

THE BIRCH AND SWINNERTON-DYER CONJECTURE

1. INTRODUCTION

Suppose that $a, b \in \mathbb{Q}$ and let

$$E : y^2 = x^3 + ax + b$$

be an elliptic curve. The set of points

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q} : y^2 = x^3 + ax + b\} \cup \{\infty\}$$

has the structure of an abelian group, where we define $P + Q + R = 0$ if P , Q , and R are three collinear points on E , and the inverse of (x, y) is $(x, -y)$.

Theorem 1 (Mordell-Weil). *The group $E(\mathbb{Q})$ is finitely generated.*

[Mordell proved this for elliptic curves over \mathbb{Q} , and Weil proved this for abelian varieties over arbitrary number fields in his thesis.]

As a consequence, we have

$$E(\mathbb{Q}) \cong G \times \mathbb{Z}^r$$

for some finite abelian group G and some non-negative integer r (called the rank).

Q: Given an elliptic curve E , how can one compute the rank r ?

In the early 1960s, Bryan Birch and Peter Swinnerton-Dyer considered the quantity

$$\prod_{p < x} \frac{N_p}{p}$$

where $N_p = \#E(\mathbb{F}_p)$ for various elliptic curves over \mathbb{Q} with known ranks. They did numerical investigations on an EDSAC computer. These led them to guess that

$$\prod_{p < x} \frac{N_p}{p} \sim C(\log x)^r,$$

where r is the rank of the elliptic curve. This led them to make the conjecture that now bears their name. It was formalized in terms of the Hasse-Weil L -function of an elliptic curve.

2. STATEMENT OF BSD

If p is prime, define

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

Theorem 2 (Hasse). *We have*

$$|a_p| \leq 2\sqrt{p}.$$

Definition. Let

$$L_p(T) = \begin{cases} 1 - a_p T + pT^2 & E \text{ is non-singular over } \mathbb{F}_p \\ 1 - T & E \text{ has split multiplicative reduction at } p \\ 1 + T & E \text{ has non-split multiplicative reduction at } p \\ 1 & E \text{ has additive reduction at } p. \end{cases}$$

The Hasse-Weil L -function of E is defined by

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

It follows from the Hasse bound that $L(E, s)$ converges absolutely for $\operatorname{Re}(s) > 3/2$.

Conjecture 3. *The function $L(E, s)$ has an analytic continuation to all of \mathbb{C} , and a functional equation relating $L(E, s)$ and $L(E, 2 - s)$.*

Finally, we state the Birch and Swinnerton-Dyer conjecture.

Conjecture 4 (BSD I). *We have*

$$\operatorname{ord}_{s=1} L(E, s) = r.$$

[The left hand side is the order of the zero of the function $L(E, s)$ at $s = 1$].

This conjecture is one of the seven Millenium Prize Problems sponsored by the Clay Mathematics Institute. Hence, there is a one million dollar prize for the proof of this conjecture.

There is a more precise conjecture that we will describe now.

Conjecture 5 (BSD II). *If r is the rank of $E(\mathbb{Q})$, then*

$$\lim_{s \rightarrow 1} \frac{L(E, s)}{(s-1)^r} = \frac{\Omega R \# \text{III}(E/\mathbb{Q}) \prod_p c_p}{\#E(\mathbb{Q})_{\text{tors}}^2}.$$

Now, we will discuss each of the pieces in the above formula.

1. $E(\mathbb{Q})_{\text{tors}}$. This is the group of torsion points on E/\mathbb{Q} .

Mazur proved that $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 10$ or $n = 12$ or $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for $1 \leq n \leq 4$. (This is a difficult theorem, exploiting the moduli interpretation of modular curves). There are explicit families of elliptic curves that have each of the torsion subgroups above.

2. “The real period,” Ω .

