Current Developments in Mathematics, 2001
Pages 179 – 219

Elliptic curves, L-functions, and CM-points

Shou-Wu Zhang

CONTENTS

Introduction

The aim of this note is to give a survey on recent development of the Gross-Zagier formulas and their applications. The formulas relate the central derivatives (or central values) of certain L-series and the heights (or periods) of so called CM points on Shimura varieties. The applications include the Birch and Swinnerton-Dyer conjecture for modular elliptic curves and the Andre-Oort conjecture for quaternion Shimura varieties.

Historically, the CM-points on modular curves were first used by Heegner [**43**] in his work on the class number problem for imaginary quadratic fields. Their significance in the arithmetic of the Jacobians of modular curves was first recognized by Birch. In [**5, 59**], these CM-points were used by Birch and Mazur to construct rational points of infinite order in the Jacobians. In [**6**], these points were studied numerically by Birch and Stephens who derived, on the basis of extensive numerical evidence, a number of striking conjectures relating these points to the behavior of related Rankin L-series. These conjectures were proved, almost before they could be precisely stated, in a landmark work of Gross and Zagier [**40**]. The work of Gross and Zagier has a number of striking applications:

1. The existence of the modular elliptic curve E over $\mathbb{Q}$ whose L-function $L(s, E)$ vanishes to order at least 3 at $s = 1$. This provides the basis of Goldfeld's solution [**33**] of the celebrated Gauss class number problem.

2. The criterion for the Heegner point on modular elliptic curve to be of infinite order in terms of L-functions. This has been used by Kolyvagin [**53**] to prove the rank-order equality predicted by the Birch and Swinnerton-Dyer conjecture when the order of vanishing is less than or equal to 1.

In [**35**], Gross proposed a program to extend the Gross-Zagier formula to modular abelian varieties of GL_2 type over totally real fields with anticyclotomic characters. On the other hand, in [**60**], Mazur discussed various questions and conjectures involving CM points, p-adic heights, and two-variable p-adic L-functions attached to elliptic curves. The present note will mainly focus on the recent progress in programs outlined by Gross and Mazur, including work of Vatsal and Cornut on nonvanishing of Heegner points and Heegner periods, and work of Bertolini and Darmon on Euler systems for anti-cyclotomic $\mathbb{Z}_p$-extensions. In the following we will discuss the details of the content of this paper.

The first four sections of the paper provide the standard background about elliptic curves and L-series. We will start with elliptic curves defined by Weierstrass equations, and address two arithmetic questions: to compute the Mordell Weil group (Lang's conjecture) and to bound the discriminant in terms of the conductor (Szpiro's conjecture). Then we assume that the L-series of elliptic curves have good analytic properties as predicted by the generalized Taniyama-Shimura conjecture. In other words, we always work on modular elliptic curves (or more generally, abelian varieties of GL_2-type). Of course, over $\mathbb{Q}$, such a conjecture has been proved recently by Wiles and completed by Taylor, Diamond, Conrad, and Brueil. Both arithmetic questions addressed earlier have their relation with L-series: the rank of the Mordell-Weil group is equal to the order of vanishing of L-series at the center (by the Birch and Swinnerton-Dyer conjecture); the discriminant is essentially the degree of the strong modular parameterization. The theory of complex multiplications then provides many examples of modular elliptic curves and abelian varieties of GL_2-type, and the foundation for the theory of Shimura varieties.

The next two sections contain basic facts about Shimura curves, CM-points, and the Gross-Zagier formula for central derivatives. In particular we define Shimura curves of type (N, K) as substitutions (over totally real fields) of modular curves $X_0(N)$ considered by Gross and Zagier. All quotients of the Jacobians of such curves are abelian varieties of GL_2-type. Conjecturally, all abelian varieties of conductor N of GL_2-type over totally real fields F are parameterized by these curves if either $[F : \mathbb{Q}]$ is odd or N is not a square. Kolyvagin's work can also be generalized in this case to obtain the BSD conjecture when L-series have minimal vanishing allowed by sign.

The last two sections are devoted to study the Birch and Swinnerton-Dyer conjecture for L-series twisted by characters. We start with Goldfeld's conjecture about the average rank of quadratic twists, and Mazur's philosophy on the nonvanishing of L-series when characters are unramified outside a fixed finite set of places. Then we come to the Gross-Zagier formula in this general setting which gives an interplay between vanishing of L-series and vanishing of CM-points.

In the classical case, many non-vanishing analytic results have been proved directly by Waldspurger, Bump-Friedberg-Hoffstein, Murty and Murty for quadratic

characters, and by Rohrlich for cyclotomic characters. Very recently, the non-vanishing in anticyclotomic case can be proved indirectly by Vatsal and Cornut using equidistribution of Heegner points (or periods).

Another interesting application of the central value formula is the equidistribution of the *toric orbits* of CM-points on quaternion Shimura varieties which has a direct relation to the Andre-Oort conjecture. Here the recent result of Cogdell, Piatetski-Shapiro, and Sarnak on sub-convexity bound of the central value plays a central rule. It should be mentioned that our central value formula should be considered as a continuation of the previous work of many authors including Waldspurger, Kohnen-Zagier, Katok-Sarnak, and Gross.

This paper grew out of notes for lectures I gave at the Columbia University, the Morningside Center of Mathematics in Chinese Academy of Sciences, and the joint conference of Harvard-MIT on current development of mathematics. I would like to thank the auditors for their interests and suggestions. My special gratitude is due to Ye Tian and Ran An for taking notes. I would also like to thank Goldfeld and Yau for their advice and encouragement.

1. Elliptic curves: geometry

In this section, we review the standard facts about the geometry of elliptic curves. The basic reference are books by Hartshorne [**42**], and Katz-Mazur [**50**], and Silverman [**77**]. We will discuss Weierstrass equations, j-invariants, twists, level structures, and complex realizations.

Weierstrass equation. By an *elliptic curve* over a field F, we mean a smooth and projective curve E over F of genus 1 with a fixed F-rational point O. Then E has a unique algebraic group structure with unit element O.

It is well known that E can be embedded into $\mathbb{P}^2$ as a cubic curve defined by a so called *Weierstrass equation*:

$$E: \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1}$$

The origin O corresponds to the point at infinity $(x : y : z) = (0 : 1 : 0)$ of the curve. Different Weierstrass equations are related by transformations:

$$x \longrightarrow u^3x + v, \qquad y \longrightarrow u^2y + \alpha x + \beta \tag{1.2}$$

with $u, v, \alpha, \beta \in F$. The group law on the set $E(F)$ of rational points over F (or more generally, any extension of F) is defined by

$$P + Q + R = 0 \tag{1.3}$$

if P, Q, R are colinear.

Case where $\mathrm{char}(F) \neq 2, 3$. In this case, E can be defined by a simpler Weierstrass equation like

$$y^2 = x^3 + ax + b, \qquad \Delta := 4a^3 + 27b^3 \neq 0. \tag{1.4}$$

The numbers a and b are completely determined by E up to transformations:

$$a \longrightarrow au^4, \qquad b \longrightarrow bu^6 \tag{1.5}$$

with $u \in F^\times$. Thus the set of isomorphic classes of elliptic curves over F is identified with the open subset of F^2 of pairs (a, b) such that $\Delta \neq 0$ modulo the action of $F^\times$

defined in (1.5). The group law can be described as follows: for two distinct points $P = (x, y)$ and $P' = (x', y')$, the x-coordinate of $P + Q = (x'', y'')$ is given by

$$x'' = \left(\frac{y' - y}{x' - x}\right)^2 - x - x'. \tag{1.6}$$

Taking the limit as $P' \longrightarrow P$ we obtain the x-coordinates of $2P = (x'', y'')$:

$$x'' = \frac{(3x^2 + a)^2}{4x^3 + 4ax + 4b} - 2x. \tag{1.7}$$

j-invariant and classification. For every elliptic curve E, there is a well defined j-invariant $j(E) \in F$ such that two elliptic curves have the same j-invariants if and only if they are isomorphic over the algebraic closure $\bar{F}$ of F. If E is given by equation (1.1), then j is a rational function of the coefficients. When the characteristic of F is not $2, 3$ and E is given by equation (1.4), we have an expression

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}. \tag{1.8}$$

Conversely, for any given $j \in F$, there is an elliptic curve with invariant j. In other words, the set of isomorphic classes of elliptic curves is identified with F when F is algebraically closed. Moreover, one can show that the coarse moduli of elliptic curves is identified with the affine line $\mathbb{A}^1$ over $\mathrm{Spec}\mathbb{Z}$. In other words, for an elliptic curve E over an arbitrary base scheme S, by which we mean a smooth and projective morphism $E \longrightarrow S$ with a fixed section O such that each fiber is of genus 1, the j-invariant $j(E)$ defines an element in $\Gamma(\mathcal{O}_S)^\times$.

But the affine line $\mathbb{A}^1$ is not a fine moduli space of elliptic curves over F even when F is algebraically closed, in the sense that there is a universal elliptic curve $\mathcal{E}$ over $\mathbb{A}^1_F$ such that for any elliptic curve E/S, E is isomorphic to the pull-back $j^*\mathcal{E}$ via the j-invariant map. The main problem is that elliptic curves have non-trivial automorphisms -1.

Twists. For general F, j does not even determine E up to isomorphism. We call two elliptic curves over F *twists* of each other, if they have the same j-invariants. In fact, the set of twists of a given elliptic curve E, is bijective to $H^1(G_F, \mathrm{Aut}(E_{\bar{F}})$ where $G_F = \mathrm{Gal}(\bar{F}/F)$. In the following we write this set more precisely in the case where $\mathrm{char}(F) \neq 2, 3$ where E can be defined by an equation (1.4).

If $j(E) \neq 0, 1728$, by equation (1.5), all twists are given by

$$E^{(d)}: \qquad dy^2 = x^3 + ax + b.$$

In Weierstrass equation form it is given by

$$E^{(d)}: \qquad y^2 = x^3 + ad^2x + bd^3.$$

Two twists $E^{(d)}$ and $E^{(d')}$ are isomorphic over F if and only if d/d' is a square over F.

If $j(E) = 0$, then twists are given by equation

$$E_{(d)}: \quad y^2 = x^3 + d$$

where $d \in F^\times$. Two twists $E_{(d)}$ and $E_{(d')}$ are isomorphic if and only if d/d' is a sixth power in F.

Similarly, if $j(E) = 1728$, then twists are given by equation

$$E_{(d)}: \quad y^2 = x^3 + dx$$

where $d \in F^\times$. Two twists $E_{(d)}$ and $E_{(d')}$ are isomorphic if and only if d/d' is a fourth power in F.

Level structure. To obtain the right moduli space of elliptic curves, one introduces the level structures. Let N be a positive integer. By a full-level structure on an elliptic curve E over a base S, we mean an isomorphism of group schemes

$$\phi: \qquad (\mathbb{Z}/N\mathbb{Z})^2_S \longrightarrow E[N]$$

where $(\mathbb{Z}/N\mathbb{Z})^2_S$ denotes the constant group scheme with fiber $(\mathbb{Z}/N\mathbb{Z})^2$ and $E[N]$ denote the subscheme of E of N-torsion points. In other words, a full level N-structure on E is a pair of two N-torsion points

$$P = \phi(1,0), \qquad Q = \phi(0,1)$$

of $E(S)$ which are linearly independent over $\mathbb{Z}/N\mathbb{Z}$. The Weil pairing of a full level N-structure will give a root of unity

$$\zeta_N = \langle P, Q\rangle \in \mu_N(S)$$

of order N over each geometric fiber at a point. Thus the existence of a full level N-structure implies that N is invertible over S. One can show that when $N \geq 3$, the fine moduli space of elliptic curves with full level N-structure exists over $\mathrm{Spec}\mathbb{Z}[1/N]$. This means that there is an elliptic curve $\mathcal{E}_N \longrightarrow \mathcal{M}_N$ over a $\mathbb{Z}[1/N]$ scheme $\mathcal{M}_N$ with a full level N-structure $(\mathcal{P}, \mathcal{Q})$ such that for any scheme S, the set

$$\{(f^*(\mathcal{E}_N), f^*(\mathcal{P}), f^*(\mathcal{Q})), \qquad f \in \mathcal{M}_N(S)\}$$

are representatives of isomorphic classes of elliptic curves over S with full level N-structure. Let ζ_N be the Weil pairing of $\mathcal{P}$ and $\mathcal{Q}$. Then $\mathcal{M}_N$ has a natural morphism to $\mathrm{Spec}\mathbb{Z}[1/N, \zeta_N]$. One can show that the last morphism has smooth and connected fibers.

Cases where $k = \mathbb{C}$. For an elliptic curve E defined over $\mathbb{C}$, the set of complex points $E(\mathbb{C})$ is a complex torus. More precisely the integration on $E(\mathbb{C})$ of the form dx/y will define an isomorphism

$$E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$$

where Λ is the group of periods of dx/y over loops of $E(\mathbb{C})$. Conversely, for any torus $\mathbb{C}/\Lambda$, there is an embedding

$$\mathbb{C}/\Lambda \longrightarrow \mathbb{P}^2, \qquad z \longrightarrow (\wp(z), \wp'(z), 1)$$

where $\wp(z)$ is the following Weierstrass $\wp$-function:

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda\in\Lambda,\lambda\neq 0} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right).$$

The image of this embedding is an elliptic curve with equation

$$y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$$

where $G_{2k}(\Lambda)$ is defined by

$$G_{2k}(\Lambda) = \sum_{\lambda\in\Lambda,\lambda\neq 0} \frac{1}{\lambda^{2k}}.$$

Thus, the study of complex elliptic curves up to isomorphisms is identical to that of the complex torus, and to that of lattices in $\mathbb{C}$. For example one can show

that every elliptic curve E is isomorphic to $E_\tau := \mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau$ with τ in the upper-half plane

$$\mathcal{H} = \{z \in \mathbb{C}, \mathrm{Im}\, z > 0\},$$

and uniquely determined up to the following action by $\mathrm{SL}_2(\mathbb{Z})$:

$$\gamma\tau = \frac{a\tau + b}{c\tau + d}, \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Thus, the coarse moduli of elliptic curves is also identified with $\mathrm{SL}_2(\mathbb{R})\backslash\mathcal{H}$. The j-invariant defines a map $\mathrm{SL}_2(\mathbb{R})\backslash\mathcal{H} \longrightarrow \mathbb{C}$ which is continuous, bijective, and holomorphic except when $j = 0, 1728$.

Moreover, for a positive integer N and a primitive root ζ_N in $\mathbb{C}$, every elliptic curve over $\mathbb{C}$ with full level N structure with Weil pairing ζ_N is isomorphic to E_τ with full level structure given by

$$P = 1/N, \quad Q = \tau/N, \qquad \mathrm{mod}\ \mathbb{Z} + \mathbb{Z}\lambda,$$

where τ is unique up to the action by

$$\Gamma(N) := \ker(\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})).$$

Thus the moduli of elliptic curves with full level N-structure is identified with

$$\mu_N^* \times \Gamma(N)\backslash\mathcal{H}$$

where μ_N^* is the set of N-th primitive roots of unity.

2. Elliptic curves: arithmetic

In this section, we want to study the arithmetic structure of elliptic curves. The basic references are Silverman's books [**77, 78**]. We will start with the Mordell-Weil theorem, and its sketched proof, and question of computing its generators: Lang's conjecture. The torsion part has been uniformly bounded by the work of Mazur and Merel. Then we come to the question of integral models and Faltings' theorem on finiteness of elliptic curves with bounded bad reductions. The effective form of this theorem is given by Szpiro's conjecture which has a lot of consequences including the abc-conjecture and new proved Fermat last theorem. The section will end up by introducing the Selmer group, the Tate-Shafarevich group, and the Goldfeld-Szpiro conjecture.

Let E be an elliptic curve defined over a number field F. One of the main objects of study of modern number theory is the group $E(F)$ of rational points on E. Its structure is given by the Mordell-Weil theorem which was conjectured by Poincaré when $F = \mathbb{Q}$:

THEOREM 2.1 (Mordell-Weil). *The group $E(F)$ is finitely generated. Thus one has an isomorphism*

$$E(F) \simeq \mathbb{Z}^r \oplus E(F)_{tor}$$

where r is a nonnegative integer.

In the following we want to describe the proof of the Mordell-Weil theorem which will be useful for the further discussion of the Birch and Swinnerton-Dyer conjecture. The proof uses *infinite decent*, a technique used in Fermat's own proof of his last theorem for the exponent 4. In our case, this technique is a combination of Kummer's theory and Neron-Tate height theory. More precisely, the proof has two steps:

1. Weak Mordell-Weil Theorem: For any positive integer m, the group $E(F)/mE(F)$ is finite.
2. There is a quadratic function

$$\|\cdot\|: \quad E(F) \longrightarrow \mathbb{R}$$

such that for any number C, the set

$$E(F)_C := \{P \in E(F): \quad \|P\| < C\}$$

is finite.

