

# The local root number of elliptic curves with wild ramification

Shin-ichi Kobayashi

Received: 31 March 2000 / Revised version: 22 November 2001 /

Published online: 23 May 2002 – © Springer-Verlag 2002

**Abstract.** Let  $E$  be an elliptic curve over a number field  $F$ . The root number is conjecturally the sign of the functional equation of  $L$ -function of  $E/F$ . It is defined as the product of local signs over all places of  $F$ . The purpose of this paper is to describe this local sign by the coefficients of a Weierstraß equation of  $E$ .

*Mathematics Subject Classification (2000):* 11G07, 11G40, 11R32

## 1. Introduction

Let  $F$  be a number field of degree  $n$  over  $\mathbb{Q}$ . Let  $E$  be an elliptic curve over  $F$  with conductor  $N(E/F)$ . Then the Hasse-Weil conjecture asserts that the  $L$ -function  $L(E/F, s)$  has an analytic continuation to the whole plane and satisfies a certain functional equation. More precisely, if we put  $\Lambda(E/F, s) := N(E/F)^{s/2} (2(2\pi)^{-s} \Gamma(s))^n L(E/F, s)$ , then  $\Lambda(E/F, s)$  is conjectured to satisfy the functional equation

$$\Lambda(E/F, s) = w \Lambda(E/F, 2 - s),$$

where  $w$  is  $\pm 1$ . We are interested in this sign  $w$ . From the functional equation, we have  $w = (-1)^{\text{ord}_{s=1} L(E/F, s)}$ . If we assume that the Birch and Swinnerton-Dyer Conjecture is true, this would give  $w = (-1)^{\text{rank } E(F)}$ .

There is another definition of  $w$  due to Langlands which is independent of any conjecture. For each place  $v$  of  $F$ , we attach to  $E/F_v$  a complex representation  $\sigma_{E,v}$  of the Weil-Deligne group of  $F_v$ . We associate to  $\sigma_{E,v}$  the  $\epsilon$ -factor and its sign, the local root number  $w(E/F_v)$  (cf. Deligne [3], Rohrlich [9]). The (global) root number is defined as the product of  $w(E/F_v)$  over all places  $v$ . This number is conjectured to be  $w$ . For  $F = \mathbb{Q}$ , this conjecture is true since  $E$  is modular [1] and there is a one to one correspondence of  $\epsilon$ -factors under the local Langlands correspondence [2]. In this case, the local root number is the negative of the eigenvalue of the Atkin-Lehner operator.

S. KOBAYASHI

Graduate School of Mathematical Sciences, University of Tokyo, Komaba 3-8-1, Tokyo, 153-8914 Japan (e-mail: koba@ms406ss5.ms.u-tokyo.ac.jp)

We would like to determine local root numbers from the coefficients of a Weierstraß equation. Rohrlich [10] gives such a formula for  $w(E/F_v)$  when  $F_v = \mathbb{Q}_p$  with  $p \geq 5$  or when  $E/F_v$  has potential multiplicative reduction. Both are the cases in which  $\sigma_{E,v}$  is tamely ramified. In this paper we give a formula in the case of wild ramification of odd residue characteristic. Moreover, a formula for  $w(E/K)$  with any local field  $K$  of odd residue characteristic is given. (For  $K = \mathbb{Q}_2$  or  $\mathbb{Q}_3$ , Halberstadt [5] made a table of  $w(E/K)$  by an ad hoc method using Cremona’s table. His expression of  $w(E/\mathbb{Q}_3)$  is different from ours.) In particular, assuming the Birch and Swinnerton-Dyer Conjecture and under some assumption on the primes over 2 (good, potentially multiplicative, ...), the parity of the Mordell-Weil group of elliptic curves over any number field can be computed. As an example, we calculate the global root number of  $E : y^2 = x^3 + D$  over an arbitrary number field.

Our main theorem (Proposition 5.1, Corollary 5.4 and Theorem 5.9) is:

**Theorem 1.1.** *Let  $K$  be a local field with residue field  $k$  of odd characteristic  $p$ . Let  $E$  be an elliptic curve over  $K$  with potential good reduction. Let  $y^2 = x^3 + ax^2 + bx + c$  be a Weierstraß equation and  $\Delta$  the discriminant of the cubic polynomial above. We denote the quadratic residue symbol on  $k^\times$  by  $\left(\frac{\cdot}{k}\right)$  and the Hilbert symbol of  $K$  by  $(\cdot, \cdot)_K$ . We extend the residue symbol to  $k$  by putting  $\left(\frac{0}{k}\right) = 1$ .*

i) *If the Kodaira-Néron type of  $E$  is  $I_0$  or  $I_0^*$ , then*

$$w(E/K) = \left(\frac{-1}{k}\right)^{\frac{v(\Delta)}{2}}.$$

ii) *If the Kodaira-Néron type of  $E$  is  $III$  or  $III^*$ , then*

$$w(E/K) = \left(\frac{-2}{k}\right).$$

iii) *If the Kodaira-Néron type of  $E$  is  $II$ ,  $IV$ ,  $IV^*$  or  $II^*$ , there exists a Weierstraß equation such that  $3 \nmid v_K(c)$ . For such equation, we have*

$$w(E/K) = \delta(\Delta, c)_K \left(\frac{v_K(c)}{k}\right)^{v(\Delta)} \left(\frac{-1}{k}\right)^{\frac{v(\Delta)(v(\Delta)-1)}{2}}$$

where  $\delta = \pm 1$  and  $\delta = 1$  if and only if  $\Delta^{\frac{1}{2}} \in K$ .

*Remark 1.2.* i) For an odd  $p$ ,  $E$  has wild ramification if and only if  $p = 3$  and of type  $II$ ,  $IV$ ,  $IV^*$  or  $II^*$ . The formula in the other cases are obtained by arguments similar to Kramer-Tunnell [7] or Rohrlich [10]. We mention these cases for the sake of completeness.

- ii) For the case that  $E$  has potential multiplicative reduction ( $E$  is of type  $I_n$  or  $I_n^*$  if  $p$  is odd), see Rohrlich [9], p. 153.
- iii) If  $p \geq 5$ , the formula in *iii*) becomes more simple:  $\delta = \left(\frac{-3}{k}\right)$  and  $w(E/K) = \left(\frac{-1}{k}\right) \left(\frac{3}{k}\right)^{\frac{v(\Delta)}{2}+1}$ .

*Acknowledgements.* This paper is based on the author’s Master’s thesis. He expresses his sincere gratitude to his thesis advisor Takeshi Saito, who suggested the problem and read the manuscript carefully. The author is very grateful to the referee for helpful comments. He would like to thank Ken-ichi Bannai for reading the manuscript carefully. He also thanks Seidai Yasuda and Tadashi Ochiai for encouragement.

## 2. The definition of the local root number

We recall briefly the definition of the local root number. For more details, see Deligne [3] or Rohrlich [9].

