note that close to the origin the graphs look like non-zero constant function, a straight line and a parabola respectively.

curve.

The structure of this dissertation is as follows. Chapter 2 more precisely lays out the problem tackled in this work, quotes the major results obtained to this end and outlines the strategy used to prove these results. 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 is dedicated to supporting numerical data, and chapter 6 contains ancillary results, and ideas for future work.

2 Problem Outline and Major Results

The central question this thesis addresses is thus: Given a rational elliptic curve E, does an algorithm exist to compute the rank of E that has provable time complexity in the conductor of the curve? We answer this question in the affirmative; however, to do so we must pay the price of having to assume three big open conjectures in number theory: the Generalized Riemann Hypothesis, The Birch and Swinnerton-Dyer conjecture, and the ABC conjecture (henceforth referred to as GRH, BSD and ABC respectively).

In this vein we establish the following result:

Theorem 2.1. *Let $E/\mathbb{Q}$ have conductor N. Contingent on BSD, GRH and ABC, there exists an algorithm to compute the algebraic rank r of E in $\tilde{O}(N^{\frac{1}{2}})$ time and $\tilde{O}(1)$ space. That is, for any $\epsilon > 0$ the algorithm is guaranteed to terminate with a correct output in $O(N^{\frac{1}{2}+\epsilon})$ time, using only $O(N^{\epsilon})$ space.*

The aforementioned algorithm is as follows:

Algorithm 2.2 (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:

1. Compute the real period Ω_E of E. This takes $\tilde{O}(1)$ time and space.
2. Let $k = 4 + 10.5 \log_2 N - \log_2 \Omega_E$. The quantity k is guaranteed to be $\tilde{O}(1)$ in size. Set $r = 0$.
3. Evaluate $\frac{L_E^{(r)}(1)}{r!}$, the rth Taylor coefficient of the L-function of E at the central point, to k bits precision. This can be provably computed in $\tilde{O}(k \cdot N^{\frac{1}{2}})$ time and $\tilde{O}(1)$ space. If all k bits are zero, increment r by 1 and repeat step 3. This step is guaranteed to repeat at most $\tilde{O}(1)$ times.
4. Output r and halt.

This algorithm itself is not new – it is just a refinement on bounding the analytic rank of a curve. What is new is the body of results in this dissertation proving that, assuming the three big three letter conjectures, if the nth derivative of the L-series attached to E is zero to k bits precision, then it *is* identically zero. This allows us to convert a polynomial-time algorithm that a priori only provides upper bounds on analytic rank, to one that computes rank exactly.

The proof of Theorem 2.1 can be found in section 12, but will require results established in the preceding sections.

Along the way, we also prove the following interesting results regarding bounds on the locations of the nontrivial zeros of the L-function attached to E:

3 Notation, Definitions and Background

3.1 Notation

For the rest of the body of this text (unless otherwise stated) 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 $r(E)$ 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 often be indicated by a subscript E instead; when there is no ambiguity, it may be dropped entirely.
- p is a (rational) prime number and q is a prime power
- s and z are generic complex numbers
- η is the Euler-Mascheroni constant $= 0.5772156649\dots$
- γ will always be used to denote the imaginary parts of nontrivial zeros of an L-function.

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

- $b_2 = a_1^2 + 4a_2$
- $b_4 = a_1a_3 + 2a_4$
- $b_6 = a_3^2 + 4a^6$
- $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$
- $c_4 = b_2^2 - 24b_4$
- $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$
- $D = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$; this is the definition of the discriminant of E
- $j = \frac{c_4}{D}$
- $\omega = \frac{dx}{2y+a_1x+a_3} = \frac{dy}{3x^2+2a_2x+a_4-a_1y}$

3.2 Definitions

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 3.1. 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

$$\limsup_{x\to\infty} \left|\frac{f(x)}{g(x)}\right| < \infty \tag{3.1}$$

  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 $k > 0$ such that

$$\limsup_{x\to\infty} \left|\frac{f(x)}{g(x)\left(\log g(x)\right)^k}\right| < \infty \tag{3.2}$$

  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 $f(x) = \tilde{O}(g(x))$ is equivalent to the statement that $f(x) = O(g(x)^{1+\epsilon})$ for any $\epsilon > 0$.

Definition 3.2. Let A be an algorithm which takes input n, where for simplicity we may think of n as a positive integer. Let $t_A(n)$ be the running time of A on the input n.

- A is said to have *polynomial time complexity* if there is some $k > 0$ such that the running time of $t_A(n) = O(n^k)$, i.e. the asymptotic running time of the algorithm scales like some polynomial function of n.
- If $t_A(n) = O(n^\epsilon)$ for any $\epsilon > 0$, then A is said to have *sub-polynomial time complexity.* Note that if $t_A(n) = \tilde{O}(1)$, then A has sub-polynomial time complexity.
- If no $k > 0$ exists such that $t_A(n) = O(n^k)$, then A is said to have *super-polynomial time complexity.* More specifically, if there is some $k > 1$ such that $t_A(n) = O(k^n)$, then A is said to have *exponential time complexity.*

The same terminology can be applied to the space requirements of an algorithm, wherein we would replace the word 'time' with 'space'.

3.2.2 Elliptic curves and their L-functions

Definition 3.3. 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 $a1, \ldots a_6 \in K$.

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 minimal and in the above form.

Definition 3.4. 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

$$f(x, y) = y^2 + a_1xy + a_3y^2 - x^3 - a_2x^2 - a_4x - a_6. \tag{3.3}$$

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 $y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6$, then for $p \neq 2$ or 3 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 3.5. 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 3.6. *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 3.3).

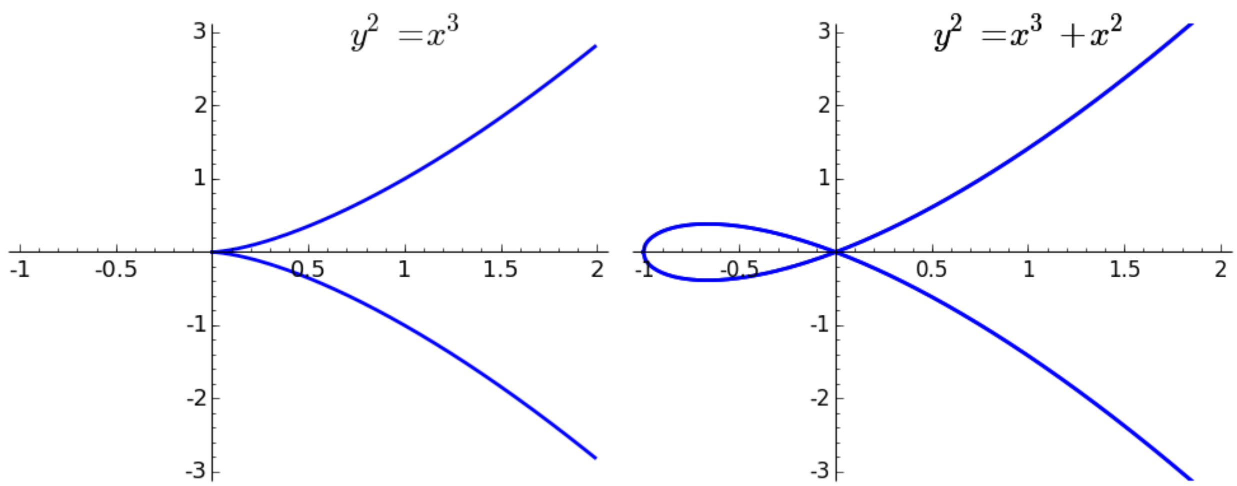

Figure 3.1: An example of two singular cubics over the rationals. The singular point for both curves is at the origin; for the the left curve the singular point is a *cusp*, and for the right curve it is a *node*.

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 3.7. 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 3.8. The conductor of E, denoted by N_E (or more often just N when the choice of E is unambiguous), is a positive integer given by

$$N_E = \prod_p p^{f_p(E)}, \tag{3.4}$$

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

$$f_p(E) = \begin{cases} 0, & \text{E has good reduction at } p \\ 1, & \text{E has multiplicative reduction at } p \\ 2, & E \text{ has additive reduction at } p. \end{cases} \tag{3.5}$$

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 [Sil94, 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 [Sil94, pp. 361-379].

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 3.9.

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

$$a_p(E) = p + 1 - \#\{E(\mathbb{F}_p)\}, \tag{3.6}$$

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

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

$$a_p(E) := \begin{cases} +1 & \text{if } E \text{ has split multiplicative reduction at } p \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p \\ 0 & \text{if } E \text{ has additive reduction at } p. \end{cases} \tag{3.7}$$

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

Theorem 3.10 (Hasse, 1936)**.** *For all elliptic curves $E/\mathbb{Q}$ and all primes p,*

$$|a_p(E)| \leq \sqrt{p} \tag{3.8}$$

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 3.11 (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 3.12.
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

$$L(E,s) = \prod_p \frac{1}{1 - a_p p^{-s} + \epsilon(p)p^{1-2s}} \tag{3.9}$$

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

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

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}. \tag{3.10}$$

  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 3.13.

