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.

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 :

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.

Typeset by $\mathcal{AMS}$-TeX

In this paper, I 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 around 1960 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. Recently the Taniyama-Shimura conjecture stating that any elliptic curve defined over $\mathbb{Q}$ is modular was shown to be true by Breuil, Conrad, Diamond and Taylor [BCDT]. This fact shed some lights on the solution of the BSD conjecture. In the final section, 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. We would like to mention that we added the nicely written expository paper [W] of Andrew Wiles about the Birch-Swinnerton-Dyer Conjecture to the list of the references.

Notations : We denote by $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ the fields of rational numbers, real numbers and complex numbers respectively. $\mathbb{Z}$ and $\mathbb{Z}^+$ denotes the ring of integers and the set of positive integers respectively.

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

$$y^2 = f(x), \tag{2.1}$$

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 ∞ as an identity element. The set $E(\mathbb{Q})$ of rational points given by

$$E(\mathbb{Q}) = \left\{ (x, y) \in \mathbb{Q}^2 \mid y^2 = f(x) \right\} \cup \{\infty\} \tag{2.2}$$

also has an abelian group structure.

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

Theorem A (Mordell, 1922). $E(\mathbb{Q})$ is finitely generated, that is,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E_{\rm tor}(\mathbb{Q}),$$

where r is a nonnegative integer and $E_{\rm tor}(\mathbb{Q})$ is the torsion subgroup of $E(\mathbb{Q})$.

Definition 1. Around 1930, A. Weil (1906-1998) proved 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 variety 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-)[Ma1] discovered the structure of the torsion subgroup $E_{\rm tor}(\mathbb{Q})$ completely using a deep theory of elliptic modular curves.

Theorem B (Mazur, 1977). Let E be an elliptic curve defined over $\mathbb{Q}$. Then the torsion subgroup $E_{\rm tor}(\mathbb{Q})$ 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 C (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 $E_{\rm tor}(\mathbb{Q})$. Then

(a) $x_0, y_0 \in \mathbb{Z}$, and

(b) $2P = 0$ or $y_0^2 | (4a^3 + 27b^2)$.

We observe that the above theorem gives an effective method for bounding $E_{\rm tor}(\mathbb{Q})$. According to Theorem B and C, we know the torsion part of $E(\mathbb{Q})$ satisfactorily. But we have no idea of the free part of $E(\mathbb{Q})$ so far. As for the algebraic rank r of an elliptic curve E over $\mathbb{Q}$, it is known by J.-F. Mestre in 1984 that values as large as 14 occur. Indeed, the elliptic curve defined by

$$y^2 = x^3 - 35971713708112\,x + 85086213848298394000$$

has its algebraic rank 14.

Conjecture D. Given a nonnegative integer n, there is an elliptic curve E over $\mathbb{Q}$ with its algebraic rank n.

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

3. Modular Elliptic Curves

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

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

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

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

is a noncompact surface, and

$$X_0(N) = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}/\Gamma_0(N) \tag{3.1}$$

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 $|f(z)|^2 (\mathrm{Im}\, z)^k$ 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

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

For each prime $p \not| N$, 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 $c \equiv 0\,(N)$ and $d \equiv p\,(N)$. The Hecke operators T_p for $p \not| N$ 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 λ be a place of the algebraic closure $\bar{\mathbb{Q}}$ in $\mathbb{C}$ above a rational prime ℓ and $\bar{\mathbb{Q}}_\lambda$ denote the algebraic closure of $\mathbb{Q}_\ell$ considered as a $\bar{\mathbb{Q}}$-algebra via λ. It is known that if $f \in S_k(N)$, there is a unique continuous irreducible representation

$$\rho_{f,\lambda} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\bar{\mathbb{Q}}_\lambda) \tag{3.3}$$

such that for any prime $p \not| N\ell$, $\rho_{f,\lambda}$ is unramified at p and $\mathrm{tr}\, \rho_{f,\lambda}(\mathrm{Frob}_p) = a_p(f)$. The existence of $\rho_{f,\lambda}$ is due to G. Shimura (1930-) if $k = 2$ [Sh], to P. Deligne (1944-) if $k > 2$ [D] and to P. Deligne and J.-P. Serre (1926-) if $k = 1$ [DS]. Its irreducibility is due to Ribet if $k > 1$ [R], and to Deligne and Serre if $k = 1$ [DS]. Moreover $\rho_{f,\lambda}$ is odd and potentially semi-stable at ℓ in the sense of Fontaine. We may choose a conjugate of $\rho_{f,\lambda}$ which is valued in $GL_2(\mathcal{O}_{\bar{\mathbb{Q}}_\lambda})$, and reducing modulo the maximal ideal and semi-simplifying yields a continuous representation

$$\bar{\rho}_{f,\lambda} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\bar{\mathbb{F}}_\ell), \tag{3.4}$$

