J. Math. Sci. Univ. Tokyo
22 (2015), 247–260.

Local Root Numbers of Elliptic Curves over Dyadic Fields

By Naoki Imai

With a great respect for Professor Kunihiko Kodaira

Abstract. We consider an elliptic curve over a dyadic field with additive, potentially good reduction. We study the finite Galois extension of the dyadic field generated by the three-torsion points of the elliptic curve. As an application, we give a formula to calculate the local root number of the elliptic curve over the dyadic field.

Introduction

Let K be a non-archimedean local field with residue field k. Let E be an elliptic curve over K. If E has potentially multiplicative reduction, then E has split multiplicative reduction over a quadratic extension of K (cf. Proposition 1.1). On the other hand, if E has potentially good reduction, then we need a bigger extension to get good reduction in general.

We assume that E has potentially good reduction. Let p be the characteristic of k. We consider a finite Galois extension L of K, which is obtained by adding the coordinates of the $(p+1)$-torsion points of E. Then E has good reduction over L (cf. Proposition 1.2). The inertia subgroup of $\mathrm{Gal}(L/K)$ is studied by Kraus in [Kra90] if the characteristic of K is zero. We will extend the results to positive characteristic cases. Actually, if $p \geq 3$, the proof in [Kra90] works without change. Hence, we focus on the case where $p = 2$. If $p = 2$, then K is called a dyadic field. Further, we study the Galois group itself not only the inertia subgroup.

The local root numbers of elliptic curves are studied by many people. If the characteristic of K is zero, they are calculated by Rohrlich in [Roh96] except the case where $p = 2, 3$ and the elliptic curves have additive potentially good reduction. Halberstadt gives a table of local root numbers of

2010 *Mathematics Subject Classification.* 11G07, 11S40.
Key words: Root number, elliptic curve.

elliptic curves in [Hal98] if K is $\mathbb{Q}_2$ or $\mathbb{Q}_3$. Kobayashi calculates them in [Kob02] in the case where $p \geq 3$ and E has potentially good reduction. Using a result of [Kra90], Dokchitser-Dokchitser shows a formula calculating the local root numbers of elliptic curves over 2-adic fields in [DD08]. In this paper, we extend the formula of Dokchitser-Dokchitser to the positive characteristic cases using the study of the Galois extension L over K. See Theorem 4.6 for details of the formula.

In Section 1, we recall basic facts on elliptic curves over non-archimedean local fields. In Section 3, we study the Galois group $\mathrm{Gal}(L/K)$ and give a classification in Theorem 3.8. In Section 4, we show a formula calculating the root numbers of elliptic curves over dyadic fields. The proof of the formula is rather independent of the classification in Theorem 3.8.

Acknowledgment. The author is grateful to a referee for careful reading and a number of suggestions for improvements.

Notation. In this paper, we use the following notation. Let K be a non-archimedean local field with a residue field k of characteristic p. We write $\mathcal{O}_K$ for the ring of integers in K. Let v be the normalized valuation of K. We take an algebraic closure K^{ac} of K. For any finite extension F of K, let W_F denote the Weil group of F.

1. Elliptic Curve

Let E be an elliptic curve over K. Then E has a minimal Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_1, \ldots, a_4, a_6 \in \mathcal{O}_K$. We put

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= a_1a_3 + 2a_4,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 24b_4,\\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6,\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,
\end{aligned}$$

$$j = c_4^3/\Delta.$$

Then we have

$$4b_8 = b_2b_6 - b_4^2, \tag{1.1}$$

$$1728\Delta = c_4^3 - c_6^2. \tag{1.2}$$

as in [Tat75, (1.3)]. Then E has potentially good reduction if and only if $v(j) \geq 0$ (cf. [Sil09, VII. Proposition 5.5]).

