Ph.D Dissertation

Simon Spicer
University of Washington

July 25, 2014

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

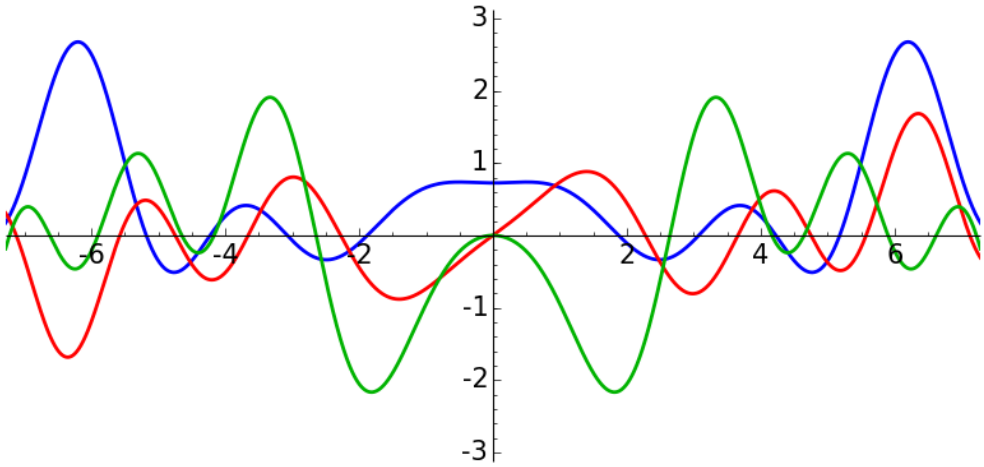

Figure 1.1: The values of three elliptic curve L-functions along the critical line $1 + it$ for $-6 \leq t \leq 6$. Blue corresponds to the curve $y^2 = x^3 - x - 1$, a rank 0 curve, red is that of $y^2 = x^3 + x + 1$, a rank 1 curve, and green is $y^2 = x^3 - 4x + 1$, a rank 2 curve. Note that close to the origin the graphs look like non-zero constant function, a straight line through the origin and a parabola through the origin respectively.

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 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

Conjecture 2.1 (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*

$$L(E,1+s) = s^r \left[\left(\frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#Ш(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{Tor}(\mathbb{Q}))^2} \right) + O(s) \right], \tag{2.1}$$

where

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

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

3 Bounding the Real Period

Cheese.

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
$$\text{Reg}_E = \det\left(\langle P_i, P_j\rangle\right)_{1\le i,j\le r} \tag{4.7}$$
where $\left(\langle P_i, P_j\rangle\right)_{1\le i,j\le r}$ is the matrix whose (i,j)th entry is the value of the pairing $\langle P_i, P_j\rangle$. If $E/\mathbb{Q}$ has rank zero, then Reg_E is defined to be 1.

Note that 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* **Q***: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic). MR 1839918 (2002d:11058)

[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).

[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.

[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.