Ph.D Dissertation

Simon Spicer
University of Washington

August 25, 2014

Abstract

Something something elliptic curves and rank.

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 $\Delta(E)$ of the curve, given by $\Delta(E) = -16(4A^3 + 27B^2)$, 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
$$N_p(E) = 1 + \#\left\{(\overline{x}, \overline{y}) \in \mathbb{F}_p^2 : \ \overline{y} \equiv \overline{x}^3 + A\overline{x} + B \pmod{p}\right\}, \tag{1.3}$$
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 $\Delta(E)$ (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 $\mathrm{Re}(s) > \frac{1}{2}$. 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 $\mathrm{Re}(s) > 1$, 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 $\mathrm{Re}(s) = 1$; moreover, because the function is defined by real coefficients $L_E(s)$ also obeys a reflection symmetry along the real axis. The point $s = 1$ is therefore in a very real sense the *central point* for the L-function, and it is the behavior of $L(E,s)$ at the central point that conjecturally captures the rank information of E. This is established concretely in the Birch and Swinnerton-Dyer Conjecture, the first part of which we state below (the full conjecture is stated in Chapter 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*

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

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

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

[Aside: Brian Birch and Peter Swinnerton-Dyer formulated the eponymous conjecture in the 1960s based in part on numerical evidence generated by the EDSAC computer at the University of Cambridge; this makes it one of the first instances of computer-generated data being used to support a mathematical hypothesis. 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

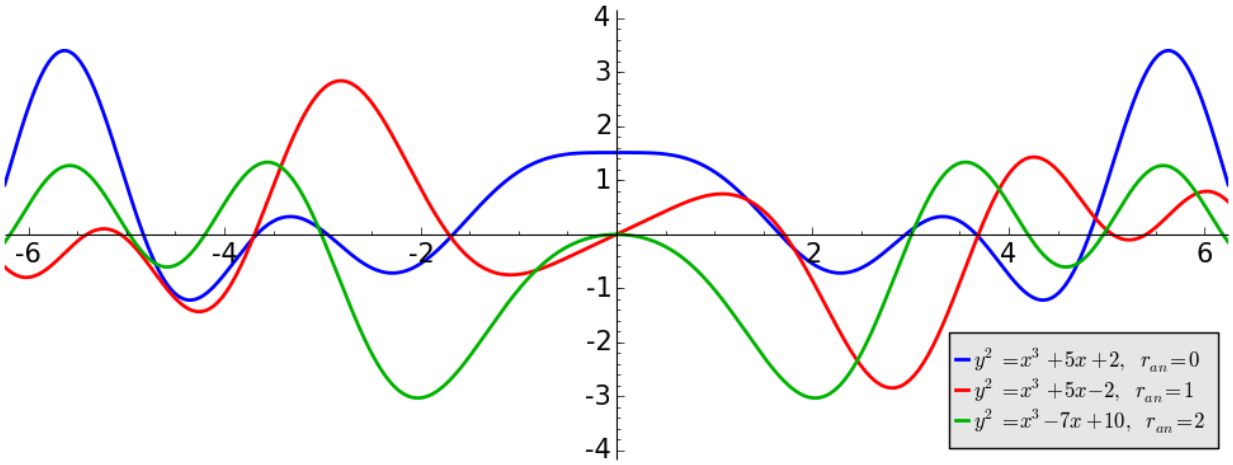

Figure 1.1: The values of three elliptic curve L-functions along the critical line $1 + it$ for $-6 \leq t \leq 6$. Blue corresponds to a rank 0 curve, red is that of a rank 1 curve, and green is a rank 2 curve. Note that close to the origin the graphs look like non-zero constant function, a straight 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 algorithm exist to compute the rank of E that has provable worst-case and average-case running times? We answer this question in the affirmative; however, to do so we must pay the price of having to assume the 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 results:

sectionNotation, Definitions and Background

2.1 Notation

For the rest of the body of this text (unless otherwise stated) we use the following terminology:

- 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, N and r are the discriminant, conductor and algebraic rank of E respectively
- r_{an} is the analytic rank of E
- 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 $= 0.5772156649\ldots$
- 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
- $j = \frac{c_4}{D}$
- $\omega = \frac{dx}{2y+a_1x+a_3} = \frac{dy}{3x^2+2a_2x+a_4-a_1y}$

2.2 Definitions: Elliptic curves and their L-functions

The rest of this chapter covers the basic definitions of and results surrounding elliptic curve L-functions. Feel free to skip this if you are familiar with them.

