American Journal of Mathematics and Statistics 2016, 6(4): 182-189
DOI: 10.5923/j.ajms.20160604.07

Review of the Birch and Swinnerton-Dyer Conjecture

R. K. Ansah[1,*], R. K. Boadi[2], W. Obeng-Denteh[2], A. Y. Omari-Sasu[2]

[1]Department of Mathematics and Statistics, UENR, Sunyani, Ghana
[2]Department of Mathematics, KNUST, Kumasi, Ghana

Abstract The Birch and Swinnerton-Dyer Conjecture is a well known mathematics problem in the area of Elliptic Curve. One of the crowning moments is the paper by Andrew Wiles which is difficult to understand let alone to appreciate the conjecture. This paper surveys the background of the conjecture treating the ranks of the elliptic curves over the field of rational numbers. Then we present major results like the theorems of Mordell and Mazur leading us to the current state of the conjecture.

Keywords Elliptic curve, Birch and Swinnerton-Dyer Conjecture, Additive abelian group, Mordell theorem

1. Introduction

L. J. Mordell began his famous paper with the words "Mathematicians have been familiar with very few questions for so long a period with so little accomplished in the way of general results, as that of finding the rational points on elliptic curves" [1]. Elliptic curves have a lot of applications, this because it possible to take two Points on the curve and generate a third point. In fact, we will show that by defining an addition operation and introducing an extra point called the point of infinity, the points on an elliptic curve form an additive abelian group [12]. There are still a number of significant open questions specific to the theory of elliptic curves themselves, such as the conjecture of Birch and Swinnerton-Dyer which would give a much more precise description of the beautiful arithmetic that exists for points on elliptic curves [14].

2. The Algebra and Geometry of Elliptic Curves

Elliptic curves are functions defined by equation of the form

$$y^2 = f(x) \tag{1}$$

$f(x)$ has no multiple roots. The cubic equation

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

does not define an elliptic curve, because

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

has 1 as a multiple root. Similarly

$$y^2 = x^3$$

is not an elliptic curve, but

$$y^2 = x^3 + 1$$

is an elliptic curve.

The general form of an elliptic curve is given below

$$y^2 = x^3 + Ax + B \tag{2}$$

Where $x, y, A\ and\ B$ belong to a specified field such as $\mathbb{R}, \mathbb{C}, or\ \mathbb{Q}$.

General we use E to represent an elliptic curve.

If we wish to consider points in a field K we write $E(K)$, which is defined as below.

$$E(K) = \{\{\infty\} \cup : y^2 = x^3 + A + B\} \tag{3}$$

2.1. We can Use Geometry to Make the Points of an Elliptic Curve into a Group

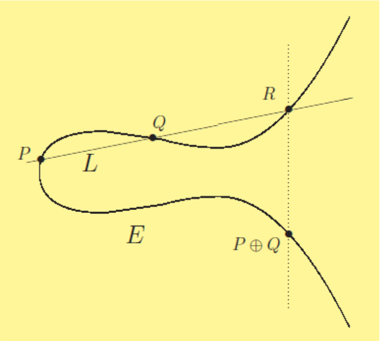


Figure 1. $P + Q$

2.2. Properties of "Addition" on Elliptic Curve

The addition law on an Elliptic curve has the following properties:

a) $P + \infty = \infty + P = P$ for all $P \in E$.
b) $P + (-P) = \infty$ for all $P \in E$.
c) $P + (Q + R) = (P + Q) + R$ for all $P, Q, R \in E$.
d) $P + Q = Q + P$ for all $P, Q \in E$.

* Corresponding author:
richans91@gmail.com (R. K. Ansah)

Published online at http://journal.sapub.org/ajms

In other words, the addition law + makes the points of E into a commutative group. [11]

2.3. The Addition Operation is Summarized below

Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E with $\mathrm{P}_1, \mathrm{P}_2 \neq \infty$.

We the define $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows

1. If $x_1 \neq x_2$ then $x_3 = m^2 - x_1 - x_2,$ $y_3 = m(x_1 - x_3) - y_1$ where $m = \frac{y_2 - y_1}{x_2 - x_1}$.
2. If $\mathrm{x}_1 = x_2$ but $y_1 \neq y_2$, then $P_1 + P_2 = \infty$.
3. If $P_1 = P_2 = (x_1, y_1\ )$ and $y_1 \neq 0$ then $x_3 = m^2 - 2x_1, y_3 = m(x_1 - x_3) - y_1$ where $m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$.
4. If $P_1 = P_2 = (x_1, y_1\ )$ and $y_1 = 0$, then $P_1 + P_2 = \infty$.

Also we define $P + \infty = P$ for all points P on E [12].

2.3.1. Example 1

Let E be the curve $y^2 = x^3 - x + 1$ and **suppose** we know the point $\left(\frac{-11}{9}, \frac{17}{27}\right)$ and (0,1) lies on the curve. To find another point on. In the notation of elliptic curve addition we have:

$$\mathrm{m} = \frac{\mathrm{y}_2 - \mathrm{y}_1}{\mathrm{x}_2 - \mathrm{x}_1} = \frac{1 - \frac{17}{27}}{0 - \frac{11}{9}} = \frac{10}{33}$$

$$\mathrm{x}_3 = \mathrm{m}^2 - \mathrm{x}_1 - \mathrm{x}_2 = \left(\frac{10}{33}\right)^2 + \frac{11}{9} - 0 = \frac{59}{121}\ ,$$

$$\mathrm{y}_3 = \mathrm{m}(\mathrm{x}_1 - \mathrm{x}_3) - \mathrm{y}_1 = \frac{10}{33}\left(\frac{-11}{9} - \frac{159}{121}\right) - \frac{17}{27} = \frac{-1861}{1331}$$

