Rose-
Hulman
Undergraduate
Mathematics
Journal

An Introduction to the Birch and Swinnerton-Dyer Conjecture

Brent A. Johnson [a]

Volume 16, No. 1, Spring 2015

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a] Villanova University

Rose-Hulman Undergraduate Mathematics Journal
Volume 16, No. 1, Spring 2015

An Introduction to the Birch and Swinnerton-Dyer Conjecture

Brent A. Johnson

Abstract. This article explores the Birch and Swinnerton-Dyer Conjecture, one of the famous Millennium Prize Problems. In addition to providing the basic theoretic understanding necessary to understand the simplest form of the conjecture, some of the original numerical evidence used to formulate the conjecture is recreated. Recent results and current problems related to the conjecture are given at the end.

Acknowledgements: I would like to thank Professor Robert Styer and Professor Alice Deanin for their incredible mentorship, patience, and friendship.

1 Introduction

An elliptic curve is a projective, nonsingular curve given by the general Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

There is no doubt that elliptic curves are amongst the most closely and widely studied objects in mathematics today. The arithmetic complexity of these particular curves is absolutely astonishing, so it isn't surprising the Birch and Swinnerton-Dyer conjecture has been honored with a place amongst the Clay Mathematics Institute's famous Millennium Prize Problems. Although some great unsolved problems carry the benefit of simplicity in statement, this conjecture is not one of them. There even seems to be an aura of "hardness" over the problem that keeps many from discovering the true beauty of the conjecture. It is our goal, then, to make this fascinating conjecture more available and understandable to those interested in elliptic curves and arithmetic geometry, and to push through the aura of difficulty to reveal the exquisite nature of the Birch and Swinnerton-Dyer conjecture. Why is this conjecture so important? Well, a proof of the conjecture would imply the algebraic rank (something we will talk about later) can be successfully computed. Furthermore, it was shown by Tunnell in 1983 that a proof of the conjecture would finally put to rest the one thousand year old congruent number problem [15].

In Section 2 we will discuss some basic preliminaries in elliptic curves. There are several great books on elliptic curves and we enthusiastically direct the reader to classic text by Silverman [11] for an excellent and thorough treatment of the subject. Section 3 and 4 are dedicated to the algebraic rank and analytic rank respectively. In Section 5 we will formally present the Birch and Swinnerton-Dyer conjecture, with Section 6 serving as a brief exposition on the results and progress made on the conjecture.

2 Elliptic Curves

The Birch and Swinnerton-Dyer conjecture is a conjecture on the relation between two important properties of an elliptic curve: an analytic part and an algebraic part. Before we describe the two parts and get down to the real business of the conjecture, we will briefly describe some basic definitions and aspects of elliptic curves. As previously stated, an elliptic curve E is given by the Weierstrass equation

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

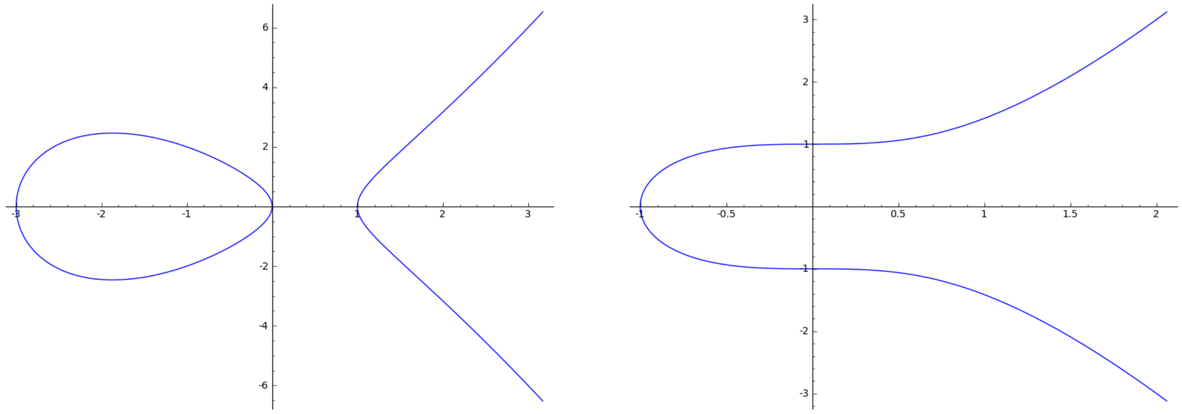
This is the general Weierstrass form, and although it is certainly true that every elliptic curve takes this form, we restrict ourselves to a much simpler case. The general form is used to ensure that an elliptic curve will be an elliptic curve over an arbitrary number field, particularly when considering fields of varying characteristic. But when we work with elliptic curves over the rationals, we have much less to worry about. The Weierstrass equation can be reduced to