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

$$\Lambda_E(s) = N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L_E(s), \tag{3.11}$$

where N 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 3.15 (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 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, then there exists some elliptic curve $E/\mathbb{Q}$ of conductor N 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 3.16.

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

$$\Lambda_E(s) = w_E \Lambda_E(2-s), \tag{3.12}$$

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

$$\lambda_E(s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \sum_{n=1}^{\infty} a_n n^{-s} \Gamma\left(s, \frac{2\pi n}{\sqrt{N}}\right), \tag{3.13}$$

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

$$\Lambda_E(s) = \lambda_E(s) + w_E \lambda_E(2-s) \tag{3.14}$$

Knapp goes through the proof of this formula in [Kna92, pp. 270-271].

Definition 3.17. 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 3.18. *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.

We may use Equation 3.13 to produce formulae for the value of $\Lambda_E(s)$ and its higher derivatives at $s = 1$:

Proposition 3.19.

1.

$$\Lambda_E(1) = \begin{cases} \frac{\sqrt{N}}{\pi} \sum_{n=1}^{\infty} \frac{a_n}{n} e^{-\frac{2\pi}{\sqrt{N}} \cdot n}, & w_E = 1 \\ 0, & w_E = -1 \end{cases} \tag{3.15}$$

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

$$\Lambda_E^{(k)}(1) = 2 \sum_{n=1}^{\infty} a_n \int_1^{\infty} \left(\log \frac{t}{\sqrt{N}}\right)^k e^{-\frac{2\pi n}{\sqrt{N}} \cdot t}\, dx \tag{3.16}$$

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

Proof. Observe we may write equation 3.13, after a change of variables and swapping integration and summation signs, as

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

where f_E is the cusp form attached to E. We may differentiate under the integral sign without issue and then evaluate at $s = 1$ to get

$$\lambda_E^{(k)}(1) = \sqrt{N} \cdot \sum_{n=1}^{\infty} a_n \int_{\frac{1}{\sqrt{N}}}^{\infty} (\log t)^k e^{-2\pi n t}\, dt \tag{3.17}$$

Equation 3.16 follows by substituting $t \mapsto \sqrt{N} \cdot t$. For $k = 0$ the integrals may be evaluated directly: $\int_1^{\infty} e^{-\frac{2\pi n t}{\sqrt{N}}}\, dt = \frac{\sqrt{N}}{2\pi n} e^{-\frac{2\pi n}{\sqrt{N}}}$. $\square$

Definition 3.20. 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 $\frac{1}{2} \leq \mathrm{Re}(s) \leq \frac{3}{2}$ 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 3.21. $\Lambda_E(1+s) \neq 0$ *for* $|\mathrm{Re}(s)| > \frac{1}{2}$.

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 section 5 for a proof (the statement can in fact be strengthened to asserting that all zeros are *strictly* inside the critical strip).

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 (stated in full in section 4) asserts that all nontrivial zeros of $L_E(s)$ lie on the critical line $\mathrm{Re}(s) = 1$, and all zeros with nonzero imaginary part are simple.

If $L_E(s)$ has a zero at the central point, it may or may not have multiplicity greater than 1. The multiplicity of this possible zero is denoted the analytic rank of E:

Definition 3.22. 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

$$L_E(z) = a_0 + a_1 z + a_2 z^2 + \ldots \tag{3.18}$$

where $z = s - 1$, 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 3.23.

- 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 $C_E = \frac{\sqrt{N}}{2\pi} \cdot C_E'$. We will most often work with the former, hence the notation.

4 Some 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.

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 4.1 (Birch, Swinnerton-Dyer)**.**

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*

$$C_E^{'} = \left(\frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{Tor}(\mathbb{Q}))^2} \right), \tag{4.1}$$

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,*
- *$\#\text{Ш}(E/\mathbb{Q})$ is the order of the Shafarevich-Tate group attached to $E/\mathbb{Q}$,*
- *$\prod_p c_p$ is the product of the Tamagawa numbers of E, and*
- *$\#E_{Tor}(\mathbb{Q})$ 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 [Wil14].

Conjecture 4.2 (Generalized Riemann Hypothesis for Elliptic Curves, version 1)**.** *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* $\mathrm{Re}(\rho) = 1$. *Moreover, all nontrivial noncentral zeros of $L_E(s)$ are simple.*

That is, all nontrivial zeros of $L_E(s)$ lie on the *critical line* $\mathrm{Re}(s) = 1$, and the only place zeros can lie on top of each other is at the central point $s = 1$. There are numerous equivalent formulations of GRH; we will most often use the following:

Conjecture 4.3 (Generalized Riemann Hypothesis for Elliptic Curves, version 2)**.** *Let E be an elliptic curve over $\mathbb{Q}$, and let $\Lambda_E(s)$ be the completed L-function attached to E. Then*

1. $\Lambda_E(1 + s) = 0 \Longrightarrow \mathrm{Re}(s) = 0$.
2. $\Lambda_E(1 + s) = 0$ *and* $\Lambda'_E(1 + s) = 0 \Longrightarrow s = 0$.

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 4.4 (Masser-Oesterlé)**.** *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*

$$c < K_\epsilon \, \mathrm{rad}(abc)^{1+\epsilon}. \tag{4.2}$$

The ABC conjecture is famous for the large number of other results that it implies. Of these, we will need the following three that relate to elliptic curves:

Conjecture 4.5 (Szpiro)**.** *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 $K(\epsilon)$ such that*

$$|D_E| < K(\epsilon) \cdot (N_E)^{6+\epsilon}. \tag{4.3}$$

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

Conjecture 4.6 (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 $K(\epsilon)$ independent of E such that*

$$\max\left\{|c_4|^3, |c_6|^2\right\} \leq K(\epsilon) \cdot (N_E)^{6+\epsilon} \tag{4.4}$$

Conjecture 4.7 (Lang)**.** *There is a positive constant K 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*

$$\hat{h}(P) \geq K \log |D_E|. \tag{4.5}$$

Conjecture 4.8 (Hall)**.** *For any $\epsilon > 0$ there is a constant $K(\epsilon)$ such that for any $x, y \in \mathbb{Z}$ such that $x^3 - y^2 \neq 0$, we have*

$$|x^3 - y^2| \geq K(\epsilon) \cdot |x|^{\frac{1}{2}-\epsilon}. \tag{4.6}$$

That is, if $x^3 - y^2 \neq 0$, then it cannot be smaller in magnitude than about $\sqrt{|x|}$.

5 Logarithmic Derivatives

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

Definition 5.1. The *logarithmic derivative* of the L-function attached to E is

$$\frac{L_E'}{L_E}(s) := \frac{d}{ds}\log L_E(s) = \frac{L_E'(s)}{L_E(s)}. \tag{5.1}$$

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 5.2.

$$\frac{\Lambda_E'}{\Lambda_E}(s) = \log\left(\frac{\sqrt{N}}{2\pi}\right) + F(s) + \frac{L_E'}{L_E}(s), \tag{5.2}$$

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

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

Note that the digamma function is well-understood and easily computable. For example, it has the following infinite sum expansion about $s = 1$:

$$F(1+s) = -\eta + \sum_{k=1}^{\infty}\frac{s}{k(k+s)} \tag{5.3}$$

This series converges absolutely for any s not equal to a negative integer, and uniformly on sets bounded away from the negative real axis.

What is perhaps surprising, however, is that $\frac{L_E'}{L_E}(s)$ can be represented by an elegant Dirichlet series. Recall that for $p \nmid N$, 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 3.9. 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 5.3. For $n \in \mathbb{N}$, let

$$b_n(E) := \begin{cases} -\left(\alpha_p^e + \beta_p^e\right)\cdot\log(p), & n = p^e \text{ a prime power } (e \geq 1), \text{ and } p \nmid N \\ -a_p^e \cdot \log(p), & n = p^e \text{ and } p \mid N \\ 0, & \text{otherwise,} \end{cases} \tag{5.4}$$

Lemma 5.4. *The Dirichlet series for* $\frac{L_E'}{L_E}(s)$ *is given by*

$$\frac{L_E'}{L_E}(s) = \sum_{n=1}^{\infty} b_n(E)\, n^{-s} \tag{5.5}$$

where the coefficients $b_n(E)$ *are defined as in Definition 5.3.*

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

$$L_E(s) = \prod_{p\mid N}\left(1 - a_p p^{-s}\right)^{-1}\prod_{p\nmid N}\left(1-\alpha_p p^{-s}\right)^{-1}\left(1-\beta_p p^{-s}\right)^{-1}. \tag{5.6}$$

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

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:

Theorem 5.5 (S.)**.**

$$b_n(E) = \begin{cases} -\Big(p^e + 1 - \#\widetilde{E}(\mathbb{F}_{p^e})\Big) \cdot \log(p), & n = p^e \;\; \textit{a prime power,} \\ 0, & \textit{otherwise} \end{cases} \tag{5.7}$$

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 at prime p of good reduction, then

$$\#E(\mathbb{F}_{p^e}) = p^e + 1 - \alpha_p^e - \beta_p^e \tag{5.8}$$

(see [Sil85, pp. 134-136] for a proof), from which the result at $p \nmid N$ follows.

