CHANGE OF ROOT NUMBERS OF ELLIPTIC CURVES UNDER EXTENSION OF SCALARS

MARIA SABITOVA

Abstract. In this paper we study how the root number attached to an elliptic curve E over a finite field extension K of $\mathbb{Q}_3$ changes when E is considered as an elliptic curve over a finite Galois extension F of K via extension of scalars. The main result is a formula relating the root number $W(E/F)$ attached to $E \times_K F$ to the root number $W(E/K)$ attached to E.

Introduction

Let K be a finite field extension of $\mathbb{Q}_p$ with a fixed algebraic closure $\overline{K}$ and let $F \subset \overline{K}$ be a finite field extension of K. The main goal of the paper is to relate the root number $W(E/K)$ attached to an elliptic curve E over K to the root number $W(E/F)$ attached to elliptic curve $E \times_K F$ over F obtained from E via extension of scalars.

Explicit formulas for $W(E/K)$ in terms of the coefficients of an arbitrary generalized Weierstrass equation of E have been obtained by D. Rohrlich [6] in the case when E has potential multiplicative reduction over K and under the additional assumption $p \geq 5$ in the case when E has potential good reduction over K. Thus Rohrlich's formulas can be used to calculate $W(E/F)$ using an arbitrary Weierstrass equation of E over K. In the case $p = 3$ formulas for $W(E/K)$ were obtained by S. Kobayashi [4] in terms of the coefficients of a minimal Weierstrass equation of E over K, so in order to apply Kobayashi's formulas to calculate $W(E/F)$ one needs to find a minimal Weierstrass equation of E over F. Our motivation is to calculate $W(E/F)$ using a Weierstrass equation of E over K. The cases $p = 2$ or 3, E has potential good reduction over K, and F is an arbitrary finite field extension of K still remain untreated in full generality. We answer the question when $p = 3$ under an additional assumption that F is Galois over K.

Assume E has potential good reduction over K and $F \subset \overline{K}$ is a finite field extension of K. By definition, the root number $W(E/K)$ is the root number of representation σ_E of the Weil group $\mathcal{W}(\overline{K}/K)$ of K attached to E. It is known that σ_E is a two-dimensional semisimple representation of $\mathcal{W}(\overline{K}/K)$. If σ_E is not irreducible, then one can easily deduce from well-known formulas that

$$W(E/F) = W(E/K)^{[F:K]}$$

Date: July 2, 2013.

Supported by NSF grant DMS-0901230 and by grants 60091-40 41, 64620-00 42 from The City University of New York PSC-CUNY Research Award Program.

(see e.g., [6], p. 128).

If σ_E is irreducible and p is odd (i.e., $p \neq 2$), then σ_E is induced by a multiplicative character of a quadratic extension $H \subset \overline{K}$ of K. Moreover, E has the Kodaira–Néron type III, III^*, II, IV, IV^*, or II^* (see Proposition 1.6 below). Furthermore,

- $H = K(\sqrt{-1})$ if E is of type III or III^*,
- $H = K(\Delta^{1/2})$ if E is of type II, IV, IV^*, or II^*, where Δ is a discriminant of E .

The main results of the paper together with easy cases, which we include for the sake of completeness, can be summarized in the following

Theorem. *Let $F \subset \overline{K}$ be a finite field extension of K with ramification index $e(F/K)$ over K. Suppose p is odd, E has potential good reduction over K, and σ_E is irreducible.*

- *If $H \subseteq F$, then*

$$W(E/F) = \left(\frac{-1}{\hat{K}}\right)^{\delta}, \quad \delta = \begin{cases} \frac{[F:K]}{2}, & \text{if } H/K \text{ ramified,} \\ 0, & \text{if } H/K \text{ unramified,} \end{cases}$$

where $\hat{K}$ denotes the residue field of K and $\left(\frac{x}{\hat{K}}\right)$ is the quadratic residue symbol of $x \in \hat{K}$ (Lemma 2.1 below).

- *If $H \not\subseteq F$, $p \geq 5$, then*

$$W(E/F) = (-1)^{\alpha+[F:K]} W(E/K)^{[F:K]},$$

where

$$\alpha = \begin{cases} 0, & \text{if } \varepsilon \mid e(F/K), \\ 1, & \text{otherwise,} \end{cases}$$

and ε denotes the ramification index of a minimal extension of K over which E has good reduction (Lemma 2.2 below).

- *If $H \not\subseteq F$, $p = 3$, F is Galois over K, and $e(H/K) = 1$, then*

$$W(E/F) = (-1)^{1+[F:K]} W(E/K)^{[F:K]}$$

(Proposition 3.1 below).

- *If $H \not\subseteq F$, $p = 3$, F is Galois over K, $e(H/K) = 2$, and $e(F/K)$ is even, then*

$$W(E/F) = (-1)^{1+\frac{e(F/K)}{2} f(F/\mathbb{Q}_3)},$$

where $f(F/\mathbb{Q}_3)$ is the residual degree of F over $\mathbb{Q}_3$ (Proposition 4.1 below).

- *If $H \not\subseteq F$, $p = 3$, F is Galois over K, $e(H/K) = 2$, and $e(F/K)$ is odd, then*

$$W(E/F) = (-1)^{1+[F:K]+af(F/\mathbb{Q}_3)} W(E/K)^{[F:K]},$$

where

$$a = \begin{cases} \frac{e_t-1}{2}, & \text{if } e_t \equiv 1 \bmod 3 \\ \frac{e_t+1}{2}, & \text{if } e_t \equiv 2 \bmod 3 \end{cases} = \begin{cases} \text{odd}, & \text{if } e_t \equiv 5 \text{ or } 7 \bmod 12 \\ \text{even}, & \text{if } e_t \equiv 1 \text{ or } 11 \bmod 12, \end{cases}$$

and e_t denotes the ramification index of the maximal tamely ramified extension of K contained in F (Theorem 4.3 below).

The paper is organized in the following way: Section 1 contains a list of general facts and notation used in the paper. Section 2 contains general formulas for $W(E/F)$ and the cases $H \subseteq F$ and $p \geq 5$. Section 3 treats the case when H is unramified over K, whereas Sections 4 and 5 treat the case when H is ramified over K. Finally, Section 6 contains specific examples showing that our formula for $W(E/F)$ becomes more complicated without the assumption that F is Galois over K.

1. Notation and general facts

1.1. **The base field and characters.** In what follows K is a local non-archimedean field of characteristic zero with ring of integers $\mathcal{O}_K$, maximal ideal $\mathfrak{p}_K \subset \mathcal{O}_K$, a uniformizer ϖ_K, and residue field $\hat{K}$ of characteristic p and cardinality q. Equivalently, K is a finite field extension of $\mathbb{Q}_p$. Let $\overline{K}$ be a fixed algebraic closure of K and we fix a valuation on K satisfying $\mathrm{val}_K\, \varpi_K = 1$. We denote by $\mathfrak{D}(K/\mathbb{Q}_p)$ the absolute different of K. If $F \subset \overline{K}$ is a finite field extension of K, then $e(F/K)$ and $f(F/K)$ denote the ramification index and the residual degree of F over K, respectively.

We call a continuous non-trivial homomorphism $\psi : K \longrightarrow \mathbb{C}^\times$ of absolute value 1 *an (additive) character of* K and we call a continuous homomorphism $\mu : K^\times \longrightarrow \mathbb{C}^\times$ *a (multiplicative) character of* $K^\times$. For an additive character ψ of K we denote by $n(\psi)$ the largest integer n such that ψ is trivial on $\varpi_K^{-n}\mathcal{O}_K$.

Let $\Phi_K \in \mathrm{Gal}(\overline{K}/K)$ be a preimage of the (arithmetic) Frobenius automorphism of the absolute Galois group of the residue field of K under the decomposition map, so that Φ_K is an arithmetic Frobenius of $\mathrm{Gal}(\overline{K}/K)$. We will call Φ_K simply *a Frobenius of* $\mathrm{Gal}(\overline{K}/K)$. By definition, the Weil group $\mathcal{W}(\overline{K}/K)$ (also denoted by $\mathcal{W}_K$) of K is a subgroup of $\mathrm{Gal}(\overline{K}/K)$ equal to $\mathrm{Gal}(\overline{K}/K^{unr}) \rtimes \langle\Phi_K\rangle$, where $K^{unr} \subset \overline{K}$ denotes the maximal unramified extension of K contained in $\overline{K}$, $\langle\Phi_K\rangle$ denotes the infinite cyclic group generated by Φ_K, and $I_K = \mathrm{Gal}(\overline{K}/K^{unr})$ is the inertia group of K. Throughout the paper we will identify one-dimensional complex continuous representations of $\mathcal{W}(\overline{K}/K)$ with characters of $K^\times$ via the local class field theory assuming that a uniformizer ϖ_K of K corresponds to an arithmetic Frobenius Φ_K of $\mathrm{Gal}(\overline{K}/K)$. We also denote by $\chi_{H/K}$ the quadratic character of $K^\times$ with kernel $N_{H/K}(H^\times)$ or, equivalently, $\chi_{H/K}$ is the one-dimensional representation of $\mathcal{W}(\overline{K}/K)$ of order 2 with kernel $\mathcal{W}(\overline{K}/H)$.

Lemma 1.1. *Let P be a local non-archimedean field of characteristic zero and let Q be a ramified quadratic extension of P. Suppose μ is a character of $Q^\times$ such that $\mu|_{P^\times} = \chi_{Q/P}$. Then either $a(\mu) = 1$ or $a(\mu)$ is positive and even.*

Proof. Since $a(\mu) \neq 0$, assume $a(\mu) = 2m+1$ for some $m \neq 0$. Since Q is ramified over P, $\mathcal{O}_Q = \mathcal{O}_P[\varpi_Q]$ for a uniformizer ϖ_Q of Q such that $\varpi_Q^2 \in \mathcal{O}_P$. Let $y = 1 + x\varpi_Q^{2m}$, $x \in \mathcal{O}_Q$.

Then $x = a + b\varpi_Q$ for $a, b \in \mathcal{O}_P$, $y = 1 + a\varpi_Q^{2m} + b\varpi_Q^{2m+1}$, and $\mu(y) = \chi_{Q/P}(1 + a\varpi_Q^{2m}) = 1$, since $a(\chi_{Q/P}) = 1$. Thus μ is trivial on $1 + \mathfrak{p}_Q^{2m}$, which contradicts $a(\mu) = 2m + 1$. □

Lemma 1.2. *Let P be a local non-archimedean field of characteristic zero and let Q be a tamely ramified Galois extension of P. Let μ be a complex continuous one-dimensional representation of $\mathcal{W}_P$ and let ν be the restriction of μ to $\mathcal{W}_Q$ (denoted by $\operatorname{Res}_P^Q \mu$). If $a(\mu) > 1$, then*

$$a(\nu) = (a(\mu) - 1)e_t + 1. \tag{1.1}$$

Proof. Let N be a finite Galois extension of P such that $\operatorname{Gal}(\overline{P}/N^{unr})$ is contained in the kernel of μ. Since $a(\mu) > 1$, $a(\mu^k) = a(\mu)$ for any k not divisible by residual characteristic p of P. Thus without loss of generality we can assume that $A = \operatorname{Gal}(N^{unr}/P^{unr})$ is a p-group and hence $N^{unr} \cap Q^{unr} = P^{unr}$. Let $T = Q^{unr}N^{unr}$, $B = \operatorname{Gal}(T/P^{unr})$, $C = \operatorname{Gal}(T/Q^{unr})$, where $C \cong A$. Then $a(\mu) = 1 + \frac{1}{e_t}\alpha$, where α depends on whether μ is trivial on the higher ramification groups B_i's of B, $i \geq 1$. On the other hand, $a(\nu) = 1 + \beta$, where β depends on whether μ is trivial on the higher ramification groups C_i's of C, $i \geq 1$. Since $C_i = C \cap B_i = B_i$, we have $\alpha = \beta$ and hence (1.1). □

Lemma 1.3 ([8], p. 316, Prop. 1)**.** *Let P be a local non-archimedean field of characteristic zero and let Q be a quadratic extension of P. Assume μ is a complex continuous one-dimensional representation of $\operatorname{Gal}(\overline{P}/Q)$. The representation of $\operatorname{Gal}(\overline{P}/P)$ induced by μ (denoted by $\operatorname{Ind}_P^Q \mu$) is irreducible and symplectic if and only if $\mu|_{P^\times} = \chi_{Q/P}$ and $\mu^2 \neq 1_Q$. Also, a complex continuous finite-dimensional representation of $\operatorname{Gal}(\overline{P}/P)$ is dihedral (i.e., two-dimensional orthogonal and irreducible) if and only if it has the form $\operatorname{Ind}_P^Q \mu$ for a quadratic extension Q of P and a character μ of $Q^\times$ satisfying $\mu|_{P^\times} = 1_P$ and $\mu^2 \neq 1_Q$.*

1.2. **Root numbers.** Suppose dx is a Haar measure on K, ψ is a (additive) character of K, π is a complex continuous finite-dimensional representation of $\mathcal{W}(\overline{K}/K)$, and $\epsilon(\pi, \psi, dx)$ is the corresponding epsilon factor. The root number W of π is defined as

$$W(\pi, \psi) = \frac{\epsilon(\pi, \psi, dx)}{|\epsilon(\pi, \psi, dx)|}.$$

It follows from a property of the epsilon factors that the root number does not depend on the choice of dx (see e.g., [7], Proposition on p. 143).

