Journal of Comprehensive Pure and Applied Mathematics

On Twists of A Family of Elliptic Curves and Their $L-$Function

Derong Qiu

School of Mathematical Sciences, Capital Normal University,
Beijing 100048, P.R.China

Article Details

Article Type: Research Article

Received date: 25^{th} August, 2025

Accepted date: 17^{th} December, 2025

Published date: 23^{rd} December, 2025

***Corresponding Author**: Derong Qiu, School of Mathematical Sciences, Capital Normal University, Beijing 100048, P.R.China.

Citation: Qiu, D. (2025). On Twists of A Family of Elliptic Curves and Their $L-$Function. *J Comp Pure Appl Math*, **3**(2):1-32. Doi: https://doi.org/10.33790/cpam1100122.

Copyright: 2025, This is an open-access article distributed under the terms of the Creative Commons Attribution License 4.0,, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract

Let E be an elliptic curve defined over a number field, the conjecture of Birch and Swinnerton-Dyer (BSD, for short) asserts a deep relation between the group $E(K)$ of rational points and the $L-$function $L(E/K, s)$ of E at $s = 1$. Very few explicit results about $E(K)$ and $L(1)$ are known, even no general method is known to determine $L(1)$ vanishing or not for a given elliptic curve. In this paper, we study some quantities related to BSD of a special class of elliptic curves, more precisely, we study the arithmetic of quadratic twists of elliptic curves $y^2 = x(x+\varepsilon p)(x+\varepsilon q)$ and their $L-$function. Based on some classical works, especially those of Greenberg, Kramer-Tunnell, Kato-Rohrlich, Manin and Mazur, under some conditions, we obtain results about the vanishing of the value at $s = 1$ of the L-function, and explicitly determine the following quantities: the norm index $\delta(E, \mathbb{Q}, K)$, the root numbers, the set of anomalous prime numbers, a few prime numbers at which the image of Galois representation are surjective. We also study the relation between the ranks of the Mordell-Weil groups, Selmer groups and Shafarevich-Tate groups, and the structure about the $l^\infty-$Selmer groups and the Mordell-Weil groups over $\mathbb{Z}_l-$extension via Iwasawa theory. These results provide some useful evidence toward verifying the BSD for a family of elliptic curves.

Keywords: Elliptic curve, $L-$function, quadratic twist, Selmer group, Shafarevich-Tate group, root number, local norm index, Iwasawa theory, BSD conjecture

2010 Mathematics Subject Classification: 11G05 (primary), 14H52, 14G05, 14G10 (Secondary).

1 Introduction

Let E be an elliptic curve over a number field K, and $L(E/K, s)$ be the $L-$function of E over K. By Mordell-Weil theorem (see, e.g. [Sil1]), the set $E(K)$ of $K-$rational points of E is a finitely generated abelian group. Hence

$$E(K) \simeq \mathbb{Z}^r \bigoplus E(K)_{\text{tors}},$$

where $r = \text{rank}(E(K)) \geq 0$ is the rank of E over K, and $E(K)_{\text{tors}}$ is the torsion subgroup of $E(K)$.

Conjecture 1.1 (see [Sil1]). The $L-$function $L(E/K, s)$ of E over K has an analytic continuation to the entire complex plane, and satisfies a functional equation relating the values at s and $2 - s$.
This conjecture was proved when $K = \mathbb{Q}$ (see [BCDT], [TW], [Wi]).
The conjecture of Birch and Swinnerton-Dyer (BSD, for short) for elliptic curves states that

Conjecture 1.2 (Birch and Swinnerton-Dyer conjecture, see [Sil1]).
(1) The rank of $E(K)$ equals the order of vanishing of $L(E/K, s)$ at $s = 1$.
(2)

$$\lim_{s \to 1} \frac{L(E/K, s)}{(s-1)^r} = \frac{\Omega \cdot \sharp\, Ш(E/K) \cdot R(E/K) \cdot \prod_{v|\mathcal{N}} c_v(E)}{\sharp E(K)^2_{\text{tors}}},$$

where $r = \text{rank} E(K), \Omega =$ the real period, $E(K)_{\text{tors}}$ is the torsion subgroup of $E(K)$, $R(E/K)$ is the regulator of $E(K)/E(K)_{\text{tors}}, \mathcal{N}$ is the conductor of $E/K, c_v(E) =$

$[E(K_v) : E_0(K_v)]$ is the Tamagawa number of E at the place v, Ш (E/K) is the Shafarevich-Tate group of E over K, which is conjectured to be a finite group.

In the literature, much important progress has been made about the BSD conjecture. For example, for elliptic curves over the rational number field $\mathbb{Q}$, let $r_{an}(E/\mathbb{Q})$ denote the order of vanishing of $L(E/\mathbb{Q}, s)$ at $s = 1$. Then one current state of the BSD conjecture is expressed by the result:

Theorem 1.3 (Gross-Zagier, Kolyvagin, etc., see [Kol3]). The equality $\text{rank}E(\mathbb{Q}) = r_{an}(E/\mathbb{Q})$ holds and $\sharp$ Ш$(E/\mathbb{Q})$ is finite if $r_{an}(E/\mathbb{Q}) \leq 1$.
Yet, at present, to explicitly determine the arithmetic quantities such as $E(K)$ and the order of $L(E/K, s)$ at $s = 1$ are generally not easy, even for the question about determining whether the value $L(E/K, 1)$ vanishing or not.
In this paper, we will study explicitly $L(1)$ and some related arithmetic quantities about twists of a family of elliptic curves E over the rational number field $\mathbb{Q}$, from which, for example, we obtain that $L(E_d/\mathbb{Q}, 1) = 0$ for many quadratic twists E_d of E. More precisely, we consider the elliptic curves

$$E = E^{\varepsilon} : \ y^2 = x(x + \varepsilon p)(x + \varepsilon q), \quad (\varepsilon = \pm 1), \tag{1.1}$$

and their quadratic $D-$twist

$$E_D = E_D^{\varepsilon} : \ y^2 = x(x + \varepsilon pD)(x + \varepsilon qD), \tag{1.2}$$

where p and q are odd prime numbers with $q - p = 2$, and $D = D_1 \cdots D_n$ is a square-free integer with distinct odd prime numbers $D_1, \cdots, D_n$ satisfying $(pq, D) = 1$. When $D = 1, E_1 = E$, and for $\varepsilon = 1$ (resp. -1), we sometimes write $E^{\varepsilon} = E^+$ (resp. E^-). By Tate's algorithm (see [Ta], [Sil2]), the discriminant, $j-$invariant and conductor of $E_D/\mathbb{Q}$ are obtained as follows, respectively

$$\Delta = 64p^2q^2D^6, \ j = \frac{64(p^2 + 2q)^3}{p^2q^2}, \ N_{E_D} = 2^5pqD^2. \tag{1.3}$$

So the equation (1.2) above is a global minimal Weierstrass equation for E_D over the rational number field $\mathbb{Q}$. Moreover, $E_D/\mathbb{Q}$ has additive reduction at $2, D_1, \cdots, D_n$, has multiplicative reduction at p, q, and has good reduction at other finite places.
In the following, we study the arithmetic of these elliptic curves. The following quantities are explicitly determined: the norm index $\delta(E, \mathbb{Q}, K)$ (see Theorem 3.3),

the root numbers (see Theorem 5.3), the set of anomalous prime numbers (see Proposition 2.4), a few prime numbers at which the image of Galois representation are surjective (see Proposition 2.7). The relation between the ranks of the Mordell-Weil groups, Selmer groups and Shafarevich-Tate groups, and the structure about the $l^\infty-$Selmer groups and the Mordell-Weil groups over $\mathbb{Z}_l-$extension via Iwasawa theory are studied (see Propositions 3.1, 4.1, 4.2, and Theorems 3.4, 3.7, 3.8, 4.3, 4.4). On $L(1)$, one of our main result is as follows

Theorem 1.4 (see Theorem 5.5 below) Let $E = E^\varepsilon$ be the elliptic curve in (1.1) and let $K = \mathbb{Q}(\sqrt{\mu D})$ be the quadratic number field with D in (1.2) and $\mu = \pm 1$. We assume that $D \equiv \mu \pmod 4$. Let $L(E/\mathbb{Q}, s) = \Sigma_{n=1}^\infty a_1(n) n^{-s}$ be the $L-$function as above. Let $E_{\mu D}/\mathbb{Q}$ be the quadratic $(\mu D)-$twist of $E/\mathbb{Q}$, and χ_K be the quadratic Dirichlet character associated to K.

(1) Assume one of the following two hypotheses holds:

(a) $\varepsilon = 1$ and $p \equiv 5, 7 \pmod 8$;

(b) $\varepsilon = -1$ and $p \equiv 3, 5 \pmod 8$.

Then $L(E/\mathbb{Q}, 1) = 2\Sigma_{n=1}^\infty \frac{a_1(n)}{n} e^{-n\pi/2\sqrt{2pq}}$.

further, for all integer $r \geq 0$,

$$L^{(r)}(E/\mathbb{Q}, 1) = 2\pi \Sigma_{n=1}^\infty a_1(n) \int_{1/4\sqrt{2pq}}^\infty [\log^r t + (-1)^r \log^r(2^5 pqt)] e^{-2n\pi t} dt. \text{ also,}$$

$$L(E_{\mu D}/\mathbb{Q}, 1) = (1 + \chi_K(-2pq)) \cdot \Sigma_{n=1}^\infty \frac{a_1(n)}{n} \chi_K(n) \cdot e^{-n\pi/2D\sqrt{2pq}},$$

In particular, if $\chi_K(-2pq) = -1$, then $L(E_{\mu D}/\mathbb{Q}, 1) = 0$.

(2) Assume one of the following two hypotheses holds:

(a′) $\varepsilon = 1$ and $p \equiv 1, 3 \pmod 8$;

(b′) $\varepsilon = -1$ and $p \equiv 1, 7 \pmod 8$.

Then $L(E/\mathbb{Q}, 1) = 0$,

further, for all integer $r \geq 0$,

$$L^{(r)}(E/\mathbb{Q}, 1) = 2\pi \Sigma_{n=1}^\infty a_1(n) \int_{1/4\sqrt{2pq}}^\infty [\log^r t + (-1)^{r+1} \log^r(2^5 pqt)] e^{-2n\pi t} dt. \text{ also,}$$

$$L(E_{\mu D}/\mathbb{Q}, 1) = (1 - \chi_K(-2pq)) \cdot \Sigma_{n=1}^\infty \frac{a_1(n)}{n} \chi_K(n) \cdot e^{-n\pi/2D\sqrt{2pq}}.$$

In particular, if $\chi_K(-2pq) = 1$, then $L(E_{\mu D}/\mathbb{Q}, 1) = 0$.

(For some concrete example on $L(1)$, see Example 5.6 below).

These results, together with some former results about Mordell-Weil groups and Selmer groups as in [QZ1] and [LQ], provide some useful evidence toward verifying the BSD for a family of elliptic curves, which we will discuss in a separate paper.

Organisation of the paper. Section 2 includes some basic facts on reduction from Tate's algorithm, and some results on anomalous prime, ramification and Galois representation deduced from the works of Mazur, Bahargava-Skinner-Zhang and Serre. In Section 3, by using Kramer's method and Kramer-Tunnell' formula, and the former results in [Q1], [QZ1], we compute the norm index, Tamagawa number, Selmer group, rank, and some congruences between rank and Shafarevich-Tate group. In Section 4, following mainly the works of Mazur, Greenberg and Kato-Rohrlich, we study the structure about the $l^\infty-$Selmer groups and the Mordell-Weil groups over $\mathbb{Z}_l-$extension via Iwasawa theory. Finally, in Section 5, by results of Rohrlich, we compute the root numbers, and by using a formula of Manin on $L(1)$, we obtain some results on the vanishing of the value at $s = 1$ of the L-function.

2 Reduction, ramification and Galois representation

In the following, unless otherwise stated, every conclusion for the elliptic curves E_D in (1.2) also holds for $E_1 = E$ in (1.1) when take $D = 1$. For a prime number l and an integer m, $(\frac{m}{l})$ is the usual Legendre quadratic residue symbol.

Lemma 2.1 Let $E_D/\mathbb{Q}$ be the elliptic curve in (1.2) above.
(1) At each prime $l \mid N_{E_D}$, the Kodaira type is as follows:
III for $l = 2$; I_2 for $l = p$ or q; and I_0^* for $l = D_1, \cdots, D_n$, respectively.
The Tamagawa number c_l is as follows:
$c_l = 2$ for $l = 2, p, q$; and $c_l = 4$ for $l = D_1, \cdots, D_n$.
(2) E_D has split multiplicative reduction at p if and only if $(\frac{2\varepsilon D}{p}) = 1$.
(3) E_D has split multiplicative reduction at q if and only if $(\frac{-2\varepsilon D}{q}) = 1$.
(4) Let l be a prime number such that $l \nmid 2pqD$. Then E_D has good supersingular reduction at l if and only if $\sum_{m=0}^{(l-1)/2} \begin{pmatrix} \frac{l-1}{2} \\ m \end{pmatrix}^2 p^m q^{\frac{l-1}{2}-m} \equiv 0 \pmod{l}$.
(5) The torsion subgroup $E_D(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and for $D = 1$, we have $E(F)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for any quadratic number field F.

