The p-parity conjecture for elliptic curves with a p-isogeny

Citation: Česnavičius, Kęstutis. "The p-Parity Conjecture for Elliptic Curves with a p-Isogeny." Journal Für Die Reine Und Angewandte Mathematik (Crelles Journal) 2016, 719 (January 2016): 45-73 © 2016 De Gruyter

As Published: http://dx.doi.org/10.1515/crelle-2014-0040

Publisher: Walter de Gruyter

Persistent URL: http://hdl.handle.net/1721.1/112218

Version: Final published version: final published article, as it appeared in a journal, conference proceedings, or other formally published context

J. reine angew. Math. **719** (2016), 45–73
DOI 10.1515/crelle-2014-0040

Journal für die reine und angewandte Mathematik

The p-parity conjecture for elliptic curves with a p-isogeny

By *Kęstutis Česnavičius* at Cambridge, MA

Abstract. For an elliptic curve E over a number field K, one consequence of the Birch and Swinnerton-Dyer conjecture is the parity conjecture: the global root number matches the parity of the Mordell–Weil rank. Assuming finiteness of $Ш(E/K)[p^\infty]$ for a prime p this is equivalent to the p-parity conjecture: the global root number matches the parity of the $\mathbb{Z}_p$-corank of the p^∞-Selmer group. We complete the proof of the p-parity conjecture for elliptic curves that have a p-isogeny for $p > 3$ (the cases $p \leq 3$ were known). Tim and Vladimir Dokchitser have showed this in the case when E has semistable reduction at all places above p by establishing respective cases of a conjectural formula for the local root number. We remove the restrictions on reduction types by proving their formula in the remaining cases. We apply our result to show that the p-parity conjecture holds for every E with complex multiplication defined over K. Consequently, if for such an elliptic curve $Ш(E/K)[p^\infty]$ is infinite, it must contain $(\mathbb{Q}_p/\mathbb{Z}_p)^2$.

1. Introduction

If E is an elliptic curve defined over a number field K, its completed L-series is conjectured to have a holomorphic continuation $\Lambda(E/K, s)$ to the whole complex plane, and to satisfy a functional equation

$$\Lambda(E/K, 2-s) = w(E/K)\Lambda(E/K, s). \tag{1}$$

Here $w(E/K) \in \{\pm 1\}$ is the *global root number* of E/K. It can be given a definition independent of (1) as the product

$$w(E/K) = \prod_{v \text{ place of } K} w(E/K_v) \tag{2}$$

of *local root numbers* $w(E/K_v) \in \{\pm 1\}$ (here K_v is the completion of K at v), with $w(E/K_v)$ defined as the root number of the Weil–Deligne representation associated to E/K_v if $v \nmid \infty$, and $w(E/K_v) = -1$ if $v \mid \infty$ (cf., for instance, [Roh94]).

Granting holomorphic continuation of $\Lambda(E/K, s)$, the Birch and Swinnerton-Dyer conjecture (BSD) predicts that

$$\operatorname{ord}_{s=1} \Lambda(E/K, s) = \operatorname{rk} E(K), \tag{3}$$

where $\operatorname{rk} E(K) := \dim_{\mathbb{Q}} E(K) \otimes \mathbb{Q}$ is the *Mordell–Weil rank* of E/K. Combining (1) and (3) one gets

Conjecture 1.1 (Parity conjecture). One has $(-1)^{\operatorname{rk} E(K)} = w(E/K)$.

The parity conjecture is more approachable than BSD, and Tim and Vladimir Dokchitser have showed [DD11, Theorem 1.2] that it holds if one assumes that the 2- and 3-primary parts of the Shafarevich–Tate group $Ш(E/K(E[2]))$ are finite ($K(E[2])$ is the smallest extension of K over which the 2-torsion of E is rational).

If one hopes for unconditional results, then one is led to consider the p^∞-Selmer rank $\operatorname{rk}_p(E/K)$ instead of $\operatorname{rk} E(K)$ for each prime p. To define it one takes the exact sequence

$$0 \to E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \varinjlim \operatorname{Sel}_{p^n}(E/K) \to Ш(E/K)[p^\infty] \to 0 \tag{4}$$

and lets

$$\operatorname{rk}_p(E/K) := \dim_{\mathbb{Q}_p} \operatorname{Hom}_{\mathbb{Z}_p}(\varinjlim \operatorname{Sel}_{p^n}(E/K), \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

