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 $s \leftrightarrow 2-s$ with the sign given by the (global) root number $w(E/K) = \pm 1$. The functional equation implies that $w(E/K) = (-1)^{\mathrm{ord}_{s=1} L(E/K,s)}$. 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 $E/K : y^2 = x^3 + ax$ and $D \in K^\times/(K^\times)^4$, the quartic 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 0 defined by the equation $E/K : y^2 = x^3 + a$ and $D \in K^\times/(K^\times)^6$, 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. Várilly-Alvarado [Vá] and Desjardins [De] consider the behaviour of the root number in the family given by the twists of an elliptic curve $E/\mathbf{Q}$ by the rational values of a polynomial $f(T)$ and present a criterion for the family to have a constant root number over $\mathbf{Q}$.

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 $v|2$,
$L = K_v(E[3])$,

2020 Mathematics Subject Classification. Primary 11G05; Secondary 11G07.

doi: 10.3792/pjaa.97.014

Table

$\mu_3 \subset K_v$		$\mu_3 \not\subset K_v$	
$(\deg\gamma_i)_i$	G	$(\deg\gamma_i)_i$	G
$(2,2,2,2)$	C_2	$(2,2,4)$	$C_2 \times C_2$
$(4,4)$	C_4	$(4,4)$	D_8
(8)	Q_8	(8)	$\begin{cases} C_8 & \text{if } \mu_4 \subset K_v \\ H_{16} & \text{if } \mu_4 \not\subset K_v \end{cases}$

$G = \mathrm{Gal}(L/K_v)$,
$\gamma(x) = x^8 + 288ax^4 - 6912a^2$,
$(\deg\gamma_i)_i$: the tuple of degrees of irreducible factors of $\gamma(x) = \prod_i \gamma_i(x)$ over K_v,
$\mu_m \subset \bar{K}_v$: the set of m-th roots of unity.

Proposition 2.1. *Let K_v be a local field at a place $v|2$. Let E/K be an elliptic curve with j-invariant 1728 defined by the equation $E/K : y^2 = x^3 + ax$. Then the structure of G is given by the above table.*

Here, C_m is the cyclic group of order m, D_8 is the dihedral group of order 8, Q_8 is the quaternion group of order 8, and H_{16} is the 2-Sylow subgroup of $GL_2(\mathbf{Z}/3\mathbf{Z})$.

Proof. The elliptic curve E/K has potentially good reduction because its j-invariant is integral (see [Si, p. 197, Proposition 5.5]) and additive reduction because $\Delta = (-4a)^3$, $c_4 = -48a$, $c_6 = 0$. Since $\Delta \in (K_v^\times)^3$, G is determined by whether $\mu_3 \subset K_v$ or not and what the irreducible factors of $\gamma(x) = x^8 + 288ax^4 - 6912a^2$ are (see [DD, Proposition 2]).

When $\mu_3 \not\subset K_v$ and $\gamma(x)$ is irreducible, there are two possible Galois groups (see [DD, Proposition 2]). Since $\Delta \in (K_v^\times)^3$, $\mu_3 \not\subset K_v$ is equivalent to the condition that $x^3 - 12^3\Delta = x^3 + (48a)^3$ 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 $-3(c_4^2 + c_4\delta + \delta^2) = -3^2(48a)^2$ is a square if and only if $\mu_4 \subset K_v$. From [DD, Lemma 3], one may verify that this is equivalent to $G = C_8$. Hence Proposition 2.1 follows from [DD, Proposition 2]. □

Proposition 2.2. *Let K_v be a local field at a place $v|2$. 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 $G = C_2$, C_4, or C_8. In particular, G is abelian.
(b) If $\mu_4 \not\subset K_v$, then $G = C_2 \times C_2$, D_8, Q_8, or H_{16}. In particular, G is not abelian except for the case that $G = C_2 \times C_2$ when $(\deg\gamma_i)_i = (2,2,4)$.

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

$$\gamma(x) = (x^4 + 144a - 96a\sqrt{3}) \times (x^4 + 144a + 96a\sqrt{3}). \tag{1}$$

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 $(\deg\gamma_i)_i = (2,2,4)$ 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. □

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

Proof of Theorem 1.1. In [Če, Proposition 6.3], Česnavičius proved that if $\sqrt{-1} \in K$, 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 $\bar{K}$ is following

$$\begin{aligned}\gamma(x) = &\left(x^2 + 4\cdot\sqrt{-1}\cdot\sqrt{a}\cdot\sqrt{9 - 6\sqrt{3}}\right)\\ &\times\left(x^2 - 4\cdot\sqrt{-1}\cdot\sqrt{a}\cdot\sqrt{9 - 6\sqrt{3}}\right)\\ &\times\left(x^2 + 4\cdot\sqrt{-1}\cdot\sqrt{a}\cdot\sqrt{9 + 6\sqrt{3}}\right)\\ &\times\left(x^2 - 4\cdot\sqrt{-1}\cdot\sqrt{a}\cdot\sqrt{9 + 6\sqrt{3}}\right),\end{aligned}$$

we may find infinitely many principal prime ideals (π_n) $(n \in \mathbf{N})$ of K such that $(\deg\gamma_{\pi_n \mathrm{i}})_\mathrm{i} \neq (2,2,4)$ for a place $v|2$, where $\gamma_{\pi_n}(x) = x^8 + 288a\pi_n x^4 - 6912a^2{\pi_n}^2$. Then G for E_{π_n}/K_v is not abelian by Proposition 2.2 (b). So E_{π_n}/K_v is chaotic and E_{π_n}/K is also chaotic, which means that there is a $\alpha_n \in K^\times/(K^\times)^2$ such that $w(E_{\pi_n{\alpha_n}^2}/K) = -w(E_{\pi_n}/K)$ (see [DD1]). We note that no $a\pi_n$, $a\pi_m$, $a\pi_n{\alpha_n}^2$, $a\pi_m{\alpha_m}^2$ $(n \neq m \in \mathbf{N})$ are congruent to each other modulo $(K^\times)^4$. This completes the proof. $\square$

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

[BK] D. Byeon and N. Kim, Elliptic curves with all cubic twists of the same root number, J. Number Theory **136** (2014), 22–27.

[Če] K. Česnavičius, The p-parity conjecture for elliptic curves with a p-isogeny, J. Reine Angew. Math. **719** (2016), 45–73.

[De] J. Desjardins, Root number of twists of an elliptic curve, J. Théor. Nombres Bordeaux **32** (2020), no. 1, 73–101.

[DD] T. Dokchitser and V. Dokchitser, Root numbers of elliptic curves in residue characteristic 2, Bull. Lond. Math. Soc. **40** (2008), no. 3, 516–524.

[DD1] T. Dokchitser and V. Dokchitser, Elliptic curves with all quadratic twists of positive rank, Acta Arith. **137** (2009), no. 2, 193–197.

[Ko] S. Kobayashi, The local root number of elliptic curves with wild ramification, Math. Ann. **323** (2002), no. 3, 609–623.

[Si] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, 106, Springer, Dordrecht, 2009.

[Vá] A. Várilly-Alvarado, Density of rational points on isotrivial rational elliptic surfaces, Algebra Number Theory **5** (2011), no. 5, 659–690.