If ω is the invariant differential on E , then

$$\Omega = \int_{E(\mathbb{R})} |\omega|.$$

If E has the equation $y^2 = x^3 + ax + b$ then $\omega = \frac{dx}{2y}$. [The number Ω is either the real period, or twice the real period, depending on whether or not $E(\mathbb{R})$ is connected.]

3. “The regulator,” R .

If $P \in E(\mathbb{Q})$, we define the naive height of $P = (u, v)$ to be

$$h(P) = \log \max(|u|, |v|).$$

Then, we define the canonical height

$$\hat{h}(P) = \frac{1}{2} \lim_{n \rightarrow \infty} \frac{h(2^n P)}{4^n}.$$

This function satisfies

$$\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q).$$

It follows from this that the Néron-Tate pairing

$$\langle P, Q \rangle = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)$$

is a bilinear form. It is also true that $\hat{h}(P) = 0$ if and only if P is a torsion point.

Finally, let P_1, \dots, P_r be a basis for $E(\mathbb{Q})/E_{\text{tors}}(\mathbb{Q})$. Let M be the matrix whose i, j entry is $\langle P_i, P_j \rangle$. Then, $R = \det M$. We take $R = 1$ if $r = 0$.

4. “The Tamagawa numbers,” c_p .

Let \mathbb{Q}_p be the field of p -adic numbers and let $E_0(\mathbb{Q}_p)$ denote the subgroup of $E(\mathbb{Q}_p)$ of points that reduce mod p to a non-singular point of $E(\mathbb{F}_p)$. If $E(\mathbb{F}_p)$ is non-singular, then $c_p = 1$, and so the product in the conjecture above is finite.

5. “The Shafarevich-Tate group,” $\text{III}(E/\mathbb{Q})$.

This abelian group is defined in terms of Galois cohomology:

$$\text{III}(E/\mathbb{Q}) = \ker \left[H^1(\mathbb{Q}, E) \rightarrow H^1(\mathbb{R}, E) \times \prod_p H^1(\mathbb{Q}_p, E) \right].$$

This is “the global cohomology classes that are locally trivial everywhere.” In more plain English the “fraction” of genus 1 curves X over \mathbb{Q} so that

- (i) $X \cong E$ over $\overline{\mathbb{Q}}$,
- (ii) There are points in $X(\mathbb{Q}_p)$ for all p .
- (iii) X doesn't have any rational points

is $\frac{1}{\#\text{III}(E/\mathbb{Q})}$.

This is the most mysterious part of the BSD picture. At some level, **III** measures the failure of the local-to-global principle. It is conjectured that $\text{III}(E/\mathbb{Q})$ is finite, but this has not been proved in general.

In 1974, John Tate remarked “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 **III** which is not known to be finite!”

To demonstrate our lack of knowledge in general about this problem, the following is open.

Problem: Let $E : y^2 = x^3 - 1267x + 17230$. One can show that

$$E(\mathbb{Q}) \cong \mathbb{Z}^4$$

and is generated by $(23, -16)$, $(15, 40)$, $(19, 4)$ and $(31, 88)$. Show that $\text{ord}_{s=1} L(E, s) = 4$.

(If one could prove this, then a stronger effective lower bound on the class number would follow than is currently known).

3. KNOWN RESULTS

Definition. An elliptic curve E/\mathbb{Q} has complex multiplication if $\text{End}(E)$, the ring of morphisms from E to itself (defined over $\overline{\mathbb{Q}}$) has other elements than multiplication by n maps.

Definition. An elliptic curve E/\mathbb{Q} is modular if there is a non-constant morphism $\phi : X_0(N) \rightarrow E$ for some positive integer N . [$X_0(N) := \mathbb{H}/\Gamma_0(N)$].

In this case, it is known that $L(E, s) = L(f, s)$ is the L -function of a weight 2 modular form. Since L -functions of modular forms have an analytic continuation and functional equation, Conjecture 3 is known in this case.