Given an elliptic curve E over K and a finite field extension $F \subset \overline{K}$ of K we are interested in calculating the root number $W(E/F)$ of elliptic curve $E \times_K F$ obtained from E via extension of scalars. Our goal is to express $W(E/F)$ in terms of $W(E/K)$ and F. We are particularly interested in the case when E has potential good reduction over K. Let l be a rational prime different from p, let $T_l(E)$ be the l-adic Tate module of E, and let σ_E denote the (2-dimensional) complex representation of $\mathcal{W}(\overline{K}/K)$ associated to the representation $\sigma_{E,l,\imath}$ of $\operatorname{Gal}(\overline{K}/K)$ on $(T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l)^* \otimes_\imath \mathbb{C}$, where $\imath$ is an embedding of $\mathbb{Q}_l$ into $\mathbb{C}$. It is known that the isomorphism class of $\sigma_{E,l,\imath}$ does not depend on the choice of l and $\imath$. Furthermore, σ_E is the restriction of $\sigma_{E,l,\imath}$ to $\mathcal{W}(\overline{K}/K)$. By definition,

$$W(E/K) = W(\sigma_E)$$

and hence $W(E/F) = W(\operatorname{Res}^F_K \sigma_E)$, where $\operatorname{Res}^F_K \sigma_E$ denotes the restriction of σ_E to $\mathcal{W}(\overline{K}/F)$. Let ω denote the unramified one-dimensional representation of $\mathcal{W}(\overline{K}/K)$ satisfying

$$\omega(\Phi_K) = q.$$

By properties of root numbers,

$$W(\sigma_E) = W(\sigma_E \otimes \omega^{1/2}) = W(\sigma),$$

where $\sigma = \sigma_E \otimes \omega^{1/2}$ is symplectic and hence $W(\sigma)$ does not depend on the choice of a character of K (see e.g., [7], Proposition on p. 150).

Lemma 1.4 ([8], p. 319, Prop. 3)**.** *Let P be a local non-archimedean field of characteristic zero and let Q be the unramified quadratic extension of P. Assume μ is a character of $Q^\times$ such that $\mu|_{P^\times} = \chi_{Q/P}$. If ψ_P is a character of P and $\psi_Q = \psi_P \circ \operatorname{Tr}_{Q/P}$, then*

$$W(\mu, \psi_Q)W(\operatorname{Ind}^Q_P 1_Q, \psi_P) = W(\mu, \psi_Q)W(\chi_{Q/P}, \psi_P) = (-1)^{a(\mu)}\mu(u_{Q/P}),$$

where $u_{Q/P} \in \mathcal{O}_Q^\times$ is any element such that $Q = P(u_{Q/P})$ and $u_{Q/P}^2 \in P$.

Remark 1.5. Note that $\mu(u_{Q/P})$ does not depend on the choice of $u_{Q/P}$. Indeed, let $v \in \mathcal{O}_Q^\times$ satisfy $v^2 \in P$ and $Q = P(v)$. This implies $u_{Q/P} = \alpha v$ for $\alpha \in \mathcal{O}_P^\times$. Thus

$$\mu(u_{Q/P}) = \mu(\alpha)\mu(v) = \chi_{Q/P}(\alpha)\mu(v) = \mu(v),$$

since $\chi_{Q/P}$ is unramified.

1.3. **Elliptic curves.** Throughout this subsection we assume that E has potential good reduction over K. The next proposition due to S. Kobayashi provides a criterion of irreducibility of σ_E in terms of the Kodaira–Néron type and discriminant $\Delta \in K$ of a Weierstrass equation of E.

Proposition 1.6 ([4], p. 613, Prop. 3.2)**.** *Suppose p is odd.*

- *If E is of type I_0 or I_0^*, then σ_E is not irreducible.*
- *If E is of type III or III^*, then σ_E is irreducible if and only if $\left(\frac{-1}{\hat{K}}\right) \neq 1$.*
- *If E is of type II, IV, IV^*, or II^*, then σ_E is irreducible if and only if $\Delta^{1/2} \notin K$.*

For the rest of this subsection we assume that $p = 3$, E has potential good reduction over K, and σ_E is irreducible. Let $\Delta \in K$ denote a fixed discriminant of E, let $\Delta^{1/4}$ be an arbitrary fixed 4-th root of Δ, $N = K(\Delta^{1/4}, E[2])$, $H = K(\Delta^{1/2})$, $M = K(E[2])$, and $S = K(\Delta^{1/4})$. It is known that $H \subset M$, M is a finite Galois extension of K with $\operatorname{Gal}(M/K)$ being isomorphic to a subgroup of the symmetric group S_3 on 3 letters, $N^{unr} = K^{unr}(\Delta^{1/4}, E[2])$ is a finite Galois extension of K^{unr}, and N^{unr} is the minimal extension of K^{unr} over which E has good reduction ([5], p. 362). In particular, σ_E is trivial on I_N by the criterion of Néron-Ogg-Shafarevič. Suppose σ_E is wildly ramified. Then H

is a quadratic extension of K and $\mathrm{Gal}(M/K) \cong S_3$. Moreover, if H is unramified over K, then $\mathrm{Gal}(N^{unr}/K^{unr}) \cong \mathbb{Z}/3\mathbb{Z}$ or $\mathrm{Gal}(N^{unr}/K^{unr}) \cong \mathbb{Z}/6\mathbb{Z}$, $\mathrm{Gal}(S^{unr}/K^{unr}) \cong \mathbb{Z}/2\mathbb{Z}$. Also, if H is ramified over K, then

$$\mathrm{Gal}(N^{unr}/K^{unr}) \cong (\mathbb{Z}/3\mathbb{Z}) \rtimes (\mathbb{Z}/4\mathbb{Z})$$

with the uniquely defined non-trivial action of $\mathbb{Z}/4\mathbb{Z}$ on $\mathbb{Z}/3\mathbb{Z}$, so that $\mathrm{Gal}(S^{unr}/K^{unr}) \cong \mathbb{Z}/4\mathbb{Z}$ and $\mathrm{Gal}(N^{unr}/S^{unr}) \cong \mathbb{Z}/3\mathbb{Z}$. Let $a \in \mathrm{Gal}(N^{unr}/S^{unr})$ be an element of order 3 and let $b \in \mathrm{Gal}(N^{unr}/K^{unr})$ be an element of order 4 that maps onto a generator of $\mathrm{Gal}(S^{unr}/K^{unr})$ under the quotient map.

Lemma 1.7. *Assume H is ramified over K and σ_E is wildly ramified. Then N is totally ramified over K and let $\Phi_N \in \mathrm{Gal}(\overline{K}/N)$ be a Frobenius considered as a Frobenius of $\mathrm{Gal}(\overline{K}/K)$. Then*

$$\mathcal{W}(\overline{K}/K)/I_N \cong (\langle a\rangle \rtimes \langle b\rangle) \rtimes \langle c\rangle,$$

where $c = \Phi_N$, $|a| = 3$, $|b| = 4$, $b^{-1}ab = a^2$, $ac = ca$, $c^{-1}bc = b^r$, and $r = (-1)^{f(K/\mathbb{Q}_3)}$. Moreover, there exist a root of unity η satisfying $\eta^2 = (-1)^{f(K/\mathbb{Q}_3)}$, a primitive third root of unity ξ, and a one-dimensional complex representation ϕ of the subgroup

$$\mathcal{W}(\overline{K}/H)/I_N \cong \langle a, b^2, c\rangle$$

such that $\phi(a) = \xi$, $\phi(b^2) = -1$, $\phi(c) = \eta$, and $\sigma = \sigma_E \otimes \omega^{1/2}$ is induced by ϕ. Thus, in a suitable basis we have

$$\sigma(a) = \begin{pmatrix} \xi & 0 \\ 0 & \xi^2 \end{pmatrix}, \quad \sigma(b) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \sigma(c) = \eta \begin{pmatrix} 1 & 0 \\ 0 & (-1)^{f(K/\mathbb{Q}_3)} \end{pmatrix}.$$

Proof. First, note that $\mathcal{W}(\overline{K}/K)/I_N \cong \mathrm{Gal}(N^{unr}/K^{unr}) \rtimes \langle \Phi_N\rangle$. It is easy to check that $\Phi_N^{-1} \circ a \circ \Phi_N = a$. Also, let $\xi_4 \in \overline{K}$ be the forth-root of unity such that $b(\Delta^{1/4}) = \xi_4 \Delta^{1/4}$. Then for $r = (-1)^{f(K/\mathbb{Q}_3)}$ we have

$$\Phi_N^{-1} \circ b \circ \Phi_N(\Delta^{1/4}) = \Phi_N^{-1} \circ b(\Delta^{1/4}) = \Phi_N^{-1}(\xi_4)\Delta^{1/4} = \xi_4^r \Delta^{1/4} = b^r(\Delta^{1/4})$$

and hence $\Phi_N^{-1} \circ b \circ \Phi_N \circ b^{-r} = a^t$ for some $t \in \{0, 1, 2\}$. For x-coordinate α of a point in $E[2]$ we have $b^{1-r}(\alpha) = a^t(\alpha)$, since $\Phi_N(\alpha) = \alpha$. If $r = 1$, then $t = 0$. If $r = -1$, then $b^2(\alpha) = a^t(\alpha)$. Since the order of a is 3 and the order of b is 4, we have $t = 0$ in this case as well.

