INTRODUCTION TO THE CONJECTURES OF BIRCH AND SWINNERTON-DYER.

SUDHANSHU SHEKHAR AND R. SUJATHA

Introduction. The aim of this article is to introduce the Birch and Swinnerton-Dyer conjectures in its entirety. One part of these conjectures predicts the equality of two different 'ranks' associated to an elliptic curve defined over a number field. These are the so called algebraic and analytic ranks. The other part of the conjectures is an exact formula expressing the leading coefficient of a certain power series associated to the elliptic curve in terms of various important and mysterious arithmetic invariants. The approach we shall take is to define and provide a brief introduction to these arithmetic invariants, thereby providing a compact introduction to this conjecture. We omit the details, referring the interested reader to Silverman's book [Si]. Other excellent references to the theme of this article are [D], [W1]. We stress that this is an expository article and is based on the lectures given at the conferences on the 'Theoretical and Computational Aspects of the BSD Conjectures' held at BICMR in December 2014.

Weierstrass equation of elliptic curves. An elliptic curve over a field K is a projective non-singular curve of genus one defined over K with a specified base point (see [Si, Chapter I, section 2] and [Si, Chapter II, section 5]). Recall that any such curve E has a (Weierstrass) equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1}$$

in $\mathbb{P}^2$, the projective space of dimension two with $a_1 \cdots a_6 \in K$ for $1 \leq i \leq 6$. Here, $O = [0, 1, 0]$ is the base point (called "the point at infinity"). By dehomogenising (i.e taking $x = X/Z$ and $y = Y/Z$) the above equation can be expressed as

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2}$$

Thus $E \subset \mathbb{P}^2$ consists of the points $P = (x, y)$ satisfying the above Weierstrass equation along with the base point O. If $Char(K) \neq 2$, then we can simplify the equation by the change of coordinate

$$y \mapsto 1/2(y - a_1x - a_3)$$

which gives an equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = f(x),$$

where

$$b_2 = a_1^2 + 4a_4,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6.$$

Associated to the above equation, we define the following quantities,

$$\begin{aligned}
&b_8 = a_1^2a_6 + 4a_2a_6 - a_2a_3^2 - a_4^2,\\
&c_4 = b_2^2 - 2b_4,\\
&c_6 = -b_2^3 + 36b_2b_4 - 216b_6,\\
&\Delta == b_2^2b_8 - 8b_4^3 + 9b_2b_4b_6,\\
&j = c_4^3/\Delta,\\
&\omega = dx/(2y + a_1x + a_3) = dy/(3x^2 + 2a_2x + a_4 - a_1y).
\end{aligned}$$

An easy verification shows that,

$$4b_8 = b_2b_6 - b_4^2 \text{ and } 1728\Delta = c_4^3 - c_6^2.$$

If $Char(K)$ is different from 2 and 3, then using the change of coordinates

$$(x, y) \mapsto (x - 3b_2/36, y/108)$$

equation (2) can further be expressed as

$$y^2 = x^3 - 27c_4x - 54c_6.$$

Substituting $A = 27c_4$ and $B = -54c_6$ we get the equation

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

called *short Weierstrass form* with $\Delta = -16(4A^3 + 27B^2)$. The quantity $\Delta \in K$ is an important invariant associated to the curve E, called the *discriminant* of E over K. Further, the non-singularity of E implies that $\Delta \neq 0$ and the cubic $f(x)$ has distinct roots. The quantity j is called the $j - invariant$ of the elliptic curve, and ω is the $invariant\ differential$ associated to the Weierstrass equation.

For a field extension L/K we define the set

$$E(L) := \{(x, y) \in L^2 | y^2 + a_1xy + a_3y = f(x)\} \cup \{O\}.$$

It is well known that for any field extension L/K there exists an abelian group structure on $E(L)$ such that

(1) O is the identity element with respect to this group structure.
(2) If $\phi_{L_1,L_2} : L_1 \longrightarrow L_2$ is a homomorphism of field extensions of K then there exists a corresponding group homomorphism $E(L_1) \overset{\phi^\star_{L_1,L_2}}{\longrightarrow} E(L_2)$ defined as $\phi^\star_{L_1,L_2}(x, y) = (\phi_{L_1,L_2}(x), \phi_{L_1,L_2}(y))$ satisfying $\phi^\star_{L_1,L_2}\phi^\star_{K,L_2} = \phi^\star_{K,L_2}$.

In particular, if L/K is a Galois extension then $E(L)$ is a Gal(L/K)-module. It is a well known and basic fact that the group operation in the group $E(K)$ can be explicitly described the chord and tangent method (see [ST, Chapter I]).

