SCIENCE CHINA
Mathematics

• ARTICLES •

July 2016 Vol. 59 No. 7: 1307–1326
doi: 10.1007/s11425-016-5128-3

Special automorphisms on Shimura curves and non-triviality of Heegner points

CAI Li[1], LI YongXiong[2,*] & WANG ZhangJie[1]

[1] *Yau Mathematical Sciences Center, Tsinghua University, Beijing* 100084*, China;*
[2] *Morningside Center of Mathematics, Academy of Mathematics and Systems Science,*
Chinese Academy of Sciences, Beijing 100190*, China*
Email: lcai@math.tsinghua.edu.cn, liyx_1029@126.com, zjwang@math.tsinghua.edu.cn

Received April 22, 2015; accepted October 20, 2015; published online February 3, 2016

Abstract We define the notion of special automorphisms on Shimura curves. Using this notion, for a wild class of elliptic curves defined over $\mathbb{Q}$, we get rank one quadratic twists by discriminants having any prescribed number of prime factors. Finally, as an application, we obtain some new results on Birch and Swinnerton-Dyer (BSD) conjecture for the rank one quadratic twists of the elliptic curve $X_0(49)$.

Keywords Shimura curves, Heegner points, BSD conjecture

MSC(2010) 11G05, 11G40

Citation: Cai L, Li Y X, Wang Z J. Special automorphisms on Shimura curves and non-triviality of Heegner points. Sci China Math, 2016, 59: 1307–1326, doi: 10.1007/s11425-016-5128-3

1 Introduction and main results

For an elliptic curve E defined over $\mathbb{Q}$, the Birch and Swinnerton-Dyer conjecture [2] predicts a relation between the special values of its Hasse-Weil L-function and its arithmetic groups, such as the Mordell-Weil group and the Tate-Shafarevich group.

If E is defined by Weierstrass equation

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q},$$

then for any nonzero square free integer d, the quadratic twist $E^{(d)}$ of E over the field $\mathbb{Q}(\sqrt{d})$ has Weierstrass equation

$$E^{(d)} : dy^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q}.$$

In 1952, Heegner [8] proved that a positive integer n congruents to $5, 6, 7$ modulo 8 with exactly one odd prime factor is a congruent number, i.e., the quadratic twist $\mathcal{C}^{(n)}$ of the elliptic curve

$$\mathcal{C} : y^2 = x^3 - x$$

over the field $\mathbb{Q}(\sqrt{-n})$ is of positive rank. Heegner [8] constructed the so-called Heegner points and proved their non-triviality. Later on, Birch [1] used the Atkin-Lehner involution acting on the Heegner points constructed by modular parametrization of E via $X_0(N)$, and obtained some non-triviality results

[*] Corresponding author

of Heegner points. Around the year 2012, Tian et al. [15–17] made a breakthrough on congruent number problem, where not only the Atkin-Lehner involution but also some other modular involutions are involved.

In this paper, we generalize the usual Atkin-Lehner operator and the involutions used in [16] to the special modular automorphisms on Shimura curves. Applying the Euler system property of Heegner points [10, 11] at both split and inert Kolyvagin primes, we get for a wild class of elliptic curves defined over $\mathbb{Q}$, a quadratic twist family with any given number of prime factors of the quadratic discriminant, which has Mordell-Weil rank equal to one. Finally, as an application, we improve some results in [5] on quadratic twists of the elliptic curve $A = (X_0(49), [\infty])$, where $[\infty]$ is the infinity cusp identified with identity element in $A(\mathbb{Q})$.

Notation. Let F be a number field with adéle ring $\mathbb{A} = F_{\mathbb{A}}$ and let $\mathbb{A}_f = F_{\mathbb{A}_f}$ be the ring of finite adéles. Let $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ and for any $\mathbb{Z}$-module M, let $\widehat{M} = M \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$, for example, $\widehat{F} = \mathbb{A}_f$. For any number field K, let $\mathcal{O}_K$ denote the ring of integers in K, K^{ab} the maximal abelian extension over K, and

$$\sigma^K : K_{\mathbb{A}}^{\times}/K^{\times} \to \mathrm{Gal}(K^{ab}/K), \quad t \mapsto \sigma_t^K$$

be the reciprocity law morphism in class field theory. If the field in the context is clear, we also write it for σ_t. If K/F is a quadratic extension of number fields and $c \subset \mathcal{O}_F$ is an integral ideal, denote

$$\mathcal{O}_c = \mathcal{O}_F + c\mathcal{O}_K$$

to be the unique order $\mathcal{O}$ of K with $[\mathcal{O}_K : \mathcal{O}] = \#(\mathcal{O}_F/c)$ and call c its conductor. For each place v of F, let $\mathcal{O}_{c,v}$ denote the localization of $\mathcal{O}_c$ at v. If B is a quaternion algebra over F and K is an imaginary quadratic field embedded into B as an F-subalgebra, we denote by K^- the K-module of elements $j \in B$ such that $jt = \overline{t}j$ for all $t \in K$, where $t \mapsto \overline{t}$ is the non-trivial element in $\mathrm{Gal}(K/\mathbb{Q})$. For a finite set S of places of F, we let $K_{\mathbb{A}}^{\times(S)}$ denote the S-off idéles of K and be viewed as a subgroup of $K_{\mathbb{A}}^{\times}$ by the natural embedding with all v-components in S being 1. For any $\mathbb{Q}$-algebra L, we write B_L (resp. $B_L^{\times}$) the base change of B (resp. $B^{\times}$) to L. Denote $[\frac{a}{b}]$ the usual cusp of the upper half plane obtained from $P^1(\mathbb{Q})$. For a group G and its subgroup H, we denote $N_G(H)$ the normalizer of H in G.

In the following of this paper, we shall always consider an elliptic curve E defined over $\mathbb{Q}$ with conductor N and an imaginary quadratic field K with discriminant D.

Let X_U be a Shmura curve over $\mathbb{Q}$ associated to an indefinite quaternion algebra B with level $U \subset B_{\mathbb{A}_f}^{\times}$. Note that any normalizer of U in $\widehat{B}^{\times}$ defines a modular automorphism of X_U over $\mathbb{Q}$.

Let $S = S_U$ be a set of finite places of $\mathbb{Q}$ containing all places dividing $2ND$ such that $U = U_S U^S$ with $U_S \subset \prod_{v \in S} G(\mathbb{Q}_v)$ and U^S is a maximal open compact subgroup of $G(\mathbb{A}_f^S)$.

The first main result of this paper is the following theorem.

Theorem 1.1. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and $\phi = \sum_{n=1} a_n q^n$ the associated new form. Let $f : X_U \to E$ over $\mathbb{Q}$ be a modular parametrization by a Shimura curve X_U associated to an indefinite quaternion algebra B of level U containing $\widehat{\mathbb{Z}}^{\times}$. Let $K \subset B$ be an imaginary quadratic field of discriminant D and let $H = H_U$ denote the abelian extension over K corresponding to the class group $K^{\times}(U \cap \widehat{K}^{\times})$.*

Assume that

(i) *$E(\mathbb{Q})$ has no order 4 torsion points*;

(ii) *$(D, 2N) = 1$ and $[H : K]$ is odd*;

(iii) *there exists $w \in N_{\widehat{B}^{\times}} U$ with $w = t_0 j$ for some $t_0 \in \widehat{K}^{\times}$ and $j \in K^-$ such that the morphism $f + f^w : X_U \to E$ is constant valued at a torsion point $Q_0 \notin 2E(\mathbb{Q})$.*

For any $r \geqslant 1$, let Σ_r denote the set of primes $\ell \notin S_U$ satisfying:

$$\text{(i) } a_\ell \equiv 0 \bmod 2^{r+1}, \quad \text{(ii) } \ell \equiv 1 \bmod 4, \quad \text{(iii) } \sigma_{t_0}^K(\sqrt{\ell}) = \sqrt{\ell}.$$

Then for any integer $M = \ell_1 \cdots \ell_r$ with $\ell_1, \ldots, \ell_r \in \Sigma_r$,

$$\mathrm{rank}_{\mathbb{Z}} E^{(DM)}(\mathbb{Q}) = 1 = \mathrm{ord}_{s=1} L(E^{(DM)}, s) \quad \text{and} \quad \mathrm{rank}_{\mathbb{Z}} E^{(M)}(\mathbb{Q}) = 0 = \mathrm{ord}_{s=1} L(E^{(M)}, s).$$

Remark 1.2. (1) The above set Σ_r of certain primes may be empty or has finite cardinality. But in some cases, it has infinite cardinality, for example, when the curve has a special supersingular primes (see Corollary 1.3).

(2) Since the torsion point $Q_0 \notin 2E(\mathbb{Q})$ must be of even order, the condition (i) implies that

$$E(\mathbb{Q})[2^\infty] = E(\mathbb{Q})[2] \neq 0.$$

(3) Some cases of the above theorem are given as follows.

(a) Suppose the imaginary quadratic field K satisfies the Heegner hypothesis and let $f : X_0(N) \to E$ be the usual modular parametrization. Then the Atkin-Lehner operator w_N is a normalizer of

$$U_0(N) \subset \mathrm{GL}_2(\mathbb{A}_f)$$

and there are $t_0 \in \widehat{K}^\times, u \in U_0(N), j \in K^-$ such that

$$w := w_N u = t_0 j.$$

The condition (iii) is satisfied if $f([0]) \notin 2E(\mathbb{Q})$.

(b) Let E be an elliptic curve of square conductor $N = M^2$ and K an imaginary quadratic field such that any prime factor of N is inert in K. We take $B = \mathrm{End}_{\mathbb{Q}}(K)$ and view K as $\mathbb{Q}$-subalgebra naturally. Let $j \in B^\times$ be the element $j(x) = \overline{x}$. Then the maximal order $\mathcal{O}_B := \mathrm{End}_{\mathbb{Z}}(\mathcal{O}_K)$ of B contains $\mathcal{O}_K$ and we have $\mathcal{O}_B = \mathcal{O}_K + \mathfrak{d}^{-1}j$, where $\mathfrak{d}$ is the differential of K over $\mathbb{Q}$. Take $R = \mathcal{O}_K + M\mathcal{O}_B$, then we have that j normalizes $\widehat{R}^\times$. Note that in this case w acting on f has an eigenvalue $-\epsilon(E)$ by a result of [14, Theorem 4]. In particular, the condition that $f^w + f$ is a constant morphism implies the sign of L-series is $+1$.

