REMARKS ON THE BIRCH-SWINNERTON-DYER CONJECTURE

JAE-HYUN YANG

Abstract. We give a brief description of the Birch-Swinnerton-Dyer conjecture which is one of the seven Clay problems and present several related conjectures. We describe the relation between the nilpotent orbits of $SL(2, \mathbb{R})$ and CM points.

1. Introduction

On May 24, 2000, the Clay Mathematics Institute (CMI for short) announced that it would award prizes of 1 million dollars each for solutions to seven mathematics problems. These seven problems are

Problem 1. The “P versus NP” Problem
Problem 2. The Riemann Hypothesis
Problem 3. The Poincaré Conjecture
Problem 4. The Hodge Conjecture
Problem 5. The Birch-Swinnerton-Dyer Conjecture (briefly, the BSD conjecture)
Problem 6. The Navier-Stokes Equations: Prove or disprove the existence and smoothness of solutions to the three dimensional Navier-Stokes equations.
Problem 7. Yang-Mills Theory: Prove that quantum Yang-Mills fields exist and have a mass gap.

Problem 1 is arisen from theoretical computer science, Problem 2 and Problem 5 from number theory, Problem 3 from topology, Problem 4 from algebraic geometry and topology, and finally problem 6 and 7 are related to physics. For more details on some stories about these problems, we refer to Notices of AMS, vol. 47, no. 8, pp. 877-879 (September 2000) and the homepage of CMI. In 2003, Problem 3 was solved by Grisha Perelman [35, 36, 37]. We refer to [12, 13, 21, 32, 33] for more details on Perelman’s work. Recently Bhargava’s school computed the Selmer groups of an elliptic curve and so solved Problem 5 partially.

The purpose of this paper is to describe the relation between the nilpotent orbits of $SL(2, \mathbb{R})$ and CM points and to present several conjectures relating to the BSD Conjecture.

The paper is organized as follows. From Section 2 to Section 5, we will explain Problem 5, that is, the Birch-Swinnerton-Dyer conjecture which was proposed by the English mathematicians, B. Birch and H. P. F. Swinnerton-Dyer [7, 8] around 1960s in some detail. This conjecture says that if $E$ is an elliptic curve defined over $\mathbb{Q}$, then the algebraic rank of $E$ equals the analytic rank of $E$. In 2001, the Shimura-Taniyama conjecture stating that any elliptic curve defined over $\mathbb{Q}$ is modular was shown to be true by Breuil, Conrad, Diamond and Taylor [10]. This fact shed some lights on the solution of the BSD conjecture. In Section 6, we describe the connection between the heights of Heegner points on modular curves $X_0(N)$ and Fourier coefficients of modular forms of half integral weight or of the Jacobi forms corresponding to them by the Skoruppa-Zagier correspondence. Most
of the materials in Section 2-6 were already printed in [46]. In Section 7, we briefly review the works
done recently by the school of Manjul Bhargava [123456]. In Section 8, we describe the adjoint
orbits of \( SL(2, \mathbb{R}) \) in its Lie algebra \( \mathfrak{sl}(2, \mathbb{R}) \) explicitly. In the final section, we describe the relation
between the nilpotent orbits of \( SL(2, \mathbb{R}) \) and CM points. We propose several conjectures relating to
the Birch-Swinnerton-Dyer conjecture.

Notations: We denote by \( \mathbb{Q}, \mathbb{R} \) and \( \mathbb{C} \) the fields of rational numbers, real numbers and com-
plex numbers respectively. \( \mathbb{Z} \) and \( \mathbb{Z}^+ \) denote the ring of integers and the set of positive integers
respectively. \( \mathbb{H} \) denotes the Poincaré upper half plane.

2. The Mordell-Weil Group

A curve \( E \) is said to be an elliptic curve over \( \mathbb{Q} \) if it is a nonsingular projective curve of genus
1 with its affine model
\[
(2.1) \quad y^2 = f(x),
\]
where \( f(x) \) is a polynomial of degree 3 with integer coefficients and with 3 distinct roots over \( \mathbb{C} \).
An elliptic curve over \( \mathbb{Q} \) has an abelian group structure with distinguished element \( \infty \) as an identity
element. The set \( E(\mathbb{Q}) \) of rational points given by
\[
E(\mathbb{Q}) = \{ (x, y) \in \mathbb{Q}^2 \mid y^2 = f(x) \} \cup \{ \infty \}
\]
also has an abelian group structure.

L. J. Mordell (1888-1972) [31] proved the following theorem in 1922.

**Theorem 2.1** (Mordell,1922). \( E(\mathbb{Q}) \) is finitely generated, that is,
\[
E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E_{\text{tor}}(\mathbb{Q}),
\]
where \( r \) is a nonnegative integer and \( E_{\text{tor}}(\mathbb{Q}) \) is the torsion subgroup of \( E(\mathbb{Q}) \).

**Definition 2.2.** Around 1930, A. Weil (1906-1998) proved that the set \( A(\mathbb{Q}) \) of rational points on
an abelian variety \( A \) defined over \( \mathbb{Q} \) is finitely generated. An elliptic curve is an abelian variet y of
dimension one. Therefore \( E(\mathbb{Q}) \) is called the Mordell-Weil group and the integer \( r \) is said to be the
algebraic rank of \( E \).

In 1977, B. Mazur (1937-) [29] discovered the structure of the torsion subgroup \( E_{\text{tor}}(\mathbb{Q}) \) completely
using a deep theory of modular curves.

**Theorem 2.3** (Mazur, 1977). Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \). Then the torsion subgroup
\( E_{\text{tor}}(\mathbb{Q}) \) is isomorphic to the following 15 groups
\[
\mathbb{Z}/n\mathbb{Z} \quad (1 \leq n \leq 10, \; n = 12),
\]
\[
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad (1 \leq n \leq 4).
\]

E. Lutz (1914-?) and T. Nagell (1895-?) obtained the following result independently.

**Theorem 2.4** (Lutz, 1937; Nagell, 1935). Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \) given by
\[
E : \quad y^2 = x^2 + ax + b, \quad a, b \in \mathbb{Z}, \; 4a^3 + 27b^2 \neq 0.
\]
Suppose that \( P = (x_0, y_0) \) is an element of the torsion subgroup \( E_{\text{tor}}(\mathbb{Q}) \). Then
(a) \( x_0, y_0 \in \mathbb{Z} \), and
(b) \( 2P = 0 \) or \( y_0^2 \mid (4a^3 + 27b^2) \).
We observe that the above theorem gives an effective method for bounding $E_{\text{tor}}(Q)$. According to Theorem B and C, we know the torsion part of $E(Q)$ satisfactorily. But we have no idea of the free part of $E(Q)$ so far. As for the algebraic rank $r$ of an elliptic curve $E$ over $Q$, Noam Elkies found an example of an elliptic curve of rank 28 in 2006. Indeed, that elliptic curve is given by

$$E_e: \ y^2 + xy + y = x^3 - x^2 - \alpha x + \beta$$

has its algebraic rank 28. Here

$\alpha = 20067762415575526585033208209338542750930230312178956502$

and

$\beta = 3448161179503055646703298569039072037485594435931918036126600829629193948732243429$.