Definition 2.1. 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, we will always assume that any given elliptic curve Weierstrass equation is minimal and in the above form, unless otherwise stated.

Definition 2.2. 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

$$f(x,y) = y^2 + a_1xy + a_3y^2 - x^3 - a_2x^2 - a_4x - a_6. \tag{2.1}$$

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 2.3. 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 2.4. *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 2.1).

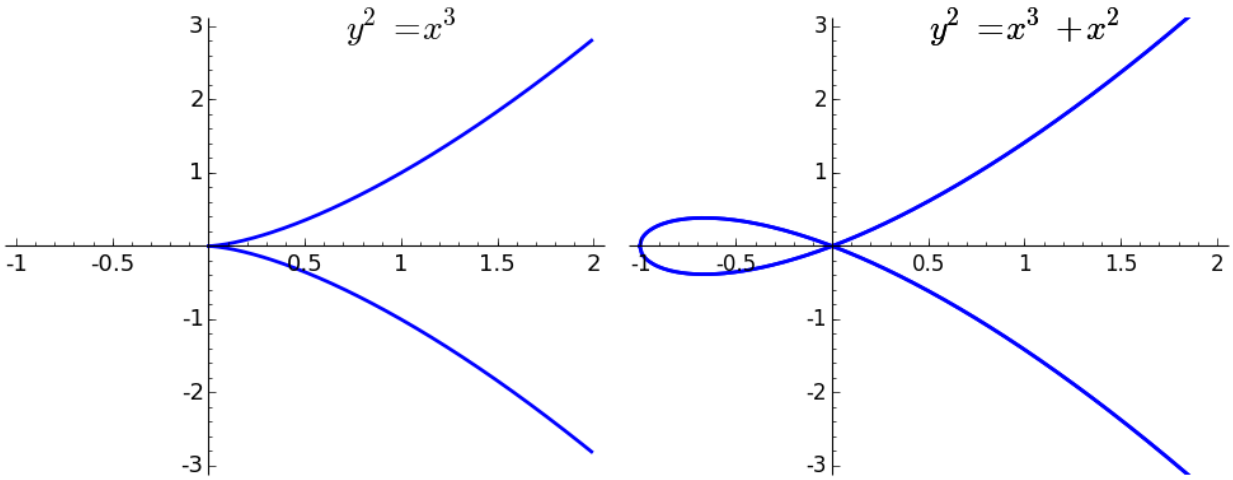

Figure 2.1: An example of two singular cubics over the rationals. The singular point for both curves is at the origin; for the the left curve the singular point is a *cusp*, and for the right curve it is a *node*.

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

Definition 2.5. 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 2.6. 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

$$N_E = \prod_p p^{f_p(E)}, \tag{2.2}$$

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

$$f_p(E) = \begin{cases} 0, & \text{E has good reduction at } p \\ 1, & \text{E has multiplicative reduction at } p \\ 2, & E \text{ has additive reduction at } p. \end{cases} \tag{2.3}$$

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 2.7.

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

$$a_p(E) = p + 1 - \#\left\{E(\mathbb{F}_p)\right\}, \tag{2.4}$$

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

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

$$a_p(E) := \begin{cases} +1 & \text{if } E \text{ has split multiplicative reduction at } p \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p \\ 0 & \text{if } E \text{ has additive reduction at } p. \end{cases} \tag{2.5}$$

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

Theorem 2.8 (Hasse, 1936)**.** *For all elliptic curves $E/\mathbb{Q}$ and all primes p,*

$$|a_p(E)| \leq \sqrt{p} \tag{2.6}$$

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 2.9 (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 2.10.

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

$$L(E,s) = \prod_p \frac{1}{1 - a_p p^{-s} + \epsilon(p) p^{1-2s}} \tag{2.7}$$

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

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

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}. \tag{2.8}$$

  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 2.11.

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

$$\Lambda_E(s) = N^{\frac{s}{2}} (2\pi)^{-s} \Gamma(s) L_E(s), \tag{2.9}$$

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 2.13 (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 2.14.