Corollary 1.3. *Let $f : X_U \to E$ be a modular parametrization of an elliptic curve over $\mathbb{Q}$ by a Shimura curve associated to a quaternion algebra B. Let $K \subset B$ be an imaginary quadratic field of discriminant D. Assume the conditions* (i)–(iii) *in Theorem* 1.1 *and the following*:

(iv) *there is a supersingular good prime q for E with $q \equiv 1 \bmod 4$ and $\sigma_{t_0}^K(\sqrt{q}) = \sqrt{q}$.*

Then for any integer $k \geqslant 1$, there are infinitely many square-free M with exactly k odd prime factors such that

$$\mathrm{ord}_{s=1} L(E^{(M)}, s) = 0 \quad \textit{and} \quad \mathrm{ord}_{s=1} L(E^{(DM)}, s) = 1.$$

Example 1.4. Let E be the elliptic curve of conductor 69 with the equation

$$y^2 + xy + y = x^3 - x - 1.$$

Then $q = 5$ is a supersingular prime for E.

Note that Corollary 1.3 follows from Theorem 1.1 by the following lemma.

Lemma 1.5. *Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N and M a non-zero integer. Suppose that there is a supersingular good prime q of E with $q \equiv 1 \bmod 4$ and $(\frac{M}{q}) = 1$. Then for any integer $r \geqslant 1$, there are infinitely many primes $\ell \nmid N$ such that $a_\ell \equiv 0 \bmod 2^{r+1}$, $\ell \equiv 1 \bmod 4$, and $(\frac{M}{\ell}) = 1$.*

Proof. Let L be the Galois extension $\mathbb{Q}(i, \sqrt{M}, E[2^{r+1}])$ over $\mathbb{Q}$ and $\mathrm{Frob}_q \subset \mathrm{Gal}(L/\mathbb{Q})$ be the conjugate class of the prime q. Then by Chebatarev density theorem, there are infinitely many primes ℓ, with positive density, unramified over L such that $\mathrm{Frob}_\ell = \mathrm{Frob}_q$. Note that $a_q = 0$ implies that $a_\ell \equiv 0 \bmod 2^{r+1}$. It is clear that ℓ satisfies the required conditions. □

In the following, we give an application of the above non-triviality results to the quadratic twists of the elliptic curve $A = (X_0(49), [\infty])$. Using the special value formula in [4] and the induction argument in [16], we obtain more information on the rank zero and rank one quadratic twists of A.

The following is a proposition on special values of L-function for the rank zero quadratic twists of the curve $A = (X_0(49), [\infty])$.

Proposition 1.6. *Let $R = q_1 \cdots q_r$ be a square-free integer with all prime factors $q_i \equiv 1 \bmod 4$ inert in $\mathbb{Q}(\sqrt{-7})$. Let $N = p_1 \cdots p_k$ $(k \geqslant 1)$ be a square-free integer with all prime factors p_j completely split in $\mathbb{Q}(A[4], \sqrt{R})$. Then for the elliptic curve $A = (X_0(49), [\infty])$, we have $\mathrm{ord}_2(L^{\mathrm{alg}}(A^{(R)}, 1)) = r - 1$, and $\mathrm{ord}_2(L^{\mathrm{alg}}(A^{(RN)}, 1)) \geqslant 2k + r + 1$.*

Remark 1.7. By the main results in [6] and descent theory, we know the above estimate on 2-adic valuation of algebraic part of L-values is always true. Here, we just give a direct proof for the above result without using Iwasawa main conjecture.

Another main result of this paper is the following theorem.

Theorem 1.8. *Let $A = (X_0(49), [\infty])$ and $M = -\ell_0 RN$ be a negative square-free integer, with*

- *$\ell_0 \equiv 3 \bmod 4$ a prime not equal to 7, which is a non square modulo 7,*
- *R a positive integer with all prime factors $\equiv 1 \bmod 4$ and inert in $\mathbb{Q}(\sqrt{-7})$,*
- *N a positive integer with all prime factors splits completely in $\mathbb{Q}(A[4], \sqrt{R})$.*

Assume that $\mathbb{Q}(\sqrt{-\ell_0 N})$ has no ideal class of exact order 4. Denote by $A^{(M)}$ the quadratic twists of A over $\mathbb{Q}(\sqrt{M})$. Then

$$\mathrm{ord}_{s=1} L(A^{(M)}, s) = 1 = \mathrm{rank}_{\mathbb{Z}} A^{(M)}(\mathbb{Q}),$$

and $\text{Ш}(A^{(M)}/\mathbb{Q})$ is finite of odd order. Moreover, the full ℓ-part BSD conjecture on $\#(\text{Ш}(A^{(M)}/\mathbb{Q})[\ell^\infty])$ holds for all primes $\ell \nmid 7M$.

In the end of introduction, we briefly give the structure of content for the following sections. In Section 2, we summarize the basis on Shimura curves and give the proof of Theorem 1.1. In Section 3, we give the estimate of the two-adic valuation on L-values which will be used in the final section. In Section 4, we will combine all the results developed before and induction method of Tian to give the proof of Theorem 1.8 and verify the BSD conjecture.

2 Generalized Birch lemma and its application

In this section, we prove Theorem 1.1 and begin with introducing some basis on Shimura curves.

2.1 Shimura curves and various actions

Let B be an indefinite quaternion algebra over $\mathbb{Q}$ with discriminant d_B and view $B^\times$ as a subgroup of $\mathrm{GL}_2(\mathbb{R})$ via an isomorphism $B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R})$. Denote $B_+^\times$ to be the element with positive determinant in $B^\times$. There is a projective system of compact Riemann surfaces

$$X_U(\mathbb{C}) \cong B_+^\times \backslash (\mathcal{H} \cup \mathbb{P}^1) \times B_{\mathbb{A}_f}^\times / U,$$

indexed by open compact subgroups U of $B_{\mathbb{A}_f}^\times$ and with the connection map

$$\varphi_{UU'} : X_U(\mathbb{C}) \to X_{U'}(\mathbb{C}), \quad U \subset U'.$$

This system has a canonical descent to a projective system of algebraic curves over $\mathbb{Q}$, which is a projective smooth irreducible, but not necessarily geometrically irreducible algebraic curve over $\mathbb{Q}$.

The Hecke action on X_U is defined as follows. For any $t \in B_{\mathbb{A}_f}^\times$, it maps $X_U(\mathbb{C})$ to $X_{t^{-1}Ut}(\mathbb{C})$, which on the points is given by $[h, g] \mapsto [h, gt]$. It is well known that the Hecke action of the right multiplication by t also descents to $\mathbb{Q}$.

We know that the structure map $X_U(\mathbb{C}) \to \pi_0(X_U(\mathbb{C}))$ descents as $X_U \to \mathrm{Spec} F_U$, where F_U is the abelian extension of $\mathbb{Q}$ corresponding to the idéle class subgroup $\mathbb{Q}_+^\times \det U \subset \mathbb{A}_f^\times$. Here X_U is geometrically irreducible over F_U, and $\pi_0(X_U(\mathbb{C}))$ is the connected components of $X_U(\mathbb{C})$.

We recall the Galois action on points of X_U as follows. For any imaginary quadratic field $K \subset \mathbb{C}$, let $\rho : K^\times \to B^\times$ be the normalized embedding with fixed point $h_0 \in \mathcal{H}$. Here normalized embedding means the one satisfying that

$$\rho(t)\begin{pmatrix} h_0 \\ 1 \end{pmatrix} = t\begin{pmatrix} h_0 \\ 1 \end{pmatrix}.$$

Let σ_t denote its image under Artin's reciprocity law in class field theory, then for any $t \in \widehat{K}^\times$,

$$[h_0, g]^{\sigma_t} = [h_0, \rho(t)g], \quad \forall\, g \in \mathrm{GL}_2(\mathbb{A}_f).$$

For any $j \in \mathrm{N}_{\mathrm{GL}_2(\mathbb{Q})}(\rho(K^\times)) \setminus \rho(K^\times)$, denote by $P \mapsto \overline{P}$ the complex conjugation action, where its explicit action on points is given by

$$\overline{[h_0, g]} = [h_0, jg], \quad \forall\, g \in \mathrm{GL}_2(\mathbb{A}_f).$$

2.2 Modular automorphisms on Shimura curves

For a Shimura curve X_U, we know for each element t in the normalizer of U in $\widehat{B}^\times_{\mathbb{A}_f}$, the Hecke action of right multiplication by t on X_U gives an automorphism on this curve which is defined over $\mathbb{Q}$. Thus we have the following map,

$$\mathrm{N}_{\widehat{B}^\times_{\mathbb{A}_f}}(U) \rightarrow \mathrm{Aut}_{\mathbb{Q}}(X_U).$$

Example 2.1. For the modular curve $X_0(N)$, we know the matrix

$$W_N = \begin{pmatrix} 0 & 1 \\ N & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}) \subset \mathrm{GL}_2(\mathbb{A}_f)$$

is a normalizer of $U_0(N)$ in $\mathrm{GL}_2(\mathbb{A}_f)$. This automorphism is called Atkin-Lehner involution in literature.

Sometimes, we not only consider a single Shimura curve, but also an imaginary quadratic field K with an algebraic embedding into B. In this case, the modular automorphism is very subtle.