Let  $K$  be a local field with residue field  $k$ . Let  $W_K$  be the Weil group of  $K$ , which is the subgroup of  $\text{Gal}(\overline{K}/K)$  generated by the inertia subgroup and a lifting of the Frobenius automorphism of  $\text{Gal}(\overline{k}/k)$ . For a finite extension  $L$  of  $K$ , we regard  $W_L$  as a subgroup of  $W_K$ . First we recall the  $\epsilon$ -factor and the local root number associated to a character.

**Definition 2.1.** Let  $\chi$  be a quasi-character  $\chi : L^\times \rightarrow \mathbb{C}^\times$  and  $\psi$  a non-trivial additive character  $\psi : L \rightarrow \mathbb{C}^\times$ . We identify  $\chi$  as a quasi-character of  $W_L$  by local class field theory. We choose the reciprocity map so that an arithmetic Frobenius corresponds to a uniformizer. Let  $dx$  be a Haar measure of  $L$ . Then the  $\epsilon$ -factor associated to  $\chi, \psi, dx$  is defined by

$$\epsilon(\chi, \psi, dx) = \begin{cases} \int_{h^{-1}O_L^\times} \chi^{-1}(x)\psi(x) dx & \text{if } \chi \text{ is ramified,} \\ \chi(h)\|h\|_L^{-1} \int_{O_L^\times} dx & \text{if } \chi \text{ is unramified,} \end{cases}$$

where  $h$  is an element of  $L^\times$  of valuation  $n(\psi) + a(\chi)$ ,  $n(\psi)$  is the largest integer  $n$  such that  $\psi(\pi^{-n}O_L) = 1$ ,  $a(\chi)$  is the conductor of  $\chi$ , and  $\| \cdot \|_L$  is the normalized absolute value of  $L$ .

The local root number  $w(\chi, \psi)$  is defined by

$$w(\chi, \psi) := \frac{\epsilon(\chi, \psi, dx_L)}{|\epsilon(\chi, \psi, dx_L)|}.$$

By definition, the local root number is a complex number of the absolute value 1.

Now we recall the definition of the local root number of elliptic curves. Let  $p$  be the residue characteristic of  $K$ . For a prime number  $l \neq p$ , let  $\sigma_E$  be the  $l$ -adic representation of  $W_K$  obtained by the Galois action on the Tate module  $V_l(E) = T_l(E) \otimes \mathbb{Q}_l$ . We extend  $\sigma_E$  to the complex representation

$$\sigma_E : W_K \longrightarrow \text{GL}_2(V_l(E) \otimes_{\mathbb{Q}_l} \mathbb{C})$$

by a fixed embedding  $\mathbb{Q}_l \hookrightarrow \mathbb{C}$ . If  $E$  has potential good reduction, then  $\sigma_E$  is continuous; that is  $\sigma_E$  factors through a finite quotient. Moreover, if  $p \neq 2$ ,  $\sigma_E$  is the direct sum of two characters or induced from a character of a quadratic extension  $H$  of  $K$  (see Proposition 3.3).

**Definition 2.2.** Suppose  $E$  has potential good reduction.

i) If  $\sigma_E = \chi \oplus \chi'$ , then  $w(E/K)$  is defined by

$$w(E/K) := w(\chi, \psi) w(\chi', \psi).$$

ii) If  $\sigma_E = \text{Ind}_{H/K} \chi$ , then  $w(E/K)$  is defined by

$$w(E/K) := w(\eta, \psi) w(\chi, \psi_H),$$

where  $\eta$  is the character  $K^\times \rightarrow K^\times/N_{H/K}H^\times \cong \pm 1 \in \mathbb{C}$ ,  $\psi$  a non-trivial additive character of  $K$ , and  $\psi_H = \psi \circ \text{Tr}_{H/K}$ .

There are many choices of  $\psi, l, \mathbb{Q}_l \hookrightarrow \mathbb{C}$  and  $\chi$ . However, since  $\sigma_E$  is essentially symplectic, the local root number  $w(E/K)$  is independent of these and is equal to  $\pm 1$  (cf. Deligne [3] or Rohrlich [9]).

### 3. The classification of $\sigma_E$

In this section, we give a criterion of irreducibility of  $\sigma_E$  in terms of the Kodaira-Néron type and the discriminant of the Weierstraß equation. We assume that  $P$  is odd and semi-simple [9], and  $E$  has potential good reduction. Then  $\sigma_E$  is semi-simple [9] and is reducible if and only if the image of  $\sigma_E$  is abelian.

We first recall some facts on the image of the inertia subgroup by  $\sigma_E$ .

**Theorem 3.1 (Kraus [6]).** *Let  $\Lambda$  be the image of the inertia group by  $\sigma_E$ . Then the field  $L = K^{\text{un}}(E[2], \Delta^{\frac{1}{4}})$  is the minimum extension of the maximal unramified extension  $K^{\text{un}}$  over which  $E$  has good reduction. In particular,  $\Lambda$  is isomorphic to  $\text{Gal}(L/K^{\text{un}})$ . The structure of  $\Lambda$  is*

- i)  $\Lambda \cong \{1\}$  if and only if  $E$  is of type  $I_0$
- ii)  $\Lambda \cong \mathbb{Z}/2\mathbb{Z}$  if and only if  $E$  is of type  $I_0^*$ .
- iii)  $\Lambda \cong \mathbb{Z}/4\mathbb{Z}$  if and only if  $E$  is of type  $III$  or  $III^*$ .

Suppose  $E$  is of type  $II, IV, IV^*$  or  $II^*$ . Then

- iv)  $\Lambda \cong \mathbb{Z}/3\mathbb{Z}$  if and only if  $v_K(\Delta) \equiv 0 \pmod{4}$ .
- v)  $\Lambda \cong \mathbb{Z}/6\mathbb{Z}$  if and only if  $v_K(\Delta) \equiv 2 \pmod{4}$ .
- vi)  $\Lambda \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$  if and only if  $v_K(\Delta) \equiv 1 \pmod{2}$ .

Now we give a criterion for the image of  $\sigma_E$  to be abelian.

**Proposition 3.2.** *i) Suppose  $E$  is of type  $I_0$  or  $I_0^*$ . The image of  $\sigma_E$  is abelian.  
 ii) Suppose  $E$  is of type  $III$  or  $III^*$ . The image of  $\sigma_E$  is abelian if and only if  $\left(\frac{-1}{k}\right) = 1$ .  
 iii) Suppose  $E$  is of type  $II$ ,  $IV$ ,  $IV^*$  or  $II^*$ . The image of  $\sigma_E$  is abelian if and only if  $\Delta^{\frac{1}{2}} \in K$ .*

*Proof.* We only prove case iii). The other cases are similar. In this case the Galois group of  $K(E[2])/K$  is cyclic of degree 3 (resp. the symmetric group  $\mathfrak{S}_3$ ) when  $\Delta^{\frac{1}{2}}$  is in  $K$  (resp. not in  $K$ ). If  $\Delta^{\frac{1}{2}} \in K$ , the extension  $K(E[2], \Delta^{\frac{1}{4}})/K$  is cyclic of order 3 or 6. Therefore it is easy to see that  $L = K^{\text{un}}(E[2], \Delta^{\frac{1}{4}})$  is an abelian extension over  $K$ . Since  $\text{Im } \sigma_E$  is a subgroup of  $\text{Gal}(L/K)$ , it is in fact abelian. If  $\Delta^{\frac{1}{2}} \notin K$ ,  $\text{Im } \sigma_E$  has a quotient isomorphic to  $\text{Gal}(K(E[2])/K) \cong \mathfrak{S}_3$ . Therefore  $\text{Im } \sigma_E$  is a posteriori non-abelian.  $\square$

**Proposition 3.3.** *i) If  $\text{Im } \sigma_E$  is abelian, then*

$$\sigma_E = \chi \oplus \chi^{-1} \parallel \|_K,$$

where  $\chi$  is a quasi-character of  $K^\times$  and  $\parallel \|_K$  is the normalized absolute value of  $K$ .

