THE REMAINING CASES OF THE KRAMER–TUNNELL CONJECTURE

KĘSTUTIS ČESNAVIČIUS AND NAOKI IMAI

Abstract. For an elliptic curve E over a local field K and a separable quadratic extension of K, motivated by connections to the Birch and Swinnerton-Dyer conjecture, Kramer and Tunnell have conjectured a formula for computing the local root number of the base change of E to the quadratic extension in terms of a certain norm index. The formula is known in all cases except some when K is of characteristic 2, and we complete its proof by reducing the positive characteristic case to characteristic 0. For this reduction, we exploit the principle that local fields of characteristic p can be approximated by finite extensions of $\mathbb{Q}_p$—we find an elliptic curve E' defined over a p-adic field such that all the terms in the Kramer–Tunnell formula for E' are equal to those for E.

1. Introduction

1.1. The Kramer–Tunnell conjecture. Let E be an elliptic curve over a local field K, and let K_χ/K be the separable quadratic extension cut out by a continuous character $\chi\colon W_K \twoheadrightarrow \{\pm 1\} \subset \mathbb{C}^\times$ of the Weil group W_K of K. In [KT82], Kramer and Tunnell conjectured the formula[1]

$$w(E_{K_\chi}) \overset{?}{=} \chi(\Delta) \cdot (-1)^{\dim_{\mathbb{F}_2}(E(K)/\mathrm{Norm}_{K_\chi/K} E(K_\chi))} \qquad (\bigstar)$$

for computing the local root number $w(E_{K_\chi})$ of the base change of E to K_χ; here $\Delta \in K^\times$ is the discriminant of any Weierstrass equation for E and $\chi(\Delta)$ is interpreted via the reciprocity isomorphism $K^\times \xrightarrow{\sim} W_K^{\mathrm{ab}}$. Even though the conjecture is purely local, its origins are global: it was inspired by the 2-parity conjecture, which itself is a special case of the rank part of the Birch and Swinnerton-Dyer conjecture combined with the predicted finiteness of Shafarevich–Tate groups. In fact, ($\bigstar$) is the backbone of one of the most general unconditional results on the 2-parity conjecture: for an elliptic curve over a number field, the 2-parity conjecture holds after base change to any quadratic extension—see [DD11, Cor. 4.8] for this result.

1.2. Known cases. The Kramer–Tunnell conjecture is known in the vast majority of cases. Kramer and Tunnell settled it in [KT82] except for (most of) the cases when all of the following hold: K is nonarchimedean of residue characteristic 2, the reduction of E is additive potentially good, and χ is ramified. In [DD11, Thm. 1.5], T. and V. Dokchitser completed the proof for K of characteristic 0. Thus, in the remaining cases, $\mathrm{char}\, K = 2$ and E has additive potentially good reduction. Our main goal is to address these remaining cases, and hence to complete the proof of

Theorem 1.3 (Theorem 4.9)**.** *The Kramer–Tunnell conjecture ($\bigstar$) holds.*

Date: April 23, 2016.

2010 *Mathematics Subject Classification.* Primary 11G07.

Key words and phrases. Elliptic curve, local field, root number, Weierstrass equation.

[1] Kramer and Tunnell phrase ($\bigstar$) differently, but the two formulations are equivalent due to the well-known formula $w(E_{K_\chi}) = w(E)w(E_\chi)\chi(-1)$, where E_χ is the quadratic twist of E by χ (in the archimedean case, all the terms in this formula are -1; in the nonarchimedean case, this formula may be proved the same way as [Čes16, Prop. 3.11]). We prefer the formulation ($\bigstar$) because it emphasizes that the right hand side is a formula for $w(E_{K_\chi})$.

1.4. The method of proof: deforming to characteristic 0. The basic idea of the proof is to exploit the principle explained in [Del84] that a local field K of positive characteristic p is, in some sense, a limit of more and more ramified finite extensions of $\mathbb{Q}_p$. More precisely, for every $e \in \mathbb{Z}_{\geq 1}$, the quotient $\mathcal{O}_K/\mathfrak{m}_K^e$ is isomorphic to $\mathcal{O}_{K'}/\mathfrak{m}_{K'}^e$ for some finite extension K' of $\mathbb{Q}_p$—for instance,

$$\mathbb{F}_{p^n}[[t]]/(t^e) \simeq (W(\mathbb{F}_{p^n})[T]/(T^e - p))/(T^e),$$

where $W(\mathbb{F}_{p^n})$ is the ring of Witt vectors—while, on the other hand, $\mathcal{O}_K/\mathfrak{m}_K^e$ already controls a significant part of the arithmetic of K, for instance, it controls the category of finite separable extensions of K whose Galois closures have trivial $(e-1)^{\mathrm{st}}$ ramification groups in the upper numbering (for further details regarding such control, see §2). In fact, in §3 we show that $\mathcal{O}_K/\mathfrak{m}_K^e$ controls so much that if we choose an integral Weierstrass equation for E, choose a large enough e (that depends on the equation), reduce the equation modulo $\mathfrak{m}_K^e$, and then lift back to an integral Weierstrass equation E' over K', then many invariants of E', such as the reduction type or the ℓ-adic Tate module, match with the corresponding invariants of E. With this at hand, in §4 we deduce ($\bigstar$) from its known characteristic 0 case: we show how to choose a K', an E', and a character $\chi' \colon W_{K'} \twoheadrightarrow \{\pm 1\}$ in such a way that the terms appearing in ($\bigstar$) for E and χ match with the ones for E' and χ'.

1.5. Reliance on global arguments. The Kramer–Tunnell formula is purely local, but global input is crucial for its current proof. This input comes in through the proof of the case when K is a finite extension of $\mathbb{Q}_2$: in [DD11, Thm. 4.7], T. and V. Dokchitser reduce this case of ($\bigstar$) to the 2-parity conjecture for certain elliptic curves over totally real number fields, and then prove the latter by combining potential modularity of elliptic curves over totally real fields, the Friedberg–Hoffstein theorem on central zeros of L-functions of quadratic twists of self-contragredient cuspidal automorphic representations of GL(2), and the extensions due to Shouwu Zhang of the results of Gross and Zagier and of Kolyvagin. Is there a purely local proof of the Kramer–Tunnell formula?

One purely local line of attack in the most difficult case of residue characteristic 2 and additive potentially good reduction is to make use of the formulas for the local root number, which are derived in this situation in [DD08] and in [Ima15]. However, it seems difficult to isolate the norm index term of ($\bigstar$) from these formulas.

1.6. Notation and conventions. If K is a nonarchimedean local field, then

- $\mathcal{O}_K$ denotes the ring of integers of K,
- $\mathfrak{m}_K$ denotes the maximal ideal of $\mathcal{O}_K$,
- $v_K \colon K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ denotes the discrete valuation of K,
- $v_K(\mathfrak{I}) := \min\{v_K(a) \mid a \in \mathfrak{I}\}$ for an ideal $\mathfrak{I} \subset \mathcal{O}_K$,
- W_K denotes the Weil group formed with respect to an implicit choice of a separable closure K^s,
- I_K denotes the inertia subgroup of W_K,
- I_K^u for $u \in \mathbb{R}_{\geq 0}$ denotes the u^{th} ramification subgroup of I_K in the upper numbering,
- $U_K^0 := \mathcal{O}_K^\times$ and $U_K^n := 1 + \mathfrak{m}_K^n$ for $n \in \mathbb{Z}_{\geq 1}$.