Theorem 6 (Coates-Wiles, 1977). *If E/\mathbb{Q} has CM, then $\#E(\mathbb{Q}) = \infty$ implies that $L(E, 1) = 0$.*

This result was Wiles Ph.D. thesis. The proof works by showing that $L(E, 1) = \alpha\beta$ with $\beta \in \mathbb{Q}$ and showing that there are infinitely many primes that divide the numerator of β . Hence, $\beta = 0$.

Theorem 7 (Gross-Zagier, 1986). *If E/\mathbb{Q} is modular and $L(E, s)$ has a simple zero at $s = 1$, then $E(\mathbb{Q})$ is infinite.*

Gross and Zagier constructed an explicit point $P \in E(\mathbb{Q})$ and showed that

$$L'(E, 1) = c\hat{h}(P)$$

where c is some explicit non-zero constant. Then, the assumption that $L'(E, 1) \neq 0$ means that $\hat{h}(P) \neq 0$ and hence P has infinite order.

The final partial result in the direction of BSD is due to Kolyvagin, with one auxiliary step dealt with by others.

Theorem 8 (Kolyvagin, others 1988-1989). *If E/\mathbb{Q} is a modular elliptic curve with rank r and $\text{ord}_{s=1}L(E, s) \leq 1$ then $\text{ord}_{s=1}L(E, s) = r$ and $|\text{III}(E/\mathbb{Q})| < \infty$.*

The most recent work relevant to BSD is the following result.

Theorem 9 (Breuil, Conrad, Diamond, Taylor, Wiles, ..., 1999). *All elliptic curves over \mathbb{Q} are modular.*

This implies that the Theorem of Kolyvagin, et. al. applies to all elliptic curves over \mathbb{Q} .

4. APPLICATIONS

Fermat's last theorem for exponent 3:

The curve

$$F_3 : x^3 + y^3 = z^3$$

is an elliptic curve. It is isomorphic to $X_0(27)$. There is a change of variables that takes it to

$$E : y^2 = x^3 - 432.$$

The torsion subgroup is $\mathbb{Z}/3\mathbb{Z}$ and these three points correspond to the trivial solutions $(x, -x, 0)$, $(x, 0, -x)$ and $(0, y, -y)$ to the original equation. It suffices to show that E has rank zero.

Fact: If E is an elliptic curve of conductor N and f is the modular form associated to E , then

$$L(E, 1) = L(f, 1) = \frac{1}{2\pi\sqrt{N}} \int_0^\infty f\left(\frac{iy}{\sqrt{N}}\right) dy.$$

In this case, the modular form is

$$f(z) = q \prod_{n=1}^{\infty} (1 - q^{3n})^2 (1 - q^{9n})^2 = q - 2q^4 - q^7 + 5q^{13} + \dots$$

The modular form will always have leading coefficient q .

The product expansion implies that f doesn't vanish on \mathbb{H} . Moreover, if y is large,

$$f\left(\frac{iy}{\sqrt{N}}\right) = e^{-2\pi y/\sqrt{N}} + O(e^{-4\pi y/\sqrt{N}}) > 0.$$

Thus, we have that $f\left(\frac{iy}{\sqrt{N}}\right)$ is

- (i) Real for all y ,
- (ii) Positive for y large,
- (iii) Non-zero for all y ,

it follows that $f\left(\frac{iy}{\sqrt{N}}\right) > 0$ for all y and hence $L(E, 1) > 0$. This implies (by Wiles theorem) that E has rank zero and FLT 3 is true!