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

Definition 2. Let $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\bar{\mathbb{Q}}_\ell)$ be a continuous representation which is unramified outside finitely many primes and for which the restriction of ρ to a decomposition group at ℓ is potentially semi-stable in the sense of Fontaine. We call ρ *modular* if ρ is isomorphic to $\rho_{f,\lambda}$ for some eigenform f and some $\lambda|\ell$.

Definition 3. An elliptic curve E defined over $\mathbb{Q}$ is said to be *modular* if there exists a surjective holomorphic map $\varphi : X_0(N) \longrightarrow E(\mathbb{C})$ for some positive integer N.

Recently C. Breuil, B. Conrad, F. Diamond and R. Taylor [BCDT] proved that the Taniyama-Shimura conjecture is true.

Theorem E ([BCDT], 2001). An elliptic curve defined over $\mathbb{Q}$ is modular.

Let E be an elliptic curve defined over $\mathbb{Q}$. For a positive integer $n \in \mathbb{Z}^+$, we define the isogeny $[n] : E(\mathbb{C}) \longrightarrow E(\mathbb{C})$ by

$$[n]P := nP = P + \cdots + P \ (n \text{ times}), \quad P \in E(\mathbb{C}). \tag{3.5}$$

For a negative integer n, we define the isogeny $[n] : E(\mathbb{C}) \longrightarrow E(\mathbb{C})$ by $[n]P := -[-n]P,\ P \in E(\mathbb{C})$, where $-[-n]P$ denotes the inverse of the element $[-n]P$. And $[0] : E(\mathbb{C}) \longrightarrow E(\mathbb{C})$ denotes the zero map. For an integer $n \in \mathbb{Z}$, $[n]$ is called the multiplication-by-n homomorphism. The kernel $E[n]$ of the isogeny $[n]$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Let

$$\mathrm{End}(E) = \{\varphi : E(\mathbb{C}) \longrightarrow E(\mathbb{C}),\ \text{an isogeny}\}$$

be the endomorphism group of E. An elliptic curve E over $\mathbb{Q}$ is said to have *complex multiplication* (or CM for short) if

$$\mathrm{End}(E) \nsubseteq \mathbb{Z} \cong \{[n] |\ n \in \mathbb{Z}\},$$

that is, there is a nontrivial isogeny $\varphi : E(\mathbb{C}) \longrightarrow E(\mathbb{C})$ such that $\varphi \neq [n]$ for all integers $n \in \mathbb{Z}$. Such an elliptic curve is called a CM *curve*. For most of elliptic curves E over $\mathbb{Q}$, we have $\mathrm{End}(E) \cong \mathbb{Z}$.

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:

$$L(E,s) = \prod_{p|\Delta_E} (1 - a_p p^{-s})^{-1} \cdot \prod_{p\nmid\Delta_E} (1 - a_p p^{-s} + p^{1-2s})^{-1}, \tag{4.1}$$

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

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

and if $p|\Delta_E$, we set $a_p := 0,\ 1,\ -1$ if the reduced curve $\bar{E}/\mathbb{F}_p$ has a cusp at p, a split node at p, and a nonsplit node at p respectively. Then $L(E,s)$ converges absolutely for $\mathrm{Re}\, s > \frac{3}{2}$ 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 $\bar{E}(\mathbb{F}_p)$ by $(x,y) \mapsto (x^p, y^p)$.

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

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

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 Taniyama-Shimura 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 ℓ, we let $\rho_{E,\ell}$ (resp. $\bar{\rho}_{E,\ell}$) denote the representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the ℓ-adic Tate module (resp. the ℓ-torsion) of $E(\bar{\mathbb{Q}})$. 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 ℓ, the representation $\rho_{E,\ell}$ is modular.

(4) For all primes ℓ, the representation $\rho_{E,\ell}$ is modular.

