ON THE BIRCH AND SWINNERTON-DYER CONJECTURE FOR CM ELLIPTIC CURVES OVER $\mathbb{Q}$

YONGXIONG LI, YU LIU AND YE TIAN

To John Coates for his 70th birthday

1. Introduction and Main Theorems

For an elliptic curve $E$ over a number field $F$, we write $L(s, E/F)$ for its complex $L$-function, $E(F)$ for the Mordell-Weil group of $E$ over $F$, and $\text{III}(E/F)$ for its Tate-Shafarevich group. For any prime $p$, let $\text{III}(E/F)(p)$ or $\text{III}(E/\mathbb{Q})[p^\infty]$ denote the $p$-primary part of $\text{III}(E/F)$. When $F = \mathbb{Q}$, we shall simply write $L(s, E) = L(s, E/\mathbb{Q})$.

**Theorem 1.1.** Let $E$ be an elliptic curve over $\mathbb{Q}$ with complex multiplication. Let $p$ be any potentially good ordinary odd prime for $E$.

(i) Assume that $L(s, E)$ has a simple zero at $s = 1$. Then $E(\mathbb{Q})$ has rank one and $\text{III}(E/\mathbb{Q})$ is finite. Moreover the order of $\text{III}(E/\mathbb{Q})(p)$ is as predicted by the conjecture of Birch and Swinnerton-Dyer conjecture.

(ii) If $E(\mathbb{Q})$ has rank one and $\text{III}(E/\mathbb{Q})(p)$ is finite, then $L(E, s)$ has a simple zero at $s = 1$.

Remark. The first part of (i) is the result of Gross-Zagier and Kolyvagin. The remaining part is due to Perrin-Riou for good ordinary primes. In this paper, we deal with odd bad primes which are potentially good ordinary. The result can be easily generalized to abelian varieties over $\mathbb{Q}$ corresponding to a CM modular form with trivial central character.

The following theorem shows that there are infinitely many elliptic curves over $\mathbb{Q}$ of rank one for which the full BSD conjecture hold.

**Theorem 1.2.** Let $n \equiv 5 \pmod{8}$ be a squarefree positive integer, all of whose prime factors are congruent to 1 modulo 4. Assume that $\mathbb{Q}(\sqrt{-n})$ has no ideal class of order 4. Then the full BSD conjecture holds for the elliptic curve $y^2 = x^3 - n^2x$ over $\mathbb{Q}$. In particular, for any prime $p \equiv 5 \pmod{8}$, the full BSD holds for $y^2 = x^3 - p^2x$.

**Sketch of Proof.** Consider the Heegner point $P$ constructed using the Gross-Prasad test vector as the below Theorem 1.3. Using an induction argument as in [16] or [17], one can show that $P$ is non-torsion. Thus both the analytic rank and Mordell-Weil rank of $E^{(n)} : y^2 = x^3 - n^2x$ are one.

By Perrin-Riou [12] and Kobayashi [8], we know that the $p$-part of full BSD holds for all primes $p \mid 2n$. The 2-part of BSD for $E^{(n)}$ is exactly the statement on 2-divisibility in Theorem 1.3 below by using explicit Gross-Zagier formula in [2] and noting that $\dim_{\mathbb{Q}} S_2(E^{(n)}/\mathbb{Q})/\text{Im}(E^{(n)}(\mathbb{Q})_{\text{tor}}) = 1$. By Theorem 1.1, the $p$-part of BSD always holds for all primes $p | n$, since all primes $p$ with $p \equiv 1 \pmod{4}$ are potentially good ordinary primes for $E^{(n)}$. □

To solve the Diophantine equation $y^2 = x^3 - n^2x$ over $\mathbb{Q}$, we define the complex uniformization of $E^{(n)}$ by the following composition.

$$
\mathcal{H} \xrightarrow{\pi} \Gamma_0(32) \backslash \mathcal{H} \cup P^1(\mathbb{Q}) = X_0(32) \xrightarrow{f_0} E^{(1)} \xrightarrow{[2-2g]} E^{(1)} \xrightarrow{\iota} E^{(n)},
$$
where
• \( \mathcal{H} \xrightarrow{\tau} \Gamma_0(32) \setminus (\mathcal{H} \cup P^1(\mathbb{Q})) = X_0(32)(\mathbb{C}) \) is the natural quotient,
• \( f_0 : X_0(32) \to E^{(1)} \) is a degree 2 morphism over \( \mathbb{Q} \) mapping \([\infty]\) to \( \mathcal{O} \),
• \([2 - 2i]\) is the multiplication by \( 2 - 2i \) on \( E^{(1)} \), where \((x, y) = (-x, iy)\),
• \( \iota : E^{(1)} \xrightarrow{\sim} E^{(n)} \) is the twist isomorphism given by \((x, y) \mapsto (-nx, -ny^{3/2})\).

The following theorem, which is equivalent to the 2-part BSD for \( E^{(n)} \) using explicit Gross-Zagier formula in [2], and can be proved exactly as in [16].

**Theorem 1.3.** Let \( n \equiv 5 \pmod{8} \) be a square-free positive integer as in Theorem 1.2. Then the image \( P_0 \in E^{(n)}(\mathbb{Q}) \) of \((4 - 4\sqrt{-n})^{-1} \in \mathcal{H} \) under the above complex uniformization is defined over the Hilbert class field \( \mathcal{H} \) of \( \mathbb{Q}(\sqrt{-n}) \). Moreover the Heegner point \( P := \sum_{\sigma \in \text{Gal}(\mathcal{H}/\mathbb{Q}(\sqrt{-n}))} P_0^\sigma \) actually belongs to \( E^{(n)}(\mathbb{Q}) \). Let \( \mu(n) \) be the number of prime factors of \( n \). Then \( P \in 2^{\mu(n)-1}E^{(n)}(\mathbb{Q}) + E^{(n)}(\mathbb{Q})_{\text{tor}} \) but \( P \notin 2^{\mu(n)}E^{(n)}(\mathbb{Q}) + E^{(n)}(\mathbb{Q})_{\text{tor}} \). In particular, \( P \) is of infinite order.