be the $\mathbb{Z}_p$-corank of the p-primary torsion abelian group $\varinjlim \operatorname{Sel}_{p^n}(E/K)$. From (4) one gets

$$\operatorname{rk}_p(E/K) = \operatorname{rk} E(K) + r_p(E/K), \tag{5}$$

where $r_p(E/K)$ is the $\mathbb{Z}_p$-corank of $Ш(E/K)[p^\infty]$ (equivalently, $r_p(E/K) =$ the number of copies of $\mathbb{Q}_p/\mathbb{Z}_p$ in $Ш(E/K)[p^\infty]$). Since $Ш(E/K)$ is conjectured to be finite [Tat74, Conjecture 1] (to the effect that $r_p = 0$), Conjecture 1.1 leads to

Conjecture 1.2 (p-parity conjecture). One has $(-1)^{\operatorname{rk}_p(E/K)} = w(E/K)$.

The p-parity conjecture is known if $K = \mathbb{Q}$ thanks to the work of Nekovář [Nek06, Section 0.17], Kim [Kim07, Theorem 1.4], and T. and V. Dokchitser [DD10], and also if K is totally real excluding some cases of potential complex multiplication [Nek09], [Nek12, Theorem A], [Nek14, Section 5.12]. Over arbitrary K and for arbitrary p the following theorem of T. and V. Dokchitser is the most general result currently known (one can weaken the assumptions on reduction types above p somewhat, see Theorem 1.16).

Theorem 1.3 ([DD08, Theorem 2] and [DD11, Corollary 5.8]). *The p-parity conjecture holds for E/K provided that E has a p-isogeny (defined over K) and either $p \leq 3$ or E has semistable reduction at all places of K above p.*

The main goal of this paper is to remove the semistable hypothesis in Theorem 1.3. Namely, we complete the proof of the following result.

Theorem 1.4 (Sections 1.13, 2.20 and 2.21, and Theorem 5.26). *The p-parity conjecture holds for E/K provided that E has a p-isogeny.*

In fact, both the global root number and the parity of the p^∞-Selmer rank do not change in an odd degree Galois extension [DD09, Proposition A.2 (3)], so this gives a slightly stronger

Theorem 1.4′. *The p-parity conjecture holds for E/K provided that the elliptic curve E acquires a p-isogeny over an odd degree Galois extension of K.*

Since $\operatorname{rk} E(K) = \operatorname{rk}_p(E/K)$ is equivalent to finiteness of the group $Ш(E/K)[p^\infty]$, from Theorem 1.4′ we get

Corollary 1.5. *The parity conjecture holds for E/K provided that the elliptic curve E acquires a p-isogeny over an odd degree Galois extension of K and $Ш(E/K)[p^\infty]$ is finite.*

Implications for elliptic curves with complex multiplication. I thank Karl Rubin for pointing out to me that one corollary of Theorem 1.4 is

Theorem 1.6 (Theorem 6.4). *Let E be an elliptic curve defined over a number field K, and suppose that $\operatorname{End}_K E \neq \mathbb{Z}$, i.e., that E has complex multiplication defined over K. Then the p-parity conjecture holds for E/K for every prime p.*

Remark 1.7. If E is an elliptic curve over a totally real field L with complex multiplication (necessarily defined over a non-trivial extension of L), the p-parity conjecture for E/L has been established by Nekovář [Nek12, Theorem A] in the cases where $2 \nmid [L : \mathbb{Q}]$ or p splits in $(\operatorname{End}_{\overline{L}} E) \otimes \mathbb{Q}$.

If E/K is as in Theorem 1.6, then $F := (\operatorname{End}_K E) \otimes \mathbb{Q}$ is an imaginary quadratic field and $E(K) \otimes \mathbb{Q}$ is an F-vector space. Consequently, $\operatorname{rk} E(K) = \dim_{\mathbb{Q}} E(K) \otimes \mathbb{Q}$ is even. This is half of

Theorem 1.8 (Proposition 6.3). *If E has complex multiplication defined over K, then the parity conjecture holds for E/K. More precisely, $\operatorname{rk} E(K)$ is even and $w(E/K) = 1$.*

Since $w(E/K) = 1$, Theorem 1.6 tells us that $\operatorname{rk}_p(E/K)$ is even. Therefore, from (5) we obtain that $r_p(E/K)$ is even as well. Concerning the conjectural finiteness of $Ш(E/K)$, this gives