Elliptic curves over the complex numbers.

Definition 1. *A lattice in the complex numbers $\mathbb{C}$ is a discrete group of the form $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, where ω_1 and ω_2 are linearly independent over the real numbers $\mathbb{R}$. Two lattices Λ and Λ' are said to be equivalent if there exists $\lambda \in \mathbb{C} - \{0\}$ with $\lambda\Lambda = \Lambda'$. A complex torus T is a quotient $\mathbb{C}/\Lambda$ of the complex plane $\mathbb{C}$ by a lattice with projection denoted by $p : \mathbb{C} \longrightarrow T = \mathbb{C}/\Lambda$.*

Remark 2. *If $\lambda \in \mathbb{C} - \{0\}$ such that $\lambda\Lambda \subset \Lambda'$ for lattices Λ and Λ' then it induces a homomorphism $\lambda : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$. Such a map is called a homothety induced by λ. A homothety $\lambda : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ is an isomorphism if $\lambda\Lambda = \Lambda'$. In fact, it can be shown that every complex analytic isomorphism between two tori is associated to a homothety.*

Definition 3. *An elliptic function f with respect to a lattice Λ is a meromorphic function on $\mathbb{C}$ such that $f(z+w) = f(z)$ for all $z \in \mathbb{C}$ and $w \in \Lambda$.*

The *Weierstrass $\wp$-function* associated to a lattice Λ is given by the infinite sum

$$\wp(z;\Lambda) = \wp(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} [\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}]. \tag{3}$$

The *Eisenstein series* of weight $2k$ associated to a lattice Λ is the series

$$G_{2k} = G_{2k}(\Lambda) = \sum_{\omega \in \Lambda - \{0\}} \omega^{-2k}. \tag{4}$$

Theorem 4. *(*[Si, Theorem 3.1, Theorem 3.5, Chapter VI.3]*)*
(a) The Eisenstein series $G_{2k}(\Lambda)$ is absolutely convergent for all $k > 1$.
(b) The series defining the Weierstrass $\wp$-function converges absolutely and uniformly on every compact subset of $\mathbb{C}\backslash\Lambda$. The series defines a meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles.
(c) The Weierstrass $\wp$-function is an even elliptic function.

The Laurent series for $\wp(z;\Lambda)$ around $z = 0$ is given by

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2}(\Lambda) z^{2k}.$$

Furthermore, we have

$$\begin{aligned}
\wp(z;\Lambda) &= \frac{1}{z^2} + 3G_2(\Lambda)z^2 + 5G_3(\Lambda)z^4 + \cdots \\
\wp'(z;\Lambda) &= \frac{-2}{z^3} + 6G_2(\Lambda)z + 20G_3(\Lambda)z^3 + \cdots \\
\wp'(z;\Lambda)^2 &= \frac{4}{z^6} - \frac{24G_2(\Lambda)}{z^2} - 80G_3(\Lambda) + \cdots \\
4\wp(z;\Lambda)^3 &= 4\wp(z;\Lambda)(\frac{1}{z^4} + 6G_2(\Lambda) + 10G_3(\Lambda)z^2 + \cdots) \\
60G_2(\Lambda)\wp(z;\Lambda) &= \frac{60G_2(\Lambda)}{z^2} + 180G_2^2(\Lambda)z^2 + \cdots .
\end{aligned}$$

Comparing the first few terms of the above expressions, one sees that for all $z \in \mathbb{C} \setminus \Lambda$, the Weierstrass $\wp$-function and its derivative satisfy the relation

$$\wp'(z;\Lambda)^2 = 4\wp(z;\Lambda)^3 - 60G_2\wp(z;\Lambda) - 140G_3(\Lambda)$$

Put $g_2 = g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3 = g_3(\Lambda) = 140G_6(\Lambda)$.

Proposition 5. *(*[Si, Proposition 3.6]*) Let $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$ be the quantities associated to a lattice $\Lambda \subset \mathbb{C}$ as above.*
(a) The polynomial

$$f(x) = 4x^3 - g_2 x - g_3$$

has distinct roots, so its discriminant

$$\Delta(\Lambda) = g_2^3 - 27g_3^3$$

is non-zero.
(b) Let $E/\mathbb{C}$ be the curve $E : 4x^3 - g_2 x - g_3$ which from (a) is an elliptic curve. Then the map

$$\phi : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}), \quad z \mapsto [\wp(z), \wp'(z), 1],$$

is a complex analytic isomorphism of complex Lie groups, i.e. it is an isomorphism of Riemann surfaces which is also a group homomorphism.