Moreover, the Mordell-Weil group \( E^{(n)}(\mathbb{Q}) \) is of rank one and the index of its subgroup generated by \( P \) and torsion points satisfies

\[
\left[ E^{(n)}(\mathbb{Q}) : \mathbb{Z}P + E^{(n)}(\mathbb{Q})_{\text{tor}} \right] = 2^{\mu(n)-1} \cdot \sqrt{\text{III}(E/\mathbb{Q})}.
\]

**Example** For the prime \( p = 1493 \equiv 5 \pmod{8} \), the Mordell-Weil group \( E^{(p)}(\mathbb{Q}) \) modulo torsion has a generator

\[
\begin{bmatrix}
1674371133 \\
744769
\end{bmatrix},
\begin{bmatrix}
51224214734700 \\
642735647
\end{bmatrix},
\]

as well that Heegner point \((x, y)\) has coordinates

\[
\begin{align*}
x &= \frac{245615354991472143968975459422696932728951498371630131453}{29585011828542075719444468687561920064681205358510529}, \\
y &= \frac{-12172578066823596873618123810557983972375660184180439465365335709906981098721585260100}{160919109605479862871753246473210772682219745687839104546974117877976688892833}.
\end{align*}
\]

It follows that \( \text{III}(E^{(p)}/\mathbb{Q}) \cong (\mathbb{Z}/32)^2 \).

Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \), with complex multiplication (= CM in what follows) by an imaginary quadratic field \( K \). Let \( p \neq 2 \) be a potential good ordinary prime for \( E \). Note that \( p \) must split in \( K \), and also \( p \) does not divide the number \( w_K \) of roots of unity in \( K \).

Assume that \( L(s, E) \) has a simple zero at \( s = 1 \). Choose an auxiliary imaginary quadratic field \( K \) such that (i) \( p \) is split over \( K \) and (ii) \( L(s, E/K) \) still has a simple zero at \( s = 1 \). Let \( E^{(K)} \) be the twist of \( E \) over \( K \), then \( L(1, E^{(K)}) \neq 0 \). Let \( \eta \) be the quadratic character associated to the extension \( K/\mathbb{Q} \) and \( \eta_K \) its restriction to \( K \). Let \( \mathbb{Q}_\infty \) be the cyclotomic \( \mathbb{Z}_p \)-extension of \( \mathbb{Q} \), and put \( \Gamma = \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \). For any finite order character \( \nu \) of \( \Gamma \), let \( \nu_K \) denote its restriction to \( \text{Gal}(K\mathbb{Q}_\infty/K) \). Consider the equality

\[
L(s, E \otimes \nu) L(s, E^{(K)} \otimes \nu) = L(s, E_K \otimes \nu_K)
\]

and its specialization to \( s = 1 \). Let \( \mathcal{L}_{E}, \mathcal{L}_{E^K} \) be the cyclotomic-line restrictions of the two Katz’s two variable \( p \)-adic \( L \)-function corresponding to \( E \) and \( E^{(K)} \), respectively. Let \( \mathcal{L}_{\varphi_E}\mathcal{L}_{\varphi_{E^K}} \) be the cyclotomic-line restriction of the \( p \)-adic Rankin-Selberg \( L \)-function for \( E \) over \( K \). The ingredients needed to prove the \( p \)-part BSD formula of \( E \) are the following.

1. Rubin’s two variable main conjecture [14] in order to relate the \( p \)-part of \( \text{III}(E/K) \) with \( \mathcal{L}_{E}(1) \). Note that \( \text{ord}_p([\text{III}(E/K)]) = 2\text{ord}_p([\text{III}(E/\mathbb{Q})]) \) for odd \( p \).
2. The complex Gross-Zagier formula [19] and the \( p \)-adic Gross-Zagier formula [4], which relate \( \mathcal{L}_{E/K}(1) \) and \( L(1, E/K) = L'(1, E/\mathbb{Q})L(1, E^{(K)}/\mathbb{Q}) \).
3. The precise relationship between \( \mathcal{L}_{E}(1) \mathcal{L}_{\varphi_{E^K}}(1) \) and \( \mathcal{L}_{E/K}(1) \), and also between \( \mathcal{L}_{\varphi_{E}}(1) \) and \( L(1, E^{(K)}) \). This follows from the above equality of \( L \)-series and the interpolation properties of these \( p \)-adic \( L \)-functions.

Suppose that \( E \) has bad reduction at \( p \) which is potential good for \( E \). Let \( p \) denote a prime of \( K \) above \( p \). There is an elliptic curve \( E' \) over \( K \) with good reduction at \( p \). In the process of proof, we need to compare periods, descend etc between \( E \) and \( E' \).
Notations. Fix a non-trivial additive character ψ : \mathbb{Q}_p \rightarrow \mathbb{C}_p^* with conductor \mathbb{Z}_p. For any character \chi : \mathbb{Q}_p^\times \rightarrow \mathbb{C}_p^\times, say of conductor \rho^n with n \geq 0, we define the root number by
\[\tau(\chi, \psi) = p^{-n} \int_{t_p(t) = -n} \chi^{-1}(t) \psi(t) dt,\]
where dt is the Haar measure on \mathbb{Q}_p such that Vol(\mathbb{Z}_p, dt) = 1. Fix embeddings \iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C} and \iota_p : \overline{\mathbb{Q}} \rightarrow \mathbb{C}_p such that \iota_p = \iota \circ \iota_\infty for an isomorphism \iota : \mathbb{C} \isom \mathbb{C}_p. For an elliptic curve E over a number field F and p a potential good prime for E, let (\cdot, \cdot)_\infty and (\cdot, \cdot)_p denote the normalized Néron - Tate height pairing, and the p-adic height pairing with respect to cyclotomic character. Let \( P_1, \ldots, P_r \in E(F) \) form a basis for \( E(F) \otimes_{\mathbb{Z}} \mathbb{Q} \), define the regulars by
\[ R_\infty(E/F) = \frac{\det ((P_i, P_j)_\infty)_{i \neq j}}{|E(K) : \sum_i ZP_i|^2}, \quad R_p(E/F) = \frac{\det ((P_i, P_j)_p)_{i \neq j}}{|E(K) : \sum_i ZP_i|^2}. \]

For any character χ of \( \hat{K}^\times \), let \( \hat{f}_\chi \subset \mathcal{O}_K \) denote its conductor. For an elliptic curve E over K, let \( f_E \) denote its conductor. For any non-zero integral ideals \( g \) and \( a \) of K, let \( g^{(a)} \) denote the prime-to-\( a \) part of \( g \). Let \( \mathfrak{d} \) be the completion of the maximal unramified extension of \( \mathbb{Z}_p \) and \( \mathfrak{d}_\chi \) the finite extension of \( \mathfrak{d} \) generated by the values of \( \chi \). Let \( L_\infty/K \) be an abelian extension whose Galois group \( \mathcal{G} = \text{Gal}(L_\infty/K) \cong \Delta \times \Gamma \) with \( \Delta \) finite and \( \Gamma \cong \mathbb{Z}_p^\times \). Then for any \( \mathcal{O}[[\mathcal{G}]] \)-module M and character \( \chi \) of \( \Delta \), put \( M_{\chi} = M \otimes_{\mathcal{O}[[\mathcal{G}]]} \mathcal{O}[[\Gamma]] \). If \( p \nmid |\Delta| \), let \( M_{\chi} \) denote its \( \chi \)-component (as a direct summand).