We follow the normalization of the reciprocity homomorphism of local class field theory used in [Del84], i.e., we require that uniformizers are mapped to *geometric* Frobenii. Whenever needed, e.g., to obtain Weil group inclusions, we implicitly assume that the choices of separable closures are made compatibly. For an elliptic curve E, we denote by $V_\ell(E)$ its Tate module with $\mathbb{Q}_\ell$ coefficients. Whenever dealing with quotients, we denote the residue class of an element a by $\overline{a}$.

Acknowledgements. We thank the referee for helpful comments and suggestions. While working on this paper, K.Č. was supported by the Miller Institute for Basic Research in Science at the University of California Berkeley, and N.I. was supported by a JSPS Postdoctoral Fellowship for Research Abroad.

2. Deligne's equivalence between extensions of different local fields

In §2, we fix a nonarchimedean local field K and we recall from [Del84] those aspects of approximation of K by another nonarchimedean local field K' that will be needed in the arguments of §§3–4.

2.1. The category $\mathsf{E}_e(K)$. Fix an $e \in \mathbb{Z}_{\geq 1}$ and consider those finite separable extensions of K whose Galois closure has a trivial e^{th} ramification group in the upper numbering. Form the category $\mathsf{E}_e(K)$ that has such extensions of K as objects and K-algebra homomorphisms as morphisms.

2.2. The triple associated to K and e. The triple in question is

$$(\mathcal{O}_K/\mathfrak{m}_K^e, \mathfrak{m}_K/\mathfrak{m}_K^{e+1}, \epsilon_K)$$

and consists of the Artinian local ring $\mathcal{O}_K/\mathfrak{m}_K^e$, its free rank 1 module $\mathfrak{m}_K/\mathfrak{m}_K^{e+1}$, and the $(\mathcal{O}_K/\mathfrak{m}_K^e)$-module homomorphism

$$\epsilon_K \colon \mathfrak{m}_K/\mathfrak{m}_K^{e+1} \to \mathcal{O}_K/\mathfrak{m}_K^e$$

induced by the inclusion $\mathfrak{m}_K \subset \mathcal{O}_K$. According to one of the main results of [Del84], this triple determines the category $\mathsf{E}_e(K)$; we will use this result in the form of Theorem 2.4 below.

2.3. Isomorphisms of triples. If K' is another nonarchimedean local field, then an isomorphism

$$(\mathcal{O}_K/\mathfrak{m}_K^e, \mathfrak{m}_K/\mathfrak{m}_K^{e+1}, \epsilon_K) \xrightarrow{\sim} (\mathcal{O}_{K'}/\mathfrak{m}_{K'}^e, \mathfrak{m}_{K'}/\mathfrak{m}_{K'}^{e+1}, \epsilon_{K'}) \tag{‡}$$

is a datum of a ring isomorphism

$$\phi\colon \mathcal{O}_K/\mathfrak{m}_K^e \xrightarrow{\sim} \mathcal{O}_{K'}/\mathfrak{m}_{K'}^e$$

and a ϕ-semilinear isomorphism

$$\eta\colon \mathfrak{m}_K/\mathfrak{m}_K^{e+1} \xrightarrow{\sim} \mathfrak{m}_{K'}/\mathfrak{m}_{K'}^{e+1}$$

for which the diagram

$$\begin{tikzcd} \mathfrak{m}_K/\mathfrak{m}_K^{e+1} \arrow[r, "\epsilon_K"] \arrow[d, "\eta", "\wr"'] & \mathcal{O}_K/\mathfrak{m}_K^e \arrow[d, "\phi", "\wr"'] \\ \mathfrak{m}_{K'}/\mathfrak{m}_{K'}^{e+1} \arrow[r, "\epsilon_{K'}"] & \mathcal{O}_{K'}/\mathfrak{m}_{K'}^e \end{tikzcd}$$

commutes. Any ϕ extends to an isomorphism (‡), albeit noncanonically: if $\pi_K \in \mathcal{O}_K$ is a uniformizer, then giving an η that is compatible with ϕ amounts to giving a lift of $\phi(\overline{\pi_K})$ to $\mathfrak{m}_{K'}/\mathfrak{m}_{K'}^{e+1}$. In contrast, any ring isomorphism

$$\mathcal{O}_K/\mathfrak{m}_K^{e+1} \xrightarrow{\sim} \mathcal{O}_{K'}/\mathfrak{m}_{K'}^{e+1}$$

induces a canonical isomorphism (‡).

Theorem 2.4 (Deligne)**.** *An isomorphism of triples (‡) gives rise to an equivalence of categories*

$$\Xi\colon \mathsf{E}_e(K) \xrightarrow{\sim} \mathsf{E}_e(K')$$

and an isomorphism

$$W_K/I_K^e \simeq W_{K'}/I_{K'}^e.$$

The latter is canonical up to an inner automorphism, preserves the images of the inertia subgroups, and maps Frobenius elements to Frobenius elements.

Proof. For the existence of Ξ, see [Del84, 3.4]. The construction there involves taking an inverse of an explicit functor that gives an intermediate equivalence of categories, so Ξ is not canonical. However, there is a natural isomorphism between any two inverses of a functor that is an equivalence, and hence also a natural isomorphism between any two Ξ that result from loc. cit. Thus, the choice of Ξ does not affect the uniqueness up to an inner automorphism of the isomorphism

$$\mathrm{Gal}(K^{\mathrm{s}}/K)/I_K^e \simeq \mathrm{Gal}(K'^{\mathrm{s}}/K')/I_{K'}^e \tag{2.4.1}$$

exhibited in [Del84, 3.5]. By [Del84, 2.1.1 (ii)], Ξ preserves unramified extensions; by construction, it also preserves their degrees. Thus, by its construction in [Del84, 3.5], (2.4.1) preserves the images of the inertia subgroups, maps Frobenii to Frobenii, and hence induces a sought isomorphism

$$W_K/I_K^e \simeq W_{K'}/I_{K'}^e. \qquad \square$$

2.5. An explicit description of Ξ. Fix an $F \in \mathsf{E}_e(K)$ and set $F' := \Xi(F)$. To describe F' explicitly, start with the maximal unramified subextension M/K of F/K, and set $M' := \Xi(M)$. By [Del84, 2.1.1 (ii)], M'/K' is the maximal unramified subextension of F'/K' and $[M' : K'] = [M : K]$. Since $\mathcal{O}_M$ and $\mathcal{O}_{M'}$ are finite étale over $\mathcal{O}_K$ and $\mathcal{O}_{K'}$ respectively, η and ϕ induce the isomorphism

$$\mathfrak{m}_M/\mathfrak{m}_M^{e+1} \cong (\mathfrak{m}_K/\mathfrak{m}_K^{e+1}) \otimes_{\mathcal{O}_K/\mathfrak{m}_K^e} \mathcal{O}_M/\mathfrak{m}_M^e \xrightarrow{\sim} (\mathfrak{m}_{K'}/\mathfrak{m}_{K'}^{e+1}) \otimes_{\mathcal{O}_{K'}/\mathfrak{m}_{K'}^e} \mathcal{O}_{M'}/\mathfrak{m}_{M'}^e \cong \mathfrak{m}_{M'}/\mathfrak{m}_{M'}^{e+1}$$

which we denote by η_M. Let

$$f(x) = \textstyle\sum_{i=0}^{[F:M]} m_i x^i \in M[x]$$

be a monic integral Eisenstein polynomial defining F/M. For $i < [F : M]$, we lift

$$\eta_M(\overline{m_i}) \quad \text{to} \quad m_i' \in \mathfrak{m}_{M'} \qquad \text{in such a way that} \quad m_1' \neq 0 \quad \text{if} \quad \mathrm{char}\, K' \neq 0,$$

so that the polynomial

$$g(x) := \textstyle\sum_{i=0}^{[F:M]} m_i' x^i \in M'[x] \qquad \text{with} \quad m'_{[F:M]} := 1$$

is separable. Then $g(x)$ is monic, separable, and Eisenstein, and the proof of [Del84, 1.4.4] supplies the sought description of F':

The polynomial $g(x)$ has a root in F', so $F' \simeq M'[x]/(g(x))$ as K'-algebras.