Corollary 6. *$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.*

Corollary 7. *Let E_1 and E_2 be two elliptic curves corresponding to lattices Λ_1 and Λ_2 as in the above proposition. Then E_1 and E_2 are isomorphic over $\mathbb{C}$ if and only if Λ_1 and Λ_2 are homothetic.*

An important theorem in the theory of elliptic curves over $\mathbb{C}$ is the $Unifomization$ *Theorem* which says that every elliptic curve E defined over $\mathbb{C}$ corresponds to a lattice Λ_E as in the above proposition, i.e. there exists a lattice Λ_E uniquely determined up to homothety such that

$$\phi : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \quad \phi(z) = [\wp(z,\Lambda), \wp'(z,\Lambda), 1]$$

is an isomorphism of complex Lie groups and E has a Weierstrass equation given by

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$

The lattice Λ_E for an elliptic curve E given by a Weierstrass equation as in (2) is in fact the set of periods

$$\int_\gamma \omega_E$$

where γ runs over all closed paths in $E(\mathbb{C})$ and ω_E is the associated invariant differential $\frac{dx}{2y+a_1x+a_3}$. Equivalently, Λ_E is the image under the homomorphism

$$H_1(E(\mathbb{C}), \mathbb{Z}) \longrightarrow \mathbb{C}$$

$$\gamma \mapsto \int_\gamma \omega_E$$

where $H_1(E(\mathbb{C}), \mathbb{Z})$ denotes the homology group of $E(\mathbb{C})$ with coefficients in $\mathbb{Z}$. The lattice Λ_E is also called the *period lattice* associated to the curve E. A generating set for Λ_E can be obtained by integrating ω_E over a basis $\{\gamma_1, \gamma_2\}$ of $H_1(E(\mathbb{C}), \mathbb{Z})$ (see [Si, Chapter VI,Proposition 5.2] for more details).

Elliptic curves over local fields. Let K be a perfect local field, complete with respect to a discrete valuation v and R be the ring of integers of K. Let $\mathfrak{m}$ be the maximal ideal of R, π be a uniformizer of K, i.e, a generator of $\mathfrak{m}$ and denote the residue field of R at $\mathfrak{m}$ by k. Further, we normalize the valuation v such that $v(\pi) = 1$.

Let E/K be an elliptic curve, and let

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5}$$

be a Weierstrass equation for E/K. By substituting $(x, y) \mapsto (\pi^{-t^2}x, \pi^{-t^3}y)$ for a sufficiently large integer t, we may assume that the $v(a_i) \geq 0$ for the coefficients a_i as in equation 5. In particular, this implies that the valuation $v(\Delta)$ of the discriminant Δ associated to the above equation is ≥ 0. Further, since v is discrete, we can choose a Weierstrass equation defined over R which minimizes the value $v(\Delta)$. Such a Weierstrass equation of E is called a *minimal* (*Weierstrass*) *equation* for E. The minimal value of $v(\Delta)$ is called the *minimal discriminant* of E at v.

Proposition 8. *(*[Si, Proposition 1.3, Chapter VII]*) (a) Every elliptic curve E/K has a minimal Weirstrass equation unique up to a change of coordinates*

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t$$

with $u \in R^\times$ and $r, s, t \in R$.
(b) The invariant differential,

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

associated to a minimal equation is unique up to multiplication by an element of $R^\times$.

Given a minimal Weierstrass equation of the form (5), we can reduce its coefficients modulo π to obtain a curve over the residue field k given by

$$\tilde{E} : y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6} \tag{6}$$

The curve $\tilde{E}$ is called the *reduction of E modulo π*. The restriction of the reduction map from

$$\mathbb{P}^2(K) \longrightarrow \mathbb{P}^2(k)$$

induces a map

$$E(K) \longrightarrow \tilde{E}(k)$$

which is again called *reduction map.* If the curve $\tilde{E}$ is non singular, then E is said to have *good reduction* over K, otherwise E is said to have *bad reduction* over K. Let $\tilde{E}_{ns}(k)$ denote the set of non singular points of $\tilde{E}(k)$. In particular, if E has good reduction over K then $\tilde{E}(k) = \tilde{E}_{ns}(k)$. If $\tilde{E}$ has bad reduction over K then the following situations occur:
(i) If $\tilde{E}$ is a cuspidal cubic and $\tilde{E}_{ns} \cong \mathbb{G}_a$, then E is said to have *additive reduction over K.*
(ii) If $\tilde{E}$ is a nodal cubic and $\tilde{E}_{ns} \cong \mathbb{G}_m$, then E is said to have *multiplicative reduction.* Two further sub-cases occur in this situation which we mention now.

