Elliptic curves with all quartic twists of the same root number

By Dongho BYEON and Gyeoul HAN

Department of Mathematical Sciences, Seoul National University, Seoul 151-747, Korea.

(Communicated by Shigefumi MORI, M.J.A., Oct. 12, 2021)

Abstract: Let $E/K$ be an elliptic curve with $j$-invariant 1728 defined over a number field $K$. In this note, we give a simple condition on $K$ which determines whether all quartic twists of $E/K$ have the same root number or not. This completes a series of works on the same root number of twists begun in [DD1] and [BK].

Key words: Elliptic curve; quartic twist; root number.

1. Introduction and results. Let $K$ be a number field, $E/K$ an elliptic curve defined over $K$, and $L(E/K,s)$ its Hasse-Weil $L$-function defined for $\Re(s) > \frac{3}{2}$. Then $L(E/K,s)$ conjecturally satisfies a functional equation under $s \mapsto 2-s$ with the sign given by the (global) root number $w(E/K) = \pm 1$. The functional equation implies that $w(E/K) = (-1)^{\ord_v L(E/K,s)}$. The root number $w(E/K)$ is the product of the local root numbers over all places $v$ of $K$,

$$w(E/K) = \prod_v w(E/K_v).$$

It is well known that there are four types of twists of elliptic curves;

- **Quadratic twist.** For an elliptic curve $E/K : y^2 = x^3 + ax + b$ and $D \in K^\times/(K^\times)^2$, the quadratic twist of $E/K$ by $D$ is $E_D/K : y^2 = x^3 + aD^2x + bD^3$.

- **Cubic twist.** For an elliptic curve $E/K$ with $j$-invariant 0 defined by the equation $E/K : y^2 = x^3 + a$ and $D \in K^\times/(K^\times)^3$, the cubic twist of $E/K$ by $D$ is $E_D/K : y^2 = x^3 + aD^2$.

- **Quartic twist.** For an elliptic curve $E/K$ with $j$-invariant 1728 defined by the equation $E/K : y^2 = x^3 + ax + b$, the quadratic twist of $E/K$ by $D$ is $E_D/K : y^2 = x^3 + aDx$.

- **Sextic twist.** For an elliptic curve $E/K$ with $j$-invariant 1728 defined by the equation $E/K : y^2 = x^3 + ax + b$ and $D \in K^\times/(K^\times)^3$, the sextic twist of $E/K$ by $D$ is $E_D/K : y^2 = x^3 + aD$.

In [DD1], Dokchitser and Dokchitser give a sufficient and necessary condition on $E/K : y^2 = x^3 + ax + b$ that its quadratic twist $E_D/K : y^2 = x^3 + aD^2x + bD^3$ has the same root number for all $D \in K^\times/(K^\times)^2$. In [BK], using Kobayashi’s computation of root numbers in [Ko], Byeon and Kim prove that for $E/K : y^2 = x^3 + a$, its cubic twist $E_D/K : y^2 = x^3 + aD^2$ has the same root number for all $D \in K^\times/(K^\times)^3$ if and only if $\sqrt{-3} \in K$. It is easily seen that this condition is also applied to sextic twist.

The aim of this note is to give a simple condition on $K$ which determines whether all quartic twists of $E/K : y^2 = x^3 + ax$ have the same root number or not. This completes a series of works on the same root number of twists.

**Theorem 1.1.** Let $E/K$ be an elliptic curve with $j$-invariant 1728 defined by the equation $E/K : y^2 = x^3 + ax$, where $a \in K^\times$. For an element $D \in K^\times/(K^\times)^4$, let $E_D : y^2 = x^3 + aDx$ be the quartic twist of $E$. Then the root number $w(E_D/K)$ is constant for all $D \in K^\times/(K^\times)^4$ if and only if $\sqrt{-1} \in K$. In particular, if $K$ contains $\sqrt{-1}$, then $w(E_D/K) = +1$ for all $D \in K^\times/(K^\times)^4$, and if $K$ does not contain $\sqrt{-1}$, then there are infinitely many $E_D/K$ such that $w(E_D/K) = +1$, and $w(E_D/K) = -1$, respectively.

Remark. Várrilly-Alvarado [Vá] and Desjardins [De] consider the behaviour of the root number in the family given by the twists of an elliptic curve $E/Q$ by the rational values of a polynomial $f(T)$ and present a criterion for the family to have a constant root number over $Q$.

2. Preliminaries. To prove Theorem 1.1, we need the following propositions. Before we state them, we introduce some notation for a place $v$ of $K$ above 2.

$K_v$: a local field with respect to a place $v|2$,

$L = K_v(E[3])$,
there are two possible Galois groups (see [DD, Proposition 2]). Since \( \Delta \in (K^\times)^3 \), \( \mu_3 \not\subset K_v \) is equivalent to the condition that \( x^3 - 12^2 \Delta = x^3 + (48a)^3 \) has exactly one root. And we find that the root is \( \delta = -48a = c_4 \). Therefore it follows that \(-3(c_4 - \delta) = 0\) is a square and \(-3(c_2^2 + c_6 \delta + \delta^2) = -3^2(48a)^2\) is a square if and only if \( \mu_4 \subset K_v \). From [DD, Lemma 3], one may verify that this is equivalent to \( G = C_3 \). Hence Proposition 2.1 follows from [DD, Proposition 2].

