Solution to the Birch and Swinnerton–dyer Conjecture

Le Thanh Duc[1]
[1]Institute of Mechanical Engineering
University of Transport Ho Chi Minh City
No 2, Vo Oanh Street, Ward 25, Binh Thanh District, Ho Chi Minh, Vietnam.

doi.org/10.51505/ijaemr.2025.1209 URL: http://dx.doi.org/10.51505/ijaemr.2025.1209

Received: May 06, 2025 Accepted: May 13, 2025 Online Published: May 16, 2025

Abstract
The Birch and Swinnerton–Dyer (BSD) conjecture is important in modern mathematical conjectures. Since the conjecture was born in 1960, many scientists have participated in solving this problem but have not been successful. The purpose of this article is to provide a way to prove this conjecture. The article's author solves it using pure mathematical theories and does not use mathematical software to find the solution. The proof process uses functions and related knowledge. In parallel, the properties of mappings and characteristics of isomorphisms are also important for clarifying the problem. The proof process confirms the correctness of the conjecture. Due to the important nature of the conjecture, it has solved a series of problems in modern mathematics. However, like other mathematical studies, more evidence is needed to contribute to further affirm the correctness of the proposed method and the proof solution. The results of this solution have important implications for number theory, numerical structures, and coding.

Keywords: mathematics, conjecture, solution, millenium, Birch & Swinnerton–Dyer.

1. Introduction

The BSD conjecture describes the set of rational solutions to an elliptic curve. It is a prominent problem in modern number theory. It states that the behaviour of the Hasse–Weil L function is related to the elliptic curve at s = 1.
In which, the Elliptic's definition curve is:

$$(E): \quad y^2 = x^3 + ax + b$$

$a, b \in R$, a,b: constants

The L function is defined as follows:

$$L(E,s) = \prod_p L_p(E,s)^{-1}$$

L_p - a function is generally defined as follows:

$$L_p(E,s) = 1 - a_p p^{-s} + p^{1-2s}$$

$$a_p = p + 1$$

Evaluating at (s = 1), we obtain:

$$L_p(E,1) = 1 - a_p p^{-1} + p^{-1}$$

The L-function can provide information about a curve's number of rational solutions. Specifically, the conjecture states that:

If the L-function has a nonzero value at (s = 1), then the elliptic curve has only a finite number of rational solutions.

If the L-function has a value of zero at (s = 1), then the elliptic curve has infinite rational solutions.

This conjecture can be stated in another way as follows: The rank r of the group of rational points E(Q) is equal to the order of the zero of the L-function, L(E,s)=0, at s = 1.

Some authors have proven exceptional cases of conjecture but have not yet fully proven all.

Key Proven Cases:

Elliptic Curves with Modular Forms: The conjecture has been verified for elliptic curves that are modular. This connection was established through the modularity theorem, which played a crucial role in Andrew Wiles' proof of Fermat's Last Theorem.

Elliptic Curves with Small Coefficients: For elliptic curves with relatively simple coefficients, computational methods have been used to confirm the conjecture in specific instances.

Applications of Modular Theory: Certain cases involving modular forms and the properties of the L-function have been rigorously tested and verified

Methods and Tools are used:

Modularity Theorem: This theorem links elliptic curves to modular forms, providing a framework to analyze the conjecture.

Computational Techniques: Advanced algorithms and numerical methods have been employed to test the conjecture for specific elliptic curves.

Arithmetic Geometry: Tools from this field have been instrumental in understanding the relationship between the rank of elliptic curves and the behavior of their L-functions.

These results, while limited to specific cases, provide strong evidence supporting the conjecture's validity. However, a general proof remains one of the most challenging and sought-after goals in modern mathematics.

This paper aims to prove the Birch & Swinnerton–Dyer conjecture. (BSD)

2. Method

The author proposes to construct a completely different mathematical model. The purpose is to transform the BSD hypothesis's mathematical model into a simpler research model. First, it is necessary to recall some mathematical concepts.

Mapping Definition

- A mapping from set X to set Y is denoted as f: X → Y, where each element x in X is mapped to an element y in Y, written as f(x) = y.
- Types of Mapping
- Surjection (Onto Mapping): Every element in Y is the image of at least one element in X.
- Injection (One-to-One Mapping): Distinct elements in X have distinct images in Y.
- Bijection (One-to-One and Onto Mapping): The mapping is both injective and surjective, meaning each element in X corresponds uniquely to an element in Y, and vice versa.