Denote $G = (\langle a\rangle \rtimes \langle b\rangle) \rtimes \langle c\rangle$. Note that σ can be considered as an irreducible symplectic representation of G. It is known that σ_E is induced by a character of $H^\times$ (see e.g., [4], p. 613, Prop. 3.3(ii)). This implies that σ is also induced by a character ϕ of $H^\times$. Note that if $\phi(a) = 1$, then σ_E is tame, which contradicts the assumption. Hence $\phi(a)$ is a primitive third root of unity ξ. It is well-known that a two-dimensional complex representation is symplectic if and only if its determinant is trivial. Calculating $\det \sigma$, we conclude that $\phi(b^2) = -1$ and if $\phi(c) = \eta$, then $\eta^2 = (-1)^{f(K/\mathbb{Q}_3)}$. □

Lemma 1.8. *Assume H is ramified over K and σ_E is wildly ramified. In the notation of Lemma 1.7 let θ be a character of $H^\times$ given by $\theta(a) = 1$, $\theta(b^2) = -1$, and $\theta(c) = \gamma$ for a root of unity γ satisfying $\gamma^2 = (-1)^{f(H/\mathbb{Q}_3)}$. Then*

$$\theta|_{K^\times} = \chi_{H/K}, \quad (\phi \otimes \theta)|_{K^\times} = 1_K, \quad \textit{and} \;\; a(\theta) = 1.$$

Proof. Interpreting the condition $(\phi \otimes \theta)|_{K^\times} = 1_K$ in terms of Weil groups via the local class field theory we need to show that $(\phi \otimes \theta) \circ tr : \mathcal{W}(\overline{K}/K)^{ab} \longrightarrow \mathbb{C}^\times$ is trivial, where $tr : \mathcal{W}(\overline{K}/K)^{ab} \longrightarrow \mathcal{W}(\overline{K}/H)^{ab}$ is the transfer map. Let $G = \langle a, b, c\rangle$ and $\Gamma = \langle a, b^2, c\rangle$. Since ϕ is trivial on I_N, it is enough to show that $\phi \otimes \theta$ composed with the transfer map $tr : G^{ab} \longrightarrow \Gamma^{ab}$ is trivial (here both ϕ and θ are considered as one-dimensional representations of Γ). By calculating the transfer map explicitly and using the definition of ϕ given in Lemma 1.7 it is easy to verify that $\theta|_{K^\times} = \phi|_{K^\times} = \chi_{H/K}$. Since the restriction of θ to the inertia group I_H has order two, we have $a(\theta) = 1$. □

Lemma 1.9. *Suppose σ_E is wildly ramified. Let F be a finite Galois extension of K contained in $\overline{K}$ such that $F \cap H = K$ and let $L = FH$. Then $L^{unr} \cap M^{unr} = H^{unr}$ and if $e(H/K) = 2$, then in addition $L^{unr} \cap N^{unr} = H^{unr}$.*

Proof. Assume that $M^{unr} \subseteq L^{unr}$. Let F_t be the maximal tamely ramified extension of K contained in F and let $L_t = F_t H$, $T = L_t M$. Since $[M : H] = e(M/H) = 3$, we have $L_t \cap M = H$, $L_t^{unr} \cap M^{unr} = H^{unr}$, and $T^{unr} \subseteq L^{unr}$. The restriction map gives the surjection $f : \mathrm{Gal}(L^{unr}/L_t^{unr}) \twoheadrightarrow \mathrm{Gal}(T^{unr}/L_t^{unr})$. Note that there are natural isomorphisms $\mathrm{Gal}(L^{unr}/L_t^{unr}) \cong \mathrm{Gal}(L/L_t)$ and $\mathrm{Gal}(T^{unr}/L_t^{unr}) \cong \mathrm{Gal}(T/L_t)$, which are induced by the restriction maps. These together with f give the surjection $g : \mathrm{Gal}(L/L_t) \twoheadrightarrow \mathrm{Gal}(T/L_t)$, which commutes with the natural action of $\mathrm{Gal}(\overline{K}/F_t)$. On the other hand, $\mathrm{Gal}(T/F_t) \cong \mathrm{Gal}(T/L_t) \rtimes \mathbb{Z}/2\mathbb{Z} \cong S_3$ and $\mathrm{Gal}(L/F_t) \cong \mathrm{Gal}(L/L_t) \times \mathbb{Z}/2\mathbb{Z}$. This implies that there exists an element j in $\mathrm{Gal}(\overline{K}/F_t)$ with $j|_{L_t} \neq \mathrm{id}_{L_t}$ that acts trivially on $\mathrm{Gal}(L/L_t)$ and non-trivially on $\mathrm{Gal}(T/L_t)$. This gives a contradiction with the existence of g.

Assume now that $e(H/K) = 2$ and $S^{unr} \subseteq L^{unr}$. Thus the restriction map gives the surjection

$$h : \mathrm{Gal}(L^{unr}/K^{unr}) \twoheadrightarrow \mathrm{Gal}(S^{unr}/K^{unr}),$$

where $\mathrm{Gal}(L^{unr}/K^{unr}) \cong \mathrm{Gal}(L^{unr}/H^{unr}) \times \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Gal}(S^{unr}/K^{unr}) \cong \mathbb{Z}/4\mathbb{Z}$. This is a contradiction, since h induces a surjection of the exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(L^{unr}/H^{unr}) & \longrightarrow & \mathrm{Gal}(L^{unr}/K^{unr}) & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{Gal}(S^{unr}/H^{unr}) & \longrightarrow & \mathrm{Gal}(S^{unr}/K^{unr}) & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 1, \end{array}$$

the first of which splits and the second does not. □

2. Root numbers of elliptic curves

We keep the notation of Section 1. Suppose E has potential good reduction over K, σ_E is irreducible, and let $F \subset \overline{K}$ be a finite field extension of K. To calculate the root number $W(E/F)$ we will follow the approach of D. Rohrlich developed in [8]. Let π be a continuous complex finite-dimensional representation of $\mathrm{Gal}(\overline{K}/F)$ with real-valued character and let $\tau = \mathrm{Ind}_K^F \pi$ denote the representation of $\mathrm{Gal}(\overline{K}/K)$ induced by π. We will need the following formula ([8], p. 321):

$$W(E,\tau) = W(\sigma_E \otimes \tau) = W((\mathrm{Res}_K^F \sigma_E) \otimes \pi)\frac{\det \tau(-1)}{\det \pi(-1)}. \tag{2.1}$$

Note that $\mathrm{Res}_K^F \sigma_E$ is the representation of $\mathcal{W}(\overline{K}/F)$ attached to E considered as an elliptic curve over F by extension of scalars, so that if $\pi = 1_F$, then (2.1) implies

$$W(E,\tau) = W(E/F)\det \tau(-1).$$

Let ψ_K be an additive character of K. Since $\sigma = \mathrm{Ind}_K^H \phi$ (see Lemma 1.7 above), by the inductive properties of root numbers (see e.g., [8], p. 316, formula (1.4)) we have

$$\begin{aligned} W(E/K) &= W(\sigma) = W(\mathrm{Ind}_K^H \phi, \psi_K) = W(\phi,\psi_H) W(\mathrm{Ind}_K^H 1_H, \psi_K) = \\ &= W(\phi,\psi_H) W(\chi_{H/K}, \psi_K), \end{aligned} \tag{2.2}$$

where $\psi_H = \psi_K \circ \mathrm{Tr}_{H/K}$.

Lemma 2.1. *Let $\tau = \mathrm{Ind}_K^F \pi$. If $H \subseteq F$, then*

$$W(E,\tau) = \left(\frac{-1}{\hat{K}}\right)^{\delta} \det\tau(-1), \quad \delta = \begin{cases} \frac{\dim \tau}{2}, & \text{if } H/K \text{ ramified,} \\ 0, & \text{if } H/K \text{ unramified,} \end{cases} \tag{2.3}$$

where $\left(\frac{x}{\hat{K}}\right)$ is the quadratic residue symbol of $x \in \hat{K}$. In particular,

$$W(E/F) = \left(\frac{-1}{\hat{K}}\right)^{\delta}, \quad \delta = \begin{cases} \frac{[F:K]}{2}, & \text{if } H/K \text{ ramified,} \\ 0, & \text{if } H/K \text{ unramified.} \end{cases}$$

Proof. The calculation is the same as on p. 321 in [8], which we repeat for the sake of completeness. Recall that $\sigma = \mathrm{Ind}_K^H \phi$. We have $\mathrm{Res}_K^F \sigma = \tilde{\phi} \oplus \tilde{\phi}^{-1}$ with $\tilde{\phi} = \mathrm{Res}_H^F \phi$, since σ is symplectic. Since π has real-valued character, using properties of root numbers we have

$$W((\mathrm{Res}_K^F \sigma) \otimes \pi) = \det(\pi \otimes \tilde{\phi})(-1) = \det \pi(-1)\phi(-1)^{[F:H]\dim \pi},$$

where $\phi(-1) = \chi_{H/K}(-1)$ (by Lemma 1.3) and $\chi_{H/K}(-1) = \left(\frac{-1}{\hat{K}}\right)$ if H/K is ramified, $\chi_{H/K}(-1) = 1$ if H/K is unramified. Hence (2.3) follows from (2.1). $\square$

For the rest of the paper we assume that $H \not\subseteq F$, i.e., $F \cap H = K$. Let $L = FH$, $\lambda = \mathrm{Res}_H^L \phi$, and let ψ_F be an additive character of F. Note that $\mathrm{Res}_K^F \sigma = \mathrm{Ind}_F^L \lambda$ and

$$W(E/F) = W(\mathrm{Res}_K^F \sigma_E) = W(\mathrm{Res}_K^F(\sigma_E \otimes \omega^{1/2})) = W(\mathrm{Res}_K^F \sigma),$$

so that by (2.2) we have

$$W(E/F) = W(\lambda, \psi_L) W(\chi_{L/F}, \psi_F), \tag{2.4}$$

where $\psi_L = \psi_F \circ \mathrm{Tr}_{L/F}$.

Lemma 2.2. *Let ε denote the ramification index of a minimal extension of K over which E has good reduction. If $p \geq 5$, then*

$$W(E/F) = (-1)^{\alpha + [F:K]} W(E/K)^{[F:K]},$$

where

$$\alpha = \begin{cases} 0, & \varepsilon \mid e(F/K), \\ 1, & \textit{otherwise}. \end{cases}$$

Proof. It is known that if $p \geq 5$, then H is unramified over K and ϕ is tame, i.e., $a(\phi) = 1$. Suppose $u_{H/K} \in \mathcal{O}_H^\times$ satisfies $u_{H/K}^2 \in \mathcal{O}_K$ and $H = K(u_{H/K})$. Recall that $\sigma = \mathrm{Ind}_K^H \phi$ is symplectic and irreducible, hence $\phi|_{K^\times} = \chi_{H/K}$ by Lemma 1.3. This implies $\lambda|_{F^\times} = \chi_{L/F}$, so that by Lemma 1.4 applied to ϕ, λ and (2.4), we have

$$\begin{aligned} W(E/K) &= (-1)^{a(\phi)} \phi(u_{H/K}), \\ W(E/F) &= (-1)^{a(\lambda)} \lambda(u_{H/K}) = (-1)^{a(\lambda)} \phi(u_{H/K})^{[F:K]}. \end{aligned}$$

Since $a(\phi) = 1$, this implies $W(E/F) = (-1)^{a(\lambda)+[F:K]} W(E/K)^{[F:K]}$. Clearly, $a(\lambda) \leq 1$ and $a(\lambda) = 0$ if and only if ε divides $e(F/K)$. □

3. Case when H/K is unramified

We keep the notation of Section 1. In this section we assume that E has potential good reduction over K, σ_E is irreducible and wildly ramified, $p = 3$, and H/K is unramified. Then $\mathrm{Gal}(N^{unr}/H^{unr}) = \langle a \rangle$, where the order $|a|$ of a is 3 or 6, and let ϕ be a one-dimensional complex continuous representation of $\mathcal{W}(\overline{K}/H)$ such that $\ker(\phi|_{I_H}) = I_N$, so that $\phi(a)$ is a primitive 3rd root of unity if $|a| = 3$ and $\phi(a)$ is a primitive 6th root of unity if $|a| = 6$ (such ϕ exists because σ is induced by a character of $H^\times$ and $\ker(\sigma_E|_{I_K}) = I_N$).

