Stockholm University

The Birch and Swinnerton-Dyer Conjecture

Thesis

Joel Fredin

March 19, 2019

Abstract

We will state Birch and Swinnerton-Dyer Conjecture and the needed theory to make sense of it. We will study the group structure of elliptic curves and introduce notions such as geometric rank and L-functions.

Contents

0 Introduction

A major research area in mathematics is the theory on elliptic curves. An elliptic curve is a particular type of two-dimensional equation with a rich theory and it turns out that they have some really unexpected connections and applications to other parts of mathematics.

The Birch and Swinnerton-Dyer Conjecture (BSD conjecture) is a huge conjecture in arithmetic geometry, which in particular concerns the theory of elliptic curves, and it is one of the seven millenium prize problems. A lot of effort has been laid down to solve it but, as of today, it is still just a conjecture. If it is true, it will give us a relationship between an L-function attached to an elliptic curve and the group structure of the elliptic curve. Not only do research on this conjecture generate interesting mathematics, but it turns out that it also has a lot of corollaries. Some of the corollaries aren't even within the field of elliptic curves any longer, see [1] for instance.

In this thesis, we will go through the theory needed to state the conjecture in the case when we are working over the rational numbers, since the theory becomes considerably much easier than working over general number fields.

1 Notations

Throughout this paper, we will write

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

with $p(x, y) = y^2 - x^3 - Ax - B \in \mathbb{K}[x, y]$, for some field $\mathbb{K}$. This gives us a convinient way to refer to the elliptic curve, since we may now simply say the elliptic curve E. We will also use the notation E/K (with K a number field, which should be read as E is defined over K), which means that the elliptic curve E is only living in the number field K. We, furhtermore, let $\mathcal{O}$ denote the point at infinity.

2 Group Structure

Notice, even though some theorems may be stated for general number fields, we are mainly interested when $K = \mathbb{Q}$.

On our road to state the conjecture, we need to understand the basics of the group structure elliptic curves admits. Let (notice we will only work with these type of elliptic curves for simplicity, there are more general ones)

$$E : Y^2 = X^3 + AX + B$$

be an elliptic curve.

Let us first define an operation on the points of the elliptic curve.

Definition 1. *Let $P, Q \in E$, let L be the line through P and Q (if $P = Q$, let L be the tangent line to L at P), and let R be the third point of intersection of L with E. Let L' be the line through R and O. Then L' intersects E at R, O and a third point. We denote the third point by $P \oplus Q$.*

We furthermore have the following proposition which proves the fact that $\oplus$ is an operation on the rational points living on the elliptic curve that makes it into a group.

Proposition 1. ***(a)*** *If a line L intersect E at the points P, Q, R, then*

$$(P \oplus Q) \oplus R = \mathcal{O}$$

(b) *If $P \oplus \mathcal{O} = P$ for all $P \in E$.*

(c) *$P \oplus Q = Q \oplus P$ for all $P, Q \in E$.*

(d) *Let $P \in E$. There is a point of E, denoted by $\ominus P$, satisfying*

$$P \oplus (\ominus P) = \mathcal{O}.$$

(e) *Let $P, Q, R \in E$. Then*

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

(f) *Suppose that E is defined over K, for a number field K. Then*

$$E(K) = \{(x, y) \in K^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

is a subgroup of E.

Proof. See [2]. □

The first property in the proposition says that it is closed under the operation $\oplus$. Also, notice that **(b)** says that $\mathcal{O}$ serves as an identity element to the group and **(d)** says that to every point P living on the elliptic curve, there is an inverse element. Property **(c)** says that the group is an abelian group. Lastly, **(f)** says that, if we do a restriction to a number field and consider only those points, then we still have $\oplus$ as a group operation.

Remark: From now on, we will drop the notation $\oplus$ and simply write $+$.

Even though we have a group structure defined on the elliptic curve, it is not too immediate how one would apply this operation on an elliptic curve. At least not algorithmically. Luckily there exit a group law algorithm, given in [2].

Theorem 1 (Group Law Algorithm)**.** *Let E be an elliptic curve, given by*

$$E : y^2 = x^3 + Ax + B.$$

Let $P_i = (x_i, y_i) \in E$ for $i = 1, 2, 3$. Then $P_1 + P_2 = P_3$ may be computed as follows.