Isomorphism definition:

In mathematics, isomorphism refers to a reversible mapping between two mathematical objects, meaning there is a way to transform one object into the other while preserving its essential mathematical properties.

Specifically, a mapping (f) from set (X) to set (Y) is called an isomorphism if there exists an inverse mapping (g) from (Y) back to (X), such that combining these mappings in both directions results in the identity mapping (meaning it leaves the original set unchanged). In other words, the structures of (X) and (Y) are equivalent.

Distance definition

The distance between two points $A(x_A, y_A)$, and $B(x_B, y_B)$ in geometric analysis is defined as follows:

$$d_{AB} = \sqrt{(x_A - x_B)^2 + (y_A - y_B)^2}$$

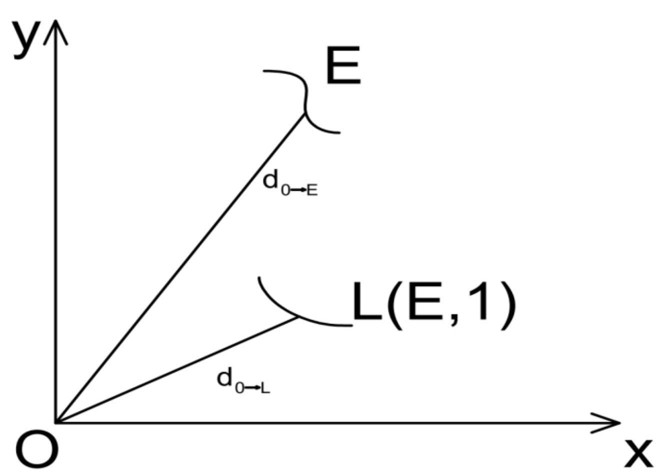

Figure 1- construct the xOy coordinate system containing E and L

Vol. 10, No. 03; 2025

ISSN: 2456-3676

As mentioned, in this axis system (E), L(E,1) has the following equation:

$$(E): \quad y^2 = x^3 + ax + b$$

$$L(E,1) = 1 - \frac{a_p}{p} + \frac{1}{p} = 1 - \frac{a_p}{x} + \frac{1}{x}$$

First, we describe the general function that calculates the distance of points on an Elliptic curve from the origin O.

$$d_{0 \to (E)} = \sqrt{x^2 + y^2}$$

From equation (1), we obtain:

$$d_{0 \to (E)} = \sqrt{x^2 + y^2} = \sqrt{x^2 + x^3 + ax + b} = \sqrt{x^3 + x^2 + ax + b}$$

Let: $f(x) = d_{0 \to (E)} = \sqrt{x^3 + x^2 + ax + b}$

In this coordinate system, we also construct a general function to calculate the distance of points on L(E,1) with the origin 0.

$$d_{0 \to L(E,1)} = \sqrt{x^2 + y^2}$$

To ensure structural equivalence, we take: $y^2 = 1 - \frac{a_p}{x} + \frac{1}{x}$

Thus: $d_{0 \to L(E,1)} = \sqrt{x^2 + 1 - \frac{a_p}{x} + \frac{1}{x}} = \sqrt{\frac{x^3 + x - a_p + 1}{x}}$

Let: $g(x) = \sqrt{\frac{x^3 + x - a_p + 1}{x}}$

There is a corresponding distance to the origin 0 for each point on E, L(E,1).
The transformation of points on E, L(E,1) to distance is isomorphic.

It is easy to see when x changes because E and L reveal their behaviour properties on the same coordinate system. This method lets us know whether or not the BSD hypothesis is correct.
In the set of complex numbers, If $f(x) = 0$ *, there will be three distinct roots; if* $g(x) = 0$ *, there will be three different roots. This result affirmed that the degree of L(E,1) is always the same as (E). Thus, the BSD conjecture is correct.*
It is also necessary to add that instead of using the origin as a reference system, we can use straight lines x or y to separate the behaviour of the functions (E) and L(E,1).