(6) Assume $3 \nmid pqD$. Let F be a number field, and let $\mathfrak{p}$ be a prime ideal of F lying over 3, let $e = e(\mathfrak{p}/3)$ and $f = f(\mathfrak{p}/3)$ be the ramification index and residue degree, respectively. Then we have

(6a) if $e(\mathfrak{p}/3) = f(\mathfrak{p}/3) = 1$, then $E_D(F)_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;

(6b) if $f(\mathfrak{p}/3) = 1$ and E_D has additive reduction at some finite places of F lying over 2, then $E_D(F)_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$;

(6c) if $f(\mathfrak{p}/3) = 1$, then $E_D(F)_{\mathrm{tors}}/E_D(F)[3^\infty] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where $E_D(F)[3^\infty]$ denotes the $3-$primary component of $E_D(F)_{\mathrm{tors}}$;

(6d) If E_D has an additive reduction at some finite places of F lying over 2, then $\sharp E_D(F)_{\mathrm{tors}} = 2^m$ or $2^m \cdot 3$ for some $m \in \mathbb{Z}_{\geq 0}$.

Proof. (1) is a consequence of direct calculation by the Algorithm of [Ta]; (2), (3) and (4) are easily obtained (see [Sil1] for the methods); (5) follows from Lemma 2 and Lemma 4 of [QZ2]; (6) is similar to the Prop.1 in [QZ1, p.1374]. □

Particularly, by (2) and (3) of Lemma 2.1, one can easily see that, E^+ has split multiplicative reduction at both p and q if $p \equiv 1, 7 \pmod 8$, and has non-split multiplicative reduction at both p and q if $p \equiv 3, 5 \pmod 8$; Also, E^- has split multiplicative reduction at p and non-split multiplicative reduction at q if $p \equiv 1, 3 \pmod 8$, and has non-split multiplicative reduction at p and split multiplicative reduction at q if $p \equiv 5, 7 \pmod 8$.

Corollary 2.2. For the elliptic curves $E_D/\mathbb{Q}$ in (1.2) above,

(1) E_D has good supersingular reduction at 3 if $3 \nmid pqD$;

(2) E_D has good ordinary reduction at 5 if $5 \nmid pqD$;

(3) E_D has good ordinary reduction at 7 if $7 \nmid pqD$ and $p \equiv 1, 4 \pmod 7$;

(4) E_D has good supersingular reduction at 7 if $7 \nmid pqD$ and $p \equiv 2, 3, 6 \pmod 7$.

Proof. Follows easily from the above Lemma 2.1(4). □

For an elliptic curve $E/\mathbb{Q}$ and a prime number l, we denote the reduction of E at l by $\widetilde{E}_l$, and let $a_l = l + 1 - \sharp\widetilde{E}_l(\mathbb{F}_l)$, where $\mathbb{F}_l$ is the field with l elements. For a positive integer m, $E[m] = \{P \in E(\overline{\mathbb{Q}}) : mP = 0\}$ is the group of $m-$division points of E, where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group, and let $\rho_l : G_{\mathbb{Q}} \longrightarrow \mathrm{Gl}_2(\mathbb{F}_l)$ be the Galois representation of $G_{\mathbb{Q}}$ given by the action of $G_{\mathbb{Q}}$ on the $l-$division points of E (see, e.g., [Sil1, p.90]). By the open image theorem of Serre ([Se1]), ρ_l is surjective for all but finitely many prime numbers l.

Lemma 2.3. For the elliptic curves $E_D/\mathbb{Q}$ in (1.2) above,

(1) if $3 \nmid pqD$, then $\sharp\widetilde{E_{D,3}}(\mathbb{F}_3) = 4$ and $a_3 = 0$.

(2) if $7 \nmid pqD$, and $p \equiv 2, 3, 6 \pmod 7$, then $\sharp\widetilde{E_{D,7}}(\mathbb{F}_7) = 8$ and $a_7 = 0$.

(3) assume $5 \nmid pqD$,

(3a) if $p \equiv 1, 2 \pmod 5$, then

$$\sharp\widetilde{E_{D,5}}(\mathbb{F}_5) = \begin{cases} 4 & \text{if } D \equiv 1, 4 \pmod 5 \\ 8 & \text{if } D \equiv 2, 3 \pmod 5, \end{cases} \quad \text{and } a_5 = \begin{cases} 2 & \text{if } D \equiv 1, 4 \pmod 5 \\ -2 & \text{if } D \equiv 2, 3 \pmod 5, \end{cases}$$

(3b) if $p \equiv 4 \pmod 5$, then

$$\sharp\widetilde{E_{D,5}}(\mathbb{F}_5) = \begin{cases} 8 & \text{if } D \equiv 1, 4 \pmod 5 \\ 4 & \text{if } D \equiv 2, 3 \pmod 5, \end{cases} \quad \text{and } a_5 = \begin{cases} -2 & \text{if } D \equiv 1, 4 \pmod 5 \\ 2 & \text{if } D \equiv 2, 3 \pmod 5. \end{cases}$$

(4) assume $7 \nmid pqD$,

(4a) if $\begin{cases} \varepsilon = 1 \\ p \equiv 1 \pmod 7 \end{cases}$ or $\begin{cases} \varepsilon = -1 \\ p \equiv 4 \pmod 7, \end{cases}$ then

$$\sharp\widetilde{E_{D,7}}(\mathbb{F}_7) = \begin{cases} 12 & \text{if } D \equiv 1, 2, 4 \pmod 7 \\ 4 & \text{if } D \equiv 3, 5, 6 \pmod 7, \end{cases} \quad \text{and } a_7 = \begin{cases} -4 & \text{if } D \equiv 1, 2, 4 \pmod 7 \\ 4 & \text{if } D \equiv 3, 5, 6 \pmod 7, \end{cases}$$

(4b) if $\begin{cases} \varepsilon = 1 \\ p \equiv 4 \pmod 7 \end{cases}$ or $\begin{cases} \varepsilon = -1 \\ p \equiv 1 \pmod 7, \end{cases}$ then

$$\sharp\widetilde{E_{D,7}}(\mathbb{F}_7) = \begin{cases} 4 & \text{if } D \equiv 1, 2, 4 \pmod 7 \\ 12 & \text{if } D \equiv 3, 5, 6 \pmod 7, \end{cases} \quad \text{and } a_7 = \begin{cases} 4 & \text{if } D \equiv 1, 2, 4 \pmod 7 \\ -4 & \text{if } D \equiv 3, 5, 6 \pmod 7. \end{cases}$$

(5) $\sharp\widetilde{E_{D,2}}(\mathbb{F}_2) = 3$, $\quad \sharp\widetilde{E_{D,_{D_i}}}(\mathbb{F}_{D_i}) = D_i + 1 \ (i = 1, \cdots, n)$,

$$\sharp\widetilde{E_{D,p}}(\mathbb{F}_p) = \begin{cases} p & \text{if } (\frac{2\varepsilon D}{p}) = 1 \\ p+2 & \text{if } (\frac{2\varepsilon D}{p}) = -1, \end{cases} \quad \text{and } \sharp\widetilde{E_{D,q}}(\mathbb{F}_q) = \begin{cases} q & \text{if } (\frac{-2\varepsilon D}{q}) = 1 \\ q+2 & \text{if } (\frac{-2\varepsilon D}{q}) = -1. \end{cases}$$

Proof. Via direct calculation. $\square$

Recall that a prime number l is said to be anomalous for an elliptic curve $E/\mathbb{Q}$ if E has good reduction at l and $\sharp\widetilde{E}_l(\mathbb{F}_l) \equiv 0 \pmod l$ (see [Ma2, p.186] and [M, p.25]). We denote $\mathrm{Anom}(E/\mathbb{Q}) = \{l : \ l \text{ is an anomalous prime number for } E/\mathbb{Q}\}$.

Proposition 2.4. For the elliptic curves $E_D/\mathbb{Q}$ in (1.2) above, we have $\mathrm{Anom}(E_D/\mathbb{Q}) = \emptyset$.

Proof. Since the conductor $N_{E_D} = 2^5 pqD^2$, we have $2, p, q, D_i \notin \mathrm{Anom}(E_D/\mathbb{Q})$ $(i = 1, \cdots, n)$. On the other hand, by Lemma 2.1(5) above, $E_D(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so by the results 2.10(b) of [M, p.26] we have $\mathrm{Anom}(E_D/\mathbb{Q}) \subset \{2,3,5\}$, and so $\mathrm{Anom}(E_D/\mathbb{Q}) \subset \{3,5\}$. For $l = 3$ or 5, we may assume that $l \nmid pqD$, then by Lemma 2.3(1) and (3) above, we have $\sharp\widetilde{E_{D,3}}(\mathbb{F}_3) = 4$ and $\sharp\widetilde{E_{D,5}}(\mathbb{F}_5) = 4$ or 8, which shows that $3, 5 \notin \mathrm{Anom}(E_D/\mathbb{Q})$, so $\mathrm{Anom}(E_D/\mathbb{Q}) = \emptyset$. □

For our next discussion, we need the following

Lemma 2.5 (see [BSZ, p.4] and [Sil2, Prop.6.1 and exer.V.5.13]). Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. Let l, l' be two prime numbers with $l \neq l'$. Suppose $l \parallel N_E$. Then $E[l']$ is ramified at l if and only if $l' \nmid \mathrm{ord}_l(\Delta_l)$ for a minimal discriminant Δ_l of E at l.

Proposition 2.6. For the elliptic curves $E_D/\mathbb{Q}$ in (1.2) above , let l be a prime number. Then

(1) $E_D[l]$ is ramified at p if and only if $l > 2$ and $l \neq p$;

(2) $E_D[l]$ is ramified at q if and only if $l > 2$ and $l \neq q$.

In particular, $E_D[p]$ is ramified at q, and $E_D[q]$ is ramified at p.

Proof. Since the equation in (1.2) above is global minimal for $E_D/\mathbb{Q}$, we have $\Delta_l = \Delta = 64p^2q^2D^6$ for any prime number l, so

$$\mathrm{ord}_l(\Delta_l) = \begin{cases} 0 & \text{if } l \nmid 2pqD \\ 6 & \text{if } l \mid 2D \\ 2 & \text{if } l = p \text{ or } q. \end{cases}$$

On the other hand, the conductor $N_{E_D} = 2^5pqD^2$, so a prime number $l \parallel N_{E_D} \Leftrightarrow l = p$ or q. By the above discussion, $\mathrm{ord}_p(\Delta_p) = \mathrm{ord}_q(\Delta_q) = 2$, so the conclusion follow from the above Lemma 2.5. □

Proposition 2.7. For the elliptic curves $E_D/\mathbb{Q}$ in (1.2) above, let l be a prime number, and ρ_l be the corresponding Galois representation.

(1) If $3 \nmid pqD$, then ρ_3 is surjective, i.e., $\rho_3(G_{\mathbb{Q}}) = \mathrm{Gl}_2(\mathbb{F}_3)$.

(2) If $7 \nmid pqD$ and $p \equiv 2, 3, 6 \pmod 7$, then ρ_7 is surjective, i.e., $\rho_7(G_{\mathbb{Q}}) = \mathrm{Gl}_2(\mathbb{F}_7)$.

(3) If $3 \nmid pqD$, $l \nmid pqD$ and $l > 3105$, then ρ_l is surjective, i.e., $\rho_l(G_{\mathbb{Q}}) = \mathrm{Gl}_2(\mathbb{F}_l)$.

Proof. (1) Under the assumption, by Cor.2.2(1) above, E_D has good supersingular reduction at 3; also, the discriminant $\Delta = (2D)^6(pq)^2$ is obviously not a cube, so the conclusion follows from Serre's theorem (see [Se1] or [PR, Prop.4.4]).

(2) Under the assumption, by Cor.2.2(4) above, E_D has good supersingular reduction at 7; also, since the conductor $N_{E_D} = 2^5pqD^2$ and the invariant $j = \frac{64(p^2+2q)^3}{p^2q^2}$,

we have $p \parallel N$ and $\mathrm{ord}_p(j) = -2 \not\equiv 0 \pmod 7$. So the conclusion follows from Serre's theorem (see [Se1] or [PR, Prop.4.4]).
(2) Under the assumption, 3 is the smallest (odd) prime number at which E_D has good reduction. Also, $j \notin \mathbb{Z}$ and $\mathrm{ord}_p(j) = -2 < 0$. Moreover, the prime number l under our assumption obviously satisfies $l > (\sqrt{3}+1)^8$. So the conclusion follows from Prop.24 of [Se1]. $\square$

3 Rank, norm index, Shafarevich-Tate group and $l-$Selmer group

Let $E/\mathbb{Q}$ be the elliptic curve in (1.1) above, and let $K = \mathbb{Q}(\sqrt{D})$ be the quadratic number field, where $D = D_1 \cdots D_n$ with distinct odd prime numbers $D_1, \cdots, D_n$ as in (1.2) above. Let M_K be a complete set of places on K, and M_K^∞ (resp. M_K^0) its subset of infinite (resp. finite) places. Let $S_K = M_K^\infty \cup \{v \in M_K^0 : \ v \mid 2pq\}$. The group of S_K-units of K is denoted by $U_{K,S}$, the ideal class group of K is denoted by $\mathrm{Cl}(K)$, and the S_K-class group of K is denoted by $\mathrm{Cl}_S(K)$, precisely, $\mathrm{Cl}_S(K)$ is the quotient of $\mathrm{Cl}(K)$ by the subgroup generated by the classes represented by the finite primes in S_K (see [Sa, p.127]). For an abelian group A and a positive integer m, we write $A[m] = \{a \in A : \ ma = 0\}$. For a vector space V over $\mathbb{F}_2$, we denote its dimension by $\dim_2 V$. For a finitely generated abelian group A, we denote its rank by $\mathrm{rank}(A)$. The next result is about $E(K)$, the group of rational points of E over K.

Proposition 3.1. Let $E/\mathbb{Q}$ be the elliptic curve in (1.1), and $K = \mathbb{Q}(\sqrt{D})$ be the quadratic number field as above, we have $\mathrm{rank}(E(K)) \leq 14 + 2\dim_2 \mathrm{Cl}_S(K)[2]$.