Example 2.2. For the modular curve $X_0(36)$, let $K = \mathbb{Q}(\sqrt{-q})$ with $q \equiv 3 \bmod 4$ be a prime such that 2 is inert in K, and 3 is split in K. One can choose an integer a such that $q + a^2 \equiv 0 \pmod 9$. Then we embed K into $M_2(\mathbb{Q})$ in the following manner:

$$\sqrt{-q} \mapsto \begin{pmatrix} a & -2 \\ \frac{q+a^2}{2} & -a \end{pmatrix}.$$

Define $R = \prod_p R_p \subset M_2(\mathbb{A}_f)$ such that

- $R_p = M_2(\mathbb{Z}_p)$ for $p \nmid 6$,
- $R_2 = \mathcal{O}_{K,2} + 2M_2(\mathbb{Z}_2)$,
- $R_3 = \{\alpha \in M_2(\mathbb{Z}_3) : \alpha \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod 9\}$. Then letting $U = R^\times$, we get a Shimura curve X_U. Let

$$j = \begin{pmatrix} 1 & 0 \\ a & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}),$$

then $j \in K^-$. Denote

$$w_3 = \begin{pmatrix} 0 & 1 \\ 9 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_3)$$

to be a local Atkin-Lehner operator. Then the element $w = j^{(3)} w_3$ gives an automorphism on the curve X_U, where $j^{(3)}$ denotes the element $j \in \mathrm{GL}_2(\mathbb{A}_f)$ with the component at the place 3 removed. One can show that the element $w = j \cdot (j_3 w_3) := tj$, with $j \in K^-, t \in \widehat{K}^\times$, where the last equality is up to an element of U. Here j_3 means the 3-component of j.

In the above example, we write the automorphism by a product of elements in $\widehat{K}^\times$ and K^- up to elements in U. We will see this kind of automorphism has an arithmetic application for the argument of the non-triviality of the Heegner point.

Definition 2.3. Let X_U be a Shimura curve, and $K \subset B$ be an imaginary quadratic field embedded in B. We call an automorphism w on Shimura curve X_U a *special automorphism* for the pair (X_U, K), if w can be written as $w = tj$, where $t \in \widehat{K}^\times, j \in K^-$, up to right multiplication by an element in U.

Remark 2.4. • From last section, we know the special automorphism is a combination of the Galois action and complex conjugation on the points.

• One can show that for the usual modular curve $X_0(N)$, an imaginary quadratic field K satisfies that every prime divisor of N splits in K. The Atkin-Lehner operator W_N is a special automorphism on $X_0(N)$.

In the end of this subsection, we give a description of the special automorphism for the pair of a Shimura curve X_U with conductor $N_-^2 N_+$, and an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-q})$ with $q \equiv 3 \bmod 4$ a prime embedded in B, such that N_- is the square free integer with prime divisors inert in K, while N_+ is the integer with prime divisors which are split in K.

Proposition 2.5. *For the pair (X_U, K) with X_U a Shimura curve of conductor $N_-^2 N_+$ and imaginary quadratic field K embedded in B given in the above paragraph, the special automorphism exists.*

Proof. Note that 2 may divide N_+, so we choose an integer a such that $a^2 + q \equiv 0 \bmod 4N_+$.Write $N_- = \prod_i p_i, N_+ = \prod_j q_j^{n_j}$. We embed K into $M_2(\mathbb{Q})$ as follows,

$$\sqrt{-q} \mapsto \begin{pmatrix} a & -2 \\ \frac{q+a^2}{2} & -a \end{pmatrix}.$$

Define $R = \prod_p R_p \subset M_2(\mathbb{A}_f)$ such that,

- $R_p = M_2(\mathbb{Z}_p)$, for $p \nmid N_- N_+$;
- $R_{p_i} = 1 + p_i M_2(\mathbb{Z}_{p_i})$, for $p_i \mid N_-$;
- $R_{q_j} = U_0(q_j^{n_j}) := \{\alpha \in M_2(\mathbb{Z}_{q_j}) : \alpha \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod q_j^{n_j}\}$, for $q_j \mid N_+$.

Then let $U = R^\times \subset \mathrm{GL}_2(\mathbb{A}_f)$ and the Shimura curve is X_U. Now we claim the following element w is the special automorphism for (X_U, K),

$$w := j^{(N_+)} \prod_{q_j | N_+} w_{q_j},$$

where

$$j = \begin{pmatrix} 1 & 0 \\ a & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}) \cap K^-$$

and $j^{(N_+)}$ denotes its N_+ removed part. The local Atkin-Lehner w_{q_j} is

$$w_{q_j} = \begin{pmatrix} 0 & 1 \\ q_j^{n_j} & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_{q_j}).$$

We have $w \in N_U(\widehat{B}^\times_{\mathbb{A}_f})$. Write w in the form $w = j \cdot (\prod_{q_j | N_+} j_{q_j} w_{q_j})$, where j_{q_j} is the q_j component of j. One can show that $\prod_{q_j | N_+} j_{q_j} w_{q_j} \in \widehat{K}^\times U$. Thus up to element of U, we know w is a special automorphism for (X_U, K). □

2.3 CM points on Shimura curves and Euler system properties

Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N and K be an imaginary quadratic field with discriminant D.

Let X_U be a Shimura curve over $\mathbb{Q}$ of level U which parametrizes E. Let $K \subset B$ be $\mathbb{Q}$-algebra embedding and $x_1 = [h_0, 1] \in X_U$ with $h_0 \in \mathcal{H}$ the unique fixed point by $K^\times \subset G = B^\times$. Let S be a set of finite places of $\mathbb{Q}$ satisfying the following:

1. S contains all places dividing $6ND$;

2. U has the form $U^S U_S$ such that $U^S = \prod_{v \notin S} K_v \subset \prod'_{v \notin S} G(\mathbb{Q}_v)$ is a maximal open compact subgroup and $U_S \subset \prod_{v \in S} G(\mathbb{Q}_v)$. Note that $d_B | N$ and therefore $\prod'_{v \notin S} G(\mathbb{Q}_v) \cong \mathrm{GL}_2(\mathbb{A}_f^{(S)})$.

Let $\mathbb{N}_S$ denote the set of integers with prime divisors which are not in S. For each prime $\ell \in \mathbb{N}_S$, fix an isomorphism $\alpha_\ell : B_\ell \xrightarrow{\sim} M_2(\mathbb{Q}_\ell)$ such that U_ℓ is identified with $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and satisfies

1. if ℓ is split in K, then

$$\alpha(K_\ell) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, a, b \in \mathbb{Q}_\ell \right\};$$

2. if ℓ is inert in K, then

$$\alpha(K_\ell) = \left\{ \begin{pmatrix} a & b\delta \\ b & a \end{pmatrix} : a, b \in \mathbb{Q}_\ell \right\},$$

for some $\delta \in \mathbb{Z}_\ell^\times \setminus \mathbb{Z}_\ell^{\times 2}$.

It follows that for any $v \notin S$, $K_v^\times \cap U_v = \mathcal{O}_{K_v}^\times$. For any positive integer k, let $g(\ell^k)$ denote the element

$$\begin{pmatrix} \ell^k & 1 \\ 0 & 1 \end{pmatrix} \in G(\mathbb{Q}_\ell) \quad \left(\text{resp. } \begin{pmatrix} \ell^k & 0 \\ 0 & 1 \end{pmatrix} \in G(\mathbb{Q}_\ell)\right)$$

in the case ℓ split (resp. inert) in K. For each integer $n = \prod_i \ell_i^{k_i} \in \mathbb{N}_S$ with ℓ_i distinct primes, let

$$g(n) = \prod_i g(\ell_i^{k_i}) \in G(\mathbb{A}_f), \quad P_n = [h_0, g(n)].$$

Note that P_n is defined over the abelian extension H_n over K which is characterized by

$$\mathrm{Gal}(H_n/K) \cong \widehat{K}^\times / K^\times \cdot (g(n) U g(n)^{-1} \cap \widehat{K}^\times),$$

via the class field theory.

We have the following theorem on norm properties of Heegner points.

Theorem 2.6 (See [10, 12]). *For any $\ell, m \in \mathrm{N}_S$ with ℓ a prime and $\ell \nmid m$, then we have that $[H_{m\ell} : H_m] = \ell + 1$ if ℓ is inert in K and $\ell - 1$ if ℓ is split and*

$$u_m \, Tr_{H_{m\ell}/H_m} P_{m\ell} = \begin{cases} \mathrm{T}_\ell P_m, & \text{if } \ell \text{ is inert in } K, \\ (\mathrm{T}_\ell - \sum_{w \mid \ell} \mathrm{Frob}_w) P_m, & \text{if } \ell \text{ is split in } K, \end{cases}$$

where T_ℓ is the Hecke correspondence, Frob_w is the Frobenius at $w \mid \ell$ in $\mathrm{Gal}(H_m/K)$, and $u_m = 1$ if $m \neq 1$ and $u_1 = [\mathcal{O}_K^\times \cap U : \mathbb{Z}^\times \cap U]$.

2.4 Generalized Birch lemma and rank one twists

We shall give the Birch lemma and its generalization in arbitrary level modular curve setting in this subsection. First, we recall the classical Birch lemma in the $\Gamma_0(N)$-level modular curve setting.

Birch's lemma. *Assume that E is an elliptic curve over $\mathbb{Q}$ and $f : X_0(N) \to E$ is a modular parametrization mapping the cusp $[\infty]$ to $O \in E$. Let K be an imaginary quadratic field of discriminant $D \neq -3, -4$. Assume that*

(1) *all prime factors of N split in K,*

(2) *$f([0]) \notin 2E(\mathbb{Q})$,*

(3) *K has odd ideal class number.*

Let $P \in X_0(H_K)$ be the CM point and define $y_K = \mathrm{Tr}_{H_K/K} f(P)$. Then we have that $2y_K \in E(K)^-$ is of infinite order.

Remark 2.7. The condition in the Birch lemma has the following meaning: The condition (1) gives a sufficient condition to construct the CM point on $X_0(N)$. The condition (2) follows from the relation $f + f^{W_N} =$ const and that this constant point is not in $2E(\mathbb{Q})$. In the following, we will generalize these two conditions to the special automorphisms that we defined.

In the case of arbitrary level modular curve parametrization, Birch's lemma has the following generalization. Before stating this lemma, we make the following convention on the 2-index of an element in an abelian group.

For any finitely generated abelian group $\mathfrak{G}$ and an element $a \in \mathfrak{G}$, define the 2-index of a to be ∞ if $a \in \mathfrak{G}_{\mathrm{tor}}$ and otherwise the maximal non-negative integer r such that $a \in 2^r\mathfrak{G}+\mathfrak{G}_{\mathrm{tor}}$ but $a \notin 2^{r+1}\mathfrak{G}+\mathfrak{G}_{\mathrm{tor}}$. Note that Ca for any odd integer C has the same 2-index as a.