The following fact is due to Tate:

Proposition 1.1 (cf. [Sil09, Appendix C. Theorem 14.1.(d)]). *If $v(j) < 0$, then E has split multiplicative reduction over a quadratic extension of K.*

For a finite extension F over K inside K^{ac} and a set S of points of $E(K^{\mathrm{ac}})$, let $F(S)$ be the extension of F inside K^{ac} obtained by adding the x and y coordinates of the points of S to F. For such an F and a point P of E, we simply write $F(P)$ for $F(\{P\})$. For a positive integer m, let $E[m]$ denote the kernel of the m-multiplication map on $E(K^{\mathrm{ac}})$.

Proposition 1.2. *Let $m \geq 3$ be an integer that is prime to p. If $v(j) \geq 0$, then E has good reduction over $K(E[m])$.*

Proof. This follows from [ST68, Corollary 3] and [Sil09, VII. Proposition 5.4.(a)]. □

2. Group Theory

For a natural number n, we write $\mathfrak{S}_n$ for the symmetric group of degree n, C_n for the cyclic group of order n, D_{2n} for the dihedral group of order $2n$, SD_{2^n} for the semidihedral group of order 2^n. We write Q_8 for the quaternion group. Here we recall an elementary fact on group theory.

Proposition 2.1. *The natural action of $GL_2(\mathbb{F}_3)$ on $\mathbb{P}^1(\mathbb{F}_3)$ defines a surjection $GL_2(\mathbb{F}_3) \to \mathfrak{S}_4$. Furthermore, 2-2 partitions of the 4 point set $\{1,2,3,4\}$ defines a surjection $\mathfrak{S}_4 \to \mathfrak{S}_3 = D_6$. For a subgroup of $GL_2(\mathbb{F}_3)$, we consider the image and kernel of the restriction of $GL_2(\mathbb{F}_3) \to D_6$ to the subgroup. Then a list of the isomorphism classes of subgroups of $GL_2(\mathbb{F}_3)$ is given by the following table:*

Ker \ Im	C_1	C_2	C_3	D_6
C_1	C_1	C_2	C_3	D_6
C_2	C_2	$C_2 \times C_2$	C_6	D_{12}
C_4	C_4	C_8, D_8	-	-
Q_8	Q_8	SD_{16}	$SL_2(\mathbb{F}_3)$	$GL_2(\mathbb{F}_3)$

Further, the images under the surjection $GL_2(\mathbb{F}_3) \to \mathfrak{S}_4$ of subgroups that are isomorphic to C_8 and D_8 are isomorphic to C_4 and $C_2 \times C_2$ respectively.

PROOF. We treat only distinction between C_8, D_8 and Q_8. It is well-known that the kernel of the surjection $GL_2(\mathbb{F}_3) \to D_6$ is the unique subgroup that is isomorphic to Q_8. The subgroups that are isomorphic to C_8 are conjugate to the subgroup generated by

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Hence, their images in $\mathfrak{S}_4$ are isomorphic to C_4. On the other hand, the subgroups that are isomorphic to D_8 are conjugate to the subgroup generated by

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Hence, their images in $\mathfrak{S}_4$ are isomorphic to $C_2 \times C_2$. □

3. Galois Group

We assume that $p \neq 3$. Let E be an elliptic curve over K with additive, potentially good reduction. We put $L = K(E[3])$ and $G = \mathrm{Gal}(L/K)$. Then E has good reduction over L by Proposition 1.2.

We put

$$g(x) = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8.$$

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of $g(x)$ in K^{ac}.

PROPOSITION 3.1. *(1) The x coordinates of the 8 non-trivial points of $E[3]$ are the roots of $g(x)$.*
(2) The set of the third roots of Δ is

$$\{b_4 - 3(\alpha_1\alpha_2 + \alpha_3\alpha_4),\ b_4 - 3(\alpha_1\alpha_3 + \alpha_2\alpha_4),\ b_4 - 3(\alpha_1\alpha_4 + \alpha_2\alpha_3)\}.$$

(3) The degree $[L : K]$ is not divided by 3 if and only if $\Delta \in (K^\times)^3$.