These two steps will imply that $E(F)$ is generated by any finite set $E(F)_C$ when it contains a set of representatives of $E(F)/2E(F)$.

Weak Mordell-Weil. For the first step, we fix an open subscheme U of $\mathrm{Spec}\mathcal{O}_F$ such that

1. m is invertible on U, and
2. E has smooth model E_U over U.

Let $G_U = \mathrm{Gal}(F_U/F)$ be the Galois group of the maximal extension of F unramified over U. Then we have exact sequences

$$0 \longrightarrow E[m] \longrightarrow E(F_U) \xrightarrow{m\cdot} E(F_U) \longrightarrow 0,$$

$$0 \longrightarrow E(F)/mE(F) \longrightarrow H^1(G_U, E[m]) \longrightarrow H^1(G_U, E(F_U))[m] \longrightarrow 0.$$

Now the Weak Mordell theorem follows from the fact that $H^1(G_U, E[m])$ is finite.

Heights. For the second step, we use a Weierstrass equation to get a projection

$$x: E \longrightarrow \mathbb{P}^1.$$

On $\mathbb{P}^1(F)$ we define a height function by

$$h(a,b) = \sum_v \log \max(|a|_v, |b|_v)$$

where v runs through the set of places of F and $|\cdot|_v$ is an absolute value on the completion F_v such that $d(ax) = |a|_v dx$ for any Haar measure on F_v. For any $P \in E(F)$, we define $h(P) = h(x(P))$. Then one can show that for any P,

$$h(2P) = 4h(P) + O(1)$$

where $O(1)$ denotes a bounded function on $E(F)$. It follows that the following limit

$$\lim_{n\to\infty} 4^{-n} h(2^n P)$$

converges and defines a quadratic norm $\widehat{h}$ on $E(F)$. The function we need for step 2 is then

$$\|P\| = \widehat{h}(P)^{1/2}.$$

Effectivity. The theorem gives a beautiful description about the structure of $E(F)$. However, its proof does not provide an effective way to find all solutions, even though people believe there should be one as the following conjecture predicts:

CONJECTURE 2.2 (Lang [**57**]). *Let E be an elliptic curve defined over a number field F of rank r. Then there exists a basis $P_1, \cdots, P_r$ for the free part of $E(F)$ satisfying*

$$\widehat{h}(P) \leq C_{\epsilon,F} \mathrm{N}_{F/\mathbb{Q}}(\Delta_E)^{1/2+\epsilon}$$

for all $1 \leq i \leq r$. Here Δ_E is the minimal discriminant (explained later), $C_{\epsilon,F}$ is a constant depends on F and ϵ.

Of course, the subgroup of torsion points $E(F)_{\mathrm{tor}}$ can be found easily. Actually it has a uniform bound by the following very deep result of Mazur and Merel:

THEOREM 2.3 (Mazur-Merel, [**62**]). *The subgroup $E(F)_{tor}$ has order bounded in terms of $[F : \mathbb{Q}]$.*

When $F = \mathbb{Q}$, Mazur even proved that $\#E(\mathbb{Q})_{\mathrm{tor}} \leq 16$.

Integral models. Let $S = \mathrm{Spec}\mathcal{O}_F$. Then E can be extended to a scheme E_S over S such that E_S is regular and E_S is minimal with respect to this property. The morphism $E_S \longrightarrow S$ may be singular but the smooth part E'_S of E_S carries a group structure which is called the Neron model of E. A precise way to get E_S is to blow-up an extension $\widetilde{E}_S$ of E by a Weierstrass equation with coefficients in $\mathcal{O}_F$ with minimal discriminant ideal Δ. Thus E_s is singular if and only if $\mathrm{ord}_s(\Delta) > 0$. One has the following well known result:

THEOREM 2.4 (Faltings [**25**]). *For any finite set Σ of primes in $\mathcal{O}_F$, there are only finitely many elliptic curves with good reduction outside of Σ.*

An elliptic curve E over F is called semistable, if all the singularities in the minimal model are ordinary double points. Let N_E be the conductor of E. In this case, N is simply the product of primes appearing in Δ. Then we have the following famous conjecture

CONJECTURE 2.5 (Szpiro [**81**]). *For any positive constant ϵ, there is a constant $C_{\epsilon,F}$ such that for any semistable elliptic curve E over F,*

$$\mathrm{N}(\Delta_E) \leq C_{\epsilon,F} \mathrm{N}(N_E)^{6+\epsilon}.$$

It is known that this conjecture implies the abc-conjecture, and Fermat's last theorem recently proved by Wiles.

To get a better understanding of the Mordell-Weil group, one must also look at the set of solutions at local fields $E(F_v)$. When $F_v \simeq \mathbb{C}$, this group is a complex torus described in the last section. When $F_v \simeq \mathbb{R}$, $E(F_v)$ is isomorphic to $\mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ depending on whether $E[2](\mathbb{R})$ has 2 or 4 points.

Local points. Now let v be a nonarchimedean place of F. Let F_v denote the completion of F at v and let k_v denote the residue field at v. Then we have an exact sequence of the reduction map

$$0 \longrightarrow E^0(F_v) \longrightarrow E(F_v) = E_S(\mathcal{O}_F) \longrightarrow E_S(k_v) \longrightarrow 0,$$

where $E^0(F_v)$ is the subgroup of $E(F_v)$ reduced to O at the special fiber. Since E_S is regular, the kernel of reduction is isomorphic to $\mathfrak{m}_{F,v}$, the maximal ideal in

$\mathcal{O}_{F,v}$. Thus topologically, $E(F_v)$ is just a union of the open unit discs indexed by $E_S(k_v)$. The size of the group $E_S(k_v)$ is close to $q_v + 1 = \#\mathbb{P}^1(k_v)$, where q_v is a cardinality of k_v. In fact, let a_v denote the difference

$$a_v := q_v + 1 - \#E_S(k_v).$$

Then we have the following well known estimate:

THEOREM 2.6 (Hasse).

$$|a_v| \leq 2\sqrt{q_v}.$$

It is also well known that the elliptic curve E/k_v over a finite field up to isogenous is uniquely determined by a_v.

Selmer group and Tate-Shafarevich group. As we see from the proof of the Mordell-Weil group, to compute $E(F)$, it suffices to compute its image in an easier group $H^1(F_U, E[m])$. One actually can replace $H^1(F_U, E[m])$ by a smaller Selmer group $S(E)[m]$ consisting of elements in $H^1(F, E[m])$ whose restriction on $H^1(F_v, E[m])$ comes from some local points in $E(F_v)$. Let $Ш(E)[m]$ denote the quotient of $S(E)[m]$ by $E(F)/mE(F)$. Then we have an exact sequence

$$0 \longrightarrow E(F)/mE(F) \longrightarrow S(E)[m] \longrightarrow Ш(E)[m] \longrightarrow 0.$$

One can show that $Ш[m]$ is the subgroup of m-torsions in a so called Tate-Sharfarevich group Ш: the group of locally trivial E-torsors over F. Thus the computation of $E(F)/mE(F)$ is reduce to compute the elements in $S(E)[m]$ and check if its image in $Ш(E)$ is trivial. The group $Ш(E)$ should be finite as conjectured by Birch and Swinnerton-Dyer. If we assume this conjecture and take m prime to the order of $Ш(E)$, then every element in $S(E)[m]$ comes from a global point in $E(F)$!

Interestingly, modulo the Birch and Swinnerton-Dyer conjecture and Riemann Hypothesis, Goldefeld and Szpiro have proved that Szpiro's Conjecture 2.5 is equivalent to the following:

CONJECTURE 2.7 (Goldfeld-Szpiro [**31**]). *For any constant $\epsilon > 0$, there is a constant $C_\epsilon(F)$ such that*

$$\#Ш(E) \leq C_\epsilon(E)\mathrm{N}_{F/\mathbb{Q}}(N)^{1/2+\epsilon}.$$

3. L-functions and modular forms

In this section we want to study L-functions and modular forms, and their relation to the arithmetic questions addressed in the last section. The basic references are Tate's papers [**83, 84**], Silverman's books [**77, 78**], Koblitz's book [**52**], and Shimura's book [**75**], and my paper [**95**]. We will start with a definition of L-series using integral models of elliptic curves or the Galois representations on Tate modules. The Taniyama-Shimura conjecture, or the modularity conjecture implies the analytic continuations already conjectured by Hasse. Then we state the Birch and Swinnerton-Dyer conjecture (in its weak form) and known evidences over $\mathbb{Q}$ and totally real fields.

Let E be an elliptic curve defined over a number field F. With notations as in the previous section, the global L-series $L(s, E)$ of E is formally defined by the Euler product:

$$L(s, E) = \prod_{v:\text{bad}} (1 - a_v q_v^{-s})^{-1} \cdot \prod_{v:\text{good}} (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1}.$$

where $a_v = 0$, 1, or -1 when E_S has bad reduction at v.

Another way to define L-series is by Galois representation which avoids using integral models. Let ℓ be a prime and let $T_\ell(E)$ denote the projective limit $\lim_{\ell^n} E[\ell^n]$. Then $T_\ell(E)$ has an action by $\mathrm{Gal}(\bar{F}/F)$. Now for any finite place v *not dividing* ℓ, let D_v denote the decomposition group of some extension w of v to $\bar{F}$, and let I_v denote the inertia group of D_v then D_v/I_v is generated by some Frobenius element Frob_v:

$$\mathrm{Frob}_v x \equiv x^{q_v} \mod w, \qquad \forall x \in \mathcal{O}_{\bar{Q}}.$$

Now the L-series at the place v can be defined to be

$$L_v(s, E) = (1 - q_v^{-s}\mathrm{Frob}_v|\mathrm{T}_\ell(E)^{I_v})^{-1}.$$

One can show that $L_s(s, E)$ does not depend on the choice of ℓ. The global L-function can be written as

$$L(s, E) := \prod_v L_v(s, E).$$

The factors $L_v(s, E)$ is a faithful invariant of the isogeny class of E:

THEOREM 3.1 (Faltings [**25**]). *Two elliptic curves E_1 and E_2 over F are isogenous if and only if they have the same L-factors at almost all places.*

The theorem of Hasse implies that the L-series $L(s, E)$ is absolutely convergent for $\mathrm{Re}(s) > 3/2$. Actually one expects much more to be true

CONJECTURE 3.2 (Modularity conjecture). *The L-series $L(s, E)$ can be analytically continued to the whole complex plane. Moreover,*

$$L(s, E) = L(s - 1/2, \Pi)$$

for some automorphic representation Π for $\mathrm{GL}_2(\mathbb{A}_F)$ with the same conductor as E.

We will not explain the meaning of Π but we will discuss the functional equation of $L(s, \Pi)$. One defines the conductor of E (denoted N) as a measure of the singularity in the *isogeny* class of E by

$$\mathrm{ord}_v(N) = \mathrm{ord}_v(\Delta) + 1 - m_v.$$

Here m_v denotes the number of connected components in E/k_v. The conjecture implies that $L(s, E)$ has a functional equation:

$$L^*(s, E) := (\Gamma\text{-functions})L(s, E) = \epsilon(E)\mathrm{N}_{F/\mathbb{Q}}(N)^{1-s}L^*(2 - s, E)$$

where $\epsilon(E) = \pm 1$ is called the sign of E or $L(s, E)$. Notice that $L(1, E) = 0$ if $\epsilon(E) = -1$. Our main concern in this paper is the following:

CONJECTURE 3.3 (Birch and Swinnerton-Dyer). *Let E be an elliptic curve defined over a number field F. Let R denote the regulator of E, i.e., the volume of free part of $E(F)$ with respect to the Neron-Tate height pairing. Let Ω be the volume of $\prod_{v|\infty} E(F_v)$ with respect to the Neron differentials of E. Then*

1. $\mathrm{ord}_{s=1}L(s, E) = \mathrm{rank}E(F)$.
2. $|Ш(E)| < \infty$.
3. $\lim_{s\to 1} L(s, E)(s - 1)^{-\mathrm{rank}E(F)} = c \cdot \Omega(E) \cdot R(E) \cdot |Ш(E)| \cdot |E(F)_{tor}|^{-2}$.

Here c is an explicitly positive integer depending only on E_v for v dividing N.

If we assume both the Birch and Swinnerton-Dyer conjecture, then we have an effective way to compute $E(F)$. Indeed, the rank can be effectively bounded by 2-torsions of the Selmer group and therefore bounded in terms of discriminant. The last formula in the Birch and Swinnerton-Dyer conjecture thus gives a way to compute $R(E)$ for every given rank. Since the minimal height of a nontorsion point in $E(F)$ can be estimated effectively, one thus has an estimate for the longest generator via Minkowski's successive minima.

Case where $F = \mathbb{Q}$. In this case, the conjecture of modularity is completely solved.

THEOREM 3.4 (Wiles, Taylor, Diamond, Conrad, Bruil [**85, 91, 11**]). *Let E be an elliptic curve over $\mathbb{Q}$ with L-series*

$$L(s, E) = \sum a_n n^{-s}.$$

Let f be a function on the upper-half complex plane defined by

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}, \qquad \mathrm{Im} z > 0.$$

Then $f(z)$ is a cusp form for the group

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \quad c \equiv 0 \pmod{N} \right\}.$$

Here N is the conductor of E. In other words the form $f(z)dz$ is invariant under the action of $\Gamma_0(N)$.

Thus, up to certain gamma factors, $L(s, E)$ has a functional equation

$$\begin{aligned} L^*(s, E) :&= \int_0^{\infty} f(yi) y^{s-1} dy = (2\pi)^{-s} \Gamma(s) L(s, E) \\ &= \epsilon(s, E) \cdot L^*(2 - s, E) \end{aligned}$$

where $\epsilon(s, E) = \epsilon(E) N^{1-s}$ with $\epsilon(E) = \pm 1$, the sign of E.

This theorem has the following geometric description. Let $X_0(N)$ denote the modular curve

$$\Gamma_0(N) \backslash \mathcal{H} \cup \{\text{cusps}\}$$

which is actually defined over $\mathbb{Q}$.

THEOREM 3.5. *Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N. Then there is a nonconstant morphism*

$$\pi : \quad X_0(N) \longrightarrow E$$

defined over $\mathbb{Q}$.

We may choose a morphism π such that π does not factor through any endomorphism of E of degree > 1 and such that $\pi(\infty) = 0$. We call such a morphism a *strong* parameterization. The strong parameterization is unique up to compositions with automorphisms of E. Then one can show that the Szpiro's conjecture is equivalent to the following:

CONJECTURE 3.6. *There are constants α and β such that for any elliptic curve E defined over $\mathbb{Q}$ with a strong parameterization $\pi : X_0(N) \longrightarrow E$, one has*

$$\deg \pi \leq \alpha \cdot N^{\beta}.$$

Example. Let E be the curve defined by

$$E : y^2 = 4x^3 - 4x + 1.$$

Then $E(\mathbb{Q}) \simeq \mathbb{Z}$ and is generated by $(0, 1)$. The sign of E is $\epsilon(E) = -1$.

One can compute the coefficients of

$$L(s, E) = \sum_{n=1}^{\infty} a_n n^{-s}$$

as follows:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a(n)	1	-2	-3	2	-2	6	-1	0	6	4	-5	-6	-2	2	6

The corresponding modular form is given by

$$f(z) = q - 2q^2 - 3q^3 + 2q^4 - q^5 + 6q^6 - q^7 + 6q^9 + \cdots, \qquad (q = e^{2\pi i z}).$$

The modular parameterization of this curve is given by the function

$$\phi : \mathcal{H} \longrightarrow \mathbb{C},$$

where

$$\phi(\tau) = 2\pi i \int_{i\infty}^{\tau} f(\tau')d\tau' = q - q^2 - q^3 + \frac{1}{2}q^4 - \frac{2}{5}q^5 + \cdots.$$

Concerning the Birch and Swinnerton-Dyer conjecture one has the following:

THEOREM 3.7 (Gross-Zagier-Kolyvagin [**53**]). *Let E be an elliptic curve defined over $\mathbb{Q}$. Assume that $\mathrm{ord}_{s=1} L(s, E) \leq 1$. Then the Sharfarevich-Tate group $Ш(E/\mathbb{Q})$ is finite, and*

$$\mathrm{ord}_{s=1} L(s, E) = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}).$$

Very little is known when $\mathrm{ord}_{s=1} L(s, E) > 1$. But if the Tate-Sharfarevich group is finite, then we will have the right parities. More precisely, the following has been proved recently:

THEOREM 3.8 (Nekovar [**66**]). *Let p be a prime such that E has good and ordinary reduction. Let $X(E)$ denote the inverse limit of $S(E)[p^{\infty}]$. Then*

$$\mathrm{rank}_{\mathbb{Z}_p} X(E) \equiv \mathrm{ord}_{s=1} L(s, E) \mod 2.$$

Notice that we only stated results for the first two parts of the BSD conjecture and not much is known for the third part. But when E is a CM-elliptic curve, a lot has been proved by Coates-Wiles [**14**], Rubin [**71**], and Greenberg [**32**].