Acknowledgment. The authors thank John Coates, Henri Darmon and Shouwu Zhang for their encouragement.

2. Katz’s \( p \)-adic L-function and Cyclotomic \( p \)-adic Formula

Let E be an elliptic curve defined over K with CM by K and \( \varphi \) its associated Hecke character. Let \( p \nmid w_K \) be a prime split in K and \( \mathfrak{p} \mathcal{O}_K = \mathfrak{p} \mathfrak{^*} \) with \( \mathfrak{p} \) induced by \( t_p \). In particular, \( K_\mathfrak{p} = \mathbb{Q}_p \) in \( \mathcal{O}_p \) and let \( \psi_\mathfrak{p} = \psi_p \) on \( K_\mathfrak{p} \) under this identification. Let \( \Omega_E \) be a \( p \)-minimal period of E over K. Let \( \varphi \) be the associated Hecke character of E and \( \varphi_\mathfrak{p} \) its \( \mathfrak{p} \)-component. Let \( f_E \) be the conductor of \( \varphi \).

Let F be an abelian extension over K with Galois group \( \Delta \). Assume that \( p \nmid |\Delta| \) and denote by \( f_{E/K} \) the conductor of F. Let \( \mathcal{G} \) be the Galois group of the extension \( F(E[p^{\infty}]) \) over K. Then \( \mathcal{G} \cong \mathcal{G}_{\text{tot}} \times \Gamma_K \) with \( \Gamma_K = \text{Gal}(F(E[p^{\infty}])/F(E[p])) \). Let \( \Lambda = \mathbb{Z}_p[[\mathcal{G}]] \). Let \( U_\infty \) and \( C_\infty \) denote the \( \mathbb{Z}_p[[\mathcal{G}]] \)-modules formed from the principal local units at the primes above \( p \), and the closure of the elliptic units for \( K(E[p^{\infty}]) \) (see §4 of [14] for the precise definitions.)

Theorem 2.1 (Two variable \( p \)-adic L-function). Let \( g \) be any prime-to-\( p \) non-zero integral ideal of K. Assume that \( f_{E/K}^{(p)} \nmid g \). There exists a unique measure \( \mu_g = \mu_{g,p} \) on the group \( \mathcal{G} = \text{Gal}(K(\mathfrak{g}^{p^{\infty}})/K) \) such that for any character \( \rho \) of \( \mathcal{G} \) of type \((1,0)\),
\[ \rho(\mu_g) = \frac{\tau(\rho, \psi_p)}{\tau(\varphi, \psi_p)} \cdot \frac{1 - \rho(p)p^{-1}}{1 - \rho(p)p^{-1}} \cdot \frac{L^{(g^{(p)})}(s, \mathfrak{p}, 1)}{\Omega_E}. \]

Here \( L^{(g^{(p)})}(s, \mathfrak{p}, 1) \) is the primitive \( L \)-series of \( \mathfrak{p} \) with Euler factors at places dividing \( \mathfrak{p} \)-removed.

Proof. It follows from the below lemma 2.3 and construction of Katz’s two variable \( p \)-adic measure, see Theorem 4.14. \( \square \)

Theorem 2.2 (Yager). For any character \( \chi \) of \( \mathcal{G}_{\text{tot}} \), let \( f_\chi^{(p)} = f_\chi \) and \( \mu_\chi^\mathfrak{p} = \chi(\mu_\chi) \in \mathcal{D}[[\Gamma_K]] \). Then we have
\[ \text{Char}(U_\infty/C_\infty)_{\chi} \otimes \mathcal{D}[[\Gamma_K]] = (\mu_\chi^\mathfrak{p}). \]

Here the measure \( \mu_\chi^\mathfrak{p} \) is defined as in Theorem 2.1.

Lemma 2.3. Let \( E/K \) be an elliptic curve associated with to a Hecke character \( \varphi \), \( p \) splits in K and write \( p \mathcal{O}_K = \mathfrak{p} \mathfrak{^*} \). Let \( \varphi_0 \) be a Hecke character over K unramified at \( p \). Let \( \Omega_E \) and \( \Omega_0 \) be \( p \)-minimal periods of E and \( \varphi_0 \), respectively. Then
\[ \text{ord}_p \left( \frac{\Omega_E \cdot \tau(\varphi_0, \psi_p)}{\Omega_0} \right) = 0. \]
Proof. This follows from Stickelberger’s theorem on prime ideal decomposition of Gauss sum. In fact, for \( p \nmid w = w_K \), \( E \) has \( p \)-minimal Weierstrass equation of form
\[
E' : y^2 = x^3 + a_2 x^2 + a_4 x + a_6, \quad a_2, a_4, a_6 \in K^\times \cap \mathcal{O}_p.
\]
Note that for \( w = 4, 6 \), we may-and do- take form \( y^2 = x^3 + a_4 x, \ y^2 = x^3 + a_6 \), respectively. Then there is an elliptic curve \( E' \) over \( K \) which has good reduction at \( p \). Let \( \varphi' \) be its associated Hecke character. Then \( \epsilon = \varphi'^{-1} \colon K_F^\times /K^\times \to \mathcal{O}_K^\times \) (also viewed as a Galois character via class field theory) is of form \( \chi(\sigma) = \sigma(d^{1/w})d^{-1/w} \) for an element \( d \in K^\times /K^\times w \). Then the twist \( E' \) has \( p \)-good model
\[
E' : \begin{cases}
y^2 = x^3 + a_2 x^2 + a_4 x + a_6, & \text{if } w = 2, \\
y^2 = x^3 + a_4 x, & \text{if } w = 4, \\
y^2 = x^3 + a_6, & \text{if } w = 6.
\end{cases}
\]
It is easy to check the \( \Omega_{E_0} = d^{1/w} \cdot \Omega_E \). Let \( \omega : \mathcal{O}_p^\times \to K \) be the character characterized by \( \omega(a) \equiv a \mod p \) and let \( \chi = \omega^{-\lfloor(p-1)/w \rfloor} \). Then \( \epsilon_p = \chi^k \) for some \( k \in \mathbb{Z}/w \mathbb{Z} \). Let \( \kappa_p \cong F_p \) be the \( p \)-adic field of \( K_p \). By Stickelberger’s theorem, the Gauss sum \( g(\epsilon_p, \psi) := -\sum_{a \in \kappa_p^\times} \epsilon_p(a)\psi(a) \) has \( p \)-valuation \( \{k/w\} \). It remains to show that \( k = \ord_p(d) \). Note that for any \( u \in \mathcal{O}_p^\times \), \( K_p(u^{1/w}) \) is unramified over \( K_p \). Thus it is equivalent to show that for any uniformizer \( \pi \) of \( K_p \),
\[
\sigma_u(\pi^{1/w})/\pi^{1/w} \equiv u^{-\lfloor(p-1)/w \rfloor} \mod p, \quad \forall u \in \mathcal{O}_p^\times.
\]
But it is easy to see this by using local class field theory for formal group associated to \( x^p - px \).