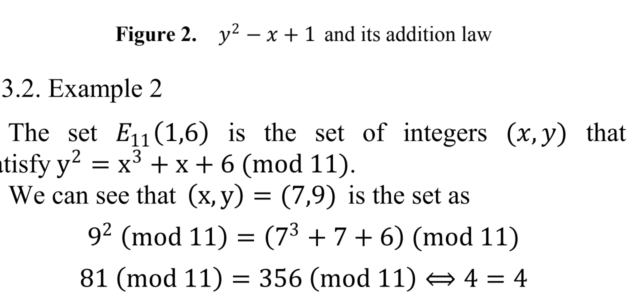

$Q = (0,1)$
$R = (\frac{159}{121}, \frac{1861}{1331})$
$P = (-\frac{11}{9}, \frac{17}{27})$
$P + Q = (\frac{159}{121}, -\frac{1861}{1331})$

Figure 2. $y^2 - x + 1$ and its addition law

2.3.2. Example 2

The set $E_{11}(1,6)$ is the set of integers (x, y) that satisfy $\mathrm{y}^2 = \mathrm{x}^3 + \mathrm{x} + 6 \text{ (mod 11)}$.

We can see that $(\mathrm{x}, \mathrm{y}) = (7,9)$ is the set as

$$9^2 \text{ (mod 11)} = (7^3 + 7 + 6) \text{ (mod 11)}$$

$$81 \text{ (mod 11)} = 356 \text{ (mod 11)} \Leftrightarrow 4 = 4$$

To find all the points in $\mathrm{E}_{11}(1,6)$ we find all the possible values $\mathrm{x}^3 + \mathrm{x} + 6 \text{ (mod 11)}$ and then see what values of y^2 will match. There are 11 choices of x, the integers $\{0,1, \ldots 10\}$. Subbing these values in turn into the cubic and reducing modulo 11 will give us the possible values of y^2.

a) x = 0 $\Longrightarrow$ RHS = 6
b) x = 1 $\Longrightarrow$ RHS = 8
c) x = 2 $\Longrightarrow$ RHS = 16 $\equiv$ 5
d) x = 3 $\Longrightarrow$ RHS = 36 $\equiv$3
e) x = 4 $\Longrightarrow$ RHS = 74 $\equiv$ 8
f) x = 5 $\Longrightarrow$ RHS = 136 $\equiv$ 4
g) x = 6 $\Longrightarrow$ RHS = 228 $\equiv$8
h) x = 7 $\Longrightarrow$ RHS = 356 $\equiv$4
i) x = 8 $\Longrightarrow$ RHS = 526 $\equiv$ 9
j) x = 9 $\Longrightarrow$ RHS = 744 $\equiv$ 7
k) x = 10 $\Longrightarrow$ RHS = 1016 $\equiv$4

So we can see that the possible values of y^2 $\{3,4,5,6,7,8,9\}$ i.e. y^2 cannot be 0, 1, 2 or 10.

Next examine the 10 possible values of y and identify which values of x they could be paired with to give a point on the curve.

a) y = 0 $\Longrightarrow$ y^2= 0$\Longrightarrow$ No points
b) y = 1 $\Longrightarrow$ y^2 = 1 $\Longrightarrow$ No points
c) y = 2 $\Longrightarrow$ y^2= 4 $\Longrightarrow$x = 5, 7, 10
d) y = 3 $\Longrightarrow$ y^2= 9 $\Longrightarrow$ x = 8
e) y = 4 $\Longrightarrow$ y^2= 16 $\equiv$ 5 $\Longrightarrow$ x = 2
f) y = 5 $\Longrightarrow$ y^2= 25 $\equiv$3 $\Longrightarrow$x = 3
g) y = 6 $\Longrightarrow$ y^2= 36 $\equiv$3 $\Longrightarrow$x = 3
h) y = 7 $\Longrightarrow$ y^2= 49 $\equiv$ 5 $\Longrightarrow$x = 2
i) y = 8 $\Longrightarrow$ y^2 = 64 $\equiv$ 9 $\Longrightarrow$x = 8
j) y = 9 $\Longrightarrow$ y^2 = 81 $\equiv$ 4 $\Longrightarrow$x = 5, 7, 10
k) y = 10 $\Longrightarrow$ y^2 = 100$\equiv$ 1 $\Longrightarrow$No points

$\mathrm{E}_{11}(1,6)\ ) -$ (the 12 found above and ∞):

$\mathrm{E}_{11}(1,6)$ = {(2, 4), (2, 7), (3, 5), (3, 6), (5, 2), (5, 9), (7, 2), (7, 9), (8, 3), (8, 8), (10, 2), (10, 9),∞}

$$\mathrm{x}_{2\mathrm{P}} = 1^2 - 2(8) = -15 = 7 \text{ (mod 11)},$$

$$\mathrm{y}_{2\mathrm{P}} = 1(8 - 7) - 3 = -2 = 9 \text{ (mod 11)}$$

So in $\mathrm{E}_{11}(1,6)$ we find $2(8,3) = (7,9)$.