(5) There is a non-constant holomorphic map $X_0(N) \longrightarrow E(\mathbb{C})$ for some positive integer N.

(6) There is a non-constant morphism $X_0(N(E)) \longrightarrow E$ which is defined over $\mathbb{Q}$.

(7) E admits a hyperbolic uniformization of arithmetic type (cf. [Ma2] and [Y1]).

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 $x, y \pmod p$ satisfying (2.1) as a congruence (mod p). Then the BSD conjecture in its crudest form says that we should have an asymptotic formula

$$\prod_{p<x} \frac{N(p)+1}{p} \sim C \ (\log p)^r \quad \text{as } x \longrightarrow \infty \tag{5.1}$$

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

$$c_0 = \lim_{s\to 1} \frac{L(E,s)}{(s-1)^m} = \alpha \cdot R \cdot |E_{\text{tor}}(\mathbb{Q})|^{-1} \cdot \Omega \cdot S, \tag{5.2}$$

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 $E(\mathbb{Q})$, Ω is a simple rational multiple (depending on the bad primes) of the elliptic integral

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

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

The Tate-Shafarevich group $\text{III}(E)$ of E is a very intersting subject to be investigated in the future. Unfortunately $\text{III}(E)$ 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 G. The Tate-Shafarevich group $\text{III}(E)$ of E is finite.

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

Result 1 (Coates-Wiles [CW], 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 [R], 1981). Let E be a CM curve over $\mathbb{Q}$. Assume that the analytic rank of E is zero. Then the Tate-Shafarevich group $\text{III}(E)$ of E is finite.

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

$$\tilde{E} \ : \quad -139\, y^2 = x^3 + 10\, x^2 - 20\, x + 8$$

satisfies the above property.

Result 5 (Kolyvagin [K], 1990 : Gross-Zagier [GZ], 1986 : Bump-Friedberg-Hoffstein [BFH], 1990 : Murty-Murty [MM], 1990 : [BCDT], 2001). Let E be an elliptic curve over $\mathbb{Q}$. Assume that the analytic rank of E is 1 and $\epsilon = -1$. Then algebraic rank of E is equal to 1.

Result 6 (Kolyvagin [K], 1990 : Gross-Zagier [GZ], 1986 : Bump-Friedberg-Hoffstein [BFH], 1990 : Murty-Murty [MM], 1990 : [BCDT], 2001). Let E be an elliptic curve over $\mathbb{Q}$. Assume that the analytic rank of E is zero and $\epsilon = 1$. 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 th e BSD conjecture holds for E'.

6. Jacobi Forms and Heegner Points

In this section, I shall describe the result of Gross-Kohnen-Zagier [GKZ] 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 $\phi(z, w)$ ($z \in \mathbb{H}$, $z \in \mathbb{C}$) satisfying the transformation formula

$$\begin{aligned} \phi\left(\frac{az+b}{cz+d}, \frac{w+\lambda z+\mu}{cz+d}\right) =& e^{-2\pi i\left\{cm(w+\lambda z+\mu)^2(cz+d)^{-1}-m(\lambda^2 z+2\lambda w)\right\}} \\ & \times (cz+d)^k \, \phi(z,w) \end{aligned} \tag{6.1}$$

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

$$\phi(z,w) = \sum_{\substack{n,r\in\mathbb{Z}^2 \\ r^2\leq 4mn}} c(n,r)\, e^{2\pi i(nz+rw)}. \tag{6.2}$$

We remark that the Fourier coefficients $c(n, r)$ depend only on the discrimnant $D = r^2 - 4mn$ 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

$$[\Gamma_2, k]^M \cong J_{k,1}(\Gamma_1) \cong M^+_{k-\frac{1}{2}}(\Gamma_0(4)) \cong [\Gamma_1, 2k-2], \tag{6.3}$$

where Γ_2 denotes the Siegel modular group of degree 2, $[\Gamma_2, k]^M$ denotes the Maass space introduced by H. Maass (1911-1993) (cf. [M1-3]), $M^+_{k-\frac{1}{2}}(\Gamma_0(4))$ denotes the Kohnen space introduced by W. Kohnen [Koh] and $[\Gamma_1, 2k-2]$ denotes the space of modular forms of weight $2k-2$ with respect to Γ_1. We refer to [Y1] and [Y3], 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 [SZ], 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 [BCDT], E is modular and hence one has a surjective holomorphic map $\phi_E : X_0(N) \longrightarrow E(\mathbb{C})$. 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 Θ be the set of all $z \in \mathbb{H}$ satisfying the following conditions

$$az^2 + bz + c = 0, \quad a, b, c \in \mathbb{Z},\ N|a,$$
$$b \equiv r \pmod{2N}, \qquad D = b^2 - 4ac.$$