Case where F is totally real. Now we assume that F is totally real, by which we mean that all embeddings of F into $\mathbb{C}$ are real. By conjecture 3.2, every elliptic curve E over F is modular, which means that there is a Hilbert new form f over F of weight $(2,\cdots,2)$, with conductor N, and with trivial central character, such that for each finite place v not dividing N,

$$a_v(E) := q_v + 1 - \#E(k_v) = a_v(f)$$

where $a_v(f)$ is the eigenvalue of the Hecke operator T_v which acts on f:

$$\mathrm{T}_v(f) = a_v(f)f.$$

See [**27, 79**] for some progress about modularity conjecture over totally real fields by Fujiwara and Skinner-Wiles. Then we have the following:

THEOREM 3.9 ([**95**]). *Let E be a modular elliptic curve over F. Assume the following holds:*

1. *$[F:\mathbb{Q}]$ is odd or the conductor N of E is not a square;*
2. *$\mathrm{ord}_{s=1}L(s,E) \leq 1$.*

Then:

$$\mathrm{ord}_{s=1}L(s,E) = \mathrm{rank}_{\mathbb{Z}}E(F)$$

and $Ш(E/F)$ is finite.

For later use, let's recall the definition of a Hilbert newform of weight $(2,\cdots,2)$ and conductor N. Let's first fix an isomorphism

$$GL_2(F_\infty) \simeq \mathrm{GL}_2(\mathbb{R})^g.$$

Then the subgroup $\mathrm{GL}_2(F)_+$ with totally positive determinants acts on the product $\mathcal{H}^g$ of g-copies of the upper half plane. Let $X_0(N)$ denote the following complex manifold

$$\mathrm{GL}_2(F)_+\backslash\mathcal{H}^g \times \times\mathrm{GL}_2(\widehat{F})/U_0(N)Z(\widehat{F}),$$

here $Z(\widehat{F})$ is the center of $\mathrm{GL}_2(\widehat{F})$, $U_0(N)$ is subgroup of $\mathrm{GL}_2(\widehat{\mathcal{O}}_F)$ of matrices congruent to upper triangular matrices modulo N. In this way, a cusp form f of weight $(2,\cdots,2)$, level N, and trivial central character, is a function on

$$\mathcal{H}^g \times \mathrm{GL}_2(\mathbb{A}_{F,f})$$

such that $f dz_1\cdots dz_g$ comes from a holomorphic g-form on $X_0(N)$ which is finite near each cusp of $X_0(N)$. We call a newform of level N if f is not a form of smaller level, and f is an eigenform for the Hecke operator T_v for each finite place v not dividing v:

$$\mathrm{T}_v f(g) = \sum_{x \pmod{\pi}} f\left(g\begin{pmatrix}\pi & x\\ 0 & 1\end{pmatrix}\right) + f\left(g\begin{pmatrix}1 & 0\\ 0 & \pi\end{pmatrix}\right)$$

where π is a uniformizer of F_v. The following is well known from the multiplicity one result of new forms:

THEOREM 3.10. *Let f be be a newform of weight $(2,\cdots,2)$, level $U_0(N)$, and trivial central character. Let L be the subfield of $\mathbb{C}$ generated by eigenvalues $\lambda_v(f)$ under T_v for v not dividing v. Then L is a totally real number field. Moreover for any embedding $\sigma : L \longrightarrow \mathbb{C}$ there is a unique newform f^σ up to constant multiple such that the eigenvalues of f^σ under T_v are given by λ^σ.*

One may define the L-series $L(s,f)$ by Mellin-transform such that $L(s,f)$ has Euler product whose local factor at v not dividing N is given by

$$(1-\lambda_v q_v^{-s}+q_v^{1-2s})^{-1}.$$

The theory of automorphic forms gives for each such newform f a unique cuspidal representation Π of $\mathrm{GL}_2(\mathbb{A}_F)$ with the same L-series

$$L(s-1/2,\Pi)=L(s,f).$$

In the case $F=\mathbb{Q}$, the modularity is equivalent to a nonconstant map $X_0(N)\longrightarrow E$ over $\mathbb{Q}$. In the general case, this is not true. But when the first condition of Theorem 3.9 is satisfied, then E can be parametrized by a Shimura curve. We will come back to this point later.

Abelian variety of GL(2) type. From the modular form point of view, all results above can be generalized to abelian varieties of GL(2) type, by which we mean that an abelian variety A such that $\mathrm{End}(A)\otimes\mathbb{Q}$ contains a totally real field L of degree equal to $\dim A$.

By an automorphic representation Π of $\mathrm{GL}_2(\mathbb{A}_F)$ with values in L, we mean a collection of automorphic representations Π^σ indexed by embeddings $\sigma: L\longrightarrow\mathbb{R}$ such that the coefficients of local factors $L_v(s,\Pi_v^\sigma)$ are images under the embeddings of the coefficients of a formal local L-functor $L_v(s,\Pi_v)$ with coefficients in L.

CONJECTURE 3.11. *Let A be a simple abelian variety defined over F with an endomorphism by an order in a number field L of degree* $\dim A$. *Then there is an automorphic representation Π of $\mathrm{GL}_2(\mathbb{A}_F)$ with value in L such that*

$$L(s,A)=\prod_{\sigma:F\longrightarrow\mathbb{R}}L(s-1/2,\Pi^\sigma).$$

Moreover when F is totally real, one may take Π to be the Hilbert cups form of weight $(2,\cdots,2)$, level N, and trivial central character.

Now we assume that the conjecture is true for an abelian variety A and an automorphic representation Π. Then $A(F)\otimes\mathbb{R}$ is an vector space over L. Thus it is a direct sum $\oplus A(\sigma)$ of eigen subspaces corresponding to embeddings σ of F into $\mathbb{R}$. Notice that for every σ,

$$\dim_L A(F)\otimes\mathbb{Q}=\dim_{\mathbb{R}}A(\sigma).$$

CONJECTURE 3.12. *Assume that the above conjecture is true for an abelian variety A and an automorphic representation Π with value in L. Then*

$$\mathrm{ord}_{s=1}L(s,\Pi^\sigma)=\dim_L A(F)\otimes\mathbb{Q}.$$

Modular forms of high weights. For N a product of two relatively prime integers ≥ 3, one can show that the universal elliptic curve over the non-cuspidal locus of $X(N)_{\mathbb{Z}}$ can be extended uniquely to a regular semistable elliptic curve $\mathcal{E}(N)$ over $X(N)$. The Kuga-Sato variety $Y=Y_k(N)$ will be defined to be a canonical resolution of the $2k-2$-tuple fiber product of $\mathcal{E}(N)$ over $X(N)$.

Let $f=\sum_{n\geq 1}a_nq^n\in S_{2k}^{\mathrm{new}}(\Gamma_0(N))$ be a normalized eigenform of weigh $2k$ on $\Gamma_0(N)$ with coefficients in $\mathbb{Q}$. Let $M=M(f)$ be the Grothendieck motive over $\mathbb{Q}$ constructed by P. Deligne [**20**], U. Jannsen [**47**] and A. J. Scholl [**73, 74**]. The ℓ-adic realization M_ℓ is a two dimensional representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ corresponding to f and appears as a factor in the cohomology group

$$H_{\text{ét}}^{2k-1}(Y\otimes\bar{\mathbb{Q}},\mathbb{Q}_\ell)(k)^H,$$

where $Y = Y(N') \otimes \mathbb{Q}$ for multiple N' of N such that N' is a product of two relatively prime integers ≥ 3, and H is the covering group $\Gamma_0(N)/\Gamma(N')$.

For any number field F, let $\mathrm{Ch}^k(Y_F)_0$ be the group of homologically trivial cycles of codimension k in Y_F modulo the rational equivalence. Let $\mathrm{Ch}(F)_f$ be the f-typical component of

$$\mathrm{Ch}^k(Y_F)_0^H \otimes \mathbb{Q}_\ell$$

under the action by Hecke operators. The ℓ-adic Abel-Jacobi map

$$\Phi_F : \mathrm{Ch}^k(Y_F)_0 \otimes \mathbb{Q}_l \to H^1_{\mathrm{cont}}(F, H^{2k-1}_{\text{ét}}(Y \otimes \bar{\mathbb{Q}}, \mathbb{Q}_l)(k))$$

induces a map

$$\Phi_{F,f} : \mathrm{Ch}(f)_\ell \to H^1_{\mathrm{cont}}(F, M(f)_\ell).$$

CONJECTURE 3.13 (Beilinson and Bloch). *The morphism $\Phi_{F,f}$ is always injective and the dimension of $\mathrm{Im}\Phi_{F,f}$ is equal to the order of $L(s, f \otimes F)$ at $s = k$.*

The following was proved by combining results of Nekovar [**64, 65**] and a Gross-Zagier formula:

THEOREM 3.14 ([**94**]). *Assume the following conditions:*

1. $k > 1$,
2. $\Phi_{K,f}$ *is injective for every imaginary quadratic field* K,
3. $\mathrm{ord}_{s=k} L(s, f) \leq 1$, *and that* ℓ *does not divide* $2N$.

Then the following equality holds:

$$\mathrm{rank}_{\mathbb{Q}_l} \mathrm{Im}(\Phi_{f,\mathbb{Q}}) = \mathrm{ord}_{s=k} L(s, f).$$

4. Complex multiplications

In this section, we study elliptic curves with complex multiplications. The basic references are Shimura's books [**75, 76**] and Silverman's book [**78**]. The main results include the algebraicity of j-invariants which will be used to construct algebraic points on Shimura varieties, and the computation of L-functions which provides examples of modular elliptic curves in terms of theta series.

By an elliptic curve with *complex multiplication* we mean an elliptic curve E over $\mathbb{C}$ such that $\mathrm{End}(E) \neq \mathbb{Z}$. In this case, $\mathrm{End}(E)$ is isomorphic to *an order* in an imaginary quadratic field K:

$$\mathrm{End}(E) \simeq \mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$$

for some $c \in \mathbb{N}$. Fix an isomorphism $\iota : K \simeq \mathrm{End}(E) \otimes \mathbb{Q}$. Then the action of $\mathrm{End}(E)$ on $\mathrm{Lie}(E)$ gives an embedding $K \longrightarrow \mathbb{C}$. Thus we may view K as a subfield of $\mathbb{C}$ by this manner.

It is easy to see that $E(\mathbb{C})$ may be taken as $\mathbb{C}/\Lambda$ with Λ an invertible $\mathcal{O}_c$-module. Two elliptic curves $E_i = \mathbb{C}/\Lambda_i$ $(i = 1, 2)$ with the same endomorphism ring $\mathcal{O}_c$ are isomorphic if and only if Λ_1 and Λ_2 are in the same class in $\mathrm{Pic}(\mathcal{O}_c)$. Thus we have a bijection:

$$j[c] := \{j(E) : \quad \mathrm{End}(E) = \mathcal{O}_c\} \longrightarrow \mathrm{Pic}(\mathcal{O}_c).$$

Notice that the group $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ is stable on the set $j[c]$. It follows that all $j(E)$ in $j[c]$ are algebraic. In other words, any CM elliptic curve $E/\mathbb{C}$ will be defined by some Weierstrass equation with coefficients in a number field. Moreover if E is defined over some field $L \subset \mathbb{C}$, then all elements in $\mathrm{End}(E)$ is defined over $L \cdot K$,

the composition of L and K. Indeed, if we let v be a generator of $\mathrm{Lie}(E/L)$ and $\iota(a) \in \mathrm{End}(E)$ then

$$d(\iota(a))v = av.$$

Applying both sides under $\sigma \in \mathrm{Gal}(\mathbb{C}/LK)$ then we have

$$d(\iota(a)^\sigma)v = av.$$

Thus we must have $\iota(a)^\sigma = a$.

The *main theorem of complex multiplication* will show the following more precise information:

1. all $j(E)$ are defined over some abelian extension of K corresponding to $\mathrm{End}(E)$;
2. if E is defined over some field L then $E_{\mathrm{tor}}(\mathbb{C})$ will be defined over $L \cdot K^{\mathrm{ab}}$, where K^{ab} denotes the maximal abelian extension of K in $\mathbb{C}$.

The Main Theorem. To state the Main Theorem of Complex Multiplication, we recall the key principles of class field theory. Let $\mathbb{A}_K$ be the ring of adeles of K, that is the subring of $\prod_v K_v$ of the product of all local fields, consisting of elements of (x_v) such that for all but finitely many v, x_v is integral. The field K is embedded into $\mathbb{A}_K$ diagonally. Let $\mathbb{A}_K^\times$ denote the group of invertible elements. Then class field theory gives an Artin map with dense image:

$$\mathbb{A}_K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K), \qquad x \longrightarrow [x, K],$$

such that the kernel consists of $K^\times \cdot K_\infty$. More precisely, for any finite extension L/K in K^{ab} and any finite place v of K unramified in L, the composition map

$$K_v^\times \longrightarrow \mathbb{A}_K^\times \longrightarrow \mathrm{Gal}(L/K)$$

will be given by $x \longrightarrow \mathrm{Frob}_v^{\mathrm{ord}_v(x)}$, i.e., for any place w over v, and any $a \in \mathcal{O}_L$,

$$a^{[x,K]} \equiv a^{|x|_v^{-1}} \mod \wp_w$$

where $\wp_w$ is the maximal ideal of $\mathcal{O}_L$ corresponding to w.

The group $\mathbb{A}_K^\times$ also acts on the set of lattices in K in the following manner: for any lattice $\Lambda \in K$, and any $s \in \mathbb{A}_K^\times$, the lattice $s\Lambda$ is defined to the unique lattice in K whose completion at a finite place v of K is given by $s_v\Lambda_v$, where L_v is the completion of L at v. The multiplication of s does not give an isomorphism from Λ to $s\Lambda$ but given an isomorphism

$$s: \quad K/\Lambda \longrightarrow K/s\Lambda$$

as both sides are direct sums of local quotients K_v/Λ_v and $K_v/s_v\Lambda_v$.

THEOREM 4.1 (The Main Theorem of Complex Multiplication). *Let E be an elliptic curve with CM by some order in K. Let $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$, $x \in \mathbb{A}_{K,f}^\times$ such that*

$$[x, K] = \sigma|_{K^{\mathrm{ab}}}.$$

Then for any complex isomorphism

$$f: \quad \mathbb{C}/\Lambda \simeq E(\mathbb{C}),$$

where Λ is a lattice in K, there is a unique complex analytic isomorphism

$$f': \quad \mathbb{C}/x^{-1}\Lambda \simeq E^\sigma(\mathbb{C})$$

such that the restriction of the map

$$\sigma: \quad E(\mathbb{C}) \longrightarrow E^{\sigma}(\mathbb{C})$$

on torsion points is given by

$$x^{-1}: \quad K/\Lambda \longrightarrow K/x^{-1}\Lambda.$$

Algebraicity of j-invariants. The first consequence of Theorem 4.1 is a precise description of the action of $\mathrm{Gal}(\mathbb{C}/K)$ on $j[c]$. More precisely, the map

$$\mathbb{C}/\Lambda \longrightarrow [\Lambda] \in \mathrm{Pic}(\mathcal{O}_c)$$

gives a bijection between $j[c]$ and $\mathrm{Pic}(\mathcal{O}_c)$ and thus admits an action by $\mathrm{Pic}(\mathcal{O}_c)$. The action of $\mathrm{Gal}(\mathbb{C}/K)$ on $j[c]$ is given by the *inverse* of the following composition:

$$\mathrm{Gal}(\mathbb{C}/K) \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K) \longrightarrow K^{\times}\backslash \mathbb{A}^{\times}/K_{\infty}^{\times} \cdot \widehat{\mathcal{O}}_c = \mathrm{Pic}(\mathcal{O}_c).$$

We call the extension $K[c]$ of K in K^{ab} fixed by $\widehat{\mathcal{O}}_c$ the ring class field of K of conductor c. Thus we have shown the following:

COROLLARY 4.2. *For every $j \in j[c]$, the field $K(j(E)) = K[c]$ is the ring class field of K of conductor c, and all $j \in j[c]$ are conjugate to each other under the Galois group* $\mathrm{Gal}(K[c]/K)$.