$$y^2 = x^3 + Ax + B,$$

and although many exciting things can occur when considering elliptic curves over various fields (the interested reader is particularly encouraged to look at the conjecture over function fields), we will only concern ourselves with the rationals as our base field. The equation above is usually referred to as the short Weierstrass form. Recall that an elliptic curve is necessarily non-singular, that is, it has no cusps or nodes. Fortunately, since we are only using the short Weierstrass form, we only need to ensure the discriminant

$$\Delta = -16(4A^3 + 27B^2)$$

is non-zero. See Washington [16] or Silverman [11] for more regarding the elliptic discriminant.



(a) The elliptic curve $E = y^2 = x^3 + 2x^2 - 3x$

(b) The elliptic curve $E = y^2 = x^3 + 1$

Figure 1: Two typical elliptic curves.

Let E be an elliptic curve over the rationals $\mathbb{Q}$. The set of rational points on this curve forms a group $E(\mathbb{Q})$ with the point at infinity serving as the identity. This group structure of elliptic curves is particularly important and since we are considering them as groups, a few natural questions arise:

- What do we know about the structure of $E(\mathbb{Q})$?
- How can we determine the group $E(\mathbb{Q})$ for specific elliptic curve?
- What groups $E(\mathbb{Q})$ are possible?

3 The Algebraic Rank

In this section, we will answer some of the questions raised above. First, we define an important subgroup:

Definition The *torsion subgroup* of $E(\mathbb{Q})$, denoted $E(\mathbb{Q})_{tors}$, consists of all points in $E(\mathbb{Q})$ of finite order.

In 1922, British-American mathematician Louis Mordell showed that the group of rational points on any elliptic curve, $E(\mathbb{Q})$, is finitely generated (a few years later, André Weil showed that for any abelian variety A over a number field K, the group $A(K)$ is finitely generated).

Theorem 3.1 (Mordell). *Let E be an elliptic curve. Then $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$ where r is the rank and $r \geq 0$.*

The rank r is also called the Mordell-Weil rank or the arithmetic rank. The theorem essentially tells us that the group of rational points $E(\mathbb{Q})$ is isomorphic to a direct product of the torsion subgroup and r copies of $\mathbb{Z}$. A theorem of Nagell and Lutz gives an effective way of computing the torsion subgroup of an elliptic curve, and any modern number theory program, such as PARI or Sage, can quickly render the subgroup. Additionally, we have the following theorem:

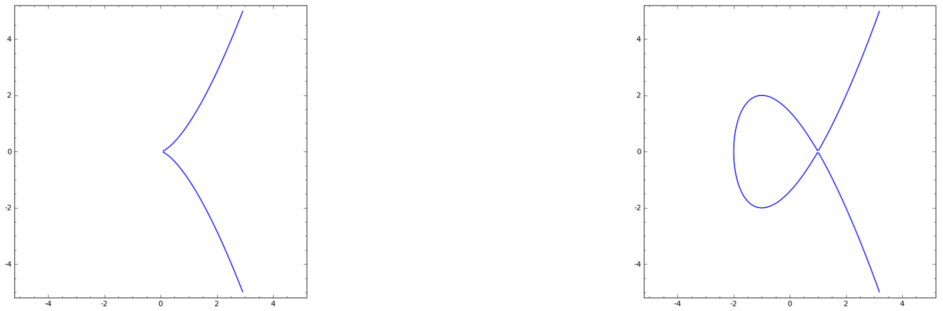
Theorem 3.2 (Mazur). *For an elliptic curve E, the torsion subgroup of $E(\mathbb{Q})$ is one of the following:*