If $x_1 \neq x_2$ let

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

and

$$\mathrm{v} = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

otherwise put

$$\lambda = \frac{3x_1^2 + A}{2y_1}$$

and

$$\mathrm{v} = \frac{-x_1^3 + Ax_1 + 2B}{2y_1},$$

then

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = -\lambda x_3 - \mathrm{v}.$$

Proof. See [2]. □

Let us now study the group structure of a specific elliptic curve defined over $\mathbb{Q}$.

Example 1.
Consider the elliptic curve $E/\mathbb{Q}$ given by $E : y^2 = x^3 + 2x + 4$.

Two solutions to this equation are given by $(x_1, y_1) = (-1, 1)$ and $b = (x_2, y_2) = (2, 4)$. This can be checked by just trying both solutions, and indeed we get

$$(-1)^3 - 2 + 4 = 1 = 1^2$$

and

$$2^3 + 2 \cdot 2 + 4 = 16 = 4^2.$$

Thus, both $(-1, 1)$ and $(2, 4)$ lives on the elliptic curve E.

We will now study how one might generate new solutions, using these two points, by applying the group group operation defined on E.

We will begin by computing $\lambda = \dfrac{y_1 - y_2}{x_1 - x_2}$,

$$\lambda = \frac{1-4}{-1-2} = 1.$$

Now, by using λ, we can compute x_3. Thus, we have

$$x_3 = \lambda^2 - x_1 - x_2 = 1 - (-1) + 2 = 0.$$

What is left to compute is y_3. Let us begin by computing v*,*

$$\mathrm{v} = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} = 2.$$

Our computation of y_3 now becomes

$$y_3 = -\lambda x_3 - \mathrm{v} = -2.$$

By using the group structure of E we have now constructed another rational point, $(0, -2)$, from two other points (again, one can check that this actually is a solution to the equation). One amazing aspect of this is that nothing stops us from creating new rational points by keep playing this game. Now we have three points we could try to add in different ways to create even more solutions.

Next thing we will illustrate, which turns out to be very important when stating the BSD-conjecture late on, is the method of adding a point to itself. That is, we choose a point $P \in E(\mathbb{Q})$ and construct another point by computing $P+P$.

Let's say we, for instance, take $P = (-1, 1)$. Computing λ gives us (now we are in the case $x_1 = x_2$)

$$\lambda = \frac{5}{2}.$$

Furthermore, x_3 becomes

$$x_3 = \frac{33}{4}.$$

To compute y_3, we first have to compute v,

$$\mathrm{v} = \frac{7}{2}$$

and lastly we have

$$y_3 = -\frac{193}{8}.$$

Thus, we have that $P+P = (\frac{33}{4}, -\frac{198}{8})$. One may once again check that this, less trivial solution, indeed solves the equation. An interesting question to consider is, what happens if we compute $P+P+P$, $P+P+P+P$ and so forth. How many solutions can we generate? □

We have now seen that it is possible to define a group structure on the rational points of an elliptic curve E. The group structure, thus, implies that we have a way to construct new rational solutions to E, by using already known solutions. In the next section, we will see a really useful result called the Mordell-Weil Theorem. In fact, that theorem is an important ingredient when stating the BSD conjecture.

3 Rank of Abelian Groups

An interesting problem to consider is, if it is possible to find a finite set of point, say $P_1, ..., P_n$, that generates all possible rational solutions to the elliptic curve (consider this as a vector space over $\mathbb{Z}$). Or an even more bold conjecture would be to ask if all rational points on elliptic curves are finitely generated. The answer to that question is positive. Let us first give a formal definition of what it means to be finitely generated group and then give the theorem.

Definition 2. *An abelian group G is called finitely generated if there exists elements $x_1, ..., x_n \in G$ such that every $x \in G$ can be written as a linear combination of these generators*

$$x = \alpha_1 x_1 + \cdots + \alpha_n x_n$$

with integers $\alpha_1, ..., \alpha_n \in G$.

The elements $x_1, ..., x_n$ are called the generators of G.

Let us now, also, state the theorem.

Theorem 2 (Mordell-Weil Theorem)**.**
Let K be a number field, and let E/K be an elliptic curve. Then the group $E(K)$ is finitely generated.