*ii) If  $\text{Im } \sigma_E$  is not abelian, then*

$$\sigma_E = \text{Ind}_{W_H}^{W_K} \chi = \text{Ind}_{H/K} \chi,$$

where  $H$  is  $K(\sqrt{-1})$  or  $K(\Delta^{\frac{1}{2}})$  according to if  $E$  is of case ii) or iii) in Proposition 3.2, and  $\chi$  is a quasi-character of  $H^\times$ .

*Proof.* Since  $\sigma_E$  is a semi-simple two dimensional complex representation (cf. Rohrlich [9]), it is decomposable if  $\text{Im } \sigma_E$  is abelian. Therefore case i) is a consequence of the determinant formula:  $\det \sigma_E = \parallel \|_K$ . Assume that  $\text{Im } \sigma_E$  is not abelian. By Proposition 3.2,  $W_H$  is a subgroup of  $W_K$  of index 2 and the image of  $\sigma_E|_{W_H}$  is abelian. Therefore  $\sigma_E|_{W_H}$  is a direct sum of two characters  $\chi, \chi'$  of  $H^\times$ . The proposition follows directly from this fact.  $\square$

#### 4. A ramification theory on elliptic curves

In this section we prove some facts on elliptic curves with wild ramification. For an odd  $p$ ,  $E$  has wild ramification if and only if  $p = 3$  and  $E$  is of type  $II$ ,  $IV$ ,  $IV^*$  or  $II^*$ .

**Proposition 4.1.** *Assume  $p \neq 2$  and  $E$  is of type  $II$ ,  $IV$ ,  $IV^*$  or  $II^*$ . There exists a Weierstraß equation  $y^2 = x^3 + ax^2 + bx + c$  such that  $3 \nmid v_K(c)$ .*

*Proof.* Let  $m$  be the number of irreducible components of the closed fibre of the minimal proper regular model of  $E$  over  $O_K^{\text{un}}$ . Using Tate’s algorithm, one finds a minimal Weierstraß equation such that  $v_K(c) = \frac{m+1}{2}$  (see Silverman [13], pp. 366-368). Since  $m$  is 1, 3, 7 or 9, this equation satisfies the condition of the proposition. (For  $p \geq 5$ , any equation such that  $a = 0$  is the one.)  $\square$

**Proposition 4.2.** *Let  $E$  be as in the previous proposition. Let  $y^2 = x^3 + ax^2 + bx + c$  be a Weierstraß equation such that  $3 \nmid v_K(c)$ . We denote  $K(E[2])$  by  $M$  and  $K(\Delta^{\frac{1}{2}})$  by  $H$ . Then the Artin conductor  $a(M/H)$  of  $M/H$  is  $v_H(\Delta^{\frac{1}{2}}/c) + 1$ .*

*Proof.* Let  $\pi_M$  be a uniformizer of  $M$  and  $g$  a generator of the cyclic group  $\text{Gal}(M/H)$  of order 3. We choose  $\alpha$ , a root of  $x^3 + ax^2 + bx + c = 0$  so that  $\Delta^{\frac{1}{2}} = N_{M/H}(\alpha - g\alpha)$ .

First we suppose  $a(M/H) = 1$ . (This condition is equivalent to the condition that  $p \geq 5$ .) We must show  $\Delta^{\frac{1}{2}}/c$  is a unit. Since  $a(M/H) = 1$  and  $M/H$  is totally ramified, we have  $g\pi_M/\pi_M \not\equiv 1 \pmod{\pi_M}$  and  $(g\pi_M/\pi_M)^3 \equiv N_{M/H}(g\pi_M/\pi_M) \equiv 1 \pmod{\pi_M}$ . Therefore  $g\pi_M/\pi_M$  modulo  $\pi_M$  is a cubic root of unity. Since  $v_M(\alpha) = v_H(c)$  is not a multiple of 3,  $g\alpha/\alpha \equiv (g\pi_M/\pi_M)^{v_M(\alpha)}$  is also a cubic root of unity. Since  $p \neq 3$ ,  $g\alpha/\alpha - 1$  is a unit, and  $\Delta^{\frac{1}{2}}/c = N_{M/H}(g\alpha/\alpha - 1)$  is also a unit.

The case  $a = a(M/H) \neq 1$  (or equivalently the case  $p = 3$ ) follows similarly. In this case, by the definition of the conductor in terms of the ramification subgroups with the lower numbering, there exists a unit  $u$  such that  $g\pi_M/\pi_M = 1 + \pi_M^{a-1}u$ . Similarly, there exists an integer  $x$  such that  $g\alpha/\alpha = 1 + \pi_M^{a-1}x$ . Taking  $v_M(\alpha)$ -th power of  $g\pi_M/\pi_M = 1 + \pi_M^{a-1}u$ , we have

$$\left(\frac{g\pi_M}{\pi_M}\right)^{v_M(\alpha)} \equiv 1 + v_M(\alpha)\pi_M^{a-1}u \pmod{\pi_M^a}. \tag{1}$$

On the other hand, let  $w$  be a unit such that  $\alpha = \pi_M^{v_M(\alpha)}w$  and let  $y$  be such that  $gw/w = 1 + y$ . Since  $M/H$  is totally ramified, we have  $v_M(gz - z) \geq a$  for all integer  $z$ . Thus we have  $y \equiv 0 \pmod{\pi_M^a}$ , and

$$\frac{g\alpha}{\alpha} \equiv \left(\frac{g\pi_M}{\pi_M}\right)^{v_M(\alpha)} \times \frac{gw}{w} \equiv \left(\frac{g\pi_M}{\pi_M}\right)^{v_M(\alpha)} \pmod{\pi_M^a}. \tag{2}$$

By (1) and (2), we have multiplicatively

$$\frac{g\alpha}{\alpha} - 1 \equiv v_M(\alpha)\left(\frac{g\pi_M}{\pi_M} - 1\right) \pmod{U_M^1} \tag{3}$$

where  $U_M^1 = 1 + \pi_M\mathcal{O}_M$ . Taking the norm  $N_{M/H}$ , we have

$$\frac{\Delta^{\frac{1}{2}}}{c} \equiv v_M(\alpha)^3 N_{M/H}\left(\frac{g\pi_M}{\pi_M} - 1\right) \pmod{U_H^1}. \tag{4}$$

The valuation of the right hand side is  $a - 1$ . Hence the proposition follows.  $\square$

*Remark 4.3.* We will use the above congruence (4) in the proof of Proposition 5.6. In the congruence, we can replace  $v_M(\alpha)^3$  by  $v_H(c)$  since  $v_M(\alpha)^3 = v_H(c)^3 \equiv v_H(c) \pmod 3$ .