- *$\mathbb{Z}/n\mathbb{Z}$ with $1 \leq n \leq 10$ or $n = 12$.*
- *$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ with $1 \leq n \leq 4$.*

Although the theorem is difficult to prove, it nonetheless gives an effective bound and classification of all possible torsion groups. With the torsion subgroup so well defined, all that remains is the integer r, the rank. Unfortunately, finding the rank is very difficult and there is currently no known algorithm that will yield a guaranteed correct result. For instance it is not known which integers can occur as the rank, or if the rank is bounded or unbounded. Several conjectures seem to point to an average rank of $\frac{1}{2}$ but no significant progress has yet been made on any of the average distribution conjectures. Fortunately, we can occasionally compute an upper and lower bound for the rank, and thus obtain a likely answer. The highest known exact rank is $r = 19$, but an elliptic curve with at least $r = 28$ is known [10].

4 The Analytic Rank

The analytic rank is somewhat more technical to define. First, we begin by reducing elliptic curves mod p with p a prime number. We must be careful though. Reducing an elliptic curve mod p will not always return an elliptic curve. If it does, then the curve is said to have *good reduction* at p. If the resulting mod p reduction yields a singular curve, that is, a curve with a node or cusp, then it is said to have *bad reduction*. Fortunately, there are only finitely many primes of bad reduction for an elliptic curve over $\mathbb{Q}$ and these are precisely the ones that divide the discriminant Δ. For instance, if we have an elliptic curve mod p, and p divides Δ, then $\Delta = 0 \mod p$. But recall that an essential requirement for elliptic curves is they must not have a non-zero discriminant!



(a) A singular curve with a cusp

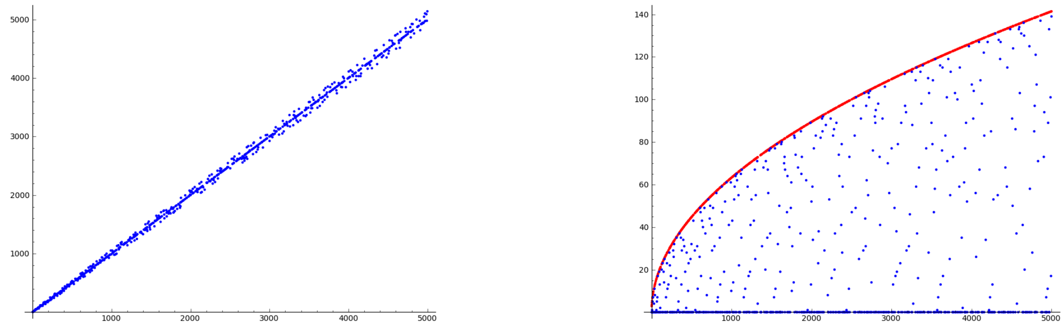
(b) A singular curve with a node

Figure 2: Two singular cubic curves.

Assume the Weierstrass equation for E is integral and minimal. Note that integrality and minimality is essential in order to ensure proper reduction at all primes of the elliptic curve. Let $E(\mathbb{F}_p)$ denote an elliptic curve reduced mod p. We expect the number of points $E(\mathbb{F}_p)$ to be about $p+1$, the extra being the point at infinity. A theorem of Hasse, originally conjectured by Emil Artin in his thesis, says that

$$|E(\mathbb{F}_p) - p - 1| \leq 2\sqrt{p}.$$

Although this error term provides an effective bound, it does not provide a way to calculate $E(\mathbb{F}_p)$ when p is large. Fortunately, there are ways of calculating such values (which prove useful in elliptic curve cryptography). Let's call the error term $E_p - p - 1$ the a_p value associated to an elliptic curve. Although this may seem like an arbitrary choice, the a_p value is actually the trace of the Frobenius endomorphism, a particularly important linear transformation.



(a) The points $(p, |E(\mathbb{F}_p)|)$ for the first 5000 primes showing roughly 1:1 correspondence as expected.