3. Elliptic Curves over Finite Fields

Let F be a finite field and E an elliptic curve defined over F. Since there are only a finite number of pairs (x, y), with $x, y \in \mathrm{F}$, the group $E(\mathrm{F})$ must itself be finite. In this section. We discuss the basic theory of elliptic curves over finite fields and also we will state Hasse's theorem which gives a bound of the size of the group defined by $E(\mathrm{F}_q)$. We also look at methods to find the order of a point in $E(\mathrm{F})$. [12].

3.1. Example 4

Let E be thr curve $y^2 = x^3 + x + 1$ over $\mathrm{F}_5 = (Z_5)$

$\{(0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3), \infty\}$

$\mathrm{E}(\mathrm{F}_5)$ has order 9. $\mathrm{E}(\mathrm{F}_5)$ is cyclic and generated by (0,1).

3.2. Methods to determine the order of $E(\mathrm{F}_q)$

Hasse's theorem gave bounds for the group of points on an elliptic curve over a finite field. In this section we discuss methods for determining the group order exactly. Suppose we have an elliptic curve defined over a finite field $\mathrm{F_q}$, we can determine the order of $E(\mathrm{F}_q)$ by listing the points. We can then determine the order of $E(F_q^n)$ for all n. [12]

3.2.1. Theorem 1

Let $\#E(\mathrm{F}_q) = q + 1 - a$ write $X^2 - aX + q = (X - \alpha)(X - \beta)$. then for all $\mathrm{n} \geq 1$

$$E(F_q^n) = q^n + 1 - (\alpha^n + \beta^n) \qquad (4)$$

3.3. Example 3

Let $E: y^2 + xy = x^3 + 1$ be an elliptic curve $\mathrm{F_2}$ satisfies $\#\mathrm{E(F_2)} = 4$.

Therefore $a = q + 1 - E(\mathrm{F}_q) = 2 + 1 - 4 = -1$ and we obtain the polynomial

$$\mathrm{X}^2 + \mathrm{X} + 2 = \left(\mathrm{X} - \frac{-1 + \sqrt{7}}{2}\right)\left(\mathrm{X} - \frac{-1 - \sqrt{7}}{2}\right)$$

$$\#\mathrm{E(F_4)} = -\left(\mathrm{X} - \frac{-1 + \sqrt{7}}{2}\right)^2 \left(\mathrm{X} - \frac{-1 - \sqrt{7}}{2}\right)^2$$

We could compute the last expression directly, but better use the recurrence relation

$\alpha^2 + \beta^2 = \mathrm{s_2} = \mathrm{as_1} - 2\mathrm{s_0} = (-1)(-1) - 2(2) = -3$

So, $\#\mathrm{E(F_4)} = 4 + 1 - (-3) = 8$, (as we calculated when listing points).

3.4. Legendre Symbol

To make a list of all the points on $y^2 = x^3 + Ax + B$ over a finite field, we listed every possible value of x, and then found the square roots, y, of $(x^3 + Ax + B)$ if they existed. This procedure will be the basis for a simple point counting algorithm.

The Legendre symbol we can generalize this to a finite field F_q, q odd, by defining for $x \in \mathrm{F}_q$

$$\left(\frac{x}{\mathrm{F}_q}\right) = \begin{cases} +1 \; if \; t^2 = x \; has \; a \; solution \\ -1 \; if \; t^2 = x \; has \; no \; solution \\ \quad 0 \; if \; x = 0 \end{cases}$$

We can now give a more accurate solution to the number of points on $E(\mathrm{F}_q)$:

$$1 + \sum_{x \in \mathrm{F}_q} \left(1 + \left(\frac{x^3 + Ax + B}{\mathrm{F}_q}\right)\right)$$

$$= q + 1 + \sum_{x \in \mathrm{F}_q} \left(1 + \left(\frac{x^3 + Ax + B}{\mathrm{F}_q}\right)\right)$$

3.4.1. Theorem 2

Let E be an elliptic curve $\mathrm{y^2 = x^3 + Ax + B}$ over $\mathrm{F_q}$. Then

$$\#E(\mathrm{F}_q) = q + 1 + \textstyle\sum_{x \in \mathrm{F}_q} \left(1 + \left(\frac{x^3 + Ax + B}{\mathrm{F}_q}\right)\right) \qquad (5)$$

Proof.

Consider a point $\mathrm{x_0} \in \mathrm{F_q}$. There are points on E with x −coodinate $\mathrm{x_0}$ if $\mathrm{x_0^3 + Ax_0 + B}$ is a non-zero square in $\mathrm{F_q}$. There is one such point if it is zero, and no such points if it is square It follows that the number of points in E with x coordinate $\mathrm{x_0}$ is

$$1 + \left(\frac{x_0^3 + Ax_0 + B}{\mathrm{F}_q}\right)$$

So to find the order of $\mathrm{E(F_q)}$ we must sum over all $\mathrm{x_0} \in \mathrm{F_q}$ and add 1 for the point at infinity:

$$\#E(\mathrm{F}_q) = 1 + \sum_{x \in \mathrm{F}_q} \left(1 + \left(\frac{x^3 + Ax + B}{\mathrm{F}_q}\right)\right)$$

$$= q + 1 + \sum_{x \in \mathrm{F}_q} \left(1 + \left(\frac{x^3 + Ax + B}{\mathrm{F}_q}\right)\right)$$

3.5. Example 5

Let E be the curve $\mathrm{y^2 = x^3 + x + 1}$ over $\mathrm{F_5}$, $1^2 = 1, 2^2 = 4, 3^2 = 9 \; (\mathrm{mod}\; 5), 4^2 = 16 = 1(\mathrm{mod}\; 5)$