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

$$\Lambda_E(s) = w_E \Lambda_E(2-s), \tag{2.10}$$

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.*

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

$$\lambda_E(s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \sum_{n=1}^{\infty} a_n n^{-s} \Gamma\left(s, \frac{2\pi n}{\sqrt{N}}\right), \tag{2.11}$$

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

$$\Lambda_E(s) = \lambda_E(s) + w_E \lambda_E(2-s) \tag{2.12}$$

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

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 the point $s = 1$ is in a very real sense the *central point* for an elliptic curve L-function. This is formalized in the following statement:

Proposition 2.15. *As a function of* s, $\Lambda_E(1+s)$ *is even if* $w_E = 1$, *and odd if* $w_E = -1$.

This follows immediately from the functional equation.

Finally, we need the definition of analytic rank:

Definition 2.16. 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

$$L_E(z) = a_0 + a_1 z + a_2 z^2 + \dots \tag{2.13}$$

where $z = s - 1$, then $a_n = 0$ for $0 \leq n < r_{an}$ and $a_{r_{an}} \neq 0$.

We will end up working a lot with the leading coefficient of the L-seres at the central point. To this end:

Definition 2.17. The leading coefficient of $L_E(s)$ at the central point (the constant $a_{r_{an}}$ in the definition above) we denote by C_E, or just C.

2.3 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 2.18 (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*

$$C_E = \left(\frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#Ш(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{Tor}(\mathbb{Q}))^2} \right), \tag{2.14}$$

where

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

For an excellent description of the conjecture and a breakdown of the arithmetic invariants mentioned above, see Andrew Wiles' official description of the BSD Conjecture on the Clay Math website [Wil14].

Conjecture 2.19 (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 2.20 (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 2.21 (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*

$$c < K_\epsilon \, \mathrm{rad}(abc)^{1+\epsilon}. \tag{2.15}$$

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 2.22 (Szpiro)**.** *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N and minimal discriminant D. Then for any $\epsilon > 0$ there is a constant K_ϵ such that*

$$|D| < K_\epsilon N^{6+\epsilon}. \tag{2.16}$$

Conjecture 2.23 (Lang)**.** *Let E be an elliptic curve over $\mathbb{Q}$ with minimal discriminant D. There is a positive constant K such that for any nontorsion point $P \in E(\mathbb{Q})$,*

$$\hat{h}(P) \geq K \log |D|, \tag{2.17}$$

where $\hat{h}(P)$ is the Néron-Tate canonical height of P.

Conjecture 2.24 (Hall)**.** *For any $\epsilon > 0$ there is a constant K_ϵ such that for any $x, y \in \mathbb{Z}$ such that $x^3 - y^2 \neq 0$, we have*

$$|x^3 - y^2| \geq K_\epsilon |x|^{\frac{1}{2}-\epsilon}. \tag{2.18}$$

That is, if $x^3 - y^2 \neq 0$, then the difference cannot be closer than about $\sqrt{|x|}$.

3 Bounding 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.

Definition 3.1. 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

$$\Omega_E = \begin{cases} 2\omega_1 & D > 0 \\ \omega_1 & D < 0 \end{cases} \tag{3.1}$$

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 3.2. *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*

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

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 2.

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*

$$\omega_1 = \frac{\pi}{AGM(\sqrt{e_3 - e_1}, \sqrt{e_3 - e_2})} \tag{3.2}$$

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*

$$\omega_1 = \frac{\pi}{AGM(|z|, s)} \tag{3.3}$$

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

We establish a lower bound on the real period Ω_E in terms of the elliptic discriminant D.

Theorem 3.3 (S.)**.** *For*

$$\Omega_E > \min\left\{1, \frac{4\pi}{|D|^{1/3} + 1}\right\}. \tag{3.4}$$

Proof. Recall that the elliptic discriminant is 16 times the discriminant of the polynomial $x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$. That is, we have

$$D = 16(e_3 - e_1)^2(e_3 - e_2)^2(e_2 - e_1)^2. \tag{3.5}$$

We consider the cases where $D > 0$ and $D < 0$ separately.