If the tangent directions at the node of $\tilde{E}$ are defined over k then E is said to have *split multiplicative reduction over K*, otherwise it has *non-split multiplicative reduction over K.*

Put

$$E_0(K) = \{P \in E(K) | \tilde{P} \in \tilde{E}_{ns}(k)\}$$
$$E_1(K) = \{P \in E(K) | \tilde{P} = O\}$$

Proposition 9. *Each of the sets $E_0(K)$, $E_1(K)$ and $\tilde{E}_{ns}(k)$ have a group structure such that $E_0(K)$ and $E_1(K)$ are subgroups of $E(K)$. Further, we have an exact sequence*

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \tilde{E}_{ns}(k) \longrightarrow 0,$$

in which the right hand map is the reduction map modulo π.

Definition 10. *The Tamagawa number of E over K is defined as the index $c_K(E) := [E(K) : E_0(K)]$.*

Theorem 11 (Kodaira, Néron)**.** *Let E/K be an elliptic curve. If E has split multiplicative reduction over K, then $E(K)/E_0(K)$ is a cyclic group of order $v(\Delta) = -v(j)$. In all other cases, the group $E(K)/E_0(K)$ is finite and has order at most* 4.

If E has split multiplicative reduction over K then by a theorem of Tate

$$E(K) \cong K^\times / q_E^{\mathbb{Z}}$$

where q_E is called the *Tate period* of E over K, and is related to the j-invariant of E via the equation $j(E) = J(q_E) = q_E^{-1} + 744 + 196884 q_E + 21493760 q_E^2 + \cdots$. Here, J denotes the modular J-function (see [T] for more details). In this case the Tamagawa number $c_K(E) = ord_v(q_E)$. If E has good reduction over K then $c_K(E) = 1$.

Elliptic curves over number fields. If K is number field and E/K is an elliptic curve then we have the following celebrated result that goes under the name of "Mordell-Weil theorem"(see [Si, Chapter VIII]).

Theorem 12. *If K is a number field and E/K is an elliptic curve defined over K, then $E(K)$ is a finitely generated as an abelian group.*

In particular

$$E(K) \cong \mathbb{Z}^{r_K(E)} \oplus E(K)_{tor}.$$

Here, $r_K(E)$ is called the *rank* of E/K and $E(K)_{tor}$ is the (finite) torsion subgroup of $E(K)$.

For an archimedean prime v of K let k_v denote the residue field at v. We say that E has good (resp. bad) reduction at v if E has good (resp. bad) reduction over the completion of K at v. For an archimedean prime v, we define an integer

$$a_v(E) := q_v + 1 - \#\tilde{E}(k_v)$$

where q_v is the number of elements in the finite field k_v.

Definition 13. *The local L-factor of the Hasse-Weil L-function of E at v is the polynomial defined as*

$$L_v(E/K,T) = \begin{cases} 1 - a_v(E)T + q_vT^2 & \text{if } E \text{ has good reduction at } v \\ 1-T & \text{if } E \text{ has split multiplicative reduction at } v \\ 1+T & \text{if } E \text{ has non-split multiplicative reduction at } v \\ 1 & \text{if } E \text{ has additive reduction at } v. \end{cases}$$

The Hasse-Weil L-function of E over K has the Euler product expansion

$$L(E/K,s) = \prod_v L_v(E/K, q_v^{-s})^{-1} \quad \text{for } Re(s) >> 0$$

where the product varies over all non-archimedean primes of K.

By a theorem of Hasse, if v is a prime of E/K of good reduction and

$$1 - a_v(E)T + q_vT^2 = (1-\alpha T)(1-\beta T)$$

then $|\alpha| = |\beta| = \sqrt{q_v}$, where $|\ \ |$ denotes the complex norm. Thus, $|a_v(E)| \leq 2\sqrt{q}$. This, in particular implies that the the above Euler product converges in the right half plane $Re(s) \geq 3/2$.

Conjecture 1. *For an elliptic curve E over a number field K, the Hasse-Weil L-function of E has an analytic continuation to the entire complex plane $\mathbb{C}$.*

As a consequence of the Modularity theorem proved by Wiles *et.al.* and the theory of base change for automorphic representations of $GL(2)$, we have the following deep

Theorem 14. *Let E be an elliptic curve defined over $\mathbb{Q}$ and K be a solvable Galois extension of $\mathbb{Q}$. Then the Hasse-Weil L-function $L(E/K,s)$ has an analytic continuation to the entire complex plane.*

The order of vanishing of $L(E/K,s)$ at $s=1$ is called the *analytic rank* of E over K.