Lemma 2.8. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and let $f : X_U \to E$ be a modular parametrization by a Shimura curve associated to an indefinite quaternion algebra B with level $U \supset \widehat{\mathbb{Z}}^\times$. Let $K \subset B$ be an imaginary quadratic field of discriminant $D \neq -3, -4$. Assume that*

(1) *there is an element $w = t_0 j \in N_{\widehat{B}^\times}U$ which is a special automorphism for (X_U, K) and such that $f + f^w$ is a constant map with value in a torsion point $Q \notin 2E(\mathbb{Q})$.*

(2) *$(D, 2N) = 1$ and $[H : K]$ is odd, where H is the abelian extension over K such that* $\mathrm{Gal}(H/K) \cong \widehat{K}^\times/K^\times(U \cap \widehat{K}^\times)$ *under the reciprocity law in class field theory.*

Let C be the cardinality of the odd part of $E(K)_{\mathrm{tor}}$, and $y_K := C \cdot \mathrm{Tr}_{H/K} f(P_1) \in E(K)$. If 2^δ denotes the the 2-part order of the point $y_K + \overline{y}_K$, then we have

$$y_K \in E(K) \setminus 2E(K) + E(K)_{\mathrm{tor}}, \tag{2.1}$$

and also the relation

$$2^\delta y_K \in E(K)^- \setminus 2^\delta E(K)^- + E(K)^-_{\mathrm{tor}}. \tag{2.2}$$

Moreover, $\overline{y}_K + y_K \in E(\mathbb{Q})[2^\infty] \setminus \{O\}$ is a multiple of Q.

We first give an example of Lemma 2.8, where the usual Heegner hypothesis, i.e., the condition (1) in Birch's lemma, is not satisfied.

Example 2.9 (Continue with Example 2.2)**.** From [7], we know $E = X_U$ has the equation

$$E : y^2 = x^3 - 27.$$

One can show that the cusp

$$[0], [\infty] \in E(\mathbb{Q})_{\mathrm{tor}} = \mathbb{Z}/2\mathbb{Z}.$$

We may assume $[0] = T$ with T the unique nonzero two torsion point on $E(\mathbb{Q})$. One can show that $[\infty] + [\infty]^w = T$, so from this generalized Birch's lemma we know that $E^{(-q)}(\mathbb{Q})$ has rank equal to one. For more precise information on this example, see [3].

Remark 2.10. Birch considered the action of Atkin-Lehner operator w_N on $X_0(N)$ in the case where Heegner hypothesis is satisfied. Birch made the assumption that the modular parametrization $f : X_0(N) \to E$ satisfies $f([0]) \notin 2E(\mathbb{Q})$. This assumption implies that the eigenvalue of w_N must be -1. Otherwise, $f \circ w_N - f$ is a constant morphism with image $f([0]) \neq 0$, but w_N has the fixed point

$$[\sqrt{-N^{-1}}] \in \Gamma_0(N)\backslash\mathcal{H}^* = X_0(N)(\mathbb{C}),$$

where the constant map takes value $0 \in E(\mathbb{Q})$, a contradiction.

Let $C \in \mathbb{Z}$ be the integer such that $f^*w_0 = C\phi(q)dq/q$, where w_0 is the Néron differential on E and $\phi(q)$ is the normalized new form associated to E (it is conjectured that $C = 1$ if f is an optimal parametrization). Let $\alpha \in H_1(X_0(N)(\mathbb{C}), \mathbb{R})$ be the path represented by the imaginary axis from 0 to $\mathrm{i}\infty$ on $\mathcal{H}$. Let $\frac{m}{n}$ be the reduced fraction with $n \geqslant 1$ such that $nf_*\alpha = m\gamma_+$, where γ_+ is a generator of $H_1(E(\mathbb{C}), \mathbb{Z})^+$. Note that n is the order of $f([0])$ in $E(\mathbb{Q})_{\mathrm{tor}}$. It follows that

$$L(E,1) = \int_\alpha 2\pi\mathrm{i}\phi(z)dz = C^{-1}\int_{f_*\alpha} w_0 = C^{-1}\frac{m}{n}\Omega^+.$$

In particular, if $n \neq 1$ then $L(E, 1) \neq 0$.

Proof of Lemma 2.8. Let $P_1 = [h_0, 1]$ be the CM point on X_U with $h_0 \in \mathcal{H}$ the unique point fixed by $K^\times$. Then P_1 is defined over H. Note that for any $t \in \widehat{K}^\times$, let $\sigma_t \in \mathrm{Gal}(H/K)$ be the image of t under the reciprocity law map. We have that

$$[h_0, t]^w = [h_0, tw] = [h_0, tt_0 j] = [h_0, j\overline{t}\overline{t}_0] = \overline{[h_0, \overline{t}\overline{t}_0]}.$$

It follows that for any $t \in \widehat{K}^\times$,

$$Q = f([h_0, t]) + f([h_0, tw]) = f(P_1)^{\sigma_t} + \overline{f(P_1)^{\sigma_{\overline{t}t_0}}}.$$

Let $h = [H : K]$. Then taking summation of the above equality over all $t \in \widehat{K}^\times / K^\times (U \cap \widehat{K}^\times)$ and noting that $\sigma_{\overline{t}} = \sigma_{t^{-1}}$ on H by the assumption that $\widehat{\mathbb{Z}}^\times \subset U$, we have that

$$T := \overline{y}_K + y_K = hCQ \in E(\mathbb{Q})[2^\delta] \setminus (2E(\mathbb{Q}) + E(\mathbb{Q})[2^{\delta-1}])$$

is of order 2^δ and it follows that $2^\delta y_K \in E(K)^-$.

We now claim that $E(K)[2^\infty] = E(\mathbb{Q})[2^\infty]$. Otherwise let $P \in E(K)[2^\infty] \setminus E(\mathbb{Q})$, then $K = \mathbb{Q}(P)$ which is only ramified at 2 and primes dividing N, which contradicts that $(2N, D) = 1$.

Suppose that $2^\delta y_K \in 2^\delta E(K)^- + E(K)_{\mathrm{tor}}$ and let $2^\delta y_K = 2^\delta y + t$ with $y \in E(K)^-$ and $t \in E(K)[2^\infty]$. Then $s := y_K - y \in E(K)[2^\infty] = E(\mathbb{Q})[2^\infty]$ and therefore

$$T = \overline{y}_K + y_K = 2s \in 2E(\mathbb{Q}),$$

a contradiction. We have shown that

$$2^\delta y_K \in E(K)^- \setminus 2^\delta E(K)^- + E(K)^-_{\mathrm{tor}}.$$

Suppose that $y_K \in 2E(K) + E(K)_{\mathrm{tor}}$. Say $y_K = 2y + t$ for some $y \in E(K)$ and $t \in E(K)[2^\infty] = E(\mathbb{Q})[2^\infty]$. It follows that $T = \overline{y}_K + y_K = 2(\overline{y} + y) + 2t \in 2E(\mathbb{Q})$, a contradiction. Thus we have that

$$y_K \in E(K) \backslash 2E(K) + E(K)_{\mathrm{tor}}. \qquad \square$$

Remark 2.11. In the statement of Lemma 2.8, the relation (2.1) gives that the point in $y_K \in E(K)$ is non-torsion, while the relation (2.2) gives that the group $E^{(D)}(\mathbb{Q})$ should have rank one.

With the above generalized Birch's lemma and Euler system property, we can get a family of rank zero and rank one quadratic twists of elliptic curves which are parametrized by arbitrary level of modular curves.

Theorem 2.12. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and $\phi = \sum_{n=1} a_n q^n$ the associated new form. Let $f : X_U \to E$ over $\mathbb{Q}$ be a modular parametrization by a Shimura curve X_U associated to an indefinite quaternion algebra B of level $U \supset \widehat{\mathbb{Z}}^\times$. Let $K \subset B$ be an imaginary quadratic field with discriminant $D \neq -3, -4$. Assume that*

(1) *$E(\mathbb{Q})$ has no order 4 torsion points*;

(2) *$(D, 2N) = 1$ and $[H : K]$ is odd, where H is the abelian extension over K such that* $\mathrm{Gal}(H/K) \cong \widehat{K}^\times / K^\times (U \cap \widehat{K}^\times)$ *under the reciprocity law in class field theory*;

(3) *there exists $w = t_0 j \in N_{\widehat{B}^\times} U$ which is a special automorphism for the pair (X_U, K) and such that $f + f^w$ is a constant morphism with value in a torsion point $Q_0 \notin 2E(\mathbb{Q})$.*

Let S be a set of finite places of $\mathbb{Q}$ containing all places dividing $2ND$ such that $U = U_S U^S$ with $U_S \subset \prod_{v \in S} G(\mathbb{Q}_v)$ and U^S is a maximal open compact subgroup of $G(\mathbb{A}_f^S)$. For any $r \geqslant 1$, let Σ_r denote the set of primes $\ell \notin S$ satisfying:

$$\text{(i) } a_\ell \equiv 0 \bmod 2^{r+1}, \quad \text{(ii) } \ell \equiv 1 \bmod 4, \quad \text{(iii) } \sigma_{t_0}^K(\sqrt{\ell}) = \sqrt{\ell}.$$

Here $\sigma : \widehat{K}^\times / K^\times \to \mathrm{Gal}(K^{ab}/K)$ is the reciprocity law morphism in class field theory. Then for any integer $M = \ell_1 \cdots \ell_r$ with $\ell_1, \ldots, \ell_r \in \Sigma_r$,

$$\mathrm{rank}_{\mathbb{Z}} E^{(DM)}(\mathbb{Q}) = 1 = \mathrm{ord}_{s=1} L(E^{(DM)}, s) \quad \textit{and} \quad \mathrm{rank}_{\mathbb{Z}} E^{(M)}(\mathbb{Q}) = 0 = \mathrm{ord}_{s=1} L(E^{(M)}, s).$$

We prove this theorem by arguing the non-triviality of the Heegner points and applying the theorem of Kolyvagin and Gross-Zagier.

First, we give the construction of the Heegner point in our situation.

Denote H_M to be the ring class field of K with conductor M and let χ_M denote the character over K defining the extension $K(\sqrt{M})$.