PROOF. These are proved in [Ser72, 5.3.b)]. □

We take $\Delta^{1/3} \in K^{\mathrm{ac}}$ so that $\Delta^{1/3} \in K$ if $\Delta \in (K^\times)^3$. We assume that $\Delta^{1/3} = b_4 - 3(\alpha_1\alpha_2 + \alpha_3\alpha_4)$ by renumbering $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. We put $K_1 = K(\Delta^{1/3})$, $s = \alpha_1 + \alpha_2$ and $t = \alpha_1\alpha_2$.

LEMMA 3.2. *(1) We have*

$$g(x) = (x^2 - sx + t)\big(3x^2 + (3s + b_2)x - (3t + \Delta^{1/3} - b_4)\big).$$

(2) We have $[K_1(s,t) : K_1] \le 2$.

PROOF. The claim (1) follows from $b_2 = -3(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)$ and $\Delta^{1/3} = b_4 - 3(\alpha_1\alpha_2 + \alpha_3\alpha_4)$.

We take a basis of $E[3]$. Then we have an embedding $G \hookrightarrow GL_2(\mathbb{F}_3)$, and the roots of $g(x)$ correspond the elements of $\mathbb{P}^1(\mathbb{F}_3)$. By considering $\mathfrak{S}_4$ as the automorphism group of $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, we have a surjection $GL_2(\mathbb{F}_3) \to \mathfrak{S}_4$ as in Proposition 2.1.

Then K_1 corresponds to the stabilizer in G of the partition $\{\{\alpha_1, \alpha_2\}, \{\alpha_3, \alpha_4\}\}$, which is the intersection of G and a subgroup of $GL_2(\mathbb{F}_3)$ that is isomorphic to SD_{16}. On the other hand, $K_1(s,t)$ corresponds to the stabilizer in G of the subset $\{\alpha_1, \alpha_2\}$, which is the intersection of G and a subgroup of $GL_2(\mathbb{F}_3)$ that is isomorphic to D_8. Therefore, we have $[K_1(s,t) : K_1] \le |SD_{16}/D_8| = 2$. □

We take a non-trivial third root of unity $\zeta_3 \in K^{\mathrm{ac}}$.

LEMMA 3.3. *We have $\zeta_3, \Delta^{1/3} \in L$.*

PROOF. We have $\zeta_3 \in L$ by the existence of the Weil pairing, and $\Delta^{1/3} \in L$ by $\Delta^{1/3} = b_4 - 3(\alpha_1\alpha_2 + \alpha_3\alpha_4)$. □

The following lemma and proposition are variants of results in [Kra90]. The proofs in [Kra90] work also in our situation. We recall the proofs for completeness.

LEMMA 3.4 (cf. [Kra90, Lemme 5]). *Let P be a non trivial element of $E[3]$. Then $[L : K(\zeta_3, P)]$ divides 3.*

PROOF. We take a point Q of $E[3]$ so that (P, Q) is an ordered basis of $E[3]$. Then it gives an injective group homomorphism $\rho\colon G \to GL_2(\mathbb{F}_3)$. Then the image of $\mathrm{Gal}\big(L/K(\zeta_3, P)\big)$ under ρ is contained in

$$\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \;\middle|\; b \in \mathbb{F}_3 \right\},$$

because $\det \rho$ is the mod 3 cyclotomic character. Hence, we have the claim. □

PROPOSITION 3.5 (cf. [Kra90, Proposition 3]). *Let K' be an extension of $K_1(\zeta_3)$ contained in L. Then the followings are equivalent:*

(1) $[L : K'] \leq 2$.

(2) $g(x)$ *has a root in* K'.

(3) $g(x)$ *has the all roots in* K'.

PROOF. It is trivial that (3) implies (2). We assume (2). Let α be a root of $g(x)$ in K. Let P be a point of $E[3]$ whose x coordinate is α. Then we have $[L : K'(P)] = 1$ by Proposition 3.1.(3) and Lemma 3.4. Hence we have (1).