Proof. Let $E' :\ y^2 = x^3 - 2\varepsilon(p+q)x^2 + 4x$. There is an isogeny φ of degree 2 between E and E' with the dual isogeny $\widehat{\varphi}$ as in [QZ1, pp.1372,1373]. Let $\mathrm{Sel}_\varphi(E/K)$ and $\mathrm{Sel}_{\widehat{\varphi}}(E'/K)$ be the $\varphi-$Selmer group of E/K and the $\widehat{\varphi}-$Selmer group of E'/K, respectively, and Ш (E/K) (resp. Ш (E'/K) be the Shafarevich-Tate groups of E/K (resp. E'/K) (see [Sil1, Chapt.10]). Then (see [Sil1, pp298, 301])

$$\begin{aligned}&\dim_2 E(K)/2E(K) + \dim_2 E'(K)[\widehat{\varphi}]/\varphi(E(K)[2]) \\ &= \dim_2 \mathrm{Sel}_\varphi(E/K) - \dim_2 Ш(E/K)[\varphi] + \dim_2 \mathrm{Sel}_{\widehat{\varphi}}(E'/K) - \dim_2 Ш(E'/K)[\widehat{\varphi}].\end{aligned}$$

Note that $E'(K)[\widehat{\varphi}] = \{O,(0,0)\}$, $\varphi(E(K)[2]) = \{O,(0,0)\}$, so $\mathrm{rank}(E(K)) \leq \dim_2\mathrm{Sel}_{\varphi}(E/K) + \dim_2\mathrm{Sel}_{\widehat{\varphi}}(E'/K) - 2$. On the other hand, the following exact sequence is known (see, e.g., [St, p.5], [Sz, p.55]): $0 \to U_{K,S}/U_{K,S}^2 \to K(S_K,2) \to \mathrm{Cl}_S(K)[2] \to 0$, where, $K(S_K,2) = \{bK^{*^2} \in K^*/K^{*^2} : \mathrm{ord}_v(b) \equiv 0 \pmod 2 \text{ for all } v \notin S_K\}$. So by the Dirichlet unit theorem (see [L, pp.104, 105]), we have $\dim_2 K(S_K,2) = \sharp S_K + \dim_2\mathrm{Cl}_S(K)[2] \leq 8 + \dim_2\mathrm{Cl}_S(K)[2]$ because $\sharp S_K = \sharp M_K^{\infty} + \sharp\{v \in M_K^0 : v \mid 2pq\} \leq 2+6 = 8$. Also, $\sharp\mathrm{Sel}_{\varphi}(E/K) \leq \sharp K(S_K,2)$ and $\sharp\mathrm{Sel}_{\widehat{\varphi}}(E'/K) \leq \sharp K(S_K,2)$ (see [Sil1, p.302]), so from the above discussion, $\mathrm{rank}(E(K)) \leq 2\dim_2 K(S_K,2) - 2 \leq 14 + 2\dim_2\mathrm{Cl}_S(K)[2]$. $\square$

Next, we need state some notations. Let F be a number field and L be a quadratic extension of F, we write M_F (resp.M_L) for a complete set of places on F (resp.L). Fix a place $w \in M_L$ lying above v for each $v \in M_F$. Denote the Galois group $\mathrm{Gal}(L_w/F_v)$ by G_w, where F_v and L_w are the completions of F at v and L at w, respectively. Let E be an elliptic curve over F. For every $v \in M_F$, we denote $\delta_v = \log_2(E(F_v) : N(E(L_w)))$, this is the local norm index studied deeply in [Kr] and [KT]. For some of their arithmetic application (see,e.g., [MR], [Q1]). Let $\delta(E,F,L)$ be the sum of all the local norm index, i.e., $\delta(E,F,L) = \sum_{v\in M_F}\delta_v$. Now, for the elliptic curve $E/\mathbb{Q}$ in (1.1) and the quadratic number field $K = \mathbb{Q}(\sqrt{D})$ as above, we come to calculate explicitly the quantity $\delta(E,\mathbb{Q},K)$ as in [Q1, p.5054, and Section 3 there], and give some application.

Lemma 3.2. Let $E/\mathbb{Q}$ be the elliptic curve in (1.1), $\mu = \pm 1$, and $K = \mathbb{Q}(\sqrt{\mu D})$ be the quadratic number field with square-free integer $D = D_1 \cdots D_n$ as in (1.2) above. Fix a place $w \in M_K$ lying above 2. Let Δ_w, c_w and f_w be the minimal discriminant, Tamagawa number and the exponent of the conductor of E at w (i.e., over K_w)(see [Sil1]), respectively.

(1) If $D \equiv 5\mu (\mathrm{mod} 8)$, then $K_w \cong \mathbb{Q}_2(\sqrt{-3})$, and
Type III, $\mathrm{ord}_w(\Delta_w) = 6$, $f_w = 5$, and $c_w = 2$.

(2) If $D \equiv 7\mu (\mathrm{mod} 8)$, then $K_w \cong \mathbb{Q}_2(\sqrt{-1})$, and
Type I_2^*, $\mathrm{ord}_w(\Delta_w) = 12$, $f_w = 6$, and $c_w = \begin{cases} 2 & \text{if } p \equiv 1 (\mathrm{mod} 4) \\ 4 & \text{if } p \equiv 3 (\mathrm{mod} 4). \end{cases}$

(3) If $D \equiv 3\mu (\mathrm{mod} 8)$, then $K_w \cong \mathbb{Q}_2(\sqrt{3})$, and
Type I_2^*, $\mathrm{ord}_w(\Delta_w) = 12$, $f_w = 6$, and $c_w = \begin{cases} 4 & \text{if } p \equiv 1 (\mathrm{mod} 4) \\ 2 & \text{if } p \equiv 3 (\mathrm{mod} 4). \end{cases}$

Proof. For the case $\mu D \equiv 3, 5, 7 (\mathrm{mod} 8)$, from the proof of Lemma3.1 in [Q1, p.5057], we have $K_w \cong \mathbb{Q}_2(\sqrt{-3}) \iff \mu D \equiv 5 \pmod 8$; $K_w \cong \mathbb{Q}_2(\sqrt{-1}) \iff \mu D \equiv 7 \pmod 8$; $K_w \cong \mathbb{Q}_2(\sqrt{3}) \iff \mu D \equiv 3 \pmod 8$. Then the conclusion follows from Tate's algorithm (see [Ta], [Sil2]), in a way as done in the proof of Lemma3.1 of [Q1, p.5057]. □

Theorem 3.3. Let $E/\mathbb{Q}$ be the elliptic curve in (1.1), $\mu = \pm 1$, and $K = \mathbb{Q}(\sqrt{\mu D})$ be the quadratic number field with square-free integer $D = D_1 \cdots D_n$ as in (1.2) above. Denote $\mu_0 = (1-\mu)/2$. Then we have $2n+\mu_0 \leq \delta(E, \mathbb{Q}, K) \leq 2n+4+\mu_0$. More precisely,

(1) $\delta(E, \mathbb{Q}, K) = 2n + \mu_0$ if and only if $D \equiv \mu (\text{mod} 8)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q}) = 1$.

(2) $\delta(E, \mathbb{Q}, K) = 2n + 1 + \mu_0$ if and only if one of the following four hypotheses holds :

(2a) $D \equiv 5\mu (\text{mod} 8)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q}) = 1$;

(2b) $D \equiv 7\mu (\text{mod} 8)$, $p \equiv 3 (\text{mod} 4)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q}) = 1$;

(2c) $D \equiv 3\mu (\text{mod} 8)$, $p \equiv 1 (\text{mod} 4)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q}) = 1$;

(2d) $D \equiv \mu (\text{mod} 8)$ and $(\frac{\mu D}{p}) + (\frac{\mu D}{q}) = 0$.

(3) $\delta(E, \mathbb{Q}, K) = 2n+2+\mu_0$ if and only if one of the following six hypotheses holds:

(3a) $D \equiv 7\mu (\text{mod} 8)$, $p \equiv 1 (\text{mod} 4)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q}) = 1$;

(3b) $D \equiv 3\mu (\text{mod} 8)$, $p \equiv 3 (\text{mod} 4)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q}) = 1$;

(3c) $D \equiv 5\mu (\text{mod} 8)$ and $(\frac{\mu D}{p}) + (\frac{\mu D}{q}) = 0$;

(3d) $D \equiv 7\mu (\text{mod} 8)$, $p \equiv 3 (\text{mod} 4)$ and $(\frac{\mu D}{p}) + (\frac{\mu D}{q}) = 0$;

(3e) $D \equiv 3\mu (\text{mod} 8)$, $p \equiv 1 (\text{mod} 4)$ and $(\frac{\mu D}{p}) + (\frac{\mu D}{q}) = 0$;

(3f) $D \equiv \mu (\text{mod} 8)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q}) = -1$.

(4) $\delta(E, \mathbb{Q}, K) = 2n + 3 + \mu_0$ if and only if one of the following five hypotheses holds:

(4a) $D \equiv 7\mu (\text{mod} 8)$, $p \equiv 1 (\text{mod} 4)$ and $(\frac{\mu D}{p}) + (\frac{\mu D}{q}) = 0$;

(4b) $D \equiv 3\mu (\text{mod} 8)$, $p \equiv 3 (\text{mod} 4)$ and $(\frac{\mu D}{p}) + (\frac{\mu D}{q}) = 0$;

(4c) $D \equiv 5\mu (\text{mod} 8)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q}) = -1$;

(4d) $D \equiv 7\mu (\text{mod} 8)$, $p \equiv 3 (\text{mod} 4)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q}) = -1$;

(4e) $D \equiv 3\mu (\text{mod} 8)$, $p \equiv 1 (\text{mod} 4)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q}) = -1$.

(5) $\delta(E, \mathbb{Q}, K) = 2n + 4 + \mu_0$ if and only if one of the following two hypotheses holds:

(5a) $D \equiv 7\mu (\text{mod} 8)$, $p \equiv 1 (\text{mod} 4)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q}) = -1$;

(5b) $D\equiv 3\mu(\mathrm{mod} 8)$, $p\equiv 3(\mathrm{mod} 4)$ and $(\frac{\mu D}{p})=(\frac{\mu D}{q})=-1$.

Proof. We consider the case $\mu=1$, the other case is similar. Let S be the set of finite places of $\mathbb{Q}$ obtained by collecting together all places that ramify in $K/\mathbb{Q}$ and all places of bad reduction for $E/\mathbb{Q}$, so $S=\{2,p,q,D_1\cdots D_n\}$. Although the cases here become more complicated, we will take our calculation in a way as in the Lemma 3.2 of [Q1, p.5058], so we need to use the same notations $S_0, S_g, S_{gu}, S_{ar}, S_a, S_{smr}, S_{nsmr}, S'_{nsmr}, S''_{nsmr}$ as in the Remark of [Q1, pp.5055,5056]. For the convenience of the reader, we write them in the present case as:

$S_0=\{v\in S:\ v \text{ is ramified or inertial in } K\}$;

$S_g=\{v\in S_0:\ v\nmid 2 \text{ and } E \text{ has good reduction at } v\}=\{D_1,\cdots,D_n\}$;

$S_{gu}=\{v\in S_0: v\mid 2,\ E \text{ has good reduction at } v \text{ and } \mathbb{Q}_v \text{ is unramified over } \mathbb{Q}_2\}$
$=\emptyset$;

$S_{ar}=\{v\in S_0:\ E \text{ has additive reduction at } v\}=\begin{cases}\{2\} & \text{if } D\equiv 3,5,7(\mathrm{mod} 8)\\ \emptyset & \text{if } D\equiv 1(\mathrm{mod} 8);\end{cases}$

$S_a=S_{ar}\cup\{v\in S_0: v\mid 2,\ E \text{ has good reduction at } v \text{ and } \mathbb{Q}_v \text{ is ramified over } \mathbb{Q}_2\}$
$=S_{ar}$;

$S_{smr}=\{v\in S_0:\ E \text{ has split multiplicative reduction at } v\}\subset\{p,q\}\cap S_0$;

$S_{nsmr}=\{v\in S_0:\ E \text{ has non-split multiplicative reduction at } v\}$
$=S'_{nsmr}\sqcup S''_{nsmr}$ (the disjoint union) $\subset\{p,q\}\cap S_0$, where

$S'_{nsmr}=\{v\in S_{nsmr}:\ v \text{ is inertial in } K\}=S_{nsmr}$,

$S''_{nsmr}=\{v\in S_{nsmr}:\ v \text{ is ramified in } K\}=\emptyset$.

Obviously, $S_0=S_g\sqcup S_{gu}\sqcup S_a\sqcup S_{smr}\sqcup S_{nsmr}$ (the disjoint union).

By definition, $\delta(E,\mathbb{Q},K)=\sum_{v\in M_{\mathbb{Q}}}\delta_v$, where $\delta_v=\log_2(E(\mathbb{Q}_v):N(E(K_w)))$ is the local norm index. Furthermore, by the results in [Kr], one can obtain that $\delta(E,\mathbb{Q},K)=\delta_\infty+\delta_f$, where δ_∞ is as in [Q, p.5054], and $\delta_f=\delta_g+\delta_m+\delta_a$ with $\delta_g,\delta_m,\delta_a$ in [Q1, pp.5055,5056], that is,

$$\delta_a=\sum_{v\in S_a}\delta_v;\quad \delta_m=\delta_{smr}+\delta_{nsmr} \text{ with } \delta_{smr}=\frac{1}{2}\sum_{v\in S_{smr}}(1+(\Delta_v,D)_{\mathbb{Q}_v}) \text{ and}$$

$$\delta_{nsmr}=\frac{1}{2}\sum_{v\in S'_{nsmr}}\left(1+(-1)^{v(\Delta_v)}\right)+\sum_{v\in S''_{nsmr}}\left(\frac{1}{2}(1+(\Delta_v,D)_{\mathbb{Q}_v})\cdot(-1)^{v(\Delta_v)}+1\right);$$

$$\delta_g=\sum_{v\in S_g}\dim_2\widetilde{E_v}(k_v)[2]+\sum_{v\in S_{gu}}\varepsilon(v),\quad \text{where}$$

$$\varepsilon(v)=\begin{cases}\frac{1}{2}\left(1-(-1)^{v(D)}\right)\cdot[\mathbb{Q}_v:\mathbb{Q}_2] & \text{if } E \text{ has good supersingular reduction at } v,\\ \frac{1}{2}(3+(\Delta_v,D)_{\mathbb{Q}_v}) & \text{if } E \text{ has good ordinary reduction at } v.\end{cases}$$

Here $\widetilde{E}_v$ is the reduction of E at v, k_v is the residue field of $\mathbb{Q}_v$, and $(,)_{\mathbb{Q}_v}$ is the Hilbert symbol (see [Se 2, Chapt.XIV]).