Elkies also computed 28 generators of $E_e(Q)$ (cf. https://web.math.pmf.unizg.hr/duje/tors/rk28.html).

**Conjecture A.** Given a nonnegative integer $n$, there is an elliptic curve $E$ over $Q$ with its algebraic rank $n$.

The algebraic rank of an elliptic curve is an invariant under an isogeny. Here an isogeny of an elliptic curve $E$ means a holomorphic map $\phi: E(C) \rightarrow E(C)$ satisfying the condition $\phi(0) = 0$.

### 3. Modular Elliptic Curves

For a positive integer $N \in \mathbb{Z}^+$, we let

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \mid N|c \right\}$$

be the Hecke subgroup of $SL(2,\mathbb{Z})$ of level $N$. Let $\mathbb{H}$ be the Poincaré upper half plane. Then

$$Y_0(N) = \Gamma_0(N)\backslash \mathbb{H}$$

is a noncompact surface, and

$$X_0(N) = Y_0(N)\backslash \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$$

is a compactification of $Y_0(N)$. We recall that a *cusp form* of weight $k \geq 1$ and level $N \geq 1$ is a holomorphic function $f$ on $\mathbb{H}$ such that for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ and for all $z \in \mathbb{H}$, we have

$$f((az + b)/(cz + d)) = (cz + d)^k f(z)$$

and $|f(z)|^2(\text{Im } z)^k$ is bounded on $\mathbb{H}$. We denote the space of all cusp forms of weight $k$ and level $N$ by $S_k(N)$. If $f \in S_k(N)$, then it has a Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} c_n(f) q^n, \quad q := e^{2\pi i z}$$

convergent for all $z \in \mathbb{H}$. We note that there is no constant term due to the boundedness condition on $f$. Now we define the $L$-series $L(f, s)$ of $f$ to be

$$(3.2) \quad L(f, s) = \sum_{n=1}^{\infty} c_n(f) n^{-s}.$$

For each prime $p \nmid N$, there is a linear operator $T_p$ on $S_k(N)$, called the Hecke operator, defined by

$$(f|T_p)(z) = p^{-1} \sum_{i=0}^{p-1} f((z+i)/p) + p^{k-1} (cpz + d)^k \cdot f((apz + d)/(cpz + d))$$
for any \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}) \) with \( c \equiv 0 \pmod{N} \) and \( d \equiv p \pmod{N} \). The Hecke operators \( T_p \) for \( p \mathbb{N} \) can be diagonalized on the space \( S_k(N) \) and a simultaneous eigenvector is called an eigenform. If \( f \in S_k(N) \) is an eigenform, then the corresponding eigenvalues, \( a_p(f) \), are algebraic integers and we have \( c_p(f) = a_p(f) c_1(f) \).

Let \( \lambda \) be a place of the algebraic closure \( \bar{\mathbb{Q}} \) in \( \mathbb{C} \) above a rational prime \( \ell \) and \( \bar{\mathbb{Q}} \), denote the algebraic closure of \( \mathbb{Q}_\ell \) considered as a \( \mathbb{Q} \)-algebra via \( \lambda \). It is known that if \( f \in S_k(N) \), there is a unique continuous irreducible representation

\[
\rho_{f,\lambda} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\bar{\mathbb{Q}}_\ell)
\]

such that for any prime \( p \nmid N\ell \), \( \rho_{f,\lambda} \) is unramified at \( p \) and \( \text{tr} \rho_{f,\lambda}(\text{Frob}_p) = a_p(f) \). The existence of \( \rho_{f,\lambda} \) is due to G. Shimura (1930- ) if \( k = 2 \) \[39\], to P. Deligne (1944- ) if \( k > 2 \) \[15\] and to P. Deligne and J.-P. Serre (1926- ) if \( k = 1 \) \[16\]. Its irreducibility is due to Ribet if \( k > 1 \) \[38\], and to Deligne and Serre if \( k = 1 \) \[16\]. Moreover \( \rho_{f,\lambda} \) is odd and potentially semi-stable at \( \ell \) in the sense of Fontaine. We may choose a conjugate of \( \rho_{f,\lambda} \) which is valued in \( GL_2(\mathcal{O}_{\bar{\mathbb{Q}}_\ell}) \), and reducing modulo the maximal ideal and semi-simplifying yields a continuous representation

\[
\tilde{\rho}_{f,\lambda} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}_\ell),
\]

which, up to isomorphism, does not depend on the choice of conjugate of \( \rho_{f,\lambda} \).

**Definition 3.1.** Let \( \rho : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\bar{\mathbb{Q}}_\ell) \) be a continuous representation which is unramified outside finitely many primes and for which the restriction of \( \rho \) to a decomposition group at \( \ell \) is potentially semi-stable in the sense of Fontaine. We call \( \rho \) modular if \( \rho \) is isomorphic to \( \rho_{f,\lambda} \) for some eigenform \( f \) and some \( \lambda | \ell \).

**Definition 3.2.** An elliptic curve \( E \) defined over \( \mathbb{Q} \) is said to be modular if there exists a surjective holomorphic map \( \varphi : X_0(N) \to E(\mathbb{C}) \) for some positive integer \( N \).

In 2001 C. Breuil, B. Conrad, F. Diamond and R. Taylor \[10\] proved that the Taniyama-Shimura conjecture is true.

**Theorem 3.3 (\[10\], 2001).** An elliptic curve defined over \( \mathbb{Q} \) is modular.
4. The L-Series of an Elliptic Curve

Let $E$ be an elliptic curve over $\mathbb{Q}$. The L-series $L(E, s)$ of $E$ is defined as the product of the local $L$-factors:

$$L(E, s) = \prod_{p|\Delta_E} (1 - a_p p^{-s})^{-1} \prod_{p\nmid\Delta_E} (1 - a_p p^{-s} + p^{-2s})^{-1},$$

where $\Delta_E$ is the discriminant of $E$, $p$ is a prime, and if $p \nmid \Delta_E$,

$$a_p := p + 1 - |E(\mathbb{F}_p)|,$$

and if $p|\Delta_E$, we set $a_p := 0, 1, -1$ if the reduced curve $\overline{E}/\mathbb{F}_p$ has a cusp at $p$, a split node at $p$, and a nonsplit node at $p$ respectively. Then $L(E, s)$ converges absolutely for $\Re s > \frac{3}{2}$ from the classical result that $|a_p| < 2\sqrt{p}$ for each prime $p$ due to H. Hasse (1898-1971) and is given by an absolutely convergent Dirichlet series. We remark that $x^2 - a_p x + p$ is the characteristic polynomial of the Frobenius map acting on $\overline{E}(\mathbb{F}_p)$ by $(x, y) \mapsto (x^p, y^p)$.