As a corollary, we give a variant of Ogg’s formula. (A proof of the usual Ogg’s formula is also given.)

**Corollary 4.4.** *Assume  $p \neq 2$  and  $E$  is of type II, IV, IV\* or II\*. Let  $y^2 = x^3 + ax^2 + bx + c$  be a Weierstraß equation of  $E$  such that  $3 \nmid v_K(c)$ . Let  $a(E/K)$  be the Artin conductor of  $E/K$ . Then we have*

$$a(E/K) = v_K(\Delta) - 2v_K(c) + 2.$$

*In particular,  $\Delta$  is minimal if and only if  $v_K(c) = \frac{m+1}{2}$ . Moreover, we always have  $v_K(c) \equiv \frac{m+1}{2} \pmod 6$  and this congruence determines  $m$ .*

*Proof.* First suppose  $\sigma_E = \text{Ind}_{H/K} \chi$ . The conductor  $a(E/K)$  and  $a(\chi)$  are related by the conductor formula of induced representations (cf. Serre [11], Chapter VI, Proposition 4). Precisely,  $a(E/K) = 2a(\chi)$  if  $H/K$  is unramified, and  $a(E/K) = a(\chi) + 1$  if  $H/K$  is ramified. We show that  $a(\chi)$  is equal to the conductor of  $M/H$ . If  $p \geq 5$ , then  $M/H$  is tame, so both conductors are 1. Suppose  $p = 3$ . By Theorem 3.1, we may consider  $\chi$  to be a faithful character of  $W_H/\text{Gal}(\overline{K}/L)$ . Since the pro- $p$ -part of the inertia subgroup of  $\text{Gal}(L/H)$  is canonically isomorphic to  $\text{Gal}(M/H)$ , the conductors are equal. Hence, by Proposition 4.2, we have  $a(\chi) = v_H(\Delta^{\frac{1}{2}}/c) + 1$ . The formula follows from these facts. The case  $\sigma_E = \chi \oplus \chi^{-1} \parallel_K$  follows similarly.

Using Tate’s algorithm, we find a minimal Weierstraß equation such that  $v_K(c) = \frac{m+1}{2}$ . Hence, from our formula, we reprove Ogg’s formula:  $a(E/K) = v_K(\Delta_{\min}) - m + 1$ . Subtracting Ogg’s formula from our formula, we obtain  $v_K(\Delta) - v_K(\Delta_{\min}) = 2(v_K(c) - \frac{m+1}{2})$ . So  $\Delta$  is minimal if and only if  $v_K(c) = \frac{m+1}{2}$ . Since  $v_K(\Delta)$  is unique modulo 12, we always have  $v_K(c) \equiv \frac{m+1}{2} \pmod 6$ . The last assertion follows from the fact that  $m$  is equal to 1, 3, 7, or 9.  $\square$

**5. Proofs of the formulas for  $w(E/K)$**

The proof of Theorem 1.1 is divided into three cases: a)  $\sigma_E$  is reducible, b)  $\sigma_E$  is induced from a character of the unramified quadratic extension of  $K$ , c)  $\sigma_E$  is induced from a character of a totally ramified quadratic extension of  $K$ . For cases a), b), the proofs are essentially due to Rohrlich [10]. However, case c) needs different considerations.

*5.1. a)  $\sigma_E$  is reducible*

**Proposition 5.1.** *Suppose  $\sigma_E = \chi \oplus \chi^{-1} \parallel_K$ . Then Theorem 1.1 is true.*

*Proof.* We have  $w(E/K) = \chi(-1)$  (cf. [9] p. 145). We may regard  $\chi|_{O_K^\times}$  as a faithful character of  $\text{Gal}(L/K^{\text{un}})$ . Suppose  $E$  is of type  $III$  or  $III^*$ . Then by Theorem 3.1,  $\chi|_{O_K^\times}$  is a character of order 4, and  $\chi^2|_{O_K^\times}$  should be a character induced by the quadratic residue symbol. We have  $\sqrt{-1} \in O_K^\times$  by Proposition 3.2. Hence  $\chi(-1) = \chi^2(\sqrt{-1}) = \left(\frac{\sqrt{-1}}{k}\right) = \left(\frac{-2}{k}\right)$ . The last equation follows from  $-2 = \sqrt{-1}(1 + \sqrt{-1})^2$ . The other cases can be proved similarly.  $\square$

5.2. *b)  $\sigma_E$  is induced from a character of the unramified quadratic extension of  $K$*

This is the case that  $E$  is of type  $III$  or  $III^*$  and  $\sqrt{-1} \notin K$  or  $E$  is of type  $II, IV, IV^*$  or  $II^*$  and  $K(\Delta^{\frac{1}{2}})$  is the unramified quadratic extension of  $K$  (cf. Proposition 3.2 and 3.3).

As before, we denote by  $\eta$  the character  $K^\times \rightarrow K^\times/N_{H/K}H^\times \cong \pm 1$ . For  $a, b \in \mathbb{C}^\times$ , we write  $a \sim b$  if  $ab^{-1}$  is a positive real number.

**Proposition 5.2 (Kramer-Tunnell [7], Rohrlich [10]).** *Suppose that  $\sigma_E = \text{Ind}_{H/K}\chi$  and  $H/K$  is unramified. Then*

$$w(E/K) \sim (-1)^{v_H(2\xi)+a(\chi)} \chi(\xi)$$

where  $\xi \in H$  is any element such that  $K(\xi) = H$  and  $\xi^2 \in K$ .

*Proof.* This is a corollary of Fröhlich-Queyrut’s theorem. See Rohrlich [10], the proof of Proposition 2, especially p. 130.  $\square$

**Proposition 5.3.** *i) Suppose that  $E$  is of type  $III$  or  $III^*$  and  $\sqrt{-1} \notin K$ . Then*

$$w(E/K) = \left(\frac{-2}{k}\right).$$

*ii) Suppose that  $E$  is of type  $II, IV, IV^*$  or  $II^*$  and  $K(\Delta^{\frac{1}{2}})$  is the unramified quadratic extension of  $K$ . Then*

$$w(E/K) = (-1)^{\frac{a(E/K)+v(\Delta)}{2}} \left(\frac{-1}{k}\right)^{\frac{v(\Delta)}{2}}$$

where  $a(E/K)$  is the conductor of  $E/K$ .