2.6. Induced isomorphisms of triples over extensions. For an $F \in \mathsf{E}_e(K)$, set $F' := \Xi(F)$. By [Del84, 3.4.1 and 3.4.2], (ϕ, η) induces a compatible canonical isomorphism

$$(\phi_F, \eta_F)\colon (\mathcal{O}_F/\mathfrak{m}_F^e, \mathfrak{m}_F/\mathfrak{m}_F^{e+1}, \epsilon_F) \xrightarrow{\sim} (\mathcal{O}_{F'}/\mathfrak{m}_{F'}^e, \mathfrak{m}_{F'}/\mathfrak{m}_{F'}^{e+1}, \epsilon_{F'}) \tag{2.6.1}$$

between the triples associated to F and F'.

Proposition 2.7. *Fix an $F \in \mathsf{E}_e(K)$, set $F' := \Xi(F)$, and let $\mathfrak{d}_{F/K} \subset \mathcal{O}_K$ and $\mathfrak{d}_{F'/K'} \subset \mathcal{O}_{K'}$ denote the discriminant ideals of the separable extensions F/K and F'/K'. Then*

$$v_K(\mathfrak{d}_{F/K}) = v_{K'}(\mathfrak{d}_{F'/K'}).$$

Proof. Let $\widetilde{F}$ be a Galois closure of F over K, and set $\widetilde{F}' := \Xi(\widetilde{F})$, so that, by Theorem 2.4, $\widetilde{F}'$ is a Galois closure of F' over K' and

$$\mathrm{Gal}(\widetilde{F}/K) \simeq \mathrm{Gal}(\widetilde{F}'/K').$$

By [Del84, 2.1.1 (iii)], the latter isomorphism preserves the ramification filtrations in the upper numbering. By [Del84, 1.5.3], it also preserves the Herbrand functions:

$$\varphi_{\widetilde{F}/K} = \varphi_{\widetilde{F}'/K'} \qquad \text{and} \qquad \psi_{\widetilde{F}/K} = \psi_{\widetilde{F}'/K'}.$$

Thus, it also preserves the ramification filtrations in the lower numbering. Therefore, the claim follows from [Ser79, III.§3 Prop. 6 and IV.§1 Cor. to Prop. 4]. □

2.8. Correspondence of representations. The inner automorphism ambiguity in Theorem 2.4 is irrelevant for the study of isomorphism classes of representations. More precisely, by Theorem 2.4, an isomorphism of triples (‡) gives a *canonical* bijection between the set of isomorphism classes of finite dimensional smooth complex representations of W_K/I_K^e and those of $W_{K'}/I_{K'}^e$. Thus, given such representations V and V' of W_K/I_K^e and $W_{K'}/I_{K'}^e$, we say that V and V' *correspond* if the canonical bijection maps the isomorphism class of V to that of V'.

Definition 2.9 ([Del84, 3.7]). *In the setup of §2.3, we say that nontrivial locally constant additive characters*

$$\psi\colon (K,+) \to \mathbb{C}^\times \qquad \textit{and} \qquad \psi'\colon (K',+) \to \mathbb{C}^\times$$

correspond *if*

(1) For every $n \in \mathbb{Z}$, we have $\psi|_{\mathfrak{m}_K^{-n}} = 1$ if and only if $\psi'|_{\mathfrak{m}_{K'}^{-n}} = 1$;

(2) Letting N denote the largest n for which the equivalent conditions of (1) hold, we have that the restrictions $\psi|_{\mathfrak{m}_K^{-N-e}}$ and $\psi'|_{\mathfrak{m}_{K'}^{-N-e}}$ induce characters that agree under the isomorphism

$$\mathfrak{m}_K^{-N-e}/\mathfrak{m}_K^{-N} \cong \left(\mathfrak{m}_K/\mathfrak{m}_K^{e+1}\right)^{\otimes(-N-e)} \xrightarrow[\eta^{\otimes(-N-e)}]{\sim} \left(\mathfrak{m}_{K'}/\mathfrak{m}_{K'}^{e+1}\right)^{\otimes(-N-e)} \cong \mathfrak{m}_{K'}^{-N-e}/\mathfrak{m}_{K'}^{-N}.$$

Remark 2.10. Any nontrivial locally constant additive character ψ has a (nonunique) corresponding ψ'. Indeed, every character $\overline{\theta}\colon \mathfrak{m}_{K'}^{-N-e}/\mathfrak{m}_{K'}^{-N} \to \mathbb{C}^\times$ is induced by a $\theta\colon (K',+) \to \mathbb{C}^\times$ that is trivial on $\mathfrak{m}_{K'}^{-N}$. To see this, fix some θ that is trivial on $\mathfrak{m}_{K'}^{-N}$ but not on $\mathfrak{m}_{K'}^{-N-1}$ and note that as $a \in \mathcal{O}_{K'}$ ranges over coset representatives of $\mathcal{O}_{K'}/\mathfrak{m}_{K'}^e$ the restrictions of the characters $a\theta\colon x \mapsto \theta(ax)$ to $\mathfrak{m}_{K'}^{-N-e}/\mathfrak{m}_{K'}^{-N}$ are distinct and hence sweep out the set of possible $\overline{\theta}$.

Proposition 2.11. *Let V and V' be finite dimensional smooth complex representations of W_K and $W_{K'}$ that are trivial on I_K^e and $I_{K'}^e$, respectively, and that correspond in the sense of §2.8. Let*

$$\psi\colon (K,+) \to \mathbb{C}^\times \qquad \textit{and} \qquad \psi'\colon (K',+) \to \mathbb{C}^\times$$

be nontrivial additive characters that correspond in the sense of Definition 2.9. Then the resulting local root numbers are equal:

$$w(V,\psi) = w(V',\psi').$$

Proof. By definition,

$$w(V,\psi) = \tfrac{\epsilon(V,\psi,dx)}{|\epsilon(V,\psi,dx)|},$$

where dx is any nonzero Haar measure on K, and likewise for $w(V',\psi')$. Thus, it suffices to apply [Del84, 3.7.1] after choosing the Haar measures in a way that the volumes of $\mathcal{O}_K$ and $\mathcal{O}_{K'}$ are 1. □

3. Approximation by an elliptic curve over a different local field

The goal of §3 is to prove in Proposition 3.2 that various invariants of an elliptic curve E over a nonarchimedean local field K are locally constant functions of the coefficients of a Weierstrass equation for E. The key difference from such continuity statements available in the literature, e.g., from [DD11, Prop. 3.3] or [Hel09, Prop. 4.2], is that, in addition to E, we also vary K. Even though the proofs are still based on Tate's algorithm, new input is needed for local constancy of ℓ-adic Tate modules because the results of [Kis99] no longer apply. This new input comes from [DD16], which proves that in the potential good reduction case the ℓ-adic Tate module is determined as a representation of the Weil group by its local L-factors taken over sufficiently many finite separable extensions of K.