Proposition 3.1. *Assume that H is unramified over K, $\sigma = \mathrm{Ind}_K^H \phi$, and ϕ is wildly ramified. Suppose $u_{H/K} \in \mathcal{O}_H^\times$ satisfies $u_{H/K}^2 \in \mathcal{O}_K$ and $H = K(u_{H/K})$. If F is a finite Galois extension of K and $\lambda = \mathrm{Res}_K^F \phi$, then*

$$a(\lambda) \equiv (a(\phi) - 1)[F:K] + 1 \ \mathit{mod}\ 2 \tag{3.1}$$

and

$$W(E/F) = (-1)^{1 + (a(\phi)-1)[F:K]} \phi(u_{H/K})^{[F:K]} = (-1)^{1+[F:K]} W(E/K)^{[F:K]}. \tag{3.2}$$

Proof. Recall that $\sigma = \mathrm{Ind}_K^H \phi$ is symplectic and irreducible, hence $\phi|_{K^\times} = \chi_{H/K}$ by Lemma 1.3. This implies $\lambda|_{F^\times} = \chi_{L/F}$, so that by Lemma 1.4 applied to ϕ, λ and (2.4), we have

$$\begin{aligned} W(E/K) &= (-1)^{a(\phi)}\phi(u_{H/K}),\\ W(E/F) &= (-1)^{a(\lambda)}\lambda(u_{H/K}) = (-1)^{a(\lambda)}\phi(u_{H/K})^{[F:K]}. \end{aligned}$$

Thus (3.1) implies (3.2) and it is enough to prove (3.1). Assume now that $\mathrm{Gal}(N^{unr}/H^{unr}) \cong \mathbb{Z}/3\mathbb{Z}$, so that $N^{unr} = M^{unr}$. Denote $L = FH$. Note that by Lemma 1.9 we have $L^{unr} \cap M^{unr} = H^{unr}$.

Let $\tilde{F}$ be the maximal tamely ramified extension of K contained in F, let $\tilde{L} = \tilde{F}H$, and let λ_t be the restriction of ϕ to $\tilde{L}$. Denote $e_t = e(\tilde{L}/H) = e(\tilde{F}/K)$. By Lemma 1.2, since $a(\phi) > 1$, we have $a(\lambda_t) = (a(\phi) - 1)e_t + 1$. Since $p = 3$ and $f(F/K)$ is odd, we have $e_t \equiv [F : K] \bmod 2$, so that

$$a(\lambda_t) \equiv (a(\phi) - 1)[F : K] + 1 \bmod 2. \tag{3.3}$$

Assume now that F is a (totally ramified) Galois extension of $\tilde{F}$ of degree 3. We will show that $a(\lambda) \equiv a(\lambda_t) \bmod 2$. Indeed, let $\tilde{T} = \tilde{L}M$, $T = LM$. Since $L \cap M = H$, we have the following diagram of field extensions:

$$\begin{array}{ccccc} F & \overset{2}{\text{——}} & L & \overset{3}{\text{——}} & T \\ {\scriptstyle 3}\big| & & {\scriptstyle 3}\big| & & \big|{\scriptstyle 3} \\ \tilde{F} & \overset{2}{\text{——}} & \tilde{L} & \overset{3}{\text{——}} & \tilde{T} \end{array}$$

Moreover, $\mathrm{Gal}(\tilde{T}/\tilde{F}) \cong S_3$ and λ_t is a faithful representation of $\mathrm{Gal}(\tilde{T}/\tilde{L})$. Let $G = \mathrm{Gal}(T/\tilde{L}) \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$. Ramification groups of G have the form

$$G = G_0 = G_1 = \cdots = G_t \supset G_{t+1} = \{1\} \quad \text{or}$$
$$G = G_0 = G_1 = \cdots = G_t \supset G_{t+1} = \cdots = G_{t+s} \supset G_{t+s+1} = \{1\}, \tag{3.4}$$

where $G_{t+1} \cong \mathbb{Z}/3\mathbb{Z}$. It is easy to see that depending on the embedding of G_{t+1} into G we have either

(1) $a(\lambda_t) = a(\lambda)$, or
(2) $a(\lambda_t) = 1 + t + \frac{s}{3}$, $a(\lambda) = 1 + t + s$, or
(3) $a(\lambda_t) = 1 + t + \frac{s}{3}$, $a(\lambda) = 1 + t$.

Since $a(\lambda_t)$ is an integer, $a(\lambda_t) \equiv a(\lambda) \bmod 2$ in cases (1) and (2). Case (3) occurs when ramification groups of G have form (3.4) and G_{t+1} embeds diagonally into G. Assume that this is the case. Let a denote a generator of $\mathrm{Gal}(\tilde{T}/\tilde{L})$, let b denote a generator of $\mathrm{Gal}(L/\tilde{L})$. Then we can identify G with $\langle a\rangle \times \langle b\rangle$ via the natural isomorphism given by restrictions and without loss of generality we can assume that $G_{t+1} = \langle ab\rangle$. Let $c = \Phi_{\tilde{F}}$ be a Frobenius of $\tilde{F}$. Since $\mathrm{Gal}(\tilde{T}/\tilde{F}) \cong S_3$ and $\mathrm{Gal}(L/\tilde{F}) \cong \mathbb{Z}/6\mathbb{Z}$, we have $cac^{-1} = a^{-1}$

and $cbc^{-1} = b$. Denote $\Gamma = \mathcal{W}_{\tilde{F}}/I_T$ and $\Lambda = \mathcal{W}_{\tilde{L}}/I_T$. Then

$$\Gamma \cong (\langle a\rangle \times \langle b\rangle) \rtimes \langle c\rangle, \quad \Lambda \cong (\langle a\rangle \times \langle b\rangle) \times \langle c^2\rangle.$$

Let ψ denote a one-dimensional complex representation of Λ given by $\psi(a) = \xi$ for a primitive third root of unity ξ, $\psi(b) = \psi(c^2) = 1$, let μ be a one-dimensional complex representation of Γ given by $\mu(a) = \mu(c) = 1$, $\mu(b) = \xi$, and let $\rho = \operatorname{Ind}_\Lambda^\Gamma \psi = \operatorname{Ind}_{\tilde{F}}^{\tilde{L}} \psi$, so that

$$\rho(a) = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}, \quad \rho(b) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho(c) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then it is easy to check that on one hand, $a(\rho \otimes \mu) = 2(t+1) + \frac{s}{3}$ and on the other hand,

$$a(\rho \otimes \mu) = a(\operatorname{Ind}_{\tilde{F}}^{\tilde{L}}(\psi \otimes \operatorname{Res}_{\tilde{F}}^{\tilde{L}} \mu)) = 2a(\psi \otimes \operatorname{Res}_{\tilde{F}}^{\tilde{L}} \mu),$$

which implies that s is even and hence $a(\lambda_t) \equiv a(\lambda) \bmod 2$ in case (3) as well.

Assume now that F is an arbitrary Galois extension of K. If F is tame over K, then (3.1) follows from (3.3). Otherwise, since $\mathrm{Gal}(F/\tilde{F})$ is a 3-group, there exists a totally ramified Galois extension F' of $\tilde{F}$ contained in F such that F is a totally ramified Galois extension of F' of degree 3. Note that $F' \cap H = K$, because $F \cap H = K$, hence $[F'H : F'] = 2$ and $e(F'H/F') = 1$. Also, $(F'H)^{unr} \cap M^{unr} = H^{unr}$, because $L^{unr} \cap M^{unr} = H^{unr}$, so that $F'H \cap M = H$ and $e(F'M/F'H) = 3$. Finally, using the results above together with the induction on the degree of F over $\tilde{F}$, we get $a(\lambda) \equiv a(\lambda_t) \bmod 2$, which together with (3.3) proves (3.1) in the case when $\mathrm{Gal}(N^{unr}/H^{unr}) \cong \mathbb{Z}/3\mathbb{Z}$.

Assume now that $\mathrm{Gal}(N^{unr}/H^{unr}) \cong \mathbb{Z}/6\mathbb{Z}$. Since $M^{unr} \not\subseteq L^{unr}$ by Lemma 1.9, λ is wildly ramified, hence $a(\lambda^2) = a(\lambda)$ and we can apply the results for the case $\mathrm{Gal}(N^{unr}/H^{unr}) \cong \mathbb{Z}/3\mathbb{Z}$ above. Thus

$$a(\lambda) \equiv (a(\phi^2) - 1)[F : K] + 1 \mod 2,$$

where $a(\phi^2) = a(\phi)$, so that (3.1) follows. □

Remark 3.2. Note that $\phi(u_{H/K})$ does not depend on the choice of $u_{H/K}$. Indeed, recall that $\sigma = \operatorname{Ind}_K^H \phi$ is symplectic and irreducible, hence by Lemma 1.3 we have $\phi|_{K^\times} = \chi_{H/K}$. Thus $\phi(u_{H/K})$ does not depend on the choice of $u_{H/K}$ by Remark 1.5.

4. Case when H/K is ramified

We keep the notation of Section 1. In this section we assume that E has potential good reduction over K, σ_E is irreducible and wildly ramified, $p = 3$, and H/K is ramified. We distinguish two cases: $L = FH$ is unramified over F (equivalently, the ramification index $e(F/K)$ of F over K is even) and L is ramified over F (equivalently, $e(F/K)$ is odd). Proposition 4.1 below treats the first case and Theorem 4.3 below treats the second.

Proposition 4.1. *Let H be ramified over K and let $\alpha \in \mathcal{O}_H$ satisfy $\alpha^2 \in \mathcal{O}_K$, $\mathrm{val}_H\, \alpha = 1$, and $H = K(\alpha)$. Let L be unramified over F (equivalently, $e(F/K)$ is even). Then*

$$W(E/F) = (-1)^{a(\lambda) + \frac{e(F/K)}{2}} \phi(\alpha)^{[F:K]}. \tag{4.1}$$

Moreover, if F is Galois over K, then

$$a(\lambda) \equiv (a(\phi)-1)\frac{e(F/K)}{2}+1 \equiv \frac{e(F/K)}{2}+1 \ mod\ 2 \tag{4.2}$$

and

$$W(E/F) = (-1)^{1+\frac{e(F/K)}{2}f(F/\mathbb{Q}_3)}. \tag{4.3}$$

Proof. Let ϖ_F be a uniformizer of F. Since $e(F/K)$ is even, we have $\alpha = u\varpi_F^k$ for $k = \frac{e(F/K)}{2}$, $u \in \mathcal{O}_L^\times$, $u^2 \in \mathcal{O}_F^\times$, and $L = F(u)$. Recall that $\sigma = \mathrm{Ind}_K^H \phi$ is symplectic and irreducible, hence $\phi|_{K^\times} = \chi_{H/K}$ by Lemma 1.3. This implies $\lambda|_{F^\times} = \chi_{L/F}$, so that by Lemma 1.4 applied to λ and (2.4), we have

$$W(E/F) = (-1)^{a(\lambda)} \cdot \lambda(u).$$

Here $\lambda(u) = \lambda(\alpha)\lambda(\varpi_F)^{-k}$, where $\lambda(\varpi_F) = \chi_{L/F}(\varpi_F) = -1$ and (4.1) follows.

Let F_t be the maximal tamely ramified extension of K contained in F, let $L_t = F_tH$, and let λ_t be the restriction of ϕ to L_t. Since L_t is unramified over F_t, Proposition 3.1 implies

$$a(\lambda) \equiv (a(\lambda_t)-1)[F:F_t]+1 \text{ mod } 2.$$

Let $e_t = \frac{e(F_t/K)}{2} = e(L_t/H)$. Using Lemma 1.2 and taking into account that $a(\phi)$ is even (by Lemma 1.1), we have

$$a(\lambda_t) = (a(\phi)-1)e_t+1 \equiv e_t+1 \text{ mod } 2.$$

This implies (4.2).