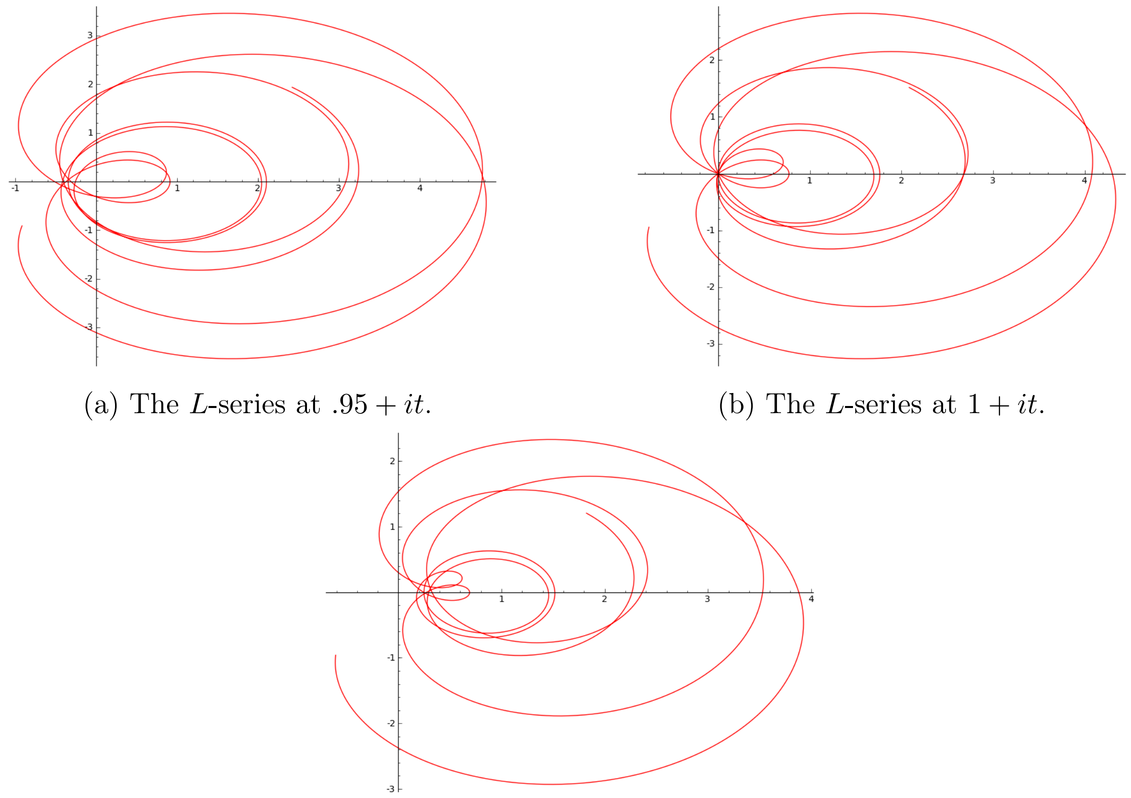
(b) The points $(p, |E(\mathbb{F}_p) - p - 1|)$ under the curve $2\sqrt{p}$ in red.

Figure 3: Properties of the error term a_p.

We further want to collect the a_p values in such a way that we can keep track of the behavior of a particular elliptic curves at certain primes. Fortunately, such a function exists. We define the L-series of an elliptic curve E at a complex number s by the Euler product

$$L(E,s) = \prod_{p\nmid\Delta}(1 - a_p p^{-s} + p^{1-2s})^{-1} \cdot \prod_{p\mid\Delta}(1 - a_p p^{-s})^{-1}.$$

The L-function converges when the real part of s, denoted as $\Re(s)$, is greater than $\frac{3}{2}$, and due to a result of Wiles et al. extends holomorphically to the entire complex plane [17],[3].



(a) The L-series at $.95 + it$.

(b) The L-series at $1 + it$.

(c) The L-series at $1.05 + it$.

Figure 4: The L-series of the elliptic curve $y^2 + xy = x^3 + 1$ at a complex number $s + it$ at different values of s and as t ranges between -10 and 10.