Lemma 3.1. *Let K be a nonarchimedean local field and let σ be a finite dimensional, smooth, semisimple, complex representation of W_K. For a finite separable extension L/K, up to isomorphism there are only finitely many finite dimensional, smooth, semisimple, complex representations σ' of W_K such that $\sigma'|_{W_L} \simeq \sigma|_{W_L}$.*

Proof. We will use the Frobenius reciprocity bijection

$$\mathrm{Hom}_{W_K}(\sigma', \mathrm{Ind}_{W_L}^{W_K}(\sigma|_{W_L})) \cong \mathrm{Hom}_{W_L}(\sigma'|_{W_L}, \sigma|_{W_L}), \tag{3.1.1}$$

as well as the functoriality of this bijection in the W_K-representation σ' (cf. [BH06, §2.4]). Namely, under (3.1.1), a W_L-isomorphism

$$\lambda\colon \sigma'|_{W_L} \xrightarrow{\sim} \sigma|_{W_L}$$

corresponds to a W_K-morphism

$$\kappa\colon \sigma' \to \mathrm{Ind}_{W_L}^{W_K}(\sigma|_{W_L})$$

that must be injective because the composition of κ with the injection $\mathrm{Ker}\,\kappa \hookrightarrow \sigma'$ of W_K-representations both vanishes and, by the functoriality of (3.1.1) in σ', corresponds to the injection $\lambda|_{\mathrm{Ker}\,\kappa}$. The injectivity of κ and the semisimplicity of $\mathrm{Ind}_{W_L}^{W_K}(\sigma|_{W_L})$ (cf. [BH06, §28.7]) ensure that σ' is a direct summand of $\mathrm{Ind}_{W_L}^{W_K}(\sigma|_{W_L})$, and the claim follows by considering decompositions into direct sums of irreducibles. ☐

Proposition 3.2. *For a nonarchimedean local field K and a Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad \text{with} \quad a_i \in \mathcal{O}_K \quad \text{and discriminant} \quad \Delta \neq 0,$$

there is an integer $e_{K,E} \in \mathbb{Z}_{\geq 1}$ such that whenever one has

- *A nonarchimedean local field K',*
- *A ring isomorphism $\phi\colon \mathcal{O}_K/\mathfrak{m}_K^e \xrightarrow{\sim} \mathcal{O}_{K'}/\mathfrak{m}_{K'}^e$ for some $e \geq e_{K,E}$, and*
- *Elements $a_i' \in \mathcal{O}_{K'}$ lifting the corresponding $\phi(\overline{a_i}) \in \mathcal{O}_{K'}/\mathfrak{m}_{K'}^e$,*

then, letting $\mathbb{F}$ denote the common residue field of K and K', one gets the following conclusions:

(i) The resulting Weierstrass equation

$$E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6' \qquad \text{with discriminant } \Delta'$$

defines an elliptic curve $E' \to \operatorname{Spec} K'$ and

$$v_K(\Delta) = v_{K'}(\Delta');$$

(ii) The minimal discriminants $\Delta_{\min}$ and $\Delta'_{\min}$ of E and E' satisfy

$$v_K(\Delta_{\min}) = v_{K'}(\Delta'_{\min});$$

(iii) The Néron models $\mathcal{E} \to \operatorname{Spec} \mathcal{O}_K$ and $\mathcal{E}' \to \operatorname{Spec} \mathcal{O}_{K'}$ of E and E' satisfy

$$\mathcal{E}^0_{\mathbb{F}} \simeq \mathcal{E}'^0_{\mathbb{F}} \qquad \text{and} \qquad (\mathcal{E}_{\mathbb{F}}/\mathcal{E}^0_{\mathbb{F}})(\mathbb{F}) \simeq (\mathcal{E}'_{\mathbb{F}}/\mathcal{E}'^0_{\mathbb{F}})(\mathbb{F});$$

(iv) The conductor exponents of E and E' are equal;

(v) The Kodaira types of E and E' agree;

(vi) If E has potential good reduction, then so does E' and for every prime $\ell \neq \operatorname{char} \mathbb{F}$ the representation $\sigma_{E'} \colon W_{K'} \to \mathrm{GL}\big(V_\ell(E')^*\big)$ factors through $W_{K'}/I^e_{K'}$;

(vii) If E has potential multiplicative reduction, then so does E' and for every prime $\ell \neq \operatorname{char} \mathbb{F}$ the representation $\sigma_{E'} \colon W_{K'} \to \mathrm{GL}\big(V_\ell(E')^*\big)$ factors through $W_{K'}/I^e_{K'}$;

(viii) If E has potential good reduction, then for every extension of ϕ to an isomorphism of triples (‡) as in §2.3 and for every embedding $\iota \colon \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$, the complex representations

$$\sigma_E \otimes_{\mathbb{Q}_\ell, \iota} \mathbb{C} \quad \text{of} \quad W_K/I^e_K \qquad \text{and} \qquad \sigma_{E'} \otimes_{\mathbb{Q}_\ell, \iota} \mathbb{C} \quad \text{of} \quad W_{K'}/I^e_{K'}$$

correspond in the sense of §2.8.

(ix) The local root numbers are equal:

$$w(E) = w(E').$$

Proof. We prove (i)–(ix) one by one, each time enlarging the cumulative $e_{K,E}$ if needed.

(i) As is seen from, say, [Del75, 1.5], Δ (resp., Δ') is the value obtained by plugging in the a_i (resp., the a'_i) into some explicit polynomial with integral coefficients. Therefore, any choice of an $e_{K,E}$ greater than $v_K(\Delta)$ will ensure that $\Delta' \neq 0$ and that $v_K(\Delta) = v_{K'}(\Delta')$.

(ii) Choose a uniformizer $\pi_K \in \mathcal{O}_K$ and use it to execute Tate's algorithm presented in [Sil94, IV.§9, pp. 366–368] to the Weierstrass equation E (our π_K is denoted by π in loc. cit.). The execution consists of finitely many steps,[2] each one of which depends solely on the results of the preceding steps and is of one of the following types:

(1) Evaluate some predetermined explicit polynomial with integral coefficients at an argument whose coordinates are in $\mathcal{O}_K$ and of the form $\pi_K^{-j} a_i$ with $j \geq 0$ for some predetermined i and j, and then check whether the value is in $\mathfrak{m}_K$ or not;

(2) Form some explicit either cubic or quadratic polynomial with coefficients in $\mathcal{O}_K$ and of the form $\pi_K^{-j} a_i$ with $j \geq 0$ for some predetermined i and j, and then find the roots in $\overline{\mathbb{F}}$ (with multiplicities) of the reduction of this polynomial modulo $\mathfrak{m}_K$ (a multiple root is always forced to be in $\mathbb{F}$);

(3) Lift some predetermined element $r \in \mathbb{F}$ to an $R \in \mathcal{O}_K$, make one of the following substitutions:

$$x \mapsto x + \pi_K^s R, \quad \text{or} \quad y \mapsto y + \pi_K^s R, \quad \text{or} \quad y \mapsto y + \pi_K^s R x$$

for some predetermined $s \in \mathbb{Z}_{\geq 0}$, and then compute the new a_i (in most cases, r is related to a multiple root mentioned in (2)).