Finally, from (4.1) and (4.2) we have

$$W(E/F) = -\phi(\alpha)^{[F:K]}.$$

Also, $\phi(\alpha^2) = \chi_{H/K}(-1) = (-1)^{f(K/\mathbb{Q}_3)}$, since $\alpha^2 \in K$, $\alpha \notin K$, and $\phi|_{K^\times} = \chi_{H/K}$. Since $[F:K]$ is even, we have

$$\phi(\alpha)^{[F:K]} = \phi(\alpha^2)^{\frac{[F:K]}{2}} = (-1)^{f(K/\mathbb{Q}_3)\frac{[F:K]}{2}} = (-1)^{\frac{e(F/K)}{2}f(F/\mathbb{Q}_3)}$$

and (4.3) follows. □

Remark 4.2. Note that $\phi(\alpha)^{[F:K]}$ does not depend on the choice of α. Indeed, let $\beta \in \mathcal{O}_H$ satisfy $\beta^2 \in \mathcal{O}_K$, $\mathrm{val}_H\,\alpha = 1$, and $H = K(\beta)$. This implies that $\alpha = u\beta$ for $u \in \mathcal{O}_K^\times$. Since $[F:K]$ is even and $\phi|_{K^\times} = \chi_{H/K}$ (by Lemma 1.3), we have

$$\phi(u)^{[F:K]} = \phi(u^2)^{\frac{[F:K]}{2}} = \chi_{H/K}(u^2)^{\frac{[F:K]}{2}} = 1,$$

since $u^2 = N_{H/K}(u)$ is in the kernel of $\chi_{H/K}$.

Theorem 4.3. *Suppose $e(F/K)$ is odd and e_t is the ramification index of the maximal tamely ramified extension of K contained in F. Assume in addition that F is Galois over K. Then there exists $\alpha \in \mathcal{O}_H$ (that depends on E and does not depend on F) such that $H = K(\alpha)$, $\alpha^2 \in \mathcal{O}_K$, $\operatorname{val}_H \alpha = 1$, and*

$$W(E/F) = (-1)^{1+af(F/\mathbb{Q}_3)}\eta^{[F:K]}\phi(\alpha)^{[F:K]}, \tag{4.4}$$

where η is given by Lemma 1.7 (it depends on E and does not depend on F) and

$$a = \begin{cases} \frac{e_t-1}{2}, & \text{if } e_t \equiv 1 \text{ mod } 3 \\ \frac{e_t+1}{2}, & \text{if } e_t \equiv 2 \text{ mod } 3 \end{cases} = \begin{cases} \text{odd}, & \text{if } e_t \equiv 5 \text{ or } 7 \text{ mod } 12 \\ \text{even}, & \text{if } e_t \equiv 1 \text{ or } 11 \text{ mod } 12. \end{cases}$$

In particular,

$$W(E/K) = -\eta\phi(\alpha)$$

and

$$W(E/F) = (-1)^{1+[F:K]+af(F/\mathbb{Q}_3)}W(E/K)^{[F:K]}.$$

Proof. Clearly, it is enough to prove (4.4). For that we will choose a special ψ_F and calculate separately $W(\chi_{L/F}, \psi_F)$ and $W(\lambda, \psi_L)$ in (2.4).

The root number $W(\chi_{L/F}, \psi_F)$. Let g be a generator of $\operatorname{Gal}(M/H)$ (recall that $M = K(E[2])$ and $\operatorname{Gal}(M/H) \cong \mathbb{Z}/3\mathbb{Z}$) and let A, B, C denote the x-coordinates of the 2-torsion points on E such that $g(A) = B$, $g(B) = C$. Let $\Delta^{1/2}$ denote a fixed quadratic root of Δ satisfying

$$\Delta^{1/2} = (A - B)(B - C)(C - A),$$

let $\Delta^{1/4}$ denote a fixed quadratic root of $\Delta^{1/2}$, and let $N = K(E[2], \Delta^{1/4})$ with our choice of $\Delta^{1/4}$. We can extend g to an element of order 3 of $\operatorname{Gal}(N/H)$, then consider g as an element of $\operatorname{Gal}(N^{unr}/H^{unr})$ via the natural isomorphism $\operatorname{Gal}(N^{unr}/H^{unr}) \cong \operatorname{Gal}(N/H)$ given by the restriction, and finally regard g as an element of $\mathcal{W}(\overline{K}/H)/I_N$ via the natural embedding $\operatorname{Gal}(N^{unr}/H^{unr}) \hookrightarrow \mathcal{W}(\overline{K}/H)/I_N$. In particular, $g(\Delta^{1/4}) = \Delta^{1/4}$. Let ψ_K denote a character of K whose restriction to $\mathcal{O}_K$ is given by

$$\psi_K(x) = \phi(g)^{-\operatorname{Tr}_{\hat{K}/\mathbb{F}_3}(\bar{x})}, \quad x \in \mathcal{O}_K,$$

where $\bar{x}$ denotes the image of x in $\hat{K}$ under the quotient map.

Let $\sigma_F = \operatorname{Res}^F_K \sigma = \operatorname{Ind}^L_F \lambda$, so that σ_F is the analogue of σ for the elliptic curve over F obtained from E by extension of scalars. Denote $P = LM$ and $T = LN$. By Lemma 1.9, the natural restriction map

$$\mu : \operatorname{Gal}(T^{unr}/L^{unr}) \longrightarrow \operatorname{Gal}(N^{unr}/H^{unr})$$

is an isomorphism. Hence σ_F is irreducible by Lemma 1.3. Let $\tilde{g} \in \operatorname{Gal}(T^{unr}/L^{unr})$ be the preimage of g under μ. We consider $\tilde{g}$ as an element of $\mathcal{W}(\overline{K}/L)/I_T$ via the natural embedding $\operatorname{Gal}(T^{unr}/L^{unr}) \hookrightarrow \mathcal{W}(\overline{K}/L)/I_T$. Thus $T = F(E[2], \Delta^{1/4})$ with the above choice of $\Delta^{1/4}$, $\tilde{g}$ fixes each element of F^{unr}, $\tilde{g}(A) = B$, $\tilde{g}(B) = C$, $\tilde{g}(\Delta^{1/4}) = \Delta^{1/4}$, and $\lambda(\tilde{g}) = \phi(g)$. Let ψ denote a character of F whose restriction to $\mathcal{O}_F$ is given by

$$\psi(x) = \phi(g)^{-\operatorname{Tr}_{\hat{F}/\mathbb{F}_3}(\bar{x})}, \quad x \in \mathcal{O}_F,$$

and let ψ_F be a character of F given by

$$\psi_F(x) = \psi(e_t x).$$

(Recall that e_t is the ramification index of the maximal tamely ramified extension F_t of K contained in F.) Let $\Phi_T \in \mathcal{W}(\overline{K}/T)$ be a Frobenius. Then by a property of root numbers (see e.g., [7], Proposition on p. 143) we have

$$W(\chi_{L/F}, \psi_F) = \chi_{L/F}(e_t) W(\chi_{L/F}, \psi). \tag{4.5}$$

On the other hand, it follows from [4] that

$$W(\chi_{L/F}, \psi) = -\lambda(\Phi_T). \tag{4.6}$$

Indeed, denote

$$G = \sum_{u \in (\hat{F})^\times} \left(\frac{u}{\hat{F}}\right) \phi(g)^{-\operatorname{Tr}_{\hat{F}/\mathbb{F}_3}(u)},$$

where $\left(\frac{u}{\hat{F}}\right)$ is the quadratic residue symbol of $u \in \hat{F}$. Using the definition of $W(\chi_{L/F}, \psi)$, one can check that

$$W(\chi_{L/F}, \psi) = C_1 \cdot G, \tag{4.7}$$

where C_1 is a real positive number. It follows from Proposition 5.7 on p. 618 in [4] that

$$G = -C_2 \cdot \lambda(\Phi_T), \tag{4.8}$$

where C_2 is a real positive number (note that in [4] instead of λ the author uses a character of $L^\times$ that induces $\operatorname{Res}_K^F \sigma_E$). Since both $W(\chi_{L/F}, \psi)$ and $\lambda(\Phi_T)$ are of absolute value 1, (4.7) and (4.8) imply (4.6). Finally, (4.5) and (4.6) give

$$W(\chi_{L/F}, \psi_F) = -\chi_{L/F}(e_t) \lambda(\Phi_T).$$

Note that since $\operatorname{Gal}(\overline{K}/T^{unr})$ is in the kernel of λ, $\lambda(\Phi_T)$ does not depend on the choice of Φ_T. Let $f = f(F/K)$. Note that $f = f(T/N)$, which follows from the assumptions that $e(H/K) = 2$, $e(F/K)$ is odd, and ϕ is wildly ramified together with Lemma 1.9. Let $\Phi_N \in \operatorname{Gal}(\overline{K}/N)$ be a fixed Frobenius. There exists $d \in I_N$ such that $\Phi_T = \Phi_N^f d$, hence $\lambda(\Phi_T) = \phi(\Phi_N)^f = \eta^f$ and

$$W(\chi_{L/F}, \psi_F) = -\chi_{L/F}(e_t) \eta^f. \tag{4.9}$$

The root number $W(\lambda, \psi_L)$. Given $L_t = F_t H$ we define characters ψ_H and ψ_L of H and L, respectively, via

$$\psi_H = \psi_K \circ \operatorname{Tr}_{H/K}, \quad \psi_L = \psi_F \circ \operatorname{Tr}_{L/F}.$$

Note that

$$\begin{aligned}\psi_F(x) &= \phi(g)^{-e_t \operatorname{Tr}_{\hat{F}/\mathbb{F}_3}(\bar{x})}, \quad x \in \mathcal{O}_F,\\ \psi_H(x) &= \phi(g)^{-2 \operatorname{Tr}_{\hat{H}/\mathbb{F}_3}(\bar{x})}, \quad x \in \mathcal{O}_H,\\ \psi_L(x) &= \phi(g)^{-2e_t \operatorname{Tr}_{\hat{L}/\mathbb{F}_3}(\bar{x})}, \quad x \in \mathcal{O}_L,\end{aligned}$$

so that $n(\psi_K) = n(\psi_F) = n(\psi_H) = n(\psi_L) = -1$ and

$$\begin{aligned}\psi_L(x) &= \psi_H \circ \operatorname{Tr}_{L_t/H}(x), \quad x \in \mathcal{O}_{L_t},\\ \psi_F(x) &= \psi_K \circ \operatorname{Tr}_{F_t/K}(x), \quad x \in \mathcal{O}_{F_t}.\end{aligned}$$

Clearly, Φ_N is a Frobenius of both $\operatorname{Gal}(\overline{K}/H)$ and $\operatorname{Gal}(\overline{K}/K)$. We fix uniformizers ϖ_H and ϖ_K of H and K, respectively, corresponding to Φ_N via the local class field theory. Analogously, we fix uniformizers ϖ_L and ϖ_F of L and F, respectively, corresponding to Φ_T via the local class field theory. In particular, we have

$$\varpi_K = N_{H/K}\varpi_H, \quad \varpi_F = N_{L/F}\varpi_L.$$

Let $\tilde{\theta} = \operatorname{Res}_H^L \theta$, where θ is defined by Lemma 1.8. Then

$$\tilde{\theta}(\varpi_L) = \theta(\varpi_H)^f = \gamma^f, \quad f = f(F/K) = f(L/H),$$

and

$$\tilde{\theta}(\varpi_L)^2 = \gamma^{2f} = (-1)^{f(L/\mathbb{Q}_3)}.$$

Let $\alpha \in \mathcal{O}_H$ satisfy $H = K(\alpha)$, $\alpha^2 \in \mathcal{O}_K$, and $\operatorname{val}_H \alpha = 1$, and let $e = e(F/K)$. By Lemma 1.9, λ is not tame and hence $a(\lambda)$ and $a(\phi)$ are even by Lemma 1.1. We denote $a(\lambda) = \kappa$, $a(\phi) = m$. To calculate $W(\lambda, \psi_L)$ we follow Rohrlich's approach, namely make use of the Fröhlich–Queyrut's formula as follows. Note that $L = F(\alpha)$. Since θ was chosen so that $(\phi \otimes \theta)|_{K^\times} = 1_K$, we have $(\lambda \otimes \tilde{\theta})|_{F^\times} = 1_F$ and hence

$$W(\lambda \otimes \tilde{\theta}, \psi_L) = \lambda(\alpha)\tilde{\theta}(\alpha) = \phi(\alpha)^{[F:K]} \cdot \theta(\alpha)^{[F:K]},$$

where the first equality follows from Theorem 3 on p. 130 in [2]. On the other hand, since $a(\tilde{\theta}) = 1$ and $n(\psi_L) = -1$, by the results on p. 546 in [1], we have

$$W(\lambda \otimes \tilde{\theta}, \psi_L) = \tilde{\theta}(z)^{-1} W(\lambda, \psi_L),$$

where $z \in L^\times$ satisfies $\operatorname{val}_L(z) = 1 - \kappa$ and

$$\lambda(1+b) = \psi_L(zb), \quad \text{for any } b \in L \text{ with } \operatorname{val}_L(b) \geq \kappa/2. \tag{4.10}$$