Consider the CM point of conductor M,

$$P_M = [h_0, g(M)] \in X_U(H_M),$$

which is defined over H_M, the abelian extension over K such that

$$\mathrm{Gal}(H_M/K) \cong \widehat{K}^\times / K^\times (g(M)Ug(M)^{-1} \cap \widehat{K}^\times)$$

via the reciprocity law map in class field theory.

Let C be an odd integer killing the odd part of $E(H_0)_{\mathrm{tor}}$, and we define the Heegner point

$$y_M := C \cdot \sum_{\sigma \in \mathrm{Gal}(H_M/K)} f(P_M)^\sigma \chi_M(\sigma).$$

Denote $H_0 = K(\sqrt{\ell_1}, \dots, \sqrt{\ell_r})$. It is clear that H_0 is contained in H_M and the prime 2 is unramified over H_0. So we have

$$E(H_0)[2^\infty] = E(\mathbb{Q})[2].$$

The following theorem is a generalization of Lemma 2.8, from which Theorem 2.12 follows.

Theorem 2.13. *Let $E, K, M = \ell_1 \cdots \ell_r$ be as in Theorem 2.12. Then the point y_M has 2-index $r-1$ in $E(\mathbb{Q}(\sqrt{DM}))^-$. Moreover, $y_M = 2^r x$ for some $x \in E(H_0)$ with $\overline{x} + x = T \in E(\mathbb{Q})[2]$ being of order 2.*

Remark 2.14. In the case $r = 0$, the statement is understood as that $y \in E(K) \setminus 2E(K) + E(K)_{\mathrm{tor}}$ and $2y \in E(K)^-$ has 2-index 0 in $E(K)^-$. The case $r = 0$ has already been proved by Lemma 2.8.

Proof of Theorem 2.13. We use induction on the number s of primes $\ell \mid M$ which splits in K.

First, we consider the initial case with $s = 0$, i.e., all primes $\ell_1, \dots, \ell_r$ are inert in K. Note that it is Birch's lemma's case when $r = 0$ and we now assume that $r > 0$.

Recall that $H_0 = K(\sqrt{\ell_1}, \dots, \sqrt{\ell_r})$ and let $y_0 = C \cdot \mathrm{Tr}_{H_M/H_0} f(P_M)$. For each positive divisor d of M, let χ_d denote the character over K defining $K(\sqrt{d})$ and let

$$y_d := C \cdot \sum_{\sigma \in \mathrm{Gal}(H_M/K)} f(P_M)^\sigma \chi_d(\sigma).$$

For each positive divisor d of M with $d \neq M$, by the norm relation of Heegner points, we have that (noting that each a_ℓ is divisible by 2^{r+1}):

$$y_d = \Bigg(\prod_{\ell \mid M/d} a_\ell \Bigg) y_d^0 = 2^r b_d y_d^0,$$

where we denote the primitive point of conductor d by

$$y_d^0 := C \cdot \sum_{\sigma \in \mathrm{Gal}(H_d/K)} f(P_d)^\sigma \chi_d(\sigma),$$

and the integer b_d is defined by

$$b_d = 2^{-r} \prod_{\ell \mid M/d} a_\ell.$$

From the following computation,

$$\begin{aligned} \sum_{d \mid M} y_d =& \sum_{d \mid M} \sum_{t \in \mathrm{Gal}(H_M/K)} f(P)^t \chi_d(t) \\ =& \sum_{t \in \mathrm{Gal}(H_M/K)} \Bigg(\sum_{d \mid M} \chi_d(t) \Bigg) f(P)^t \\ =& 2^r y_0, \end{aligned}$$

we get the relation

$$\sum_{d\,|\,M} y_d = 2^r \cdot y_0.$$

Thus we can write y_M in the following form,

$$y_M = 2^r R, \quad \text{where } R := \Bigg(y_0 - \sum_{d\,|\,M, d\neq M} b_d y_d^0\Bigg),$$

which shows that 2-index of y is at least r in $E(H_0)$. Noting that $\sigma_{t_0}^K(\sqrt{\ell_i}) = \sqrt{\ell_i}$, i.e., $\sigma_{t_0}|_{H_0} = 1$, and that

$$[H_M : H_0] = [H : K] \cdot \prod_{i=1}^{r} \frac{\ell_i + 1}{2}$$

is an odd number by our assumption that $\ell_i \equiv 1 \bmod 4$ and $[H : K]$ is odd, we know that

$$T := \overline{R} + R = \overline{y}_0 + y_0 = [H_M : H_0] \cdot C \cdot Q_0 \in E(H_0)[2^\infty] = E(\mathbb{Q})[2]$$

is of order 2.

Consider the (injective) descent map

$$\delta : E(K(\sqrt{M}))/2^r E(K(\sqrt{M})) \to H^1(K(\sqrt{M}), E[2^r]),$$

and the inflation-restriction exact sequence

$$0 \to H^1(H_0/K(\sqrt{M}), E[2^r](H_0)) \to H^1(K(\sqrt{M}), E[2^r]) \to H^1(H_0, E[2^r]).$$

Note that $\delta(y_M)$ has image zero in $H^1(H_0, E[2^r])$ since $y_M = 2^r R$ with $R \in E(H_0)$. Thus

$$\delta(y_M) \in H^1(H_0/K(\sqrt{M}), E[2^r](H_0)),$$

which is killed by 2. It follows that $2y_M \in 2^r E(K(\sqrt{M}))$ and then

$$y_M = 2^{r-1} z + t,$$

for some $z \in E(K(\sqrt{M}))$ and $t \in E(\mathbb{Q})[2]$.

Noting the relation $y_M = 2^r R$ and the previous result, we also get

$$z = 2R + s$$

for some $s \in E(\mathbb{Q})[2]$.

We now claim that $z \in E(\mathbb{Q}(\sqrt{DM}))^-$, i.e., the 2-index of y_M in $E(\mathbb{Q}(\sqrt{DM}))^-$ is at least $r-1$.

Let $\sigma \in \mathrm{Gal}(K(\sqrt{M})/K)$ be the non-trivial element and still let σ denote its fixed lift to H_0. Then

$$0 = y_M + y_M^\sigma = 2^r(R + R^\sigma)$$

gives

$$R + R^\sigma \in E[2^r](H_0) = E(\mathbb{Q})[2],$$

and note the relation

$$z = 2R + s, \quad s \in E(\mathbb{Q})[2],$$

which implies that

$$z + z^\sigma = 0.$$

On the other hand, we have seen that

$$T := y_0 + \overline{y}_0 = [H_M : H_0] \cdot C \cdot Q_0$$

is of order 2. Then

$$z+\overline{z}=2(R+\overline{R})=2T=0.$$

Now, consider the biquadratic extension $K(\sqrt{M})=\mathbb{Q}(\sqrt{D},\sqrt{M})$ over $\mathbb{Q}$, and the relation

$$\overline{z}+z=0,\quad z+z^{\sigma}=0.$$

We get the result

$$z\in E(\mathbb{Q}(\sqrt{DM}))^{-}.$$

Therefore,

$$y_M\in 2^{r-1}E(\mathbb{Q}(\sqrt{DM}))^{-}+E(\mathbb{Q})[2]$$

has 2-index in $E(\mathbb{Q}(\sqrt{DM}))^{-}$ at least $r-1$.

Now, we show that the 2-index of y_M is exactly $r-1$, i.e., $y_M\notin 2^rE(\mathbb{Q}(\sqrt{DM}))^{-}+E(\mathbb{Q})_{\mathrm{tor}}$. Otherwise, suppose we have $y_M=2^rz+t$ for some $z\in E(\mathbb{Q}(\sqrt{DM}))^{-}$ and $t\in E(\mathbb{Q}(\sqrt{DM}))^{-}_{\mathrm{tor}}$. By $y_M=2^rR$, we have that $(z-R)\in E(\mathbb{Q})[2]$, and it follows that

$$0=(z+\overline{z})-(R+\overline{R})=-(y_0+\overline{y}_0),$$

which contradicts that $\overline{y}_0+y_0$ is of order 2.

Thus we complete the proof of the case where all primes $\ell\,|\,M$ are inert in K.

Now assume that the number s of the split prime factors of M is greater than 0. Write $M=M_+M_-$ with M_+ (resp. M_-) the product of prime factors of M split (resp. inert) in K. By Euler system property of the Heegner points, we know for each positive divisor d of M,

$$y_d=\Bigg(\prod_{\ell\,|\,M_-/(d,M_-)}a_\ell\cdot\prod_{\ell\,|\,M_+/(d,M_+)}(a_\ell-\mathrm{Fr}_{w_\ell}-\mathrm{Fr}_{\overline{w}_\ell})\Bigg)y_d^0,$$

where

$$y_d^0=C\cdot\sum_{\sigma\in\mathrm{Gal}(H_d/K)}f(P_d)^{\sigma}\chi_d(\sigma).$$

Considering the relation,

$$y_M+\sum_{1\leqslant d\,|\,M,d\neq M}y_d=2^ry_0,$$

we have that

$$y_M+\sum_{M_-|d|M,d\neq M}(\pm 2^{\mu(M/d)})y_d^0\equiv 2^ry_0\mod 2^{r+1}E(H_0)^{-},$$

where $E(H_0)^{-}$ is the subgroup of elements $P\in E(H_0)$ such that $\overline{P}+P=0$.

By induction, we know that each $y_d^0=2^{\mu(d)}x_d$ with $x_d\in E(H_0)$ such that $\overline{x}_d+x_d=T\in E(\mathbb{Q})[2]$ is of order 2. It follows that

$$y_M\equiv 2^r\Bigg(y_0-\sum_{M_-|d|M,d\neq M}(\pm x_d)\Bigg)\mod 2^{r+1}E(H_0)^{-}.$$

It is now clear that $y_M=2^rx_M$ for some $x_M\in E(H_0)$ with $\overline{x}_M+x_M=T\in E(H_0)_{\mathrm{tor}}$ being of even order. It follows the same as before by Kummer descent, and one can get $2y_M\in 2^rE(K(\sqrt{M}))$.