**Conjecture B.** Let $N(E)$ be the conductor of an elliptic curve $E$ over $\mathbb{Q}$ ([?], p. 361). We set

$$\Lambda(E, s) := N(E)^{s/2} (2\pi)^{-s} \Gamma(s) L(E, s), \quad \Re s > \frac{3}{2}.$$

Then $\Lambda(E, s)$ has an analytic continuation to the whole complex plane and satisfies the functional equation

$$\Lambda(E, s) = \epsilon \Lambda(E, 2 - s), \quad \epsilon = \pm 1.$$

The above conjecture is now true because the Shimura-Taniyama conjecture is true (cf. Theorem E). We have some knowledge about analytic properties of $E$ by investigating the $L$-series $L(E, s)$. The order of $L(E, s)$ at $s = 1$ is called the analytic rank of $E$.

Now we explain the connection between the modularity of an elliptic curve $E$, the modularity of the Galois representation and the $L$-series of $E$. For a prime $\ell$, we let $\rho_{E, \ell}$ (resp. $\overline{\rho}_{E, \ell}$) denote the representation of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $\ell$-adic Tate module (resp. the $\ell$-torsion) of $E(\mathbb{Q})$. Let $N(E)$ be the conductor of $E$. Then it is known that the following conditions are equivalent:

1. The $L$-function $L(E, s)$ of $E$ equals the $L$-function $L(f, s)$ for some eigenform $f$.
2. The $L$-function $L(E, s)$ of $E$ equals the $L$-function $L(f, s)$ for some eigenform $f$ of weight 2 and level $N(E)$.
3. For some prime $\ell$, the representation $\rho_{E, \ell}$ is modular.
4. For all primes $\ell$, the representation $\rho_{E, \ell}$ is modular.
5. There is a non-constant holomorphic map $X_0(N) \to E(\mathbb{C})$ for some positive integer $N$.
6. There is a non-constant morphism $X_0(N(E)) \to E$ which is defined over $\mathbb{Q}$.
7. $E$ admits a hyperbolic uniformization of arithmetic type (cf. [30] and [42]).

5. The Birch-Swinnerton-Dyer Conjecture

Now we state the BSD conjecture.
The BSD Conjecture. Let \( E \) be an elliptic curve over \( \mathbb{Q} \). Then the algebraic rank of \( E \) equals the analytic rank of \( E \).

I will describe some historical backgrounds about the BSD conjecture. Around 1960, Birch (1931- ) and Swinnerton-Dyer (1927- ) formulated a conjecture which determines the algebraic rank \( r \) of an elliptic curve \( E \) over \( \mathbb{Q} \). The idea is that an elliptic curve with a large value of \( r \) has a large number of rational points and should therefore have a relatively large number of solutions modulo a prime \( p \) on the average as \( p \) varies. For a prime \( p \), we let \( N(p) \) be the number of pairs of integers \( x, y \) (mod \( p \)) satisfying (2.1) as a congruence (mod \( p \)). Then the BSD conjecture in its crudest form says that we should have an asymptotic formula

\[
\prod_{p \leq x} \frac{N(p) + 1}{p} \sim C \ (\log p)^r \quad \text{as } x \to \infty
\]

for some constant \( C > 0 \). If the \( L \)-series \( L(E, s) \) has an analytic continuation to the whole complex plane (this fact is conjectured; cf. Conjecture F), then \( L(E, s) \) has a Taylor expansion

\[
L(E, s) = c_0(s - 1)^m + c_1(s - 1)^{m + 1} + \cdots
\]

at \( s = 1 \) for some non-negative integer \( m \geq 0 \) and constant \( c_0 \neq 0 \). The BSD conjecture says that the integer \( m \), in other words, the analytic rank of \( E \), should equal the algebraic rank \( r \) of \( E \) and furthermore the constant \( c_0 \) should be given by

\[
c_0 = \lim_{s \to 1} \frac{L(E, s)}{(s - 1)^m} = \alpha \cdot R \cdot |E_{\text{tor}}(\mathbb{Q})|^{-1} \cdot \Omega \cdot S,
\]

where \( \alpha > 0 \) is a certain constant, \( R \) is the elliptic regulator of \( E \), \( |E_{\text{tor}}(\mathbb{Q})| \) denotes the order of the torsion subgroup \( E_{\text{tor}}(\mathbb{Q}) \) of \( E(\mathbb{Q}) \), \( \Omega \) is a simple rational multiple (depending on the bad primes) of the elliptic integral

\[
\int_{\gamma}^{\infty} \frac{dx}{\sqrt{f(x)}} \quad (\gamma = \text{the largest root of } f(x) = 0)
\]

and \( S \) is an integer square which is supposed to be the order of the Tate-Shafarevich group III(\( E \)) of \( E \).

The Tate-Shafarevich group III(\( E \)) of \( E \) is a very interesting subject to be investigated in the future. Unfortunately III(\( E \)) is still not known to be finite. So far an elliptic curve whose Tate-Shafarevich group is infinite has not been discovered. So many mathematicians propose the following.

Conjecture C. The Tate-Shafarevich group III(\( E \)) of \( E \) is finite.

There are some evidences supporting the BSD conjecture. I will list these evidences chronologically.

Result 1 (Coates-Wiles [14], 1977). Let \( E \) be a CM curve over \( \mathbb{Q} \). Suppose that the analytic rank of \( E \) is zero. Then the algebraic rank of \( E \) is zero.

Result 2 (Rubin [38], 1981). Let \( E \) be a CM curve over \( \mathbb{Q} \). Assume that the analytic rank of \( E \) is zero. Then the Tate-Shafarevich group III(\( E \)) of \( E \) is finite.

Result 3 (Gross-Zagier [19], 1986; [10], 2001). Let \( E \) be an elliptic curve over \( \mathbb{Q} \). Assume that the analytic rank of \( E \) is equal to one and \( \epsilon = -1 \) (cf. Conjecture F). Then the algebraic rank of \( E \) is equal to or bigger than one.

Result 4 (Gross-Zagier [19], 1986). There exists an elliptic curve \( E \) over \( \mathbb{Q} \) such that rank \( E(\mathbb{Q}) = \text{ord}_{s=1} L(E, s) = 3 \). For instance, the elliptic curve \( \tilde{E} \) given by

\[
\tilde{E} : -139 y^2 = x^3 + 10 x^2 - 20 x + 8
\]

satisfies the above property.
**Result 5** (Kolyvagin [24], 1990: Gross-Zagier [19], 1986: Bump-Friedberg-Hoffstein [11], 1990: Murty-Murty [34], 1990: [10], 2001). Let $E$ be an elliptic curve over $\mathbb{Q}$. Assume that the analytic rank of $E$ is $1$ and $\varepsilon = -1$. Then algebraic rank of $E$ is equal to $1$.

**Result 6** (Kolyvagin [24], 1990: Gross-Zagier [19], 1986: Bump-Friedberg-Hoffstein [11], 1990: Murty-Murty [34], 1990: [10], 2001). Let $E$ be an elliptic curve over $\mathbb{Q}$. Assume that the analytic rank of $E$ is zero and $\varepsilon = 1$. Then algebraic rank of $E$ is equal to zero.

Cassels proved the fact that if an elliptic curve over $\mathbb{Q}$ is isogeneous to another elliptic curve $E'$ over $\mathbb{Q}$, then the BSD conjecture holds for $E$ if and only if the BSD conjecture holds for $E'$.