For primes of bad reduction, recall

$$a_p(E) := \begin{cases} +1, & E \text{ has split multiplicative reduction at } p \\ -1, & E \text{ has non-split multiplicative reduction at } p \\ 0, & E \text{ has additive reduction at } p \end{cases} \tag{5.9}$$

Let $E_{\mathrm{ns}}(\mathbb{F}_{p^e})$ be the group of nonsingular points on $\widetilde{E}(\mathbb{F}_{p^e})$.
When E has additive reduction at p, $E_{\mathrm{ns}}(\mathbb{F}_{p^e}) \simeq (\mathbb{F}_{p^e}, +)$, 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, $E_{\mathrm{ns}}(\mathbb{F}_{p^e}) \simeq (\mathbb{F}_{p^e}^*, \times)$, 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 $E_{\mathrm{ns}}(\mathbb{F}_{p^e}) \simeq \ker(\mathrm{Norm}_{L/\mathbb{F}_{p^e}})$.
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 [Sil85, 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 5.6. The logarithmic derivative of the shifted L-function $L_E(1+s)$ is given by Dirichlet series

$$\frac{L'_E}{L_E}(1+s) := \sum_n c_n n^{-s} = \sum_n \frac{b_n}{n} n^{-s}, \tag{5.10}$$

i.e. $c_n = b_n/n$, where the b_n are as defined in Definition 5.3.

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 $\frac{\zeta'}{\zeta}(s) = \sum -\lambda(n) n^{-s}$ for $\mathrm{Re}(s) > 1$, where $\lambda(n)$ is the von Mangoldt function, given by

$$\lambda(n) = \begin{cases} \log p & n = p^e \;\; \text{a perfect prime power,} \\ 0 & \text{otherwise.} \end{cases} \tag{5.11}$$

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 behavior of $L_E(s)$ is tightly constrained.

Lemma 5.7. *Let E be an elliptic curve L-function $L_E(s)$. For $\mathrm{Re}(s) > \frac{1}{2}$ we have*

$$2\frac{\zeta'}{\zeta}\left(\frac{1}{2} + \mathrm{Re}(s)\right) < \left|\frac{L_E'}{L_E}(1+s)\right| < -2\frac{\zeta'}{\zeta}\left(\frac{1}{2} + \mathrm{Re}(s)\right). \tag{5.12}$$

Proof. Let $\sigma = \mathrm{Re}(s)$. By Hasse's Theorem we have that $|q + 1 - \#\widetilde{E}(\mathbb{F}_q)| \leq 2\sqrt{q}$ for any prime power q. Hence

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

The inequality in the middle is strict, as Hasse's bound cannot be hit when n is prime. The left inequality is proved in the same way with the signs reversed. □

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

Corollary 5.8. $\Lambda_E(1+s)$ *has no zeros outside the critical strip* $|\mathrm{Re}(s)| \leq \frac{1}{2}$.

Proof. 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 $|\mathrm{Re}(s)| > \frac{1}{2}$. □

$\Lambda_E(1+s)$ 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 5.9.

1.
$$\Lambda_E(1+s) = C_E \cdot s^{r_{an}} \cdot \prod_{\gamma > 0}\left(1 + \frac{s^2}{\gamma^2}\right) \tag{5.13}$$

   where C_E is the leading coefficient of $L_E(s)$ at the central point (i.e. that defined in Conjecture 4.1), and the product is taken over all 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.
$$\frac{\Lambda_E'}{\Lambda_E}(1+s) = \sum_{\gamma} \frac{s}{s^2 + \gamma^2}, \tag{5.14}$$

   where the sum is taken over **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.*

Note that if we assume GRH (as we always do), then 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 5.14 appears exactly twice. It is therefore often useful to rewrite it as

$$\frac{\Lambda_E'}{\Lambda_E}(1+s) = \frac{r_{an}}{s} + 2\sum_{\gamma > 0} \frac{s}{s^2 + \gamma^2}. \tag{5.15}$$

Proof. Observe that $\Lambda_E(1+s)$ has a zero of order r_{an} 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

$$\Lambda_E(1+s) = C_E s^{r_{an}} \prod_{\gamma \neq 0} \left(1 - \frac{s}{i\gamma}\right), \tag{5.16}$$

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 5.13; logarithmic differentiation then yields Equation 5.15, which can be simplified to Equation 5.14. $\square$

Corollary 5.10. $\frac{\Lambda_E'}{\Lambda_E}(1+s)$ *is an odd function.*

Lemma 5.7 and Equation 5.14 may be used to provide a crude bound on the analytic rank of E with respect to its conductor:

Corollary 5.11. *Let E have analytic rank r and conductor N. Then*

$$r < 1.6 + \frac{1}{2}\log N \tag{5.17}$$

Proof. From Equation 5.14 we have the point estimate

$$r < \sum_{\gamma} \frac{1}{1+\gamma^2} = \frac{\Lambda_E'}{\Lambda_E}(2) \tag{5.18}$$

while from Lemma 5.7 we get

$$\frac{\Lambda_E'}{\Lambda_E}(2) = \log\left(\frac{\sqrt{N}}{2\pi}\right) + F(2) + \frac{L_E'}{L_E}(2) < \frac{1}{2}\log N - \log 2\pi + 1 - \eta - 2\frac{\zeta'}{\zeta}\left(\frac{3}{2}\right), \tag{5.19}$$

where $F(s)$ 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. $\square$

We will later use a related technique to show firstly that the constant of 1.6 can be replaced with -0.4; better yet, we will in fact show that maximum analytic rank grows more slowly than $\epsilon \log N$ for any $\epsilon > 0$.

The following corollary of Proposition 5.9 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 5.12. *Let $\mathrm{Re}(s) > 0$, and write $s = \sigma + i\tau$, i.e. $\sigma > 0$. Then*

$$\sum_{\gamma} \frac{\sigma}{\sigma^2 + (\gamma - \tau)^2} = \mathrm{Re}\left(\frac{\Lambda_E'}{\Lambda_E}(1+s)\right), \tag{5.20}$$

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 5.14 we have

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

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

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

□

Observe that GRH implies that $\operatorname{Re}(\frac{\Lambda_E'}{\Lambda_E}(1+s)) > 0$ for $\operatorname{Re}(s) > 0$, 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 $\operatorname{Re}(\frac{\Lambda_E'}{\Lambda_E}(1+s)) < 0$ for all $\operatorname{Re}(s) < 0$, and $\operatorname{Re}(\frac{\Lambda_E'}{\Lambda_E}(1+s)) = 0 \Rightarrow \operatorname{Re}(s) = 0$.

Mazur and Stein in [MS13] define the *bite* of an elliptic curve L-function:

Definition 5.13. The *bite* of $L_E(s)$ is

$$\beta(E) := \sum_{\gamma\neq 0} \gamma^{-2}, \tag{5.21}$$

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

This quantity ends up controlling the rate of convergence in many of the sums that appear in explicit formula-type relations for $L_E(s)$. 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.

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

Definition 5.14. For positive integer n, the *higher order bite* of order n for $L_E(s)$ is

$$\beta_n(E) := \sum_{\gamma\neq 0} \gamma^{-n}. \tag{5.22}$$

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

Corollary 5.15. *The Laurent expansion of* $\frac{\Lambda_E'}{\Lambda_E}(1+s)$ *about zero is given by*

$$\begin{aligned}
\frac{\Lambda_E'}{\Lambda_E}(1+s) &= \frac{r_{an}}{s} + \beta_2(E)s - \beta_4(E)s^3 + \beta_6(E)s^5 - \dots \quad &(5.23)\\
&= \frac{r_{an}}{s} + \sum_{k=1}^{\infty}\left[(-1)^{k-1}\beta_{2k}(E)\right]s^{2k-1} \quad &(5.24)
\end{aligned}$$

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 5.14 and collecting terms.

Corollary 5.16. *Let $E/\mathbb{Q}$ have conductor N, 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*

$$L_E(1+s) = C'_E\, s^{r_{an}} \left[1 + a \cdot s + b \cdot s^2 + O(s^3)\right] \tag{5.25}$$

Then

$$a = -\left[-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right] \tag{5.26}$$

$$2b = \left[-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right]^2 - \frac{\pi^2}{6} + \beta_E, \tag{5.27}$$

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

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

$$\digamma(1+s) = -\eta - \sum_{k=1}^{\infty} (-1)^k \zeta(k+1) s^k, \tag{5.28}$$

where η is the Euler-Mascheroni constant, and $\zeta(s)$ is the Riemann zeta function.
Thus by equation 5.2 and Corollary 5.15 we have that

$$\frac{L'_E}{L_E}(1+s) = \frac{r_{an}}{s} - \left[-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right] + \left[-\zeta(2) + \sum_{\gamma \neq 0} \gamma^{-2}\right] \cdot s + O(s^2)$$

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

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

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 $\left[-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right]$, inverse sums of even powers of the nontrivial zeros, and $\zeta(n)$ for n a positive integer.