Thus we may write

$$y_M=2^{r-1}z+t$$

with $z\in E(K(\sqrt{M}))$ and $t\in E(\mathbb{Q})[2]$. It follows from $2^{r-1}z+t=2^rx_M$ that

$$(z-2x_M)\in E(H_0)[2^\infty]=E(\mathbb{Q})[2].$$

Writing explicitly $z=2x_M+s$, with $s\in E(\mathbb{Q})[2]$, we get $z+\overline{z}=0$.

Now, choose $\sigma \in \mathrm{Gal}(K(\sqrt{M})/K)$ to be the non-trivial element and lift this element to $\mathrm{Gal}(H_0/K)$. From the definition of y_M we get

$$2^r(x_M + x_M^\sigma) = y_M + y_M^\sigma = 0.$$

Thus

$$x_M + x_M^\sigma \in E(H_0)[2^r] = E(\mathbb{Q})[2].$$

From the relation $z = 2x_M + s$ we get

$$z + z^\sigma = 0.$$

It follows that $y_M \in E(\mathbb{Q}(\sqrt{DM}))^-$ has 2-index at least $r-1$.

Now, we show y_M has 2-index exactly equal to $r-1$. Suppose that the 2-index of y_M is no less than r. We may write $y_M = 2^r z_M + t$ with some $z_M \in E(\mathbb{Q}(\sqrt{DM}))^-$ and $t \in E(\mathbb{Q}(\sqrt{DM}))^-_{\mathrm{tor}}$. Then we have that $(z_M - x_M) \in E(\mathbb{Q})[2]$ and therefore $(\overline{x}_M + x_M) = (\overline{z}_M + z_M) = 0$, which contradicts $\overline{x}_M + x_M = T \neq 0$. □

3 Special value of L-function for rank zero twists of $X_0(49)$

In this section, we will prove a result on the estimate of special values of L-function for the rank zero twist of the elliptic curve $A = (X_0(49), [\infty])$. This result will be used in the final section to compare the height relation of the Heegner points.

First, we recall the explicit Waldspurger formula for the curve A, which is already proved in [5].

Theorem 3.1 (Explicit Waldspurger formula). *Let $A = (X_0(49), [\infty])$, K be an imaginary quadratic field with discriminant D, and χ an unramified quadratic character over K. Assume that $L(s, A, \chi)$ has global root number equal to $+1$ (thus 7 must be ramified in K and χ must be corresponding to $K(\sqrt{d})$ for some positive fundamental discriminant d dividing D). Let f be the Gross-Prasad test vector for (A, χ). Then we have*

$$\left| \sum_{t \in \widehat{K}^\times / K^\times \widehat{\mathcal{O}}_B^\times} f(t)\chi(t) \right|^2 = 2^{2+\delta} L^{(\mathrm{alg})}(A^{(d)}, 1) L^{(\mathrm{alg})}(A^{(D/d)}, 1),$$

where $\delta = 0$ if $K_7 \cong \mathbb{Q}_7(\sqrt{-7})$, and $\delta = 1$ if $K_7 \cong \mathbb{Q}_7(\sqrt{-35})$.

Now, using this formula we get the following proposition which is the main result of this section.

Proposition 3.2. *Let $R = q_1 \cdots q_r$ be a square-free integer with all prime factors $q_i \equiv 1 \bmod 4$ inert in $\mathbb{Q}(\sqrt{-7})$. Let $N = p_1 \cdots p_k$ $(k \geqslant 1)$ be a square-free integer with all prime factors p_j completely split in $\mathbb{Q}(A[4], \sqrt{R})$. Then for the elliptic curve $A = (X_0(49), [\infty])$, we have that* $\mathrm{ord}_2(L^{\mathrm{alg}}(A^{(R)}, 1)) = r - 1$, *and* $\mathrm{ord}_2(L^{\mathrm{alg}}(A^{(RN)}, 1)) \geqslant 2k + r + 1$.

We remark here that the first assertion in the proposition on two-adic valuation of L-value for the curve $A^{(R)}$ has been already done in [5, Theorem 5.7]. So in the following proof we only discuss the second assertion for the curve $A^{(RN)}$.

Proof of Proposition 3.2. The key idea for proving the proposition is similar to that in [5, Theorem 5.8]. But here we include all the details for completeness.

Keep the same notation as in [5] (note that we write R_+, N_+ for R, N here), take $K = \mathbb{Q}(\sqrt{-7RN})$. We may assume $r \geqslant 1$, since the case $r = 0$ is already treated in [5, Proposition 5.10].

We begin to treat the case $r = 1$, then the assumption under this case in the proposition for the p_i's is the same as those made in [5, Theorem 5.11]. Thus refering the proof there we get the assertion.

The difference in the argument in this proposition is that the assumption on p_i may not always give $\#(2\mathcal{A})$ an even number and this difference appears in the case of $r = 2$.

First we remark that in the case $r = 2$, analyzing the Rédei matrix, we can see that $\#(2\mathcal{A})$ is even. While for even $r \geqslant 4$'s case, we need not use the fact that $\#(2\mathcal{A})$ is an even number.

We prove the case of $r \geqslant 2$ with r even uniformly in the following. Noting $K_7 \cong \mathbb{Q}_7(\sqrt{-7})$, we choose the test vector f for $(A, \chi^{(RN)})$ according to [5, Theorem 5.3]. We use induction on $k+r$. Then we have

$$\sum_{1\leqslant d\,|\,RN,\ \mu((d,R))\ \text{even}} y_d = \sum_{1\leqslant d\,|\,RN} y_d = 2^{r+k} \sum_{t\in 2\mathcal{A}} f(t).$$

Noting that in this case, from [5, Lemma 5.6], we have $y_d = y_{n/d}$, and so the above summation can be rewritten as

$$\sum_{1\leqslant d\,|\,RN,\ \mu((d,R_+))\ \text{even},\ d\geqslant\sqrt{RN}} y_d = 2^{r+k-1} \sum_{t\in 2\mathcal{A}} f(t).$$

Analyze all the terms in the above formula except y_{RN}. By induction hypothesis,

$$y_s^2 = 4L^{(\text{alg})}(A^{(s)},1)L^{(\text{alg})}(A^{(\frac{R}{s}\cdot N_+)},1), \quad \forall\, s\,|\,R, \quad \text{even } \mu(s)$$

gives $\mathrm{ord}_2(y_s) \geqslant k + \frac{r}{2} + 1$.

Also we know that

$$y_{st}^2 = 4L^{(\text{alg})}(A^{(st)},1)L^{(\text{alg})}(A^{(\frac{R_+}{s}\cdot\frac{N}{t})},1), \quad \forall\, s\,|\,R, \quad \text{even } \mu(s), \quad 1\neq t\,|\,N, \quad st\neq NR$$

gives $\mathrm{ord}_2(y_{st}) \geqslant k + \frac{r}{2} + 2$.

Note also that

$$\mathrm{ord}_2\Bigg(2^{r+k-1}\sum_{t\in 2\mathcal{A}} f(t)\Bigg) \geqslant r+k-1$$

for all $r \geqslant 4$, and

$$\mathrm{ord}_2\Bigg(2^{r+k-1}\sum_{t\in 2\mathcal{A}} f(t)\Bigg) \geqslant r+k$$

for $r = 2$.

Putting all these facts together, we obtain

$$\mathrm{ord}_2(y_{N_+R_+}) \geqslant k + \frac{r}{2} + 1,$$

whence, using Waldspurger's formula in Theorem 3.1, we obtain

$$\mathrm{ord}_2(L^{(\text{alg})}(A^{(NR)},1)) \geqslant 2k + r + 1.$$

This completes the proof in this case.

While for the case of odd $r \geqslant 3$, we do not use the fact that $\#(2\mathcal{A})$ is an even number. Noting $K_7 \cong \mathbb{Q}_7(\sqrt{-35})$, we choose f to be the test vector for $(A, \chi^{(R_+N_+)})$ according to [5, Theorem 5.3], similar to the even case, by using induction method on $r+k$. We have

$$\sum_{1\leqslant d\,|\,R_+N_+,\,\text{odd }\ \mu((d,R_+))} y_d = \sum_{1\leqslant d\,|\,R_+N_+} y_d = 2^{r+k} \sum_{t\in 2\mathcal{A}} f(t).$$

We analyze all the terms except $y_{R_+N_+}$ as follows.

By induction hypothesis,

$$y_s^2 = 8L^{(\text{alg})}(A^{(s)},1)L^{(\text{alg})}(A^{(\frac{R_+}{s}\cdot N_+)},1), \quad \forall\, s\,|\,R_+, \quad \text{odd } \mu(s)$$

gives $\mathrm{ord}_2(y_s) \geqslant k + \frac{r+3}{2}$, while

$$y_{st}^2 = 8L^{(\text{alg})}(A^{(st)},1)L^{(\text{alg})}(A^{(\frac{R_+}{s}\cdot\frac{N_+}{t})},1), \quad \forall\, s\,|\,R_+, \quad \text{odd } \mu(s), \quad 1\neq t\,|\,N_+, \quad st\neq N_+R_+$$

gives $\mathrm{ord}_2(y_{st}) \geqslant k + \frac{r+5}{2}$.

Note also that $\mathrm{ord}_2(2^{r+k}\sum_{t\in 2\mathcal{A}} f(t)) \geqslant r+k$.

Putting these facts together, we obtain $\mathrm{ord}_2(y_{N_+R_+}) \geqslant k + \frac{r+3}{2}$, whence using the Waldspurger's formula in Theorem 3.1 gives

$$\mathrm{ord}_2(L^{(\text{alg})}(A^{(N_+R_+)},1)) \geqslant 2k + r + 1. \qquad \square$$

4 Rank one quadratic twist and BSD conjecture

In this section, we will prove the main theorem concerning an infinite quadratic rank one twist family for the elliptic curve of conductor 49, which generalizes the result in [5].

First, we state the main theorem.