For general Hecke character \( \varphi_0 \) over \( K \) unramified at \( p \) (not necessarily \( K \)-valued) and \( \Omega_0 \) its \( p \)-minimal period, it is easy to see that \( \ord_p(\Omega_0/\Omega_{E_0}) = 0 \).

Let \( \chi_{\text{cyc}, K} : \mathcal{G} \to \mathbb{Z}_p^\times \) be the \( p \)-adic cyclotomic character defined by the action on \( p \)-th power roots of unity. Define
\[
\mathcal{L}_{E,F}(s) := \mu_{1/p}(\varphi_E \chi_{\text{cyc}, K}^{1-s}), \quad \forall s \in \mathbb{Z}_p.
\]
Rubin’s two variable main conjecture implies the following theorem.

**Theorem 2.4.** Let \( E \) be an elliptic curve over \( K \) with CM by \( K \) and \( \varphi \) its associated Hecke character. Let \( p \nmid w_K \) be a prime split in \( K \) and \( p \mathcal{O}_K = p \mathcal{O}_K^* \). Let \( r \) be the \( \mathcal{O}_K \)-rank of \( E(K) \). Assume that \( \text{III}(E(K)/p) \) is finite and the \( p \)-adic height pairing of \( E \) over \( K \) is non-degenerate. Then

1. both \( \mathcal{L}_{E,F}(s) \) and \( \mathcal{L}_{E,F}(s) \) have a zero at \( s = 1 \) of exact order \( r \).
2. the \( p \)-adic BSD conjecture holds for \( E/K \):
\[
\ord_p(\text{III}(E(K)/p)) = \ord_p \left( \frac{\mathcal{L}_{E,F}(r)(1)}{R_p(E/K)} \prod_{v \mid p} (1 - \varphi_E(v)) \left(1 - \overline{\varphi_E(v)} \right)^{-2} \right)
\]
provided the assumption that if \( w_K = 4 \) or \( 6 \) then \( E \) has bad reduction at both \( p \) and \( p^* \) or good reduction at both \( p \) and \( p^* \).

Moreover, if \( E \) is defined over \( \mathbb{Q} \), then we have
\[
\ord_p(\text{III}(E/\mathbb{Q})) = \ord_p \left( \frac{\mathcal{L}_{E,F}(r)(1)}{R_p(E/\mathbb{Q})} \prod_{v \mid p} (1 - \varphi_E(v)) \left(1 - \overline{\varphi_E(v)} \right)^{-1} \right).
\]

**Proof.** Let \( \epsilon \) be a Galois character over \( K \) valued in \( \mathcal{O}_K^\times \) such that \( \varphi' = \varphi \) is unramified at both \( p \) and \( p^* \). Let \( E' \) be the elliptic curve over \( K \) as \( \epsilon \)-twist of \( E \) so that \( \varphi' \) as its Hecke character. Then \( E' \) has good reduction above \( p \). Let \( F \) be the abelian extension over \( K \) cut by \( \epsilon \), then \([F : K][w_K]\). Moreover, \( E \) and \( E' \) are isomorphism over \( F \), \( E'(F)(\epsilon) \cong E(K) \), and \( \text{III}(E'(F)/p)[\mathbb{Q}^{\infty}(\epsilon)] \cong \text{III}(E(K)/p)[\mathbb{Q}^{\infty}] \). Let \( F_0 = F(E[p]) \) and \( \chi : \text{Gal}(F_0/K) \to \mathcal{O}_K^\times \) be the character giving the action on \( E[p] \).

Let \( F_{\infty} = F(E[p^{\infty}]) \). Let \( M_{\infty,p} \) be the maximal \( p \)-extension over \( F_{\infty} \) unramified outside \( p \) and \( X_{\infty,p} = \text{Gal}(M_{\infty,p}/F_{\infty}) \). Denote by \( U_{\infty} \) and \( C_{\infty} \subset U_{\infty} \) the \( \Lambda = \mathbb{Z}[[\text{Gal}(F_{\infty}/K)]]-\text{modules} \) of the principal local units at \( p \) and elliptic units for the extension \( F_{\infty} \) (defined as in [14], §4). Rubin’s two variable main conjecture, together Yager [18], says that
\[
\text{Char}_{\Lambda}(X_{\infty,p}) \otimes \text{Gal}(F_{\infty}/F_0) = \left( \mu_{1/p}^{\chi_{\text{cyc}, K}^r} \right).
\]
where for an integral ideal $g$ of $K$ prime to $p$, the measure $g$ is given as in Theorem 2.1. Let $\text{Sel}(F_{\infty}, E[p^\infty])$ be the $p$-Selmer group of $E$ over $F_{\infty}$ and $\text{Sel}(F_{\infty}, E[p^\infty])^\vee$ its Pontryagin dual. Then $\text{Sel}(F_{\infty}, E[p^\infty])^\vee$ is a finitely generated $A$-torsion module and
\[
\text{Char}_A(\text{Sel}(F_{\infty}, E[p^\infty])^\vee) = \iota_p \text{Char}(X_{\infty, p}),
\]
where $\iota_p : A \to \Lambda, \gamma \mapsto \kappa_p(\gamma)\gamma$ for any $\gamma \in \text{Gal}(F_{\infty}/K)$ and $\kappa_p$ is the character of $\text{Gal}(F_{\infty}/K)$ giving the action on $E[p^\infty]$. Similarly, we also have that
\[
\text{Char}_A(X_{\infty, p}) \mathbb{D}[\text{Gal}(F_{\infty}/F_0)] = \left(\mu_{f_{\infty}}(p), p\right), \quad \text{Char}_A(\text{Sel}(F_{\infty}, E[p^\infty])^\vee) = \iota_p \text{Char}(X_{\infty, p}).
\]