What's also worth pointing out here is that the above suggests that the Taylor expansion about $s = 1$ of the L-series attached to E essentially contains no new information about the curve's attached invariants beyond that which can be found in the first nonzero coefficient - unless that information is somehow encoded in the bites $\beta_{2n}(E)$ for $n \in \mathbb{N}$. Whether this is the case or not, however, is an open question.

6 Zero Sums and the Explicit Formula

Combining equations 5.2, 5.3 and 5.14 we get the following equality:

Proposition 6.1. *Let $E/\mathbb{Q}$ have conductor N. 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 5.3 and 5.6. Then*

$$\sum_\gamma \frac{s}{s^2+\gamma^2} = \left[-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right] + \sum_{k=1}^{\infty} \frac{s}{k(s+k)} + \sum_{n=1}^{\infty} c_n n^{-s} \tag{6.1}$$

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 formula that resemble the above in some way. We reproduce lemma 2.1 from [Bob11], 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 6.2. *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*

$$\hat{f}(y) = \int_{-\infty}^{\infty} e^{-ixy} f(x)\, dx \tag{6.2}$$

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

$$\sum_\gamma f(\gamma) = \frac{1}{\pi}\left[\log\left(\frac{\sqrt{N}}{2\pi}\right)\hat{f}(0) + \mathrm{Re}\int_{-\infty}^{\infty} F(1+it) f(t)\, dt + \frac{1}{2}\sum_{n=1}^{\infty} c_n \left(\hat{f}(\log n) + \hat{f}(-\log n)\right)\right] \tag{6.3}$$

A proof can be found in [IK04, Theorem 5.12]. Note that Equation 6.1 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 6.2. 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 6.3 (S.). *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,*

$$\langle f, \varphi_E \rangle = \int_{-\infty}^{\infty} f(x) \left(\sum_{\gamma \in S_E} \delta(x-\gamma)\right) dx = \sum_{\gamma \in S_E} f(\gamma). \tag{6.4}$$

Then as distributions,

$$\varphi_E = \sum_\gamma \delta(x-\gamma) = \frac{1}{\pi}\left[-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right) + \sum_{k=1}^{\infty}\frac{x^2}{k(k^2+x^2)} + \frac{1}{2}\sum_{n=1}^{\infty} c_n \left(n^{ix} + n^{-ix}\right)\right]. \tag{6.5}$$

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 $0 < \mathrm{Re}(s) \leq 1$.

7 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 [Mes86], and used by Brumer in [Bru92] 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 [HB04].

The method stems from invoking the explicit formula as stated in Lemma 6.2 on a function f of a specific form:

Lemma 7.1. *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*

$$\sum_{\gamma} f(\Delta\gamma) = \frac{1}{\Delta\pi} \log\left(\frac{\sqrt{N}}{2\pi}\right) + \mathrm{Re}\int_{-\infty}^{\infty} \digamma(1+it) f(\Delta t)\, dt + \frac{1}{\Delta\pi} \sum_{n<e^{\Delta R}} c_n \hat{f}\left(\frac{\log n}{\Delta}\right) \tag{7.1}$$

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 6.2, 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, $\sum_\gamma f(\Delta\gamma) = r_{an} + \sum_{\gamma\neq 0} f(\Delta\gamma)$. 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

$$f(x) = \text{sinc}^2(x) = \left(\frac{\sin(\pi x)}{\pi x}\right)^2 \tag{7.2}$$

is what is used by Mestre, Brumer, Heath-Brown in the publications above, and by Bober in [Bob11]. This is due to its Fourier transform is the triangular function:

$$\hat{f}(y) = \int_{-\infty}^{\infty} e^{-ixy} f(x)\, dx = \begin{cases} 1 - \frac{|y|}{2\pi}, & |y| \le 2\pi \\ 0, & |y| > 2\pi \end{cases} \tag{7.3}$$

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

$$\mathrm{Re}\int_{-\infty}^{\infty} \digamma(1+it) f(\Delta t)\, dt = -\frac{\eta}{\pi\Delta} + \frac{1}{2\pi^2\Delta^2}\left(\frac{\pi^2}{6} - \mathrm{Li}_2\left(e^{-2\pi\Delta}\right)\right), \tag{7.4}$$

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

Combining the above, we get a specialization of Lemma 7.1:

Corollary 7.2. *Let γ range over the nontrivial zeros of $L_E(s)$, and let $\Delta > 0$. Then*

$$\sum_{\gamma} sinc^2(\Delta\gamma) = \frac{1}{\Delta\pi}\left[\left(-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right) + \frac{1}{2\pi\Delta}\left(\frac{\pi^2}{6} - Li_2\left(e^{-2\pi\Delta}\right)\right) + \sum_{n<e^{2\pi\Delta}} c_n \cdot \left(1 - \frac{\log n}{2\pi\Delta}\right)\right] \tag{7.5}$$

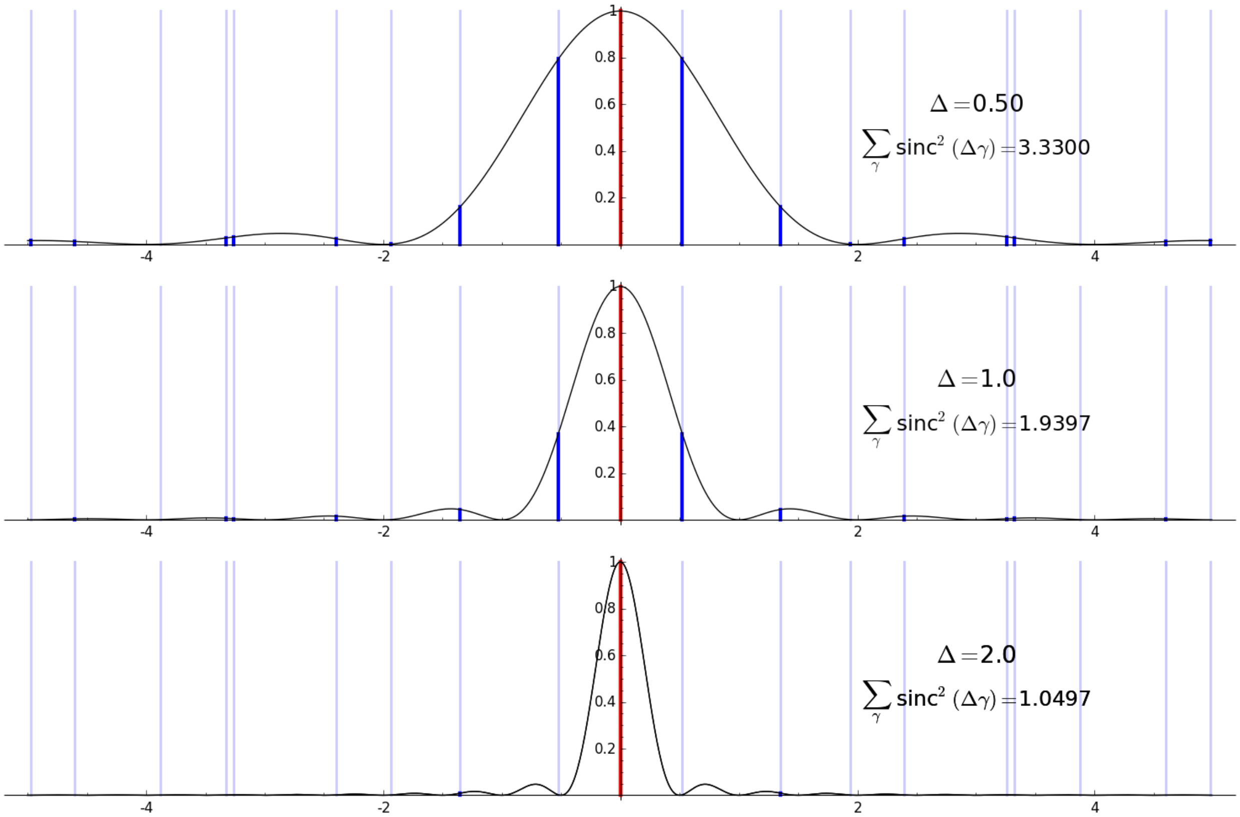

Figure 7.1: A graphic representation of the sinc^2 sum for the elliptic curve $E : y^2 = x^3 - 18x + 51$, a rank 1 curve with conductor $N = 750384$, for three increasing values of the parameter Δ. Vertical lines have been plotted at $x = \gamma$ whenever $L_E(1 + i\gamma) = 0$ – red for the single central zero, and blue for noncentral zeros; the height of the darkened portion of each line is given by the black curve $\mathrm{sinc}^2(\Delta x)$. 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.

What's notable about the above formula is that 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.

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 $\log(N)$:

Corollary 7.3. *For any $\epsilon > 0$ there is a constant $K_\epsilon > 0$ such that for any $E/\mathbb{Q}$ with conductor N, we have*

$$r_{an}(E) < \epsilon \log N + K_\epsilon \tag{7.6}$$

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 7.5 is equal to $\frac{1}{2\pi\Delta} \log N$ 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. $\square$

[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 $\sqrt{\log N}$ (existing numerical evidence would seem to support this), but this is still very much an open problem.]