It is easy to see here that $\delta_\infty = 0$ since $D > 0$. So we only need to calculate $\delta_g, \delta_m, \delta_a$. For this, we divide our discussion into the following cases.

Case for δ_g. Since E has good reduction at each $D_i (i = 1, \cdots, n)$, we have an injective homomorphism $E(\mathbb{Q})_{\text{tors}} \hookrightarrow \widetilde{E}_{D_i}(\mathbb{F}_{D_i})$ (see [Kn, p.130]). So by Lemma 2.1(5) above, we have $\widetilde{E}_{D_i}(\mathbb{F}_{D_i})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$. and so

$\delta_g = \sum_{l \in S_g} \dim_2 \widetilde{E}_l(\mathbb{F}_l)[2] = \sum_{i=1}^n \dim_2 \widetilde{E}_{D_i}(\mathbb{F}_{D_i})[2] = 2n$, i.e., $\delta_g = 2n$.

Case for δ_m. Since the equation (1.1) is global minimal for $E/\mathbb{Q}$, we have $\text{ord}_p(\Delta_p) = \text{ord}_q(\Delta_q) = 2$, so $1 + (-1)^{\text{ord}_l(\Delta_l)} = 2$ for $l = p$ or q, and so $\delta_{nsmr} = \sharp S_{nsmr}$. Also $(\Delta_p, D)_{\mathbb{Q}_p} = (\Delta_q, D)_{\mathbb{Q}_q} = 1$ because $\Delta_p = \Delta_q = (8pq)^2$. So $\delta_{smr} = \sharp S_{smr}$. Hence $\delta_m = \sharp S_{smr} + \sharp S_{nsmr} = \sharp(S_0 \cap \{p, q\}) \leq 2$. The set S_0 can be determined as follows.

If $D \equiv 1 (\text{mod} 8)$, then $S_0 = \begin{cases} \{D_1, \cdots, D_n, p\} & \text{if } (\frac{D}{p}) = -1 \text{ and } (\frac{D}{q}) = 1 \\ \{D_1, \cdots, D_n, q\} & \text{if } (\frac{D}{p}) = 1 \text{ and } (\frac{D}{q}) = -1 \\ \{D_1, \cdots, D_n\} & \text{if } (\frac{D}{p}) = (\frac{D}{q}) = 1 \\ \{D_1, \cdots, D_n, p, q\} & \text{if } (\frac{D}{p}) = (\frac{D}{q}) = -1; \end{cases}$

If $D \equiv 3, 5, 7 (\text{mod} 8)$, then $S_0 = \begin{cases} \{2, D_1, \cdots, D_n, p\} & \text{if } (\frac{D}{p}) = -1 \text{ and } (\frac{D}{q}) = 1 \\ \{2, D_1, \cdots, D_n, q\} & \text{if } (\frac{D}{p}) = 1 \text{ and } (\frac{D}{q}) = -1 \\ \{2, D_1, \cdots, D_n\} & \text{if } (\frac{D}{p}) = (\frac{D}{q}) = 1 \\ \{2, D_1, \cdots, D_n, p, q\} & \text{if } (\frac{D}{p}) = (\frac{D}{q}) = -1. \end{cases}$

From this, we get

$\delta_m = \begin{cases} 0 & \text{if } (\frac{D}{p}) = (\frac{D}{q}) = 1 \\ 1 & \text{if } (\frac{D}{p}) + (\frac{D}{q}) = 0 \\ 2 & \text{if } (\frac{D}{p}) = (\frac{D}{q}) = -1. \end{cases}$

Case for δ_a. Since $S_a = S_{ar}$ is given above, we have

$\delta_a = \sum_{v \in S_a} \delta_v = \begin{cases} \delta_2 & \text{if } D \equiv 3, 5, 7 (\text{mod} 8) \\ 0 & \text{if } D \equiv 1 (\text{mod} 8). \end{cases}$ So the remainder is to compute the local norm index δ_2 when $D \equiv 3, 5, 7 (\text{mod} 8)$. So we assume now $D \equiv 3, 5, 7 (\text{mod} 8)$. By the Theorem 7.6 in [KT, p.332] (see also [Q1, p.5054]),

$$\delta_2 = \log_2 \left(\frac{c_2 c_{D,2}}{c_w} \left(\frac{\parallel \Delta_2 \Delta_{D,2} d(K_w/\mathbb{Q}_2)^{-6} \parallel_{\mathbb{Q}_2}}{\parallel \Delta_w \parallel_{K_w}} \right)^{1/12} \right).$$

By Lemma 2.1(1) above, we have $c_2 = c_{D,2} = 2, \Delta_{D,2} = 64p^2q^2D^6$. Also, by the results in [Q1, p.5058], we have $d(K_w/\mathbb{Q}_2) = \begin{cases} D & \text{if } D \equiv 5 (\text{mod} 8) \\ 4D & \text{if } D \equiv 3, 7 (\text{mod} 8). \end{cases}$ From these discussion together with the results of c_w and Δ_w in Lemma 3.2 above, one can work out δ_2 as follows.

If $D \equiv 5 (\text{mod} 8)$, then $\delta_2 = 1$;

If $D \equiv 7 (\text{mod} 8)$, then $\delta_2 = \begin{cases} 2 & \text{if } p \equiv 1 (\text{mod} 4) \\ 1 & \text{if } p \equiv 3 (\text{mod} 4); \end{cases}$

If $D \equiv 3 (\text{mod} 8)$, then $\delta_2 = \begin{cases} 1 & \text{if } p \equiv 1 (\text{mod} 4) \\ 2 & \text{if } p \equiv 3 (\text{mod} 4). \end{cases}$

Now our conclusion follows. $\square$

Recall that Ш (E/K) is the Shafarevich-Tate group of E/K. We have the following explicit parity relation between $\text{rank}(E(K))$ and $\dim_2 Ш(E/K)[2]$.

Theorem 3.4. Let $E/\mathbb{Q}$ be the elliptic curve in (1.1), $\mu = \pm 1$, and $K = \mathbb{Q}(\sqrt{\mu D})$ be the quadratic number field with square-free integer $D = D_1 \cdots D_n$ as in (1.2) above. Denote $\mu_0 = (1 - \mu)/2$. Then we have

(1) $\text{rank}(E(K)) \equiv \mu_0 + \dim_2 Ш(E/K)[2] \ (\text{mod} 2)$ if one of the following six hypotheses holds:

(1a) $D \equiv \mu (\text{mod} 8)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q})$;

(1b) $D \equiv 3\mu (\text{mod} 8)$, $p \equiv 3 (\text{mod} 4)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q})$;

(1c) $D \equiv 3\mu (\text{mod} 8)$, $p \equiv 1 (\text{mod} 4)$ and $(\frac{\mu D}{p}) + (\frac{\mu D}{q}) = 0$;

(1d) $D \equiv 5\mu (\text{mod} 8)$ and $(\frac{\mu D}{p}) + (\frac{\mu D}{q}) = 0$;

(1e) $D \equiv 7\mu (\text{mod} 8)$, $p \equiv 1 (\text{mod} 4)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q})$;

(1f) $D \equiv 7\mu (\text{mod} 8)$, $p \equiv 3 (\text{mod} 4)$ and $(\frac{\mu D}{p}) + (\frac{\mu D}{q}) = 0$.

(2) $\text{rank}(E(K)) \equiv \mu_0 + 1 + \dim_2 Ш(E/K)[2] \ (\text{mod} 2)$ if one of the following six hypotheses holds:

(2a) $D \equiv \mu (\text{mod} 8)$ and $(\frac{\mu D}{p}) + (\frac{\mu D}{q}) = 0$;

(2b) $D \equiv 3\mu (\text{mod} 8)$, $p \equiv 1 (\text{mod} 4)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q})$;

(2c) $D \equiv 3\mu (\text{mod} 8)$, $p \equiv 3 (\text{mod} 4)$ and $(\frac{\mu D}{p}) + (\frac{\mu D}{q}) = 0$;

(2d) $D \equiv 5\mu (\text{mod} 8)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q})$;

(2e) $D \equiv 7\mu (\text{mod} 8)$, $p \equiv 3 (\text{mod} 4)$ and $(\frac{\mu D}{p}) = (\frac{\mu D}{q})$;

(2f) $D \equiv 7\mu (\text{mod} 8)$, $p \equiv 1 (\text{mod} 4)$ and $(\frac{\mu D}{p}) + (\frac{\mu D}{q}) = 0$.

Proof. By Theorem 1 of [Kr, p.130], we have
$\text{rank}(E(K)) \equiv \sum_{v \in M_{\mathbb{Q}}} \delta_v + \dim_2 Ш(E/K)[2] = \delta(E, \mathbb{Q}, K) + \dim_2 Ш(E/K)[2] \ (\text{mod} 2)$.
So the conclusion follows from Theorem 3.3 above. $\square$

Corollary 3.5. Let $E/\mathbb{Q}$ and K be as in Theorem 3.4 above. If $\sharp\, Ш(E/K)[2]$ is a square integer, then under one of the conditions in (2) for $\mu = 1$ (or in (1) for $\mu = -1$) of Theorem 3.4, we have $\text{rank}(E(K)) > 0$.

Proof. Obvious. $\square$

Now for an elliptic curve E over a number field F, and a positive integer m, let $\mathrm{Sel}_m(E/F)$ be the $m-$Selmer group of E/F (see [Sil1, Chapt.10]).

Corollary 3.6. For the elliptic curves $E/\mathbb{Q}$ in (1.1) and $E_D/\mathbb{Q}$ in (1.2) above, let μ and μ_0 be as in Theorem 3.4 above. Then we have
(1) $\dim_2 \mathrm{Sel}_2(E_{\mu D}/\mathbb{Q}) \equiv \mu_0 + \dim_2 \mathrm{Sel}_2(E/\mathbb{Q}) \pmod 2$ if one of the six hypotheses in (1) of Theorem 3.4 above holds.
(2) $\dim_2 \mathrm{Sel}_2(E_D/\mathbb{Q}) \equiv \mu_0 + 1 + \dim_2 \mathrm{Sel}_2(E/\mathbb{Q}) \pmod 2$ if one of the six hypotheses in (2) of Theorem 3.4 above holds.

Proof. Let $K = \mathbb{Q}(\sqrt{\mu D})$ be as in Theorem 3.4 above. By Kramer's theorem (see [MR, Thm.2.7]), we have
$\dim_2 \mathrm{Sel}_2(E_{\mu D}/\mathbb{Q}) \equiv \dim_2 \mathrm{Sel}_2(E/\mathbb{Q}) + \delta(E, \mathbb{Q}, K) \pmod 2$. So the conclusion follows from Theorem 3.3 above. $\square$

For an elliptic curve $E/\mathbb{Q}$, let $L(E/\mathbb{Q}, s)$ be its $L-$ function (see [Sil1]). We denote its analytic rank by $r_{an}(E/\mathbb{Q})$, i.e., $r_{an}(E/\mathbb{Q}) = \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s)$, which is the order of $L(E/\mathbb{Q}, s)$ vanishing at $s = 1$.

Theorem 3.7. Let $E_D/\mathbb{Q}$ be the elliptic curve in (1.2) above ($E_1 = E$ in (1.1) when take $D = 1$). Assume that one of the following four hypotheses holds:
(1) $p > 37$ and the $p-$Selmer group $\mathrm{Sel}_p(E_D/\mathbb{Q})$ is trivial;
(2) $p > 37$ and the $q-$Selmer group $\mathrm{Sel}_q(E_D/\mathbb{Q})$ is trivial;
(3) $5 \nmid pqD$, $E_D[5]$ is an irreducible $G_{\mathbb{Q}}-$module, and the $5-$Selmer group $\mathrm{Sel}_5(E_D/\mathbb{Q})$ is trivial;
(4) $7 \nmid pqD$, $p \equiv 1, 4 \pmod 7$, $E_D[7]$ is an irreducible $G_{\mathbb{Q}}-$module, and the $7-$Selmer group $\mathrm{Sel}_7(E_D/\mathbb{Q})$ is trivial.
Then the rank and analytic rank of $E_D/\mathbb{Q}$ are both equal to 0, i.e., $\mathrm{rank}(E_D(\mathbb{Q})) = r_{an}(E_D/\mathbb{Q}) = 0$.

Proof. First, assume (1) (resp. (2)), then
(a) E_D has multiplicative reduction at both p and q;
(b) Since E_D has no complex multiplication, by the work of [Ma1] (or see[Cha, p.175]), for $p > 37$, both $E_D[p]$ and $E_D[q]$ are irreducible $G_{\mathbb{Q}}-$modules;
(c) By Prop.2.6 above, $E_D[p]$ is ramified at q, and $E_D[q]$ is ramified at p;
(d) By assumption, $\mathrm{Sel}_p(E_D/\mathbb{Q})$ (resp. $\mathrm{Sel}_q(E_D/\mathbb{Q})$) is trivial.
So all the conditions (a), (b), (c), (d) in Theorem 5 of [BSZ, p.3] hold, and the

conclusion follows.