So the non-zero squares modulo 5 are 1 and 4.

$$\#E(\mathrm{F}_q) = 1 + \sum_{x \in \mathrm{F}_q} \left(1 + \left(\frac{x^3 + Ax + B}{\mathrm{F}_q}\right)\right)$$

$$= 5 + 1 + \sum_{x=0}^{4} \left(\frac{x^3 + x + 1}{\mathrm{F}_5}\right)$$

$$= 6 + \left(\frac{1}{\mathrm{F}_5}\right) + \left(\frac{3}{\mathrm{F}_5}\right) + \left(\frac{11}{\mathrm{F}_5}\right) + \left(\frac{31}{\mathrm{F}_5}\right) + \left(\frac{69}{\mathrm{F}_5}\right)$$

$$= 6 + \left(\frac{1}{\mathrm{F}_5}\right) + \left(\frac{3}{\mathrm{F}_5}\right) + \left(\frac{1}{\mathrm{F}_5}\right) + \left(\frac{1}{\mathrm{F}_5}\right) + \left(\frac{4}{\mathrm{F}_5}\right)$$

$$= 6 + 1 - 1 + 1 + 1 = 9$$

3.6. Theorem 3 (Hasse's Theorem)

Let E be an elliptic curve over the finite field F_q. Then the order of $\#E(\mathrm{F}_q)$ satisfies the following inequality.

$$|q + 1 - \#E(\mathrm{F}_q)| \leq 2\sqrt{q}$$

3.7. The Frobenius Endomorphism

The Frobenius Map is the function

$$T_p: E(\overline{\mathrm{F}_q}) \longrightarrow E(\overline{\mathrm{F}_q}),$$
$$\tau_p(x, y) = (x^p, y^p) \qquad (4)$$

The quality $a_p = p + 1 - \#E(\mathrm{F}_q)$ is called the Trace of Frobenius. [16]

What are rational solutions? This question is even more difficult in general. If the degree of the equation is higher than three, little is known. If the degree is exactly three, we have essentially an elliptic curve. [17]

3.8. Theorem 4 (Henri Poincare's Theorem, 1901)

Let E be an elliptic curve defined over a field K. Then $E(K)$ is an abelian group under +.

4. Conjecture 1 (Henri Poincare's Conjecture, 1901)

Let E be an elliptic curve. Then $E(\mathbb{Q})$ is finitely generated Mordell gave a good partial answer in 1923 (based on a conjecture of Henri Poincare in 1901), known as Mordell's Theorem. This result states that the group $E(\mathbb{Q})$ of rational points on an elliptic curve is "finitely generated". This means that, if there are any rational solutions, then they can all be determined from a certain finite subset of them.

Unfortunately, there are two things that Mordell's result does not do. First, it provides no way to tell whether any rational points exist (other than the "point at infinity"). Second, it does not provide an "effective" means (i.e. an algorithm) for finding a set of generators for the group of rational points. In some cases Mordell's methods are able to do this. And it has been conjectured, but not yet proven, that the methods will work in all cases. There is a general theorem about finitely generated abelian groups such as $E(\mathbb{Q})$. It states that any finitely generated abelian group is the "direct sum" of the subgroup consisting of elements of finite order and zero or more copies of the additive group $\mathbb{Z}$ of integers. [14]

4.1. Theorem 5 (Mordell Theorem)

If E is an elliptic curve over $\mathbb{Q}$, then the commutative group $E(\mathbb{Q})$ is finitely generated.

By Mordell's theorem we can write

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$$

Where r is a nonnegative integer and T is the Torsion subgroup of elements of finite order in $E(\mathbb{Q})$. This subgroup is called the torsion subgroup of $E(\mathbb{Q})$. The integer r is called the rank of E and is written rank (E).

Determining r theoretically and in practice is currently the main problem of arithmetic elliptic curve theory. As it happens, much more is known about the torsion part of the group $E(\mathbb{Q})$, denoted by T.

A theorem due to Elisabeth Lutz and Trygve Nagell in the 1930's showed how to compute T in any particular case. [1]

4.2. Torsion Subgroups

The torsion subgroup is "well-understood". First, there is an effective algorithm to determine T given E.

4.2.1. Theorem 6 (Nagell-Lutz)

Let E be the elliptic curve $y^2 = x^3 + Ax + B$. If $(x, y) \in T$ and Then $(x, y) \neq \infty$, then

1. $(x,y) \in \mathbb{Z}$
2. either $y = 0$ or y^2 divides $4A^3 + 27B^2$

4.2.2. Corollary 1

Let E bean elliptic curve defined over $\mathbb{Q}$. Then the torsion subgroup T is finite.

Proof: Suppose $E = (x, y) \in T$. By Lutz-Nagell, $y = 0$ or y^2 divides $4A^3 + 27B^2$ so there are only finitely many possibilities for y. Fixing y, there are at most 3 solutions to E in x, thus T is finite group.