Choosing $\epsilon = \frac{1}{2}$ and collecting and bounding all the conductor-independent terms allows us to improve upon Corollary 5.11:

Corollary 7.4. *Let E have analytic rank r and conductor N. Then*

$$r < \frac{1}{2}\log N - 0.4 \tag{7.7}$$

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

Finally, one other thing worth noting is that when $\Delta \leq \frac{\log 2}{2\pi}$, the c_n sum is empty. Thus we have the following:

Corollary 7.5. *Let $E/\mathbb{Q}$ have conductor N. Let η be the Euler-Mascheroni constant $= 0.5772\ldots$, and let γ range over the nontrivial zeros of $L_E(s)$. Then*

$$\sum_{\gamma} sinc^2\left(\frac{\log 2}{2\pi}\cdot\gamma\right) = \frac{\log N}{\log 2} + K, \tag{7.8}$$

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 7.5 at $\Delta = \frac{\log 2}{2\pi}$ and simplify, noting that $\mathrm{Li}_2\left(\frac{1}{2}\right) = \frac{\pi^2}{6} - \frac{(\log 2)^2}{2}$. ☐

8 The Distribution of Nontrivial Zeros

Definition 8.1. For non-negative t, let $M_E(t)$ be the modified non-trivial zero counting function for $L_E(s)$, i.e.

$$M_E(t) := \sum_{|\gamma|\le t}{}' \frac{1}{2} \tag{8.1}$$

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, where r is the analytic rank of E.

Note that $M_E(0) = \frac{r}{2}$, 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.

Proposition 8.2 (S.).

$$M_E(t) = \frac{1}{\pi}\left[\left(-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right)t + \sum_{k=1}^{\infty}\left(\frac{t}{k} - \arctan\left(\frac{t}{k}\right)\right) + \sum_{n=1}^{\infty}\frac{c_n}{\log n}\cdot\sin(t\log n)\right] \tag{8.2}$$

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

$$f_t(x) = \begin{cases} \frac{1}{2}, & |x| < t \\ \frac{1}{4}, & |x| = t \\ 0 & |x| > t \end{cases} \tag{8.3}$$

Informally, we obtain the above formula by integrating both sides of Equation 6.5 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 8.2 converges point wise to $M_E(t)$ as m and $n \to \infty$. $\square$

Equation 8.2 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 locations. 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

$$\frac{1}{\pi}\left[\left(-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right)t + \sum_{k=1}^{\infty}\left(\frac{t}{k} - \arctan\left(\frac{t}{k}\right)\right)\right] \tag{8.4}$$

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

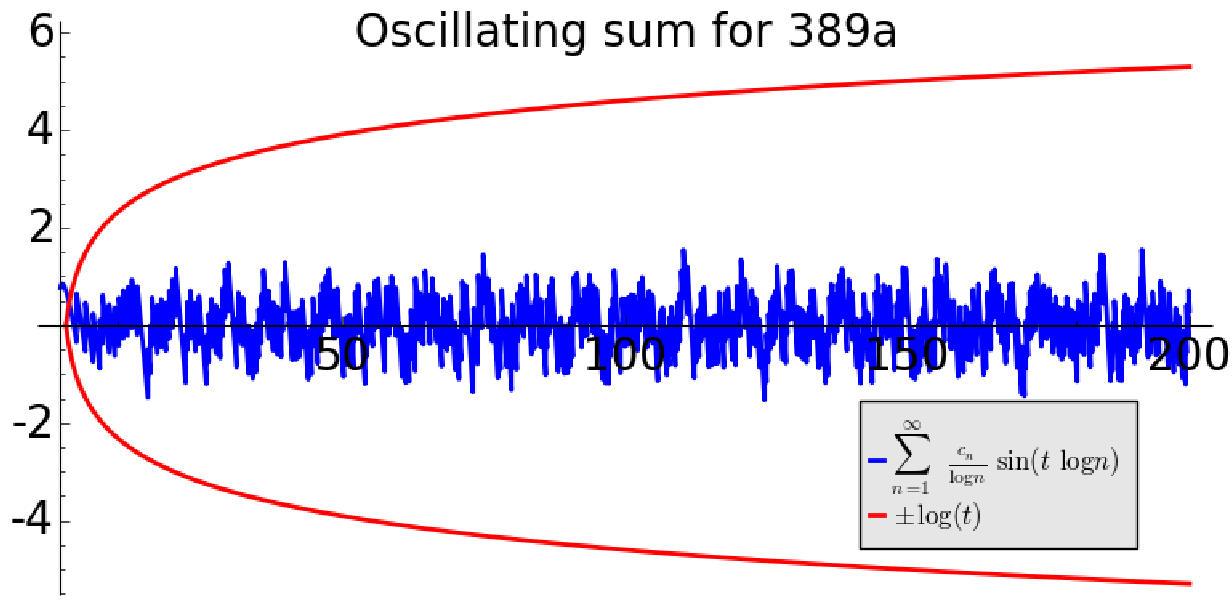

Figure 8.1: The oscillating sum $\sum_{n=1}^{\infty} \frac{c_n}{\log n} \cdot \sin(t \log n)$ for the curve with Cremona label $389a$ (with equation $y^2 + y = x^3 + x^2 - 2x$) versus $\pm \log(t)$ for $0 \leq t \leq 200$. Numerically we actually see the maximum value of the sum grow slower than $\log(t)$ - possibly $\log(t)^{\alpha}$ for some $0 < \alpha < 1$, or even $\log\log(t)$.

Conjecture 8.3.

$$\sum_{n=1}^{\infty} \frac{c_n}{\log n} \cdot \sin(t \log n) = O(\log t) \tag{8.5}$$

This statement should follow from GRH, and is borne out by numerical evidence:

Lemma 8.4. *For $t >> 0$,*

$$\sum_{k=1}^{\infty} \left(\frac{t}{k} - \arctan\left(\frac{t}{k}\right)\right) = t \log t + (\eta - 1)t + \frac{\pi}{4} + O\left(\frac{1}{t}\right), \tag{8.6}$$

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

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:

$$\mathrm{Re}\left(\digamma(1+ix)\right) = \log x + \frac{1}{12}x^{-2} + O(x^{-4}) \tag{8.7}$$

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. $\square$

Conjecture 8.3 and lemma 8.4 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 8.5 (S.). *Let E have conductor N. Then for $t >> 0$ we have*

$$M_E(t) = \frac{t}{\pi} \log\left(\frac{t\sqrt{N}}{2\pi e}\right) + \frac{1}{4} + O(\log t), \tag{8.8}$$

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

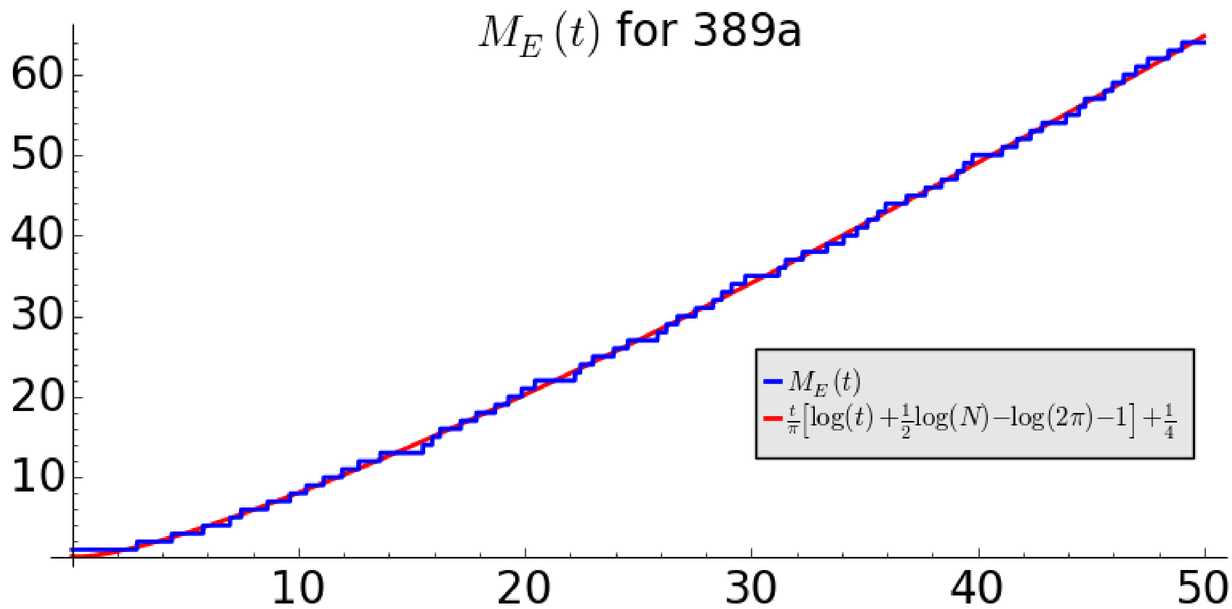

Figure 8.2: The number of zeros up to t versus $\frac{t}{\pi}\left[\log\left(\frac{t\sqrt{N}}{2\pi}\right)-1\right]+\frac{1}{4}$ for the Cremona curve $389a$. The match up is extremely good.