The total number of steps in the chosen execution is finite, so the structure of the algorithm and the descriptions (1)–(3) imply that there is some large $e_{K,E} \in \mathbb{Z}_{\geq 1}$ that forces the

[2] Our "steps" are substeps of the steps presented in loc. cit.

execution of the algorithm for any E' to be entirely analogous granted that we choose the lifts $R' \in \mathcal{O}_{K'}$ needed in (3) and a uniformizer $\pi_{K'}$ used throughout subject to

$$\phi(\overline{R}) = \overline{R'} \qquad \text{and} \qquad \phi(\overline{\pi_K}) = \overline{\pi_{K'}}.$$

Such choices are possible, so the resulting execution for E' will have the same sequence of steps with the same results as the fixed execution for E.

The difference

$$v_{K'}(\Delta') - v_{K'}(\Delta'_{\min})$$

depends solely on the sequence and the results of the steps. Therefore, once the $e_{K,E}$ of (i) is enlarged to exceed the $e_{K,E}$ of the previous paragraph, the equality

$$v_K(\Delta_{\min}) = v_{K'}(\Delta'_{\min})$$

follows from the equality $v_K(\Delta) = v_{K'}(\Delta')$ supplied by (i).

(iii) By loc. cit., the $\mathbb{F}$-group scheme $\mathcal{E}'^0_{\mathbb{F}}$ and the abelian group $(\mathcal{E}'_{\mathbb{F}}/\mathcal{E}'^0_{\mathbb{F}})(\mathbb{F})$ also depend solely on the sequence and the results of the steps in an execution of Tate's algorithm for E'. Therefore, the proof of (ii) also gives (iii).

(iv) The proof is the same as the proof of (iii).

(v) The proof is the same as the proof of (iii).

(vi) Fix a finite Galois extension L of K over which E has good reduction—for definiteness, set $L := K(E[\ell_0])$, where ℓ_0 is the smallest odd prime with $\ell_0 \neq \operatorname{char}\mathbb{F}$. Since (i)–(iii) are already settled, there is an $e_{L,E} \in \mathbb{Z}_{\geq 1}$ for which the Weierstrass equation E viewed over L satisfies the conclusions of (i)–(iii). Fix a $u \in \mathbb{R}_{>0}$ such that the u^{th} ramification group of L/K in the upper numbering is trivial, and choose an $e_{K,E} \in \mathbb{Z}_{\geq 1}$ subject to

$$e_{K,E} \geq \max(e_{L,E}, u).$$

With $e_{K,E}$ at hand, consider an isomorphism ϕ as in the claim. Use §2.3 to choose an extension of ϕ to an isomorphism of triples (‡), and then let

$$\Xi\colon \mathsf{E}_e(K) \xrightarrow{\sim} \mathsf{E}_e(K')$$

denote an equivalence of categories that results from Theorem 2.4. Since $e \geq e_{K,E} \geq u$, the extension L is an object of $\mathsf{E}_e(K)$. Set $L' := \Xi(L)$ and let

$$\phi_L\colon \mathcal{O}_L/\mathfrak{m}_L^e \xrightarrow{\sim} \mathcal{O}_{L'}/\mathfrak{m}_{L'}^e$$

be the extension of ϕ supplied by (2.6.1). Then, since $e \geq e_{K,E} \geq e_{L,E}$, we conclude from (iii) that the Weierstrass equation E' viewed over L' gives rise to an elliptic curve that has good reduction. Therefore, due to the criterion of Néron–Ogg–Shafarevich, $\sigma_{E'}$ factors through $W_{K'}/I^e_{K'}$.

(vii) The proof is completely analogous to the proof of (vi): with the same notation, E' will have multiplicative reduction over L', so the inertial action of $W_{L'}$ on $V_\ell(E')^*$ will be tame, and hence $I^e_{K'}$, being pro-p (with $p = \operatorname{char}\mathbb{F}$), will have to act trivially.

(viii) We adopt the notations of the proof of (vi) and, for brevity, we set

$$\sigma := \sigma_E \otimes_{\mathbb{Q}_\ell,\iota} \mathbb{C} \qquad \text{and} \qquad \sigma' := \sigma_{E'} \otimes_{\mathbb{Q}_\ell,\iota} \mathbb{C}.$$

If we use an isomorphism $W_K/I_K^e \simeq W_{K'}/I_{K'}^e$ induced by Ξ to view σ' as a representation of W_K, then, due to the choice of $e_{K,E}$ made in (vi), (iii) applied to E over L ensures that there is a W_L-isomorphism

$$\lambda\colon \sigma|_{W_L} \simeq \sigma'|_{W_L}.$$

Thus, by Lemma 3.1, there is a finite set of finite dimensional, smooth, semisimple complex W_K-representations that depends solely on the data determined by the coefficients a_i (for instance, on σ and on L) and such that σ' is isomorphic to one of the representations in this set. Due to [DD16, Thm. 2.1], this set then gives rise to a finite set $\{K_j\}_{j\in J}$ of finite separable extensions of K such that λ may be upgraded to a sought W_K-isomorphism $\sigma \simeq \sigma'$ if and only if there is an equality of L-factors

$$L(\sigma|_{W_{K_j}}, s) = L(\sigma'|_{W_{K_j}}, s) \qquad \text{for every} \quad K_j. \tag{3.2.1}$$

The local L-factor of an elliptic curve is determined by the connected component of the identity of the special fiber of the Néron model, so, due to §2.6, (3.2.1) will be forced to hold once we enlarge $e_{K,E}$ to exceed every $e_{K_j,E}$, where $e_{K_j,E}$ is a fixed integer for which the Weierstrass equation E viewed over K_j satisfies the conclusions of (i)–(iii).

(ix) If E has potential good reduction, then the claim follows from (viii) and Proposition 2.11 (combined with Remark 2.10) because, by definition,

$$w(E) = w(\sigma_E \otimes_{\mathbb{Q}_\ell,\iota} \mathbb{C},\, \psi)$$

for any embedding ι and any nontrivial additive character ψ and likewise for E'.

If E has split multiplicative (resp., nonsplit multiplicative) reduction, then, by (iii), so does E', and the claim follows from the local root number being -1 (resp., 1) in the split multiplicative (resp., nonsplit multiplicative) case.