4.2.3. Example 6

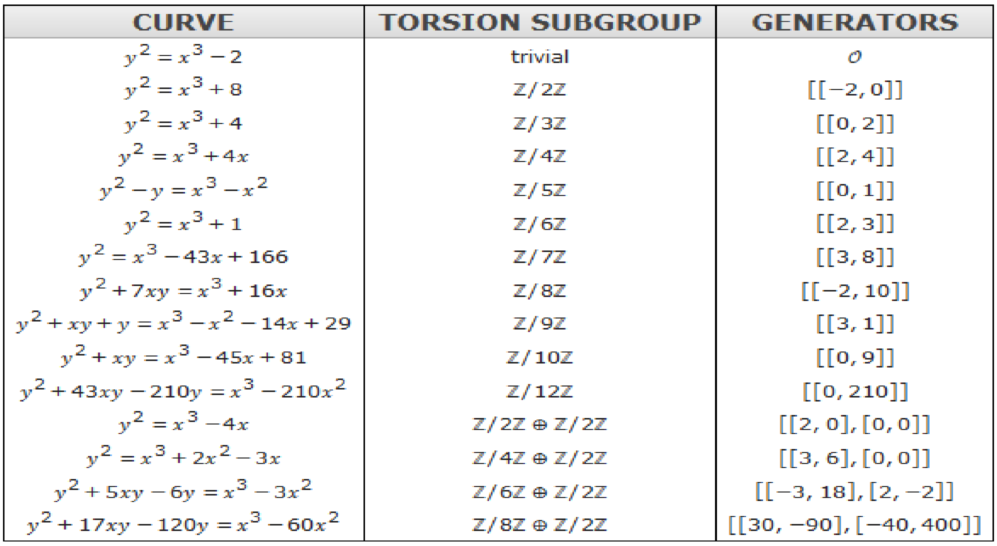
Let $y^2 = x^3 + 1$, then Torsion subgroup (T) are

1) (-1, 0) has order 2
2) (0,±1) has order 3
3) (2,±3) has order 6

4.2.4. Theorem 7 (Mazur Theorem)

If E is an elliptic curve, then T is one of the following 15 groups:

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



CURVE	TORSION SUBGROUP	GENERATORS
$y^2 = x^3 - 2$	trivial	$\emptyset$
$y^2 = x^3 + 8$	$Z/2Z$	[[−2, 0]]
$y^2 = x^3 + 4$	$Z/3Z$	[[0, 2]]
$y^2 = x^3 + 4x$	$Z/4Z$	[[2, 4]]
$y^2 - y = x^3 - x^2$	$Z/5Z$	[[0, 1]]
$y^2 = x^3 + 1$	$Z/6Z$	[[2, 3]]
$y^2 = x^3 - 43x + 166$	$Z/7Z$	[[3, 8]]
$y^2 + 7xy = x^3 + 16x$	$Z/8Z$	[[−2, 10]]
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$Z/9Z$	[[3, 1]]
$y^2 + xy = x^3 - 45x + 81$	$Z/10Z$	[[0, 9]]
$y^2 + 43xy - 210y = x^3 - 210x^2$	$Z/12Z$	[[0, 210]]
$y^2 = x^3 - 4x$	$Z/2Z \oplus Z/2Z$	[[2, 0], [0, 0]]
$y^2 = x^3 + 2x^2 - 3x$	$Z/4Z \oplus Z/2Z$	[[3, 6], [0, 0]]
$y^2 + 5xy - 6y = x^3 - 3x^2$	$Z/6Z \oplus Z/2Z$	[[−3, 18], [2, −2]]
$y^2 + 17xy - 120y = x^3 - 60x^2$	$Z/8Z \oplus Z/2Z$	[[30, −90], [−40, 400]]

Figure 3. Examples of torsion subgroups of elliptic curves [9]

Each of the groups in Theorem 6 occurs infinitely often as the torsion subgroup of an elliptic curve over $\mathbb{Q}$.

4.3. Ranks

The rank of an elliptic curve is a measure of the size of the set of rational points. There is no analogue of Theorems 12 or 14 for ranks:

- there is no known algorithm guaranteed to determine rank of E;
- it is not known exactly which integers can occur as the rank of an elliptic curve. [1]

4.4. Reduction of an Elliptic Curve Modulo p

Let E be an elliptic curve given by an equation

$E: y^2 = x^3 + Ax + B$ with $a, b \in \mathbb{Z}$. We can reduce the coefficients of E modulo a prime p to get an elliptic curve $\bar{E}$ with coefficients in F_p

$$E: y^2 = x^3 + \bar{A}x + \bar{B}$$

With $\bar{A}, \bar{B} \in \mathrm{F}_p$. However, remember we must check that $\bar{E}$ is not singular, which means that we need the discriminant

$$\bar{\Delta} = 4\bar{A}^3 + 27\bar{B}^2 \neq 0 \; in \; \mathrm{F}_p$$

We say that E has Good Reduction at p if p does not divide the discriminant $\Delta = 4A^3 + 27B^2$ and we say that E has Bad Reduction at $\boldsymbol{p}$ if p does divide the discriminant.

$\Delta = 4A^3 + 27B^2$. When we talk about reduction modulo p, we will generally assume that we have good reduction at P. [13]

4.5. The Reduction Modulo *p* Homomorphism

It is hard to overstate the importance of reduction modulo p. A first indication is:

4.6. Theorem 8

If E has good reduction, then the reduction modulo p map

$$E(\mathbb{Q}) \longrightarrow E(\mathrm{F}_p), P \longrightarrow \tilde{P},$$

is a group homomorphism.