Galois action on torsion points. To understand the action on torsion points we assume that E is defined over some number field L containing K. We recall that we still have the Artin map

$$\mathbb{A}_L^{\times} \longrightarrow \mathrm{Gal}(L^{\mathrm{ab}}/L), \qquad x \longrightarrow [x, L],$$

with kernel generated by $L^{\times}$ and the connected component of $\mathbb{A}_L^{\times}$. Let

$$\mathbb{A}_L^{\times} = \mathbb{A}_{L,f}^{\times} \cdot \mathbb{A}_{L,\infty}^{\times}$$

be the decomposition of $\mathbb{A}_L^{\times}$ into finite or infinite ideles.

Let $\sigma \in \mathrm{Gal}(\mathbb{C}/L)$. Let $x \in \mathbb{A}_L^{\times}$ such that

$$[x, L] = \sigma|_{L^{\mathrm{ab}}}.$$

Then $E^{\sigma} \simeq E$. So we may replace E^{σ} by E in Theorem 4.1. Two parameterizations f and f' are related by the multiplication of a unique $\alpha(x) \in K^{\times}$. Obviously, $x \longrightarrow \alpha(x)$ is a homomorphism from $\mathbb{A}_L^{\times}$ to $K^{\times}$. For $x \in L^{\times}$, $[x, L] = 1$. Thus the corollary implies that $\alpha(x) = \mathrm{N}_{L/K}(x)$. In other words, α can be extended to a Hecke character $\psi_{E/L}$ on $\mathbb{A}_L^{\times}$ by

$$\psi_{E/L}(x) = \alpha_{E/L}(x)\mathrm{N}_{L/K}(x^{-1})_{\infty}.$$

Notice that ψ has the following properties:

$$\begin{cases} \psi_{E/L}(x) \in K^{\times} & \text{if } x \in \mathbb{A}_{L,f}^{\times} \\ \psi_{E/L}(x) = \mathrm{N}_{L/K}(x)^{-1} & \text{if } x \in \mathbb{A}_{L,\infty}^{\times}. \end{cases} \tag{4.1}$$

COROLLARY 4.3. *Let E be an elliptic curve defined over a number field L such that* $\mathrm{End}(E)$ *is some order $\mathcal{O}_c$ in an imaginary quadratic field K. Assume that L contains K. Then for any $\sigma \in \mathrm{Gal}(\mathbb{C}/L)$, $x \in \mathbb{A}_L^{\times}$ such that $\sigma|_{L^{\mathrm{ab}}} = [x, L]$, and any analytic isomorphism*

$$f: \quad \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}),$$

where Λ is a lattice in K, the restriction of $[x, L]$ on $K/\Lambda \subset E(L^{\mathrm{ab}})$ is given by

$$\psi(x)\mathrm{N}_{L/K}(x)^{-1}: \quad K/\Lambda \simeq K/\Lambda.$$

L-series. Now lets compute the L-series from the above corollary by noticing that $T_\ell(E) \simeq \Lambda \otimes \mathbb{Z}_\ell$ for the uniformization $\mathbb{C}/\Lambda \simeq E(\mathbb{C})$. Thus the Galois action of $\mathrm{Gal}(\bar{L}/L)$ on $T_\ell(E) \simeq \Lambda_\ell$ is given by the following composition:

$$\mathrm{Gal}(\bar{L}/L) \longrightarrow \mathbb{A}_{L,f}^\times / K^\times \xrightarrow{\psi(x)\mathrm{N}_{L/K}(x)_\ell^{-1}} \mathcal{O}_{c,\ell}^\times.$$

The above corollary implies the following:

THEOREM 4.4 (Deuring). *Let E/L be an elliptic curve with complex multiplication by some order in K. Assume that K is included in L. Let $\psi_{E/L} : \mathbb{A}_L^\times \longrightarrow \mathbb{C}^\times$ be the Grossencharcter attached to E/L. Then*

$$L(E/L, s) = L(s, \psi_{E/L}) \cdot L(s, \bar{\psi}_{E/L}).$$

The correspondence

$$E \longrightarrow \{\psi_{E/L}, \bar{\psi}_{E/L}\}$$

is bijective between the set of isogeny classes of elliptic curves over L and the set of conjugate classes of Grossencharacters of L satisfying (4.1).

Recall that the Hecke character $\psi : L^\times \backslash \mathbb{A}_L^\times$ has the decomposition $\psi = \otimes \psi_v$, where ψ_v is the composition

$$L_v^\times \longrightarrow \mathbb{A}_L^\times \longrightarrow \mathbb{C}^\times.$$

The L-function $L(s, \psi)$ is defined as the product

$$L(s, \psi) = \prod_v L(s, \psi_v),$$

where the local L-function is defined as follows:

$$L(s, \psi_v) = \begin{cases} (1 - \psi(\pi_v) q_v^{-s})^{-1} & \text{if } \psi_v \text{ is unramified,} \\ 1 & \text{otherwise,} \end{cases}$$

where π_v is the local parameter of L_v. One immediate consequence of this theorem is the holomorphic continuation of $L(s, E)$ and the functional equation which were proved in Tate's thesis [**82**]. Actually, the theorem tell us that E is modular in the sense of conjecture 3.2 with $L(s, E) = L(s - 1/2, \Pi)$ where Π is an automorphic representation of $\mathrm{GL}_2(\mathbb{A}_L)$ induced from the following character χ on the subgroup of upper triangular matrices:

$$\chi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = \psi(a)\bar{\psi}(d)|a/d|^{1/2}.$$

Now we want to consider the case where K is not included into L. Let E/L be an elliptic curve with complex multiplication by some order in K. Let $\psi_{E/L'}$ be a Grossenchacter attached to E/L'. Then one can show that the restriction of ψ on $\mathbb{A}_L^\times$ satisfies the following:

$$\psi(x) = \epsilon(x)|x|^{-1} \tag{4.2}$$

where ϵ is a quadratic character of $\mathbb{A}_L^\times$ corresponding to the extension L'/L.

THEOREM 4.5 (Deuring). *With notation as above, one has the following*

$$L(E/L, s) = L(s, \psi_{E/L'}).$$

The correspondence

$$E \longrightarrow \{\psi_{E/L'}, \bar{\psi}_{E/L'}\}$$

is bijective between the set of isogeny classes of elliptic curves over L and the set of conjugate classes of characters of $\mathbb{A}_{L'}^{\times}$ satisfying (4.1) and (4.2).

Again it follows from Tate's thesis, $L(s, E)$ has holomorphic continuation and functional equation. Moreover, E is modular with $L(s, E) = L(s - 1/2, \Pi)$ where Π is the representation of $\mathrm{GL}_2(\mathbb{A}_L)$ which is a theta lifting from the character ψ of $\mathrm{GL}_1(\mathbb{A}_{L'})$.

Abelian varieties with complex multiplications. A natural generalization of a CM elliptic curve is a CM abelian variety A, which means that $\mathrm{End}(A) \otimes \mathbb{Q}$ contains a subfield of degree $2\dim(A)$. One may show that these abelian varieties are defined over number fields and that their L-functions are *products* of the complex conjugations of automorphic representations over GL(2) of the base field (these are either principal or theta liftings).

5. Shimura curves

In this section, we study Shimura curves as generalization of modular curves. The basic references are papers by Deligne [**19**], Boutot-Carayol [**10**], Carayol [**13**], and myself [**95**]. We will start with constructions of quaternion algebras over F, Shimura curves, and Shimura curves X of type (N, K), a direct generalization of the modular curve $X_0(N)$. The main result of Shimura is that these curves are defined over F. When $F = \mathbb{Q}$, we give some moduli interpretations for these curves. Then we come to Hecke's theory and Eichler-Shimura theory. The main consequence is that the Jacobian of X provides abelian varieties of GL_2-type over F of conductor N. It is conjectured that every abelian variety of conductor N of GL_2-type is a quotient of $\mathrm{Jac}(X)$ and thus parameterized (*admissibly*) by X.

Quaternion algebra. Let F be a number field. Let B be a quaternion algebra over F by which we mean a simple algebra over F of rank 4. It is isomorphic to the following $B_{a,b}$ over F generated by two elements x and y such that

$$a := x^2 \in F, \quad b := y^2 \in F, \quad xy + yx = 0.$$

For example, $B_{1,1} = M_2(F)$. For any place v of F, $B_v = B \otimes F_v$ is either isomorphic to $M_2(F_v)$, the matrix algebra of rank 2, or the division algebra D_v of rank 2 over F_v. If v is an archimedean place, D_v exists only if $F_v \simeq \mathbb{R}$ where D_v can be taken as the usual Hamiltonians:

$$D_v = B_{-1,-1}.$$

If v is a nonarchimedean place, then we may take

$$D_v = B_{a,b}$$

where a, b are chosen such that $F_v(\sqrt{a})$ is ramified over F_v , and $F_v(\sqrt{b})$ is unramified over F_v.

Let Σ be the set of all places over which B is non-split. Then Σ is a finite subset with even cardinality. Moreover the correspondence $B \longrightarrow \Sigma$ is bijective between the set of isomorphism classes of B and the set of finite subsets of places of even cardinality. For example, $B \simeq M_2(F)$ if and only if $\Sigma \simeq \emptyset$. See Vignéras' book [**88**] for basic facts about quaternion algebras.

Shimura curves. Now we assume that F is totally real and that B is split at a fixed place τ of F and non-split at the rest of archimedean places. We view F as a subfield of $\mathbb{C}$ via τ. Let G denote the algebraic group $B^\times$ over F. Then group $G(F_\tau) \simeq \mathrm{GL}_2(\mathbb{R})$ acts on $\mathcal{H}^\pm = \mathbb{C} - \mathbb{R}$. Now for any open subgroup U of $G(\mathbb{A}_f)$ which is compact modulo the center $Z(\mathbb{A}_f)$, we have a Shimura curve

$$\mathbb{S}_U = G(F)\backslash \mathcal{H}^\pm \times G(\widehat{F})/U.$$

Shimura proved that these were the complex points of an algebraic curve $\mathbb{S}_U$ defined over F. Moreover the isomorphic class of curve $\mathbb{S}_U$ over F depends only on the finite subset $\Sigma \setminus \{\tau\}$.

This curve is compact if $F \neq \mathbb{Q}$. Notice that the curve $\mathbb{S}_U$ may not be connected. The map to its set of connected components is identified with the norm map

$$\det : \quad G(\mathbb{Q})\backslash \mathcal{H}^\pm \times G(\mathbb{A}_f)/U \longrightarrow F^\times \backslash \{\pm 1\} \times \mathbb{A}_{F,f}^\times / \det U \simeq F_+^\times \backslash \mathbb{A}_f^\times / \det U.$$

Each connected component is defined over the field an abelian extension F_U of F corresponding to the subgroup $\det(U)$ of $\widehat{F}$ via the class field theory:

$$\mathrm{Gal}(F_U/F) \simeq F_+^\times \backslash \mathbb{A}_{F,f}^\times / \det(U).$$

The action of $\mathrm{Gal}(F_U/F)$ on the set of connected components is the inverse-multiplication of $\mathbb{A}_F^\times$.

Shimura curves of (N, K)-type. One special case is the Shimura curves with *minimal* level which corresponds to the case U is a maximal compact subgroup of $G(\mathbb{A}_f)$ modulo the center. In this case, there is a maximal order $\mathcal{O}_B$ of B such that $U = Z(\mathbb{A}_f) \cdot \widehat{\mathcal{O}}_B^\times$.

A more general case is the Shimura curve with *a level $U_0(N)$ structure*, where N is an ideal of $\mathcal{O}_F$ which is invertible at all places where B is ramified. In this case, $U = Z(\mathbb{A}_f) \prod U_v$ where U_v is maximal at the place where v is ramified in B. If v is not ramified in B, then there is an isomorphism $B_v \simeq M_2(F_v)$ such that U_v corresponds to the subgroup of matrices of $\mathrm{GL}_2(\mathcal{O}_v)$ which are triangular when modulo N. It is well known that all Shimura curves with level $U_0(N)$ structure are all isomorphic to each other, and that every geometric component of $\mathbb{S}_U$ is defined over the *narrow* class field H_F of F since $\det U = \widehat{\mathcal{O}}_F^\times \cdot (\mathbb{A}_{F,f}^\times)^2$.

In case $F = \mathbb{Q}$, the Shimura curves with $U_0(N)$-structure is the usual $X_0(N)$.

An even more general case is the Shimura curve of *type* (N, K) where

1. K is a totally imaginary quadratic extension of F embedded into B;
2. N is an ideal of $\mathcal{O}_F$ which is prime to the relative discriminant of K/F.

Then we take $U = Z(\mathbb{A}_f) \cdot \widehat{R}^\times$ where R is an order of B containing $\mathcal{O}_K$ with relative discriminant N. The existence of such a Shimura curve is equivalent to the following condition: *B is ramified at a finite place v if and only if v is inert in K and $\mathrm{ord}_v(N)$ is odd.* Moreover such a Shimura curve is unique up to isomorphism once it exits. The Shimura curve with $U_0(N)$ level structure corresponding to the case where for each finite place v dividing N, either $\mathrm{ord}_v(N) = 1$ or v is split in K.

Moduli interpretation. If $F = \mathbb{Q}$, then $\mathbb{S}_U$ parameterize elliptic curves or abelian surfaces as follows. Fix one maximal order $\mathcal{O}_B$ of B.

THEOREM 5.1. *Assume that $F = \mathbb{Q}$ and U is included in $\widehat{\mathcal{O}}_B^\times$. For U sufficiently small, the curve $\mathbb{S}_U$ represents the functor*

$$\mathcal{M}_U : \quad \mathrm{Sch}/\mathbb{C} \longrightarrow \mathrm{Set}$$

defined as follows: for any $S \in \mathrm{Sch}/\mathbb{C}$, $\mathcal{M}_U(S)$ *is the set of isomorphic classes of the triple* $(A, \iota, \bar{\kappa})$ *so that*

1. A *is an abelian variety over* S *of relative dimension* 2;
2. $\iota : \mathcal{O}_B \longrightarrow \mathrm{End}(A)$ *is an action of* $\mathcal{O}_B$ *on* A;
3. $\bar{\kappa}$ *is a level* U *structure over* A *which means a class modulo* U *of isomorphisms:*

$$\kappa : \widehat{\mathcal{O}}_B \longrightarrow \widehat{\mathrm{T}}(A).$$

When $B = M_2(\mathbb{Q})$, $\mathcal{O}_B = M_2(\mathbb{Z})$, then for every object (A, ι, κ) as in the theorem, A has a canonical splitting

$$A = E \oplus E, \qquad E = \iota\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right) A,$$

such that ι is given by usual matrix multiplication. The level structure κ is induced by a level structure κ_E of E. Thus, we have the following:

THEOREM 5.2. *Assume that* $F = \mathbb{Q}$, $B = M_2(\mathbb{Q})$, *and* U *is included in* $M_2(\mathbb{Z})$. *For* U *sufficiently small, the curve* $\mathbb{S}_U$ *represents the functor*

$$\mathcal{M}_U : \quad \mathrm{Sch}/\mathbb{C} \longrightarrow \mathrm{Set},$$

defined as follows: for any $S \in \mathrm{Sch}/\mathbb{C}$, $\mathcal{M}_U(S)$ *is the set of isomorphic classes of the triple* $(E, \bar{\kappa})$ *so that*

1. A *is an elliptic curve over* S;
2. $\bar{\kappa}$ *is a level* U *structure over* E *which means a class modulo* U *of isomorphisms:*

$$\kappa : \widehat{\mathbb{Z}}^2 \longrightarrow \widehat{\mathrm{T}}(E).$$

Example. The algebraic curve structure over $\mathbb{Q}$ of $X_0(N)$ is defined by the modular interpretation that $X_0(N)$ parameterizes the set of isogenies $E_1 \longrightarrow E_2$ with kernels isomorphic to $\mathbb{Z}/N\mathbb{Z}$. A point $x \in X_0(N)$ will represent the object

$$[N] : \quad \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau \longrightarrow \mathbb{C}/\mathbb{Z} + \mathbb{Z}N\tau$$

where $\tau \in \mathcal{H}$ maps to x. For all but finitely many $x \in \mathcal{H}$, the minimal subfield of $\mathbb{C}$ which defines x is $\mathbb{Q}(j(\tau), j(N\tau))$ where $j : \quad \mathcal{H} \longrightarrow \mathbb{C}$ is the usual j-function:

$$j(\tau) = 1728 g_2^3/\Delta = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots$$

When $F \neq \mathbb{Q}$, $\mathbb{S}_U$ does not have a natural modular interpretation. Instead, one needs to fix an auxiliary totally imaginary quadratic extension K of F and consider the group $G' = G \times_{F^\times} K^\times$ and embed $\mathbb{S}_U$ into $\mathbb{S}'_{U'}$, the Shimura curve corresponding to G'. We will not give a description here since it is rather involved.