In the remaining case when E has additive potential multiplicative reduction, let F be the separable ramified quadratic extension of K over which E has split multiplicative reduction. Fix a $v \in \mathbb{R}_{>0}$ such that the v^{th} ramification group of F/K in the upper numbering is trivial, fix an $e_{F,E} \in \mathbb{Z}_{\geq 1}$ for which the Weierstrass equation E viewed over F satisfies the conclusions of (i)–(iii), enlarge $e_{K,E}$ so that

$$e_{K,E} \geq \max(e_{F,E}, v),$$

and set $F' := \Xi(F)$, where Ξ is obtained as in the proof of (vi). Then, by (iii) and (2.6.1), E' has additive reduction over K' and split multiplicative reduction over F'. Let

$$\nu_{F/K}\colon W_K/I_K^e \twoheadrightarrow \{\pm 1\} \qquad \text{and} \qquad \nu_{F'/K'}\colon W_{K'}/I_{K'}^e \twoheadrightarrow \{\pm 1\}$$

be the quadratic characters with kernels W_F/I_K^e and $W_{F'}/I_{K'}^e$; then $\nu_{F/K}$ and $\nu_{F'/K'}$ correspond in the sense of §2.8. Let ω and ω' be the cyclotomic characters of W_K and $W_{K'}$; then ω and ω' are unramified and also correspond. By [Roh94, §15, Prop.], the complex Weil–Deligne representations associated to E and E' are isomorphic to

$$(\nu_{F/K} \cdot \omega^{-1}) \otimes \mathrm{sp}(2) \qquad \text{and} \qquad (\nu_{F'/K'} \cdot \omega'^{-1}) \otimes \mathrm{sp}(2),$$

respectively. In particular, since $\nu_{F/K}$ and $\nu_{F'/K'}$ are ramified,

$$w(E) = w(\nu_{F/K} \cdot \omega^{-1} \oplus \nu_{F/K}, \psi) \qquad \text{and} \qquad w(E') = w(\nu_{F'/K'} \cdot \omega'^{-1} \oplus \nu_{F'/K'}, \psi')$$

for any nontrivial additive characters

$$\psi\colon (K, +) \to \mathbb{C}^\times \qquad \text{and} \qquad \psi'\colon (K', +) \to \mathbb{C}^\times.$$

It remains to apply Proposition 2.11 (with Remark 2.10) to get $w(E) = w(E')$. $\square$

Remark 3.3. The choice $K' = K$ in Proposition 3.2 recovers some of the local constancy statements referred to in the beginning of §3.

4. Reduction of the Kramer–Tunnell conjecture to the characteristic 0 case

Throughout §4, we fix a nonarchimedean local field K of positive characteristic p, a nontrivial character $\chi\colon W_K \twoheadrightarrow \{\pm 1\} \subset \mathbb{C}^\times$ together with the corresponding separable quadratic extension K_χ of K, and an elliptic curve $E \to \operatorname{Spec} K$ together with a choice of its integral Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad \text{with} \quad a_i \in \mathcal{O}_K \quad \text{and discriminant} \quad \Delta. \qquad (\lozenge)$$

We let E_χ denote the quadratic twist of E by χ.

Our goal is to show that the Kramer–Tunnell conjecture ($\bigstar$) for E and χ follows if it holds for some other elliptic curve $E' \to \operatorname{Spec} K'$ and some other χ' with $[K' : \mathbb{Q}_p] < \infty$. Since the Kramer–Tunnell conjecture is known in characteristic 0, this allows us to deduce it in general in Theorem 4.9. The Kramer–Tunnell conjecture is also known in the case of odd residue characteristic, so we could have also assumed that $p = 2$; we avoid this assumption because the deformation to characteristic 0 argument is simpler in the case $p \neq 2$ and still contains all the essential ideas.

4.1. A Weierstrass equation for E_χ in the case $p \neq 2$. If $p \neq 2$, then $K_\chi = K(\sqrt{d})$ for some $d \in \mathcal{O}_K$ normalized by $v_K(d) \leq 1$. With this normalization, $(d) \subset \mathcal{O}_K$ is necessarily the discriminant ideal of K_χ/K. As noted in [KT82, (7.4.2) on p. 331], an integral Weierstrass equation for E_χ is

$$E_\chi \colon y^2 = x^3 + \tfrac{1}{4}d(a_1^2 + 4a_2)x^2 + \tfrac{1}{2}d^2(a_1a_3 + 2a_4)x + \tfrac{1}{4}d^3(a_3^2 + 4a_6),$$

and the discriminant Δ_χ of this equation equals $d^6\Delta$.

4.2. A Weierstrass equation for E_χ in the case $p = 2$. If $p = 2$, then $K_\chi = K(\theta)$, where θ is a root of the Artin–Schreier equation $x^2 - x + \gamma = 0$ for some $\gamma \in K$. We fix one such γ normalized by insisting that $v_K(\gamma) \leq 0$ and that either $v_K(\gamma)$ be odd or $v_K(\gamma) = 0$;[3] to see that these requirements may be met, use an isomorphism $K \simeq \mathbb{F}((t))$, where $\mathbb{F}$ is the residue field of K. Furthermore, we fix a uniformizer $\pi_K \in \mathcal{O}_K$ and let $r \in \mathbb{Z}_{\geq 0}$ be minimal such that $\pi_K^{2r}\gamma \in \mathcal{O}_K$. Then

$$X^2 - \pi_K^r X + \pi_K^{2r}\gamma = 0 \qquad \text{is the minimal polynomial of } \pi_K^r\theta.$$

Moreover, if $v_K(\gamma)$ is odd, then K_χ/K is ramified and $\pi_K^r\theta$ is a uniformizer of $\mathcal{O}_{K_\chi}$, and if $v_K(\gamma) = 0$, then K_χ/K is unramified. In both cases, $\mathcal{O}_{K_\chi} = \mathcal{O}_K[\pi_K^r\theta]$, so the discriminant ideal of K_χ/K is $(\pi_K^{2r}) \subset \mathcal{O}_K$. By [KT82, (7.4.4) on p. 331], an integral Weierstrass equation for E_χ is

$$E_\chi \colon y^2 + \pi_K^r a_1xy + \pi_K^{3r}a_3y = x^3 + \pi_K^{2r}(a_2 + \gamma a_1^2)x^2 + \pi_K^{4r}a_4x + \pi_K^{6r}(a_6 + \gamma a_3^2),$$

and the discriminant Δ_χ of this equation equals $\pi_K^{12r}\Delta$.

4.3. Construction of K'. Let $c(\chi)$ be the smallest nonnegative integer with $\chi(I_K^{c(\chi)}) = 1$. Fix positive integers $e_{K,E}$ and $e_{K_\chi,E}$ for which Proposition 3.2 holds for the Weierstrass equation $(\lozenge)$ viewed over K and over K_χ, respectively. Fix a positive integer e_{K,E_χ} for which Proposition 3.2 holds for the Weierstrass equation of E_χ chosen in §4.1 or in §4.2. Finally, fix an $e \in \mathbb{Z}_{\geq 1}$ subject to

$$e \geq \max\{e_{K,E}, e_{K_\chi,E}, e_{K,E_\chi}, v_K(\Delta) + c(\chi), v_K(\mathfrak{d}_{K_\chi/K})\},$$

[3] This normalization of γ will ensure that the discriminant of K_χ/K is (π_K^{2r}), which will be needed for our reliance on [KT82, p. 331 and Theorem 7.6]. For general γ, the claim in the last paragraph of [KT82, p. 331] that d generates the discriminant ideal of K/F becomes incorrect (for instance, the discriminant ideal of the extension of $\mathbb{F}_2((t))$ cut out by the polynomial $x^2 - x + \frac{1}{t^4} = (x + \frac{1}{t} + \frac{1}{t^2})^2 - (x + \frac{1}{t} + \frac{1}{t^2}) + \frac{1}{t}$ is (t^2) and not (t^4)); the normalization of γ that we have imposed avoids this issue.