Then Θ is invariant under the action of $\Gamma_0(N)$ and Θ 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 $\phi_E(z_1), \cdots, \phi_E(z_{h_K})$ 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

$$P_{D,r} = \sum_{i=1}^{h_K} \phi_E(z_i). \tag{6.4}$$

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

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

$$E^{(D)} \ : \ Dy^2 = f(x). \tag{6.5}$$

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 H (Gross-Zagier [GZ], 1986 ; [BCDT], 2001). Let E be an elliptic curve of conductor N such that $\epsilon = -1$. Assume that D is odd. Then

$$L'(E, 1)\, L(E^{(D)}, 1) = c_E\, u^{-2}\, |D|^{-\frac{1}{2}}\, \hat{h}(P_{D,r}), \tag{6.6}$$

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 [BCDT], 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 obtained the following result.

Theorem I (Gross-Kohnen-Zagier, [GKZ] ; BCDT], 2001). Let E be a modular elliptic curve with conductor N and suppose that $\epsilon=-1,\ r=1$. Suppose that $(D_1,D_2)=1$ and $D_i\equiv r_i^2 \,(\mathrm{mod}\, 4N)\ (i=1,2)$. 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 [Y4] and [Z] for more details.

Corollary. There is a point $P_0\in E(\mathbb{Q})\otimes_{\mathbb{Z}}\mathbb{R}$ such that

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

for all D and $r\,(D\equiv r^2\,(\mathrm{mod}\,4N))$ 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 4. R. Borcherds [B] 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 $1+\frac{b}{2}$.

References

[**BSD1**] B. Birch and H.P.F. Swinnerton-Dyer, *Notes on elliptic curves (I)*, J. Reine Angew. Math. **212** (1963), 7-25.

[**BSD2**] B. Birch and H.P.F. Swinnerton-Dyer, *Notes on elliptic curves (II)*, J. Reine Angew. Math. **218** (1965), 79-108.

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

[**BCDT**] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$, Journal of AMS **109** (2001), 843-939.

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

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

[**EZ**] M. Eichler and D. Zagier, *The theory of Jacobi forms*, vol. 55, Birkhäuser, 1985.

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

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

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

[**K1**] V. A. Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and* $III(E,\mathbb{Q})$ *for a subclass of Weil curves (Russian)*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), 522-54 ; English translation in Math. USSR-IZv. **32** (1980), 523-541.

[**K2**] ———, *Euler systems, the Grothendieck Festschrift (vol. II), edited by P. Cartier and et al*, Birkhäuser **87** (1990), 435-483.

[**M1**] H. Maass, *Über eine Spezialschar von Modulformen zweiten Grades I*, Invent. Math. **52** (1979), 95-104.

[**M2**] H. Maass, *Über eine Spezialschar von Modulformen zweiten Grades II*, Invent. Math. **53** (1979), 249-253.

[**M3**] H. Maass, *Über eine Spezialschar von Modulformen zweiten Grades III*, Invent. Math. **53** (1979), 255-265.

[**Ma1**] B. Mazur, *Modular curves and the Eisenstein series*, Publ. IHES **47** (1977), 33-186.

[**Ma2**] ———, *Number Theory as Gadfly*, Amer. Math. Monthly **98** (1991), 593-610.

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

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

[**S**] J.H. Silvermann, *The Arithmetic of Elliptic Curves*, vol. Graduate Text in Math. 106, Springer-Verlag, 1986.

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

[**W**] A. Wiles, *The Birch and Swinnerton-Dyer Conjecture*, The Millennium Prize Problems, edited by J. Carlson, A. Jaffe and A. Wiles, Clay Mathematics Institute, American Mathematical Society (2006), 29-41.

[**Y1**] 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.

[**Y2**] ———, *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.

[**Y3**] ______, *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.

[**Y4**] ______, *Past twenty years of the theory of elliptic curves (Korean)*, Comm. Korean Math. Soc. **14** (1999), 449-477.

[**Z**] 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 402-751
Republic of Korea

email : jhyang@inha.ac.kr