Hecke's operators. Let $\mathbb{S}_U$ be a Shimura curve defined as above. Let $\mathcal{O}_B$ be a maximal order of B such that U is included in $Z(\widehat{F})\widehat{\mathcal{O}}_B^\times$. Let m be an ideal of $\mathcal{O}_F$ such that at every prime ideal $\wp$ of m, U is maximal and B is split. Let G_m denote the set of elements of $\widehat{\mathcal{O}}_B$ which has component 1 at the the place not dividing m, and such that $\det(g)$ generates $\det m$ in $\widehat{\mathcal{O}}_F$. The Hecke correspondence $\mathrm{T}(m)$ on $\mathbb{S}_U$ is defined by the formula:

$$\mathrm{T}(m)x = \sum_{\gamma \in G_m/G_1} [(z, g\gamma)],$$

where (z, g) is a representative of x in $\mathcal{H} \times G(\mathbb{A}_{F,f})$, and $[(z, g\gamma)]$ is the projection of $(z, g\gamma)$ on X. One can show that $\mathrm{T}(m)$ is actually an algebraic correspondence on $\mathbb{S}_U$, i.e, defined by some divisor on $\mathbb{S}_U \times \mathbb{S}_U$ over F.

As in the modular curves or Hilbert modular varieties case, we may define the notion of modular forms on $\mathbb{S}_U$. Here we are only interested in forms of weight 2, namely functions on $\mathcal{H} \times G(\mathbb{A}_{F,f})$ such that $f(z, g)dz$ gives a holomorphic 1-form on the compactification of $\mathbb{S}_U$. One may define the Hecke operator $\mathrm{T}(m)$ on forms by the following formula:

$$\mathrm{T}(m)f(x) = \sum_{\gamma \in G_m/G_1} f([z, g\gamma]).$$

THEOREM 5.3 (Jacquet-Langlands). *Let f be a cusp form on $\mathbb{S}_U$ of weight 2 which is an eigenform of the Hecke operators $\mathrm{T}(m)$. Then there is a unique newform ϕ for $\mathrm{PGL}_2(\mathbb{A}_F)$ of weight $(2, \cdots, 2)$, with conductor N prime to m with the same eigenvalues of the Hecke operators. Moreover at each place v over which B is ramified, $\mathrm{ord}_v(N)$ is odd.*

We call $f \longrightarrow \phi$ a Jacquet-Langlands correspondence. We have the following converse:

THEOREM 5.4. *Assume that f is a newform for $\mathrm{PGL}_2(\mathbb{A}_F)$ of weight $(2, \cdots, 2)$ with level $U_0(N)$ such that $\mathrm{ord}_v(N)$ is odd when v is ramified in B. Then the Jacquet-Langlands correspondence of f exists and is unique on a Shimura curve $\mathbb{S}_U$ of type (N, K).*

Modular parameterization. In order to construct some points in the Jacobian $J_U := \mathrm{Jac}(\mathbb{S}_U)$ of $\mathbb{S}_U$ we need to define a map from $\mathbb{S}_U$ to J_U. In the modular curve case, one uses the cusp ∞ to send $x \in \mathbb{S}_U$ to the class of $x - \infty$ in J_U. In the general case, we use the Hodge class $\xi \in \mathrm{Pic}(\mathbb{S}_U) \otimes \mathbb{Q}$: the unique class whose degree is 1 on each connected component and such that

$$\mathrm{T}(m) = \deg(\mathrm{T}(m))\xi,$$

for all integral ideals m prime to the level of $\mathbb{S}_U$. Now each divisor x on $\mathbb{S}_U$ defines a point $\pi(x) := [x - \deg(x)\xi]$ in J_U. Notice that ξ can be analytically defined as follows. Write $\mathbb{S}_U(\mathbb{C})$ as a union $\coprod_i X_i$ of connected components of the form

$$X_i = \Gamma_i \backslash \mathcal{H} \coprod \{\text{cusps}\},$$

where $\Gamma_i \subset B_+^\times / F^\times \subset \mathrm{PGL}_2(\mathbb{R})$. Then one has $\mathrm{Pic}(\mathbb{S}_U)(\mathbb{C}) = \prod \mathrm{Pic}(X_i)$. The restriction of ξ on X_i is given by the formula:

$$\xi_i = \left\{ [\Omega^1_{X_i}] + \sum_{p \in X_i} (1 - u_p^{-1})[p] + [\text{cusps}] \right\} / \mathrm{vol}(X_i)$$

where for any non-cuspidal point $p \in X_i$, u_p denotes the cardinality of the group of stabilizer of $\widetilde{p}$ in Γ_i, where $\widetilde{p}$ is a lifting of p in $\mathcal{H}$. Now we can map $\mathbb{S}_U$ to its Jacobian (modulo torsion) by sending $x \in X$ to the class of $x - \deg(x)\xi$, where $\deg(x)$ is the multi-degree of x on the connected components. We take this as a certain standard embedding:

DEFINITION 5.5. *A morphism π from a Shimura curve $\mathbb{S}_U$ to an abelian variety is called admissible if $\pi(\xi) = 0$. Let $\mathrm{Hom}(X, A)$ denote the group of admissible parameterizations.*

Now we have the following reformulation of Theorem 5.4.

THEOREM 5.6. *Let X be a Shimura curve of type (N, K). Let f be a newform for $\mathrm{PGL}_2(\mathbb{A}_F)$ of weight $(2, \cdots, 2)$ with level structure $U_0(N)$ such that $\mathrm{ord}_v(N)$ is odd when v is not split in B. Then there is a unique abelian variety A over $\mathbb{C}$ up to isogeny, and an admissible parameterization*

$$\pi : \quad X \longrightarrow A$$

such that

$$\pi^*(\Omega^1_A) = \oplus \mathbb{C} f^\sigma(z)dz.$$

Moreover any such A is of GL_2-type with multiplication by the subring $\mathcal{O}_\phi$ in $\mathbb{C}$ generated by Hecke eigenvalues for f.

Indeed, A can be constructed simply by integrations of forms f^σ. Now the Eichler-Shimura theory gives the following:

THEOREM 5.7. *The abelian variety in Theorem 5.6 is defined over F as a quotient of $\mathrm{Jac}(X)$ with L-function*

$$L(s, A) = \prod_{\sigma : \mathcal{O}_\phi \longrightarrow \mathbb{C}} L(s, \phi^\sigma).$$

Moreover $\mathrm{Hom}(X, A) \otimes \mathbb{Q}$ is a free module of rank 1 over $\mathrm{End}(A) \otimes \mathbb{Q}$.

Conversely, we have the following modularity conjecture:

CONJECTURE 5.8. *Let A be a simple abelian variety A over F of GL_2-type with conductor N. Then $\mathrm{Hom}(X, A) \otimes \mathbb{Q}$ is a free module of rank 1 over $\mathrm{End}(A) \otimes \mathbb{Q}$.*

6. CM-points and Heegner points

In this section, we state a Gross-Zagier formula given in [**95, 96**]. The original formulation for the modular curve $X_0(N)$ is in [**40**]. We will start with an adelic description of CM-points. Then we state our Gross-Zagier formula, and survey three related results in the classical case: the work of Gross-Kohnen-Zagier [**38**] on positions of Heegner points when the quadratic fields vary, the work of Kolyvagin [**53**] which actually gives an effective way to compute $E(\mathbb{Q})$, and the work of Goldfeld [**29**] on Gauss' class number problem.

CM-points. Let K be a fixed imaginary quadratic extension of F which is embedded into B. Let T denote the torus of G defined by $K^\times \subset B^\times$. A point $x \in \mathbb{S}_U$ is called a CM-point by K if it is represented by $(z, g) \in \mathcal{H}^\pm \times G(\mathbb{A}_f)$ with z fixed by a torus of $G(F)$ isomorphic to $K^\times/\mathbb{Q}^\times$. Let z_0 be the unique point in $\mathcal{H}$ fixed by $T(F)$. Then the set C_U of CM-points by K is identified with

$$C_U = G(F)_+ \backslash G(F)_+ z_0 \times G(\widehat{F})/U = T(F) \backslash G(\widehat{F})/U.$$

All points of C_U are defined over the maximal abelian extension K^{ab} of K. The Galois action of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ on C_U is given by class field theory

$$T(\mathbb{A}_f) \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

and the inverse multiplication of $T(\mathbb{A}_f)$ from the left hand side. The projective limit C of C_U is identified with

$$C = T(\mathbb{Q}) \backslash G(\mathbb{A}_f).$$

It admits both a Galois action of $T(\widehat{F})$ and a Hecke action of $G(\widehat{F})$.

We may also give a modular interpretation of CM-points. In particular when $F = \mathbb{Q}$, a point on $\mathbb{S}_U$ representing (A, ι, κ) has CM by K if and only if $\mathrm{End}_B(A) \otimes \mathbb{Q} \simeq K$. If this is the case, then the action of K on $\mathrm{Lie}(A)$ gives an embedding $K \longrightarrow \mathbb{C}$. Moreover, since $B \otimes K \simeq M_2(K)$, A must be isogenous to a product $E \oplus E$ of elliptic curves with CM by K. The main theorem of complex multiplication still works here.

A CM-point on a Shimura curve X of type (N, K) is called a Heegner point if it is represented by $[z, g]$ where z is fixed by $T(F)$ and $g \in T(\widehat{F})$. As we see from above, all these Heegner points are defined over the Hilbert class field H of K and all conjugates of $x = [z, 1]$.

Let f be a newform of level N. Then we have a parameterization $\pi \in \mathrm{Hom}(X, A) \otimes \mathbb{Q}$. Define

$$y_K := u_x^{-1} \sum_{\sigma \in \mathrm{Gal}(H/K)} \pi(x^\sigma) \in A(K) \otimes \mathbb{Q}$$

and let $y_f \in A(K) \otimes \mathbb{C}$ be the f-isotypical component of z. Then we have the following:

THEOREM 6.1 ([**95**]). *Let $L_K(s, f)$ denote the product $L(s, f)L(s, \epsilon, f)$ where $L(s, \epsilon, f)$ is the L-function of f twisted by ϵ. Then $L_K(1, f) = 0$ and*

$$L'_K(1, f) = \frac{(8\pi^2)^g}{d_F^2 \sqrt{d_K}} [U_0(1) : U_0(N)] \|f\|^2 \|y_f\|^2,$$

where

1. *$\|y_f\|^2$ is the Neron-Tate height of z_f;*
2. *d_F is the discriminant of F, and d_K is the norm of the relative discriminant of K/F;*
3. *$\|f\|^2$ is inner product with respect to the standard measure on*

$$Z(\mathbb{A}_F)\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A}_F).$$

When $F = \mathbb{Q}$ and every prime factor of N splits in K, this is due to Gross and Zagier [**40**]. In this case, a point x on $X_0(N)(\mathbb{C})$ is a Heegner point of order $\mathcal{O}_K$ if x represents an isogeny

$$\phi: \quad E_1 \longrightarrow E_2$$

such that

$$\mathrm{End}(E_1) \simeq \mathrm{End}(E_2) \simeq \mathcal{O}_K.$$

Fix one embedding $K \longrightarrow \mathbb{C}$. Then one has ideals $\mathfrak{a} \subset \mathfrak{b}$ such that

$$E_1 \simeq \mathbb{C}/\mathfrak{a}, \qquad E_2 \simeq \mathbb{C}/\mathfrak{b}.$$

The morphism ϕ is then induced by the natural morphism

$$\mathbb{C}/\mathfrak{a} \longrightarrow \mathbb{C}/\mathfrak{b}.$$

Now the kernel is

$$\mathbb{Z}/N\mathbb{Z} \simeq \mathfrak{b}/\mathfrak{a} \simeq \mathcal{O}_K/\mathfrak{n}$$

where $\mathfrak{n} = \mathfrak{a} \cdot \mathfrak{b}$. Obviously the existence of a Heegner point of order $\mathcal{O}_K$ is equivalent to the existence of such $\mathfrak{n}$ which is equivalent to the following so called *Heegner condition*:

Every prime factor p of N is either split or ramified in $\mathcal{O}_K$.

Once the Heegner condition is satisfied, there will be $2^s h_K$ Heegner points, where s is the number of prime factors of N split in $\mathcal{O}_K$, and h_K is the class number of K. More precisely, the map

$$x \longrightarrow ([\mathfrak{a}], \mathfrak{n})$$

defines an bijection between the Heegner points of $\mathcal{O}_K$ and the pairs of an ideal class $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_K)$ and an ideal $\mathfrak{n}$ of $\mathcal{O}_K$ such that $N\mathcal{O}_K = \mathfrak{n} \cdot \bar{\mathfrak{n}}$.

By the theory of complex multiplication, all Heegner points are defined over the Hilbert class field H of K. The action of $\mathrm{Gal}(H/K) \simeq \mathrm{Pic}(\mathcal{O}_K)$ is given by the inverse multiplication of $\mathrm{Pic}(\mathcal{O}_K)$.

For the proof of Theorem 3.9, we assume that $L(s, E)$ has order less than or equal to 1. By some anaytic result, there is a K such that $L_K(s, E)$ has order equal to 1 at $s = 1$. It follows from the above theorem that z_f has infinite order. Then Theorem 3.9 follows from Kolyvagin's method.

Position of Heegner points. Let E be an modular elliptic curve defined over a totally real field F such that $L(s, E)$ has order 1 at $s = 1$. Then by Theorem 3.9,

$$E(F) \otimes \mathbb{Q} \simeq \mathbb{Q}.$$

Thus all Heegner points y_K are proportional. When $F = \mathbb{Q}$, even before Kolyvagin, the ratios of these y_K has been studied by Kohnen, Gross, Zagier:

THEOREM 6.2 (Gross-Kohnen-Zagier [**38**]). *Assume that* $F = \mathbb{Q}$, *and that* $\mathrm{ord}_{s=1} L(s, E$ 1. *Let* $f = \sum a_n q^n \in S_2(\Gamma_0(N))$ *correspond to* E *and let* $g = \sum_n c_n q^n \in S_{3/2}(\Gamma_0(4N))$ *be its Shimura lifting. Then for any imaginary quadratic extension* K *of discriminant* D, $y_K \neq 0 \in E(\mathbb{Q}) \otimes \mathbb{Q}$ *if and only if* $c_D \neq 0$, *and in the case*

$$y_K / c_D \in E(\mathbb{Q})_{\mathbb{Q}}$$

is independent of K.

Recall that the Fourier coefficients of f and g are related by the following formula:

$$a(n)c(-d) = \sum_{r|n} \left(\frac{d}{r}\right) c(-dn^2/r^2)$$

where $n \in \mathbb{N}$ and $d < 0$ a fundamental discriminant.

Example. We still consider the elliptic curve

$$E: \qquad y^2 - y = x^3 - x$$

p	3	7	11	47	67	71	83	107	127	139	151	211	223
c_p	1	1	1	1	6	1	1	0	1	0	2	3	3

d	4	40	84	95	104	111	115	120	123	136	148
c_d	1	2	1	0	0	1	6	2	3	4	3

Effectivity on Mordell group. Using his theory of Euler systems, Kolyvagin has finally proved the following:

THEOREM 6.3 (Kolyvagin [**53**]). *If y_K has infinite order, then $[E(\mathbb{Q}) : \mathbb{Z}y_K]$ is finite.*

Moreover the work of Kolyvagin allows us to compute $E(\mathbb{Q})$ and check effectively the following:

- the sign of the functional equation of $L(s, E)$;
- a Heegner point $y_K \in E(\mathbb{Q})$;
- the set $E(\mathbb{Q})/\mathbb{Z}y_K$ when y_K is of infinite order.

Gauss class number problem. For certain elliptic curve E of odd sign, one can show that the Heegner point is torsion. It follows that $L(s, E)$ vanishes at $s = 1$ with order ≥ 3. It follows from a result of Goldfeld [**29**] that:

THEOREM 6.4. *For any $\epsilon > 0$, there is an effective computational constant $\kappa(\epsilon) > 0$ such that*

$$h(D) > \kappa(\epsilon)(\log|D|)^{1-\epsilon}.$$

Forms of high weight. For an elliptic curve E with a CM by $\sqrt{D}$, let $Z(E)$ denote the divisor class on $E \times E$ of $\Gamma - E \times \{0\} - D\{0\} \times E$, where Γ is the graph of $\sqrt{D}$. For k a positive integer, then $Z(E)^{k-1}$ is a cycle of codimension $k-1$ in E^{2k-2}. Let $S_k(E)$ denote the cycle

$$c \sum_{g \in G_{2k-2}} \mathrm{sgn} g^*(Z(E)^{k-1}),$$

where G_{2k-2} denotes the symmetric group of $2k-2$ letters which acts on E^{2k-2} by permuting the factors, and c is a real number such that the self-intersection of $S_k(E)$ on each fiber is $(-1)^{k-1}$.