We assume (1). Taking a basis of $E[3]$, we have an injective group homomorphism $\rho\colon G \to GL_2(\mathbb{F}_3)$. Then the image of $\mathrm{Gal}(L/K')$ under ρ is contained in

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Then, the all roots of $g(x)$ is fixed by the action of $\mathrm{Gal}(L/K')$. Hence, we have (3). □

The following lemma is also a variant of a lemma in [Kra90]. Our proof is different from that in [Kra90].

LEMMA 3.6 (cf. [Kra90, Lemme 6]). *Let $\alpha_0 \in K^{\mathrm{ac}}$ be a root of $g(x)$. Then $K_1(\zeta_3, \alpha_0)$ contains s and t.*

PROOF. By Lemma 3.5, $K_1(\zeta_3, \alpha_0)$ contains the all roots of $g(x)$. Hence the claim follows. □

We simply write α for α_1, and take $\beta \in K^{\mathrm{ac}}$ such that

$$\beta^2 + a_1\alpha\beta + a_3\beta = \alpha^3 + a_2\alpha^2 + a_4\alpha + a_6.$$

LEMMA 3.7. *We have $L = K_1(\zeta_3, \alpha, \beta)$.*

PROOF. By Lemma 3.4, $[L : K_1(\zeta_3, \alpha, \beta)]$ divides 3. On the other hand, 3 does not divide $[L : K_1]$ by Proposition 3.1.(2). Hence the claim follows. □

THEOREM 3.8. *(1) Suppose $\zeta_3 \in K$ and $\Delta^{1/3} \in K$.*

(a) If $\alpha \in K$, then $G \simeq C_2$.

(b) If $\alpha \notin K$ and $s, t \in K$, then $G \simeq C_4$.

(c) If $K(s,t) \neq K$ and $\alpha \in K(s,t)$, then $G \simeq C_4$.

(d) If $K(s,t) \neq K$ and $\alpha \notin K(s,t)$, then $G \simeq Q_8$.

(2) Suppose $\zeta_3 \in K$ and $\Delta^{1/3} \notin K$.

(a) If $\alpha, \beta \in K_1$, then $G \simeq C_3$.

(b) If $\alpha \in K_1$ and $\beta \notin K_1$, then $G \simeq C_6$.

(c) If $K_1(s,t) \neq K_1$, then $G \simeq SL_2(\mathbb{F}_3)$.

(3) Suppose $\zeta_3 \notin K$ and $\Delta^{1/3} \in K$.

(a) If $\alpha \in K(\zeta_3)$, then $G \simeq C_2 \times C_2$.

(b) If $\alpha \notin K(\zeta_3)$, $s, t \in K(\zeta_3)$ *and* $K(s,t) \neq K$, *then* $G \simeq C_8$.

(c) If $\alpha \notin K(\zeta_3)$ *and* $s, t \in K$, *then* $G \simeq D_8$.

(d) If $K(\zeta_3, s, t) \neq K(\zeta_3)$ *and* $\alpha \in K(\zeta_3, s, t)$, *then* $G \simeq D_8$.

(e) If $K(\zeta_3, s, t) \neq K(\zeta_3)$, *then* $\alpha \notin K(\zeta_3)$ *and* $G \simeq SD_{16}$.

(4) Suppose $\zeta_3 \notin K$ *and* $\Delta^{1/3} \notin K$.

(a) If $\alpha, \beta \in K_1(\zeta_3)$, *then* $G \simeq D_6$.

(b) If $\alpha \in K_1(\zeta_3)$ *and* $\beta \notin K_1(\zeta_3)$, *then* $G \simeq D_{12}$.

(c) If $K_1(\zeta_3, s, t) \neq K_1(\zeta_3)$, *then* $\alpha \notin K_1(\zeta_3)$ *and* $G \simeq GL_2(\mathbb{F}_3)$.