Let $F_{\text{cyc}}$ be the cyclotomic $\mathbb{Z}_p$ extension, and $\Lambda_{\text{cyc}} = \mathbb{Z}_p[[\text{Gal}(F_{\text{cyc}}/K)]] \cong \Delta \times \Gamma$ where $\Delta = \text{Gal}(F/K)$ and $\Gamma = \text{Gal}(F_{\text{cyc}}/F)$. Let $\text{Sel}(F_{\text{cyc}}, E[p^\infty])$ denote the $p$-Selmer group of $E$ over $F_{\text{cyc}}$ and then its Pontryagin dual $\text{Sel}(F_{\text{cyc}}, E[p^\infty])^\vee$ is a finitely generated torsion $\Lambda_{\text{cyc}}$-module. We have
\[
\text{Sel}(F_{\text{cyc}}, E[p^\infty]) = \text{Sel}(F_{\text{cyc}}, E[p^\infty]) \oplus \text{Sel}(F_{\text{cyc}}, E[p^\infty]) = \text{Hom}(X_{\infty, p}, E[p^\infty])^\vee \oplus \text{Hom}(X_{\infty, p}^*, E(p^\infty))^\vee \text{Gal}(F_{\infty}/F_{\text{cyc}})
\]
Here the second equality is given [10] Proposition (1.3), Theorem (1.6) and Lemma (1.1), the last one is by the same reason as [14] Theorem 12.2. It follows that
\[
\text{Char}_{\Lambda_{\text{cyc}}}(\text{Sel}(F_{\text{cyc}}, E[p^\infty])^\vee) \mathbb{D}[\text{Gal}(F_{\text{cyc}}/F)] = \left(\iota_p \mu_{f_{\text{cyc}}}(p), \iota_p (\mu_{f_{\text{cyc}}}^*)(p)\right).
\]

Denote by $\chi_{\text{cyc}}$ the cyclotomic character. Let $f_E$ be a generator of $\text{Char}_{\mathbb{Z}_p[[\Gamma]]}(\text{Sel}(F_{\text{cyc}}, E[p^\infty])^\vee)('\Delta\Delta$ and define
\[
\mathcal{L}(s) = \chi_{\text{cyc}}^s(f_E), \quad \forall s \in \mathbb{Z}_p.
\]
Then we have $\mathcal{L}(s) = u(s)\mathcal{L}_{\varphi_p}(s)\mathcal{L}_{\varphi_p}(s)$ for some function $u(s)$ valued in $\mathbb{D}^\times$.

Note that $E$ over $F$ has good reduction above $p$. Employing the descend argument as in [15], noting that the “descent diagram” in [15] §7 for $E$ over $F$ is $\Delta = \text{Gal}(F/K)$-equivariant, and taking $\Delta$-invariant part, we have

**Proposition 2.5.** Let $r := \text{rank}_{\mathbb{Q}_p} E(K)$. Assume that $\text{III}(E/K)[p^\infty]$ is finite and $p$-adic height pairing is non-degenerate on $E(K)$. Then $\mathcal{L}(s)$ has exact vanishing order $2r$ at $s = 1$ and if let $\mathcal{L}'(1)$ denote its leading coefficient at $s = 1$,
\[
\frac{\mathcal{L}'(1)}{R_p(E/K)} \sim |\text{III}(E/K)| \cdot \prod_{v \mid p} \frac{1}{\text{H}^1(\text{Gal}(F/F_{\text{cyc}}/F_{\infty}), E(F(\mu_{p^\infty}) \otimes K_v)^\vee)^2}.
\]

Here for any $a, b \in \mathbb{C}_p^\times$, write $a \sim b$ if $\text{ord}_p(a/b) = 1$.

The follow lemma will complete the proof.

**Lemma 2.6.** Let $v_0 = p$ or $p^*$. Assume that if $w_K = 4$ or 6 then $E$ has bad reduction at both $p$ and $p^*$ or good reduction at both $p$ and $p^*$. Then
\[
|\text{H}^1(\text{Gal}(F(\mu_{p^\infty})/F), E(F(\mu_{p^\infty}) \otimes K_{v_0}))^\vee | \sim (1 - \varphi_E(v_0))(1 - \varphi_E(v_0)).
\]

The remain part of this section will devote to the proof of this lemma. Note that [15] handled the case where $E$ has good reduction above $p$. We now assume that $E$ has bad reduction either at $p$ or at $p^*$. The isomorphism between $E$ and $E'$ over $F$ gives rise to an isomorphism
\[
\text{H}^1(\text{Gal}(F(\mu_{p^\infty})/F), E(F(\mu_{p^\infty}) \otimes K_{v_0}))^\vee \sim \text{H}^1(\text{Gal}(F(\mu_{p^\infty})/F), E'(F(\mu_{p^\infty}) \otimes K_{v_0}))^\vee.
\]

We will need Proposition 2 in [15] that for any elliptic curve $A$ over a local field $k$ with good ordinary reduction and let $\tilde{A}$ denote its reduction over the the residue field $k$ of $k$, we have
\[
|\text{H}^1(\text{Gal}(k(\mu_{p^\infty})/k), \text{A}(k(\mu_{p^\infty})))| = |\tilde{A}(k)[p^\infty]|.
\]

Let $w|v_0$ be a place of $F$ above $v_0$ and $\kappa_w/\kappa_{v_0}$ be the residue fields of $F_w$ and $K_{v_0}$ respectively, we have
\[
|E'(\kappa_w)| \sim \left(1 - \varphi_{E'}(v_0)^{[\kappa_w/\kappa_{v_0}]}\right) \left(1 - \varphi_{E'}(v_0)^{[\kappa_{v_0}/\kappa_{v_0}]}\right).
\]
Proof. The claim follows from the relations as associated Hecke character. Then we have element contained in the representation (Φ, ψ) = \left| \text{Gal}(\mathbb{F}(\mu_{p^n})/\mathbb{F}_w) \right| \left| \text{Gal}(\mathbb{F}(\mu_{p^n})/\mathbb{F}_v) \right| \left| \text{Gal}(\mathbb{F}(\mu_{p^n})/\mathbb{F}_w) \right| \left| \text{Gal}(\mathbb{F}(\mu_{p^n})/\mathbb{F}_v) \right|.