Hence,

$$W(\lambda, \psi_L) = \phi(\alpha)^{[F:K]} \cdot \theta(\alpha)^{[F:K]} \cdot \tilde{\theta}(z). \tag{4.11}$$

Let $y \in H^\times$ with $\operatorname{val}_H(y) = 1 - m$ satisfy

$$\phi(1+a) = \psi_H(ya), \quad \text{for any } a \in H \text{ with } \operatorname{val}_H(a) \geq m/2. \tag{4.12}$$

Lemma 4.4. *We have*

$$\tilde{\theta}(z) = \theta(y)^{e_t f}. \tag{4.13}$$

Proof. See Section 5 below. □

Let $n = a(\phi)/2 = m/2$. Note that $\phi^{-1}(1+\alpha\varpi_K^{n-1}b)$ is an additive character in $b \in \mathcal{O}_K$ and hence there exists $u \in K^\times$ such that

$$\phi^{-1}(1+\alpha\varpi_K^{n-1}b) = \psi_K(ub), \quad \forall b \in \mathcal{O}_K.$$

Moreover, $\operatorname{val}_K u = 0$, so that $u \in \mathcal{O}_K^\times$. Thus there exists $\alpha \in H$ depending on ϕ, ψ_K, and our choice of ϖ_K such that $H = K(\alpha)$, $\alpha^2 \in \mathcal{O}_K$, $\operatorname{val}_H \alpha = 1$, and

$$\phi^{-1}(1+\alpha\varpi_K^{n-1}b) = \psi_K(b), \quad \forall b \in \mathcal{O}_K. \tag{4.14}$$

In particular, it follows from our choices of ψ_K and ϖ_K that α in (4.14) depends on E and does not depend on F. Taking into account that $\operatorname{val}_H\left(\alpha\varpi_K^{n-1}b\right) \geq n$ for any $b \in \mathcal{O}_K$ and using (4.12) we get

$$\psi_H(b) = \phi(1+\alpha\varpi_K^{n-1}b) = \psi_H(y\alpha\varpi_K^{n-1}b).$$

Hence $y\alpha\varpi_K^{n-1} \equiv 1 \bmod \mathfrak{p}_H$ (since $n(\psi_H) = -1$) and $\theta(y) = \theta(\alpha)^{-1}$. This together with (4.11) and (4.13) yields

$$W(\lambda, \psi_L) = \phi(\alpha)^{[F:K]} \cdot \theta(\alpha)^{[F:K]-e_t f}. \tag{4.15}$$

We now prove (4.4). It follows from (2.4), (4.9), and (4.15) that

$$W(E/F) = -\eta^f \chi_{L/F}(e_t)\phi(\alpha)^{[F:K]}\theta(\alpha)^{[F:K]-e_t f}. \tag{4.16}$$

Let $\alpha = u\varpi_H$ for some $u \in \mathcal{O}_H^\times$. Note that $\theta(\varpi_H) = \gamma$, $\theta|_{\mathcal{O}_H^\times}$ has order 2, and $[F:K]-e_t f$ is even, so that

$$\theta(\alpha)^{[F:K]-e_t f} = \gamma^{[F:K]-e_t f}. \tag{4.17}$$

Assume $f(F/\mathbb{Q}_3)$ is even. Then $\chi_{L/F}(e_t) = 1$. Also, using Lemmas 1.7 and 1.8, it is easy to check that $\gamma^{[F:K]-e_t f} = 1$ and $\eta^f = \eta^{[F:K]}$, so that (4.4) follow from (4.16) together with (4.17).

Assume $f(F/\mathbb{Q}_3)$ is odd, so that both $f(F/K)$ and $f(K/\mathbb{Q}_3)$ are odd. Then $\eta^2 = -1$ and we choose $\gamma = \eta$, which gives

$$\eta^{f+[F:K]-e_t f} = (-1)^{\frac{e_t-1}{2}}\eta^{[F:K]}.$$

Calculating $(-1)^{\frac{e_t-1}{2}}$ and $\chi_{L/F}(e_t) = \left(\frac{e_t}{3}\right)$ explicitly, we get (4.4). □

5. Proof of Lemma 4.4

In this section we keep the notation and assumptions of the previous section. We consider three cases: 1) F is tamely ramified over K (equivalently, L is tamely ramified over H), 2) F is a totally ramified Galois extension of K of degree 3 (hence, L is a totally ramified Galois extension of H of degree 3), and 3) the general case.

L **is tamely ramified over** H**.** Note that in this case we have $L = L_t$ and hence $\psi_L = \psi_H \circ \mathrm{Tr}_{L/H}$ on $\mathcal{O}_L$. Since by assumption ϕ is not tame, by Lemma 1.2 we have $\kappa = (m-1)e_t + 1$. This implies

$$\mathrm{val}_L\, y = \mathrm{val}_L\, z = (1-m)e_t.$$

For any $b \in L$ with $\mathrm{val}_L(b) \geq (m-1)e_t$ using (4.10) we have

$$\psi_L(zb) = \lambda(1+b) = \phi(\mathrm{N}_{L/H}(1+b)) = \phi(1 + \mathrm{Tr}_{L/H}(b) + b'), \quad b' \in H, \tag{5.1}$$

where $\mathrm{val}_L(\mathrm{Tr}_{L/H}(b)) \geq me_t/2$ and $\mathrm{val}_L(b') \geq me_t$. Thus

$$\mathrm{val}_H(\mathrm{Tr}_{L/H}(b)) \geq m/2, \quad \mathrm{val}_H(b') \geq a(\phi), \text{ and } yb \in \mathcal{O}_L,$$

hence by (4.12)

$$\phi(1 + \mathrm{Tr}_{L/H}(b) + b') = \psi_H(y\, \mathrm{Tr}_{L/H}(b)) = \psi_H(\mathrm{Tr}_{L/H}(yb)) = \psi_L(yb). \tag{5.2}$$

Therefore, comparing (5.1) and (5.2) we get $\psi_L(zb) = \psi_L(yb)$ or, equivalently,

$$\psi_L((z-y)b) = 1.$$

Since the last equation holds for all $b \in \mathfrak{p}_L^{(m-1)e_t}$, we conclude that

$$\mathrm{val}_L((z-y)\varpi_L^{(m-1)e_t}) \geq 1. \tag{5.3}$$

Let $y = u\varpi_L^{\mathrm{val}_L y}$, $z = v\varpi_L^{\mathrm{val}_L y}$ for $u, v \in \mathcal{O}_L^\times$. Then (5.3) implies $u \equiv v \bmod \mathfrak{p}_L$ and hence

$$\tilde{\theta}(z) = \tilde{\theta}(\varpi_L)^{\mathrm{val}_L y} \cdot \tilde{\theta}(u) = \tilde{\theta}(y) = \theta(y)^{[L:H]}. \tag{5.4}$$

L **is a totally ramified Galois extension of** H **of degree** 3**.** Let $T = LN$. We first study the relation between $a(\phi)$ and $a(\lambda)$. In particular, we will show that $a(\lambda) \geq a(\phi)$. For that we analyze the higher ramification groups of $\mathrm{Gal}(T^{unr}/H^{unr})$. Denote

$$\begin{aligned} P &= \mathrm{Gal}(N^{unr}/H^{unr}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \\ Q &= \mathrm{Gal}(L^{unr}/H^{unr}) \cong \mathbb{Z}/3\mathbb{Z}, \\ G &= \mathrm{Gal}(T^{unr}/H^{unr}), \\ C &= \mathrm{Gal}(T^{unr}/L^{unr}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \end{aligned}$$

(here we used Lemma 1.9). The higher ramification groups of P are

$$P = P_0 \supset P_1 = \cdots = P_n \supset P_{n+1} = \{1\},$$

where $P_1 \cong \mathbb{Z}/3\mathbb{Z}$, n is even (as follows from the results on the action of inertia groups on higher ramification groups), $m = 1 + n/2$, and since m is even, we have $n/2$ is odd. Let $R = \mathrm{Gal}(L^{unr}/K^{unr}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Then the higher ramification groups of R are

$$R = R_0 \supset R_1 = \cdots = R_\alpha \supset R_{\alpha+1} = \{1\},$$

where $R_1 \cong \mathbb{Z}/3\mathbb{Z}$ and α is even. Then the higher ramification groups Q_i of Q have the form $Q_i = Q \cap R_i$, so that

$$Q = Q_0 = \cdots = Q_\alpha \supset Q_{\alpha+1} = \{1\},$$

where α is even. Finally, the higher ramification groups of C are

$$C = C_0 \supset C_1 = \cdots = C_\delta \supset C_{\delta+1} = \{1\},$$

where $C_1 \cong \mathbb{Z}/3\mathbb{Z}$, δ is even, $\kappa = 1 + \delta/2$, and since κ is even, we have $\delta/2$ is odd. Since $L^{unr} \cap N^{unr} = H^{unr}$, the restriction maps give the isomorphism

$$\mu : G \xrightarrow{\cong} \mathrm{Gal}(N^{unr}/H^{unr}) \times \mathrm{Gal}(L^{unr}/H^{unr}),$$

so that $G \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2$ is an abelian group of order 18. As a result, the higher ramification groups of G can have two forms:

$$G = G_0 \supset G_1 = \cdots = G_t \supset G_{t+1} = \{1\}, \tag{5.5}$$

where $G_1 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, t is even, or

$$G = G_0 \supset G_1 = \cdots = G_t \supset G_{t+1} = \cdots = G_{t+s} \supset G_{t+s+1} = \{1\}, \tag{5.6}$$

where $G_1 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $G_{t+1} \cong \mathbb{Z}/3\mathbb{Z}$, t is even, and s is divisible by 6. We will show, in particular, that (5.5) does not occur.

Assume that (5.5) holds. By comparing the higher ramification groups of G with the higher ramification groups of its quotients Q and P, it is not hard to see that in this case we have $\alpha = t/2$, $n = t$, which is a contradiction, since by above α is even and $n/2$ is odd.