*Proof.* i) We apply Proposition 5.2 to  $\xi = \sqrt{-1}$ . Then we have  $w(E/K) = -\chi(\sqrt{-1})$ . Since  $H/K$  is the unramified quadratic extension, we have  $\sqrt{2} \in H$ . Then similar arguments as in the proof of Proposition 5.1 show that  $\chi(\sqrt{-1}) = \chi^{-2}(\sqrt{2})\chi^2(1 + \sqrt{-1}) = \left(\frac{2}{k}\right)$ .

ii) We apply Proposition 5.2 to  $\xi = \Delta^{\frac{1}{2}}$ . Since  $a(\chi) = a(E/K)/2$  by the conductor formula of induced representation (cf. Serre [11], Chapter VI, Proposition 4), we have  $w(E/K) \sim (-1)^{\frac{a(E/K)+v(\Delta)}{2}} \chi(\Delta^{\frac{1}{2}})$ . We let  $\Delta^{\frac{1}{2}} = \pi_K^n u$  for  $u \in O_H^\times$ . Similar arguments with the proof of Proposition 5.1 show that  $\chi(u) = \left(\frac{u}{k_H}\right)^{v(\Delta)/2} = (-1)^{v(\Delta)/2} \left(\frac{-1}{k}\right)^{v(\Delta)/2}$ . Since  $\chi|_{K^\times} = \eta \cdot \|\cdot\|_K$  by the determinant formula of induced representations (cf. Deligne [3], Proposition 1.2), we have  $\chi(\pi_K) \sim -1$ . Hence  $\chi(\Delta^{\frac{1}{2}}) \sim \left(\frac{-1}{k}\right)^{v(\Delta)/2}$ .  $\square$

**Corollary 5.4.** *Suppose that  $E$  is of type  $II, IV, IV^*$  or  $II^*$  and  $K(\Delta^{\frac{1}{2}})$  is the unramified quadratic extension of  $K$ . Then Theorem 1.1 is true.*

*Proof.* The valuation of  $\Delta$  is even. By Corollary 4.4, the Hilbert symbol  $(\Delta, c)_K$  is  $(-1)^{v_K(c)} = (-1)^{\frac{m+1}{2}}$ . The Proposition follows from Proposition 4.1 and 5.3 ii).  $\square$

5.3. *c)  $\sigma_E$  is induced from a character of a totally ramified quadratic extension of  $K$ .*

This is the case that  $p = 3, E$  is of type  $II, IV, IV^*$  or  $II^*$  and  $v_K(\Delta)$  is odd. This is also equivalent to the case that the conductor  $a(E/K)$  is odd and greater than 1.

We first fix notations. As before, let  $M = K(E[2])$  and  $H = K(\Delta^{\frac{1}{2}})$ . In our case,  $M/H$  is a totally ramified cyclic extension of degree 3. We fix an isomorphism  $\phi : \text{Gal}(M/H) \rightarrow \mathbb{F}_3$  and let  $g_\phi = \phi^{-1}(1)$ . We also fix  $\Delta^{\frac{1}{2}}$  as  $(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$  where  $\alpha, \beta, \gamma$  are the  $x$ -coordinate of 2-torsion points of  $E$  such that  $g_\phi(\alpha) = \beta, g_\phi(\beta) = \gamma$ . Let  $\Delta^{\frac{1}{4}}$  be one quadratic root of  $\Delta^{\frac{1}{2}}$  and we put  $N = K(E[2], \Delta^{\frac{1}{4}})$ . We extend  $g_\phi$  to an element of  $W_H$  so that it fixes each element of  $K^{\text{un}}$  and  $\Delta^{\frac{1}{4}}$ .

We first recall a formula for the  $\epsilon$ -factor of a character of even conductor.

**Proposition 5.5.** *Let  $L$  be a local field. Let  $\chi, \psi$  and  $dx$  be as in Definition 2.1. We take  $\psi$  so that  $n(\psi) = -1$ . Assume that the conductor  $a(\chi)$  is even. Then*

$$\epsilon(\chi, \psi, dx) \sim \chi^{-1}(\xi)\psi(\xi),$$

where  $\xi$  is an element of  $L$  which satisfies  $\chi(1+x) = \psi(\xi x)$  for all  $x$  such that  $v_L(x) \geq \frac{a(\chi)}{2}$ .

*Proof.* The integral in the definition of  $\epsilon(\chi, \psi, dx)$  is computed directly using the relation  $\chi(1+x) = \psi(\xi x)$ . See calculations in Deligne [3] 4.16 or 11.6.  $\square$

For  $a, b \in \mathbb{C}^\times$ , we write  $a \approx b$  if  $ab^{-1}$  is in the multiplicative group generated by the positive real numbers and the 3-power roots of unity.

**Proposition 5.6.** *Suppose  $\sigma_E = \text{Ind}_{H/K} \chi$  and  $H/K$  is totally ramified. Let  $y^2 = x^3 + ax^2 + bx + c$  be a Weierstraß equation such that  $3 \nmid v_K(c)$ . Then  $\chi(g_\phi)$  is a cubic root of unity, and*

$$w(E/K) \approx \chi(-\Delta^{\frac{1}{2}}/v_H(c)c) G$$

where  $G$  is the Gauss sum  $\sum_{u \in k^\times} \left(\frac{u}{k}\right) \chi(g_\phi)^{-\text{Tr}_{k/\mathbb{F}_3}(u)}$ .

*Proof.* By Theorem 3.1, we may consider  $\chi$  to be a faithful character of  $W_H/\text{Gal}(\bar{K}/L)$ . The restriction of  $g_\phi$  to  $L$  is regarded as an element of  $\text{Gal}(L/K^{\text{un}}(\Delta^{\frac{1}{4}})) \cong \text{Gal}(M/H)$ . Hence  $\chi(g_\phi)$  is a cubic root of unity.

By definition, we have  $w(E/K) = w(\chi, \psi_H)w(\eta, \psi)$ . We choose  $\psi$  so that  $n(\psi) = -1$  and the restriction of  $\psi$  to  $O_K$  is equal to the map  $O_K \rightarrow \mathbb{C}^\times, x \mapsto \chi(g_\phi)^{-\text{Tr}_{k/\mathbb{F}_3}(\bar{x})}$ . Then, since  $a(\eta) = 1$ , direct calculation of the integral in the definition of  $w(\eta, \psi)$  shows that  $w(\eta, \psi) \sim G$ . We calculate  $w(\chi, \psi_H)$ . Since  $a(E/K) = a(\chi) + 1$  by the conductor formula of induced representation (cf. Serre [11], Chapter VI, Proposition 4), the conductor  $a(\chi)$  is even. Hence by Proposition 5.5, we have  $w(\chi, \psi_H) \approx \chi^{-1}(\xi)$ .

Let  $\delta_\phi = N_{M/H}(1 - g_\phi \pi_M / \pi_M)$ . Then by Serre [11], Chapter XV, §3, exercise 1, we have the commutative diagram:

$$\begin{CD} U_H^t/U_H^{t+1} @>r>> \text{Gal}(M/H) \\ @V\phi_UVV @VV\phi V \\ k @>\text{Tr}_{k/\mathbb{F}_3}>> \mathbb{F}_3, \end{CD}$$

where  $t = a(M/H) - 1$ ,  $r$  is the reciprocity map and  $\phi_U$  is the isomorphism  $x \mapsto (x-1)/\delta_\phi$ . This diagram shows that for each  $v \in O_H$ , we have  $\chi(1 + \delta_\phi v) = \chi(g_\phi)^{\text{Tr}_{k/\mathbb{F}_3}(\bar{v})}$ . On the other hand, let  $u = \xi \delta_\phi$ . Then by the definition of  $\xi$ , we have  $\chi(1 + \delta_\phi v) = \psi_H(uv) = \psi(-uv) = \chi(g_\phi)^{\text{Tr}_{k/\mathbb{F}_3}(\bar{uv})}$ . Hence  $u \in U_H^1$  and  $\chi^{-1}(\xi) \approx \chi(\delta_\phi)$ . In the proof of Proposition 4.2 (see also Remark 4.3), we already have  $-\Delta^{\frac{1}{2}}/c \equiv v_H(c) \delta_\phi \pmod{U_H^1}$ . Hence the proposition follows.  $\square$

Next we also express  $\chi(-\Delta^{\frac{1}{2}}/v_H(c)c)$  using Gauss sum  $G$ . We need the following proposition.