Now, consider an elliptic curve E defined over a number field K. If the class number of K is one, then it is possible to find a Weierstrass equation which is simultaneously minimal at all non-archimedean primes of K. Such an equation is called a *global Weierstrass minimal equation* of E. Suppose that

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x_2 + a_4x + a_6$$

is a global Weierstrass minimal equation of E over K. Then, the *real period* of E is defined as

$$\Omega_{E/K} := \int_{E(\mathbb{R})} \frac{dx}{2y + a_1x + a_3} \in \mathbb{R}$$

Note that by $\Omega_{E/K} \in \Lambda_E$ where Λ_E is the period lattice associated to E. If we assume Conjecture 1, then we have a uniformly convergent power series expansion of $L(E/K,s)$ around the point 1 in $\mathbb{C}$. We shall see later that the real period of E associated to a global Weierstrass minimal equation appears in the formula for the leading term of this power series expansion. If K has positive class number, then the global minimal Weierstrass minimal equation may not exist (see [Si, VIII, Corollary 8.3]). In this case, the real period is defined by integrating a suitably chosen differential on the Néron model of E over K called the Néron differential of E. We will not describe the Néron model of E in this exposition and refer the reader to [BLR]. We remark in passing that the theory of periods is profound in itself, a full exposition of which would require delving into cohomology theories and principles of algebraic geometry.

Height function on Elliptic curves. Fix an algebraic closure $\bar{K}$ of a number field K. For a projective n-space $\mathbb{P}^n$, the absolute *logarithmic height* $H : \mathbb{P}^n(\bar{K}) \longrightarrow [0, \infty)$ is the function

$$H([x_0, \cdots, x_n]) = \sum_{all\ places\ v} (max\{\log |x_0|_v, \cdots, \log |x_n|_v\})$$

where $| - |_v$ is the absolute value at v normalized so that $\prod_v |x|_v = 1$ for all $x \neq 0$ in K. It can be easily checked that H is well defined. For an elliptic curve E defined over K by the Weierstrass equation

$$y^2 = x^3 + ax^2 + bx + c,$$

consider the morphism of projective spaces $f : E(\bar{K}) \longrightarrow \mathbb{P}^1(\bar{K})$ given by $f([x : y : 1]) = [x : 1]$ and $f([0 : 1 : 0]) = [0 : 1]$. The naïve height on $E(\bar{K})$ is the function defined by

$$h : E(\bar{K}) \longrightarrow [0, \infty)$$
$$h(P) = H_1(f(P)).$$

Finally, the *canonical height* (also called Néron-Tate height) is the function $\hat{h} : E(K) \longrightarrow [0, \infty)$ defined by the formula

$$\hat{h}(P) := \lim_{n\to\infty} 4^{-n} h([2^n]P).$$

Theorem 15. *(Néron, Tate) Let E/K be an elliptic curve and $\hat{h}$ be the canonical height on E.*
(a) $\hat{h}(P) = (1/2)h(P) + O(1)$ for all $P \in E(\bar{K})$.
(b) $\hat{h}(P) = 0$ if and only if P is a torsion point.
(c) The canonical height $\hat{h}$ is a quadratic form on $E(\bar{K})$, i.e. $\hat{h}$ is an even function, and the pairing

$$< \cdot, \cdot >: E(\bar{K}) \times E(\bar{K}) \longrightarrow \mathbb{R}$$
$$< P, Q >= \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)$$

is bilinear.
(d) For all $P \in E(\bar{K})$ and all $m \in \mathbb{Z}$,

$$\hat{h}([m]P) = m^2 \hat{h}(P).$$

(e) For all $P, Q \in E(\bar{K})$, $\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q)$
(f) The canonical height $\hat{h}$ extends to a positive definite quadratic form on the vector space $E(K) \otimes \mathbb{R}$.
(d) Any function $E(K) \longrightarrow \mathbb{R}$ which satisfy (a) and (d) is equal to the canonical height function $\hat{h}$.

We remark that the above properties of the canonical height function are crucially used in the proof of the Mordell-Weil Theorem (see [Si, Chapter VIII]).

Definition 16. *The Néron-Tate height pairing on $E(K)$ is the bilinear form*

$$< P, Q >_{NT} = (\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)) \text{ for all } P, Q \in E(K).$$

The elliptic regulator of E over K is defined by

$$Reg_K(E) := det(< P_i, P_j >_{NT})_{1 \leq i,j \leq r_K(E)}$$

where $P_i, \cdots, P_{r_K(E)}$ is a basis for $E(K)/E(K)_{tor}$.