4.7. Example 6

Let E be the elliptic curve

$$E : y^2 = x^3 + 2x + 4$$

Some points in are

$$P = (2, 4), Q = \left(\frac{1}{4}, \frac{17}{8}\right), P + Q = \left(\frac{-54}{49}, \frac{-232}{343}\right)$$

The reduction modulo 11 map

$$E(\mathbb{Q}) \longrightarrow E(\mathrm{F}_{11})$$

$$\widetilde{\mathrm{P}} = (2, 4)\, \widetilde{\mathrm{Q}} = (3, 9), \widetilde{\mathrm{P}} + \widetilde{\mathrm{Q}} = (9, 5) = \overline{\mathrm{P} + \mathrm{Q}}$$

5. The Birch and Swinnerton-Dyer Conjecture

Fix an elliptic curve $\mathrm{E} : \mathrm{y}^2 = \mathrm{x}^3 + \mathrm{Ax} + \mathrm{B}$ over $\mathbb{Q}$. For every prime number p not dividing the discriminant.

$\Delta = 4A^3 + 27B^2$ of E, we can reduce A and B modulo p and view E as an elliptic curve over the finite field F_p.

Reduction modulo P induces a group homomorphism.

$$E(\mathbb{Q}) \longrightarrow E(\mathrm{F}_p), P \longrightarrow \widetilde{\mathrm{P}},$$

The idea of Birch and Swinnerton-Dyer was that the large $E(\mathbb{Q})$ is, the larger $E(\mathrm{F}_p)$'s should be "on average" as p varies. The size of can be measured by rank of E, but how can one measure the average size of the $E(\mathrm{F}_p)$'s? [1]

5.1. What does $E(\mathrm{F}_p)$ look like?

The group $E(\mathrm{F}_p)$ is obviously a finite group. Indeed, it clearly has no more than $2p + 1$ points. For each $x \in \mathrm{F}_p$, there is a "50% chance" that the value of $f(x) = x^3 + Ax + B$ is a square in F_p. And if $f(x) = y^2$ is a square, then we (usually) get two points $(x, \pm y)$ in $E(\mathrm{F}_p)$. Plus there's the point at infinity ∞. Thus we might expect to contain approximately [13]

$$E(\mathrm{F}_p) \approx \frac{1}{2} \cdot 2 \cdot p + 1 = p + 1 \; points$$

A famous theorem of Hasse makes this precise.

5.2. Theorem 9 (Hasse's Theorem)

Let E be an elliptic curve

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

with $A, B \in \mathrm{F}_p$ .Then

$$\left|\#E(F_p) - p + 1\right| \leq 2\sqrt{p}$$

For every prime number p not dividing Δ .

Let $N_p = \#E(F_p)$.

5.2.1. Numerical experiments of the Birch and Swinnerton-Dyer

To test their idea, in the 1950's Birch and Swinnerton-Dyer computed

$$\prod_E (X) = \prod_{p \leq X, p' \Delta} \frac{Np}{p}$$

as x grows, for certain elliptic curves E.

Figure 2 shows the behaviour of $\prod_{E_d}(X)$ for x up to about 1.5×10^7 for five different curves

$$E_d : y^2 = x^3 - d^2 x .$$

The horizontal axis is $log \, log(x)$ and the vertical axis is $\log(\prod_{E_d}(X))$.

From their data Birch and Swinnerton-Dyer were led to conjecture that

$$\prod_E \sim C(log(X))^{rank \, (E)} \tag{5}$$

As $X \rightarrow \infty$ for some constant $\mathbb{C}$ depending only on E. (Note that this relation is consistent with the data in Figure 2. if the axes were to scale, then the slopes of the lines would be the ranks of the curves.) The function $\prod_E(X)$ does not behave very nicely and therefore is difficult to work with.

Birch and Swinnerton-Dyer stated a related conjecture, using the L-function of E in place of $\prod_E(X)$. [1]

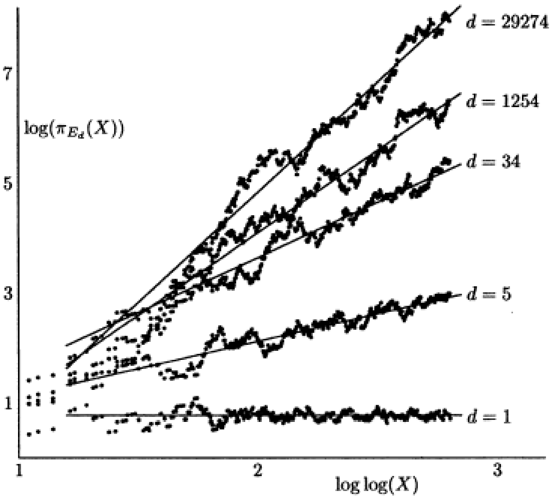


Figure 4. Birch and swinnerton-Dyer data for $y^2 = x^3 - d^2x$

5.3. The L-Series of an Elliptic Curve

Let $a_p = \#E(F_p) - p + 1$ Analogous to the Euler factors of the Riemann zeta function, we define the local L-factor of E to be

$$L(E,s) = (1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}})^{-1} \quad (6)$$

The variable s is a complex variable $s \in \mathbb{C}$.