Next, assume (3) (resp. (4)), then

(a) By Cor.2.2 above, E_D has good ordinary reduction at 5 (resp. 7);

(b) $E_D[5]$ (resp. $E_D[7]$) is an irreducible $G_{\mathbb{Q}}$−module;

(c) By Prop.2.6 above, $E_D[5]$ (resp. $E_D[7]$) is ramified at p;

(d) $\mathrm{Sel}_5(E_D/\mathbb{Q})$ (resp. $\mathrm{Sel}_7(E_D/\mathbb{Q})$) is trivial.

So all the conditions (a), (b), (c), (d) in Theorem 5 of [BSZ, p.3] hold, and the conclusion follows. □

Theorem 3.8. Let $E_D/\mathbb{Q}$ be the elliptic curve in (1.2) above ($E_1 = E$ in (1.1) when take $D = 1$). Assume that one of the following two hypotheses holds:

(1) $5 \nmid pqD$, $E_D[5]$ is an irreducible $G_{\mathbb{Q}}$−module, and the 5−Selmer group $\mathrm{Sel}_5(E_D/\mathbb{Q})$ has order 5;

(2) $7 \nmid pqD$, $p \equiv 1, 4 \pmod 7$, $E_D[7]$ is an irreducible $G_{\mathbb{Q}}$−module, and the 7−Selmer group $\mathrm{Sel}_7(E_D/\mathbb{Q})$ has order 7.

Then the rank and analytic rank of $E_D/\mathbb{Q}$ are both equal to 1, i.e., $\mathrm{rank}(E_D(\mathbb{Q})) = r_{an}(E_D/\mathbb{Q}) = 1$.

Proof. Assume (1) (resp. (2)), then

(a) By Cor.2.2 above, E_D has good ordinary reduction at 5 (resp. 7);

(b) $E_D[5]$ (resp. $E_D[7]$) is an irreducible $G_{\mathbb{Q}}$−module;

(c) By Prop.2.6 above, $E_D[5]$ (resp. $E_D[7]$) is ramified at l for $l = p$ or q;

(d) The conductor N of E_D is obviously not square-free, and there are two distinct prime factors $l \parallel N$ (i.e., p, q) such that $E_D[5]$) (resp. $E_D[7]$)is ramified at l;

(e) E_D obviously has good reduction at 5 (resp. 7);

(f) $\mathrm{Sel}_5(E_D/\mathbb{Q})$ (resp. $\mathrm{Sel}_7(E_D/\mathbb{Q})$) has order 5 (resp. 7.)

So all the conditions (a), (b), (c), (d), (e), (f) in Theorem 9 of [BSZ, p.4] hold, and the conclusion follows. □

Remark. For the elliptic curve E_D in Theorem 3.8 above, since its conductor $N = 2^5 pqD^2$ has two distinct prime factors of order one, i.e., p and q, by Theorem 1.5 of [Zh, p.8], we know that the following two statements are equivalent:

(1) $\mathrm{rank}(E_D(\mathbb{Q})) = 1$ and $\sharp\,\text{Ш}(E_D/\mathbb{Q}) < +\infty$;

(2) $r_{an}(E_D/\mathbb{Q}) = 1$.

4 Iwasawa theory for E_D

Let E be an elliptic curve defined over a number field F, m be a positive integer and l be a prime number. Then for any place $v \in M_F$, we have the Kummer homomorphisms
$\kappa_{v,m}: E(F_v)\otimes\mathbb{Z}/m\mathbb{Z} \to \mathrm{H}^1(F_v, E[m])$, and $\kappa_{v,l^\infty}: E(F_v)\otimes\mathbb{Q}_l/\mathbb{Z}_l \to \mathrm{H}^1(F_v, E[l^\infty])$, where $\mathbb{Z}_l$ is the ring of $l-$adic integers and $E[l^\infty]$ is the $l-$primary torsion subgroup of E. Recall that the $m-$Selmer group $\mathrm{Sel}_m(E/F)$ of E/F is defined as
$\mathrm{Sel}_m(E/F) = \ker\{\mathrm{H}^1(F, E[m]) \longrightarrow \prod_{v\in M_F} \mathrm{H}^1(F_v, E[m])/\mathrm{Im}(\kappa_{v,m})\}$,
and the $l^\infty-$Selmer group $\mathrm{Sel}_{l^\infty}(E/F)$ is defined as
$\mathrm{Sel}_{l^\infty}(E/F) = \ker\{\mathrm{H}^1(F, E[l^\infty]) \longrightarrow \prod_{v\in M_F} \mathrm{H}^1(F_v, E[l^\infty])/\mathrm{Im}(\kappa_{v,l^\infty})\}$.
Note that the $l^\infty-$Selmer group can be defined for E over any algebraic extension M of $\mathbb{Q}$ (see [Gr, p.63]). There is a natural surjective homomorphism (see [Zh, p.3])

$$\mathrm{Sel}_l(E/F) \longrightarrow \mathrm{Sel}_{l^\infty}(E/F)[l],$$

and the properties of $\mathrm{Sel}_{l^\infty}(E/F)$ can sometimes be deduced from the ones of $\mathrm{Sel}_l(E/F)$ (see [BS, p.6]).
Let $\mathbb{Q}_\infty$ be a $\mathbb{Z}_l-$extension, i.e., it is a Galois extension of $\mathbb{Q}$ such that $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_l$, the additive group of $l-$adic integers. So we have $\mathbb{Q}_\infty = \cup_{n\geq 0}\mathbb{Q}_n$, where for each $n, \mathbb{Q}_n$ is a cyclic extension of $\mathbb{Q}$ of degree l^n and $\mathbb{Q} = \mathbb{Q}_0 \subset \mathbb{Q}_1 \subset \cdots \subset \mathbb{Q}_n \subset \cdots$. We write $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$, and let $\gamma \in \Gamma$ be a fixed topological generator. The completed group ring $\Lambda = \mathbb{Z}_l[[\Gamma]] \cong \mathbb{Z}_l[[T]]$, where the indeterminate T is identified with $\gamma - 1$. We write $\Gamma_n = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_n)$, then $\Gamma_n = \Gamma^{l^n}$. For the structure of the Iwasawa algebra Λ, see [Wa]. For an elliptic curve E defined over $\mathbb{Q}$, the Pontryagin dual of its $l^\infty-$Selmer group $\mathrm{Sel}_{l^\infty}(E/\mathbb{Q}_\infty)$ is denoted by $X(E/\mathbb{Q}_\infty) = \mathrm{Hom}(\mathrm{Sel}_{l^\infty}(E/\mathbb{Q}_\infty), \mathbb{Q}_l/\mathbb{Z}_l)$. It is a $\Lambda-$module via the natural action of Γ on the group $\mathrm{H}^1(\mathbb{Q}_\infty, E[l^\infty])$, and one says that $\mathrm{Sel}_{l^\infty}(E/\mathbb{Q}_\infty)$ is $\Lambda-$cotorsion if $X(E/\mathbb{Q}_\infty)$ is $\Lambda-$torsion (see [Gr, p.55]).

Now let $E_D/\mathbb{Q}$ be the elliptic curve in (1.2) above ($E_1 = E$ in (1.1) when take $D = 1$). Assume that the prime number l satisfies one of the following two hypotheses:
(1) $l = 5$ and $5 \nmid pqD$;
(2) $l = 7$, $7 \nmid pqD$, and $p \equiv 1, 4 (\mathrm{mod} 7)$.
Then by Cor.2.2 above, E_D has good ordinary reduction at such l. So by Mazur's

control theorem (see [Gr, p.54]), the natural maps

$$\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_n) \longrightarrow \mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)^{\Gamma_n}$$

have finite kernel and cokernel, of bounded order as n varies.
Such $E_D/\mathbb{Q}$ also has multiplicative reduction at p and q, so for the prime number l such that $l = p, q$ or satisfies one of the above two hypotheses (1) and (2), by Kato-Rohrlich's theorem (see [Gr, p.55]), we know that $\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)$ is $\Lambda-$cotorsion. Furthermore, under this hypothesis, we have the following results.

Proposition 4.1. Let $E_D/\mathbb{Q}$ be the elliptic curve in (1.2) above ($E_1 = E$ in (1.1) when take $D = 1$). Let l be a prime number satisfying one of the following two hypotheses:
(1) $l = 5$ and $5 \nmid pqD$;
(2) $l = 7,\ 7 \nmid pqD$, and $p \equiv 1, 4 (\mathrm{mod} 7)$.
Then the map

$$\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}) \longrightarrow \mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)^{\Gamma}$$

is surjective. If $\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}) = 0$, then $\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty) = 0$ also.

Proof. By Cor.2.2 above, E_D has good ordinary reduction at such l; by Lemma 2.3 above, we have $l \nmid \sharp\widetilde{E_{D,l}}(\mathbb{F}_l)$; and by Lemma 2.1, $l \nmid c_{l'}$ for any prime number l'. So the conditions (i), (ii), (iii) of Prop.3.8 in [Gr, p.80] hold (see also the Remark there), and the conclusion follows. □

Proposition 4.2. Let $E_D/\mathbb{Q}$ be the elliptic curve in (1.2) above ($E_1 = E$ in (1.1) when take $D = 1$). Let l be a prime number satisfying one of the following three hypotheses:
(1) $l = p$ or q;
(2) $l = 5$ and $5 \nmid pqD$;
(3) $l = 7,\ 7 \nmid pqD$, and $p \equiv 1, 4 (\mathrm{mod} 7)$.
Then for all $n \geq 0$, the map $\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_n) \longrightarrow \mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)$ is injective. Moreover,

$$\mathrm{corank}_{\mathbb{Z}_l}(\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)) \equiv \mathrm{corank}_{\mathbb{Z}_l}(\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}))(\mathrm{mod} 2).$$

Proof. Under our assumption, E_D has good ordinary or multiplicative reduction at l. Also, by the above discussion, we know that $\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)$ is $\Lambda-$cotorsion, so the conclusion follows from the Prop.3.9 and Prop.3.10 of [Gr, pp.81, 82]. □

Now for the elliptic curves $E_D/\mathbb{Q}$ and the prime number l as in the above Proposition 4.2, by Mazur and Swinnerton-Dyer's construction, there is an element $\mathfrak{L}(E_D/\mathbb{Q}, T) \in \Lambda \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ with some interpolation property, from which one can define the $l-$adic $L-$ function $L_l(E_D/\mathbb{Q}, s)$. For the general theory of $l-$adic $L-$function of elliptic curves, see [MSD] and [Gr]. By Weierstrass' preparation theorem, we have $\mathfrak{L}(E_D/\mathbb{Q}, T) = l^{m_1} \cdot U(T) \cdot f(T)$, where $f(T)$ is a distinguished polynomial, $U(T)$ is an invertible power series and $m_1 \in \mathbb{Z}$. As in [GV, pp.19, 20], we write $f_{E_D}^{\text{anal}}(T) = l^{m_1} \cdot f(T)$. On the other hand, since $\text{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)$ is $\Lambda-$cotorsion, i.e., $X(E_D/\mathbb{Q}_\infty)$ is $\Lambda-$torsion, one has a pseudo-isomorphism

$$X(E_D/\mathbb{Q}_\infty) \sim (\oplus_{i=1}^n \Lambda/(f_i(T)^{a_i})) \oplus (\oplus_{j=1}^m \Lambda/(l^{b_j})),$$

where $f_i(T)$ are irreducible distinguished polynomials in Λ, and a_i, b_j are non-negative integers. Then the characteristic polynomial for the $\Lambda-$module $X(E_D/\mathbb{Q}_\infty)$ is defined by $f_{E_D}^{\text{alg}}(T) = l^{m_2} \cdot \prod_{i=1}^n f_i(T)^{a_i}$, where $m_2 = \sum_{j=1}^m b_j$. By Kato's theorem about the main conjecture (see [GV, p.21]), the polynomial $f_{E_D}^{\text{alg}}(T)$ divides $f_{E_D}^{\text{anal}}(T)$ in $\mathbb{Q}_l[T]$. Moreover, by Greenberg's theorem (see [Gr, p.61]), the characteristic ideal of $X(E_D/\mathbb{Q}_\infty)$ is fixed by the involution ι of Λ induced by $\iota(\sigma) = \sigma^{-1}$ for all $\sigma \in \Gamma$.

Theorem 4.3. Let $E_D/\mathbb{Q}$ be the elliptic curve in (1.2) above ($E_1 = E$ in (1.1) when take $D = 1$). Let l be a prime number satisfying one of the following three hypotheses:

(1) $l = p$ or q;

(2) $l = 5$ and $5 \nmid pqD$;

(3) $l = 7,\ 7 \nmid pqD$, and $p \equiv 1, 4 (\text{mod} 7)$.

Then $\text{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)$ has no proper $\Lambda-$submodules of finite index. In particular, if $\text{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty) \neq 0$, then $\text{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)$ is finite.

Moreover, for l satisfying the hypothesis (2) or (3) here, if $\text{Sel}_{l^\infty}(E_D/\mathbb{Q})$ is finite, then $f_{E_D}^{\text{alg}}(0) \sim \sharp \text{Sel}_{l^\infty}(E_D/\mathbb{Q})$. Here, for $a, b \in \mathbb{Q}_l^\times$, we write $a \sim b$ to indicate that a and b have the same $l-$adic valuation.