where $\mathfrak{d}_{K_\chi/K} \subset \mathcal{O}_K$ is the discriminant ideal of K_χ/K. With this choice of e, one has $K_\chi \in \mathsf{E}_e(K)$ in the notation of §2.1. With e at hand, set

$$K' := (W(\mathbb{F})[T]/(T^e - p))\,[\tfrac{1}{p}], \qquad \text{so that} \qquad \mathcal{O}_{K'} = W(\mathbb{F})[T]/(T^e - p),$$

where $W(\mathbb{F})$ is the ring of Witt vectors of the residue field $\mathbb{F}$ of K. Fix an isomorphism $K \simeq \mathbb{F}((t))$ and define the $\mathbb{F}$-algebra isomorphism

$$\phi\colon \mathcal{O}_K/\mathfrak{m}_K^e \xrightarrow{\sim} \mathcal{O}_{K'}/\mathfrak{m}_{K'}^e \qquad \text{by the requirement} \quad \phi(\bar{t}) = \overline{T}$$

and the ϕ-semilinear isomorphism

$$\eta\colon \mathfrak{m}_K/\mathfrak{m}_K^{e+1} \xrightarrow{\sim} \mathfrak{m}_{K'}/\mathfrak{m}_{K'}^{e+1} \qquad \text{by the requirement} \quad \eta(\bar{t}) = \overline{T}.$$

The pair (ϕ, η) induces an isomorphism of triples as in (‡). Therefore, by Theorem 2.4, (ϕ, η) gives rise to an equivalence of categories $\Xi\colon \mathsf{E}_e(K) \xrightarrow{\sim} \mathsf{E}_e(K')$ and to an isomorphism $W_K/I_K^e \simeq W_{K'}/I_{K'}^e$.

4.4. Construction of E'. With K' as in §4.3, choose elements $a_i' \in \mathcal{O}_{K'}$ lifting $\phi(\overline{a_i}) \in \mathcal{O}_{K'}/\mathfrak{m}_{K'}^e$ and consider the Weierstrass equation

$$E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'. \qquad (\Diamond')$$

By Proposition 3.2 (i), the equation $(\Diamond')$ defines an elliptic curve $E' \to \operatorname{Spec} K'$.

4.5. Construction of χ'. Define the quadratic character χ' by

$$\chi'\colon W_{K'}/I_{K'}^e \twoheadrightarrow (W_{K'}/I_{K'}^e)^{\mathrm{ab}} \cong (W_K/I_K^e)^{\mathrm{ab}} \xrightarrow{\chi} \{\pm 1\} \subset \mathbb{C}^\times,$$

where the middle isomorphism is canonical because the isomorphism $W_K/I_K^e \simeq W_{K'}/I_{K'}^e$ mentioned in §4.3 is well-defined up to an inner automorphism. The characters χ and χ' correspond in the sense of §2.8 and, by construction, $\Xi(K_\chi)$ is the separable quadratic extension $K'_{\chi'}$ of K' fixed by the kernel of χ'. Moreover, by [Del84, 2.1.1 (iii)], $\chi'(I_{K'}^{c(\chi)}) = 1$.

Lemma 4.6. *The local root numbers of E_{K_χ} and of $E'_{K'_{\chi'}}$ are equal:*

$$w(E_{K_\chi}) = w(E'_{K'_{\chi'}}).$$

Proof. Combine §2.6 with Proposition 3.2 (ix). □

Lemma 4.7. *The discriminants Δ and Δ' of the Weierstrass equations $(\Diamond)$ and $(\Diamond')$ satisfy*

$$\chi(\Delta) = \chi'(\Delta').$$

Proof. As explained in [Del84, 1.2], the isomorphisms ϕ and η induce an isomorphism

$$\xi\colon K^\times/U_K^e \xrightarrow{\sim} K'^\times/U_{K'}^e$$

and, since $e \geq c(\chi)$, also a compatible isomorphism

$$\bar{\xi}\colon K^\times/U_K^{c(\chi)} \xrightarrow{\sim} K'^\times/U_{K'}^{c(\chi)}.$$

Moreover, the images of Δ and Δ' in

$$\mathfrak{m}_{K'}^{v_K(\Delta)}/\mathfrak{m}_{K'}^{v_K(\Delta)+c(\chi)} \subset \mathcal{O}_{K'}/\mathfrak{m}_{K'}^{v_K(\Delta)+c(\chi)}$$

agree, so $\bar{\xi}(\overline{\Delta}) = \overline{\Delta'}$. Thus, to get the desired $\chi(\Delta) = \chi'(\Delta')$, it remains to use local class field theory to identify χ (resp., χ') with a character of $K^\times/U_K^{c(\chi)}$ (resp., of $K'^\times/U_{K'}^{c(\chi)}$) and to apply [Del84, 3.6.1] to get $\chi = \chi' \circ \bar{\xi}$. □

Lemma 4.8. *Let $E'_{\chi'}$ denote the quadratic twist of E' by χ'.*

(a) *The minimal discriminants* $\Delta_{\chi,\min}$ *and* $\Delta'_{\chi',\min}$ *of* E_χ *and* $E'_{\chi'}$ *satisfy*

$$v_K(\Delta_{\chi,\min}) = v_{K'}(\Delta'_{\chi',\min}).$$

(b) *The Néron models* $\mathcal{E}_\chi \to \operatorname{Spec} \mathcal{O}_K$ *and* $\mathcal{E}'_{\chi'} \to \operatorname{Spec} \mathcal{O}_{K'}$ *of* E_χ *and* $E'_{\chi'}$ *satisfy*

$$\mathcal{E}^0_{\chi,\mathbb{F}} \simeq \mathcal{E}'^0_{\chi',\mathbb{F}} \qquad \text{and} \qquad (\mathcal{E}_{\chi,\mathbb{F}}/\mathcal{E}^0_{\chi,\mathbb{F}})(\mathbb{F}) \simeq (\mathcal{E}'_{\chi',\mathbb{F}}/\mathcal{E}'^0_{\chi',\mathbb{F}})(\mathbb{F}).$$

(c) *We have*[4]

$$\dim_{\mathbb{F}_2}(E(K)/\mathrm{Norm}_{K_\chi/K}E(K_\chi)) = \dim_{\mathbb{F}_2}(E'(K')/\mathrm{Norm}_{K'_{\chi'}/K'}E'(K'_{\chi'})).$$

Proof. In proving (a) and (b), we treat the cases $p \neq 2$ and $p = 2$ separately. The $p \neq 2$ case, which we consider first, is simpler.

If $p \neq 2$, then let $d \in \mathcal{O}_K$ with $v_K(d) \le 1$ be the element fixed in §4.1, so that

$$K_\chi = K(\sqrt{d}).$$

If $v_K(d) = 0$, choose a $d' \in \mathcal{O}_{K'}$ lifting $\phi(\overline{d})$; if $v_K(d) = 1$, choose a $d' \in \mathfrak{m}_{K'}$ lifting $\eta(\overline{d})$. Then $v_{K'}(d') \le 1$ and, by §2.5,

$$K'_{\chi'} \simeq K'(\sqrt{d'}).$$

Moreover, by [KT82, (7.4.2) on p. 331],

$$y^2 = x^3 + \tfrac{1}{4}d'(a_1'^2 + 4a_2')x^2 + \tfrac{1}{2}d'^2(a_1'a_3' + 2a_4')x + \tfrac{1}{4}d'^3(a_3'^2 + 4a_6')$$

is an integral Weierstrass equation for $E'_{\chi'}$. By construction, this equation is congruent via ϕ to the one for E_χ fixed in §4.1. Thus, if $p \neq 2$, then (a) and (b) result from Proposition 3.2 (ii) and (iii).