As a consequence of Theorem 15(f), we have the following

Corollary 17. *The elliptic regulator $Reg_K(E) > 0$.*

Selmer group and Tate-Shafarevich group of elliptic curves. In this section, we discuss the Galois cohomology of elliptic curves and define the Tate-Shafarevich group which is an important invariant associated to an elliptic curve defined over a number field. It is conjectured to be finite and its size appears in the exact formula for the leading term of the power series expansion of the associated Hasse-Weil L-function as predicted by BSD conjectures which is discussed below.

For a field K and a discrete module A over the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ of K, let $H^i(K, A)$ denote the i-th Galois cohomology group of A. Let E be an elliptic curve defined over K. The absolute Galois group of K acts continuously on the discrete group $E(\bar{K})$ (resp. $E(\bar{K})_{tor}$). Now, suppose that K is a number field and let E be an elliptic curve defined over K. We denote by E_{tor} the Galois module $E(\bar{K})_{tor}$. For every prime v of K, we have a natural restriction map from $H^1(K, E_{tor}) \longrightarrow H^1(K_v, E(\bar{K})$ induced by the inclusion $E_{tor} \hookrightarrow E(\bar{K}_v)$. The Selmer group $\mathrm{Sel}(E/K)$ of E over K is defined as

$$\mathrm{Sel}(E/K) := Ker(H^1(K, E_{tor}) \longrightarrow \prod_v H^1(K_v, E(\bar{K}_v))$$

and the Tate-Shafarevich group denoted by Ш(E/K), is defined as

$$Ш(E/K) := Ker(H^1(K, E(\bar{K})) \longrightarrow \prod_v H^1(K_v, E(\bar{K}_v))$$

where, v varies over the set of primes of K. Using the fact that $E(\bar{K})$ is divisible, for every positive integer m, we get the exact sequence

$$0 \longrightarrow E(\bar{K})[m] \longrightarrow E(\bar{K}) \xrightarrow{\times m} E(\bar{K}) \longrightarrow 0.$$

From the associated long exact sequence of Galois cohomology for every positive integer m, we have the exact sequence

$$0 \longrightarrow E(K)/mE(K) \longrightarrow H^1(K, E(\bar{K})[m]) \longrightarrow H^1(K, E(\bar{K})[n].$$

Since,

$$\varinjlim_m H^1(K, E(\bar{K})[m]) = H^1(K, E(\bar{K})_{tor}),$$

taking the direct limit over integers m we have an exact sequence,

$$0 \longrightarrow E(K) \otimes \mathbb{Q}/\mathbb{Z} \longrightarrow H^1(K, E(\bar{K})_{tor}) \longrightarrow H^1(K, E(\bar{K})) \longrightarrow 0.$$

Using this exact sequence and snake lemma we get that the sequence

$$0 \longrightarrow E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}(E/K) \longrightarrow Ш(E/K) \longrightarrow 0.$$

is exact.

Proposition 18. *For a prime number p let $\mathrm{Sel}_p(E/K)$ denote the p-primary part of $\mathrm{Sel}(E/K)$. Then for any number field K and elliptic curve E defined over K we have that*

$$\mathrm{Sel}_p(E/K) \cong (\mathbb{Q}/\mathbb{Z})^{s_p(E/K)} \oplus \ Fin,$$

where, Fin is a finite p-group. The number $s_p(E/K)$ is called the p-Selmer rank of E over K.

The conjectures of Birch and Swinnerton-Dyer (BSD). We are now ready to state the Birch and Swinnerton-Dyer conjectures as formulated by Birch and Swinnerton-Dyer following extensive numerical calculations that they made in the 1960's (see [BS], [B]).

Conjecture 2. *(Birch, Swinnerton-Dyer) For a number field K and an elliptic curve defined over K,*
(a) $order_{s=1}L(E/K,s) = r_K(E)$.
(b) The Tate-Shararevich group $Ш(E/K)$ is finite. In particular, $s_p(E/K) = r_K(E)$ for all prime p.
(c)

$$\lim_{s\longrightarrow 1}\frac{L(E/K,s)}{(s-1)^{r_K(E)}} = \frac{\Omega_{E/K} \times Reg_K(E) \times \#Ш(E/K)\prod_{v<\infty} C_{K_v}(E)}{\sqrt{|disc_K|} \times (\#E(K)_{tor})^2}$$

where $|disc_K|$ denotes modulus of the discriminant of the field K over $\mathbb{Q}$.