Proof. By Lemma 2.1(5) above, the torsion subgroup $E_D(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so for the prime number l under our assumption, $E_D(\mathbb{Q})_{\text{tors}}[l^\infty] = 0$. Also, by the above discussion, we know that $\text{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)$ is $\Lambda-$cotorsion, so our first conclusion follows from the Prop.4.14 of [Gr, p.102].

Next we come to show our second conclusion. As $\text{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)$ is $\Lambda-$cotorsion,

let $f_{E_D}^{\mathrm{alg}}(T)$ be its characteristic polynomial as above, i.e., $f_{E_D}^{\mathrm{alg}}(T)$ is a generator of the characteristic ideal of the $\Lambda-$module $X(E_D/\mathbb{Q}_\infty)$, the Pontryagin dual of $\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)$. Denote $\theta_n = \gamma^{l^n} - 1 = (1+T)^{l^n} - 1 \in \Lambda$ for each $n \geq 0$. We know, $X(E_D/\mathbb{Q}_\infty)/\theta_n X(E_D/\mathbb{Q}_\infty)$ is the Pontryagin dual of $\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)^{\Gamma_n}$, and the torsion subgroup of $X(E_D/\mathbb{Q}_\infty)/\theta_n X(E_D/\mathbb{Q}_\infty)$ is then dual to
$\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)^{\Gamma_n}/(\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)^{\Gamma_n})_{\mathrm{div}}$ (see [Gr, p.82]),
In particular, $X(E_D/\mathbb{Q}_\infty)/TX(E_D/\mathbb{Q}_\infty)$ is the Pontryagin dual of $\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)^{\Gamma}$. As assumed, $\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q})$ is finite, and so by the above discussion, $\mathrm{Sel}_{l^\infty}(E_D/\mathbb{Q}_\infty)^{\Gamma}$ is also finite, hence $X(E_D/\mathbb{Q}_\infty)/TX(E_D/\mathbb{Q}_\infty)$ is finite. Therefore, $T \nmid f_{E_D}^{\mathrm{alg}}(T)$, so $f_{E_D}^{\mathrm{alg}}(0) \neq 0$. In the following, For an element $c \in \mathbb{Z}_l$, the highest power of l dividing c is denoted by $c^{(l)}$.
Now we assume that l satisfies the hypothesis (2), i.e., $l = 5$ and $5 \nmid pqD$. Then E_D has good ordinary reduction at 5, and by Lemma 2.3 above, $\sharp\widetilde{E_{D,5}}(\mathbb{F}_5) = 4$ or 8. So $\widetilde{E_{D,5}}(\mathbb{F}_5)[5^\infty] = 0$. Also by Lemma 2.1, we have $c_{l'} = 2$ or 4 for any $l' \mid N_{E_D}$, the conductor of E_D, and $E_D(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. So $c_{l'}^{(5)} = 1$ for any $l' \mid N$, and $E_D(\mathbb{Q})[5^\infty] = 0$. Hence by Theorem 4.1 of [Gr, p.85], we get

$$\begin{aligned} f_{E_D}^{\mathrm{alg}}(0) &\sim (\prod_{l' \mid N_{E_D}} c_{l'}^{(5)}) \cdot (\sharp\widetilde{E_{D,5}}(\mathbb{F}_5)[5^\infty])^2 \cdot \sharp\mathrm{Sel}_{5^\infty}(E_D/\mathbb{Q})/(\sharp E_D(\mathbb{Q})[5^\infty])^2 \\ &= 1 \cdot 1^2 \cdot \sharp\mathrm{Sel}_{5^\infty}(E_D/\mathbb{Q})/1^2 = \sharp\mathrm{Sel}_{5^\infty}(E_D/\mathbb{Q}), \end{aligned}$$

i.e., $f_{E_D}^{\mathrm{alg}}(0) \sim \sharp\mathrm{Sel}_{5^\infty}(E_D/\mathbb{Q})$. The case for l satisfying the hypothesis (3) can be similarly done, and the proof is completed. □

Remark. For the elliptic curve $E_D/\mathbb{Q}$ in (1.2) above, for every prime number $l > 2$, by Lemma 2.1 above, we have $E_D(\mathbb{Q})[l^\infty] = 0$, so $E_D(\mathbb{Q}_\infty)[l^\infty] = 0$ because Γ is pro-l (see [Gr, p.102, line -10]). so $E_D(\mathbb{Q}_\infty)_{\mathrm{tors}}$ is a $2-$group, i.e., its every element is of $2-$power order.

For the elliptic curve $E_D/\mathbb{Q}$ as in (1.2) above, let Ω_D be its Néron period. Now we let l be a prime number satisfying one of the following two hypotheses:
(1) $l = 3$ and $3 \nmid pqD$;
(2) $l = 7$, $7 \nmid pqD$, and $p \equiv 2, 3, 6 (\mathrm{mod} 7)$.

Then by Cor.2.2 above, we know that E_D has good supersingular reduction at such l. By Lemma 2.1 above, we have $c_{l'} = 2$ or 4 for any prime number $l' \mid N_{E_D} = 2^5 pqD^2$, so our $l \nmid \mathrm{Tam}(E_D/\mathbb{Q}) = \prod_{l' < \infty} c_{l'}$. Also by Prop.2.7 above, we have $\rho_l(G_{\mathbb{Q}}) = \mathrm{Gl}_2(\mathbb{F}_l)$. Therefore, if $\mathrm{ord}_l(L(E_D/\mathbb{Q},1)/\Omega_D) = 0$, then over the $\mathbb{Z}_l-$extension $\mathbb{Q}_\infty/\mathbb{Q}$ as above, by The Theorem 0.1 of [Ku, p.196], we have the following conclusion:

(1) $(\text{Ш}\,(E_D/\mathbb{Q}_\infty)[l^\infty])^\wedge \cong \Lambda$ as $\Lambda-$modules, where $(\text{Ш}\,(E_D/\mathbb{Q}_\infty)[l^\infty])^\wedge$ is the Pontryagin dual of $\text{Ш}\,(E_D/\mathbb{Q}_\infty)[l^\infty]$;

(2) $\mathrm{rank}(E_D(\mathbb{Q}_n)) = 0$ and $\sharp\, \text{Ш}(E_D/\mathbb{Q}_n)[l^\infty] = l^{e_n}$ with $e_n = [\frac{l^{n+1}}{l^2-1} - \frac{n}{2}]$ for any $n \geq 0$;

(3) $(\text{Ш}\,(E_D/\mathbb{Q}_n)[l^\infty])^\wedge \cong \mathbb{Z}_l[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})]/(\theta_{\mathbb{Q}_n}, v_{n-1,n}(\theta_{\mathbb{Q}_{n-1}}))$ as $\mathbb{Z}_l[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})]-$modules for any $n \geq 0$, where $\theta_{\mathbb{Q}_n}$ is the modular element of Mazur and Tate (see [Ku] for the detail).

In fact, the Mordell-Weil group $E_D(\mathbb{Q}_n)$ in the above result (2) can be determined as follows.

Theorem 4.4. Let $E_D/\mathbb{Q}$ be the elliptic curve in (1.2) above ($E_1 = E$ in (1.1) when take $D = 1$). Let l be a prime number satisfying one of the following two hypotheses:

(1) $l = 3$ and $3 \nmid pqD$;

(2) $l = 7,\ 7 \nmid pqD$, and $p \equiv 2, 3, 6 (\mathrm{mod} 7)$.

If $\mathrm{ord}_l(L(E_D/\mathbb{Q},1)/\Omega_D) = 0$, then over the $\mathbb{Z}_l-$extension $\mathbb{Q}_\infty/\mathbb{Q}$ as above, we have $E_D(\mathbb{Q}_n) \cong \mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z}$ for all $n \geq 0$.

Proof. By the above discussion, we know that $\mathrm{rank}(E_D(\mathbb{Q}_n)) = 0$. So $E_D(\mathbb{Q}_n) = E_D(\mathbb{Q}_n)_{\mathrm{tors}}$. Since E_D has good supersingular reduction at such l, $E_D(\mathbb{Q}(\mu_{l^{n+1}}))$ does not contain a point of order l for any $n \geq 0$ (see [Ku, p.200, line-2]), where $\mu_{l^{n+1}}$ is the group of $l^{n+1}-$th roots of unity. Since $\mathbb{Q}_\infty$ is in fact the cyclotomic $\mathbb{Z}_l-$extension of $\mathbb{Q}$, we have $\mathbb{Q}_n \subset \mathbb{Q}(\mu_{l^{n+1}})$, and so $E_D(\mathbb{Q}_n)[l^\infty] = 0$ for any $n \geq 0$. On the other hand, l is totally ramified in $\mathbb{Q}_n$. Let $\mathfrak{p}_n$ be the unique prime ideal of $\mathbb{Q}_n$ lying over l, then the residue degree $f(\mathfrak{p}_n/l) = 1$, and the residue field $k_{\mathfrak{p}_n} = \mathbb{F}_l$. So if $l = 3$, then by Lemma 2.1(6) above, we have $E_D(\mathbb{Q}_n)_{\mathrm{tors}}/E_D(\mathbb{Q}_n)[3^\infty] \cong \mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z}$, and then our conclusion follows because $E_D(\mathbb{Q}_n)[3^\infty] = 0$. If $l = 7$, then by Lemma 4.2(1) of [QZ1, p.1379], we have $\sharp E_D(\mathbb{Q}_n)_{\mathrm{tors}} \mid \sharp \widetilde{E_{D,\mathfrak{p}_n}}(\mathbb{F}_7) \cdot 7^{2t_7}$ for some $t_7 \in \mathbb{Z}_{\geq 0}$. By Lemma 2.3 above, $\sharp \widetilde{E_{D,\mathfrak{p}_n}}(\mathbb{F}_7) = 8$. Also, by the above discussion, $7 \nmid \sharp E_D(\mathbb{Q}_n)_{\mathrm{tors}}$. So $\sharp E_D(\mathbb{Q}_n)_{\mathrm{tors}} \mid 8$. Obviously, $E_D(\mathbb{Q}_n)_{\mathrm{tors}} \supset E_D(\mathbb{Q}_n)[2] \cong \mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z}$, so $E_D(\mathbb{Q}_n)_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times Z/4\mathbb{Z}$. The remainder is to show that $E_D(\mathbb{Q}_n)_{\rm tors} \ncong \mathbb{Z}/2\mathbb{Z} \times Z/4\mathbb{Z}$, and this follows from the following

Assertion. $E_D(\mathbb{Q}(\mu_{7^n}))$ does not contain a point of order 4 for any $n \geq 0$.

To see this, firstly, by Lemma 2.1 above, $E_D(\mathbb{Q})_{\rm tors} \cong \mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z}$, so we may as well assume that $n > 0$. Obviously $E_D[2] = \{O, (0,0), (-\varepsilon pD, 0), (-\varepsilon qD, 0)\}$, so $E_D(\mathbb{Q}(\mu_{7^n}))$ contains a point P_4 of order 4 if and only if $2P_4 = (0,0), (-\varepsilon pD, 0)$ or $(-\varepsilon qD, 0)$. And by Theorem 4.2 of [Kn, p.85], this is equivalent to say that (we write $F = \mathbb{Q}(\mu_{7^n})$): (a) $\varepsilon pD, \varepsilon qD \in F^2$; or (b) $-\varepsilon pD, 2\varepsilon D \in F^2$; or (c) $-\varepsilon qD, -2\varepsilon D \in F^2$. But all of these cases are impossible because 7 is the unique prime number which ramifies in F and $7 \nmid pq$. So the above Assertion follows, and the proof is completed. $\square$

5 $L-$function, root number and parity conjecture

Let $E/\mathbb{Q}$ be the elliptic curve in (1.1), and its quadratic $D-$twist $E_D/\mathbb{Q}$ in (1.2) above. Let $K = \mathbb{Q}(\sqrt{D})$ and $K' = \mathbb{Q}(\sqrt{-D})$. The $(-D)-$twist of such E is

$$E_{-D} = E^{\varepsilon}_{-D}: \ y^2 = x(x - \varepsilon pD)(x - \varepsilon qD). \tag{5.1}$$

So, $E^{\varepsilon}_{-D} = E^{-\varepsilon}_{D}$.