FLT for exponent 4:

The curve

$$F_4 : x^4 + y^4 = z^4$$

has genus 3. It is isomorphic to $X_0(64)$. This follows from the identity

$$\vartheta_2^4 + \vartheta_4^4 = \vartheta_3^4,$$

where

$$\begin{aligned} \vartheta_2(z) &= \sum_{n \in \mathbb{Z}} q^{(n+1/2)^2} \\ \vartheta_3(z) &= \sum_{n \in \mathbb{Z}} q^{n^2} \\ \vartheta_4(z) &= \sum_{n \in \mathbb{Z}} (-1)^n q^{n^2}. \end{aligned}$$

It has 8 automorphisms (defined over \mathbb{Q}), one of which is $\phi((x, y, z)) = (y, x, z)$. The quotient of the curve by a finite group is always defined, and in this case $F_4/\langle\phi\rangle$ is the elliptic curve

$$Y^2Z = X^3 - XZ^2$$

The map is given by

$$\begin{aligned} X &= -x^3y + x^3z - x^2y^2 + x^2yz + y^4 - z^4 \\ Y &= 2x^3y + x^2y^2 - x^2z^2 - y^4 + z^4 \\ Z &= -x^3y + x^3z + x^2yz - x^2z^2 \end{aligned}$$

The affine points are those on

$$y^2 = x^3 - x.$$

This elliptic curve has conductor 32 and the corresponding modular forms is

$$\eta^2(4z)\eta^2(8z).$$

Again, it is non-vanishing on \mathbb{H} and so $L(E, 1) > 0$. The torsion subgroup is $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. The points are the point at infinity, $(0, 0)$, $(1, 0)$ and $(-1, 0)$. One can check that the preimages of these four points are the four trivial solutions $(0, 1, 1)$, $(0, -1, 1)$, $(1, 0, 1)$ and $(-1, 0, 1)$.

FLT for exponent 7:

Consider

$$F_7 : x^7 + y^7 + z^7 = 0.$$

If we set $X_1 = x^3z$, $Y_1 = y^3x$ and $Z_1 = z^3y$, then

$$Q : X_1^3Y_1 + Y_1^3Z_1 + Z_1^3X_1 = 0.$$

This is the Klein quartic and is isomorphic to $X(7) := \mathbb{H}/\Gamma(7)$.

Now, if $\alpha = \begin{bmatrix} 0 & -1 \\ 7 & 0 \end{bmatrix}$, then the map

$$z \mapsto \alpha z$$

gives an isomorphism of $\mathbb{H}/\Gamma(7) \rightarrow \mathbb{H}/\Gamma$, where

$$\Gamma = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a \equiv d \equiv 1 \pmod{7}, 49|c \right\}$$

This is a subgroup of $\Gamma_0(49)$, and hence $X_0(49)$ is a quotient of this. Now, $X_0(49)$ is an elliptic curve, and it is isomorphic to

$$E : Y_2^2Z_2 + X_2Y_2Z_2 = X_2^3 - X_2^2Z_2 - 2X_2Z_2^2 - Z_2^3.$$

(The map from $X(7) \rightarrow X_0(49)$ is given by polynomials of degree 10).

If $f(z) \in S_2(\Gamma_0(49))$ is the modular form corresponding to E , then a version of the valence formula for $\Gamma_0(49)$ gives that

$$\frac{k}{12} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(49)] = \sum_{p \in \mathbb{H}/\Gamma_0(49)} \frac{1}{e_p} \mathrm{ord}_p(f),$$

where $e_p = 1$ unless p is one of the two elliptic fixed points of order 3, in which case $e_p = 3$. Now, $\Gamma_0(49)$ has 8 cusps, and two elliptic fixed points at

$$\frac{37 + i\sqrt{-3}}{98}, \frac{61 + i\sqrt{-3}}{98}.$$

of order 3. At these points, the transformation law for f implies that f must have a double zero. However,

$$8 + 2 \cdot \frac{2}{3} = \frac{28}{3} = \frac{2}{12} \cdot 56 = \frac{k}{12} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(49)].$$

It follows that f is non-vanishing on the imaginary axis, and the same argument as above implies that $L(f, 1) > 0$. Thus, E has rank zero.

The torsion subgroup of E is $\mathbb{Z}/2\mathbb{Z}$, and one can check that neither point on E produces a non-trivial point on

$$x^7 + y^7 + z^7 = 0.$$