Figure 4 shows some examples of an L-series at different values of $\Re(s)$. Those familiar with the traditional zeta function will recognize the same 'looping' behavior. We define the *analytic rank* r_{an} of an elliptic curve to be the order of vanishing of its L-function at $s = 1$. Succintly,

$$r_{an}(E) = \text{ord}_{s=1} L(E,s).$$

As with the algebraic rank, certain problems exist for the analytic rank. In general, the analytic rank is impossible to compute. Fortunately, due to the methods of Dokchitser and Cremona, there exists effective ways of computing $r_{an}(E)$ when $r_{an}(E) \leq 3$.

5 The Birch and Swinnerton-Dyer Conjecture

The groundwork laid by the two young mathematicians began around 1958. They had the rare privilege of access to one of the only serious computers at the time, EDSAC. With it, they started a roughly seven year project that finally culminated in two groundbreaking papers. The conjecture was outlined in the second paper, "Notes on elliptic curves II" [2]. They used their computer to study values of the L-function at $\Re(s) = 1$. At this particular value, we have

$$L(E, 1) = \prod_p \frac{p}{\#E(\mathbb{F}_p)}.$$

They noticed as the algebraic rank of $E(\mathbb{Q})$ increased, the $\#E(\mathbb{F}_p)$ tended to increase as well. In fact, they noticed the ord $L(E, 1)$, the analytic rank, seemed to coincide with the number of generators of infinite order of $E(\mathbb{Q})$, the algebraic rank. This led them to the now famous problem:

Conjecture 5.1 (Birch and Swinnerton-Dyer)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then the analytic rank and the algebraic rank are equal:*

$$r(E) = r_{an}(E).$$

The original statement, as it appeared exactly in their paper in 1965 (their g is our rank r), reads as follows.

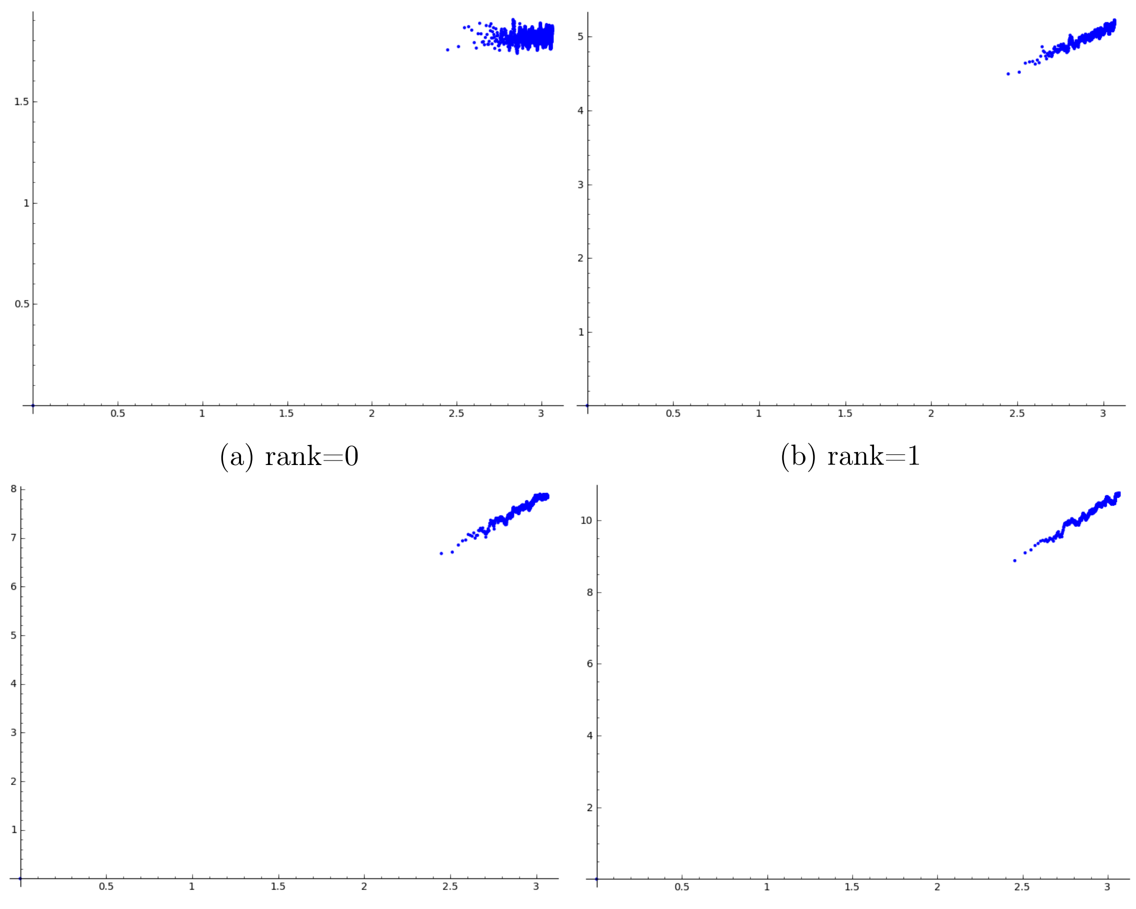
Conjecture 5.2. *If g is the number of generators of $E(\mathbb{Q})$ of infinite order, then*