PROOF. By taking a basis of $E[3]$, we consider G as a subgroup of $GL_2(\mathbb{F}_3)$. We note that (1), (2), (3) and (4) in this theorem correspond the 1st, 3rd, 2nd and 4th column in Proposition 2.1 respectively. We use Proposition 2.1 without mention.

We prove (1). Since E has bad reduction, the claim (1a) follows from Lemma 3.5. If $\alpha \notin K$, then $[L : K] \geq 4$ by Proposition 3.1.(3) and Lemma 3.5. On the other hand, if $s, t \in K$, then $[L : K] \leq 4$ by Lemma 3.7. Hence the claim (1b) follows. By applying Lemma 3.5 to $K(s,t)$, we have the claims (1c) and (1d).

We prove (2). The claims (2a) and (2b) follows from Lemma 3.7. If $K_1(s,t) \neq K_1$, $[L : K_1] \geq 4$ by (1c) and (1d). Hence we have (2c), because there is no subgroup of $SL_2(\mathbb{F}_3)$ with order 12.

We prove (3). By replacing K by $K(\zeta_3)$ in (1), we have (3a), (3e), and $[L : K] = 8$ in the case (3b), (3c) and (3d). In the case (3b), $g(x)$ is irreducible by Lemma 3.2.(1). Then G act transitively on the roots of $g(x)$. Hence we have (3b). In the case (3c), we have two distinct quadratic extensions $K(\zeta_3)$ and $K(\alpha)$ of K. In the case (3d), we have two distinct quadratic extensions $K(\zeta_3)$ and $K(s,t)$ of K. Hence we have (3c) and (3d).

By replacing K by $K(\zeta_3)$ in (2), we obtain (4). □

REMARK 3.9. In some case, the inertia subgroup I of G is determined by the Kodaira-Néron type of E. In fact, $I \simeq \mathbb{Z}/3\mathbb{Z}$ if and only if the Kodaira-Néron type of E is IV or IV^*, where we use the Kodaira symbol after [Kod64]. This fact can be proved similarly as [Kra90, Théorème 2] also in the positive characteristic case.

4. Root Number

We assume that K is a dyadic field. Let $\phi\colon \mathbb{F}_2 \to \mathbb{C}^\times$ be the non-trivial character. We take an additive character $\psi\colon K \to \mathbb{C}^\times$ such that $\psi(a) = \phi(\mathrm{Tr}_{k/\mathbb{F}_2}(\bar{a}))$ for $a \in \mathcal{O}_K$, where $\bar{a}$ denotes the image of a in k. Let $d\mu$ be a Haar measure on K. Let σ be a finite dimensional smooth representation of W_K over $\mathbb{C}$. Then we can consider a local ϵ-factor $\epsilon(\sigma, \psi, d\mu) \in \mathbb{C}^\times$ as in [Del73, §4]. We put

$$w(\sigma, \psi) = \frac{\epsilon(\sigma, \psi, d\mu)}{|\epsilon(\sigma, \psi, d\mu)|},$$

which is independent of the choice of $d\mu$. We call $w(\sigma, \psi)$ the local root number of σ with respect to ψ. For a finite extension F over K and a finite dimensional smooth representation of W_F over $\mathbb{C}$, we always consider the root number with respect to $\psi \circ \mathrm{Tr}_{F/K}$. We simply write $w(\sigma)$ for $w(\sigma, \psi)$ in the sequel.

Let $T_3(E)$ be the 3-adic Tate module of E. We put $V_3(E) = T_3(E) \otimes_{\mathbb{Z}_3} \mathbb{Q}_3$. We take an embedding $\mathbb{Q}_3 \to \mathbb{C}$. Then the natural action of W_K on $V_3(E)$ induces a smooth representations

$$\sigma_E\colon W_K \to \mathrm{Aut}(V_3(E) \otimes_{\mathbb{Q}_3} \mathbb{C}),$$

because E has potentially good reduction. We put $w(E/K) = w(\sigma_E)$, which is called the local root number of E.