**Proposition 2.2.** Let \( K_v \) be a local field at a place \( v \mid 2 \). Let \( E/K \) be an elliptic curve with \( j \)-invariant 1728 defined by the equation \( E/K : y^2 = x^3 + ax \).

(a) If \( \mu_4 \subset K_v \), then \( G = C_2 \times C_2 \), \( C_4 \), or \( C_8 \). In particular, \( G \) is abelian.

(b) If \( \mu_4 \not\subset K_v \), then \( G = C_2 \times C_2 \times C_3 \), \( C_4 \times C_3 \), or \( C_8 \). In particular, \( G \) is not abelian except for the case that \( G = C_2 \times C_2 \) when \( (\deg \gamma)_3 = (2, 2, 4) \).

**Proof.** (a) Suppose that \( \mu_4 \subset K_v \). If \( \mu_3 \subset K_v \), then \( \sqrt{3} \in K_v \), so \( \gamma(x) \) is reducible over \( K_v \) and its factorization is

\[
\gamma(x) = (x^4 + 144a - 96a\sqrt{3}) \\
\times (x^4 + 144a + 96a\sqrt{3}).
\]

Hence \( G = C_2 \) or \( C_4 \) from Proposition 2.1. If \( \mu_3 \not\subset K_v \), then \( \gamma(x) \) is irreducible. From Proposition 2.1, we obtain \( G = C_8 \).

(b) Suppose that \( \mu_4 \not\subset K_v \) and \( \sqrt{3} \in K_v \). Then \( \mu_3 \not\subset K_v \) but \( \gamma(x) \) is reducible over \( K_v \), factoring as (1).

If both factors of \( \gamma(x) \) in (1) are irreducible, then we have \( G = D_8 \) from Proposition 2.1. If \( \gamma(x) \) has an irreducible factor of degree 2, then the possible \( G \) is only \( C_2 \times C_2 \) when \( (\deg \gamma)_3 = (2, 2, 4) \) from Proposition 2.1. Suppose that \( \mu_4 \not\subset K_v \) and \( \sqrt{3} \notin K_v \). Then \( \gamma(x) \) is irreducible. So we have \( G = Q_8 \) when \( \mu_3 \subset K_v \) or \( H_{16} \) when \( \mu_3 \not\subset K_v \) from Proposition 2.1.

\( \square \)

**3. Proof of Theorem 1.1.** Now we can prove Theorem 1.1.

**Proof of Theorem 1.1.** In [Će, Proposition 6.3], Česnaviačius proved that if \( \sqrt{-1} \notin K \), then any elliptic curve with \( j \)-invariant 1728 over \( K \) has root number 1. Now we will show that the structure of \( G \) prevent this in the case that \( \sqrt{-1} \notin K \). We will use the fact that there are infinitely many principal prime ideals (of residue class degree 1) in \( K \), which follows from the Frobenius density theorem.

Assume that \( \sqrt{-1} \notin K \). Since the factorization of \( \gamma(x) \) over \( K \) is following

\[
\gamma(x) = (x^2 + 4 \sqrt{-1} \cdot \sqrt{a} \cdot \sqrt{9 - 6\sqrt{3}}) \\
\times (x^2 - 4 \sqrt{-1} \cdot \sqrt{a} \cdot \sqrt{9 + 6\sqrt{3}}) \\
\times (x^2 + 4 \sqrt{-1} \cdot \sqrt{a} \cdot \sqrt{9 + 6\sqrt{3}}) \\
\times (x^2 - 4 \sqrt{-1} \cdot \sqrt{a} \cdot \sqrt{9 + 6\sqrt{3}}),
\]

we may find infinitely many principal prime ideals \( \pi(n) \) \((n \in \mathbb{N})\) of \( K \) such that \( (\deg \gamma_{\pi(n)}) \neq (2, 2, 4) \) for a place \( v|2 \), where \( \gamma_{\pi(n)}(x) = x^3 + 288a_\pi n x^4 - 6912a^2 \pi^2 \). Then \( G \) for \( E_{\pi(n)}/K_v \) is not abelian by Proposition 2.2 (b). So \( E_{\pi(n)}/K_v \) is chaotic and \( E_{\pi(n)}/K \) is also chaotic, which means that there is an \( a_\alpha \in K^\times/(K^\times)^2 \) such that \( w(E_{\pi(n)}a_\alpha/K) = w(E_{\pi(n)}/K) \) (see [DD1]). We note that no \( a_\pi \), \( a_\pi^2 \), \( a_\pi a_\alpha \), \( a_\pi a_\alpha^2 \) \((n \neq m \in \mathbb{N})\) are congruent
to each other modulo \((K^\times)^4\). This completes the proof.

**Acknowledgments.** The authors thank the referees for their careful readings and many valuable suggestions.

The authors were supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2020R1F1A1A01053449).

**References**