### 6. Jacobi Forms and Heegner Points

In this section, I shall describe the result of Gross-Kohnen-Zagier [20] roughly.

First we begin with giving the definition of Jacobi forms. By definition a Jacobi form of weight $k$ and index $m$ is a holomorphic complex valued function $\phi(z, w) (z \in \mathbb{H}, w \in \mathbb{C})$ satisfying the transformation formula

$$
\phi \left( \frac{az + b}{cz + d}, \frac{w + \lambda z + \mu}{cz + d} \right) = e^{-2\pi i \{ cm(w+\lambda z+\mu)(cz+d)^{-1} - m(\lambda^2 z + 2\lambda w) \}} \times (cz + d)^k \phi(z, w)
$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$ and $(\lambda, \mu) \in \mathbb{Z}^2$, and having a Fourier expansion of the form

$$
\phi(z, w) = \sum_{n,r \in \mathbb{Z}, r^2 \leq 4mn} c(n, r) e^{2\pi i (nz + rw)}.
$$

We remark that the Fourier coefficients $c(n, r)$ depend only on the discriminant $D = r^2 - 4mn$ and the residue $r \pmod{2m}$. From now on, we put $\Gamma_1 := SL(2, \mathbb{Z})$. We denote by $J_{k,m}(\Gamma_1)$ the space of all Jacobi forms of weight $k$ and index $m$. It is known that one has the following isomorphisms

$$
[\Gamma_2, k]^M \cong J_{k,1}(\Gamma_1) \cong M_{\frac{k}{2}}^{+}(\Gamma_0(4)) \cong [\Gamma_1, 2k - 2],
$$

where $\Gamma_2$ denotes the Siegel modular group of degree 2, $[\Gamma_2, k]^M$ denotes the Maass space introduced by H. Maass (1911-1993) (cf. [20], [27], [28]), $M_{\frac{k}{2}}^{+}(\Gamma_0(4))$ denotes the Kohnen space introduced by W. Kohnen [22] and $[\Gamma_1, 2k - 2]$ denotes the space of modular forms of weight $2k - 2$ with respect to $\Gamma_1$. We refer to [12] and [41], pp. 65-70 for a brief detail. The above isomorphisms are compatible with the action of the Hecke operators. Moreover, according to the work of Skoruppa and Zagier [41], there is a Hecke-equivariant correspondence between Jacobi forms of weight $k$ and index $m$, and certain usual modular forms of weight $2k - 2$ on $\Gamma_0(N)$.

Now we give the definition of Heegner points of an elliptic curve $E$ over $\mathbb{Q}$. By [10], $E$ is modular and hence one has a surjective holomorphic map $\phi_E : X_0(N) \to E(\mathbb{C})$. Let $K$ be an imaginary quadratic field of discriminant $D$ such that every prime divisor $p$ of $N$ is split in $K$. Then it is easy to see that $(D, N) = 1$ and $D$ is congruent to a square $r^2$ modulo $4N$. Let $\Theta$ be the set of all $z \in \mathbb{H}$ satisfying the following conditions

$$
a z^2 + bz + c = 0, \quad a, b, c \in \mathbb{Z}, \quad N | a,
$$

$$
b \equiv r \pmod{2N}, \quad D = b^2 - 4ac.
$$

Then $\Theta$ is invariant under the action of $\Gamma_0(N)$ and $\Theta$ has only a $h_K \Gamma_0(N)$-orbits, where $h_K$ is the class number of $K$. Let $z_1, \cdots, z_{h_K}$ be the representatives for these $\Gamma_0(N)$-orbits. Then
\(\phi_{E}(z_1), \cdots, \phi_{E}(z_{h})\) are defined over the Hilbert class field \(H(K)\) of \(K\), i.e., the maximal everywhere unramified extension of \(K\). We define the Heegner point \(P_{D,r}\) of \(E\) by

\[
P_{D,r} = \sum_{i=1}^{h} \phi_{E}(z_i).
\]

We observe that \(e = 1\), then \(P_{D,r} \in E(\mathbb{Q})\).

Let \(E^{(D)}\) be the elliptic curve (twisted from \(E\)) given by

\[
E^{(D)} : \quad Dy^2 = f(x).
\]

Then one knows that the \(L\)-series of \(E\) over \(K\) is equal to \(L(E, s) L(E^{(D)}, s)\) and that \(L(E^{(D)}, s)\) is the twist of \(L(E, s)\) by the quadratic character of \(K/\mathbb{Q}\).

**Theorem 6.1** (Gross-Zagier [19, 10]). Let \(E\) be an elliptic curve over \(\mathbb{Q}\) of conductor \(N\) such that \(e = -1\). Assume that \(D\) is odd. Then

\[
L'(E, 1) L(E^{(D)}, 1) = c_E u^{-2} |D|^{-\frac{3}{2}} \hat{h}(P_{D,r}),
\]

where \(c_E\) is a positive constant not depending on \(D\) and \(r\), \(u\) is a half of the number of units of \(K\) and \(\hat{h}\) denotes the canonical height of \(E\).

Since \(E\) is modular by [10], there is a cusp form of weight 2 with respect to \(\Gamma_0(N)\) such that \(L(f, s) = L(E, s)\). Let \(\phi(z, w)\) be the Jacobi form of weight 2 and index \(N\) which corresponds to \(f\) via the Skoruppa-Zagier correspondence. Then \(\phi(z, w)\) has a Fourier series of the form (6.2).

B. Gross, W. Kohnen and D. Zagier [20] obtained the following result.

**Theorem 6.2** (Gross-Kohnen-Zagier [20, 10]). Let \(E\) be an elliptic curve over \(\mathbb{Q}\) with conductor \(N\) and suppose that \(e = -1\), \(r = 1\). Suppose that \((D_1, D_2) = 1\) and \(D_i \equiv r_i^2 \pmod{4N} (i = 1, 2)\). Then

\[
L'(E, 1) c((r_1^2 - D_1)/(4N), r_1) c((r_2^2 - D_2)/(4N), r_2) = c'_E < P_{D_1,r_1}, P_{D_2,r_2} >,
\]

where \(c'_E\) is a positive constant not depending on \(D_1, r_1\) and \(D_2, r_2\) and \(<, >\) is the height pairing induced from the Néron-Tate height function \(\hat{h}\), that is, \(\hat{h}(P_{D,r}) = < P_{D,r}, P_{D,r} >\).

We see from the above theorem that the value of \(< P_{D_1,r_1}, P_{D_2,r_2} >\) of two distinct Heegner points is related to the product of the Fourier coefficients \(c((r_1^2 - D_1)/(4N), r_1) c((r_2^2 - D_2)/(4N), r_2)\) of the Jacobi forms of weight 2 and index \(N\) corresponded to the eigenform \(f\) of weight 2 associated to an elliptic curve \(E\). We refer to [15] and [17] for more details.

**Corollary.** There is a point \(P_0 \in E(\mathbb{Q}) \otimes \mathbb{R}\) such that

\[
P_{D,r} = c((r^2 - D)/(4N), r) P_0
\]

for all \(D\) and \(r (D \equiv r^2 \pmod{4N})\) with \((D, 2N) = 1\).

