The Birch and Swinnerton-Dyer Conjecture On The Rank Of Elliptic Curves Over Rational Numbers

by Stephen Crowley

August 28, 2025

Table of contents

1 The Birch and Swinnerton-Dyer Conjecture

The Birch and Swinnerton-Dyer conjecture is fundamentally about elliptic curves over the rational numbers and specifically about understanding when these curves have infinitely many rational solutions versus only finitely many.

1.1 Foundational Definitions

Definition 1. *The integers* $\mathbb{Z}$ *are the set* $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Definition 2. *The rational numbers* $\mathbb{Q}$ *are the set* $\{p / q : p, q \in \mathbb{Z}, q \neq 0\}$.

Definition 3. *A monomial in variables* $x_1, \ldots, x_n$ *is an expression of the form* $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ *where each* $a_i \geq 0$ *is a nonnegative integer.*

Definition 4. *The degree of a monomial* $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ *is the sum* $a_1 + a_2 + \cdots + a_n$.

Definition 5. *A polynomial in variables* $x_1, \ldots, x_n$ *with coefficients in* $\mathbb{Q}$ *is a finite linear combination of monomials:* $f(x_1, \ldots, x_n) = \sum c_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n}$ *where* $c_{\mathbf{a}} \in \mathbb{Q}$ *and only finitely many* $c_{\mathbf{a}}$ *are nonzero.*

Definition 6. *A homogeneous polynomial of degree* d *in variables* $x_1, \ldots, x_n$ *is a polynomial* f *such that every monomial term in* f *has total degree* d. *That is, if* $f = \sum c_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n}$ *where* $c_{\mathbf{a}} \neq 0$, *then* $a_1 + \cdots + a_n = d$ *for all such terms.*

Definition 7. *The projective plane* $\mathbb{P}^2(\mathbb{Q})$ *over* $\mathbb{Q}$ *consists of equivalence classes* $[x\colon y\colon z]$ *where* $(x, y, z) \in \mathbb{Q}^3 \setminus \{(0,0,0)\}$ *and* $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$ *for any nonzero* $\lambda \in \mathbb{Q}$.

Definition 8. *A projective curve* C *in* $\mathbb{P}^2(\mathbb{Q})$ *is the set* $C = \{[x\colon y\colon z] \in \mathbb{P}^2(\mathbb{Q})\colon F(x, y, z) = 0\}$ *where* $F(x, y, z)$ *is a homogeneous polynomial with coefficients in* $\mathbb{Q}$.

Definition 9. *The partial derivative of a polynomial* $F(x, y, z)$ *with respect to* x *is the polynomial* $\frac{\partial F}{\partial x}$ *obtained by differentiating each term: if* $F = \sum c_{ijk} x^i y^j z^k$, *then* $\frac{\partial F}{\partial x} = \sum i \cdot c_{ijk} x^{i-1} y^j z^k$.

Definition 10. *A point* $P = [a\colon b\colon c]$ *on a projective curve* C *defined by* $F(x, y, z) = 0$ *is singular if all three partial derivatives vanish at* P*:*

$$\frac{\partial F}{\partial x}(a, b, c) = \frac{\partial F}{\partial y}(a, b, c) = \frac{\partial F}{\partial z}(a, b, c) = 0$$

Definition 11. *A projective curve is non-singular (or smooth) if it contains no singular points.*

Definition 12. *The genus of a non-singular projective curve defined by a homogeneous polynomial of degree* d *is* $g = \frac{(d-1)(d-2)}{2}$.

Definition 13. *An elliptic curve over* $\mathbb{Q}$ *is a non-singular projective curve of genus 1 equipped with a specified rational point. It can be written in Weierstrass form as:*

$$E\colon y^2 z = x^3 + a x z^2 + b z^3$$

where $a, b \in \mathbb{Q}$ *and the discriminant* $\Delta = -16(4a^3 + 27b^2) \neq 0$.

Definition 14. *The point at infinity on an elliptic curve in Weierstrass form is* $O = [0\colon 1\colon 0]$.