Proof. See [2]. □

A consequence of the above theorem is that we can factorize $E(\mathbb{Q})$ in the following way

$$E(\mathbb{Q}) \cong E_{\text{tors}}(\mathbb{Q}) \times \mathbb{Z}^{r_g(E)}.$$

$E_{\text{tors}}(\mathbb{Q})$ are called the torsion points. A torsion point is a point P such that there exist an integer k such that

$$kP = \mathcal{O}.$$

Thus, the torsion points are points of finite order. The slightly more interesting object to study is $\mathbb{Z}^{r_g(E)}$. The number $r_g(E)$ determines how many linearly independent points there exist of infinite order. Or, if we put this in other words, these are points we can use to create infinitely many new rational solutions to an elliptic curve. Let us consider the following example.

Example 2.
Let $E/\mathbb{Q}$ be the elliptic curve given in Example 1. By the SageMath code given in the appendix, we compute

$$r_g(E) = 2.$$

Thus, there are two linearly independent points of $E(\mathbb{Q})$ with infinite order. These are given by $(-1, 1)$ and $(0, 2)$. As a side note, $E_{\text{tors}}(\mathbb{Q}) = \{\mathcal{O}\}$. A consequence of this is that $(-1, 1)$ and $(0, 2)$ in fact generates all rational points living on E! □

We have now introduced the notion of a geometric rank. The BSD conjecture relates the geometric rank to another type of object called an L-function, which we will define in the next section.

4 L-functions

L-functions are complex-valued functions that are built from other interesting objects. In this section, we will see how one can construct L-functions related to the elliptic curves by counting solutions to the elliptic curve over finite fields. We will notice that the function we first construct is not defined where it should be defined to make sense of BSD. Thus, we will make the function entire by applying an analytic continuation to it (this will be possible as we will see). After we have done that, we can define the analytic rank and relate it to the geometric rank.

Definition 3. *Let $E/\mathbb{Q}$ be an ellipic curve. For a prime p of good reduction, let $\tilde{E}_p$ be the reduction of E mod p, and set*

$$L_p(s) = (1 - a_p \cdot p^{-s} + p \cdot p^{-2s})^{-1}.$$

Define the Euler factors for prime p of bad reduction by

$$L_p(s) = \begin{cases} (1 - p^{-s})^{-1} & \textit{if } E \textit{ has bad split multiplicative reduction at } p \\ (1 + p^{-s})^{-1} & \textit{if } E \textit{ has bad non-split multiplicative reduction at } p \\ 1 \quad \textit{if } E \textit{ has bad additive reduction at } p \end{cases}$$

$$L_{E/Q}(s) = \prod_{p \text{ not bad reduction}} L_p(s) \prod_{p \text{ bad reduction}} L_p(s),$$

$$a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p).$$

As the reader might notice, that the L-function is divided into two products. One where the reduction of the elliptic curve is bad and one where it isn't. Since, the bad reduction is quite technical, we will skip it in this thesis. This theorem is also possible to state in a more general setting, as one can investigate in [2].

Let us now consider an example, how one might compute some of the factors in the product.

Example 3.
Let us keep working with with the elliptic curve $E : y^2 = x^3 + 2x + 4$ defined over $\mathbb{Q}$. We first compute the discriminant, which is given by

$$\Delta_E = -2^8 \cdot 29.$$

Thus, we have bad reduction at the primes 2 and 29. So these are the only two primes we won't bother with.

We now compute $a_3 = 3 + 1 - E(\mathbb{F}_3)$. One may do this by simply trying every possible pair of points in $\mathbb{F}_3^2$. We do have that $(0, 1)$ is a point since

$$1^3 + 2 \cdot 1 + 4 \equiv_3 4 \equiv_3 1 = 1^2.$$

Another point is given by $(1, 2)$ since,

$$1^3 + 2 \cdot 1 + 4 \equiv_3 4 = 2^2.$$

One may keep doing this, naive way, to find solutions. Since finite fields finite, it will be possible to try every point. In the following table, we list all the solutions to E over the fields $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$ and $\mathbb{F}_{11}$.