**Proposition 5.7.** *Let  $\Phi \in W_N$  be a lifting of the “arithmetic” Frobenius of  $\text{Gal}(\bar{k}/k)$ . We have an equality of operators*

$$\Phi = - \sum_{u \in k^\times} \left(\frac{u}{k}\right) g_\phi^{-\text{Tr}_{k/\mathbb{F}_3}(u)}$$

on the Tate module  $V_l(E)$ .

We first prove Theorem 1.1.

**Proposition 5.8.** *Under the same notation as in Proposition 5.6, we have*

$$\chi(-\Delta^{\frac{1}{2}}/v_H(c)c) \approx (\Delta, v_H(c)c)_K(-G)^{v_K(\Delta)}.$$

*Proof.* First we compute  $\chi(v_H(c)c)$ . By the determinant formula of induced representations (cf. Deligne [3], Proposition 1.2), we have  $\chi|_{K^\times} = \eta \cdot \| \cdot \|_K$ . By definition,  $\eta$  is the homomorphism  $x \mapsto (\Delta, x)_K$ . Hence  $\chi(v_H(c)c) \approx (\Delta, v_H(c)c)_K$ .

Next we show  $\chi(-\Delta^{\frac{1}{2}}) = (-G)^{v_K(\Delta)}$ . Let  $\Phi$  be an arithmetic Frobenius of  $W_N$  and let  $\Psi$  be an element of  $W_H$  corresponding to  $-\Delta^{\frac{1}{2}}$  by the reciprocity law of  $H$ . Since  $-\Delta^{\frac{1}{2}}$  is the norm from  $N$  (i.e.  $-\Delta^{\frac{1}{2}} = N_{M/H}(\beta - \alpha)$  and  $-\Delta^{\frac{1}{2}} = N_{K(\Delta^{\frac{1}{4}})/H}(\Delta^{\frac{1}{4}})$ ),  $\Psi$  fixes each element of  $N$ . Therefore  $\Psi \circ \Phi^{-v_K(\Delta)}$  fixes  $L = K^{\text{un}}N$ . Hence we have  $\chi(-\Delta^{\frac{1}{2}}) = \chi(\Psi) = \chi(\Phi^{v_K(\Delta)})$ . Since  $\sigma_E|_H = \chi \oplus \chi^{-1} \| \cdot \|_H$ , there exists a one dimensional subspace  $V_\chi$  of  $V_l(E) \otimes_{\mathbb{Q}_l} \mathbb{C}$  where  $W_H$  acts by  $\chi$ . By looking at the action of the operators in Proposition 5.7 on  $V_\chi$ , we have  $\chi(\Phi) = -G$ . □

**Theorem 5.9.** *Suppose  $\sigma_E = \text{Ind}_{H/K} \chi$  and  $H/K$  is totally ramified. Then there exists a Weierstraß equation  $y^2 = x^3 + ax^2 + bx + c$  such that  $3 \nmid v_K(c)$ . For such equation, we have*

$$w(E/K) = -(\Delta, v_K(c)c)_K \left(\frac{-1}{k}\right)^{\frac{v_K(\Delta)-1}{2}}.$$

*Proof.* The first part is nothing more than Proposition 4.1. We have  $w(E/K) \approx -(\Delta, v_H(c)c)_K G^{v_K(\Delta)+1}$  by Proposition 5.6 and 5.8. The square of the Gauss sum is real and its sign is  $\left(\frac{-1}{k}\right)^{\frac{v_K(\Delta)+1}{2}}$ . Hence we have  $G^{v_K(\Delta)+1} \approx \left(\frac{-1}{k}\right)^{\frac{v_K(\Delta)+1}{2}}$ . This proves the theorem modulo “ $\approx$ ”, but since both sides are  $\pm 1$ , they are in fact equal. □

Now we prove Proposition 5.7. We translate it geometrically.

By Theorem 3.1,  $E$  has good reduction over  $N$ . Let  $\mathcal{E}_N$  be a proper smooth model of  $E$  over  $O_N$  and let  $\mathcal{E}_L$  be the scalar extension to  $O_L$ . We denote its reduction by  $\tilde{\mathcal{E}}_L$ . Let  $W_K^+$  be the semigroup in  $W_K$  generated by the inertia group and a lifting of the “geometric” Frobenius of  $\text{Gal}(k/k)$ . We translate  $g \in W_K^+$  to an endomorphism of  $\tilde{\mathcal{E}}_L$ .

We fix an isomorphism  $\iota : E \otimes_K N \rightarrow \mathcal{E}_N \otimes_{O_N} N$  over  $N$ . For  $g \in W_K^+$ , there exists a unique morphism  $\mathcal{E}_L \rightarrow \mathcal{E}_L$  which makes the following diagram commutative (the uniqueness of the proper smooth model).

$$\begin{array}{ccc} E \otimes L & \xrightarrow{1 \otimes g} & E \otimes L \\ \downarrow \iota & & \downarrow \iota \\ \mathcal{E}_L \otimes L & \longrightarrow & \mathcal{E}_L \otimes L. \end{array}$$

By reduction, we get an endomorphism of  $\widetilde{\mathcal{E}}_L$ . Since this endomorphism may not be defined over  $\bar{k}$ , we compose it with some (positive) power of the absolute Frobenius of  $\widetilde{\mathcal{E}}_L$  induced from the  $p$ -th power endomorphism of the function field. Then we get an endomorphism of  $\widetilde{\mathcal{E}}_L$  over  $\bar{k}$ . We also denote this endomorphism by  $g$ .

The following theorem is the geometric translation of Proposition 5.7.

**Theorem 5.10.** *Let  $\Phi \in W_N$  be any lifting of the “geometric” Frobenius of  $\text{Gal}(\bar{k}/k)$ . As endomorphisms of  $\widetilde{\mathcal{E}}_L$ , we have*

$$\Phi = - \sum_{u \in k^\times} \left( \frac{u}{k} \right) g_\phi^{\text{Tr}_{k/\mathbb{F}_3}(u)}.$$

Since the natural map on valued points  $\mathcal{E}_L(O_L) \rightarrow \mathcal{E}_L(L)$  is bijective and the reduction map  $\mathcal{E}_L(O_L) \rightarrow \widetilde{\mathcal{E}}_L(\bar{k})$  is injective on  $l^n$ -torsion points, Proposition 5.7 follows from the above theorem. We remark that the morphism  $1 \otimes g : E \otimes L \rightarrow E \otimes L$  induces the Galois action  $g^{-1}$  on valued points  $E(L)$  and the absolute Frobenius acts trivially on  $\widetilde{\mathcal{E}}_L(\bar{k})$ .