If $p = 2$, then let $\gamma \in K$ and $\pi_K \in \mathcal{O}_K$ be the element and the uniformizer fixed in §4.2, so that

$$K_\chi \simeq K[x]/(x^2 - x + \gamma)$$

and either $v_K(\gamma) = 0$ or $v_K(\gamma)$ is both negative and odd. As in §4.2, let $r \in \mathbb{Z}_{\ge 0}$ be minimal such that $\pi_K^{2r}\gamma \in \mathcal{O}_K$. Then

$$K_\chi \simeq K[x]/(x^2 - \pi_K^r x + \pi_K^{2r}\gamma),$$

and the polynomial $x^2 - \pi_K^r x + \pi_K^{2r}\gamma$ cuts out the unramified quadratic extension if $r = 0$ and is Eisenstein if $r > 0$. Choose a $\pi_{K'} \in \mathfrak{m}_{K'}$ lifting $\eta(\overline{\pi_K})$. If $r = 0$, choose a $\gamma' \in \mathcal{O}_{K'}$ lifting $\phi(\overline{\gamma})$; if $r > 0$, choose a $\gamma' \in K'$ in such a way that $\pi_{K'}^{2r}\gamma' \in \mathfrak{m}_{K'}$ lifts $\eta(\overline{\pi_K}^{2r}\overline{\gamma})$. By §2.5,

$$K'_{\chi'} \simeq K'[x]/(x^2 - \pi_{K'}^r x + \pi_{K'}^{2r}\gamma')$$

and $r \in \mathbb{Z}_{\ge 0}$ is minimal such that $\pi_{K'}^{2r}\gamma' \in \mathcal{O}_{K'}$. By Proposition 2.7 (or by reasoning as in §4.2), the discriminant ideal of $K'_{\chi'}/K'$ is $(\pi_{K'}^{2r}) \subset \mathcal{O}_{K'}$. By construction, $v_{K'}(2) = e$ and $e \ge v_K(\mathfrak{d}_{K_\chi/K}) = 2r$, so $4\gamma' \in 2\mathcal{O}_{K'}$. Therefore, by [KT82, (7.4.4) on p. 331],

$$\begin{aligned}&y^2 + \pi_{K'}^r(1-4\gamma')a_1'xy + \pi_{K'}^{3r}(1-4\gamma')^2a_3'y = \\ &\quad x^3 + \pi_{K'}^{2r}(1-4\gamma')(a_2' + \gamma'a_1'^2)x^2 + \pi_{K'}^{4r}(1-4\gamma')^2(a_4' + 2\gamma'a_1'a_3')x + \pi_{K'}^{6r}(1-4\gamma')^3(a_6' + \gamma'a_3'^2)\end{aligned}$$

is an integral Weierstrass equation for $E'_{\chi'}$. By construction, this equation is congruent via ϕ to the one for E_χ fixed in §4.2. Thus, (a) and (b) again follow from Proposition 3.2 (ii) and (iii).

Due to [KT82, Thm. 7.6], (c) follows from the proof of (a) and (b) given above and from Proposition 3.2 (i)–(iii) applied to E and to E_{K_χ}. Namely, it remains to note that due to

[4] As explained in [KT82, Prop. 7.3], the quotient $E(K)/\mathrm{Norm}_{K_\chi/K}E(K_\chi)$ is finite even when $\operatorname{char} K = 2$.

[KT82, Lemma 7.1 (1)], the "stretching factors" considered in [KT82, Thm. 7.6] are determined by the valuations of the minimal discriminant and of the discriminant of the model at hand. □

Theorem 4.9. *The Kramer–Tunnell conjecture* (★) *holds.*

Proof. Due to Lemma 4.6, Lemma 4.7, and Lemma 4.8 (c), all the terms in (★) for E and χ match with the corresponding terms for some E' and χ' in characteristic 0. To finish the proof, recall that the characteristic 0 case of the Kramer–Tunnell conjecture has been proved in most cases in [KT82] and in all the remaining cases in [DD11, Thm. 4.7]. □

References

[BH06] Colin J. Bushnell and Guy Henniart, *The local Langlands conjecture for* GL(2), Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 335, Springer-Verlag, Berlin, 2006. MR2234120 (2007m:22013)

[Čes16] Kęstutis Česnavičius, *The p-parity conjecture for elliptic curves with a p-isogeny*, J. reine angew. Math., to appear (2016). Available at `http://arxiv.org/abs/1207.0431`.

[Del75] P. Deligne, *Courbes elliptiques: formulaire d'après J. Tate*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, pp. 53–73. Lecture Notes in Math., Vol. 476 (French). MR0387292 (52 #8135)

[Del84] ———, *Les corps locaux de caractéristique p, limites de corps locaux de caractéristique* 0, Représentations des groupes réductifs sur un corps local, Travaux en Cours, Hermann, Paris, 1984, pp. 119–157 (French). MR771673 (86g:11068)

[DD08] Tim Dokchitser and Vladimir Dokchitser, *Root numbers of elliptic curves in residue characteristic 2*, Bull. Lond. Math. Soc. **40** (2008), no. 3, 516–524, DOI 10.1112/blms/bdn034. MR2418807 (2009k:11093)

[DD11] ———, *Root numbers and parity of ranks of elliptic curves*, J. reine angew. Math. **658** (2011), 39–64, DOI 10.1515/CRELLE.2011.060. MR2831512

[DD16] ———, *Euler factors determine local Weil representations*, J. reine angew. Math., to appear (2016). Available at `http://arxiv.org/abs/1112.4889`.

[Hel09] H. A. Helfgott, *On the behaviour of root numbers in families of elliptic curves*, preprint (2009). Available at `http://arxiv.org/abs/math/0408141`.

[Ima15] Naoki Imai, *Local root numbers of elliptic curves over dyadic fields*, J. Math. Sci. Univ. Tokyo **22** (2015), no. 1, 247–260. MR3329196

[Kis99] Mark Kisin, *Local constancy in p-adic families of Galois representations*, Math. Z. **230** (1999), no. 3, 569–593, DOI 10.1007/PL00004706. MR1680032 (2000f:14034)

[KT82] K. Kramer and J. Tunnell, *Elliptic curves and local ε-factors*, Compositio Math. **46** (1982), no. 3, 307–352. MR664648 (83m:14031)

[Roh94] David E. Rohrlich, *Elliptic curves and the Weil-Deligne group*, Elliptic curves and related topics, CRM Proc. Lecture Notes, vol. 4, Amer. Math. Soc., Providence, RI, 1994, pp. 125–157. MR1260960 (95a:11054)

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg. MR554237 (82e:12016)

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368 (96b:11074)

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA

E-mail address: `kestutis@berkeley.edu`

Graduate School of Mathematical Sciences, The University of Tokyo, 3-8-1 Komaba, Meguro-ku, Tokyo, 153-8914, Japan

E-mail address: `naoki@ms.u-tokyo.ac.jp`