$\mathbb{F}_3$	$\mathbb{F}_5$	$\mathbb{F}_7$	$\mathbb{F}_{11}$
$(0,1)$	$(0,2)$	$(0,2)$	$(0,2)$
$(0,2)$	$(0,3)$	$(0,5)$	$(0,9)$
$(1,1)$	$(2,1)$	$(1,0)$	$(2,4)$
$(1,2)$	$(2,4)$	$(2,3)$	$(2,7)$
$(2,1)$	$(4,1)$	$(2,4)$	$(3,2)$
$(2,2)$	$(4,4)$	$(3,3)$	$(3,9)$
–	–	$(3,4)$	$(6,1)$
–	–	$(6,1)$	$(6,10)$
–	–	$(6,6)$	$(7,3)$
–	–	–	$(7,8)$
–	–	–	$(8,2)$
–	–	–	$(8,9)$
–	–	–	$(9,5)$
–	–	–	$(9,6)$
–	–	–	$(10,1)$
–	–	–	$(10,10)$

Table 1: Counting points of $E(\mathbb{F}_p)$ for $p = 3, 5, 7, 11$.

The local L-functions $L_p(s)$ may now easily be computed. Since $a_3 = 4-6 = -2$, $a_5 = 6-6 = 0$, $a_7 = 8-9 = -1$ and $a_{11} = 12-16 = -4$. Furthermore, we have

$$\begin{aligned} L_3(s) &= (1 + 2 \cdot 3^{-s} + 3^{1-2s})^{-1} \\ L_5(s) &= (1 + 5^{1-2s})^{-1} \\ L_7(s) &= (1 + 7^{-s} + 7^{1-2s})^{-1} \\ L_{11}(s) &= (1 + 4 \cdot 11^{-s} + 11^{1-2s})^{-1}. \end{aligned}$$

□

The problem is that $L_{E/\mathbb{Q}}(s)$ is only defined whenever $\mathrm{Re}(s) \geq \frac{3}{2}$. To solve this issue one has to do an analytic continuation. The following theorem, which proves the analytic continuation part, has a long and rich history.

Theorem 3.
Let E be an elliptic curve defined over $\mathbb{Q}$. Then the function $L_E(s)$ has an analytic continuation to the entire complex plane.

Remark: The above theorem is stated for $\mathbb{Q}$ and not a general number field. In fact, if one replaces $\mathbb{Q}$ with just an arbitrary number field K, then it is still only a conjecture.

To prove the Theorem 3, one need two results. One of the result is a very striking and beautiful theorem, called the modularity theorem.

Theorem 4 (Modularity Theorem)**.**
If $E/\mathbb{Q}$ is an elliptic curve, then E is modular.

The proof of the Modularity Theorem, just as Theorem 3, has a long story. Andrew Wiles proved this result for semistable elliptic curves over $\mathbb{Q}$, [3], and then Breuil, Brian, Fred and Richard proved the general statement, [4].

Theorem 5.
The L-function of a modular form has an analytic continuation to the entire complex plane.

Since every elliptic curve over $\mathbb{Q}$ is modular, Theorem 5 tells us that its L-function can be analytic continued to an entire function.The above theorem was also proven by several mathematicians. Two of them are Eichler and Shimura, see [5].

We have now went through all theory needed to understand the conjecture. If we now define the analytic rank of $E(\mathbb{Q})$ as the order of the zero at $s = 1$ for $L_{E/\mathbb{Q}}$, then the conjecture says.

Conjecture 1.
Let $E/\mathbb{Q}$ be an elliptic curve, then

The analytic rank of $E(\mathbb{Q})$ equals the geometric rank of $E(\mathbb{Q})$.

5 Appendix/Code (SageMath)

```
# Constructs the elliptic curve.
E = EllipticCurve([0,0,0,2,4]);
# Computes the geometric rank of E.
E.rank()
```

References

[1] Michael Stoll, *Rational 6-cycles under iteration of quadratic polynomials.* LMS J. Comput. Math. 11 (2008), 367–380.

[2] Joseph H. Silverman, *The Arithmetic of Elliptic Curves.* Springer (Second edition), 2009.

[3] Andrew John Wiles, *Modular Elliptic Curves and Fermat's Last Theorem.* Annals of Mathematics (Vol 141, pages 443-551), 1995.

[4] Christophe Breuil, Brian Conrad, Fred Diamond, Richard Taylor, *On the Modularity of Elliptic Curves Over Q: Wild* 3*-adic Exercises.* Journal of the American Mathematical Society (Vol 14, number 4, pages 843-939), , Electronically published on May 15, 2001

[5] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions.* Publications of the Mathematical Society of Japan (Vol 11), Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kano Memorial Lectures 1