Using results in Section 3, we can extend results in [DD08] to positive characteristic cases. Here, we treat only the most non-trivial case, where $G \simeq GL_2(\mathbb{F}_3)$.

Remark 4.1. Our choice of ψ is different from that in [DD08]. It is the reason why the formulas in Lemma 4.2 and Theorem 4.6 look different from those in [DD08].

We assume that $G \simeq GL_2(\mathbb{F}_3)$. We put $f = [k : \mathbb{F}_2]$ and $n(E) = v(\Delta)$. We note that f is odd and $K(\zeta_3)$ is the unramified quadratic extension by the assumption. Let $\eta\colon W_K \to \mathbb{C}^\times$ be the unramified character that sends the arithmetic Frobenius to $(\sqrt{2}i)^f$. We put $\sigma_{E,\eta} = \sigma \otimes \eta^{-1}$.

LEMMA 4.2 (cf. [DD08, Lemma 1]). *The W_K-representation $\sigma_{E,\eta}$ factors through G. Moreover, we have*

$$w(E/K) = (-i)^{f(n(E)-2)} w(\sigma_{E,\eta}).$$

PROOF. The proof in [DD08, Lemma 1] works also in our situation. □

LEMMA 4.3. *The discriminant of $g(x)$ is equal to $-27\Delta^2$.*

PROOF. Using Proposition 3.1.(2), we see that the discriminant of $g(x)$ is equal to

$$\begin{aligned} 3^6 \prod_{1\le i<j\le 4} (\alpha_i - \alpha_j)^2 \\ &= (\Delta^{1/3} - \zeta_3\Delta^{1/3})^2(\Delta^{1/3} - \zeta_3^2\Delta^{1/3})^2(\zeta_3\Delta^{1/3} - \zeta_3^2\Delta^{1/3})^2 \\ &= -27\Delta^2. \ \square \end{aligned}$$

We put

$$\begin{aligned} s' &= \zeta_3(\alpha_1 + \alpha_2) + \zeta_3^2(\alpha_3 + \alpha_4), \\ t' &= \zeta_3\alpha_1\alpha_2 + \zeta_3^2\alpha_3\alpha_4 \end{aligned}$$

and $M = K_1(s', t')$.

LEMMA 4.4. *We have an isomorphism $\mathrm{Gal}(L/M) \simeq C_8$.*

PROOF. Let h_0 be the element of $\mathfrak{S}_4 = \mathrm{Aut}(\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\})$ defined by

$$\alpha_1 \mapsto \alpha_3 \mapsto \alpha_2 \mapsto \alpha_4 \mapsto \alpha_1.$$

Let H be the preimage of the subgroup generated by h_0 under $G \to \mathfrak{S}_4$. Then H is isomorphic to C_8 by Proposition 2.1. Any lift of h_0 in G send ζ_3 to ζ_3^2, because it fixes $\Delta^{1/3}$ and permutes $\zeta_3\Delta^{1/3}$ and $\zeta_3^2\Delta^{1/3}$. Hence,

H fixes s' and t' by the definition. This implies that $H \subset \mathrm{Gal}(L/M)$ and $[M : K_1] \leq 2$. Therefore, it suffices to show $M \neq K_1$.

Since $K_1(s,t) \neq K_1$ by the assumption $G \cong GL_2(\mathbb{F}_3)$, either

$$\alpha_1 + \alpha_2 \neq \alpha_3 + \alpha_4 \quad \text{or} \quad \alpha_1\alpha_2 \neq \alpha_3\alpha_4$$

holds. Hence, M is not fixed by $\mathrm{Gal}(L/K_1)$. This show $M \neq K_1$. □

Let $\mathcal{E}$ be the elliptic curve over $\mathbb{F}_2$ defined by $x^3 = y^2 + y$. The following fact is well-known:

Lemma 4.5 (cf. [IT12]). *Let m be a positive integer. Then we have $\sharp\mathcal{E}(\mathbb{F}_{2^m}) = 2^m + 1 - (\sqrt{2}i)^m - (-\sqrt{2}i)^m$.*