Theorem 4.1. *Let $A = (X_0(49), [\infty])$ and $M = -\ell_0 RN$ be a square-free integer, where $\ell_0 \equiv 3 \bmod 4$ is a prime not equal to 7 and is a non square modulo 7, R is a positive integer with all prime factors $\equiv 1 \bmod 4$ inert in $\mathbb{Q}(\sqrt{-7})$, and N is a positive integer with all prime factors splits completely in the field $\mathbb{Q}(A[4], \sqrt{R})$. Assume that*

$$K_N = \mathbb{Q}(\sqrt{-\ell_0 N})$$

has no ideal class of exact order 4. Then for the quadratic twist $A^{(M)}$ of A by the field $\mathbb{Q}(\sqrt{M})$, we have

$$\mathrm{ord}_{s=1} L(A^{(M)}, s) = 1 = \mathrm{rank}_{\mathbb{Z}} A^{(M)}(\mathbb{Q}),$$

and the Shafarevich-Tate group $Ш(A^{(M)}/\mathbb{Q})$ is finite of odd order. Moreover, the p-part of the full BSD conjecture holds for all primes $p \nmid 7M$.

We prove Theorem 4.1 via constructing the Heegner points, and show that the corresponding point is non-torsion.

Assume that $M = -\ell_0 RN$ is an integer in Theorem 4.1. Let H_R be the ring class field of K_N of conductor R and let $H_0 \subset H$ be the maximal exponential-2 sub-extension over K_N. It is clear that H_0 is generated over $\mathbb{Q}$ by $\sqrt{\ell^*}$, where ℓ runs all prime factors of M and

$$\ell^* = (-1)^{\frac{\ell-1}{2}} \ell \equiv 1 \bmod 4.$$

In particular, $K_N(\sqrt{R}) \subset H_0$.

Let $P \in A(H_R)$ be the CM point of conductor R, and let χ_R be the quadratic character of K_N defining the extension $K_N(\sqrt{R})$ over K_N. We define the Heegner point,

$$y_R = \sum_{\sigma \in \mathrm{Gal}(H_R/K_N)} P^\sigma \chi_R(\sigma) \in A(K_N(\sqrt{R})).$$

It is clear that Theorem 4.1 follows from the below theorem and together with an application of explicit Gross-Zagier formula in [4], we can verify the two-part BSD conjecture for $E^{(M)}$.

Theorem 4.2. *Let $M = -\ell_0 RN$ be a negative square-free integer and assume that*

(1) *$\ell_0 \neq 7$ is a prime $\equiv 3 \bmod 4$, which is a non square modulo 7,*

(2) *R is a product of r primes congruent to 1 modulo 4, which is inert in $\mathbb{Q}(\sqrt{-7})$,*

(3) *N is a product of k primes complete split in $\mathbb{Q}(A[4])$ and $\mathbb{Q}(\sqrt{R})$.*

Let A be the elliptic curve as in Theorem 4.1. Then the Heegner point y_R satisfies

$$y_R \in 2^{k+r-1} A(\mathbb{Q}(\sqrt{M}))^- + A(\mathbb{Q}(\sqrt{M}))_{\mathrm{tor}}.$$

Note that when $k = r = 0$, the above statement is understood as $2y_R \in A(\mathbb{Q}(\sqrt{M}))^-$.

Moreover, if $K_N = \mathbb{Q}(\sqrt{-\ell_0 N})$ has no order 4 ideal class, then

$$y_R \notin 2^{k+r} A(\mathbb{Q}(\sqrt{M}))^- + A(\mathbb{Q}(\sqrt{M}))_{\mathrm{tor}}.$$

Remark 4.3. The conditions here generalize [5, Theorem 6.1] in two sides. First we remove the conditions on the prime factor of R that should be inert in $\mathbb{Q}(\sqrt{-\ell_0})$, second we generalize the condition for the p_i's, and just need them split completely in $\mathbb{Q}(A[4], \sqrt{R})$.

Proof of Theorem 4.2. The proof of the theorem combines the generalized Birch lemma, the Euler system properties for the inert and split prime, the explicit Gross-Zagier formula and Tian's induction argument on Heegner points.

Keeping the same notation as above, we denote s to be the number of primes dividing R which splits in K_N. We use induction on s, and in each s's argument we argue by induction on k, the number of primes divide N.

We begin to deal with the case $s=0$, and induct on the number k of the primes dividing N. The case of $k=0$ has been already done according to Theorem 2.12. Now we treat the case $k \geqslant 1$. For any $d \,|\, RN$, denote the character χ_d to correspond the quadratic extension $K_N(\sqrt{d})$ of K_N, and define the Heegner point by

$$y_d := \sum_{\sigma_t \in \mathrm{Gal}(H_R/K_N)} P^{\sigma_t} \chi_d(\sigma_t).$$

By considering the Galois action of the nontrivial element of the group $\mathrm{Gal}(K_N(\sqrt{d})/K_N)$ and complex conjugation on the point y_d, we know that this point belongs to $A(\mathbb{Q}(\sqrt{-l_0Nd}))^-$. Noting the property of Euler system for the inert primes, we know when $R \nmid d$, i.e., there exists a prime $q \mid R$ such that $q \nmid D$, then $a_q = 0$, and

$$y_d = \sum_{\sigma \in \mathrm{Gal}(H_{R/q}/K_N)} \chi_D(\sigma)(\mathrm{Tr}_{H_R/H_{R/q}} P_R)^\sigma = \sum_{\sigma \in \mathrm{Gal}(H_{R/q}/K_N)} \chi_D(\sigma)(a_q P_{R/q})^\sigma = 0.$$

Define $y_0 := \mathrm{Tr}_{H_R/H_0} P$, and then by the observation

$$\sum_{d \,|\, RN} \chi_d(\sigma_t) = 2^{k+r} \delta_{\sigma_t \in \mathrm{Gal}(H_R/H_0)}.$$

Here,

$$\delta_{\sigma_t \in \mathrm{Gal}(H_R/H_0)} = \begin{cases} 1, & \text{if } \sigma_t \in \mathrm{Gal}(H_R/H_0), \\ 0, & \text{otherwise.} \end{cases}$$

We get

$$\sum_{R|d|RN} y_d = \sum_{d \,|\, RN} y_d = 2^{k+r} y_0.$$

Write the above formula in the following form,

$$y_R = 2^{k+r} y_0 - \sum_{1<d \,|\, N} y_{dR}. \tag{4.1}$$

By the earlier observation, we know

$$y_{dR} \in A(\mathbb{Q}(\sqrt{-l_0 R N_d}))^-, \quad \text{where } N_d = \frac{N}{d}.$$

Similarly, let $K_0 = \mathbb{Q}(\sqrt{-\ell_0 N_d})$ and construct the analogous point y, denoted by y^0_{dR}. By the theorem of Kolyvagin, we know that either y^0_{dR} is torsion point, or the $\mathbb{Q}$-vector space $A(\mathbb{Q}(\sqrt{-\ell_0 R N_d}))^- \otimes_{\mathbb{Z}} \mathbb{Q}$ is of one dimension, and we can do the ratio, by explicit Gross-Zagier formula theorem in [4]:

$$[y_{dR} : y^0_{dR}]^2 = \frac{\widehat{h}_K(y_{dR})}{\widehat{h}_{K_0}(y^0_{dR})} = \frac{L^{(\mathrm{alg})}(1, A^{(dR)})}{L^{(\mathrm{alg})}(1, A^{(R)})}.$$

By induction hypothesis (with respect to k's induction), we know that

$$y_{dR} = 2^{k+r} y'_{dR}.$$

Using this relation and (4.1), we know that

$$y_R = 2^{k+r}\left(y_0 - \sum_{1<d \,|\, N} y'_{dR}\right) =: 2^{k+r} x_R. \tag{4.2}$$

We remark here that when $\mathbb{Q}(\sqrt{-l_0N})$ has no ideal class of order 4, we will get that the degree $[H_R : H_0]$ is odd and

$$x_R + \overline{x}_R = y_0 + \overline{y}_0 = T,$$

where T is the nontrivial order 2 point on A over $\mathbb{Q}$.

Noting (4.2), we know $x_R \in A(H_0)$. So from the following two exact sequences,

$$0 \to \frac{A(\mathbb{Q}(\sqrt{-l_0NR}))}{2^{k+r}A(\mathbb{Q}(\sqrt{-l_0NR}))} \to H^1(\mathbb{Q}(\sqrt{-l_0NR}), A[2^{k+r}])$$

and

$$0 \to H^1(\mathrm{Gal}(H_0/\mathbb{Q}(\sqrt{-l_0NR})), A[2]) \to H^1(\mathbb{Q}(\sqrt{-l_0NR}), A[2^{k+r}]) \to H^1(H_0, A[2^{k+r}])$$

we know that the image of y_R in $H^1(H_0, A[2^{k+r}])$ is zero, so

$$2y_R \in 2^{k+r}A(\mathbb{Q}(\sqrt{-l_0NR}))^-.$$

Thus,

$$y_R \in 2^{k+r-1}A(\mathbb{Q}(\sqrt{-l_0NR}))^- + A(\mathbb{Q}(\sqrt{-l_0NR}))_{\mathrm{tor}}.$$

Now, we claim that if $\mathbb{Q}(\sqrt{-l_0N})$ has no ideal class of order 4, then

$$y_R \notin 2^{k+r}A(\mathbb{Q}(\sqrt{-l_0NR}))^- + A(\mathbb{Q}(\sqrt{-l_0NR}))_{\mathrm{tor}}$$

otherwise, we have

$$y_R = 2^{k+r}z_R + T$$

with $z_R \in A(\mathbb{Q}(\sqrt{-l_0NR}))^-, T \in A(\mathbb{Q}(\sqrt{-l_0NR}))_{\mathrm{tor}} = A(\mathbb{Q})[2]$.

Thus from the formula (4.2), we know

$$z_R = y_0 - \sum_{1<d\,|\,N} y^0_{dR} + t, \quad t \in A(\mathbb{Q})[2],$$

so from the degree $[H_R : H_0]$ being odd and this formula, we know that

$$z_R + \overline{z}_R = y_0 + \overline{y}_0 = T$$

with T the nontrivial two torsion point in $A(\mathbb{Q})$.

But our assumption on z_R gives

$$z_R + \overline{z}_R = 0.$$

This contradiction gives our claim.

Now we prove the case $s = 0$, while for the general $s > 0$ case, we also use induction on k, the number of prime divisors of N. The initial $k = 0$'s case has been already done by Theorem 2.12. Now for the case of $k > 0$, first we know that

$$\sum_{d\,|\,RN} y_d = 2^{k+r}y_0.$$

With the same reason as above, we know $y_d \neq 0$ only if $R_- \mid d$, here R_- denotes the products of the prime factors of R which are inert in K.