Let us investigate  $\mathcal{E}_N$  and  $\iota$  explicitly.

**Proposition 5.11.** *Suppose that  $E$  is given by a Weierstraß equation  $y^2 = (x - \alpha)(x - \beta)(x - \gamma)$  over  $N$ . Let  $\mathcal{E}_N$  be the closure in  $\mathbb{P}^3_{O_N}$  of the affine scheme defined by  $Y^2 = X(X + 1)(X - \frac{\gamma - \alpha}{\alpha - \beta})$ . Then  $\mathcal{E}_N$  is a proper smooth model of  $E$  over  $O_N$ . Its special fibre is given by the equation:  $Y^2 = X^3 - X$ .*

*Proof.* First, we show the generic fibre of  $\mathcal{E}_N$  is isomorphic to  $E$  over  $N$ . We let  $\sqrt{\alpha - \beta}$  be one of the square roots of  $\alpha - \beta$ . Since  $\frac{\alpha - \beta}{\beta - \gamma}, \frac{\alpha - \beta}{\gamma - \alpha} \in U_M^1$  (look at the norm  $N_{M/H}$  on the residue field) and  $(\alpha - \beta)^3 = \Delta^{\frac{1}{2}} \frac{\alpha - \beta}{\beta - \gamma} \frac{\alpha - \beta}{\gamma - \alpha}$  has square roots in  $N$ ,  $\sqrt{\alpha - \beta}$  is an element of  $N$ . The isomorphism  $\iota : E \otimes N \rightarrow \mathcal{E}_N \otimes N$  is given by  $x = (\alpha - \beta)X + \alpha, y = \sqrt{\alpha - \beta}^3 Y$ . The last assertion, which proves smoothness, follows from  $\frac{\gamma - \alpha}{\alpha - \beta} \in U_M^1$ . □

We fix  $\iota$  as the isomorphism in the above proof.

**Proposition 5.12.** *Let  $\Phi$  be as in Theorem 5.10. As an endomorphism of  $\widetilde{\mathcal{E}}_L : Y^2 = X^3 - X, \Phi$  is the Frobenius:  $X \mapsto X^q, Y \mapsto Y^q$  where  $q = \#k$  and  $g_\phi$  is the automorphism  $\rho : X \mapsto X + 1, Y \mapsto Y$ .*

*Proof.* For  $g \in W_K^+$ , we see the induced morphism  $\mathcal{E}_L \otimes L \rightarrow \mathcal{E}_L \otimes L$  explicitly. This is actually the morphism  ${}^s(\mathcal{E}_L \otimes L) \rightarrow \mathcal{E}_L \otimes L$  over  $L$ , where  ${}^s$  denotes the twist of the base by  $g$ . On the function field this is given by  $({}^s\iota)^{-1} \circ \iota$  where  ${}^s\iota$  is the morphism obtained by acting  $g$  on the coefficients of  $\iota$ . For  $g_\phi$ , this is

$$(X, Y) \mapsto \left( \frac{\alpha - \beta}{\beta - \gamma}(X + 1), \frac{\sqrt{\alpha - \beta}^3}{g_\phi(\sqrt{\alpha - \beta}^3)} Y \right).$$

Since this map is defined over the integer ring  $O_N$ , it induces a morphism  $\mathcal{E}_L \rightarrow \mathcal{E}_L$ . Since  $g_\phi$  fixes  $K^{\text{un}}$  and  $\sqrt{\alpha - \beta}$ , the reduction of the morphism is defined over  $\bar{k}$  and is equal to  $\rho$ . For  $\Phi$ , it fixes  $N$ . So the proof is straightforward.  $\square$

Now Theorem 5.10 is a consequence of the following proposition.

**Proposition 5.13.** *(A Gauss sum in  $\text{End}(\tilde{E})$ .) Let  $\mathbb{F}_q$  be the finite extension of  $\mathbb{F}_3$  of  $q$  elements. Let  $\tilde{E}/\mathbb{F}_q$  be the elliptic curve defined by  $y^2 = x^3 - x$ . We denote the automorphism  $x \mapsto x + 1, y \mapsto y$  by  $\rho$  and the  $q$ -th power Frobenius by  $\text{Fr}_q$ . Then*

$$\text{Fr}_q = - \sum_{u \in \mathbb{F}_q^\times} \left( \frac{u}{\mathbb{F}_q} \right) \rho^{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(u)}.$$

*Proof.* First, we consider the case  $\mathbb{F}_q = \mathbb{F}_3$ . Then the formula says that three points  $(x + 1, y), (x - 1, -y), (x^3, y^3)$  of  $\tilde{E}$  are on the same line. The line through the first two points is given by  $Y = y(X - x)$  on the  $XY$ -plane. Since  $y^2 = x^3 - x$ , the third point is also on this line. The general case follows from the Hasse-Davenport theorem :  $-\sum_{u \in \mathbb{F}_q^\times} \left( \frac{u}{\mathbb{F}_q} \right) \rho^{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(u)} = (-\sum_{u \in \mathbb{F}_3^\times} \left( \frac{u}{\mathbb{F}_3} \right) \rho^u)^{[\mathbb{F}_q:\mathbb{F}_3]}$ .  $\square$

### 6. An example of calculations of root numbers

We calculate the global root number of  $E : y^2 = x^3 + D$  over a number field  $F$ . It is computed in Liverance [8] when  $F = \mathbb{Q}$ . However, it would be interesting to see the root numbers over various number fields since if the root number changed for some field extension, there would be a new rational point of  $E$  of infinite order in that field.

First we determine the local root numbers at the primes over 2.

**Proposition 6.1.** *Let  $K$  be a local field of even residue characteristic with the valuation  $v$ . Let  $E$  be an elliptic curve  $E : y^2 = x^3 + D$  over  $K$ . Then*

$$w(E/K) = \begin{cases} (-1, D)_K & \text{if } v(\Delta) \equiv 0 \pmod{3} \text{ or } \sqrt{-3} \in K, \\ (-1)^{a/2+v(2)}(3, D)_K & \text{otherwise,} \end{cases}$$

where  $a = a(E/K)$  is the conductor of  $E/K$ .