$$f(P) \sim C(\log P)^g$$

where $P = \prod\limits_p \frac{p}{\#E(\mathbb{F}_p)}$ and as $P \to \infty$.

Limited computational power of the time also limited numeric evidence for the conjecture. Modern efforts to crunch numbers, however, have been much more fruitful. Figure 5 shows four graphs of what original computational efforts may have revealed. The data was collected in Sage using a program like

```
E=EllipticCurve('11a1').minimal_model()
A=1.000*prod((E.Np(p)/p) for p in prime_range(E.conductor));
BSDlist=[[0,0]];
p=E.conductor().next_prime();
for j in range(1,10000):
     for k in range (1,1000):
          A=(A*(E.Np(p)/p))
          p=next_prime(p)
     BSDlist=BSDlist + [[log(log(p)),log(A)]]
point(BSDlist)
```



(a) rank=0

(b) rank=1

(c) rank=2

(d) rank=3

Figure 5: Computational data (10^5 points) for the conjecture. Notice the slope of the points roughly corresponds to the value of the rank.

A stronger form of the conjecture exists. It predicts the value of the nonzero number C in the equation

$$L(E,s) \sim C(\log P)^g \quad \text{as } s \to 1.$$

By solving for C and making a quick substitution for the L-series, we have

$$C = \lim_{s\to 1} \frac{L(E,s)}{(s-1)^{r(E)}} = \frac{1}{r!} L^{(r)}(E,1).$$

A heuristically valid, though totally unjustified substitution, reveals a third and more ambitious version of the conjecture:

Conjecture 5.3. *Let E be an elliptic curve over $\mathbb{Q}$ of rank r. Then $r = \operatorname{ord}_{s=1} L(E,s)$ and*

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_E \cdot \operatorname{Reg}(E) \cdot \#Ш(E/\mathbb{Q}) \cdot \prod_p c_p}{\#E(\mathbb{Q})^2_{tor}}.$$

Although this variant of the conjecture is more complex, it is still not hard to see that the conjecture is talking about an analytic aspect of elliptic curves, the L-series, on the left, and an algebraic aspect, the invariants, on the right. All of the invariants in the equation are well defined except for one. The regulator $\mathrm{Reg}(E)$ and real period Ω_E are easily computed by PARI or Sage. The c_p values contain local information about the elliptic curve and, along with the torsion subgroup, are readily calculated. The only difficult aspect lies with $Ш(E/\mathbb{Q})$, the Tate-Shaferavich group. Unfortunately, little is known about this mysterious group. It is not even known to be finite, although it is conjectured to be so. A proof of the conjecture will likely need to tackle the problems with this group first.

6 Progress

> "This remarkable conjecture relates the behavior of a function L, at a point where it is not at present known to be defined, to the order of a group Ш, which is not known to be finite." - John Tate, on the Birch-Swinnerton-Dyer Conjecture.