By Lemma 4.2, we consider $\Sigma_{E,\eta}$ as a representation of G. We take a character $\chi\colon \mathrm{Gal}(L/M) \to \mathbb{C}^\times$ such that $\Sigma_{E,\eta}|_{\mathrm{Gal}(L/M)}$ is the direct sum of χ and its conjugate. For a character ϕ of a subgroup of G, let $w(\phi)$ denote the root number of the character of the Weil group corresponding to ϕ. For a finite extension F of K and its quadratic extension F', let $w_{F'/F}$ be the root number of the non-trivial character of W_F that factors through $\mathrm{Gal}(F'/F)$. The following is a main theorem, which is proved at [DD08, Theorem 7] in the case where K is of characteristic 0.

Theorem 4.6. *We have*

$$w(E/K) = (-i)^{f(n(E)-2)} \frac{w(\chi)}{w_{K(\alpha,\beta)/K(\alpha)}},$$

where f and $n(E)$ are defined after Remark 4.1.

Proof. We take an ordered basis (P,Q) of $E[3]$ such that the coordinate of P is (α,β). We identify G with $GL_2(\mathbb{F}_3)$ by this ordered basis. By Lemma 4.2, it suffices to show

$$w(\sigma_{E,\eta}) = \frac{w(\chi)}{w_{K(\alpha,\beta)/K(\alpha)}}. \tag{4.1}$$

Let $B_{12} \subset GL_2(\mathbb{F}_3)$ be the $\mathbb{F}_3$-rational points of the upper triangle Borel subgroup of GL_2. Let $\det_{B_{12}}$ be the determinant character, and $\sigma_{B_{12}}$ be the non-trivial character that factors through

$$B_{12} \to \mathbb{F}_3^\times;\ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto a.$$

We take a non-trivial character τ of $SL(\mathbb{F}_3)$. (We note that the abelianization of $SL(\mathbb{F}_3)$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.) Let k_2 be the residue field of $K(\zeta_3)$. By the local class field theory, τ corresponds to a non trivial character χ_τ of $k_2^\times/(k_2^\times)^3$. Then the formula

$$w(\sigma_{E,\eta}) = \frac{w(\chi)w(\det_{B_{12}})w(\tau)}{w(\sigma_{B_{12}})} \tag{4.2}$$

is proved in the proof of [DD08, Theorem 7] without using the assumption that the characteristic of K is 0. Since B_{12} is the subgroup of G preserving the subgroup of $E[3]$ generated by P, we have $w(\sigma_{B_{12}}) = w_{K(\alpha,\beta)/K(\alpha)}$. We have

$$w(\det_{B_{12}}) = w_{K(\alpha,\zeta)/K(\alpha)} = (-1)^{[K(\alpha):K]-v(\mathfrak{D}(K(\alpha)/K))} = 1,$$

where we have the second equality by [BH06, 23.5. Lemma 1 and Proposition], and the third equality holds since $v(\mathfrak{D}(K(\alpha)/K))$ is even by Lemma 4.3. We put $q = p^f$. We have

$$\begin{aligned} w(\tau) &= q^{-1}\sum_{x\in k_2^\times}\chi_\tau(x)^{-1}\phi(\mathrm{Tr}_{k_2/\mathbb{F}_2}(x)) \\ &= q^{-1}\left\{\sum_{x\in(k_2^\times)^3}\phi(\mathrm{Tr}_{k_2/\mathbb{F}_2}(x)) - \sum_{x\in\zeta_3(k_2^\times)^3}\phi(\mathrm{Tr}_{k_2/\mathbb{F}_2}(x))\right\} \end{aligned} \tag{4.3}$$

using [BH06, 23.5. Theorem] and that

$$\left\{x\in\zeta_3(k_2^\times)^3 \;\middle|\; \mathrm{Tr}_{k_2/\mathbb{F}_2}(x)=0\right\} \to \left\{x\in\zeta_3^2(k_2^\times)^3 \;\middle|\; \mathrm{Tr}_{k_2/\mathbb{F}_2}(x)=0\right\};\ x\mapsto x^2$$

is a bijection. We put

$$\begin{aligned} N_1 &= \sharp\left\{y\in k_2 \;\middle|\; y+y^2\in(k_2^\times)^3\right\}, \\ N_2 &= \sharp\left\{y\in k_2 \;\middle|\; y+y^2\in\zeta_3(k_2^\times)^3\right\}. \end{aligned}$$