1. Suppose $D > 0$. Minimizing ω_1 for a given D is equivalent to maximizing $\mathrm{AGM}(\sqrt{e_3 - e_1}, \sqrt{e_3 - e_2})$. This occurs when $e_2 - e_1$ is small, and the quantities $e_3 - e_1$ and $e_3 - e_2$ are approximately equal. So assume $e_2 - e_1 << e_3 - e_2$. Then

$$??\tag{3.6}$$

□

4 Bounding 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 4.1. 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

$$h(P) := \ln(d). \tag{4.1}$$

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

$$\hat{h}(P) := \lim_{n\to\infty} \frac{h(2^n P)}{(2^n)^2}, \tag{4.2}$$

where h is the naïve logarithmic height defined above.

Theorem 4.3 (Néron-Tate)**.** *Néron-Tate has defines a canonical quadratic form on $E(\mathbb{Q})$ modulo torsion. That is,*

1. *For all $P, Q \in E(\mathbb{Q})$,*
$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\left[\hat{h}(P) + \hat{h}(Q)\right] \tag{4.3}$$
i.e. $\hat{h}$ obeys the parallelogram law;

2. *For all $P \in E(\mathbb{Q})$ and $n \in \mathbb{Z}$,*
$$\hat{h}(nP) = n^2 \hat{h}(P) \tag{4.4}$$

3. *$\hat{h}$ is even, and the pairing $\langle\ ,\ \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}$ by*
$$\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q) \tag{4.5}$$
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 4.4. 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

$$\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q) \tag{4.6}$$

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 4.5. 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

$$\mathrm{Reg}_E = \det\left(\langle P_i, P_j\rangle\right)_{1\leq i,j\leq r} \tag{4.7}$$

where $\left(\langle P_i, P_j\rangle\right)_{1\leq i,j\leq r}$ 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 turns out that one can construct elliptic curves with arbitrarily large regulators (for example, fix some x_0 and y_0 with large denominators, and then find A and B such that $P = (x, y)$ lies on $E : y^2 = x^2 + Ax + B$). However, 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 4.6. *Let $E/\mathbb{Q}$ have minimal discriminant Δ_E. There exists an absolute constant $M_0 > 0$ independent of E such that any non-torsion point $P \in E(\mathbb{Q})$ satisfies*

$$\hat{h}(P) >= M_0 \log|\Delta_E|. \tag{4.8}$$

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; since we are already assuming strong abc, we have this result for free.

Since the conductor of a curve always divides the minimal discriminant, an immediate consequence of the height conjecture is the following:

Corollary 4.7. *Let $E/\mathbb{Q}$ have conductor N_E. There exists an absolute constant $M_1 > 0$ independent of E such that any non-torsion point $P \in E(\mathbb{Q})$ satisfies*

$$\hat{h}(P) >= M_0 \log N_E. \tag{4.9}$$

(Note that the two versions of the height conjecture are fully equivalent under Szpiro's Conjecture).

Conjecture 4.8. *$M_0 = 0.000213016731929803\ldots$ and $M_1 = 0.00107510998642534\ldots$; these two constants are attained by the rank 1 curve $E : y^2 + xy + y = x^3 + x^2 - 125615x + 61201397$ with Cremona label* `3990v1`*, conductor $N_E = 3990$ and minimal discriminant $\Delta_E = -1494018600480000000$. Furthermore, the curve's generator for the group of rational points $P = (7107, -602054)$ and its negative attain the minimum height of any non-torsion point on any elliptic curve over $\mathbb{Q}$, namely $\hat{h}(P) = 0.00891432445568635\ldots$.*

This conjecture is grounded on numerical evidence.

This allows us to bound the regulator of E from below in terms of its conductor and the global constant M_1:

Theorem 4.9. *Let $E/\mathbb{Q}$ have conductor N_E. Assume strong abc, and let M_1 be the absolute constant in Lang's height conjecture. Then*

$$\mathrm{Reg}_E \geq \textit{What goes here?} \tag{4.10}$$

Proof. Let E have minimal discriminant Δ_E and algebraic rank r. Since $|\Delta_E| \geq N_E$, it follows that

$$\mathrm{Reg}_E \geq (M_1 \log N_E)^r \geq M_1^r$$

Numerically we determine that $M_1 < 1$. For example, the rank 1 curve with Cremonal label `1430k1` has a group generator with height $0.009739\ldots$; its regulator is therefore the same value. We thus must have that $M_1 \leq 0.00974/\log(1430) = 0.001340\ldots$.

From Lemma ??? we have that $r < \frac{1}{5}\log N$; hence

□

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)

[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.

[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).

[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).

[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.