The corollary is obtained by combining Theorem H and Theorem I with the Cauchy-Schwarz inequality in the case of equality.

**Remark 6.3.** R. Borcherds [9] generalized the Gross-Kohnen-Zagier theorem to certain more general quotients of Hermitian symmetric spaces of high dimension, namely to quotients of the space associated to an orthogonal group of signature \((2, b)\) by the unit group of a lattice. Indeed he relates the Heegner divisors on the given quotient space to the Fourier coefficients of vector-valued holomorphic modular forms of weight \(1 + b/2\).
7. Brief Reviews on the Works of Bhargava’s School

In this section, we briefly describe the recent works done by Bhargava’s School. First we review the Selmer group. Let $A = A(K)$ and $B = B(K)$ be abelian varieties over number field $K$ and let $f : A \to B$ be a nonzero isogeny with finite kernel

$$A[f] = \{ a \in A \mid f(a) = 0 \}.$$ 

Then we get a short exact sequence:

$$0 \longrightarrow A[f] \overset{\alpha}{\longrightarrow} A \overset{f}{\longrightarrow} B \longrightarrow 0.$$ 

Let $G_K = \text{Gal}(\overline{K}/K)$ be the Galois group of $\overline{K}$ over $K$. Then we have the following long exact sequence of Galois cohomology groups:

$$0 \longrightarrow A[f]^{G_K} = A(K)[f] \longrightarrow A^{G_K} = A(K) \overset{f}{\longrightarrow} B^{G_K} = B(K) \longrightarrow 0.$$ 

(7.1)

From (7.1) we obtain the following short exact sequence:

$$0 \longrightarrow B(K)/(f(A(K))) \overset{\delta}{\longrightarrow} H^1(G_K, A[f]) \longrightarrow H^1(G_K, A[f])/f \longrightarrow 0.$$ 

(7.2)

We let $K_v$ and $G_v$ the completion at $v$ and the decomposition group of $K_v$ respectively. We put $A_v := A(\overline{K}_v)$. Since $G_v$ acts on $A_v$, $B_v$ and $A_v[f]$, we get the short exact sequence:

$$0 \longrightarrow B_v(K_v)/(f(A_v(K_v))) \overset{\delta}{\longrightarrow} H^1(G_v, A_v[f]) \longrightarrow H^1(G_v, A_v[f])/f \longrightarrow 0.$$ 

(7.3)

From the above short exact sequences (7.2) and (7.3), we have the following commutative diagram:

$$
\begin{array}{cccccccc}
0 & \longrightarrow & B(K)/(f(A(K))) & \overset{\delta}{\longrightarrow} & H^1(G_K, A[f]) & \longrightarrow & H^1(G_K, A[f])/f & \longrightarrow & 0 \\
& & \downarrow & & \bigcap & & \bigcap & & \\
0 & \longrightarrow & \prod_v B_v(K_v)/(f(A_v(K_v))) & \overset{\delta}{\longrightarrow} & \prod_v H^1(G_v, A_v[f]) & \longrightarrow & \prod_v H^1(G_v, A_v[f])/f & \longrightarrow & 0 \\
\end{array}
$$

Here $\text{Res}_v(\xi) = \xi|_{G_v}$ for $\xi \in H^1(G_K, A[f])$.

**Definition 7.1.** With the above notations, the $f$-Selmer group of $A/K$ is defined by

$$\text{Sel}^{(f)}(A/K) = \text{Ker}\left( H^1(G_K, A[f]) \to \prod_v H^1(G_v, A_v[f]) \right),$$

$$= \bigcap_v \text{Ker}\left( H^1(G_K, A[f]) \to H^1(G_v, A_v[f]) \right).$$

**Definition 7.2.** The Shafarevich-Tate group of $A/K$ is defined by

$$\text{III}(A/K) = \text{Ker}\left( H^1(G_K, A) \to \prod_v H^1(G_v, A_v) \right),$$

$$= \bigcap_v \text{Ker}\left( H^1(G_K, A) \to H^1(G_v, A_v) \right).$$

**Theorem 7.3.** With the above notations, we get the following facts:
(a) There is an exact sequence
\[ 0 \rightarrow B(K)/(f(A(K))) \rightarrow \text{Sel}^{(f)}(A/K) \rightarrow \Pi(A/K)[f] \rightarrow 0. \]

(b) The Selmer group \( \text{Sel}^{(f)}(A/K) \) is finite.

**Example 7.1.** Let \( A = B = E \) be an elliptic curve over \( K = \mathbb{Q} \) and let \( f = [m] \) be the multiplication by \( m \) endomorphism. Then we obtain the following exact sequence:
\[ 0 \rightarrow E(\mathbb{Q})/mE(\mathbb{Q}) \rightarrow \text{Sel}^{[m]}(E/\mathbb{Q}) \rightarrow \Pi(E/\mathbb{Q})[m] \rightarrow 0. \]

\( \text{Sel}_m := \text{Sel}^{[m]}(E/\mathbb{Q}) \) is called the \( m \)-Selmer group.

Any elliptic curve \( E \) over \( \mathbb{Q} \) is isomorphic to the unique cubic curve \( E_{A,B} \) in the plane of the form
\[ E_{A,B} : y^2 = x^3 + Ax + B, \]
where \( A, B \in \mathbb{Z} \) and for all primes \( p : p^3 \nmid A \) whenever \( p^2 \mid A \). Let \( \mathcal{E} \) be the set of all such \( E_{A,B} \). If \( E = E_{A,B} \in \mathcal{E} \), then we define the (naive) height of \( E \) by
\[ H(E_{A,B}) := \max\{4|A^3|, 27B^2\}. \]

For \( X \in \mathbb{R}_{>0} \), we define \( \mathcal{E}_{<X} := \{ E \in \mathcal{E} \mid H(E) < X \} \).

**Definition 7.4.** For any \( \phi : \mathcal{E} \rightarrow \mathbb{R} \), we define
\[ \text{Average}_{\mathcal{E}}(\phi)(\phi) = \text{Aver}_{\mathcal{E}}(\phi) := \lim_{X \to \infty} \frac{\sum_{E \in \mathcal{E}_{<X}} \phi(E)}{X}. \]

If the limit exists. Define \( \overline{\text{Aver}}_{\mathcal{E}}(\phi) \) and \( \underline{\text{Aver}}_{\mathcal{E}}(\phi) \) using limsup or liminf. If the property \( P \) can be identified with characteristic function \( \chi_P : \mathcal{E} \rightarrow \{0, 1\} \),
\[ \text{Prob}_{\mathcal{E}}(P) := \text{Average}(\chi_P). \]

Similarly we define \( \overline{\text{Prob}}_{\mathcal{E}}(P) \) and \( \underline{\text{Prob}}_{\mathcal{E}}(P) \).