Definition 15. *An abelian group is a set* G *with an operation* $+\colon G \times G \to G$ *such that:*

1. *(Associativity)* $(a + b) + c = a + (b + c)$ *for all* $a, b, c \in G$
2. *(Identity) There exists* $0 \in G$ *such that* $a + 0 = 0 + a = a$ *for all* $a \in G$
3. *(Inverse) For each* $a \in G$, *there exists* $-a \in G$ *such that* $a + (-a) = 0$
4. *(Commutativity)* $a + b = b + a$ *for all* $a, b \in G$

Definition 16. *A group homomorphism* $f\colon G \to H$ *between abelian groups* G *and* H *is a function such that* $f(g_1 + g_2) = f(g_1) + f(g_2)$ *for all* $g_1, g_2 \in G$.

Definition 17. *Let $f: G \rightarrow H$ be a group homomorphism between groups G and H with identity elements 0_G and 0_H respectively. The kernel of f is the set:*

$$\ker(f) = \{g \in G: f(g) = 0_H\}$$

It is a subgroup of G consisting of all elements mapped to the identity element 0_H of H.

Definition 18. *The set $E(\mathbb{Q})$ of rational points on an elliptic curve E forms an abelian group under the chord-and-tangent law with identity element O and group operation defined as follows: For distinct points $P = [x_1: y_1: 1], Q = [x_2: y_2: 1] \in E(\mathbb{Q})$ with $P, Q \neq O$:*

1. *If $x_1 \neq x_2$, let ℓ be the line through P and Q. This line intersects E at exactly three points: P, Q, and a third point R. Define $P + Q$ to be the point such that $P + Q + R = O$ under the group law.*
2. *If $x_1 = x_2$ and $y_1 = -y_2$, then $P + Q = O$.*
3. *If $P = Q$ and $y_1 \neq 0$, let ℓ be the tangent line to E at P. This intersects E at P (with multiplicity 2) and one other point R. Define $2P$ such that $2P + R = O$.*
4. *For any $P \in E(\mathbb{Q})$: $P + O = O + P = P$.*

Definition 19. *The rank of an abelian group G is the dimension of $G \otimes \mathbb{Q}$ as a $\mathbb{Q}$-vector space.*

Definition 20. *A square-free integer is an integer n such that no perfect square other than 1 divides n.*

1.2 Galois Theory and Cohomology

Definition 21. *The algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ is the field consisting of all algebraic numbers (roots of polynomials with rational coefficients).*

Definition 22. *The absolute Galois group $G_{\mathbb{Q}} = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ is the group of all field automorphisms of $\bar{\mathbb{Q}}$ that fix every element of $\mathbb{Q}$.*

Definition 23. *A $G_{\mathbb{Q}}$-module is an abelian group M together with a group homomorphism $G_{\mathbb{Q}} \rightarrow Aut(M)$.*

Definition 24. *For a $G_{\mathbb{Q}}$-module M, the first Galois cohomology group $H^1(\mathbb{Q}, M)$ is the set of continuous maps $f: G_{\mathbb{Q}} \rightarrow M$ satisfying $f(\sigma\tau) = f(\sigma) + \sigma(f(\tau))$ for all σ, $\tau \in G_{\mathbb{Q}}$, modulo the equivalence relation where $f \sim g$ if there exists $m \in M$ such that $f(\sigma) - g(\sigma) = \sigma(m) - m$ for all $\sigma \in G_{\mathbb{Q}}$.*

Definition 25. *A place of $\mathbb{Q}$ is either a prime number p (finite place) or the symbol ∞ (infinite place).*

Definition 26. *For a finite place p, the completion $\mathbb{Q}_p$ is the field of p-adic numbers, obtained by completing $\mathbb{Q}$ with respect to the p-adic absolute value $|x|_p$.*

Definition 27. *For the infinite place ∞, the completion $\mathbb{Q}_\infty = \mathbb{R}$ is the field of real numbers.*

Definition 28. *For each place v of $\mathbb{Q}$, the local Galois group is $G_{\mathbb{Q}_v} = Gal(\overline{\mathbb{Q}_v}/\mathbb{Q}_v)$ where $\overline{\mathbb{Q}_v}$ is the algebraic closure of $\mathbb{Q}_v$.*

Definition 29. *The Shafarevich-Tate group $\text{X}(E/\mathbb{Q})$ of an elliptic curve E over $\mathbb{Q}$ is the kernel of the natural map:*

$$\text{X}(E/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q}, E) \to \prod_v H^1(\mathbb{Q}_v, E)\right)$$

where the product runs over all places v of $\mathbb{Q}$ and the maps are the natural restriction maps from global to local cohomology.