If E has good reduction at v_0, then F/K is unramified at v_0. If v_0 is split over F, then F \otimes K v_0 \cong K^2 v_0 and \epsilon v_0 = 1. It is easy to see

\left| \text{Gal}(\mathbb{F}(\mu_{p^n})/\mathbb{F}), E'(\mathbb{F}(\mu_{p^n}) \otimes K v_0) \right| \sim (1 - \varphi_E(v_0))(1 - \varphi_E(v_0)).

If v_0 is inert in F, let w be the unique prime of F above v_0. Note that \varphi_{v_0} = \varphi_{v_0} \epsilon v_0 and \epsilon(v_0) = -1.

\left| \text{Gal}(\mathbb{F}(\mu_{p^n})/\mathbb{F}), E'(\mathbb{F}(\mu_{p^n}) \otimes K v_0) \right| \sim \frac{(1 - (\varphi(v_0))(1 - \varphi(v_0)))^2}{(1 - (\varphi(v_0))(1 - \varphi(v_0)))} = (1 - \varphi(v_0))(1 - \varphi(v_0)).

If w_K = 4 or 6, by our assumption, v_0 must be ramified over F and \epsilon is non-trivial on its inertia subgroup. The proof is now similar to the previous ramified case.

\square

3. \textit{∞}-adic and p-adic Gross-Zagier Formulae

Let E be an elliptic curve over Q of conductor N and let its associated newform. Let p be a prime where E is potential good ordinary or potential semi-stable. Let \alpha : Q^* \longrightarrow Z^*_p be the character contained in the representation (V_p E)^{ss} of \Gamma Q_p such that \alpha|_{Z^*_p} is of finite order.

Let K be an imaginary quadratic field such that \epsilon(E/K) = -1 and p splits in K. Let \Gamma_K be the Galois group of the Z^*_p-extension over K. Recall that [4] there exists a p-adic measure \mu_{E/K} on \Gamma_K such that for any finite order character \chi of \Gamma_K

\chi(\mu_{E/K}) = \frac{L(p)}{8\pi^2} \prod_{w \mid p} Z_w(\chi_w, \psi_w),

where (\phi, \psi) is the Petersen norm of \phi:

(\phi, \psi) = \iint_{\Gamma_{w}(N) \backslash \Gamma} |\phi(z)|^2 dx dy, \quad z = x + iy,

and for each prime w\mid p of K, let \alpha_w = \alpha \circ N_{K_w/Q_w} and \psi_w = \psi_p \circ \text{Tr}_{K_w/Q_w}, and let \varphi_w be a uniformizer of K_w, then

Z_w(\chi_w, \psi_w) = \begin{cases} (1 - \alpha_w \chi_w(\varphi_w)^{-1})(1 - \alpha_w \chi_w(\varphi_w)p^{-1})^{-1}, & \text{if } \alpha_w \chi_w \text{ is unramified}, \\ p^n \tau((\alpha_w \chi_w)^{-1}, \psi_w), & \text{if } \alpha_w \chi_w \text{ is of conductor } n \geq 1. \end{cases}

The following lemma will be used to prove our main theorem.

Lemma 3.1. Let E be an elliptic curve over Q with CM by an imaginary quadratic field K. Assume p is also split in K write p\mathcal{O}_K = pp^* with p induced by \psi, i.e. identify K_p with Q_p and the non-trivial element \tau \in Gal(K/Q) induces an isomorphism on K_p and thus \tau : K_p \longrightarrow K_p = Q_p. Let \varphi be its associated Hecke character. Then we have \alpha = \varphi_p \otimes \tau^{-1} and (\alpha^{-1}\chi_{\text{cyc}})(x) = \varphi_p(x)x^{-1} for any x \in Q^*_p. Moreover, for any place w\mid p of K, any finite order character \nu : Q^*/Q^*_p \times Z^*_p \longrightarrow \mu_{p^n} viewed as character on \Gamma_K by composition with norm

Z_w(\alpha_w \nu, \psi) = \tau(\varphi_p \nu^{-1}, \psi) \cdot \frac{1 - (\varphi_p \nu^{-1})(p)p^{-1}}{1 - (\varphi_p \nu p^{-1})(p)p^{-1}}.

Proof. The claim follows from the relations \varphi \varphi = 1_{K_p^{\infty}} and \varphi^* = \varphi.

\square
Let $\chi_{\text{cyc}, K} : \Gamma_K \to \mathbb{Z}_p^\times$ denote the $p$-adic cyclotomic character of $G_K$. Let $\chi$ be an anticyclotomic character. Define $\mathcal{L}_{E/K, \chi}$ to be the $p$-adic $L$-function

$$
\mathcal{L}_{E/K, \chi}(s) = \mu_{E/K}(\chi \chi_{\text{cyc}, K}^{s-1}), \quad s \in \mathbb{Z}_p.
$$

For trivial $\chi$, we write $\mathcal{L}_{E/K}$ for $\mathcal{L}_{E/K, \chi}$.

**Theorem 3.2** (See [19] and [4]). Let $E$ be an elliptic curve over $\mathbb{Q}$ and $K$ an imaginary quadratic field. Let $p$ be a potentially good ordinary prime for $E$ and split over $K$. Assume that $\epsilon(E/K) = -1$. Then

$$
\frac{\mathcal{L}'_{E/K, \chi}(1)}{R_p(E/K, \chi)} = \frac{L_p(E/K, \chi, 1)}{\prod_{w \nmid p} Z_w(\chi_w, \psi_w)}.
$$

Here $L_p(E/K, \chi, 1)$ is the Euler factor at $p$. In particular, $\mathcal{L}'_{E/K}(1) = 0$ if and only if $L'(E/K, 1) = 0$.

**Proof.** Let $B$ be an indefinite quaternion algebra over $\mathbb{Q}$ ramified exactly at the places $v$ of $\mathbb{Q}$ where $c_v(E(\overline{K}), 1) = -1$. It is known that there exists a Shimura curve $X$ over $\mathbb{Q}$ (with suitable level) and a non-constant morphism $f : X \to E$ over $\mathbb{Q}$ mapping a divisor in Hodge class to the identity of $E$ such that its corresponding Heegner cycle $P_\chi(f)$ is non-trivial if and only if $L'(1, \phi, \chi) = 0$ by Theorem 1.2 in [19], and if and only if $\mathcal{L}'_{E/K, \chi}(1) = 0$ by Theorem B in [4]. Thus $L'(E/K, \chi, 1) = 0$ if and only if $\mathcal{L}'_{E/K, \chi}(1) = 0$.