Corollary 8.6. *For $t >> 0$, the number of zeros on the critical line in a unit interval*

$$M_E(t) - M_E(t-1) = \frac{1}{\pi} \log\left(\frac{t\sqrt{N}}{2\pi}\right) + O(\log t), \tag{8.9}$$

where again the error term contributes no net bias.

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

Neglecting the oscilating error term in Equation 8.8, 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 8.7. *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. Then*

$$\gamma_n \sim \frac{2\pi e}{\sqrt{N}} \cdot \exp\left(W_0\left[\left(\frac{r}{2}+n-\frac{3}{4}\right)\cdot\frac{\sqrt{N}}{2e}\right]\right) \tag{8.10}$$

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 8.8 sans the oscillating error term, we solve for t in

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

□

[Aside: The principle branch of the Lambert W-function has the asymptotic expansion $W_0(x) = \log x - \log\log x + o(1)$, for $n >> 0$ 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:

$$\lim_{n\to\infty} \frac{\gamma_n}{\frac{n}{\log n}} = \pi \tag{8.11}$$

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 8.8. 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.

$$\delta_n = \gamma_n - \frac{2\pi e}{\sqrt{N}} \cdot \exp\left(W_0\left[\left(\frac{r}{2} + n - \frac{3}{4}\right) \cdot \frac{\sqrt{N}}{2e}\right]\right) \tag{8.12}$$

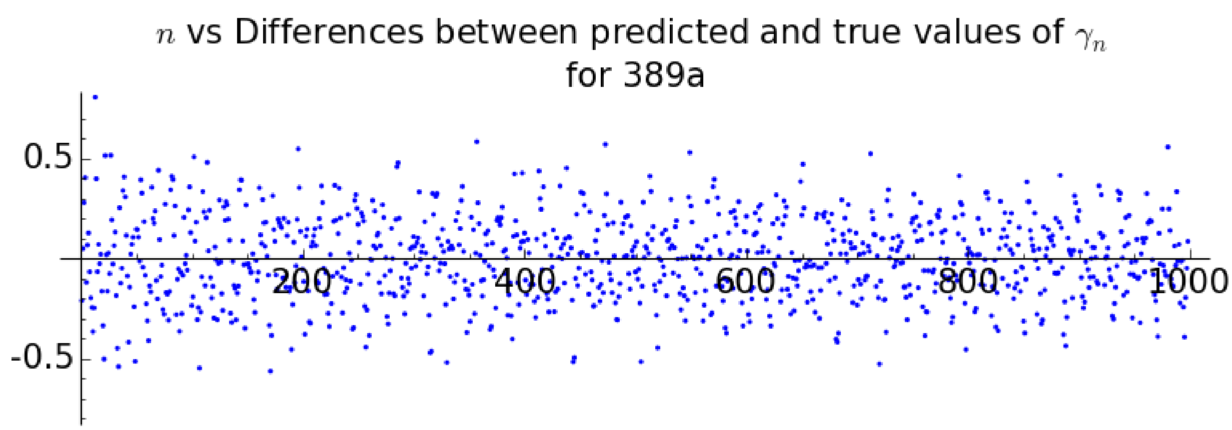

Figure 8.3: A scatter plot of zero dispersions for the first 1000 nontrivial zeros of the Cremona curve 389a, the rank 3 curve with smallest conductor. The values are seldom more than $\frac{1}{2}$.

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.

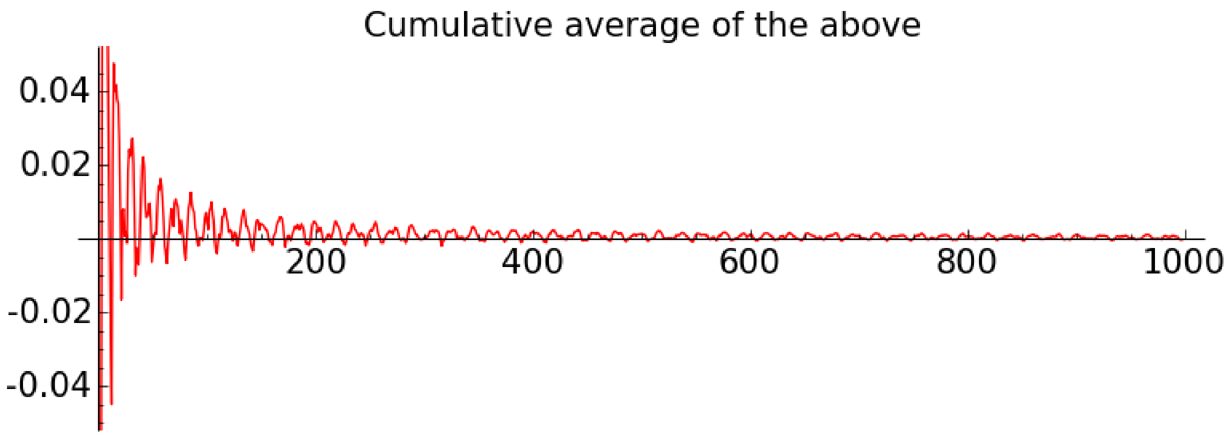

Figure 8.4: A cumulative average plot of the above, showing clearly that asymptotically, the average difference between the predicted and true values of γ_n is zero. The positive bias at the beginning comes from the $O(1/t)$ term in Lemma 8.4. Interestingly, although the deviations might a priori appear 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.

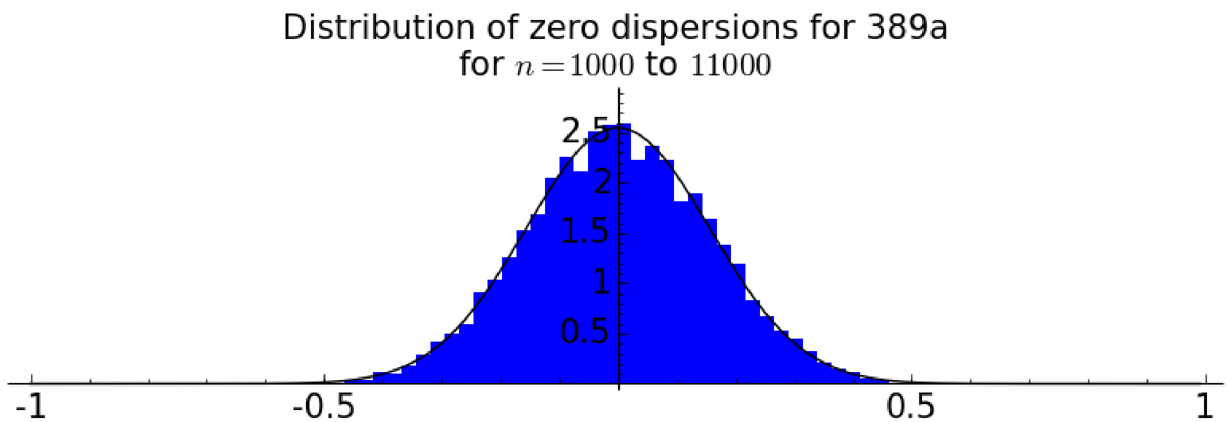

Figure 8.5: A histogram of zero dispersions for the curve 389 for the 1000th through 11000th zeros (we discard the first 1000 zeros to avoid the small-height bias observable in the the cumulative average plot above.

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. 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 8.2 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:

Proposition 8.9. *For a curve E with large conductor N, the best guess for the imaginary part of the first* *nontrivial noncentral zero* γ_1 *of* $L_E(s)$ *in the upper half plane is*

$$\gamma_1 = \frac{(r+1)\pi}{\log(N) - 2\log(2\pi) - 2\eta} \tag{8.13}$$

where r *is the analytic rank of* E

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 $r/2$ to $r/2+1$; at that point $M_E(t) = r/2 + 1/2 = \frac{r+1}{2}$, so the expected value of γ_1 is given by setting equation 8.2 equal to $\frac{r+1}{2}$ 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 8.4 is dominated by the $\frac{1}{\pi}\left(-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right)t$ term when N is large. Solving for t yields the desired value.

9 The Bite and the Central Leading Coefficient

It is a relatively straightforward affair to obtain unconditional upper bounds on the magnitude of C_E, the central leading coefficient of $L_E(s)$, as a function of the curve's conductor; this can be achieved by doing some analysis on $\frac{\Lambda_E'}{\Lambda_E}(1+s)$ and the bite β_E. Lower bounds are more difficult, however. It is only by assuming full BSD that we have any way of obtain C_E from below.

As zero density on the critical line grows proportional to $\frac{1}{2}\log N$ (see Theorem 8.5), we expect the bite $\beta_E = \sum_{\gamma\neq 0}\gamma^{-2}$ to grow like $\frac{1}{2}\log N$. This is indeed the case, at least in terms of concrete lower bounds on β_E:

Lemma 9.1 (S.). *For all $\epsilon > 0$ there is a constant $K_\epsilon > 0$ such that for all elliptic curves E, the bite of E obeys*

$$\beta_E = \sum_{\gamma\neq 0}\frac{1}{\gamma^2} > \frac{1}{2+\epsilon}\log N - K_\epsilon. \tag{9.1}$$

where N is the conductor of E.