Assume that (5.6) holds. There are three sub-cases depending on the embedding of $G_{t+1} \cong \mathbb{Z}/3\mathbb{Z}$ into $G_t \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Let $S \subseteq N$ be a quadratic extension of H such that S^{unr}/H^{unr} is the maximal tamely ramified subextension of N^{unr}/H^{unr}. Again, as in the previous paragraph, by comparing the higher ramification groups of G with the higher ramification groups of its subgroup C and quotients Q and P, it is not hard to see that

$$\begin{array}{llll} \alpha = \frac{t}{2} + \frac{s}{6}, & n = t, & \delta = t, & \text{if } \mu(G_{t+1}) = \mathrm{Gal}(L^{unr}/H^{unr}), \\ \alpha = \frac{t}{2}, & n = t + \frac{s}{3}, & \delta = t + s, & \text{if } \mu(G_{t+1}) = \mathrm{Gal}(N^{unr}/S^{unr}), \\ \alpha = \frac{t}{2} + \frac{s}{6}, & n = t + \frac{s}{3}, & \delta = t, & \text{otherwise.} \end{array} \tag{5.7}$$

Thus, in the third sub-case in (5.7) we get $\alpha = n/2$, which is a contradiction, since by above α is even and $n/2$ is odd. Hence $\mu(G_{t+1}) = \mathrm{Gal}(L^{unr}/H^{unr})$ or $\mu(G_{t+1}) = \mathrm{Gal}(N^{unr}/S^{unr})$ and $a(\lambda) \geq a(\phi)$.

Remark 5.1. It turns out that both first two cases in (5.7) can occur. Explicit examples of elliptic curves over $K = \mathbb{Q}_3$ can be found in [3].

Note that since L is wildly ramified over H, by our choice $\psi_H = \psi_L$ on $\mathcal{O}_H$. Let $x \in L$ with $\mathrm{val}_L(x) \geq \kappa - 1$. Then

$$\psi_L(zx) = \lambda(1 + x) = \phi\left(\mathrm{N}_{L/H}(1 + x)\right). \tag{5.8}$$

By Lemmas 4 and 5 on p. 83 in [9] we have

$$\begin{aligned} \text{(5.9)}\quad \mathrm{N}_{L/H}(1+x) &\equiv 1+\mathrm{Tr}_{L/H}(x)+\mathrm{N}_{L/H}(x) \mod \mathfrak{p}_H^{l_1}, & l_1 = \left[\frac{2}{3}(\kappa+\alpha)\right], \\ \mathrm{Tr}_{L/H}(x) &\equiv 0 \mod \mathfrak{p}_H^{l_2}, & l_2 = \left[\frac{\kappa+2\alpha+1}{3}\right]. \end{aligned}$$

(Here, for $r \in \mathbb{R}$ the symbol $[r]$ denotes the largest integer $\leq r$.) In both cases when $\mu(G_{t+1}) = \mathrm{Gal}(L^{unr}/H^{unr})$ or $\mu(G_{t+1}) = \mathrm{Gal}(N^{unr}/S^{unr})$, using formulas (5.7) and $a(\lambda) = \kappa = 1+\delta/2$, $a(\phi) = m = 1+n/2$, it is easy to check that $l_1 \geq m$. Let

$$x = a\varpi_L^{\kappa-1},\ z = w\varpi_L^{1-\kappa},\ y = u\varpi_L^{3(1-m)}, \quad a \in \mathcal{O}_L,\ w, u \in \mathcal{O}_L^\times.$$

Assume that $\mu(G_{t+1}) = \mathrm{Gal}(L^{unr}/H^{unr})$. In this case we have $\kappa = m$, $l_2 \geq m$, and $\mathrm{val}_H \mathrm{N}_{L/H}(x) \geq \kappa - 1 = m-1 \geq m/2$. Thus using (5.8) and (5.9) we get

$$\psi_L(zx) = \phi\left(1+\mathrm{N}_{L/H}(x)\right) = \psi_L(y\,\mathrm{N}_{L/H}(x)). \tag{5.10}$$

Note that the group $\mathrm{Gal}(L/H)$ coincides with its α-th ramification subgroup, where $\alpha \geq 1$, so that $g(\varpi_L)\varpi_L^{-1} \equiv 1 \bmod \mathfrak{p}_L$ for any $g \in \mathrm{Gal}(L/H)$. Then easy calculation shows that

$$y\,\mathrm{N}_{L/H}(x) = y\,\mathrm{N}_{L/H}(a)\,\mathrm{N}_{L/H}(\varpi_L)^{\kappa-1} \equiv ua^3 \bmod \mathfrak{p}_L.$$

Thus, (5.10) implies $aw - ua^3 \in \ker\psi_L$. Let $f = f(L/\mathbb{Q}_3)$. We have $u^{3^f} \equiv u \bmod \mathfrak{p}_L$ and

$$ua^3 \equiv u^{3^f}a^3 - u^{3^{f-1}}a + u^{3^{f-1}}a \equiv u^{3^{f-1}}a \bmod \ker\psi_L,$$

since it follows from the definition of ψ_L that $u^{3^f}a^3 - u^{3^{f-1}}a \in \ker\psi_L$. This implies $a\cdot(w - u^{3^{f-1}}) \in \ker\psi_L$ for all $a \in \mathcal{O}_L$ and hence $w \equiv u^{3^{f-1}} \bmod \mathfrak{p}_L$ (because $n(\psi_L) = -1$). Since the restriction of $\tilde\theta$ to $\mathcal{O}_L^\times$ has order 2, we have

$$\tilde\theta(y) = \tilde\theta(u)\tilde\theta(\varpi_L)^{3(1-\kappa)} = \tilde\theta(w)\tilde\theta(\varpi_L)^{3(1-\kappa)} = \tilde\theta(w)^3\tilde\theta(\varpi_L)^{3(1-\kappa)} = \tilde\theta(z)^3.$$

On the other hand, $\tilde\theta(y) = \theta(y)^3$, since $y \in H^\times$. Finally, recall that $\theta(\beta)^4 = 1$ for any $\beta \in \mathcal{W}(\overline{K}/H)$, hence

$$\tilde\theta(z) = \theta(y). \tag{5.11}$$

Assume now that $\mu(G_{t+1}) = \mathrm{Gal}(N^{unr}/S^{unr})$. In this case $l_2 = m-1 \geq m/2$ and $\mathrm{val}_H \mathrm{N}_{L/H}(x) \geq \kappa - 1 \geq m$. Hence, using (5.8) and (5.9) we get

$$\psi_L(zx) = \phi\left(1+\mathrm{Tr}_{L/H}(x)\right) = \psi_L(y\,\mathrm{Tr}_{L/H}(x)). \tag{5.12}$$

Note that without loss of generality we can assume $w \in \mathcal{O}_H^\times$. Indeed, since L is totally ramified over H, there exists $w_0 \in \mathcal{O}_H^\times$ such that $w - w_0 \in \mathfrak{p}_L$. Then $\psi_L(zx) = \psi_L(w_0\varpi_L^{1-\kappa}x)$ (because $n(\psi_L) = -1$) and $\tilde\theta(z) = \tilde\theta(w_0\varpi_L^{1-\kappa})$ (because $a(\tilde\theta) = 1$). For any $a \in \mathcal{O}_H$ equation (5.12) yields

$$a\cdot(w - y\,\mathrm{Tr}_{L/H}(\varpi_L^{\kappa-1})) \in \mathcal{O}_H \cap \ker\psi_L$$

and hence $w \equiv y\,\mathrm{Tr}_{L/H}(\varpi_L^{\kappa-1}) \bmod \mathfrak{p}_H$. Our next step is to calculate $y\,\mathrm{Tr}_{L/H}(\varpi_L^{\kappa-1})$. Denote $\varpi_L = \varpi$, $\kappa - 1 = j$, and let g be a generator of $\mathrm{Gal}(L/H)$, so that

$$\mathrm{Tr}_{L/H}(\varpi^j) = \varpi^j + g(\varpi)^j + g^2(\varpi)^j.$$

Note that $\mathrm{val}_L(y) + j + 2\alpha = 0$. We have $g(\varpi) = \varpi(1 + c\varpi^\alpha)$ for some $c \in \mathcal{O}_L^\times$ and $g(c) \equiv c \bmod \mathfrak{p}_L^{\alpha+1}$. Using this, it is easy to check that

$$\begin{aligned} \mathrm{Tr}_{L/H}(\varpi^j) &= \varpi^j + \varpi^j(1 + c\varpi^\alpha)^j + g(\varpi)^j(1 + g(c)g(\varpi)^\alpha)^j \equiv \\ &\equiv \varpi^j(3 + 3cj\varpi^\alpha + c^2 j(\alpha + j)\varpi^{2\alpha}) \bmod \mathfrak{p}_L^{j+2\alpha+1}. \end{aligned} \tag{5.13}$$

Let $b = e(H/\mathbb{Q}_3)$. Then $e(N/\mathbb{Q}_3) = 6b$ and $e(L/\mathbb{Q}_3) = 3b$. It is known (see e.g., [9], p. 72, Exc. 3c) that

$$n \leq \frac{1}{2}e(N/\mathbb{Q}_3) \ \text{ and } \ \alpha \leq \frac{1}{2}e(L/\mathbb{Q}_3),$$

which implies $t + \frac{s}{3} \leq 3b$ and since $s \neq 0$, we conclude that $2\alpha = t < 3b$. In other words, $\mathrm{val}_L 3 > 2\alpha$ and it follows from (5.13) that

$$y\,\mathrm{Tr}_{L/H}(\varpi^j) \equiv uc^2 j(\alpha + j) \bmod \mathfrak{p}_L.$$

Recall that $j = \kappa - 1 = \frac{\delta}{2} = \frac{t}{2} + \frac{s}{2}$, $\alpha = \frac{t}{2}$ and since $s \equiv 0 \bmod 3$, we have

$$w \equiv y\,\mathrm{Tr}_{L/H}(\varpi^j) \equiv 2c^2t^2u \bmod \mathfrak{p}_L.$$

Since w is a unit, we see that t is not divisible by 3 and since the restriction of $\tilde\theta$ to $\mathcal{O}_L^\times$ has order 2, we have

$$\tilde\theta(z) = \tilde\theta(w)\tilde\theta(\varpi_L)^{1-\kappa} = \theta(2)\tilde\theta(u)\tilde\theta(\varpi_L)^{1-\kappa}.$$

Recall that $y = u\varpi_L^{3(1-m)}$. Also, $1 - \kappa - 3(1 - m) = t$, where $t = 2\alpha$ and α is even, so t is divisible by 4 and hence

$$\tilde\theta(\varpi_L)^{1-\kappa} = \tilde\theta(\varpi_L)^{3(1-m)}.$$

Thus,

$$\tilde\theta(z) = \theta(2)\tilde\theta(y) = \theta(2)\theta(y)^3.$$

Writing $y \in H^\times$ as the product of a unit in $\mathcal{O}_H^\times$ and $\varpi_H^{\mathrm{val}_H y}$ and taking into account that $\theta(2) = (-1)^{f(H/\mathbb{Q}_3)}$, $\theta(\varpi_H)^2 = (-1)^{f(H/\mathbb{Q}_3)}$, $\mathrm{val}_H y = 1 - m$ is odd, and the restriction of θ to $\mathcal{O}_H^\times$ has order two, we get $\theta(2)\theta(y)^2 = 1$. Therefore,

$$\tilde\theta(z) = \theta(y). \tag{5.14}$$

General case. We now assume that F is an arbitrary finite Galois extension of K. Let F_t be the maximal tamely ramified extension of K contained in F. Since the group $\mathrm{Gal}(F/F_t)$ is a p-group with $p = 3$, it has a quotient that is a cyclic group of order 3, hence, there exists a finite Galois extension F_1 of F_t contained in F with $\mathrm{Gal}(F_1/F_t) \cong \mathbb{Z}/3\mathbb{Z}$. We put $L_1 = F_1H$, $L_t = L_0$ and for each $i \in \{0, 1\}$ denote $\phi_i = \mathrm{Res}_H^{L_i}\phi$, $\theta_i = \mathrm{Res}_H^{L_i}\theta$,

$\psi_0 = \psi_H \circ \mathrm{Tr}_{L_t/H}$. Also, let ψ_1 be a character of L_1 such that $\psi_1 = \psi_L$ on $\mathcal{O}_{L_1}$ and let $z_i \in L_i^\times$ be the analogues of z for ϕ_i, i.e., we have

$$\phi_i(1+a) = \psi_i(z_i a), \quad a \in L_i^\times,\ \mathrm{val}_{L_i}(a) \geq a(\phi_i)/2.$$

(Note that ψ_i is non-trivial and $a(\phi_i)$ is even by Lemma 1.9 and Lemma 1.1.) Using the inductive hypothesis on the order of $\mathrm{Gal}(L/L_t) \cong \mathrm{Gal}(F/F_t)$ together with (5.11) and (5.14), we get

$$\tilde{\theta}(z) = \theta_1(z_1) = \theta_0(z_0).$$

Finally, using (5.4) we have

$$\tilde{\theta}(z) = \theta_0(z_0) = \theta(y)^{[L_t:H]}.$$

6. Example of a non-Galois F/K

We keep the notation of Section 1 and assume $p = 3$, E has potential good reduction over K, σ_E is irreducible and wildly ramified.