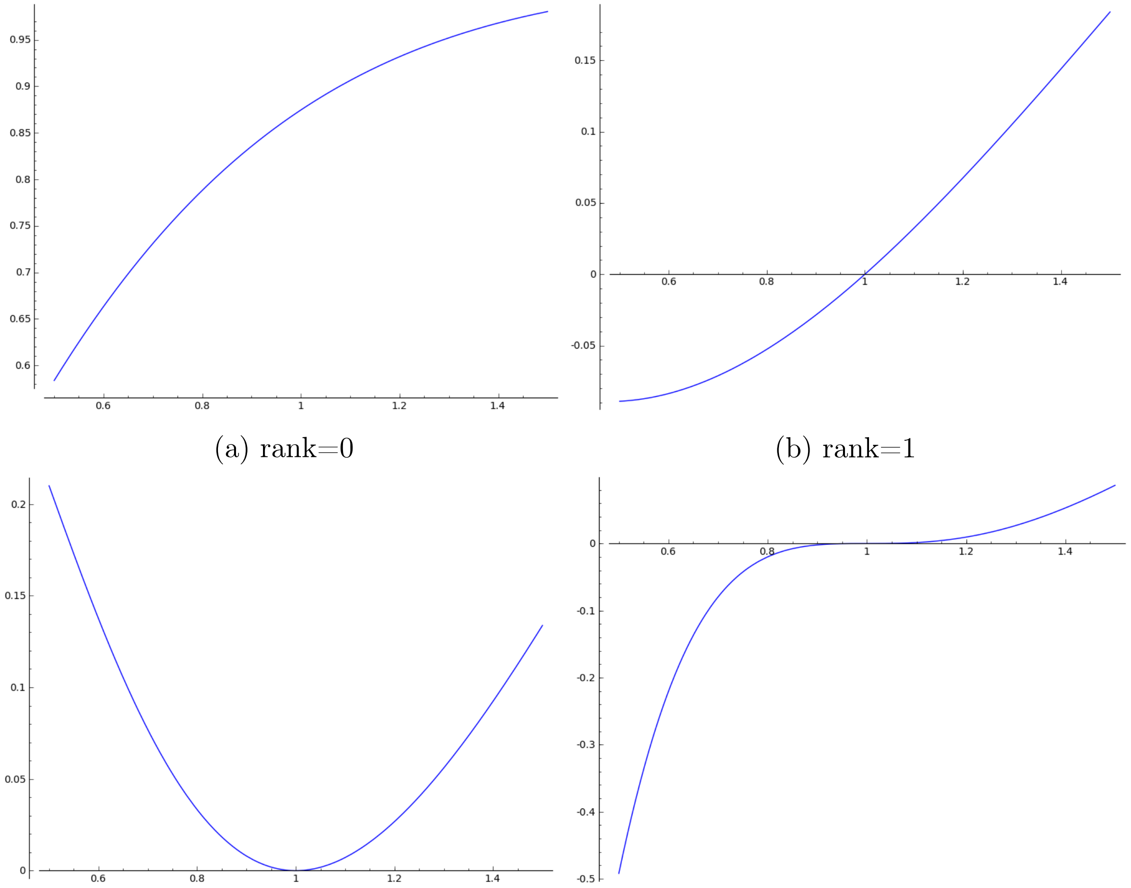
Progress was steady through the 70's and 80's with the biggest breakthroughs concerning elliptic curves with complex multiplication. John Coates and his then student Andrew Wiles tackled such curves in the late 70's [4]. Definitive work by Rubin in the late 80's not only shed light on elliptic curves with complex multiplication, but also the Tate-Shaferavich group of such curves [9]. Benedict Gross and Don Zagier added a breakthrough for modular elliptic curves with the groundbreaking Gross-Zagier theorem on Heegner points [7]. One of the most promising and most significant advances was made by Kolyvagin in 1989. By using his newly developed Euler systems, Kolyvagin was able to prove the following result:

Theorem 6.1. *If $E(\mathbb{Q})$ is infinite, then $L(E,1) = 0$.*

In fact, Kolyvagin, along with results from others, proved if an elliptic curve has rank 0 or 1 then the conjecture holds [8].