Bhargava and Shankar \[1\] \[2\] \[3\] \[4\] proved the following results:

**Theorem 7.5** (Bhargava and Shankar).
- (1) \( \text{Aver}_{\mathcal{E}}(\#\text{Sel}_2) = 3 \). (cf. \[1\])
- (2) \( \text{Aver}_{\mathcal{E}}(\#\text{Sel}_3) = 4 \). (cf. \[2\])
- (3) \( \text{Aver}_{\mathcal{E}}(\#\text{Sel}_4) = 7 \). (cf. \[3\])
- (4) \( \text{Aver}_{\mathcal{E}}(\#\text{Sel}_5) = 6 \). (cf. \[4\])

**Corollary 7.6** (Bhargava and Shankar \[4\], 2013).
\[ \text{Aver}_{\mathcal{E}}(\text{rank}) \leq 0.885. \]

**Theorem 7.7** (T. Dokchitser - V. Dokchitser \[17\], 2010). Let \( E \) be an elliptic curve over \( \mathbb{Q} \) and let \( p \) be any prime. Let \( s_p(E) \) and \( t_p(E) \) denote the rank of the \( p \)-Selmer group of \( E \) and the rank of \( E(\mathbb{Q})[p] \), respectively. Then the quantity \( r_p(E) := s_p(E) - t_p(E) \) is even if and only if the root number of \( E \) is \( +1 \). Here we recall that \( s_p(E) \) and \( t_p(E) \) are defined as
\[ s_p(E) := \log_p(\#\text{Sel}_p(E)) \quad \text{and} \quad t_p(E) := \log_p(\#E(\mathbb{Q})[p]) \]
respectively.

Bhargava and Shanker \[4\] \[5\] proved the following:

**Theorem 7.8.**
- (1) \( \text{Prob}_{\mathcal{E}}(r = 0) \geq 0.2062 \). (cf. \[4\])
- (2) \( \text{Prob}_{\mathcal{E}}(r = 1) \geq 0.2612 \). (cf. \[4\])
(3) \( \text{Prob}_{\mathcal{E}}(r = 0 \text{ or } r = 1) \geq 0.8375. \) (cf. [4])
(4) \( \text{Prob}_{\mathcal{E}}(r = r_{an} = 0) \) is positive. (cf. [2])
(5) \( \text{Prob}_{\mathcal{E}}(r = r_{an} = 1) \) is positive. (cf. [5])

The results (4) and (5) in Theorem 7.8 imply that a positive proportion of \( \mathcal{E} \) satisfies the BSD conjecture.

Quite recently Bhargava, Elkies and Shnidman [6] computed the average size of the \( \phi_k \)-Selmer group as \( k \) varies over the integers, where \( \phi_k : E_k \to E_{-27k}, \quad E_k : y^2 = x^3 + k \) is a natural 3-isogeny.

8. Adjoint Orbits of \( SL(2, \mathbb{R}) \)

In this section, we describe the adjoint orbits of the special linear group \( SL(2, \mathbb{R}) \) explicitly.

For brevity, write \( G = SL(2, \mathbb{R}) \) and let \( K = SO(2) \) be a maximal compact subgroup of \( G \). The Lie algebra \( g \) of \( G \) is given by

\[
g = \left\{ \begin{pmatrix} x & y \\ z & -x \end{pmatrix} \mid x, y, z \in \mathbb{R} \right\}.
\]

We put \( X = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \)

Then the set \( \{X, Y, Z\} \) forms a basis for \( g \). We define an element \( F(x, y, z) \in g \) by

\[
F(x, y, z) := xX + yY + zZ = \begin{pmatrix} x & y + z \\ y - z & -x \end{pmatrix}.
\]

Then we have the relations

\[
X^2 + Y^2 - Z^2 = 3I_2, \quad [X, Y] = 2Z, \quad [X, Z] = 2Y, \quad [Y, Z] = -2X.
\]

It is easy to see that \( X \) and \( Y \) are hyperbolic elements and \( Z \) is an elliptic element. For a nonzero real number \( \alpha \), the \( G \)-orbit of \( \alpha X \) is represented by the one-sheeted hyperboloid

\[
x^2 + y^2 - z^2 = \alpha^2.
\]

The \( G \)-orbit of \( \alpha Y (\alpha \in \mathbb{R}^\times) \) is also represented by the hyperboloid [8,2]. The \( G \)-orbit of \( \alpha Z (\alpha \in \mathbb{R}^\times) \) is represented by two-sheeted hyperboloids

\[
x^2 + y^2 - z^2 = -\alpha^2.
\]

Since

\[
F(x, y, z)^2 = (x^2 + y^2 - z^2) \cdot I_2,
\]

we have for any \( k \in \mathbb{Z}^+, \)

\[
F(x, y, z)^{2k} = (x^2 + y^2 - z^2)^k \cdot I_2.
\]

Thus we see that \( F(x, y, z) \) is nilpotent if and only if \( x^2 + y^2 - z^2 = 0 \). Therefore the set \( \mathcal{N}_g \) of all nilpotent elements in \( g \) is given by

\[
\mathcal{N}_g = \left\{ F(x, y, z) = \begin{pmatrix} x & y + z \\ y - z & -x \end{pmatrix} \mid x^2 + y^2 - z^2 = 0 \right\}.
\]
We put
\begin{equation}
S = \frac{1}{2}(Y + Z) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad T = \frac{1}{2}(Y - Z) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.
\end{equation}

Obviously $S$ and $T$ are nilpotent elements in $\mathcal{N}_R$ and they satisfy
\begin{equation}
[X, S] = 2S, \quad [X, T] = -2T, \quad [S, T] = X
\end{equation}
and
\begin{equation}
\theta(X) = -X, \quad \theta(S) = -T, \quad \theta(T) = -S.
\end{equation}

where $\theta$ is the Cartan involution defined by $\theta(g) = -t g$ for $g$ in $g$.

According to equation (8.6) and (8.7), \{X, S, T\} and \{-X, -S, -T\} are KS-triples in $g$.

The $G$-orbit of $\alpha S$ ($\alpha \in \mathbb{R}^\times$) is represented by the cone
\begin{equation}
x^2 + y^2 - z^2 = 0, \quad (x, y, z) \neq (0, 0, 0)
\end{equation}
derpending on the sign of $\alpha$.

If $\alpha > 0$, the $G$-orbit of $\alpha S$ is characterized by the one-sheeted cone
\begin{equation}
x^2 + y^2 - z^2 = 0, \quad z > 0.
\end{equation}
If $\alpha < 0$, the $G$-orbit of $\alpha S$ is characterized by the one-sheeted cone
\begin{equation}
x^2 + y^2 - z^2 = 0, \quad z < 0.
\end{equation}
The $G$-orbits of $\alpha T$ ($\alpha > 0$) are characterized by the one-sheeted cone \begin{equation}(8.10)\end{equation} and the $G$-orbits of $\alpha T$ ($\alpha < 0$) are characterized by the one-sheeted cone \begin{equation}(8.9)\end{equation}.

We define the $G$-orbits $\mathcal{N}_R^+$ and $\mathcal{N}_R^-$ by
\begin{equation}
\mathcal{N}_R^+ = G \cdot S = \{gSg^{-1} \in \mathcal{N}_R \mid g \in G\}
\end{equation}
and
\begin{equation}
\mathcal{N}_R^- = G \cdot T = \{gTg^{-1} \in \mathcal{N}_R \mid g \in G\}.
\end{equation}
Then we obtain
\begin{equation}
\mathcal{N}_R = \mathcal{N}_R^+ \cup \{0\} \cup \mathcal{N}_R^-.
\end{equation}
According to (8.2), (8.3) and (8.13), we see that there are infinitely many hyperbolic orbits and elliptic orbits, and on the other hand there are only three nilpotent orbits in $g$.