Conjecture 2(a) is known as the weak BSD conjecture and 2(b) and 2(c) together are know as the strong form of the BSD conjectures. Conjecture 2(c) is also called as the BSD exact formula. The BSD conjectures have been proved in some special cases due to work of Coates-Wiles, Gross-Zagier, Kolyvagin, Rubin and others. We mention that Iwasawa theory and the theory of Euler systems have proved to be effective tools in attacking the BSD conjectures. In 1977, Coates and Wiles proved the following theorem,

Theorem 19 (Coates-Wiles)**.** *If E is an elliptic curve defined over $\mathbb{Q}$ or a quadratic imaginary extension K of $\mathbb{Q}$, E has complex multiplication by K and $L(E/K,s)$ is non-zero at 1, then $E(K)$ is finite.*

In 1989 Kolyvagin used the notion of Euler systems to prove the following theorem.

Theorem 20 (Kolyvagin)**.** *Statements (a) and (b) of Conjecture 2 hold for all elliptic curves E over $\mathbb{Q}$ with $order_{s=1}L(E/\mathbb{Q},s) \leq 1$. In particular, $Ш(E/\mathbb{Q})$ is finite for all such elliptic curves.*

A crucial input to the theorem of Kolyvagin was provided by the following theorem of Gross-Zagier proved in 1986.

Theorem 21 (Gross-Zagier). *If an elliptic curve E defined over $\mathbb{Q}$ satisfies order$_{s=1}L(E/\mathbb{Q},s) = 1$, then E has rank ≥ 1.*

All the above results assumed the truth of Conjecture 1, which itself was proved by Wiles *et.al.* in the late 1990's (see [W], [BCDT]). There is also a related conjecture known as the parity conjecture.

Conjecture 3. *order$_{s=1}L(E/K,s) = r_K(E)$ mod 2.*

Theorem 22. *(Monsky) The parity conjecture is true for an elliptic curve E defined over $\mathbb{Q}$ if $Ш(E/\mathbb{Q})$ is finite.*

In recent years, there has been some significant progress towards the proof of the parity conjecture due to the work of Dokchitser-Dokchitser, Greenberg, Nekovar and others. In particular, Dokchitser-Dokchitser show that if the p-primary part of $Ш(E/\mathbb{Q})$ is finite for an elliptic curve E defined over $\mathbb{Q}$ and for some prime p, then the parity conjecture holds for E. Recent work of Bhargava and Shankar shows that in a statistical sense, a sizeable proportion of elliptic curves defined over $\mathbb{Q}$ has rank zero and another sizeable proportion has rank one. In particular, for a sizeable proportion of elliptic curves over $\mathbb{Q}$, the BSD conjectures are true.

So far, there is no general algorithm known which can compute the rank of a given elliptic curve defined over a number field. One can compute the rank of an elliptic curve by computing the derivative of the associated Hasse-Weil L-function only if the BSD conjectures are known. But at present, we do not know a single example of an elliptic curve over $\mathbb{Q}$ of rank ≥ 2 for which $Ш(E/\mathbb{Q})$ is finite.

Numerical examples. The BSD conjectures have been verified extensively for numerous concrete examples. As remarked earlier, the conjecture itself was formulated based on the data obtained by explicit computations. In the last half a century, remarkable progress on the computational side has been made possible, thanks to advances in computing and theoretical knowledge. We refer the reader to the excellent data base compiled by Cremona, Stein, Watkins and others ([C],[WS]). Thus the beauty of BSD conjectures lies in its intricacy, combined with the fact that most of the invariants in the exact formula can be explicitly computed.

In this final section, we provide a few illustrative numerical examples using the mathematical software Sage. We shall provide three examples of elliptic curves with analytic rank zero, one and two respectively. Consider the ellipic curve E given by the Weierstrass equation

$$E : y^2 + y = x^3 - x^2 - 7820x - 263580$$

over $\mathbb{Q}$. The discriminant Δ of E over $\mathbb{Q}$ is 11 and the j invariant of E is equal to $1 \times 212 \times 11^{-1} \times 29^3 \times 809^3$. The curve E has split multiplicative reduction at 11. The BSD invariants of E are as follows:

- analytic rank, $r = 0$,
- regulator, $Reg_{\mathbb{Q}}(E) = 1$,
- real period $\Omega = 0.253841860856\cdots$

- torsion order, $\#E(\mathbb{Q})_{tor} = 1$
- $L(E/\mathbb{Q}, 1) = 0.253841860856\cdots$
- Tamagawa Number at 11, $c_{11}(E) = 1$.