We note that $N_2 = (q^2-2-N_1)/2$. Then (4.3) is equal to

$$\begin{aligned} &q^{-1}\left\{\left(\frac{N_1}{2}-\left(\frac{q^2-1}{3}-\frac{N_1}{2}\right)\right)-\left(\frac{N_2}{2}-\left(\frac{q^2-1}{3}-\frac{N_2}{2}\right)\right)\right\} \\ &\quad = \frac{3N_1-q^2+2}{2q} = 1, \end{aligned}$$

because $N_1 = (q^2 + 2q - 2)/3$ by Lemma 4.5. Therefore (4.1) follows from (4.2). □

REMARK 4.7. The elliptic curve $\mathcal{E}$ appears in a semi-stable reduction of a Lubin-Tate curve over a dyadic field (cf. [IT11]). Hence, it is studied in [IT12]. Actually, a similar calculation as the calculation of $w(\tau)$ in the proof of Theorem 4.6 appears in [IT12].

References

[BH06] Bushnell, C. J. and G. Henniart, The local Langlands conjecture for GL(2), volume 335 of *Grundlehren der Mathematischen Wissenschaften*, Springer-Verlag, Berlin, 2006.

[DD08] Dokchitser, T. and V. Dokchitser, Root numbers of elliptic curves in residue characteristic 2, Bull. Lond. Math. Soc. **40**(3) (2008), 516–524.

[Del73] Deligne, P., Les constantes des équations fonctionnelles des fonctions L, In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 501–597, Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973.

[Hal98] Halberstadt, E., Signes locaux des courbes elliptiques en 2 et 3, C. R. Acad. Sci. Paris Sér. I Math. **326**(9) (1998), 1047–1052.

[IT11] Imai, N. and T. Tsushima, Stable models of Lubin-Tate curves with level three, 2011, arXiv:1111.1893.

[IT12] Imai, N. and T. Tsushima, Geometric realization of the local Langlands correspondence for representations of conductor three, 2012, arXiv:1205.0734.

[Kob02] Kobayashi, S., The local root number of elliptic curves with wild rami cation, Math. Ann. **323**(3) (2002), 609–623.

[Kod64] Kodaira, K., On the structure of compact complex analytic surfaces. I, Amer. J. Math. **86** (1964), 751–798.

[Kra90] Kraus, A., Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive, Manuscripta Math. **69**(4) (1990), 353–385.

[Roh96] Rohrlich, D. E., Galois theory, elliptic curves, and root numbers, Compositio Math. **100**(3) (1996), 311–349.

[Ser72] Serre, J.-P., Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15**(4) (1972), 259–331.

[Sil09] Silverman, J. H., The arithmetic of elliptic curves, volume 106 of *Graduate Texts in Mathematics*, Springer, Dordrecht, second edition, 2009.

[ST68] Serre, J.-P. and J. Tate, Good reduction of abelian varieties, Ann. of Math. 2 **88** (1968), 492–517.

[Tat75] Tate, J., Algorithm for determining the type of a singular ber in an

elliptic pencil, In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52, Lecture Notes in Math., Vol. 476, Springer, Berlin, 1975.

(Received June 27, 2014)
(Revised September 8; September 11, 2014)

Graduate School of Mathematical Sciences
The University of Tokyo
3-8-1 Komaba, Meguro-ku
Tokyo 153-8914, Japan
E-mail: naoki@ms.u-tokyo.ac.jp