For N' a product of two relatively prime integers ≥ 3, recall that the Kuga-Sato variety $Y = Y_k(N')$ is defined to be a canonical resolution of the $2k-2$-tuple fiber product of the universal elliptic curve $\mathcal{E}(N')$ over $X(N')$. If y is a CM-point on $X(N')$, the CM-cycle $S_k(y)$ over x will be defined to be $S_k(\mathcal{E}_y)$ in Y.

For N a factor of N', if x a CM-divisor on $X_0(N)_{\mathbb{Z}}$, the CM-cycle $S_k(x)$ over x will be defined to be $\sum S_k(x_i)/\sqrt{\deg p}$, where p denotes the canonical morphism from $X(N')$ to $X_0(N)$, and $\sum x_i = p^* x$. One can show that $S_k(x)$ has zero intersection with any cycle of Y supported in the special fiber of $Y_{\mathbb{Z}}$, and that the class of $S_k(x)$ in $H^{2k}(Y(\mathbb{C}), \mathbb{C})$ is zero. So there is a green's current $g_k(x)$ on $Y(\mathbb{C})$ such that $\frac{\partial\bar{\partial}}{\pi i} g_k(x) = \delta_{S_k(x)}$. The arithmetic CM-cycle $\widehat{S}_k(x)$ over x, in the sense of Gillet and Soulé [**28**], is defined to be $(S_k(x), g_k(x))$.

If x and y are two CM-points on $X_0(N)$, then the height pairing of the CM-cycles $S_k(x)$ and $S_k(y)$ will be defined to be

$$\langle S_k(x), S_k(y) \rangle := (-1)^k \widehat{S}_k(x) \cdot \widehat{S}_k(y).$$

Let K be an imaginary quadratic field with the discriminant D, such that every prime factor of N is split in K. Let H denote the Hilbert class field of K. Let σ be a fixed element $\mathrm{Gal}(H/K)$, and $\mathcal{A}$ the ideal class in $\mathcal{O}_K$ corresponding to σ via the Artin map.

Set $s_K = \sum_{\sigma \in G} s_k(x^\sigma)$ where $s'_k(x^\sigma)$ is the image of $s_k(x^\sigma)$ in V'. Let $f \in S_{2k}^{\mathrm{new}}(\Gamma_0(N))$ be a normalized eigenform and let $s_{K,f}$ be the f-isotropic component of s_K.

THEOREM 6.5 ([**96**]).

$$L'_K(k,f) = \frac{2^{4k-1}\pi^{2k}(f,f)}{(2k-2)!u^2h\sqrt{|D|}}\langle s_{K,f}, s_{K,f}\rangle.$$

p-adic formulas. In [**67**], when $F = \mathbb{Q}$ and all prime factors of N split in K, Perin-Riou obtained a formula relating the first derivative of the two variable p-adic L-function of E/K to the p-adic height of the Heegner point $P_K \in E(K)$. This formula has been refined or extended by Rubin [**72**] for elliptic curves with complex multiplications, and by Nekovar [**64, 65**] to high forms with high weight.

7. L-functions with characters

In this section we study L-functions and Mordell-Weil groups twisted by various characters. The main reference is Mazur's paper [**60**]. We will start with basic definitions and the BSD conjecture in this context. The first family of characters considered here are L-functions with quadratic twists. This is the *horizontal case* called by B. Mazur. We will explain Goldfeld's conjecture on the average order of vanishing, and work of Waldspurger, Bump-Friedberg-Hoffstein, and Murty and Murty. The second family are L-series twisted by characters with bounded ramifications. This is the *vertical* case called by Mazur. We will state a generalization of a conjecture by Mazur on nonvanishing of L-series. A lot has been proved in the case $F = \mathbb{Q}$: the work of Rohrlich and Kato, and the work of Bertolini-Darmon and very recent work of Vatsal and Cornut. A better way to understand Mazur's conjecture is in context of p-adic L-functions and Iwasawa theory which unfortunately will not be covered here.

Now, we fix an elliptic curve E over a number field F and study $E(L)$ for some finite or infinite abelian extension L of F. When L/F is finite, by the Mordell-Well theorem, $E(L)$ is finitely generated and we have the following decomposition

$$E(L)\otimes\mathbb{C} = \oplus E(\chi)$$

where $\chi : \mathrm{Gal}(L/F) \longrightarrow \mathbb{C}^\times$ ranges through all characters, and $E(\chi)$ is the χ-eigen subspace in $E(L)\otimes\mathbb{C}$. On the other hand, the L-series series has the decomposition

$$L(s,E/L) = \prod_\chi L(s,\chi,E)$$

where $L(s,\chi,E)$ is the twist of $L(s,E)$ by a character χ. More precisely, assume that $L(s,E)$ has conductor N with good local factors at $v \nmid N$,

$$(1 - a_v q_v^{-s} + q_v^{1-2s})^{-1},$$

and that χ has conductor c, then $L(s,\chi,E)$ has a local term at $v \nmid cN$ given by

$$(1 - a_v\chi(\mathrm{Frob}_v)q_v^{-s} + \chi(\mathrm{Frob}_v)^2 q_v^{1-2s})^{-1}.$$

Again, to understand the bad factors, one can look at the representation of $\mathrm{Gal}(\bar{F}/F)$ on $\mathrm{T}_\ell(E)$ twisted by the character χ to obtain

$$\det(1 - \mathrm{Frob}(v)|_{\mathrm{T}_\ell(E)(\chi)^{I_v}})^{-1},$$

where $\mathrm{T}_\ell(E)(\chi)$ denotes the usual Tate module with action twisted by χ. Notice that both $E(\chi)$ and $L(s,\chi,E)$ depends only on the composition $\chi : \mathrm{Gal}(\bar{F}/F) \longrightarrow \mathbb{C}^\times$. The Birch and Swinnerton-Dyer conjecture for E/L can be refined as follows:

CONJECTURE 7.1. *For any character χ of $\mathrm{Gal}(\bar{F}/F)$, one has*

$$\dim E(\chi) = \mathrm{ord}_{s=1} L(s, \chi, E).$$

Here we already assume the holomorphic continuation of $L(s, \chi, E)$ and the functional equation:

$$L(s, \chi, E) = \epsilon(s, \chi, E) \cdot L(2 - s, \chi^{-1}, E)$$

Quadratic characters. The first example we want to consider is the case of quadratic twists. To be more precise, we fix one elliptic curve E as above and consider the quadratic characters $\chi : \mathrm{Gal}(\bar{F}/F) \longrightarrow \{\pm 1\}$. Obviously, χ is uniquely determined by a unique element $d \in F^\times/(F^\times)^2$ such that χ factors through $\mathrm{Gal}(K/F)$ for some $K = F(\sqrt{d})$. It is not difficult to show that

$$L(s, \chi, E) = L(s, E^{(d)})$$

where

$$E^{(d)} : \quad y^2 = x^3 + ad^2x + bd^3.$$

Thus the study of the family of $E(\chi)$ and $L(s, \chi, E)$ is the same as the study of the Mordell-Weil groups and L-series of the family of twisted elliptic curves $E^{(d)}$, or in other words, the family of elliptic curves over F with the *same j-invariant* as E when $j \neq 0, 1728$.

It is interesting thing to the following simple rule of changes of signs of $E^{(d)}$. Assume that d is prime to N (the conductor of E), the conductor of E, then we have

$$\mathrm{sgn}(E) \cdot \mathrm{sgn}(E^{(d)}) = (-1)^{\Sigma},$$

where Σ is a finite set of places of F, consisting of places dividing ∞ or N which are non-split in K. If we order χ by the norm of its conductor, then there are about 50% of $E^{(d)}$ having sign $+1$ and 50% having sign -1. It is conjectured that the rank r of $E^{(d)}(F)$ can be as large as possible but the case $r > 1$ occurs 0% of the time. Thus 1/2 of elliptic curves have rank 1, and 1/2 of elliptic curves have rank 0. Modulo the BSD conjecture, one should have the same estimate for the analytic rank:

CONJECTURE 7.2 (Goldfeld[**30**]). *If we order χ by the norm of its conductor, then at $s = 1$, 50% of $L(s, E^{(d)})$ have order 0 and 50% have order 1.*

This conjecture is still open. Recently, the following results were proved by Waldspurger [**89, 90**], Bump-Friedberg-Hoffstein [**12**], Murty-Murty [**63**]:

THEOREM 7.3. *Let Σ be a finite set of places of F and let $\bar{d}_v$ be a class of $F_v^\times/(F_v^\times)^2$ for each $v \in \Sigma$. Then there is a $d \in F^\times$ such that $d \in \bar{d}_v$ for each $v \in \Sigma$ and that*

$$\mathrm{ord}_{s=1} L(s, E^{(d)}) \leq 1.$$

THEOREM 7.4. *The sequence of $L(1, E^{(d)})$ is proportional to the coefficients of Shimura's lifting of a form corresponding to E.*

See also Kazta-Sarnak [**51**] for some interpretation in terms of random matrices, and Ono-Skinner [**68**] for examples of positive density results.

While much is understood about the 50% of those elliptic curves having rank 0 since the estimate of Mazur and Merel, but what can we say about the 50% of those elliptic curves having rank 1? For example,

Does there exist a generic way to construct a solution when the rank is 1*?* This is probably the main motivation of the work of Gross-Zagier.

Example. Let E be the elliptic curve of conductor 37 defined by

$$E: \qquad y^2 = 4x^3 - 4x + 1$$

and let $E^{(d)}$ be its quadratic twists:

$$E^{(d)}: \qquad y^2 = 4x^3 - 4d^2x + d^3.$$

We consider the 22 fundamental discriminants satisfying $-150 < d < 0$ and

$$\Sigma = \{\infty, 37\}.$$

The following 18 of them $E^{(d)}$ have rank 0:

-3, -4, -7, -11, -40, -47, -67, -71, -83, -84, -111, -115, -120, -123, -127, -132, -136, -148.

The following 4 of them $E^{(d)}$ have rank ≥ 2:

-95, -104, -107, -139.

Also, for the following fundamental d's between 0 and -150 with

$$\Sigma(d) = \{37\},$$

the curve $E^{(d)}$ has rank 1:

-8, -15, -19, -20, -23, -24, -31, -35, -39, -43, -51, -52, -53, -55, -56, -59, -68, -79, -87, -116, -119, -131, -143

The following table gives the x-coordinates of generators of $E^{(d)}$:

d	-8	-15	-19	-20	-23	-24	-31	-35	-39
x	-4	-5	-2831/324	-15	46	-20	310/9	-55/4	-26

Characters with bounded ramifications. Now let Σ be a fixed finite set of finite places of F. One considers the family of characters χ unramified outside of Σ, i.e., the characters factor through $\mathrm{Gal}(F_\Sigma^{\mathrm{ab}}/F)$ where F_Σ^{ab} denotes the maximal abelian extension of F unramified outside of Σ. It can be shown that the group $\mathrm{Gal}(F_\Sigma^{\mathrm{ab}}/F)$ is topologically finitely generated.

In the following we would like to define the so called *minimal order of* $L(s, \chi, E)$. It is well known that $L(s, \chi, E) = L(s, M)$ for

$$M := \mathrm{Ind}_{G_F}^{G_{\mathbb{Q}}}(\mathrm{T}_\ell(E)(\chi)).$$

Let $\oplus M_i$ be semi-simplification of M as $G_{\mathbb{Q}}$-modules where M_i are irreducible. Then we have the decomposition

$$L(s, \chi, E) = L(s, M) = \prod_i L(s, M_i),$$

and each M_i has functional equation

$$L(s, M_i) = \epsilon(s, M_i) L(2 - s, M_i^\vee)$$

where

$$M_i^\vee = \mathrm{Hom}(M, \mathbb{Z}_\ell(1)).$$

We define the minimal order of $L(s,\chi,E)$ to be

$$m(\chi,E) := \#\{i: \quad M_i \simeq M_i^\vee, \quad \epsilon(1,M_i) = -1\}$$

Then of course,

$$\mathrm{ord}_{s=1} L(s,\chi,E) \geq m(\chi,E).$$

One expects $\mathrm{ord}_{s=1} L(s,\chi,E)$ and $E(\chi)$ to be as small as possible:

CONJECTURE 7.5 (Generalized Mazur Conjecture). *For all but finitely many characters χ unramified outside of Σ,*

$$\mathrm{ord}_{s=1} L(s,\chi,E) = m(\chi,E).$$

When $F=\mathbb{Q}$, $m(\chi,E)=0$ unless χ is quadratic with sign -1. In this case the conjecture is true:

THEOREM 7.6 (Rohlich [**69, 70**]). *Assume that $F=\mathbb{Q}$. For all but finitely many χ unramified outside of Σ,*

$$L(1,\chi,E) \neq 0.$$

THEOREM 7.7 (Kato [**48**]). *Assume that $F=\mathbb{Q}$. Let χ be a character such that $L(1,\chi,E)\neq 0$ then $E(\chi)=0$.*

Anticyclotomic characters. Let E be defined over a number field F, K a quadratic extension of F, and χ a character of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. We want to consider the L-series

$$L(s,\chi,E) := L(s,\chi,E_K)$$

where E_K denote the base change of E to K. Then the group of such characters has an involution defined by

$$\chi \longrightarrow {}^c\chi, \qquad {}^c\chi(\sigma) = \chi(c\sigma c^{-1}),$$

where $c\in \mathrm{Gal}(K^{\mathrm{ab}}/F)$ extends the conjugation on K/F. Since $L(s,\chi)=L(s,{}^c\chi)$ one obtains

$$L(s,\chi,E) = \epsilon(s,\chi,E)\cdot L(2-s,{}^c\chi^{-1},E).$$

DEFINITION 7.8. *A quasi-character χ is called anticyclotomic (resp. cyclotomic) if*

$${}^c\chi = \bar{\chi} \qquad (\textit{resp.}\ {}^c\chi = \chi).$$

If χ is cyclotomic, then χ is factored by a character χ_F of $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ and

$$L(s,\chi,E) = L(s,\chi_F,E)\cdot L(s,\chi_F,E^{(d)}).$$

Almost every character χ can be written as a product of a cyclotomic character χ_+ and an anticyclotomic character χ_-.

From now on, we assume that χ is anti-cyclotomic. In this case, the functional equation will read as

$$L(s,\chi,E) = \epsilon(s,\chi,E)L(2-s,\chi,E).$$

Let $s=1$. One obtains that

$$\epsilon(\chi,E) := \epsilon(1,\chi,E) = \pm 1.$$

Moreover, if we further assume that the discriminant $d_{K/F}$ of K/F, the conductor N_E of E, and the conductor $c(\chi)$ of χ are all coprime, then the sign does not depend on χ.

When $F = \mathbb{Q}$ we may compute $m(\chi, E)$ as follows. Notice that

$$\mathrm{Ind}_K^{\mathbb{Q}}(\mathrm{T}_\ell(E)(\chi)) = \mathrm{T}_\ell(E) \otimes \mathrm{Ind}_K^{\mathbb{Q}}(\chi),$$

which is irreducible if E does not have CM by K. Otherwise

$$\mathrm{T}_\ell(E) = \mathrm{Ind}_K^{\mathbb{Q}}(\psi), \qquad \mathrm{Ind}_K^{\mathbb{Q}}\mathrm{T}_\ell(E)(\chi) = \mathrm{Ind}_K^{\mathbb{Q}}(\chi\psi) \oplus \mathrm{Ind}_K^{\mathbb{Q}}(\chi\bar{\psi}),$$

where ψ is an anticyclotomic character of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ with values in $K_\ell^\times$. Notice that $L(s, \chi\phi)$ and $L(s, \bar{\chi}\phi)$ have the same sign and $\dim E(\chi)$ is even as $E(\chi)$ is a free module of $K \otimes_{\mathbb{Q}} \mathbb{C} = \mathbb{C}^2$.

DEFINITION 7.9. *We say (χ, E) is in the exceptional case if E has CM by K and both $L(s, \chi\psi)$ and $L(s, \bar{\chi}\psi)$ have an odd sign in their functional equations.*

Thus we have the following:

LEMMA 7.10. *When $F = \mathbb{Q}$ and χ is anticyclotomic, the values of $m(\chi, E)$ are given as follows:*

$$m(\chi, E) = \begin{cases} 2 & \text{if } (\chi, E) \text{ is exceptional,} \\ 1 & \text{if } \mathrm{sgn}(\chi, E) = -1, \\ 0 & \text{otherwise.} \end{cases}$$

Ring class characters. By class field theory, there is one-to-one correspondence between the set of finite characters of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ and the set of finite characters of $\mathbb{A}_K^\times/K^\times$. A character χ on $\mathbb{A}_K^\times$ is anti-cyclotomic iff $\chi(\bar{x}) = \overline{\chi(x)}$. Or in other words, χ-factors through $\mathbb{A}_K^\times/\mathrm{N}_{K/F}(\mathbb{A}_K)K^\times$. Thus a character is anti-cyclotomic if and only if its restriction on $\mathbb{A}_F^\times$ is either trivial or equal to the quadratic character corresponding to the extension K/F.