As before, Let $L(E/\mathbb{Q}, s)$, $L(E_D/\mathbb{Q}, s)$ and $L(E_{-D}/\mathbb{Q}, s)$ be the $L-$functions of $E/\mathbb{Q}$, $E_D/\mathbb{Q}$ and $E_{-D}/\mathbb{Q}$ respectively, and write

$$L(E/\mathbb{Q}, s) = \Sigma_{n=1}^{\infty} a_1(n) n^{-s}, \ L(E_D/\mathbb{Q}, s) = \Sigma_{n=1}^{\infty} a_D(n) n^{-s},$$
$$L(E_{-D}/\mathbb{Q}, s) = \Sigma_{n=1}^{\infty} a_{-D}(n) n^{-s}$$

with coefficients $a_1(n), a_D(n), a_{-D}(n)$ respectively. Let

$$\Lambda(E/\mathbb{Q}, s) = (\frac{\sqrt{N_E}}{2\pi})^s \Gamma(s) L(E/\mathbb{Q}, s), \ \Lambda(E_D/\mathbb{Q}, s) = (\frac{\sqrt{N_{E_D}}}{2\pi})^s \Gamma(s) L(E_D/\mathbb{Q}, s),$$
$$\Lambda(E_{-D}/\mathbb{Q}, s) = (\frac{\sqrt{N_{E_{-D}}}}{2\pi})^s \Gamma(s) L(E_{-D}/\mathbb{Q}, s),$$

where N_E, N_{E_D} and $N_{E_{-D}}$ are the conductors of E, E_D and E_{-D}, respectively. Since these curves are modular over $\mathbb{Q}$, their $L-$functions have analytic continuation to $\mathbb{C}$ and satisfy functional equations (see [Sil1, p.362]):

$$\Lambda(E/\mathbb{Q}, 2 - s) = \omega_E \Lambda(E/\mathbb{Q}, s), \ \Lambda(E_D/\mathbb{Q}, 2 - s) = \omega_{E_D} \Lambda(E_D/\mathbb{Q}, s),$$
$$\Lambda(E_{-D}/\mathbb{Q}, 2 - s) = \omega_{E_{-D}} \Lambda(E_{-D}/\mathbb{Q}, s),$$

where $\omega_E, \omega_{E_D}, \omega_{E_{-D}} \in \{1, -1\}$ are the corresponding root numbers. Let χ_K and $\chi_{K'}$ be the quadratic Dirichlet characters associated to K and K', respectively. Then if $(d(K), 2N_E) = 1$, we have $L(E_D/\mathbb{Q}, s) = L(E/\mathbb{Q}, \chi_K, s)$ (see, e.g., [Kol1, p.524], [Kol2, p.475]). So $L(E/K, s) = L(E/\mathbb{Q}, s) \cdot L(E/\mathbb{Q}, \chi_K, s) = L(E/\mathbb{Q}, s) \cdot L(E_D/\mathbb{Q}, s)$ (see also [DFK, p.186]), from which their root numbers satisfy $\omega_{E/K} = \omega_{E/\mathbb{Q}} \cdot \omega_{E_D/\mathbb{Q}}$. Similar for $L(E_{-D}/\mathbb{Q}, s)$. We write
$L(E/\mathbb{Q}, \chi_K, s) = \Sigma_{n=1}^{\infty} a_1(n)\chi_K(n)n^{-s}$ with coefficients $a_1(n)\chi_K(n)$.

Lemma 5.1. Assume that $(D, 2pq) = 1$. Then for the above root numbers ω_E, ω_{E_D} and $\omega_{E_{-D}}$, we have
(1) if $D \equiv 1(\text{mod}4)$, then $\omega_{E_D} = \chi_K(-2pq)\omega_E$.
(2) if $D \equiv 3(\text{mod}4)$, then $\omega_{E_{-D}} = \chi_{K'}(-2pq)\omega_E$.

Proof. The discriminants of the quadratic number fields K and K' are

$$d(K) = \begin{cases} D & \text{if } D \equiv 1(\text{mod}4) \\ 4D & \text{if } D \equiv 3(\text{mod}4), \end{cases} \quad \text{and } d(K') = \begin{cases} -4D & \text{if } D \equiv 1(\text{mod}4) \\ -D & \text{if } D \equiv 3(\text{mod}4), \end{cases}$$

respectively. If $(d(K), N_E) = 1$, then $\omega_{E_D} = \chi_K(-N_E)\omega_E$, and if $(d(K'), N_E) = 1$, then $\omega_{E_{-D}} = \chi_{K'}(-N_E)\omega_E$ (see [DFK, p.186]). Note that $N_E = 2^5pq$, the conclusion follows. □

The curve $E/\mathbb{Q}$ in (1.1) above is 2−isogeny to the following elliptic curve

$$E' : \ y^2 = x^3 - 2\varepsilon(p+q)x^2 + 4x, \tag{5.2}$$

and the isogeny is as follows.
$\varphi : \ E \longrightarrow E', \ (x, y) \mapsto (x + \varepsilon(p+q) + pq \cdot x^{-1}, \ y - pqy \cdot x^{-2}).$
This will be used in the following calculation of the root numbers. Obviously, the conductor of $E'/\mathbb{Q}$ is $N_{E'} = N_E = 2^5pq$, and the discriminant is $\Delta_{E'} = 2^{12}pq$. Firstly, we need the following result.

Lemma 5.2. Let $E'/\mathbb{Q}$ be the elliptic curve in (5.2) above.
(1) At each prime $l \mid N_{E'}$, the Kodaira type is as follows:
I_3^* for $l = 2$, and I_1 for $l = p$ or q.
(2) The Tamagawa number $c_2 = 2$ or 4, more precisely,
$c_2 = 2$ if one of the following three hypotheses holds:
(a) $p \equiv 3(\text{mod}8)$; (b) $\varepsilon = 1$ and $p \equiv 1(\text{mod}8)$; (c) $\varepsilon = -1$ and $p \equiv 5(\text{mod}8)$.
$c_2 = 4$ if one of the following three hypotheses holds:

(a′) $p \equiv 7 (\mathrm{mod} 8)$; (b′) $\varepsilon = 1$ and $p \equiv 5 (\mathrm{mod} 8)$; (c′) $\varepsilon = -1$ and $p \equiv 1 (\mathrm{mod} 8)$.

(3) The Tamagawa numbers $c_p = c_q = 1$.

Proof. This is a consequence of direct calculation by the Algorithm of [Ta]. □

Now we come to calculate the root numbers.

Theorem 5.3. Let ω_E be the root number of the the elliptic curve $E/\mathbb{Q}$ in (1.1) above.

(1) If $\varepsilon = 1$, then $\omega_E = \begin{cases} 1 & \text{if } p \equiv 5, 7 \pmod 8 \\ -1 & \text{if } p \equiv 1, 3 \pmod 8); \end{cases}$

(2) If $\varepsilon = -1$, then $\omega_E = \begin{cases} 1 & \text{if } p \equiv 3, 5 \pmod 8 \\ -1 & \text{if } p \equiv 1, 7 \pmod 8). \end{cases}$

Proof. To begin with, from [Roh, p.122], we have $\omega_E = \prod_{l \leq \infty} \omega_l$, where $\omega_l = \pm 1$ is the local root number. And by Prop.1 in [Roh1, p.123] one has $\omega_\infty = -1$, so $\omega_E = -\prod_{l<\infty} \omega_l$. Since the conductor is $N_E = 2^5 pq$, for any prime number $l \neq 2, p, q, E$ has good reduction at l, so by Prop.2(iv) in [Roh, p.126], we have $\omega_l = 1$ for every such l. Also, since $E/\mathbb{Q}$ has multiplicative reduction at both p and q, by discussion in Lemma 2.1 above, and by Prop.3(iii) in [Roh, p.132], we have

(1) $\omega_p = \omega_q = 1$ if $\varepsilon = 1$ and $p \equiv 3, 5 \pmod 8$;

(2) $\omega_p = \omega_q = -1$ if $\varepsilon = 1$ and $p \equiv 1, 7 \pmod 8$;

(3) $\omega_p = -1,\ \omega_q = 1$ if $\varepsilon = -1$ and $p \equiv 1, 3 \pmod 8$;

(4) $\omega_p = 1,\ \omega_q = -1$ if $\varepsilon = -1$ and $p \equiv 5, 7 \pmod 8$.

So the remainder is the most difficult factor ω_2. To work out ω_2, from [D], one can obtain the following formula

$$\omega_2 = \sigma_\varphi(E/\mathbb{Q}_2) \cdot (\varepsilon(p+q), -pq)_{\mathbb{Q}_2} \cdot (-2\varepsilon(p+q), 4)_{\mathbb{Q}_2},$$

recall that $(,)_{\mathbb{Q}_2}$ is the Hilbert symbol (see [Se2, p.206]), φ is the isogeny in (5.2) above, and here,

$$\sigma_\varphi(E/\mathbb{Q}_2) = (-1)^{\mathrm{ord}_2(\frac{\sharp \mathrm{coker} \varphi_2}{\sharp \ker \varphi_2})} = (-1)^{1 + \mathrm{ord}_2 \sharp \mathrm{coker} \varphi_2},$$

where $\varphi_2 : E(\mathbb{Q}_2) \longrightarrow E'(\mathbb{Q}_2)$ is the local homomorphism induced by φ. Since $(,)_{\mathbb{Q}_2}$ is biadditive, we have $(-2\varepsilon(p+q), 4)_{\mathbb{Q}_2} = (-2\varepsilon(p+q), 2)^2_{\mathbb{Q}_2} = 1$, so $\omega_2 = \sigma_\varphi(E/\mathbb{Q}_2) \cdot (\varepsilon(p+q), -pq)_{\mathbb{Q}_2}$. To calculate $(\varepsilon(p+q), -pq)_{\mathbb{Q}_2}$, we consider the equation $\varepsilon(p+q)x^2 - pqy^2 = 1$. Let $f(x, y) = \varepsilon(p+q)x^2 - pqy^2 - 1$, then $\frac{\partial f}{\partial y}(x, y) = -2pqy$, and it is easy to see that $\mathrm{ord}_2(f(1, 1)) \geq 3 > 2 \cdot \mathrm{ord}_2(\frac{\partial f}{\partial y}(1, 1))$. So by Hensel's lemma (see [Sil1, p.322]), $f(x,y)$ has a root in $\mathbb{Q}_2\times\mathbb{Q}_2$, and so $(\varepsilon(p+q),-pq)_{\mathbb{Q}_2}=1$ (see [Weib, Examp.6.2.2, p.253]). Therefore,

$$\omega_2=\sigma_\varphi(E/\mathbb{Q}_2)=(-1)^{1+\mathrm{ord}_2\sharp\mathrm{coker}\varphi_2}.$$

To calculate the integer $\sharp\mathrm{coker}\varphi_2=\sharp(E'(\mathbb{Q}_2)/\varphi_2(E(\mathbb{Q}_2)))$, we use Lemma 3.8 of [Sc, pp.91, 92]. For this, let

$$z=-\frac{x}{y},\ \text{and}\ z'=-\frac{x+\varepsilon(p+q)+pqx^{-1}}{y-pqyx^{-2}}=-\frac{y}{x^2-pq}.$$

From the Chapter IV of [Sil1], one has $x=\frac{z}{w(z)}$ and $y=-\frac{1}{w(z)}$, where $w(z)=z^3(1+\varepsilon(p+q)z^2+\cdots)$. So

$$\begin{aligned}z'&=\frac{w(z)}{z^2-pqw(z)^2}=\frac{z^3(1+\varepsilon(p+q)z^2+\cdots)}{z^2-pqz^6(1+\varepsilon(p+q)z^2+\cdots)^2}\\&=z(1+\varepsilon(p+q)z^2+\cdots)\cdot(1+pqz^4(1+\varepsilon(p+q)z^2+\cdots)^2+\cdots)\\&=z+(\text{terms of higher degree}),\end{aligned}$$

i.e., the leading coefficient of z' is 1. So $|\varphi_2'(0)|_2^{-1}=1$ (see [Sc, p.92]), and so by Lemma 3.8 of [Sc, p.91], we get

$$\sharp\mathrm{coker}\varphi_2=\frac{|\varphi_2'(0)|_2^{-1}\cdot\sharp E(\mathbb{Q}_2)[\varphi_2]\cdot c_2(E')}{c_2(E)}=\frac{\sharp E(\mathbb{Q}_2)[\varphi_2]\cdot c_2(E')}{c_2(E)},$$

where $c_2(E)$ and $c_2(E')$ are the Tamagawa numbers of E and E' at 2, respectively, and $E(\mathbb{Q}_2)[\varphi_2]=\ker\varphi_2=\{O,(0,0)\}$. So by Lemma 2.1 and Lemma 5.2 above, we get $\sharp\mathrm{coker}\varphi_2=2$ or 4, that is,

$\sharp\mathrm{coker}\varphi_2=2$ if one of the following three hypotheses holds:

(a) $p\equiv 3(\mathrm{mod}8)$; (b) $\varepsilon=1$ and $p\equiv 1(\mathrm{mod}8)$; (c) $\varepsilon=-1$ and $p\equiv 5(\mathrm{mod}8)$.

$\sharp\mathrm{coker}\varphi_2=4$ if one of the following three hypotheses holds:

(a′) $p\equiv 7(\mathrm{mod}8)$; (b′) $\varepsilon=1$ and $p\equiv 5(\mathrm{mod}8)$; (c′) $\varepsilon=-1$ and $p\equiv 1(\mathrm{mod}8)$.

From this the value of $\sigma_\varphi(E/\mathbb{Q}_2)$ and hence ω_2 is obtained. The proof is completed. □

On the parity conjecture of some special $E/\mathbb{Q}$ in (1.1) above, we have

Corollary 5.4. Let $E/\mathbb{Q}$ be the elliptic curve in (1.1) above. If one of the following three hypotheses holds:

(1) $\varepsilon=1$ and $p\equiv 5\ (\mathrm{mod}\ 8)$;

(2) $\varepsilon = -1$ and $p \equiv 3, 5 \pmod 8$;
(3) $\varepsilon = 1$, $p \equiv 3 \pmod 8$ and $q = a_1^2 + a_2^2$ with $(a_1 + \varepsilon_1)^2 + (a_2 + \varepsilon_2)^2 = a_3^2$ for some rational integers $a_1, a_2, a_3 \in \mathbb{Z}$ and some $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$.
Then the parity conjecture is true for $E/\mathbb{Q}$, i.e., $\omega_E = (-1)^{\mathrm{rank}E(\mathbb{Q})}$.

Proof. For the cases (1) and (2), by Theorems 1 and 2 of [QZ1], we have $\mathrm{rank}E(\mathbb{Q}) = 0$, and for the case (3), by Theorem 3 of [QZ1], we have $\mathrm{rank}E(\mathbb{Q}) = 1$. Then the conclusion follows from Theorem 5.3 above. □

Remark. As pointed out by an anonymous referee, the result of these special $E/\mathbb{Q}$ in Cor.5.4 above also follows by Monsky's theorem on the 2-parity conjecture, because their Ш $(E/\mathbb{Q})[2]$ have been shown to be trivial in [QZ1, Theorems 1,2].