Proof. □

Proposition 9.2. *Let E have completed L-function $\Lambda_E(s)$ and analytic rank r. Then*

$$\beta_E \cdot C_E = \frac{\Lambda_E^{(r+2)}(1)}{(r+2)!},. \tag{9.2}$$

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 5.13 we have that

$$\Lambda_E(1+s) = C_E\left(s^r + \beta_E s^{r+2} + O(s^{r+4})\right) \tag{9.3}$$

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

From this we derive a straightforward way to compute the bite of E from the rth and $(r+2)$th Taylor coefficients of the L-series attached to E (this of course relies on knowing the analytic rank of E):

Corollary 9.3.

$$\beta_E = \frac{1}{(r+1)(r+2)}\cdot\frac{\Lambda_E^{(r+2)}(1)}{\Lambda_E^{(r)}(1)} \tag{9.4}$$

$$= \frac{2}{(r+1)(r+2)}\cdot\frac{L_E^{(r+2)}(1)}{L_E^{(r)}(1)} - \left(-\eta + \log\left(\frac{\sqrt{N}}{2\pi}\right)\right)^2 + \frac{\pi^2}{6} \tag{9.5}$$

Proof. The first line follows immediately from Proposition 9.2 and the fact that $C_E = \frac{\Lambda^{(r)}(1)}{r!}$. The second line comes from the formula for the $(r+2)$th Taylor coefficient of L_E at the central point derived in Corollary 5.16. □

This allows us to compute the bite of a curve *without* having to compute the locations of the zeros themselves. Moreover, the bite can be computed to arbitrary precision in polynomial time (in the conductor and the number of bits of precision) using, for example, Tim Dokchitser's `computel` PARI code, which can compute the Taylor series expansion of a motivic L-function at a given point.

To establish bounds on the coefficients of the Taylor expansion of $\Lambda_E(s)$ about the central point, we will need the following technical lemma:

Lemma 9.4. *Let $N, n \in \mathbb{Z}_{>0}$, and suppose k is a positive integer such that $k < \frac{1}{2}\log N$. Then*

$$\left|\int_{\frac{1}{\sqrt{N}}}^{\infty} (\log t)^k e^{-2\pi n t}\, dt\right| < \frac{\left(\frac{1}{2}\log N\right)^k}{2\pi n}\left[e^{-\frac{2\pi n}{\sqrt{N}}} + \frac{e^{-2\pi n\sqrt{N}}}{2\pi n\sqrt{N}}\right]. \tag{9.6}$$

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

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

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

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

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

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

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 kth Taylor coefficient of $\Lambda_E(s)$ at the central point.

Proposition 9.5. *Let E have conductor N and completed L-function $\Lambda_E(s)$. Then so long as $k < \frac{1}{2}\log N$, the kth derivative of $\Lambda_E(s)$ at the central point is bounded explicitly in terms of N and k by*

$$\left|\Lambda_E^{(k)}(1)\right| < \frac{(\frac{1}{2}\log N)^k}{2\pi^2}\left(N + \frac{1}{e^{2\pi\sqrt{N}} - 1}\right). \tag{9.7}$$

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

Proof. From Lemma 9.4 and Equation 3.17 we have that

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

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

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

Now

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

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

Note that for fixed N, if we allow $k \to \infty$, we actually have that the kth derivative can grow like $O\left(\frac{k!!}{(2\pi e)^{k/2}}\right)$, where $k!! = k(k-2)\cdots$ is the double factorial on k - i.e., faster than exponentially in k. However, this behavior only starts to show when $k >> \log N$ - hence our restriction on the magnitude of k. 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 $\log N$ (c.f. Corollary 5.11), we will never need to consider $\Lambda_E^{(k)}(1)$ for $k > \frac{1}{2}\log N$.

10 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 $D < 0$, as this makes some of the presentation more natural. Given that we are only interested in the real period below, however, this is a philosophical debate best left to another time.]

Definition 10.1. Let $E/\mathbb{Q}$ have discriminant D, 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

$$\Omega_E = \begin{cases} 2\omega_1 & D > 0 \\ \omega_1 & D < 0 \end{cases} \tag{10.1}$$

The real generator ω_1 may be computed using the (real version of the) Gauss arithmetic-geometric mean. Recall its definition: 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. We omit the proof that both sequences converge to the same value, but convergence is quadratic (i.e. extremely quick).

Proposition 10.2. *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*

$$\left(y + \frac{a_1x + a_3}{2}\right)^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} = (x - e_1)(x - e_2)(x - e_3) \tag{10.2}$$

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 at the beginning of section 3.

1. *If $D > 0$, 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*

$$\omega_1 = \frac{\pi}{AGM(\sqrt{e_3 - e_1}, \sqrt{e_3 - e_2})} \tag{10.3}$$

2. *If $D < 0$, 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*

$$\omega_1 = \frac{\pi}{AGM(|z|, s)} \tag{10.4}$$

Proof. Cremona and Cremona-Thongjunthug give a good explanations and derivations this formula in [Cre97] and [CT13] respectively. ☐

Using the above we can readily establish an upper bound on Ω_E:

Proposition 10.3. *Let E have discriminant D and real period Ω_E. Then*

$$\Omega_E < \pi D^{-\frac{1}{12}} \tag{10.5}$$

where the factor of 2 may be omitted if $D < 0$. That is, the real period goes to zero as the discriminant of the curve goes to infinity.

Proof. Cheese ☐

Corollary 10.4. *Assuming 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 10.2 that Ω_0 can be computed by a) finding the roots of a cubic polynomial, and then b) applying the AGM to a certain simple function there.

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 4.6) the conductor of of a curve is bounded 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.

The AGM converges quadratically when both the inputs are positive real. Hence step b) t ☐

Note that the real period is *not* invariant under isomorphism over $\mathbb{Q}$. As the elliptic discriminant D 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. We formalize this statement with the following:

Lemma 10.5. *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 $\mathbb{Q}$-isomorphic to E, and let $D_{E'}$ and $\Omega_{E'}$ be defined analogously. Then there exists a $u \in \mathbb{Z}$ such that $D_{E'} = u^{12} D_E$ and $\Omega_{E'} = \frac{1}{u}\Omega_E$.*

A proof of the result regarding the discriminant can be found on pages 48-49 of [Sil85]; the result regarding the real period follows, for example, from chasing through how the a- and b-invariants change under isomorphism in Proposition 10.2.

Regardless of the model chosen, however, we can establish a lower bound on the real period Ω_E in terms of that model's b-invariants:

Lemma 10.6 (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 the invariants b_2, b_4 and b_6 as at the beginning of section 3. Then*

$$\Omega_E > \frac{\alpha\pi}{\sqrt{1 + \frac{1}{4}\max\{|b_2|, 2|b_4|, |b_6|\}}}, \tag{10.6}$$

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

Proof. Let

$$d(E) = \max\left\{|e_i - e_j| : \ e_i, e_j \text{ are roots of } 4x^3 + b_2x^2 + 2b_4x + b_6, i \neq j\right\} \tag{10.7}$$

be the maximum root separation of the cubic polynomial on the RHS of equation 10.2. Observe that for both positive and discriminant cases, the AGM in the denominators in equations 10.3 and 10.4 is at most $\sqrt{d}$.

We now apply Rouche's Theorem on $x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$. Observing that $|\frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}| < |x^3|$ when $|x| < 1 + \max\left\{\frac{|b_2|}{4}, \frac{|b_4|}{2}, \frac{|b_6|}{4}\right\}$, we obtain that $|e_i| < 1 + \frac{1}{4}\max\{|b_2|, 2|b_4|, |b_6|\}$. Hence

$$\omega_1 \geq \frac{\pi}{\sqrt{\delta}} > \frac{\pi}{2\sqrt{1 + \frac{1}{4}\max\{|b_2|, 2|b_4|, |b_6|\}}}.$$

The result follows. ☐

This bound is close to 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

$$E_n : \ \ y^2 = x^3 - (nx - 1)^2. \tag{10.8}$$

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

$$\Omega_{E_n} = \frac{2\pi}{n} + O\left(\frac{1}{n}\right). \tag{10.9}$$

On the other hand, for a given n

$$1 + \frac{1}{4}\max\{|b_2|, 2|b_4|, |b_6|\} = 1 + n^2. \tag{10.10}$$

for $n \geq 2$. So for this family of curves the lower bound given by inequality 10.6 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 exponent.

Finally, if we assume the Szpiro conjecture, Conjecture 10.6 allows us to the real period of a minimal model of E from below in terms of that curve's conductor. Recall the Szpiro Conjecture: if D_E is the discriminant of a minimal model of E and N_E its conductor, then for any $\epsilon > 0$ there is a constant $K(\epsilon)$ independent of E such that $|D_E| \leq K(\epsilon) \cdot (N_E)^{6+\epsilon}$. In other words, the minimal discriminant of a curve can't be much bigger than the $(6+\epsilon)$th power of its conductor.