DEFINITION 7.11. *A character of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is called a ring class character if the corresponding character on $\mathbb{A}_K^\times$ factors through $\mathbb{A}_K^\times/\mathbb{A}_F^\times$.*

In the rest of this section, we restrict ourselves to an imaginary quadratic extension $K/\mathbb{Q}$. Then any ring class character factors through $\mathbb{A}_K^\times/\widehat{\mathcal{O}}_c^\times$ for some positive integer c, where $\mathcal{O}_c$ is an order of K of conductor c defined by

$$\mathcal{O}_c = \mathbb{Z} + \mathbb{Z}c\tau, \qquad \text{if} \qquad \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\tau_K.$$

Then one can show that $j(\mathcal{O}_c) = j(c\tau_K)$ is an algebraic integer. One defines H_c, the ring class field of K of order c, to be $K(j(c\tau_K))$. Class field theory establishes an isomorphism of groups

$$\mathrm{Gal}(H_c/K) \simeq \mathrm{Pic}(\mathcal{O}_c)$$

where $\mathrm{Pic}(\mathcal{O}_c)$ denotes the group of invertible $\mathcal{O}_c$-ideal classes. The minimal c is the conductor of χ.

Assume that d_K, N are coprime, and let χ be a ring class character of conductor c prime to $d_K N$. Then the sign of the functional equation is given by

$$\epsilon(\chi, E) = \epsilon(N) = (-1)^\Sigma,$$

where Σ is the set places p where N is a norm from $K \otimes \mathbb{Q}_p$.

The combination of the Gross-Zagier formulas explained in the next sections [**96**], the work of Vatsal [**86, 87**], Cornut [**13**] on nonvanishing of Heegner points, and the work of Bertolini-Darmon [**2, 3**] on Euler system gives the following:

THEOREM 7.12. *Assume the following:*

1. $F = \mathbb{Q}$,
2. *E is not exceptional,*
3. *for each prime p dividing N, either p is split in K, or p is innert in K and* $\mathrm{ord}_p(N) = 1$,
4. *Σ does not contain any prime dividing N and discriminant d of $K/\mathbb{Q}$.*

Then for all but finitely many characters of χ unramified outside of Σ,

$$\mathrm{ord}_{s=1} L(s, \chi, E) \leq 1.$$

THEOREM 7.13. *Assume the following:*

1. $F = \mathbb{Q}$,
2. *E is not exceptional,*
3. *each prime p dividing N, either p is split in K, or p is innert in K and* $\mathrm{ord}_p(N) = 1$,
4. *χ has conductor prime to Nd,*
5. $$\mathrm{ord}_{s=1} L(s, \chi, E) \leq 1.$$

Then

$$\mathrm{ord}_{s=1} L(s, \chi, E) = \dim E(\chi).$$

8. CM-points with characters

In this section we want to describe some Gross-Zagier formulas for L-functions with characters proved in [**96**]. We will first define the conductors and orientations of CM-points on Shimura curves or varieties of (N, K)-type using Gross' idea of *optimal embedding*. Then the Gross-Zagier formulas give relations between central derivatives (resp. central values) of L-series and the heights (resp. periods) of these CM-points with the same conductor as anti-cyclotomic characters. Since the formulas were originally proved on towers of Shimura curves, consequently the constants in the Gross-Zagier formulas on Shimura curves of (N, K) have not yet been well computed in this context. We then state a generalized Mazur's conjecture and BSD conjecture on non-vaninshing of these CM-points. When $F = \mathbb{Q}$, these conjectures are theorems of Bertolini-Darmon, Vatsal, and Cornut. At the end of this section we will give some application of central value formula to equidistribution of *toric orbits* of CM-points on quaternion Shimura varieties. These equidistribution results are motivated by the Andre-oort conjecture and are proved by using the *subconvexity bound* of Cogdell, Piatetski-Shapiro, and Sarnak.

CM-points of type (N, K). Now let's fix a Shimura curve X of type (N, K) which is the generalization of $X_0(N)$. Then the set of CM-points on X is given by

$$C_U = G(F)_+ \backslash \mathrm{GL}_2(F)_+ z_0 \times G(\widehat{F})/U = T(F) \backslash G(\widehat{F})/U,$$

where $U = Z(\widehat{F})\widehat{R}^\times$ with R an order of B containing $\mathcal{O}_K$ of relative discriminant N. Thus, the set of CM-points admits an action by Hecke operators $\mathrm{T}(m)$ for m prime to N, and Galois actions of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ via class field theory and multiplication of $T(\widehat{F})$ from the left hand side.

For a CM-point z represented by $g \in G(\widehat{F})$, let ϕ_g denote the homomorphism

$$K \longrightarrow \widehat{B}, \qquad z \longrightarrow g^{-1} z g.$$

The order

$$\mathrm{End}(z) := \phi_g^{-1}(R),$$

which does not depend on the choice of g, and is called the *order* of z. The ideal c of $\mathcal{O}_F$, such that

$$\mathrm{End}(z) = \mathcal{O}_F + c\mathcal{O}_K$$

is called the conductor of z. For each prime $\wp$ not dividing c, the homomorphism ϕ_g defines an orientation in

$$U_\wp := \mathrm{Hom}(\mathcal{O}_{K,\wp}, R_\wp)/R_\wp^\times.$$

This set has only one element if $\wp$ does not divide N; otherwise it has two elements: the positive orientation defined by our fixed embedding $K \longrightarrow B$, and the negative orientation defined by the conjugate of the positive one.

The curve X admits an action by the group

$$\mathcal{W} := \left\{ b \in \widehat{B}^\times : \quad b^{-1}\widehat{R}^\times b = \widehat{R}^\times \right\} / \widehat{R}^\times.$$

This group has 2^s elements, where s is the number of prime factors of N. The action of $\mathcal{W}$ on CM-points does not change orders, and the induced action on the set of *orientations* $\prod_{\wp|N} U_\wp$ is free and transitive.

Let Y_c denote the subset of CM-points of conductor c with positive orientations. Then Y_c is stable under the action of $\mathrm{Gal}(\bar{K}/K)$ and each point is defined over the ring class field H_c of K of conductor c. More precisely, Y_c is identified with

$$K^\times \backslash \widehat{K}^\times g_c \widehat{R}^\times / \widehat{R}^\times \simeq K^\times \backslash \widehat{K}^\times / \widehat{\mathcal{O}}_c^\times$$

where g_c is some fixed element. The Galois action of $\mathrm{Gal}(H_c/K)$ on Y_c is given by the inverse of the Artin map

$$\mathrm{Gal}(H_c/K) \simeq K^\times \backslash \widehat{K}^\times / \widehat{\mathcal{O}}_c^\times.$$

Let f be a Hilbert newform for $\mathrm{PGL}_2(\mathbb{A}_F)$ of weight $(2, \cdots, 2)$ with level $U_0(N)$. Let A be an abelian variety over F corresponding to f. Then we have an admissible parameterization

$$\pi : \quad X \longrightarrow A.$$

Let χ be a ring class character of $\mathrm{Gal}(\bar{K}/K)$ of conductor c prime to N and $d_{K/F}$. Then we can define a point

$$y_\chi := \sum_{\sigma \in \mathrm{Gal}(H_c/K)} \chi^{-1}(\sigma)\pi(y_c^\sigma) \in A(\chi)$$

where y_c is represented by g_c.

We have the following generalization of the Gross-Zagier formula:

THEOREM 8.1. *Let $y_{f,\chi}$ be the f-typical component of y_χ. Then $L(1,\chi,f) = 0$ and*

$$L'(1,\chi,f) = \kappa \cdot \|y_{f,\chi}\|^2 \cdot \|f\|^2.$$

Here c is a positive constant.

Notice that κ has been computed in terms of *quasi-newforms and χ-newforms* in [**96**] but has not yet been explicitly computed in the context of Shimura curves of (N,K)-type. But it is known that κ is a product of local constants κ_v at places dividing ∞, N, d, $c(\chi)$, and that κ_v depends only on the local components of representations at v of χ and Π corresponding to f.

One consequence of this theorem is the following restatement of the Birch and Swinnerton-Dyer conjecture and Mazur's conjecture of the last section:

CONJECTURE 8.2 (Birch and Swinnerton-Dyer conjecture). *Assume that $y_{f,\chi}$ is nonzero in $A(\chi)$. Then the f-typical component $A(\chi)_f$ of $A(\chi)$ has dimension equal to* 1.

CONJECTURE 8.3 (Generalized Mazur Conjecture). *For all but finitely many characters unramified outside of an fixed finite set Σ of places of F,*

$$y_{f,\chi} \neq 0$$

in $A(\chi)_f$.

A lot have been proved in case $A = E$ is an elliptic curve defined over $F = \mathbb{Q}$.

THEOREM 8.4 (Cornut [**18**], Vatsal [**86**]). *Assume the following:*

1. $F = \mathbb{Q}$,
2. *E is not exceptional,*
3. *for each prime p dividing N, either p is split in K, or p is innert in K and* $\mathrm{ord}_p(N) = 1$,
4. *Σ does not contain any prime dividing N and discriminant d of $K/\mathbb{Q}$.*

Then for all but finitely many characters of χ unramified outside of Σ,

$$y_\chi \neq 0 \qquad in \qquad E(\chi).$$

THEOREM 8.5 (Bertolini-Darmon [**2**]). *Assume the following*

1. $F = \mathbb{Q}$,
2. *E is not exceptional,*
3. *for each prime p dividing N, either p is split in K, or p is innert in K and* $\mathrm{ord}_p(N) = 1$,
4. *χ has conductor prime to Nd,*
5. *$y_\chi \neq 0$ in $E(\chi)$*

Then

$$\dim E(\chi) = 1.$$

Central values. Now we would like to have a similar formula for the central value $L(1, \chi, E)$ when the sign of the functional equation of $L(s, \chi, E)$ is $+1$. We actually will consider a much more general case $L(s, \chi, f)$ where f is a Hilbert newform form for $\mathrm{PGL}_2(\mathbb{A}_F)$ with level N, which is holomorphic in $g - d$ variables of weight 2 and nonholomorphic in d variables of weight 0. Again, we assume that the conductor N of f, the discriminant d of K/F and conductor c of χ are all coprime to each other. The Gross-Zagier formula is then an expression:

$$L(1, \chi, f) = c \cdot \|x\|^2,$$

where c is a positive constant and x is a periodic integral of some forms on certain Shimura varieties described as follows.

Quaternion Shimura varieties. Let Σ be the set of places of F consisting of archimedean places where f has weight 2 and nonarchimedean places v where $\epsilon_v(N) = -1$. Since the functional equation $L(s, \chi, f)$ has sign $+1$, Σ has even cardinality. Then there is a unique quaternion algebra B over F which is ramified exactly over Σ. Let G denote $B^\times$ as an algebraic group over F. Let S denote the subset of archimedean places in Σ. Let d denote the cardinality of S. Then there is an isomorphism

$$B \otimes \mathbb{R} \simeq M_2(\mathbb{R})^d \oplus \mathbb{H}^{g-d}$$

over $F \otimes \mathbb{R}$. Further, the group $G(F)_+$ of elements in $G(F)$ of positive norms, act on the product $\mathcal{H}^d$ of d copies of the Poincare upper-half plane. Now for each open subgroup U of $G(\mathbb{A}_f)$ which is compact modulo the center $Z(\widehat{F})$, one has a Shimura variety

$$\mathbb{S}_U := G(F)_+ \backslash \mathcal{H}^d \times G(\mathbb{A}_f)/U. \tag{8.1}$$

By Shimura's theory [**19**], every variety M_U is actually defined over the following *reflexive field*:

$$E = \mathbb{Q}\left(\sum_{\sigma \in S} \sigma(x) : \quad x \in F\right). \tag{8.2}$$

The action of $\mathrm{Gal}(\bar{E}/E)$ on the set of connected components

$$Z_U := F_+ \backslash \mathbb{A}_f / \det U \tag{8.3}$$

is a composition of the following maps:

- the reciprocity law:
$$\mathrm{Gal}(\bar{E}/E) \longrightarrow E^\times \backslash \mathbb{A}_{E,f}^\times;$$
- an algebraic map of algebraic groups over F:
$$r : \quad E^\times \longrightarrow F^\times,$$
which induces a map of corresponding ideles;
- the left multiplication of $\mathbb{A}_f^\times$ on Z_U.

To define r, we let $\mathrm{Hom}^*(F, \mathbb{C})$ denote all embeddings of F into $\mathbb{C}$ which is a left $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$-set. The stabilizer of S is exactly $\mathrm{Gal}(\mathbb{C}/E)$. Then r is given such that for any $x \in E$ and any embedding $\sigma : F \longrightarrow \mathbb{C}$,

$$\sigma(r(x)) = \prod_{\tau : \sigma \in \tau S} \tau(x) \tag{8.4}$$

where τ runs through a set of representatives of the quotient $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})/\mathrm{Gal}(\mathbb{C}/E)$.

As in the case of Shimura curves, there are also Shimura varieties X of type (N, K). More precisely, let K be an totally imaginary quadratic extension of F embedded into B. Let R be an order of B containing $\mathcal{O}_K$ with discriminant N. Shimura variety is obtained by taking $U = \widehat{F}^\times \cdot \widehat{R}^\times$. The following is a consequence of Jacquet-Langlands theory:

THEOREM 8.6. *There is a one to one correspondence $f \longrightarrow \widetilde{f}$ between the set of newforms f on $\mathrm{PGL}(\mathbb{A}_F)$ of conductor N, weight $(0, \cdots, 2, \cdots)$, and the set of newforms on X of weight $(0, \cdots, 0)$ such that f and $\widetilde{f}$ have the same eigenvalues under the Hecke operators T_v when v prime to N.*

CM-points. Let T denote the subgroup $K^\times$ of G. Then T has a fixed point z_0 in $\mathcal{H}^d$. A point x on $\mathbb{S}_U$ is called a CM-point by K, if it is represented by (z, g) with $z \in G(F)_+ \cdot z_0 \subset \mathcal{H}^d$ and $g \in G(\mathbb{A}_f)$. Thus, the set of CM-points by K on $\mathbb{S}_U$ is identified with

$$\begin{aligned} C_U :=& G(F)_+ \backslash G(F)_+ \cdot z_0 \times G(\mathbb{A}_f)/U \\ =& T(F) \backslash G(\mathbb{A}_f)/U. \end{aligned} \tag{8.5}$$

Similarly, the set of CM-points C_U is defined over a reflexive field:

$$E_T = \mathbb{Q}\left(\sum_{\sigma\in S}\sigma(x): \quad x\in K^\times\right),$$

where each place $\sigma \in S$ is lifted to an embedding $\sigma : K \longrightarrow \mathbb{C}$ such that the image of each $x \in K^\times$ in $G_\sigma(\mathbb{R})_+ \simeq \mathrm{GL}_2(\mathbb{R})_+$ is conjugate to $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ if $\sigma(x) = a + bi$. The action of $\mathrm{Gal}(\bar{E}_T/E_T)$ on C_U is given by the exact same formulation as above.

Just as in the case of Shimura curves, we may also define a CM-point y_0 on the Shimura variety X of (N, K)-type of conductor c, and define a certain period $y_{f,\chi}$ for a character χ as follows: Let f be a newform for $\mathrm{PGL}_2(\mathbb{A}_F)$ of level $U_0(N)$ corresponding to a form $\widetilde{f}$ of weight 0 on X. Then we define

$$y_{f,\chi} := \sum_{t\in K^\times\backslash\widehat{K}^\times/\widehat{F}^\times\widehat{\mathcal{O}}_c^\times} \chi(t)^{-1}\widetilde{f}(ty_0) \in \mathbb{C}.$$

The Gross-Zagier formula (for the central value) we want to prove is the following:

THEOREM 8.7. *With notation as above,*

$$L(1,\chi,f) = c\cdot|y_{f,\chi}|^2$$

where c is a positive constant.

When $F = \mathbb{Q}$, N is prime, and χ is unramified, this formula is due to Gross [**37**] and generalized by Hatcher [**41**] to modular form of high weights. In his thesis at Columbia, H. Xue [**92**] has obtained a full generalization to forms of high weight.

Some related formula have been also obtained by Waldspurger [**89**], Kohnen-Zagier [**55**], and Katok-Sarnak [**49**].