*Proof.* Since  $E$  has complex multiplication, it has potential good reduction. Let  $L$  be the field  $K^{\text{un}}(E[3])$ . Then the kernel of  $\sigma_E$  is  $\text{Gal}(\bar{K}/L)$ . It is easy to see that the defining equation of  $x$ -coordinate of the non-trivial 3-torsion points is  $3x^4 + 12Dx = 0$  (cf. Serre [12], p. 305). Hence  $L = K^{\text{un}}(\sqrt[3]{D}, \Delta^{\frac{1}{3}})$  and  $\Delta = -2^4 3^3 D^2$ . Therefore  $\text{Gal}(L/K)$  is abelian if and only if  $v(\Delta) \equiv 0 \pmod{3}$  or  $\sqrt{-3} \in K$  (cf. Proposition 3.2). Then the root number is determined similarly as in b) of the previous section. We prove it only for the case

that  $\text{Gal}(L/K)$  is not abelian. Let  $H$  be  $K(\sqrt{-3})$ . Then  $\sigma_E$  is induced by a character  $\chi$  of  $H$  (cf. Proposition 3.3). Hence by Proposition 5.2, we have  $w(E/K) \sim (-1)^{v_H(2\sqrt{-3}+a(\chi))} \chi(\sqrt{-3})$ . Since  $\chi|_{O_H}$  is a faithful character of  $\text{Gal}(H(\sqrt{D}, \Delta^{\frac{1}{3}})/H)$ , we have  $\chi(\sqrt{-3}) \sim (\sqrt{-3}, D)_H = (3, D)_K$ .  $\square$

Since the local root number over an archimedean field is always equal to  $-1$ , the global root number is computed by Theorem 1.1 and Proposition 6.1. Under some assumptions, we can determine it more explicitly.

**Theorem 6.2.** *Suppose  $v(D) = 0$  or  $6 \nmid v(D)$  for all finite places  $v$  of  $F$ . For the places  $v$  over 3, we assume  $3 \nmid v(D)$  and for the places over 2, we assume  $2 \nmid v(D)$ . Then the global root number  $w$  is given by*

$$w = (-1)^{r_1+r_2+\frac{f'_3+n}{2}} \delta_2 \delta_3 \left(\frac{d}{3}\right).$$

The notations are the following:

$r_1 + r_2$  is the number of the infinite places of  $F$ ,  
 $n = [F : \mathbb{Q}]$  and  $f_v$  is the residue index  $[k_v : \mathbb{F}_p]$ ,

$f'_3 := \sum'_{v|3} f_v$ , where the sum is over the places such that  $2 \nmid v(3)$ ,

$\delta_2 := (-1)^{\sum'_{v|2} 1+v(2)}$ , where  $\sum'$  is over the places such that  $\sqrt{-3} \notin F_v$  and  $v(D) \not\equiv v(2) \pmod{3}$ ,

$\delta_3 := \prod_{v|3} \delta_v$ , where  $\delta_v = \pm 1$  and  $\delta_v = 1$  if and only if  $\sqrt{-3} \in F_v$ ,

$d := \prod_{v|3} v(D)^{n_v} \prod_{p|\Delta, p \neq 3} p^{f_p}$ , where  $n_v = [F_v : \mathbb{Q}_p]$  and  $f_p = \sum_{v|p} f_v$ .

*Proof.* Let  $F_v$  be the completion of  $F$  at  $v$ . We first determine the local root numbers over  $F_v$  of the residue characteristic  $p \geq 5$ . By Tate's algorithm,  $E/F_v$  is of type  $I_0^*$  if  $3 \mid v(D)$ . Otherwise, the type is  $II, IV, IV^*$  or  $II^*$ . Hence, by Theorem 1.1, we have  $w(E/F_v) = (3, D)_{F_v} \left(\frac{-3}{k_v}\right)$  (since  $6 \nmid v(D)$ ,  $v(D)$  is odd if  $3 \mid v(D)$ ). By the quadratic reciprocity law, we have  $\prod_{v|p} \left(\frac{-3}{k_v}\right) = \left(\frac{p}{3}\right)^{f_p}$ . For  $p = 3$ ,  $E$  is of type  $II, IV, IV^*$  or  $II^*$ . Therefore

$$w(E/F_v) = \delta_v (3, D)_{F_v} \left(\frac{v(D)}{k_v}\right)^{v(3)} \left(\frac{-1}{k_v}\right)^{\frac{v(3)(v(3)+1)}{2}}$$

by Theorem 1.1. We have  $\left(\frac{v(D)}{k_v}\right)^{v(3)} = \left(\frac{v(D)}{3}\right)^{n_v}$  and  $\prod_{v|3} \left(\frac{-1}{k_v}\right)^{\frac{v(3)(v(3)+1)}{2}} = (-1)^{\frac{\sum_v e_v^2 f_v + n}{2}} = (-1)^{\frac{n+f'_3}{2}}$ . For  $p = 2$ ,  $E$  is of type  $II, I_0^*$  or  $II^*$  by Tate's algorithm. Therefore,  $a(E/F_v)/2 \equiv v(D) \equiv 1 \pmod{2}$ . We have  $(-3, D)_{F_v} = (-3, N_{K/\mathbb{Q}_2} D)_{\mathbb{Q}_2} = (-1)^{f_v v(D)} = (-1)^{f_v}$ .

Hence the formula follows from the product formula of the Hilbert symbol.  $\square$

If  $F$  is unramified at 2 and 3, the type of  $E$  is determined in terms of  $D$  and we get a similar formula of the root number without the assumption on  $v(D)$ .

**Corollary 6.3.** *If  $F$  contains  $\mathbb{Q}(\sqrt{-3})$ , then  $w = 1$ .*

*Proof.* Easy computation. □

Since  $w = 1$ , the rank of  $E/F$  would be even. In fact, the rank of a CM elliptic curve  $E/F$  is even if all endomorphisms (over  $\mathbb{C}$ ) are defined on  $F$ , for  $E(F) \otimes \mathbb{Q}$  is an  $\text{End}(E) \otimes \mathbb{Q}$ -vector space.

## References

1. C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over  $\mathbb{Q}$ : wild 3-adic exercises. *J. Amer. Math. Soc.* **14** (2001), no. 4, 843–939
2. H. Carayol, Sur les représentations  $l$ -adiques associées aux formes modulaires de Hilbert, *Ann. Sci. École Norm. Sup. (4)* **19** (1986), no. 3, 409–468
3. P. Deligne, Les constantes des équations fonctionnelles des fonctions L, *Modular Functions of One Variable II*, Lect. Note in Math 349
4. A. Fröhlich and J. Queyruet, On the functional equation of the Artin  $L$ -function for characters of real representations, *Invent Math.* **20** (1973), 125–138
5. E. Halberstadt, Signes locaux des courbes elliptiques en 2 et 3. *C. R. Acad. Sci. Paris Série, I Math.* **326** (1998), no. 9, 1047–1052
6. A. Kraus, Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta Math.* **69** (1990), no. 4, 353–385
7. K. Kramer and J. Tunnell, Elliptic curves and local  $\epsilon$ -factors, *Compositio Math.* **46** (1982), 307–352
8. E. Liverance, A formula for the root number of a family of elliptic curves. *J. Number Theory* **51** (1995), 288–305
9. D. E. Rohrlich, Elliptic curves and the Weil-Deligne group. *Elliptic curves and related topics*, 125–157, CRM Proc. Lecture Notes, 4, Amer. Math. Soc., Providence, RI, 1994
10. D. E. Rohrlich, Variation of the root number in families of elliptic curves, *Compositio Math.* **87** (1993), 119–151
11. J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1962
12. J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972), 259–331
13. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*. Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994
14. J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, *Modular Functions of One Variable IV*, Lect. Note in Math 476