3. Results

In this study, the paper analyzed the equivalent mathematical model of the BSD conjecture and obtained important results. The BSD conjecture is entirely correct. Although the solution is brief, it has solved all the problems, including those other authors have not solved. In addition, the study also shows that there are no contradictions in the results of previous achievements related to the process of proving the conjecture. The logic and tight reasoning show that the results are reliable. The results presented in the study clearly illustrate the similarity between the mathematical model of the conjecture and the proof model. Provide insight into this method's application and development potential to solve other future mathematical problems.

4. Discussion

The important mathematical properties of the BSD conjecture have direct implications for practical and theoretical applications. BSD opens up new advances in number theory, a better understanding of elliptic curves, and the solution of many complex problems. BSD's potential is extensive and will be helpful in other research.

References

Adrian Barquero-Sanchez And Jimmy Calvo-Monge. *The Density And Distribution Of Cm Elliptic Curves Over Q*. DOI:10.48550/arXiv.2411.13526

Amod Agashe. *The Birch and Swinnerton-Dyer conjectural formula and visibility*, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=cd554f7d347ebafdcd3ad0f9cee09b00fcb4bc19

Amod Agashe and William Stein, with an Appendix by J. Cremona and B. Mazur. (2004). *Visible Evidence For The Birch And Swinnerton-Dyer Conjecture For Modular Abelian Varieties Of Analytic Rank Zero*, https://wstein.org/papers/shacomp/shacomp_v13.pdf

Dorian M. Goldfeld. (1976). *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*. http://www.numdam.org/item?id=ASNSP_1976_4_3_4_623_0

Gunter Harder and Don Zagier. *The Conjecture Of Birch And Swinnerton-Dyer*. https://people.mpim-bonn.mpg.de/zagier/files/tex/BSDwHarder/fulltext.pdf

Hubert Schaetzel. (2020). *Enquiry on the mainly stochastic nature of Birch and Swinnerton-Dyer's conjecture.* https://hal.science/hal-03020623v1

J.I. Samuels. (2021). *The Birch and Swinnerton -Dyer Conjecture. DOI: 10.13140/RG.2.2.11344.23044.*

J.N. Cook with D. P. Allen and G. Volk. (2023). *A Direct Proof of the Birch and Swinnerton-Dyer Conjecture.* https://www.researchgate.net/publication/373161320

Joe P. Buhler, Benedict H. Gross and Don B. Zagier, *On the Conjectureof Birch and Swinnerton-Dyer for an Elliptic Curveof Rank 3*, http://www.jstor.org/stable/2007967

Jonathan J. Wilson. (2024). *A Comprehensive Proof of the Birch and Swinnerton-Dyer Conjecture Using the CASU Framework*, DOI:10.13140/RG.2.2.35243.86564

Lynn. H. Loomis and Shlomo Sternberg. (1990). *Advanced Calculus.* Jones and Bartlett Publishers, Inc, USA.

Quynh Ho Nguyen, Tri Nguyen Nguyen, Dinh Van Ta. *Advanced Mathematics.* Vietnam Education Publishing House Limited Company., 11 edition, 2013.

R. van Bommel. (2016). *Birch and Swinnerton-Dyer conjecture*, https://raymondvanbommel.nl/talks/bsdtalk.pdf

Rwanda Basic Education Board. (2020). *Advanced Mathematics.* Government of Rwanda.

Seoyoung Kim and M. Ram Murty, with an appendix by Andrew V. Sutherland, (2023), *From The Birch And Swinnerton-Dyer Conjecture To Nagao's Conjecture,* https://doi.org/10.1090/mcom/3773

Séminaire N. Bourbaki. (1966). *On the Conjectures of Birch and Swinnerton-Dyer and a Geometric analog*, http://www.numdam.org/item?id=SB_1964-1966__9__415_0

Stephan Siklos. (2016). *Advanced Problems In Mathematics*. Lightning Source for Open Book Publishers, UK, US.

William A. Stein. (1991). *The Birch and Swinnerton-Dyer Conjecture, a Computational Approach.* https://williamstein.org/books/bsd/bsd.pdf

William Stein. (2004). *Solving Certain Cubic Equations: An Introduction to the Birch and Swinnerton-Dyer Conjecture,* http://modular.fas.harvard.edu/sums

Xin Wan. (2020). *Iwasawa theory for modular forms.* Development of Iwasawa Theory — the Centennial of K. Iwasawa's Birth pp. 61–78.

Ye Tian. (2022). The Congruent Number Problem And Elliptic Curves. EMS Press