Nonvanishing of periods. In view of the BSD-conjecture and Mazur's conjecture one should have the following:

CONJECTURE 8.8 (Generalized Mazur's conjecture). *Let Σ be a finite subset of F. Then for all but finitely many ring class characters χ unramified outside of Σ, one has*

$$y_{f,\chi} \neq 0.$$

CONJECTURE 8.9 (Birch and Swinnerton-Dyer conjecture). *Assume that f is holomorphic and corresponds to an abelian variety A, and that $y_{f,\chi} \neq 0$. Then $A(\chi)$ is finite.*

Mazur's original conjecture is for the classical case and has been proved by Vatsal:

THEOREM 8.10 (Vatsal [**86**]). *Assume the following:*

1. *$F = \mathbb{Q}$,*
2. *f is holomorphic of weight 2,*
3. *for every $p \mid N$, either p is inert in K and $\mathrm{ord}_p(N) = 1$, or p is split in K.*

Then Mazur's conjecture is true.

Let E be the elliptic curve corresponding to f. Then we have following result concerning the Birch and Swinnerton-Dyer conjecture

THEOREM 8.11 (Bertolini-Darmon [**3**]). *Assume the following:*

1. $F = \mathbb{Q}$,
2. *f is holomorphic of weight 2,*
3. *for every $p \mid N$, either p is inert in K and $\mathrm{ord}_p(N) = 1$, or p is split in K,*
4. $y_{f,\chi} \neq 0$.

Then $E(\chi)$ is finite.

Equidistribution. Now we assume that χ is unramified. If we assume GRH, then we have the estimate (for any $\delta < 1/2$):

$$|L(s, \chi, f)| << \mathrm{N}(D)^{1/2-\delta} \tag{8.6}$$

for any unramified χ. By a well known estimate of Siegel:

$$h(T) := \#T(F)\backslash T(\mathbb{A}_f)/T(\widehat{\mathcal{O}}_F) >> \mathrm{N}(D)^{1/2-\epsilon}.$$

Theorem 8.7 then implies that

$$h(T)^{-1}\,|y_{f,\chi}| << \mathrm{N}(D)^{-\delta/2+\epsilon}. \tag{8.7}$$

For the trivial character χ_0, the estimate on L-series with $\delta = 1/100$ has been proved recently by Cogdell, Pieteski-Shapiro, and Sarnak [**17**]. Thus, one has the following

THEOREM 8.12. *Let U be a maximal open subgroup of $G(\mathbb{A}_f)$ which is compact modulo the center. Let x_n be any sequence of CM-points on $\mathbb{S}_U$ associated to maximal tori T_n of G. Then the orbits $T_n(\mathbb{A}_f)x_n$ are equidistributed.*

This is a generalization of a result of W. Duke [**24**] where $\mathbb{S}_U = \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$. A proof using Duke's original method is also announced by Paula Cohen [**18**].

Now let Γ be a subgroup of $T(F)\backslash T(\mathbb{A}_f)/T(\widehat{\mathcal{O}}_F)$ of index $i(\Gamma)$. Consider all characters which are trivial on Γ. Then each χ is unramified, and $f_\chi = f$. Then it follows that

$$\#\Gamma^{-1}\left|\sum_{\gamma\in\Gamma} f(\gamma)\right| = i(\Gamma)\left|\#\Gamma^{-1}\sum_{\chi|_\Gamma=1} h(T)^{-1}\ell_\chi(f)\right| \leq i(\Gamma)d_K^{-\delta/2+\epsilon}.$$

We have the following:

THEOREM 8.13. *Assume the following subconvexity bound: for a fixed $\delta > 0$,*

$$L(1/2, \chi, f) << \mathrm{N}(D)^{1/2-\delta}$$

for any unramified character χ. Let U be a maximal open subgroup of $G(\mathbb{A}_f)$ which is compact modulo the center. Let x_n be any sequence of CM-points on M_U associated to maximal tori T_n of G. Let Γ_n be subgroups of $T_i(F)\backslash T_i(\mathbb{A}_f)$ of index $i(\Gamma_n)$ such that

$$i(\Gamma_n) << d(T_n)^{\delta/2-\epsilon}$$

where $d(T_n)$ is the absolute value of the discriminant of quadratic fields defining T_n. Then the orbits $\Gamma_n x_n$ are equidistributed.

The interesting case is when Γ_n is the image of the reciprocity law:

$$\mathrm{Gal}(\bar{E}_{T_n}/E_{T_n}) \longrightarrow T_n(F)\backslash T_n(\mathbb{A}_f).$$

The theorem shows that the Galois orbits of x_n over *any fixed field* are equidistributed once the Galois orbit is sufficiently big in comparison with the toric orbit. It thus provides evidence for the following Andre-Oort conjecture for quaternion Shimura varieties:

CONJECTURE 8.14 (Andre-Oort). *Let x_n be a sequence of CM-points on a quaternion Shimura variety $\mathbb{S}_U$. Assume that no infinite subsequence is included in a Shimura subvariety of $\mathbb{S}_U$. Then the sequence x_n is Zariski dense in $\mathbb{S}_U$.*

Actually one expects much more:

CONJECTURE 8.15 (Andre-Oort). *Let x_n be a sequence of CM-points on a quaternion Shimura variety $\mathbb{S}_U$. Assume that no infinite subsequence is included in a Shimura subvariety of $\mathbb{S}_U$. Then the sequence of Galois orbits of the sequence x_n is equidistributed.*

Notice that the subconvexity bound holds for the case $F = \mathbb{Q}$ by recent work of Kowalski, Michel, and Vanderkam [**56, 61**]. Thus, we do have equidistribution of Galois orbits of CM-points on Modular curves and Shimura curves.

References

[1] A. A. Beilinson, *Heights pairing between algebraic cycles*, Comtemp. Math. **67** (1987), 1–24

[2] M. Bertolini and H. Darmon, *Kolyvagin's descent and Mordell-Weil groups over ring class fields*, Journal für die rein und angewande Mathematik, **412** (1990), 63-74.

[3] M. Bertolini and H. Darmon, *Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions*, manuscript (2001)

[4] M. Bertolini and H. Darmon, *A rigid analytic Gross-Zagier formula and arithmetic application*, with an appendix by Bas Edixhoven, Ann. Math. (2), **146** (1997), 111-147.

[5] B. J. Birch, *Elliptic curves and modular functions*, Symp. Math. Inst. Alta Math. **4** (1970), 27-32.

[6] B. J. Birch and N. M. Stephens, *Computation of Heegner points*, Modular forms (Durham, 1983), 13–41, Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester (1984).

[7] S. Bloch, *Height paring for algebraic cycles*, J. Pure Appl. Algebra **34**, pp. 119-145 (1984).

[8] S. A. Bloch and O. Ogus, *Gerstein's conjecture and homology of schemes*, Ann. Sci. Éc. Norm. Super., IV. Ser. **7** (1974), 181-202.

[9] J.-L. Brylinski, *Heights for local system on curves*, Duke Math. J. **59**(1989), 1–26.

[10] J.-F. Boutot and H. Carayol, *Uniformisation p-adique des courbes de Shimura: les thérèmes de Cerednik et de Drinfeld*, Astérisque **196-197** (1991), 45-158.

[11] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), 843–939

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

[13] H. Carayol, *Sur la mauvaise réduction des courbes de Shimura*, Comp. Math. **59** (1986), 151-230.

[14] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223-251.

[15] C. Cornut, *Réduction de familles de points CM*, Ph.D Thesis, Université Louis Pasteur, Strasbourg, 2000.

[16] W. Casselman, *On some results of Atkin and Lehner*, Math. Ann. **201** (1973), 301-314.

[17] Cogdell, Piateski-Shapiro, and Sarnak, *Esitmates for Hilbert modular L-functions and applications*, in preparation.

[18] P. Cohen, *Hyperbolic distribution problems on Siegel 3-folds and Hilbert modular varieties*, in preparation.

[19] P. Deligne, *Travaux de Shimura*, Séminaire Bourbaki, In: Lect. Notes Math. **244**, Springer-Verlag, 123-165.

[20] P. Deligne, *Formes modulaire et représentation l-adiques*, Séminaire Bourbaki 1968/69 exp. 355. In: Lect. Notes Math. **179**, Berlin-Heidelberg-New York: Springer (1971), 139–172

[21] P. Deligne, *Le déterminant de la cohomologie*, Comtemporary Mathematics **67**, 93-178.

[22] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, in: Modular function of one variable II (ed. P. Deligne, W. Kuyk), Lect. Notes Math. **349**, Berlin-Heidelberg-New York: Springer (1973), 143–316

[23] V. G. Drinfeld, *Coverings of p-adic symmetric regions*, Funct. Anal. Appl. **10** (1976), 29-40.
[24] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms,* Invent. Math. **92** (1988), 73-90
[25] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349-366.
[26] G. Faltings, *Calculus on arithmetic surfaces*, Ann. Math., **119** (1984), 387-424.
[27] K. Fujiwara, *Deformation rings and Hecke algebras in the totally real case*, Preprint.
[28] H. Gillet and C. Soulé, *Arithmetic intersection theory*, I.H.E.S Publ. Math. **72** (1990), 94-174.
[29] D. Goldfeld, *The class numbers of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. **4** (1976), 624-663.
[30] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields,* in Number Theory, Carbondale (1979), Lect. Notes in Math. **751**, Springer-Verlag, Berlin (1979), 108-118.
[31] D. Goldfeld and L. Szpiro, *Bounds for the order of the Tate-Shafarevich group*, Compositio Math. **97** (1995), 71-87.
[32] R. Greenberg, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **72** (1977), 241-265.
[33] B. H. Gross, *On canonical and quasi-canonical liftings*, Invent. Math. **84** (1986), 321-326 .
[34] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, in: L-function and Arithmetic (ed. J. Coates and M. J. Taylor) Cambridge University Press (1991).
[35] B. H. Gross, *Heegner points on $X_0(N)$*, in Modular Forms (ed. R. A. Rankin). Ellis Horwood (1984)
[36] B. H. Gross, *Local Heights on curves*, in Arithmetic Geometry (edited by Cornell and Silverman). Springer-Verlag, New York (1986)
[37] B. H. Gross, *Heights and the special values of L-series*, Number theory (Montreal, Que., 1985), CMS Conf. Proc., 7, Amer. Math. Soc., Providence, RI (1987), 115–187
[38] B. Gross, W. Kohnen, and D. Zagier, *Heegner points and derivatives of L-series. II*, Math. Ann. **278** (1987), 497–562.
[39] B. H. Gross and D. Prasad, *Test vectors for linear forms*. Math. Ann. **291** (1991), 343–355.
[40] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.
[41] R. J. Hatcher, *Heights and L-series*, Canad. J. Math. 42 (1990), 533-560.
[42] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York (1977)
[43] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z., **56** (1952), 227-253.
[44] H. Iwaniec, *Introduction to the spectral theory of automorphic forms,* Bibl. Rev. Mat. Iber., Madrid, (1995).
[45] H. Jacquet, *Automorphic forms on GL_2 II*, Lect. Notes. Math. **289**, Springer-Verlag (1972).
[46] H. Jacquet and R. Langlands, *Automorphic forms on GL_2*, Lect. Notes. Math. **114**, Springer-Verlag (1971).
[47] U. Jannsen, *Mixed Motives and algebraic K-theory*. Lect. Notes Math, vol. 1400) Berlin-Heidelberg-New York: Springer 1990.
[48] K. Kato, *p-adic Hodge theory and zeta functions of modular curves*, preprint.
[49] S. Katok and P. Sarnak, *Heegner points, cycles and Maass forms,* Israel J. Math. 84 (1993), 193–227
[50] N. Katz and B. Mazur, *Arithmetic moduli of elliptic cuvres,* Ann. Math. Studies **108** (1985).
[51] N. Katz and P. Sarnak, *Zeroes of zeta functions and symmetry*, Bull. A.M.S. **36** (1999), 1-26.
[52] N. Koblitz, *Introduction of elliptic curves and modular forms*, Graduate Text in Mathematics **97**, Springer-Verlag, New York, 1993
[53] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift. Prog. in Math., Boston, Birkhauser (1990).
[54] V. A. Kolyvagin and D. Yu. Logachev, *Finiteness of Ш over totally real fields*, Math. USSR Izvestiya, vol **39**(1992), 829-853 .
[55] W. Kohnen and D. Zagier, *Values of L-series of modular forms at the center of the critical strip*, Invent. Math. 64 (1981), 175–198.
[56] E. Kowalski, P. Michel, and J. Vanderkam, *Rankin-Selberg L-functions in the level aspects*, Preprint (2000)
[57] S. Lang, *Conjectured diophantine estimates on elliptic curves*, Progress in Math. **35**, Birkhaüser, (1983)
[58] B. Mazur, *Modular curves and Eisenstein ideal*, Publ. Math. I. H. E. S. **47** (1977), 33-186.

[59] B. Mazur, *On the arithmetic of special values of L-functions*, Invent. Math. **55** (1979), 207-240.
[60] B. Mazur, *Modular curves and arithmetic*, Proceedings of International Congruence of Mathematicians, Warsaw (1983), 185-211.
[61] P. Michel, *The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points I*, preprint (2001).
[62] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombers*, Invent. Math. *124* (1996), 437-449
[63] M. R. Murty and V. K. Murty, *Mean values of derivatives of modular L-series*. Ann. Math.**133**(1991), 447-475.
[64] J. Nekovar, *Kolyvagin's method for Chow groups of Kuga-Sato varieties*, Invent. Math. **107** (1992), 99-125.
[65] J. Nekovar, *On the p-adic heights of Heegner cycles*, Math. Ann. **302** (1995), 609-686.
[66] J. Nekovár, *On the parity of ranks of Selmer group II*, Preprint.
[67] B. Perrin-Riou, *Points de Heegner et dérivées de fonction L p-adiques*, Invent. Math. **89** (1987), 455-510.
[68] K. Ono and C. Skinner, *Non-vanishing of qudratic twists of modular L-functions*, Invent. Math. **134** (1998), 261-265.
[69] D. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. 75 (1984), 404-423
[70] D. Rohrlich, *On L-functions of elliptic curves and anti-cyclotomic towers*, Invent. Math. 75 (1984), 383-408
[71] K. Rubin, *The "Main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), 25-68.
[72] K. Rubin, *p-adic L-functions and rational points on elliptic curves with complex multiplication*, Invent. Math. **107**, (1992), 323-350.
[73] A. J. Scholl, *Motives for modular forms*, Invent. Math. **100** (1990), 419–430 .
[74] A. J. Scholl, *Height pairings and special values of L-functions*, Proc. Sym. AMS. **55**, part 1 (1994), 571-598.
[75] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press (1971)
[76] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematics Series **46**, Princeton Univ. Press (1998).
[77] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York (1986)
[78] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York (1994)
[79] C. Skinner and A. Wiles, *Residually reducible representations and modular forms*. Inst. Hautes Itudes Sci. Publ. Math. No. 89 (1999), 5-126 (2000).
[80] L. Szpiro (ed), *Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell*, Asterique **127** (1985)
[81] L. Szpiro, *Discriminant et conducteur des courbes elliptiques*, in Sminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988). Astrisque **183** (1990), 7–18.
[82] J. Tate, *Fourier analysis in number fields and Hecke's zeta-functions*, Algebraic number theory, edited by J. W. S. Cassels and A. Fröhlich, Academic Press (1967).
[83] J. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179-206.
[84] J. Tate, *On the conjecture of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 1965/1966, Exp. No. 306 (1966), 26pp.
[85] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), 553–572.
[86] V. Vatsal, *Uniform distribution of Heegner points*, preprint.
[87] V. Vatsal, *Special values of anticyclotomic L-functions*, preprint.
[88] M. -F. Vignéras, *Arithmétique des alg'ebres de quaternions*, Lect. Notes in Math. **800**, Springer-Verlag, New York, 1980
[89] J. -L. Waldspurger, *Sur les valeurs de certaines fonctions L automorphes en leur centre de symtrie*, Compositio Math. 54 (1985), 173–242.
[90] J. -L. Waldspurger, *Correspondences de Shimura et quaternions*, Forum Math., **3** (1991), 219-307.
[91] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math. **141** (1995), 443-551.

[92] H. Xue, *Central values for twisted Rankin L-functions*, Thesis at Columbia. (2002)
[93] S. Zhang, *Admissible pairings on curves*, Invent. Math. **112** (1993), 171-193.
[94] S. Zhang, *Heights of Heegner cycles and derivatives of L-series*, Invent. math. **130** (1997), 99-152.
[95] S. Zhang, *Heights of Heegner points on Shimura curves*, Annals of Mathematics (2), **153** (2001), 27-147.
[96] S. Zhang, *Gross-Zagier formula for* GL_2, Asian J. Math., **5** (2001), 183-290.

Department of Mathematics, Columbia University, New York, NY 10027