When evaluating its value at s = 1, we retrieve the arithmetic information at p

$$L(E,1) = \frac{p}{p+1-a} = \frac{p}{\#E(\mathrm{F}_p)} \quad (7)$$

Notice that each point in $E(\mathbb{Q})$ reduces to a point in $E(\mathrm{F}_p)$. So when $E(\mathbb{Q})$ then $L(E,1)$ tends to be small. Birch and Swinnerton-Dyer observed that if $E(\mathbb{Q})$ is infinite, then the reduction of the points in $E(\mathbb{Q})$ tend to make $\#E(\mathrm{F}_p)$ large than usual. So they conjectured Birch and Swinnerton-Dyer did numerical experiments and suggested

$$L(E,1) = 0 \; if \; and \; only \; if \; \#E(\mathbb{Q}) \; is \; infinite.$$

The L-function of E is defined to be the product of all local L

$$L(E,1) = \prod_{p \nmid \Delta} \left(1 - \frac{a_p}{p} + \frac{1}{p}\right)^{-1} = \prod_{p \nmid \Delta} \frac{p}{\#E(\mathrm{F}_p)} \quad (8)$$

So intuitively the rank of $E(\mathbb{Q})$ will correspond to the value of *L(E, s)* at s=1: the larger r is, the "smaller" *L(E, 1)* is. However, the value of *L (E, s)* at s = 1 does not make sense since the product of *L (E, s)* only converges when R(s) > 3/2.

Nevertheless, if *L(E, s)* can be continued to an analytic function on the whole of $\mathbb{C}$, it may be reasonable to believe that the behavior of *L(E, s)* at s = 1 contains the arithmetic information of the rank of $E(\mathbb{Q})$.

A deep theorem of Wiles et al., which many consider the crowning achievement of 1990s number theory, implies that *L(E, s)* can be analytically continued to an analytic function on all $\mathbb{C}$. This implies that *L(E, s)* has a Taylor series expansion about s = 1. [12]

5.4. Theorem 10 (Wiles' Theorem)

The function *L(E, s)* extends to an analytic function on all of $\mathbb{C}$ and satisfies a function equation

$$\Lambda(s) = w_E \Lambda(2-s) \quad (9)$$

where $w_E = \pm 1$ and

$$\wedge\,(s) = N^{\frac{s}{2}}(2\pi)^{-1}\Gamma(s)L(E,s) \quad (10)$$

for some positive N(depending on E).

$$rank(E) = \begin{cases} even\; if\; w_E = +1 \\ odd\; if\; w_E = -1 \end{cases}$$

Where $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}\,dt$

5.5. Taylor expansion of L(E,s) about s = 1

$$L(E,s) = c_E(s-1)^r, c_E = \frac{1}{r!}L^{(r)}(E,1)$$

with $r = r_{an}$ the analytic rank

$$L(E,s) = c_0 + c_1(s-1) + c_2(s-1)^2 + \cdots$$

Define the analytic rank (r_{an}) of E to be the order of vanishing of *L (E, s)* as s = 1. [5]

The famous Birch and Swinnerton-Dyer conjecture asserts that Birch and Swinnerton-Dyer conjecture.

5.6. Conjecture 1

$ord_{s=1}L(E,s)\; the\; analytic\; rank\; o\; f\; E.$ The Birch and Swinnerton-Dyer Conjecture can then be stated simply as: for any elliptic curve E over $\mathbb{Q}$. Then the algebraic and analytic ranks of E are the same. Goldfeld also proved the following surprising result, which says in particular that, the connection between $\prod_E(X)$ and $L(E,s)$ is off by a factor of $\sqrt{2}$. [17]

5.7. Theorem 11. (Goldfled Theorem)

Suppose $\prod_E(X) \sim C(log(X))^r$ where $r = rank(E)$ with constants $C \in \mathbb{R}^+$ and $r \in \mathbb{R}$. Then $r = ord_{s=1}L(E,s)$ and $lim_{s\to 1}\frac{L(E,s)}{(s-1)^r} = \sqrt{2}e^{r\gamma}C^{-1}$.

Where γ Euler's constant. In particular, if *r = 0* then

$$L(E,s) = \sqrt{2}\left(\prod_{p \nmid \Delta} \frac{p}{\#E(\mathrm{F}_p)}\right)$$

The lines $log(c) + rloglog(X)\; in$ figure 2 were calculated using equation 5, Theorem 11, and the full Birch and Swinnerton-Dyer Conjecture to determine C and r.

5.8. Theorem 12

Suppose E is an elliptic curve over $\mathbb{Q}$ and that $r_{an} \leq 1$. Then the algebraic and analytic ranks of E are the same.

A quote from William A. Stein:

In 2000, Conjecture 1 was declared a million dollar millennium prize problem by the Clay Mathematics Institute, which motivated even more work, conferences, etc., on the conjecture. Since then, to the best of my knowledge, not a single new result directly about Conjecture 1 has been proved. The class of curves for which we know the conjecture is still the set of curves over $\mathbb{Q}$ with $r_{an} \leq 1$, along with a finite set of individual curves on which further computer calculations have been performed (by Cremona, Watkins, myself, and others).

"A new idea is needed".

Nick Katz on BSD, at a 2001 Arizona Winter School.

The following theorem, a combination of work of Kolyvagin, Gross and Zagier, and others, is the best result to date in the direction of the Birch and Swinnerton-Dyer Conjecture. [17]

5.9. Theorem 13 (Gross-Zagier, Kolyvagin Theorem)

(i) $rankan(E) = 0 \Rightarrow rank(E) = 0,$

(ii) $rankan(E) = 1 \Rightarrow rank(E) = 1$

Assertion (i) can be rephrase as "$L(E,1) \neq 0 \Rightarrow E(\mathbb{Q})$ is finite"Assertion (ii) can be rephrase as "$L(E,1) = 0$ and $L^{'}(E,s) \neq 0,$ then r = 1, and there is an efficient method for calculating $E(\mathbb{Q})$.

The case $rankan(E) \geq 2,$ remains completely open problem.

5.9.1. Example 23

If E is the curve $y^2 = x^3 - x$, then

$$L(E,1) = 0.65551438857302995 \neq 0$$

Thus theorem 22 (i) shows that $E(\mathbb{Q})$ is finite.