Now assume that $L'(E/K, 1) = 0$. By an argument of Kolyvagin, we know that $(E(\overline{K}) \otimes \mathcal{O}_\chi)^!$ is of $\mathcal{O}_\chi$-rank one,

$$
\frac{\hat{h}_\infty(P_\chi(f))}{R_p(E/K, \chi)} = \frac{\hat{h}_p(P_\chi(f))}{R_p(E/K, \chi)} \in \mathbb{Q}^\times.
$$

By [19] theorem 1.2,

$$
\frac{L'(E/K, \chi, 1)}{R_p(E/K, \chi)} = \frac{\hat{h}_p(P_\chi(f))}{R_p(E/K, \chi)} \prod_{w \nmid p} Z_w(\chi_w, \psi_w) L(1, \pi, \text{ad}) \alpha^{-1}(f, \chi),
$$

and by [4] theorem B (with our definition of $\mathcal{L}_{E/K, \chi}$),

$$
\frac{\mathcal{L}'_{E/K, \chi}(1)}{R_p(E/K, \chi)} = \frac{h_p(P_\chi(f))}{R_p(E/K, \chi)} \prod_{w \nmid p} Z_w(\chi_w, \psi_w) L(1, \pi, \text{ad}) \alpha^{-1}(f, \chi),
$$

where the $\alpha(f, \chi) \in \mathbb{Q}^\times$. The theorem follows. \hfill \square

Now we give an explicit form of $p$-adic Gross-Zagier formula as an application. Let $c$ be the conductor of $\chi$. Assume the following Heegner hypothesis holds:

1. $(c, N) = 1$, and no prime divisor $q$ of $N$ is inert in $\mathcal{O}_c$, and also $q$ must be split in $K$ if $q^2 | N$.
2. $\chi([q]) \neq a_q$ for any prime $q | (N, D)$, where $q$ is the unique prime ideal of $\mathcal{O}_c$ above $q$ and $[q]$ is its class in $\text{Pic}(\mathcal{O}_c)$.

Let $X_0(N)$ be the modular curve over $\mathbb{Q}$, whose $\mathbb{C}$-points parametrize isogenies $E_1 \to E_2$ between elliptic curves over $\mathbb{C}$ whose kernel is cyclic of order $N$. By the Heegner condition, there exists a proper ideal $\mathfrak{N}$ of $\mathfrak{o}$, such that $\mathcal{O}_c/\mathfrak{N} = \mathbb{Z}/N\mathbb{Z}$. For any proper ideal $\mathfrak{a}$ of $\mathcal{O}_c$, let $P_\mathfrak{a} \in X_0(N)$ be the point representing the isogeny $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}N^{-1}$, which is defined over the ring class field $H_\mathfrak{c}$ over $K$ of conductor $c$, and only depends on the class of $\mathfrak{a}$ in $\text{Pic}(\mathcal{O}_c)$. Let $J_0(N)$ be the Jacobian of $X_0(N)$. Let $f : X_0(N) \to E$ be a modular parametrization mapping the cusps $\infty$ at infinity to the identity $O \in E$. Denote by $\text{deg} f$ the degree of the morphism $f$. Define the Heegner divisor to be

$$
P_\chi(f) := \sum_{[\mathfrak{a}] \in \text{Pic}(\mathcal{O}_c)} f(P_\mathfrak{a}) \otimes \chi([\mathfrak{a}]) \in E(H_\mathfrak{c})[\mathfrak{a}].
$$

**Theorem 3.3.** Let $E, \chi$ be as above satisfying the Heegner conditions (1) and (2). Then

$$
L'(1, E, \chi) = 2^{-\mu(N, D)} \frac{8\pi^2(\phi, \phi)_{\Gamma_0(N)}}{u^2[\text{Disc}(E)]^2} \hat{h}_\infty(P_\chi(f)) \frac{1}{\text{deg} f},
$$

where $\mu(N, D)$ is the number of prime factors of the greatest common divisor of $N$ and $D$, $u = [\mathcal{O}_c^\times : \mathbb{Z}_c^\times]$ is half of the number of roots of unity in $\mathcal{O}_c$, and $\hat{h}_\infty$ is the Néron-Tate height on $E$ over $K$. \hfill 7
Moreover, let \( p \) be a prime split in \( K \) and assume that \( E \) is potential ordinary at \( p \) (i.e. either potential good ordinary or potential semistable), then we have
\[
\mathcal{L}_{E/K,\chi}(1) = \prod_{w|p} Z_w(\chi_w, \psi_w) \frac{2^{-\nu(N,D)} \hat{h}_p(P_\chi(f))}{\deg f},
\]
where \( \hat{h}_p \) is the \( p \)-adic height on \( E \) over \( K \).

**Proof.** The explicit form of Gross-Zagier formula is proved in [2]. The explicit form of \( p \)-adic Gross-Zagier formula then follows from the relation in Theorem 4.1. \( \square \)

4. **Proof of Main Theorem 1.1**

In this section, let \( E \) be an elliptic curve over \( \mathbb{Q} \) with CM by \( K \) and \( \Omega_E \) the minimal real period of \( E \) over \( \mathbb{Q} \). Let \( p \nmid w \) be a prime split both in \( K \).

**Lemma 4.1.** Let \( K \) be an imaginary quadratic field where \( p \) splits, \( \eta \) the associated quadratic character, and \( \eta_K \) its base change to \( K \). Assume that \( \epsilon(E/K) = -1 \). Then there exists a \( p \)-adic unit \( u \) such that
\[
\mathcal{L}_{E/K} = \tau(\varphi_p, \psi_p)^2 \cdot \Omega_E^2 \frac{\mu_0(\varphi_p, \psi_p)}{\deg f} \cdot \mathcal{L}_{\varphi, \psi} \mathcal{L}_{\varphi, \eta_K}.
\]

**Proof.** It’s enough to show that for any finite order character \( \nu : \hat{Q}/\hat{Q}^\times \hat{Z}/\hat{Z}_{p, \text{tor}} \to \mathbb{C}^\times \), we have
\[

\nu_K(\mu_{E/K}) = \frac{\tau(\varphi_p, \psi_p)}{8\pi^2(\varphi, \psi)} \frac{\Omega_E^2}{\mu_0(\varphi_p, \psi_p)} \cdot \frac{\mu_0(\varphi_p, \psi_p)}{\deg f} \cdot \mathcal{L}_{\varphi, \psi} \mathcal{L}_{\varphi, \eta_K}.
\]