9. Final Remarks

In the final section, we describe the relation between the nilpotent orbits of $SL(2, \mathbb{R})$ and CM points, and propose several conjectures relating to the BSD conjecture.

Let $G = SL(2, \mathbb{R})$ and let $g$ be the Lie algebra of $G$. Let $\mathcal{E}_R$, $\mathcal{H}_R$ and $\mathcal{N}_R$ be the set of all $G$-elliptic orbits in $g$, the set of all $G$-hyperbolic orbits in $g$, and the set of all $G$-nilpotent orbits in $g$ respectively. Let $\exp : g \rightarrow G$ be the exponential map and let $\phi : G \rightarrow \mathbb{H}$ be the map defined by
\begin{equation}
\phi(g) = \frac{ai + b}{ci + d}, \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G, \quad i = \sqrt{-1}.
\end{equation}
We define the composition map $\omega := \phi \circ \exp : g \rightarrow \mathbb{H}$.
Proposition 9.1.
\[ \omega(\mathcal{N}_R) = \mathbb{H}. \]

Proof. The proof can be found in [25].

First we recall the thirteen CM points
\[
\begin{align*}
\alpha_1 &= \frac{1+i\sqrt{3}}{2}, & \alpha_2 &= i, & \alpha_3 &= \frac{1+i\sqrt{7}}{2}, & \alpha_4 &= i\sqrt{2}, \\
\alpha_5 &= \frac{1+i\sqrt{11}}{2}, & \alpha_6 &= i\sqrt{3}, & \alpha_7 &= 2i, & \alpha_8 &= \frac{1+i\sqrt{19}}{2}, \\
\alpha_9 &= \frac{1+i\sqrt{27}}{2}, & \alpha_{10} &= i\sqrt{7}, & \alpha_{11} &= \frac{1+i\sqrt{43}}{2}, \\
\alpha_{12} &= \frac{1+i\sqrt{67}}{2}, & \alpha_{13} &= \frac{1+i\sqrt{163}}{2}.
\end{align*}
\]
We put \( q := e^{2\pi i \tau} \) (\( \tau \in \mathbb{H} \)). The \( q \)-expansion of the modular invariant \( j(\tau) \) is given by
\[
j(\tau) = q^{-1} + 744 + \sum_{n=1}^{\infty} c(n) q^n = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots.
\]
It is known that
\[
\begin{align*}
 j(\alpha_1) &= 0, & j(\alpha_2) &= 2^6\cdot3^3, & j(\alpha_3) &= -3^3\cdot5^3, & j(\alpha_4) &= 2^6\cdot5^3, \\
 j(\alpha_5) &= -2^{15}, & j(\alpha_6) &= 2^4\cdot3^3\cdot5^3, & j(\alpha_7) &= 2^3\cdot3^3\cdot11^3, & j(\alpha_8) &= -2^{15}\cdot3^3, \\
 j(\alpha_9) &= -2^{15}\cdot3^3\cdot5^3, & j(\alpha_{10}) &= 3^3\cdot5^3\cdot17^3, & j(\alpha_{11}) &= -2^{18}\cdot3^3\cdot5^3, \\
 j(\alpha_{12}) &= -2^{15}\cdot3^3\cdot5^3\cdot11^3, & j(\alpha_{13}) &= -2^{18}\cdot3^3\cdot5^3\cdot23^3\cdot29^3.
\end{align*}
\]

For any element \( \tau \in \mathbb{H} \), we let
\[
E_\tau := \mathbb{C}/\Lambda_\tau
\]
be the elliptic curve over \( \mathbb{C} \), where \( \Lambda_\tau := \mathbb{Z} + \mathbb{Z}\tau \) is the lattice in \( \mathbb{C} \).

For any \( g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \), we write
\[
g < \tau > := \frac{a\tau + b}{c\tau + d}, \quad \tau \in \mathbb{H}.
\]
Let
\[
\mathcal{O}_j := K < \alpha_j > := \{ k < \alpha_j > \mid k \in K \}, \quad 1 \leq j \leq 13
\]
be the \( K \)-orbit of \( \alpha_j \). Clearly \( \mathcal{O}_2 = \{ i \} \).

We propose the following conjecture.

Conjecture D. Let \( \tau \) be an element of \( \mathcal{O}_j \) (\( 1 \leq j \leq 13 \)) such that \( E_\tau \) is defined over \( \mathbb{Q} \). Then the BSD conjecture for \( E_\tau \) holds.

For any \( \alpha_j \) (\( j \neq 2, 1 \leq j \leq 13 \)), by Proposition 9.1, we can choose \( F(a_j, b_j, c_j) \in \mathcal{N}_R \) with \( c_j \neq 0 \). We define
\[
\mathcal{E}_j := \{ F(x, y, c_j) \in \mathcal{N}_R \mid x^2 + y^2 = c_j^2 \}, \quad j \neq 2, 1 \leq j \leq 13
\]
and
\[
\mathcal{X}_j := \omega(\mathcal{E}_j), \quad j \neq 2, 1 \leq j \leq 13.
\]
We also define
\[
\mathcal{D}_j := \{ F(x, b_j, z) \in \mathcal{N}_R \mid x^2 + b_j^2 = z^2 \}, \quad j \neq 2, 1 \leq j \leq 13
\]
We propose the following conjectures.

Conjecture E. Let \( \tau \) be an element of \( X_j (j \neq 2, 1 \leq j \leq 13) \) such that \( E_\tau \) is defined over \( \mathbb{Q} \). Then the BSD conjecture for \( E_\tau \) holds.

Conjecture F. Let \( \tau \) be an element of \( Y_j (j \neq 2, 1 \leq j \leq 13) \) such that \( E_\tau \) is defined over \( \mathbb{Q} \). Then the BSD conjecture for \( E_\tau \) holds.

Conjecture G. Let \( \tau \) be an element of \( Z_j (j \neq 2, 1 \leq j \leq 13) \) such that \( E_\tau \) is defined over \( \mathbb{Q} \). Then the BSD conjecture for \( E_\tau \) holds.

References

[1] M. Bhargava and A. Shankar, Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves, Annals of Mathematics 181, no. 1 (2015), 191–242.

[2] M. Bhargava and Arul Shankar, Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0, Annals of Mathematics 181, no. 2 (2015), 587–621.

[3] M. Bhargava and A. Shankar, The average number of elements in the 4-Selmer groups of elliptic curves is 7, arXiv:1312.7333v1 [math.NT] 27 Dec 2013.

[4] M. Bhargava and A. Shankar, The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1, arXiv:1401.0233v1 [math.NT] 1 Jan 2014.

[5] M. Bhargava and C. Skinner, A positive proportion of elliptic curves over \( \mathbb{Q} \) have rank 0, Annals of Mathematics 181, no. 1 (2015), 191–242.