The sign w_E in the functional equation for $L(E,s)$ determines the parity of $rankan(E)$:

$$rank(E) = \begin{cases} even\ if\ w_E = +1 \\ odd\ if\ w_E = -1 \end{cases}$$

The Birch and Swinnerton-Dyer Conjecture predicts in particular that *rank(E)* and *rankan(E)* have the same parity, so the following is a consequence of the Birch and Swinnerton-Dyer Conjecture.

5.10. Conjecture 2. (Parity Conjecture)

$$rank(E) = \begin{cases} even\ if\ w_E = +1 \\ odd\ if\ w_E = -1 \end{cases}$$

To explain the recent progress concerning the Parity Conjecture, we need to introduce the Tate-Shafarevich group and the Selmer group. The Tate-Shafarevich group III_E is a torsion group that measures the failure of the Hasse's Principle for curves that is principal homogeneous spaces for E.

5.11. Conjecture 3 (Birch and Swinnerton-Dyer)

Let E be an elliptic curve over $\mathbb{Q}$ of rank r. Then $r = ord_{s=1}L(E,s)$ and

$$\frac{1}{r!}L^{(r)}(E,r) = \frac{w_E.Reg(E).\#.\prod_p}{\#E(\mathbb{Q})^2_{t0r}}$$

And another quote from Bertolini-Darmon (2001):

"The following question stands as the ultimate challenge concerning the Birch and Swinnerton-Dyer conjecture for elliptic curves over $\mathbb{Q}$: Provide evidence for the Birch and Swinnerton-Dyer conjecture in cases where $\mathrm{ord}_{s=1}\mathrm{L(E,s)} > 1$". [17]

6. Conclusions

In conclusion, although there has been little success in the last fifty years in finding the number of rational points on an elliptic curve, there are still almost no methods for finding such points. It is to be hoped that a proof of the Birch and Swinnerton-Dyer conjecture will give some insight on the number of rational points on an elliptic curve.

ACKNOWLEDGEMENTS

The authors thank the staff at the Mathematics Department of Kwame Nkrumah University of Science and Technology for their support and kindness during the period this paper was written.

REFERENCES

[1] R. Karl and S. Alice. Rank of Elliptic Curves. American Mathematical Society Pages 455474 S 0273-0979(02) 00952-7, 2002, Vol.39, No.4. http://dx.doi.org/10.1090/s0273-0979-02-00952-7.

[2] J. H. Silverman. The Arithmetic of Elliptic Curves. New York: Springer, 2009. Print. http://dx.doi.org/10.1007/978-0-387-09494-6.

[3] J. Coates, A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. Swinnerton-Dyer, Invent. Math. 1977, 39, 223-251 http://dx.doi.org/10.1007/bf01402975.

[4] B. Gross, D. Zagier .Heegner Points and Derivatives of L-series. n vent. Math. 84, 1986, pp. 225-320 http://dx.doi.org/10.1007/bf01388809.

[5] J. Cremona. Algorithms for Modular Elliptic Curves, Cambridge: Cambridge University Press. 1992 http://dx.doi.org/10.2307/3618360

[6] L. Washington. Number Theory and Cryptography. Chapman and Hall/CRC, 2003. An introduction to elliptic curves and ECC at an advanced undergraduate/beginning graduate level. http://dx.doi.org/10.5860/choice.41-4097.

[7] J. Conway. Functions of One Complex Variable I. Springer, 1986. ISBN 0-387-90328-3. http://dx.doi.org/10.1007/978-1-4612-6313-5.

[8] Alozano, Examples of torsion subgroups of elliptic curves [Online]. Available: 2013-02-02. From http:// www.planetmath.org.

[9] A. Wiles, the Birch and Swinnerton-Dyer conjecture. [Online]. Available http://www.claymath.org/prize problems /birchsd.htm.

[10] J. B. Fraleigh. A first course in abstract algebra. 5th edition, Addison- Wesley. 1994 http://dx.doi.org/10.2307/3617251.

[11] J. H. Silverman. The arithmetic of elliptic curves. Graduate Texts in Mathematics, 106.Springer-Verlag, New York, 1986. [The number theory of elliptic curves at a level suitable for advanced graduate students.]. http://dx.doi.org/10.1007/978-1-4757-1920-8.

[12] M. England, Elliptic curve cryptography. Heriot-Watt University. Summer 2006.

[13] J. H. Silverman, An Introduction to the Theory of Elliptic Curves. Summer School on Computational Number Theory and Applications to Cryptography University of Wyoming June 19 -July 7.

[14] C. Daney.Elliptic Curves and Modular Forms. Retrieved 2015-01-13 from http://www.openquestions.com/oq-main.htm,2002.

[15] Z. DeStefano,. 2010. On the Torsion Subgroup of an Elliptic Curve Retrieved 2015-02-13 from http://wwwmath.nyu.edu/degree/undergrad/ug research/presentation2.pdf, S.U.R.E Presentation.

[16] E. H. Goins, Why Should I Care About Elliptic Curves Department of Mathematics, Purdue University MAA Math Fest, and Retrieved 2015-01-13 from http://www.math.buffalo.edu/mad/PEEPS/blackwell david.htlm.

[17] W. Stein. The Birch and Swinnerton-Dyer Conjecture, a Computational Approach. Retrieved 2015-01-13 from http://www.wstein.org/books/modform/stein-modform.pdf.