Note that \( K/\mathbb{Q} \) splits at \( p \) and then \( \eta_p \) is trivial, the right hand side of the formula in the lemma is
\[
\frac{L(p)(1, \phi, \nu^{-1})}{8\pi^2(\phi, \psi)} \prod_{w|p} Z_w(\alpha_w \nu_w, \psi_w),
\]
Note that \( K/\mathbb{Q} \) splits at \( p \) and then \( \eta_p \) is trivial, the right hand side of the formula in the lemma is
\[
\frac{L(p)(1, \phi, \nu^{-1})}{8\pi^2(\phi, \psi)} \prod_{w|p} Z_w(\alpha_w \nu_w, \psi_w),
\]
Then the formula follows from lemma 3.1. \( \square \)

We are ready to prove Theorem 1.1. Assume that \( L(s, E/\mathbb{Q}) \) has a simple zero at \( s = 1 \) and that \( p \) is a bad but potentially good ordinary prime for \( E \). Let \( \varphi \) be the Hecke character associated to \( E \) and \( f_0 \) its the prime-to-\( p \) conductor. We may choose an imaginary quadratic field \( K \) such that

- \( L(s, E/K) \) also has a simple zero at \( s = 1 \).
- \( p \) is splits in \( K \).
- the discriminant of \( K \) is prime to \( f_0 \).

Note that related Euler factors are trivial in this case, we then have
\[
\begin{align*}
\mathcal{L}_{\varphi_K}(1) &= \frac{L(1, E(K))}{\Omega_{E/K}}, \\
\mathcal{L}_{E/K}(1) &= \frac{L(E/K, 1)}{\Omega_{E/K}}, \\
\mathcal{L}_{E/K}(1) &= \frac{L(E/K, 1)}{\Omega_{E/K}}, \\
\text{ord}_p(\Omega_{E/K}) &= \text{ord}_p \left( \frac{L(E/K, 1)}{\Omega_{E/K}} \right), \\
\text{ord}_p \left( \frac{\mathcal{L}_{E/K}(1)}{\Omega_{E/K}} \right) &= \text{ord}_p \left( \frac{L(E/K, 1)}{\Omega_{E/K}} \right) = 0.
\end{align*}
\]
It follows that
\[
\text{ord}_p(\Omega_{E/K}) = \text{ord}_p \left( \frac{L(E/K, 1)}{\Omega_{E/K}} \right).
\]
This proves Theorem 1.1 (i). Assume that \( E(\mathbb{Q}) \) has rank one and \( \text{III}(E(\mathbb{Q}))(p) \) is finite, or equivalently, \( E(K) \) has \( \mathcal{O}_K \)-rank one and \( \text{III}(E/K) \) is finite. By [1], the cyclotomic \( p \)-adic height pairing is non-degenerate. Thus both \( \mathcal{L}_{\varphi_K} \) and \( \mathcal{L}_{\varphi_K}^\eta \) have exactly order 1 at \( s = 1 \), therefore \( \mathcal{L}_{E/K} \) has exactly order
It follows from $p$-adic Gross-Zagier formula that the related Heegner point is non-trivial and therefore $L(E, s)$ has a simple zero at $s = 1$. This completes the proof of Theorem 1.1.

**References**

[1] Daniel Bertrand, *Propriétés Arithmétiques de Fonctions Thêta à plusieurs variables*, Lect. Notes in Math., vol 1068, pp. 17-22. Berlin-Heidelberg-New York-Tokyo: Springer 1984.

[2] L. Cai, J. Shu and Y. Tian, *Explicit Gross-Zagier and Waldspurger formulae*. Algebra Number Theory 8 (2014), no. 10, 2523-2572.

[3] J. Coates and A. Wiles, *On $p$-adic L-functions and elliptic units*. J. Austral. Math. Soc. Ser. A 26 (1978), no. 1, 1-25.

[4] Daniel Diegni, *The $p$-adic Gross Zagier formula on Shimura curves*, Preprint.

[5] E. de Shalit, *The Iwasawa theory of elliptic curves with complex multiplication*, Perspect. Math. Vol.3 (1987).

[6] G. Faltings, *Crystalline cohomology and $p$-adic Galois-representations*. Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988), Johns Hopkins Univ. Press, Baltimore, MD, 1989.

[7] S. Friedberg and J. Hoffstein, *Nonvanishing theorems for automorphic $L$-functions on $GL(2)$*. Ann. of Math. (2) 142 (1995), no. 2, 385-423.

[8] Kobayashi, Shinichi, *The $p$-adic Gross-Zagier formula for elliptic curves at supersingular primes*. Invent. Math. 191 (2013), no. 3, 527-569.

[9] B. Mazur, J. Tate, and J. Teitelbaum, *On $p$-adic analogues of the conjectures of Birch and Swinnerton-Dyer*. Invent. Math. (1986) Volume 84, no. 1, pp 1-48.

[10] B. Perrin-Riou, *Groupe de Selmer d’une courbe elliptique multiplication complexe*, Compositio Math. 43 (1981), no. 3, 387-417.

[11] B. Perrin-Riou, *Descend enfin et hauteur $p$-adique sur les courbes elliptiques multiplication complexe*, Invent. Math. 79 (1982/83), no. 3, 369-398.

[12] B. Perrin-Riou, *Points de Heegner et dérivées de fonctions $L$ $p$-adiques*, Invent. Math. 89 (1987), no. 3, pp. 455-510.

[13] K. Rubin, *Tate-Shafarevich groups and $L$-functions of elliptic curves with complex multiplication*, Invent. Math. 89 (1987), no. 3, 527-559.

[14] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 103 (1991), no. 1, 23-68.

[15] P. Schneider, *Iwasawa $L$-functions of varieties over algebraic number fields. A first approach*, Invent. Math. 71 (1983), no. 2, 251-293.

[16] Y. Tian, *Congruent Numbers and Heegner Points*, Cambridge J. of Math. Vol. 2.1, 117-161, 2014.

[17] Y. Tian, X. Yuan and S. Zhang, *Genus Periods, Genus Points and Congruent Number Problem*, to appear in Asian Journal of Mathematics.

[18] R. Yager, *On two variable $p$-adic $L$-functions*, Ann. of Math. (2) 115 (1982), no. 2, 411-449.

[19] X. Yuan, S. Zhang, and W. Zhang, *The Gross-Zagier Formula on Shimura Curves*, Annals of Mathematics Studies Number 184, 2013.