Although Tate's quote was accurate at the time it was made, we fortunately have at least started to understand the L-series. Andrew Wiles's proof of the Taniyama-Shimura conjecture (and subsequently Fermat's Last Theorem), along with work done by Richard Taylor et al., showed the L-series has an analytic continuation to the entire complex plane. Thanks to the work of Tim Dokchitser, the L-function can be more easily computed and interpreted by programs like Sage by changing it into a "Dokchitser" L-function. This interpretation allows for a closer analysis of the order of the L-function. Instead of a looping behavior seen previously, we get a much different picture as seen in Figure 6. Notice that the value of the L-series at $s = 1$ for the rank 0 curve is nonzero as predicted.

Breakthroughs have been few and far between since the conjecture's induction as a Millennium Prize Problem in 2000. However, the recent work of Bhargava and Shankar has shattered the relative silence and ignited a new flame of hope for the problem. They were able to show in their incredible paper that the average algebraic rank of all elliptic curves over $\mathbb{Q}$ is less than 1.17. This means at least 62.5% of elliptic curves have rank 0 or 1! They are further able to show, by combining their own work with that of Dokchitser and Dokchitser [6], and Skinner and Urban[13], that a positive proportion of elliptic curves have analytic rank 0, and therefore by Kolyvagin's theorem a positive proportion of elliptic curves satisfy the Birch and Swinnerton-Dyer conjecture [1].



(a) rank=0

(b) rank=1

(c) rank=2

(d) rank=3

Figure 6: Dokchitser L-functions evaluated at $s = 1$

Despite the computational evidence and the new and impressive work brilliant mathematicians all around the world perform every day, several problems still stand as serious road blocks to a proof of the conjecture. The Tate-Shafaravich group is only conjectured to be finite and very little is known about this group. Just trying to compute its order for a specific elliptic curve is a serious undertaking. Neither the analytic rank nor the algebraic rank can be reliably calculated in general. The analytic rank is well defined, since we now know the L-function has an analytic continuation, but current computational algorithms are only certain up to $r_{an} \leq 3$. There is still no algorithm guaranteed to yield the correct value of the algebraic rank. Current methods rely on a technique called 2-descent, and although this method is useful, it is only viable when the order of $Ш(E/\mathbb{Q})$ is trivial.

The Birch and Swinnerton-Dyer conjecture today remains, of course, unsolved and most mathematicians agree that new ideas will need to be developed to tackle the great problem. A proof will take a great deal of work and mathematical power, but it would not be a Millennium Prize Problem with a one million dollar reward if it were easy.

References

[1] Manjul Bhargava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *arXiv preprint arXiv:1007.0052*, 2010.

[2] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[3] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4):843–939, 2001.

[4] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39(3):223–251, 1977.

[5] Tim Dokchitser. Computing special values of motivic L-functions. *Experimental Mathematics*, 13(2):137–149, 2004.

[6] Tim Dokchitser and Vladimir Dokchitser. On the Birch-Swinnerton-Dyer quotients modulo squares. *Ann. of Math.(2)*, 172(1):567–596, 2010.

[7] B. Gross, W. Kohnen, and D. Zagier. Heegner points and derivatives of L-series. II. *Math. Ann.*, 278(1-4):497–562, 1987.

[8] V. A. Kolyvagin. Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

[9] Karl Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103(1):25–68, 1991.

[10] Alice Silverberg et al. Ranks "cheat sheet".

[11] Joseph H Silverman. *The Arithmetic of Elliptic Curves*, volume 106. Springer, 2009.

[12] Joseph H Silverman and John Tate. *Rational points on elliptic curves*. Springer Verlag, 1992.

[13] Christopher Skinner and Eric Urban. The Iwasawa main conjectures for GL2. *Inventiones mathematicae*, 195(1):1–277, 2014.

[14] W. A. Stein et al. *Sage Mathematics Software (Version x.y.z).* The Sage Development Team, 2013. `http://www.sagemath.org`.

[15] Jerrold B Tunnell. A classical Diophantine problem and modular forms of weight 3/2. *Inventiones mathematicae*, 72(2):323–334, 1983.

[16] Lawrence C Washington. *Elliptic curves: Number theory and Cryptography*, volume 50. Chapman and Hall/CRC, 2008.

[17] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Annals of Mathematics*, pages 443–551, 1995.