[6] M. Bhargava, N. Elkies, and A. Shnidman, The average size of the 3-isogeny Selmer groups of elliptic curves \( y^2 = x^3 + k \), arXiv:1610.05759v1 [math.NT] 18 Oct 2016.

[7] B. Birch and H.P.F. Swinnerton-Dyer, Notes on elliptic curves (I), J. Reine Angew. Math. 212 (1963), 7–25.

[8] B. Birch and H.P.F. Swinnerton-Dyer, Notes on elliptic curves (II), J. Reine Angew. Math. 218 (1965), 79–108.

[9] R. Borchers, The Gross-Kohnen-Zagier theorem in higher dimensions, Duke Math. J. 97, no. 2 (1999), 219–233.

[10] B. Bump, S. Friedberg and J. Hoffstein, Nonvanishing theorems for L-functions of modular forms and their derivatives, Invent. Math. 102 (1990), 543–618.

[11] H.-D. Cao and X.-P. Zhu, Complete Proof of the Poincaré and geometrization conjectures-application of the Hamilton-Perelman theory of the Ricci flow, Asian Journal of Mathematics 10(4), 663AÂ–664.

[12] H.-D. Cao and X.-P. Zhu, Erratum to "A complete proof of the Poincaré and geometrization conjectures" application of the Hamilton-Perelman theory of the Ricci flow", Asian J. Math., Vol. 10, No. 2, 165–492, 2006, Asian Journal of Mathematics. 10(4), 663AÂ–664.

[13] J. Coates and A. Wiles, On the Birch-Swinnerton-Dyer conjecture Invent. Math. 39 (1977), 223–252.

[14] P. Deligne, Formes modulaires et représentations ℓ-adiques, Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Exp. No. 355, 139–172, Lecture Notes in Math., 175, Springer, Berlin (1971).

[15] P. Deligne and J.-P. Serre, Formes modulaires de poids 1, Ann. Sci. Ec. Norm. Sup., IV. Ser. 7 (1974), 507–530.

[16] T. Dokchitser - V. Dokchitser, On the Birch-Swinnerton-Dyer quotients modulo squares, Annals of Mathematics 172, no. 1 (2010), 567–596.

[17] M. Eichler and D. Zagier, The theory of Jacobi forms, Birkhäuser 55 (1985).

[18] B. Gross and D. Zagier, Heegner points and derivatives of L-series, Invent. Math. 84 (1986), 225–320.

[19] B. Gross, W. Kohnen and D. Zagier, Heegner points and derivatives of L-series. II, Math. Ann., 278 (1987), 497–562.

[20] B. Kleiner and J. Lott, Notes on Perelmanâ€™s papers, Geom. Topol 12.5(2008), 2587–2855.

[21] W. Kohnen, Modular forms of half integral weight on \( \Gamma_0 (4) \), Math. Ann. 248 (1980), 249–266.

[22] V. A. Kolyvagin, Finiteness of \( E(\mathbb{Q}) \) and \( \text{III}(E, \mathbb{Q}) \) for a subclass of Weil curves (Russian), Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), 522–540, 670–671; English translation in Math. USSR-Izv. 32 (1988), 523–541.
[24] V. A. Kolyvagin, *Euler systems, the Grothendieck Festschrift (vol. II)*, edited by P. Cartier and et al., Birkhäuser 87 (1990), 435-483.

[25] Y.-J. Kwon and J.-H. Yang, *Nilpotent Orbits of $SL(2,\mathbb{R})$ and Elliptic Curves with Complex Multiplication*, in preparation.

[26] H. Maass, *Über eine Spezialschar von Modulformen zweiten Grades I*, Invent. Math. 52 (1979), 95–104.

[27] H. Maass, *Über eine Spezialschar von Modulformen zweiten Grades II*, Invent. Math. 53 (1979), 249–253.

[28] H. Maass, *Über eine Spezialschar von Modulformen zweiten Grades III*, Invent. Math. 53 (1979), 255–265.

[29] B. Mazur, *Modular curves and the Eisenstein series*, Publ. IHES 47 (1977), 33-186.

[30] B. Mazur, *Number Theory as Gadfly*, Amer. Math. Monthly 98 (1991), 593–610.

[31] L. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Philos. Soc. (1922), pp. 179–192.

[32] J. Morgan, G. Tian, *Completion of Perelman’s proof of the geometrization conjecture*, arXiv:0809.4040

[33] J. Morgan, G. Tian, *Ricci flow and the Poincaré conjecture*, Clay Mathematics Monographs 3, Amer. Math. Soc. (2007).

[34] M. R. Murty and V. K. Murty, *Mean values of derivatives of modular $L$-series*, Ann. Math. 133 (1991), 447–475.

[35] G. Perelman, *The entropy formula for the Ricci flow and its geometric applications*, arXiv:math/0211159v1 [math.DG] 11 Nov 2002.

[36] G. Perelman, *Ricci flow with surgery on three-manifolds*, [arXiv:math/0303109v1 [math.DG]] 10 Mar 2003.

[37] K. Rubin, *Elliptic curves with complex multiplication and the BSD conjecture*, Invent. Math. 64 (1981), 455-470.

[38] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, Graduate Text in Math. 106 (1986).

[39] N.-P. Skoruppa and D. Zagier, *Jacobi forms and a certain space of modular forms*, Invent. Math. 94 (1988), 113–146.

[40] J.-H. Yang, *Remarks on Jacobi forms of higher degree*, Proceedings of the 1993 Conference on Automorphic Forms and Related Topics, edited by J.-W. Son and J.-H. Yang, Pyungsan Institute for Mathematical Sciences 1 (1993), 33–58.

[41] J.-H. Yang, *Note on Taniyama-Shimura-Weil conjecture*, Proceedings of the 1994 Conference on Number Theory and Related Topics, edited by J.-W. Son and J.-H. Yang, Pyungsan Institute for Mathematical Sciences 2 (1995 ), 29–46.

[42] J.-H. Yang, *Kac-Moody algebras, the Monstrous Moonshine, Jacobi Forms and Infinite Products*, Proceedings of the 1995 Symposium on Number Theory, Geometry and Related Topics, edited by J.-W. Son and J.-H. Yang, Pyungsan Institute for Mathematical Sciences 3 (1996), 13–82.

[43] J.-H. Yang, *Past twenty years of the theory of elliptic curves (Korean)*, Comm. Korean Math. Soc. 14 (1999), 449–477.

[44] J.-H. Yang, *The Birch-Swinnerton-Dyer Conjecture*, Proceedings of the 2002 International Conference on Related Subjects to Clay Problems, the Institute of Pure and Applied Mathematics, Cheonbuk National Univ., Jeonju, Korea, Vol. 1 (2002), 134–151 or arXiv:math/0611423v1 [math.HO] 14 Nov 2006.

[45] D. Zagier, *L-series of Elliptic Curves, the BSD Conjecture, and the Class Number Problem of Gauss*, Notices of AMS 31 (1984), 739–743.

Department of Mathematics, Inha University, Incheon 22212, Korea
E-mail address: jhyang@inha.ac.kr