Theorem 5.5. Let $E/\mathbb{Q}$ be the elliptic curve in (1.1) and let $K = \mathbb{Q}(\sqrt{\mu D})$ be the quadratic number field with D in (1.2) and $\mu = \pm 1$. We assume that $D \equiv \mu \pmod 4$. Let $L(E/\mathbb{Q}, s) = \Sigma_{n=1}^{\infty} a_1(n) n^{-s}$ be the $L-$function as above. Let $E_{\mu D}/\mathbb{Q}$ be the quadratic $(\mu D)-$twist of $E/\mathbb{Q}$, and χ_K be the quadratic Dirichlet character associated to K.
(1) Assume one of the following two hypotheses holds:
(a) $\varepsilon = 1$ and $p \equiv 5, 7 \pmod 8$;
(b) $\varepsilon = -1$ and $p \equiv 3, 5 \pmod 8$.
Then $L(E/\mathbb{Q}, 1) = 2\Sigma_{n=1}^{\infty} \frac{a_1(n)}{n} e^{-n\pi/2\sqrt{2pq}}$.
further, for all integer $r \geq 0$,

$$L^{(r)}(E/\mathbb{Q}, 1) = 2\pi\Sigma_{n=1}^{\infty} a_1(n) \int_{1/4\sqrt{2pq}}^{\infty} [\log^r t + (-1)^r \log^r(2^5 pqt)] e^{-2n\pi t} dt. \text{ also,}$$

$$L(E_{\mu D}/\mathbb{Q}, 1) = (1 + \chi_K(-2pq)) \cdot \Sigma_{n=1}^{\infty} \frac{a_1(n)}{n} \chi_K(n) \cdot e^{-n\pi/2D\sqrt{2pq}},$$

In particular, if $\chi_K(-2pq) = -1$, then $L(E_{\mu D}/\mathbb{Q}, 1) = 0$.
(2) Assume one of the following two hypotheses holds:
(a′) $\varepsilon = 1$ and $p \equiv 1, 3 \pmod 8$;
(b′) $\varepsilon = -1$ and $p \equiv 1, 7 \pmod 8$.
Then $L(E/\mathbb{Q}, 1) = 0$,

further, for all integer $r \geq 0$,

$$L^{(r)}(E/\mathbb{Q},1) = 2\pi\Sigma_{n=1}^{\infty}a_1(n)\int_{1/4\sqrt{2pq}}^{\infty}[\log^r t + (-1)^{r+1}\log^r(2^5 pqt)]e^{-2n\pi t}dt. \text{ also,}$$

$$L(E_{\mu D}/\mathbb{Q},1) = (1-\chi_K(-2pq))\cdot\Sigma_{n=1}^{\infty}\frac{a_1(n)}{n}\chi_K(n)\cdot e^{-n\pi/2D\sqrt{2pq}}.$$

In particular, if $\chi_K(-2pq) = 1$, then $L(E_{\mu D}/\mathbb{Q},1) = 0$.

Proof. Since $E/\mathbb{Q}$ is modular (see [TW],[Wi],[BCDT]), the function $f_E(z) = \sum_{n=1}^{\infty} a_1(n)e^{2\pi inz}$ satisfies the Hecke equation $f_E(z) = -\omega_E N^{-1}z^{-2}f(-\frac{1}{Nz})$, and the differential $f_E(z)dz$ is invariant under the usual modular group $\Gamma_0(N)$, where $N = 2^5pq$ is the conductor, and ω_E is the root number of $E/\mathbb{Q}$. Also by assumption, the discriminant $d(K) = \mu D$ satisfying $(d(K), 2N_E) = 1$. So $L(E_{\mu D}/\mathbb{Q},1) = L(E/\mathbb{Q},\chi_K,1)$. Hence by Theorem 9.3 of [M, P.61], we have

$$L(E/\mathbb{Q},1) = (1+\omega_E)\Sigma_{n=1}^{\infty}\frac{a_1(n)}{n}e^{-2n\pi/\sqrt{N}},$$

$$L^{(r)}(E/\mathbb{Q},1) = 2\pi\Sigma_{n=1}^{\infty}a_1(n)\int_{1/\sqrt{N}}^{\infty}[\log^r t + \omega_E(-1)^r\log^r(Nt)]e^{-2n\pi t}dt,$$

$$L(E_{\mu D}/\mathbb{Q},1) = \Sigma_{n=1}^{\infty}\frac{a_1(n)}{n}[\chi_K(n) + \overline{\chi_K}(n)\cdot\frac{g(\chi_K)}{g(\overline{\chi_K})}\cdot\chi_K(-n)\cdot\omega_E]e^{-2n\pi/\sqrt{N}d(K)},$$

where $g(\chi_K) = \sum_{b \bmod d(K)}\chi_K(b)e^{2\pi ib/d(K)}$ is the Gaussian sum. Note that $\chi_K(n) = 0, \pm 1$ $(\forall n \in \mathbb{Z})$, so $\overline{\chi_K} = \chi_K$, and $g(\chi_K) = g(\overline{\chi_K})$. Then by our results about the root numbers in Lemma 5.1 and Theorem 5.3 above, the conclusion follows. □

Example 5.6. For the elliptic curves $E: y^2 = x(x+3\varepsilon)(x+5\varepsilon)$ and the field $K = \mathbb{Q}(\sqrt{-119})$, the conductor $N_E = 2^5\cdot 3\cdot 5 = 480$ and the discriminant $d(K) = -119$. By Theorem 5.3 above, the root number of $E/\mathbb{Q}$ is $\omega_E = -\varepsilon$. So for the $L-$function $L(E/\mathbb{Q},s)$, we have $L(E/\mathbb{Q},1) = 0$ in the case $\varepsilon = 1$. And in this case, the Mordell-Weil group $E(\mathbb{Q}) \cong \mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. For the other case $\varepsilon = -1$, $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ (see [QZ1, p.1373]), and by Theorem.5.5 above, $L(E/\mathbb{Q},1) = 2\Sigma_{n=1}^{\infty}\frac{a_1(n)}{n}e^{-n\pi/2\sqrt{30}}$. Moreover, $d(K) = -119 \equiv 61^2 \pmod{4N_E}$. So the Heegner hypothesis holds for E and K, and then there is a Heegner point $P_K \in E(K)$ such that $\sigma(2P_K) = -2\omega_E P_K$ (see [Kol3,4]) because $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, where σ is the generator of the Galois group $\text{Gal}(K/\mathbb{Q})$. Since $\omega_E = -\varepsilon$, we have $\sigma(2P_K) = 2\varepsilon P_K$. Now for any prime number $l > 37$, the Galois representation ρ_l is irreducible (see [Cha, p.175]). Also every such prime number l satisfies $l \nmid d(K), l^2 \nmid$

N_E, so by Cha's theorem in [Cha], we have $\mathrm{ord}_l \sharp Ш(E/K) \leq 2 \cdot \mathrm{ord}_l([E(K) : \mathbb{Z}P_K])$.
□

Remark

I thank the anonymous expert for pointing out that the result of Corollary 5.4 above also follows by Monsky's theorem on the 2-parity conjecture. Some further application toward verifying the BSD for a family of elliptic curves will be discussed in a separate paper.

Acknowledgments

I would like to thank the referee for helpful suggestions and comments.

Conflict of interest

The author has no conflict of interest.

References

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

[2] Bahargava, M. and Skinner, C. (2014). A positive proportion of elliptic curves over $\mathbb{Q}$ have rank one, arXiv: 1401.0233.

[3] Bahargava, M., Skinner, C., Zhang, W. (2014). A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture, arXiv: 1407.1826 v2.

[4] Cha, B. (2005). Vanishing of some cohomology groups and bounds for the Shafarevich-Tate groups of elliptic curves, *J. Number Theory*, **111**, 154-178.

[5] Dokchitser, T. (2012). Notes on the parity conjecture, arXiv: 1009.5389 v2.

[6] Dokchitser, T. and Dokchitser, V. (2009). Root numbers and parity of ranks of elliptic curves, arXiv: 0906.1815 v1.

[7] C.David, C., Fearnley, J., Kisilevsky, H. (2004). On the vanishing of twisted $L-$functions of elliptic curves, *Experimental Math.*, **13**, 185-198.

[8] Greenberg, R. (1999). Iwasawa theory for elliptic curves. In Arithmetic Theory of Elliptic Curves, Lecture Notes in Math., Vol.1716. New York: Springer-Verlag, 51-144.

[9] Greenberg, R. and Vatsal, V. (2000). On the Iwasawa invariants of elliptic curves, *Invent. math.*, **142**, 17-63.

[10] Knapp, A.W. (1992). Elliptic Curves, Mathematical Notes 40, Princeton: Princeton University Press.

[11] Kolyvagin, V.A. Finiteness of $E(\mathbb{Q})$ and Ш$(E/\mathbb{Q})$ for a subclass of Weil curves, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), 522-540, 670-671; translation in Math. USSR-Izv. 32 (1989), 523-541.

[12] Kolyvagin, V.A. The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), 1154-1180, 1327; translation in Math. USSR-Izv. 33 (1989), 473-499.

[13] Kolyvagin, V.A (1990). On the Mordell-Weil group and Shafarevich-Tate group of modular elliptic curves, *Proceedings of the international congress of mathematicians*, Kyoto, Japan, 429-436.

[14] Kramer, K. (1981). Arithmetic of elliptic curves upon quadratic extension, Transactions of the American Mathematical Society, **264**, 121-135.

[15] Kramer, K. and Tunnell, J. (1982). Elliptic curves and local $\varepsilon-$factors, *Compositio Math.*, **46**, 307-352.

[16] Kurihara, M. (2002). On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I, *Invent. math.*, 149, 195-224.

[17] Lang, S. (1994). Algebraic Number Theory, 2nd Edition, New York: Springer-Verlag.

[18] Li, F. and Qiu, D. R. (2010). On several families of elliptic curves with arbitrary large Selmer groups, *Science in China (series A)*, **53**, 2329-2340.

[19] Manin, J. I. (1971). Cyclotomic fields and modular curves, *Russian Math.* Surveys, **26**, 7-78.

[20] Mazur, B. (1978). Rational isogenies of prime degree (with an appendix by D.Goldfeld), *Invent. math.*, **44**, 129-162.

[21] Mazur, B. (1972). Rational points of Abelian varieties with values in towers of number fields, *Invent. math.*, **18**, 183-266.

[22] Mazur, B. and Rubin, K. (2010). Ranks of twists of elliptic curves and Hilbert's tenth problem, *Invent. math.*, **181**, 541-575.

[23] Mazur, B. and Swinnerton-Dyer, H. (1974). Arithmetic of Weil curves, *Invent. math.*, **25**, 1-61.

[24] Perrin-Riou, B. (2003). Arithmétique des courbes elliptiques à réduction supersingulière en p, *Experimental Math.*, **12**, 155-186.

[25] Qiu, D.R. 2014. On quadratic twists of elliptic curves and some applications of a refined version of Yu's formula, *Communications in Algebra*, **42**, 5050-5064.

[26] Qiu, D.R. (2015). On elliptic curves $y^2 = x(x + \varepsilon p)(x + \varepsilon q)$ and their twists, arXiv: 1511.07581 v1.

[27] Qiu, D.R. and Zhang, X.K. (2002). Mordell-Weil groups and Selmer groups of twin-prime elliptic curves, *Science in China (series A)*, **45**, 1372-1380.

[28] Qiu, D.R. and Zhang, X.K. (2001). Elliptic curves and their torsion subgroups over number fields of type $(2, \cdots, 2)$, *Science in China (series A)*, **44**, 159-167.

[29] Rohrlich, D.E. (1993). Variation of the root number in families of elliptic curves, *Compositio math.*, **87**, 119-151.

[30] Sands, J.W. (2004). Popescu's conjecture in multi-quadratic extensions, *Contemporary Math.*, **Vol.358**, 127-141.

[31] Schaefer, E.F. (1996). Class groups and Selmer groups, *J. Number Theory*, **56**, 79-114.

[32] Serre, J.P. (1972). Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.*, **15**, 259-331.

[33] Serre, J.P. (1979). Local fields, New York: Springer-Verlag, 1979.

[34] Silverman, J.H. (1986). The Arithmetic of Elliptic Curves, GTM 106, New York: Springer-Verlag.

[35] Silverman, J.H. (1999). Advanced topics in the Arithmetic of Elliptic Curves, GTM 151, New York: Springer-Verlag.

[36] Skinner, C. (2014). Multiplicative reduction and the cyclotomic main conjecture for Gl_2, arXiv: 1407.1093.

[37] Skinner, C. and Zhang, W. (2014). Indivisibility of Heegner points in the Multiplicative case. arXiv: 1407.1099.

[38] Stoll, M. (2006). Descent on elliptic curves, arXiv: 0611694 v1.

[39] Szymiczek, K. (1998). $2-$ranks of class groups of Witt equivalent number fields, *Annales Mathematicae Silesianae* **12**, 53-64. 1979.

[40] Tate, J. (1975). Algorithm for determing the type of a singular fiber in an elliptic pencil, in: Modular functions of one variable, IV, (Proc. Internat. Summer School, Univ. Antwerp 1972), pp.33-52. Lecture Notes in Math. **476**, Springer, Berlin.

[41] Taylor, R. and Wiles, A. (1995). Ring-theoretic properties of certain Hecke algebras, *Ann. Math.*, **141**, 553-572.

[42] Washington, L.C. (1997). Introduction to Cyclotomic Fields, 2nd Edition, New York: Springer-Verlag.

[43] Weibel, C.A. (2013). The K-Book, An Introduction to Algebraic K-Theory, AMS, Providence, Rhode Island.

[44] Wiles, A. (1995). Modular elliptic curves and Fermat's last theorem, *Ann. Math.*, **141**, 443-551.

[45] Zhang, W. (2014). Selmer groups and the Indivisibility of Heegner points, *Cambridge J. Math.*, **2**, 191-253.