1.3 L-Functions

Definition 30. *Let $\mathbb{F}_p$ denote the field with p elements, where p is prime.*

Definition 31. *An elliptic curve E over $\mathbb{Q}$ has good reduction at a prime p if the curve obtained by reducing the coefficients of its Weierstrass equation modulo p is non-singular over $\mathbb{F}_p$.*

Definition 32. *An elliptic curve E over $\mathbb{Q}$ has multiplicative reduction at a prime p if the reduced curve modulo p has exactly one singular point, which is a node (intersection of two distinct lines).*

Definition 33. *An elliptic curve E over $\mathbb{Q}$ has additive reduction at a prime p if the reduced curve modulo p has a cusp or worse singularity.*

Definition 34. *The Hasse-Weil L-function $L(E, s)$ of an elliptic curve E over $\mathbb{Q}$ is defined as the Euler product:*

$$L(E, s) = \prod_{p prime} L_p(E, s)^{-1}$$

which converges absolutely for $\mathrm{Re}(s) > \frac{3}{2}$, where each local L-factor $L_p(E, s)$ is defined as:

1. *If E has good reduction at p: $L_p(E, s) = 1 - a_p p^{-s} + p^{1-2s}$ where $a_p = p + 1 - |E(\mathbb{F}_p)|$*
2. *If E has multiplicative reduction at p: $L_p(E, s) = 1 - a_p p^{-s}$ where $a_p = \pm 1$*
3. *If E has additive reduction at p: $L_p(E, s) = 1$*

Definition 35. *The order of vanishing of a function $f(s)$ at $s = s_0$ is the largest integer k such that $(s - s_0)^k$ divides $f(s)$ in a neighborhood of s_0.*

Definition 36. *The Tamagawa number $c_p(E)$ of an elliptic curve E at a prime p is the index $[E(\mathbb{Q}_p)\colon E^0(\mathbb{Q}_p)]$, where $E^0(\mathbb{Q}_p)$ is the subgroup of points with good reduction.*

Definition 37. *The real period Ω_E of an elliptic curve E is $\int_{E(\mathbb{R})} |\omega|$ where ω is the invariant differential on E.*

Definition 38. *The regulator $\operatorname{Reg}(E/\mathbb{Q})$ is the determinant of the Gram matrix of the canonical height pairing on the free part of $E(\mathbb{Q})$.*

1.4 The Conjecture

Conjecture 39. *[Birch and Swinnerton-Dyer] Let E be an elliptic curve over $\mathbb{Q}$. Then:*

1. *The Shafarevich-Tate group $\text{Ш}(E/\mathbb{Q})$ is finite.*
2. $\operatorname{ord}_{s=1} L(E, s) = \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q})$
3. $\lim_{s \to 1} \frac{L(E, s)}{(s-1)^r} = \frac{\Omega_E \cdot \operatorname{Reg}(E/\mathbb{Q}) \cdot |\text{Ш}(E/\mathbb{Q})| \prod_p c_p(E)}{|E(\mathbb{Q})_{\text{tors}}|^2}$ *where* $r = \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q})$.

1.5 Connection to Square-Free Numbers

Definition 40. *The quadratic twist of an elliptic curve $E\colon y^2 = x^3 + a\,x + b$ by a square-free integer n is the curve $E_n\colon n\,y^2 = x^3 + a\,x + b$.*

Definition 41. *A congruent number is a square-free positive integer n that is the area of a right triangle with rational side lengths.*

Theorem 42. *Let n be a square-free positive integer. Then n is a congruent number if and only if the elliptic curve $E_n\colon y^2 = x^3 - n^2\,x$ has positive rank. By the Birch and Swinnerton-Dyer conjecture, this is equivalent to $L(E_n, 1) = 0$.*

The conjecture involves square-free numbers because the behavior of L-functions $L(E_n, s)$ at $s = 1$ for quadratic twists by square-free integers n determines the solvability of fundamental Diophantine equations.