Write the above formula as follows,

$$y_R + \sum_{R_-|d|R\ d\neq R} y_d + \sum_{R_-|d|RN\ \mu(d,N)\geqslant 1} y_d = 2^{k+r}y_0. \tag{4.3}$$

We call the above formula's second term the type I and the third term the type II. We will treat them separately.

For the type I terms, by the Euler system properties for the split primes, we have

$$y_d = \sum_{\sigma\in \mathrm{Gal}(H_d/K_N)} (\mathrm{Tr}_{H_R/H_d} P)^{\sigma}\chi_d(\sigma) = 2^{\mu(R/d)} y_d',$$

where y_d' is just the corresponding Heegner point constructed from H_d (which is just up to the plus or minus sign).

Notice that the split prime divisor of d is less than s, so by induction hypothesis with respect to s, we know

$$y_d' = 2^{r-\mu(R/d)+k} Y_d,$$

where

$$Y_d \in A(H_0).$$

So we have $y_d = 2^{k+r}Y_d$ and noticing that when the field K_N has no ideal class of order four, by the argument in the induction hypothesis with respect to s, we have

$$Y_d + \overline{Y}_d = T \quad \text{for all} \quad R_-|d|R \quad \text{with} \quad d \neq R.$$

For the type II terms, write $y_d = y_{st}$, with $s \,|\, R, 1 < t \,|\, N$. Similar to that before, we know

$$y_{st} \in A(\mathbb{Q}(\sqrt{-l_0 s N_t}))^- \quad \text{with} \quad N_t = \frac{N}{t}.$$

Let $K_0 = \mathbb{Q}(\sqrt{-l_0 N_t})$ and construct the analogous point y, denoted by y_{st}^0. By the theorem of Kolyvagin, we know that either y_{st}^0 is a torsion point, or the $\mathbb{Q}$-vector space $A(\mathbb{Q}(\sqrt{-l_0 s N_t}))^- \otimes_{\mathbb{Z}} \mathbb{Q}$ is one-dimensional, and we can do the ratio, by explicit Gross-Zagier formula in [4]:

$$[y_{st} : y_{st}^0]^2 = \frac{\widehat{h}_K(y_{st})}{\widehat{h}_{K_0}(y_{st}^0)} = \frac{L^{(\mathrm{alg})}(1, A^{(st)})}{L^{(\mathrm{alg})}(1, A^{(s)})}.$$

Using the induction hypothesis both with respect to s and k, we know

$$y_{st} = 2^{k+r} y_{st}' \quad \text{with} \quad y_{st}' \in A(\mathbb{Q}(\sqrt{-l_0 s N_t}))^-.$$

Thus from (4.3), we know

$$y_R = 2^{k+r} Z_R \quad \text{with} \quad Z_R \in A(H_0).$$

Using the same cohomology argument as the case $s = 0$, we get

$$2y_R \in 2^{k+r} A(\mathbb{Q}(\sqrt{-l_0 NR}))^-,$$

equivalently,

$$y_R \in 2^{k+r-1} A(\mathbb{Q}(\sqrt{-l_0 NR}))^- + A(\mathbb{Q}(\sqrt{-l_0 NR}))_{\mathrm{tor}}.$$

Now, assume the field K_N has no ideal class of order four. Then we claim that

$$y_R \notin 2^{k+r} A(\mathbb{Q}(\sqrt{-l_0 NR}))^- + A(\mathbb{Q}(\sqrt{-l_0 NR}))_{\mathrm{tor}}.$$

Otherwise, suppose we have

$$y_R = 2^{k+r} z_R + t,$$

with $z_R \in A(\mathbb{Q}(\sqrt{-l_0 NR}))^-, t \in A(\mathbb{Q}(\sqrt{-l_0 NR}))_{\mathrm{tor}} = A(\mathbb{Q})[2]$. Similarly to the case $s = 0$, we get

$$z_R = y_0 - \sum_{\text{type I}} Y_d - \sum_{\text{typeII}} y_d' + s, \quad s \in A(\mathbb{Q})[2].$$

So from the number of the type I terms in the summation being odd, we get

$$z_R + \overline{z}_R = T$$

contradicting our choice of z_R. This gives the assertion for k, moreover the assertion for s. Now the theorem is proved. □

Now, applying the explicit L-value formula in [4], we give the verification of the two-part BSD conjecture for the above rank one quadratic twist families of A.

Proof of Theorem 4.1. Consider the curve A, which is given by the equation

$$y^2 = x^3 + 21x^2 + 112x.$$

From the Tamagawa numbers and periods of their quadratic twists result in [5, Propositions 3.10 and 3.12], first we know that elliptic curve $A^{(R)}$ has Mordell-Weil rank 0 and the full BSD holds for $A^{(R)}$, i.e.,

$$L(1, A^{(R)})/\Omega^{(R)} = 2^{r-1}\#\text{Ш}(A^{(R)}/\mathbb{Q}).$$

By the theorem of Kolyvagin and Gross-Zagier, we know that

$$\mathrm{ord}_{s=1}L(A^{(M)}, s) = 1 = \mathrm{rank}_{\mathbb{Z}}A^{(M)}(\mathbb{Q})$$

and the full BSD for $A^{(M)}$ becomes

$$L'(1, A^{(M)})/\Omega^{(M)} \overset{?}{=} 2^{2k+r} \cdot R(A^{(M)}) \cdot \#\text{Ш}(A^{(M)}/\mathbb{Q}).$$

The explicit Gross-Zagier formula for $K_N = \mathbb{Q}(\sqrt{-\ell_0 N})$ and $\chi = \chi_R$ quadratic character of $\mathrm{Gal}(H_R/K_N)$ defining $K_N(\sqrt{R})$ is

$$L'(1, A, \chi_R) = \frac{8\pi^2(\phi, \phi)_{\Gamma_0(N)}}{\sqrt{\ell_0 N R^2}} \cdot (2\widehat{h}_{\mathbb{Q}}(y_R)).$$

Note that

$$\Omega^{(R)}\Omega^{(M)} = \frac{8\pi^2(\phi, \phi)_{\Gamma_0(N)}}{\sqrt{\ell_0 N R^2}},$$

thus the BSD conjecture for $A^{(M)}$ is reduced to

$$[A^{(M)}(\mathbb{Q})/A^{(M)}(\mathbb{Q})_{\mathrm{tor}} : \mathbb{Z}y_M]^2 \overset{?}{=} 2^{2(k+r-1)} \cdot \#\text{Ш}(A^{(M)}/\mathbb{Q}) \cdot \#\text{Ш}(A^{(R)}/\mathbb{Q}). \qquad (*)$$

It follows from Kolyvagin's work that the right-hand side is finite. For any prime $\ell \nmid 14M$, the ℓ-part of BSD follows from the work of Perrion-Riou [13] and Kobayashi [9].

Now, we show the 2-part of the BSD conjecture for $A^{(M)}$. It follows from Theorem 4.2 that the 2-part of the left-hand side of $(*)$ is $2(k + r - 1)$. It follows from the 2-descent computation, for example see [5, Section 3], that

$$\dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(A^{(M)}/\mathbb{Q})/A^{(M)}[2](\mathbb{Q}) = 1 \quad \text{and} \quad \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(A^{(R)}/\mathbb{Q})/A^{(R)}[2](\mathbb{Q}) = 0.$$

Thus $\#\text{Ш}(A^{(M)}/\mathbb{Q})\#\text{Ш}(A^{(R)}/\mathbb{Q})$ is an odd integer and thus the 2-part of $(*)$ holds. □

Acknowledgements The authors thank Professor John Coates and Professor Ye Tian for encouragement and helpful advices.

References

1 Birch B. Elliptic curves and modular functions. Symp Math, 1970, 4: 27–32

2 Birch B, Swinnerton-Dyer P. Notes on elliptic curves (II). J Reine Angew Math, 1965, 218: 79–108

3 Cai L, Chen Y, Liu Y. Euler system of Gross points and quadratic twist of elliptic curves. ArXiv:1601.04415, 2016

4 Cai L, Shu J, Tian Y. Explicit Gross-Zagier and Waldspurger formulae. Algebra Number Theory, 2014, 8: 2523–2572

5 Coates J, Li Y, Tian Y, et al. Quadratic twists of elliptic curves. Proc Lond Math Soc (3), 2015, 110: 357–394

6 Gonzalez-Aviles C. On the conjecture of Birch and Swinnerton-Dyer. Trans Amer Math Soc, 1997, 349: 4181–4200

7 Gross B. Local orders, root numbers, and modular curves. Amer J Math, 1988, 110: 1153–1182

8 Heegner K. Diophantische analysis und modulfunktionen. Math Z, 1952, 56: 227–253

9 Kobayshi S. The p-adic Gross-Zagier formula for elliptic curves at supersingular primes. Invent Math, 2013, 191: 527–629

10 Kolyvagain V. Finiteness of $E(\mathbb{Q})$ and $Ш(E,\mathbb{Q})$ for a subclass of Weil curves (in Russian). Izv Akad Nauk SSSR Ser Mat, 1988, 52: 522–540

11 Kolyvagain V. Euler system. In: The Grothendieck Festschrift II. Progress in Mathematics, vol. 87. Boston: Birkhauser, 1990, 435–483

12 Nekovář J. The Euler system method for CM points on Shimura curves. In: L-functions and Galois Representations. LMS Lecture Note Series, vol. 320. Cambridge: Cambridge University Press, 2007, 471–547

13 Perrin-Riou B. Points de Heegner et dérivées de fonctions L_p-adiques. Invent Math, 1987, 89: 455–510

14 Prasad D. Some applications of seesaw duality to braching laws. Math Ann, 1996, 304: 1–20

15 Tian Y. Congruent numbers with many prime factors. Proc Nat Acad Sci India Sect A, 2012, 109: 21256–21258

16 Tian Y. Congruent numbers and Heegner points. Cambridge J Math, 2014, 2: 117–161

17 Tian Y, Yuan X, Zhang S. Genus periods, genus points, and congruent number problem. ArXiv:1411.4728, 2014