We will invoke a slight reformulation of Modified Szpiro (Conjecture 4.6): 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 $K(\epsilon)$ independent of E such that

$$\max\left\{|A|^3, |B|^2\right\} \leq K(\epsilon) \cdot (N_E)^{6+\epsilon} \tag{10.11}$$

(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 entirely equivalent). Using this, we obtain the following:

Proposition 10.7. *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 $K(\epsilon)$, independent of E, such that*

$$\Omega_E > K(\epsilon) \cdot (N_E)^{-\frac{3}{2}-\epsilon} \tag{10.12}$$

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 10.6 the real period of E obeys

$$\Omega_E > \frac{\pi}{2\sqrt{1 + \max\{|A|, |B|\}}} \tag{10.13}$$

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 10.13, the result follows. □

Note that this is an overly conservative lower bound on Ω_E: in reality we see

The 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 10.8. *Let E have conductor N_E, and let Ω_E be the real period of a minimal model of E. Then*

$$\Omega_E > (N_E)^{-2} \tag{10.14}$$

11 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.

Definition 11.1. The *naïve logarithmic height* of P is a measure of the "complexity" of the coefficients of P. Specifically, any non-identity rational point P may be written as $P = (\frac{a}{d^2}, \frac{b}{d^3})$, with $a, b, d \in \mathbb{Z}$, $d > 0$ and $\gcd(a, b, d) = 1$; we then define the naïve height of P to be

$$h(P) := \ln(d). \tag{11.1}$$

Moreover, define $h(\mathcal{O}) = 0$.

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

$$\hat{h}(P) := \lim_{n\to\infty} \frac{h(2^n P)}{(2^n)^2}, \tag{11.2}$$

where h is the naïve logarithmic height defined above.

Theorem 11.3 (Néron-Tate)**.** *Néron-Tate has defines a canonical quadratic form on $E(\mathbb{Q})$ modulo torsion. That is,*

1. *For all $P, Q \in E(\mathbb{Q})$,*
$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\left[\hat{h}(P) + \hat{h}(Q)\right] \tag{11.3}$$
i.e. $\hat{h}$ obeys the parallelogram law;
2. *For all $P \in E(\mathbb{Q})$ and $n \in \mathbb{Z}$,*
$$\hat{h}(nP) = n^2 \hat{h}(P) \tag{11.4}$$
3. *$\hat{h}$ is even, and the pairing $\langle\ ,\ \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}$ by*
$$\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q) \tag{11.5}$$
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 [Sil85, pp. 227-232].

Definition 11.4. 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

$$\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q) \tag{11.6}$$

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 $E(\mathbb{Q})/E_{\text{tor}}(\mathbb{Q}) \hookrightarrow \mathbb{R}^r$ under the quadratic form $\hat{h}$ as a (rank r) lattice.

Definition 11.5. The *regulator* Reg_E of $E/\mathbb{Q}$ is the covolume of the lattice that is the image of $E(\mathbb{Q})$ under $\hat{h}$. That is, if $\{P_1, \ldots, P_r\}$ generates $E(\mathbb{Q})$, then

$$\mathrm{Reg}_E = \det\left(\langle P_i, P_j \rangle\right)_{1 \leq i,j \leq r} \tag{11.7}$$

where $(\langle P_i, P_j \rangle)_{1 \leq i,j \leq r}$ 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 if $E/\mathbb{Q}$ has rank 1, then its regulator is just the smallest height of a non-torsion point $P \in E(\mathbb{Q})$.

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.

It is straightforward exercise to construct elliptic curves with arbitrarily large regulators. For example, one could fix some x_0 and y_0 with large denominators, and then find A and B such that $P = (x, y)$ lies on $E : y^2 = x^2 + Ax + B$. The more interesting question to ask – and the one that is relevant to this thesis – is "how small can the regulator get?". Specifically, given $E/\mathbb{Q}$ with discriminant D_E, what is the smallest Reg_E can be as a function of D_E?

This is an open question. However, the following conjecture has been made by Lang [Lan97]:

Conjecture 11.6. *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*

$$\hat{h}(P) >= M_0 \log |D_E|. \tag{11.8}$$

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 [HS88] show that the ABC conjecture implies Lang's height conjecture and give an explicit lower bound on M_0:

$$M_0 \geq 6 \times 10^{-11} \tag{11.9}$$

Since we are already assuming strong ABC, we have this result for free.

There is general agreement in the literature is that the value of M_0 above is in no way close to being optimal; however, there is no strong consensus as to how much larger M_0 could be. A survey by Elkies and Stein [ES02] 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 the data compiled by Elkies and Stein, it seems quite likely that there are as-yet undiscovered instances of points with exceptionally low height driving the quantity down even further.

One can make the more conservative following observation:

Corollary 11.7. *Assuming BSD, 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*

$$\hat{h}(P) >= M_1. \tag{11.10}$$

The smallest absolute point height found in the aforementioned Elkies-Stein survey 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 Elkies' 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 Hindry-Silverman bound above would seem so small as to be useless in all practical applications, we can use it to bound a curve's regulator from below in terms of an inverse power of its conductor.

Theorem 11.8. *Let $E/\mathbb{Q}$ have conductor N_E. Assuming BSD, GRH and Conjecture 11.6, we have that*

$$\mathrm{Reg}_E \geq 4429.16 \cdot N_E^{-10.49} \tag{11.11}$$

Proof. For curves of conductor ≤ 350000, we consulted Cremona's tables and verified numerically that the inequality holds. Thus without loss of generality we may assume $D_E > N_E > 350000$. Thus for any point $P \in E(\mathbb{Q})$ by Conjecture 11.6 we have that

$$\hat{h}(P) >= 6 \times 10^{-11} \cdot \log|D_E| \geq 6 \times 10^{-11} \cdot \log(350000) = 7.6594 \times 10^{-10} \tag{11.12}$$

Let r be the algebraic rank of E. Since Reg_E is the volume of the co-lattice of point heights in $\mathbb{R}^r$, we must have that

$$\mathrm{Reg}_E \geq \left(\min\left\{\hat{h}(P),\ P \in E(\mathbb{Q})\right\}\right)^r \geq K^r,$$

where $K = 7.6594 \times 10^{-10}$. By BSD, $r = r_{an}$ so (assuming GRH) Corollary 7.4 has $r < \frac{1}{2}\log N_E - 0.4$. Thus

$$\begin{aligned}\mathrm{Reg}_E &\geq K^{\frac{1}{2}\log N_E - 0.4} \\ &= K^{-0.4} \cdot (N_E)^{\frac{1}{2}\log K} \\ &= 4429.16\ldots \cdot (N_E)^{-10.494957\ldots}\end{aligned}$$

□

Note that the first step isn't strictly necessary, and only serves to improve the constants in bound by a small amount. However, it serves to highlight that the power of N_E in this bound could 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 we instead get

$$\mathrm{Reg}_E \geq 6.6064\,(N_E)^{-2.36} \tag{11.13}$$

Even so, we do *not* expect this 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. 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 11.8 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 2.2.

12 Proof of the Main Theorem

In this section we prove Theorem 2.1: specifically, that Algorithm 2.2 is guaranteed, assuming BSD, GRH and ABC, 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.

Proof. Cheese $\square$

13 Remarks and Future Work

References

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic). MR 1839918 (2002d:11058)

[Bob11] Jonathan W. Bober, *Conditionally bounding analytic ranks of elliptic curves*, The arXiv (2011), 1–9.

[Bru92] Armand Brumer, *The average rank of elliptic curves i*, Inventiones mathematicae **109** (1992), no. 1, 445–472 (English).

[Cre97] John E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, 1997.

[CT13] John E. Cremona and Thotsaphon Thongjunthug, *The complex agm, periods of elliptic curves over and complex elliptic logarithms*, Journal of Number Theory **133** (2013), no. 8, 2813 – 2841.

[ES02] Noam D. Elkies and William A. Stein, *Nontorsion points of low height on elliptic curves over q*, 2002.

[HB04] D. R. Heath-Brown, *The average analytic rank of elliptic curves*, Duke Mathematical Journal **122** (2004), no. 3, 591–623.

[HS88] M. Hindry and J.H. Silverman, *The canonical height and integral points on elliptic curves*, Inventiones mathematicae **93** (1988), no. 2, 419–450 (English).

[IK04] Henry Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society colloquium publications, no. v. 53, American Mathematical Society, 2004.

[Kna92] Anthony W. Knapp, *Elliptic curves*, Mathematical Notes - Princeton University Press, Princeton University Press, 1992.

[Lan97] Serge Lang, *Survey of diophantine geometry*, corr. 2nd printing ed., Berlin: Springer, 1997 (English).

[Mes86] Jean-Franois Mestre, *Formules explicites et minorations de conducteurs de varits algbriques*, Compositio Mathematica **58** (1986), no. 2, 209–232 (French).

[MS13] Barry Mazur and William Stein, *How explicit is the explicit formula?* (English).

[Sil85] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, Springer, Dec 1985.

[Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, Springer, 1994.

[TW95] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572. MR 1333036 (96d:11072)

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR 1333035 (96d:11071)

[Wil14] ———, *The birch and swinnerton-dyer conjecture*, 2014.