Since $L(E/\mathbb{Q}, 1) \neq 0$, BSD conjectures are true for E over $\mathbb{Q}$. In particular, $r_{\mathbb{Q}}(E) = 0$ and from the above data we get that $\#\text{Ш}(E/\mathbb{Q}) = 1$. Next, we consider the following elliptic curve E of positive rank :

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

The curve E has non-split multiplicative reduction at 43. The discriminant of E is -43 and the j invariant is $-1 \times 3^{12} \times 43^{-1}$. The BSD invariants of E are given by

- analytic rank, $r = 1$,
- regulator, $Reg_{\mathbb{Q}}(E) = 0.0628165070875\cdots$,
- real period $\Omega = 5.46868952997\cdots$
- torsion order, $\#E(\mathbb{Q})_{tor} = 1$
- $L(E/\mathbb{Q}, 1) = 0$ and $L'(E/\mathbb{Q}, 1) = 0.343523974618\cdots$
- Tamagawa Number at 43, $c_{43}(E) = 1$.

Since E has analytic rank 1 over $\mathbb{Q}$, BSD conjectures hold and we get that $r_{\mathbb{Q}}(E) = 1$ and $\#\text{Ш}(E/\mathbb{Q}) = 1$. We shall end by providing an example of elliptic curve for which we still do not know if the BSD conjectures are true. Consider the elliptic curve

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

The curve E has split multiplicative reduction at 389. The discriminant of E is 389 and the j invariant is $2^{12} \times 7^3 \times 389^{-1}$. The BSD invariant of E are given by

- analytic rank, $r = 2$,
- regulator, $Reg_{\mathbb{Q}}(E) = 0.15246017794\cdots$,
- real period $\Omega = 4.98042512171\cdots$
- torsion order, $\#E(\mathbb{Q})_{tor} = 1$
- $L(E/\mathbb{Q}, 1) = 0$ and $L'(E/\mathbb{Q}, 1) = 0$ and $L''(E/\mathbb{Q}, 1) = 0.759316500288\cdots$
- Tamagawa Number at 389, $c_{389}(E) = 1$.

The BSD conjecture for E over $\mathbb{Q}$ predicts that the $r_{\mathbb{Q}}(E) = 2$ and $\#\text{Ш}(E/\mathbb{Q}) = 1$. In this case it can be shown (using the method of "2-descent") that $r_{\mathbb{Q}}(E) = 2$ and $\#\text{Ш}(E/\mathbb{Q})[2] = 1$ (see [C1]). A set of generators of the Mordell-Weil group of E over $\mathbb{Q}$ is given by $\{(1, 1), (0, 0)\}$. At present we do not know if the predictions on the size of $\#\text{Ш}(E/\mathbb{Q})$ is true.

References

[BCDT] C. Breuil, B. Conrad, Fred Diamond, and R. Taylor, On the modularity of elliptic curves over Q: wild 3-adic exercises, J. Amer. Math. Soc. 14 (2001), no. 4, 843939 (electronic). MR 2002d:11058

[BS] B. Birch and H. Swinnerton-Dyer, Notes on elliptic curves II, Journ. reine u. angewandte Math. 218 (1965), 79108

[B] B.J. Birch, Elliptic curves over Q: A progress report, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, R.I., 1971, pp. 396400.

[BLR] Seigfried Bosch, Werner Lutkeböhmert, Nichel Raynaud, Néron Models, Springer-Verlag, A series of Modern Serveys in Mathematics, 1989.

[C] J. E. Cremona, Algorithms for modular elliptic curves, second ed., Cambridge University Press, Cambridge, 1997, http://www.maths.nott.ac.uk/personal/jec/book/

[C1] J. E. Cremona, Numerical evidence for the BirchSwinnerton-Dyer conjecture, http://homepages.warwick.ac.uk/staff/J.E.Cremona/papers/bsd50.pdf

[D] Henri Darmon, Rational points on modular elliptic curves, http://www.math.mcgill.ca/darmon/pub/Articles/Research/36.NSF-CBMS/chapter.pdf

[Si] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Second Edition, Graduate Texts in Mathematics 106, Springer.

[ST] Joseph H. Silverman, John Tate, Rational Points on Elliptic curves, Undergraduate Text in Mathematics, Springer.

[T] J. Tate, A review of non-archimedean elliptic functions, Elliptic Curves, Modular Forms and Fermats Last Theorem, International Press (1995), 162-184.

[W] A. J. Wiles, Modular elliptic curves and Fermats last theorem, Ann. of Math. (2) 141 (1995), no. 3, 443551. MR 1333035 (96d:11071)

[W1] A. J. Wiles, The Birch and Swinnerton-Dyer Conjecture, http://www.claymath.org/prize problems/birchsd.htm.

[WS] William A. Stein, Modular Forms database, http://modular.math.washington.edu/Tables/

IISER Mohali and Mathematics Center Heidelberg (MATCH)
E-mail address: sshekhars2012@gmail.com

University British Columbia
E-mail address: sujatha@math.ubc.ca