Lemma 6.1. *Let H be unramified over K and let $u_{H/K} \in \mathcal{O}_H^\times$ satisfy $u_{H/K}^2 \in \mathcal{O}_K$ and $H = K(u_{H/K})$. Suppose F is a degree 3 extension of K such that the Galois closure F^g of F over K is totally ramified over K. Then there exists $t \in \mathbb{N}$ such that*

$$W(E/F) = (-1)^A \phi(u_{H/K})^{[F:K]},$$

where

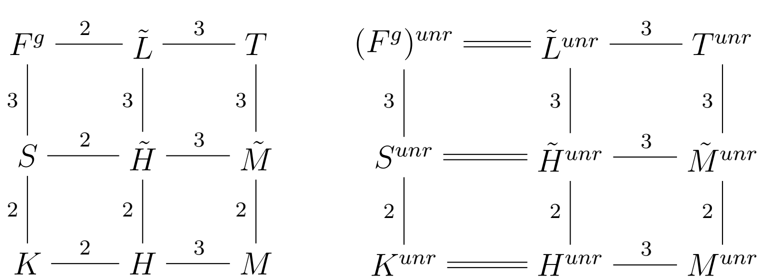
$$A = \begin{cases} a(\phi), & \text{if } F/K \text{ is Galois,} \\ a(\phi) + t, & \text{if } F/K \text{ is not Galois.} \end{cases} \tag{6.1}$$

In particular, if F is Galois over K, then $W(E/F) = W(E/K)$. If F is not Galois over K, then $W(E/F) = (-1)^t W(E/K)$ and both cases t is even and t is odd can occur.

Proof. The case when F is Galois over K is done in Proposition 3.1. Suppose F is not Galois over K, so that $\mathrm{Gal}(F^g/K) \cong S_3$. By Proposition 4 and its proof on p. 320 in [8] we have

$$W(E/F) = (-1)^{a(\sigma\otimes\tau)/2 - a(\tau)} \phi(u_{H/K})^{[F:K]}, \tag{6.2}$$

where $\tau = \mathrm{Ind}_K^F 1_F$. Let S/K be the maximal tamely ramified subextension of F^g/K, i.e., $[S:K] = 2$. Let $T = F^g M$, $\tilde{H} = SH$, $\tilde{L} = F^g H$, and $\tilde{M} = SM$. By Lemma 1.9 above, M is not contained in $\tilde{L}$ and hence we have the following diagrams of field extensions:



Let μ be a character of $S^\times$ such that $\ker\mu = \mathrm{Gal}(\overline{K}/F^g)$, let $\tilde{\mu} = \mathrm{Res}_S^{\tilde{H}}\mu$, $\tilde{\phi} = \mathrm{Res}_H^{\tilde{H}}\phi$. Then $a(\tilde{\phi}) = 2a(\phi) - 1$ by Lemma 1.2 and hence $a(\tilde{\phi})$ is odd. Also, it is easy to check that $\mu|_{K^\times} = 1_K$ and hence $a(\mu) = a(\tilde{\mu})$ is even by Lemma 4 on p. 132 in [2]. Let $G = \mathrm{Gal}(T^{unr}/H^{unr}) \cong S_3 \times \mathbb{Z}/3\mathbb{Z}$. Ramification groups of G have the form

$$G = G_0 \supset G_1 = \cdots = G_t \supset G_{t+1} = \{1\} \quad \text{or} \tag{6.3}$$

$$G = G_0 \supset G_1 = \cdots = G_t \supset G_{t+1} = \cdots = G_{t+s} \supset G_{t+s+1} = \{1\}, \tag{6.4}$$

where $G_1 = \mathrm{Gal}(T^{unr}/\tilde{H}^{unr}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and in (6.4) we have $G_{t+1} \cong \mathbb{Z}/3\mathbb{Z}$. It is easy to see that in case (6.3) and in case (6.4) with G_{t+1} embedded diagonally into G_1, we have $a(\tilde{\phi}) = a(\tilde{\mu})$, which is a contradiction, since by above one number is odd and the other is even. Thus (6.3) does not occur and in (6.4) we have either $G_{t+1} = \mathrm{Gal}(T^{unr}/\tilde{L}^{unr})$ or $G_{t+1} = \mathrm{Gal}(T^{unr}/\tilde{M}^{unr})$. If $G_{t+1} = \mathrm{Gal}(T^{unr}/\tilde{L}^{unr})$, then we have $a(\tilde{\phi}) = a(\tilde{\phi} \otimes \tilde{\mu}) = 1 + t + \frac{s}{3}$, $a(\tilde{\mu}) = 1 + t$. Since $a(\tilde{\phi})$ is odd and $a(\tilde{\mu})$ is even, we conclude that both t and $a(\tilde{\phi} \otimes \tilde{\mu})$ are odd. Analogously, if $G_{t+1} = \mathrm{Gal}(T^{unr}/\tilde{M}^{unr})$, then $a(\tilde{\phi}) = 1 + t$, $a(\tilde{\mu}) = a(\tilde{\phi} \otimes \tilde{\mu}) = 1 + t + \frac{s}{3}$, so that both t and $a(\tilde{\phi} \otimes \tilde{\mu})$ are even.

On the other hand, $\tau = \mathrm{Ind}_K^F 1_F \cong 1_K + \mathrm{Ind}_K^S \mu$ and using the inductive properties of function $a(-)$ one can see that

$$a(\sigma \otimes \tau)/2 - a(\tau) \equiv a(\phi) + a(\tilde{\phi} \otimes \tilde{\mu}) \equiv a(\phi) + t \bmod 2,$$

so that using (6.2) we have $A \equiv a(\phi) + t \bmod 2$ in (6.1).

We now show that both cases t is even and t is odd can occur. Let $K = \mathbb{Q}_3$ and let $B = \mathrm{Gal}(F^g/K) \cong S_3$, $C = \mathrm{Gal}(M/H) \cong \mathbb{Z}/3\mathbb{Z}$. Then the ramification groups of B and C are

$$B = B_0 \supset B_1 = \cdots = B_\alpha \supset B_{\alpha+1} = \{1\}, \quad B_1 \cong \mathbb{Z}/3\mathbb{Z},$$
$$C = C_0 = C_1 = \cdots = C_\beta \supset C_{\beta+1} = \{1\}.$$

Thus $a(\mu) = 1 + \alpha$ and $a(\phi) = 1 + \beta$. By the previous paragraph we also have two cases:

(1) $a(\mu) = 1 + t$, $a(\phi) = 1 + \frac{1}{2}(t + \frac{s}{3})$ or
(2) $a(\mu) = 1 + t + \frac{s}{3}$, $a(\phi) = 1 + \frac{t}{2}$.

On the other hand, $\alpha \le e(F^g/\mathbb{Q}_3)/2 = 3$, $\beta \le e(M/\mathbb{Q}_3)/2 = 1.5$ (see e.g., [9], p. 72, Exc. 3c). Thus $\beta = 1$ and since $a(\mu)$ is even, $\alpha = 1$ or $\alpha = 3$. Furthermore, by comparing $a(\mu)$ and $a(\phi)$ in terms of α, β with those in terms of t, s, we have two cases

(1) $\alpha = t$, $\beta = \frac{1}{2}(t + \frac{s}{3}) = 1$, hence $\alpha = t = 1$, or
(2) $\alpha = t + \frac{s}{3}$, $\beta = \frac{t}{2} = 1$, hence $t = 2$, $\alpha = 3$.

Consider the following elliptic curves over $\mathbb{Q}_3$:

$$E : y^2 + xy + y = x^3 - x^2 - 5x + 5,$$
$$E_1 : y^2 + y = x^3,$$
$$E_2 : y^2 + y = x^3 - 1.$$

Let Δ, Δ_1, and Δ_2 denote the minimal discriminants of E, E_1, and E_2, respectively. It is shown in [3] that E, E_1, and E_2 are of the Kodaira-Néron reduction type II, $\mathrm{val}_{\mathbb{Q}_3}(\Delta) = a(\sigma_E) = 4$, $\mathrm{val}_{\mathbb{Q}_3}(\Delta_1) = a(\sigma_{E_1}) = 3$, $\mathrm{val}_{\mathbb{Q}_3}(\Delta_2) = a(\sigma_{E_2}) = 5$. It is not hard to check that this implies, in particular, that E satisfies the hypothesis of Lemma 6.1. Also, denote $M_i = \mathbb{Q}_3(E_i[2])$, $i = 1, 2$. Then one can check that $\mathrm{Gal}(M_i/\mathbb{Q}_3) \cong S_3$ and M_i is totally ramified over $\mathbb{Q}_3$. For $i \in \{1, 2\}$ let ϕ_i denote the analogue of ϕ for E_i (note that each ϕ_i is wildly ramified), M_i will play a role of F^g in our notation above, and let α_i denote the analogue of α for M_i. From $a(\sigma_{E_1}) = 3$ and $a(\sigma_{E_2}) = 5$ we can find $a(\phi_1) = 2$, $a(\phi_2) = 4$. Moreover, note that $a(\phi_i) = \alpha_i + 1$, so that $\alpha_1 = 1$, $\alpha_2 = 3$. Hence by cases (1) and (2) above there exist non-Galois cubic extensions $F_i/\mathbb{Q}_3 \subset M_i/\mathbb{Q}_3$ such that $t(F_1) = 1$ and $t(F_2) = 2$. □

Acknowledgements. I would like to thank Kenneth Kramer and David Rohrlich for their interest in this work and useful inspiring discussions. I am also very grateful to Shinichi Kobayashi for answering a question regarding his paper [4]. Last but not least I would like to thank the anonymous referee for valuable suggestions that greatly improved the paper.

References

[1] P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 501–597. Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973.

[2] A. Fröhlich, J. Queyrut, *On the functional equation of the Artin L-function for characters of real representations*, Invent. Math. 20 (1973), 125–138.

[3] M. Kida, *Variation of the reduction type of elliptic curves under small base change with wild ramification*, Cent. Eur. J. Math. 1 (2003), no. 4, 510–560.

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

[5] A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. 69 (1990), no. 4, 353–385.

[6] D. E. Rohrlich, *Variation of the root number in families of elliptic curves*, Compositio Math. 87 (1993), no. 2, 119–151.

[7] D. E. Rohrlich, *Elliptic curves and the Weil-Deligne group*, Elliptic Curves and Related Topics (CRM Proc. Lecture Notes, 4, Amer. Math. Soc., Providence, RI, 1994), 125–157.

[8] D. E. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Compositio Math. 100 (1996), 311–349.

[9] J.-P. Serre, *Local fields* (Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979).

Department of Mathematics, CUNY Queens College, 65-30 Kissena Blvd., Flushing, NY 11367, USA, phone: 718-997-5800, fax: 718-997-5882

E-mail address: Maria.Sabitova@qc.cuny.edu