Theorem 1.9. *If E has complex multiplication defined over K and $Ш(E/K)[p^\infty]$ is infinite, then $Ш(E/K)[p^\infty]$ contains $(\mathbb{Q}_p/\mathbb{Z}_p)^2$.*

If $Ш(E/K)_{\mathrm{div}}$ denotes the divisible part of the Shafarevich–Tate group

$$Ш(E/K) \cong Ш(E/K)_{\mathrm{div}} \oplus (Ш(E/K)/Ш(E/K)_{\mathrm{div}}),$$

then from the Cassels–Tate pairing [Cas62] one knows that $\dim_{\mathbb{F}_p}(Ш(E/K)/Ш(E/K)_{\mathrm{div}})[p]$ is even. As $\dim_{\mathbb{F}_p} Ш(E/K)_{\mathrm{div}}[p] = r_p(E/K)$, we obtain

Theorem 1.10. *If E has complex multiplication defined over K, then the $\mathbb{F}_p$-dimension of $Ш(E/K)[p]$ is even.*

Theorem 1.10 is a special case of the following weaker version of the Shafarevich–Tate conjecture:

Conjecture Ш$\mathrm{T}_p(K)$ ([MR10, p. 545]). For every elliptic curve E/K, the $\mathbb{F}_p$-dimension of $Ш(E/K)[p]$ is even.

For an application of Conjecture $Ш\mathrm{T}_p(K)$ to Hilbert's Tenth Problem, see [MR10, Theorem 1.2].

The strategy of proof of Theorem 1.4. It is known (see Section 1.13) that a conjectural formula of T. and V. Dokchitser (Conjecture 1.12) for the local root number implies Theorem 1.4 if $p > 2$. In fact, Theorem 1.3 was proved in [DD08, Section 5] and [DD11] for $p \geq 3$ by establishing appropriate cases of this formula (recalled in Section 2). We introduce it after the following preparations.

1.11. The setup. Let K_v (to be renamed K from Section 2.1 on) be a local field of characteristic 0 and let E/K_v be an elliptic curve with a (K_v-rational) isogeny

$$E \xrightarrow{\phi} E'$$

of prime degree $p \geq 3$. Let

$$\psi\colon \mathrm{Gal}(\overline{K}_v/K_v) \to \mathrm{Aut}(E[\phi]) \cong \mathbb{F}_p^\times$$

be the character giving the Galois action on the kernel $E[\phi]$ of the isogeny and let

$$K_{v,\psi} = K_v(E[\phi])$$

be the fixed field of $\ker\psi$. We denote by $\phi_v\colon E(K_v) \to E'(K_v)$ the map on K_v-points induced by ϕ and note that the long exact cohomology sequence for ϕ tells us that $\#\operatorname{coker}\phi_v$ is finite. Thus it is legitimate to set

$$\sigma_{\phi_v} = (-1)^{\mathrm{ord}_p\left(\frac{\#\operatorname{coker}\phi_v}{\#\ker\phi_v}\right)},$$

where $\mathrm{ord}_p a$ is the p-adic valuation of $a \in \mathbb{Q}^\times$. Denoting by $(\psi, -1)_v$ the Artin symbol defined by

$$(\psi,-1)_v = \begin{cases} 1, & \text{if } -1 \text{ is a norm in } K_{v,\psi}/K_v, \\ -1, & \text{if not,} \end{cases} \tag{6}$$

(see Section 2.13 for another description), we are ready to state

Conjecture 1.12 (p-isogeny conjecture [DD11, Conjecture 5.3]). One has

$$w(E/K_v) = (\psi,-1)_v \cdot \sigma_{\phi_v}.$$

1.13. Conjecture 1.12 implies Theorem 1.4 for $p \geq 3$. A well-known global arithmetic duality argument using the Cassels–Poitou–Tate exact sequence (see, for instance, [CFKS10, Theorem 2.3]) shows that for $p \geq 3$

$$(-1)^{\mathrm{rk}_p(E/K)} = \prod_{v \text{ place of } K} \sigma_{\phi_v},$$

almost all factors on the right hand side being 1. Hence, Conjecture 1.12, the product formula for the Artin symbol from global class field theory, and (2) imply Theorem 1.4 if $p \geq 3$. Conjecture 1.12 has been settled in many cases, including the case $p = 3$ (see Section 2.22 and Theorem 5.2 for a summary of known cases); to prove Theorem 1.4 we settle the remaining cases, hence completing the proof of the following theorem.

Theorem 1.14 (Theorem 5.26). *The p-isogeny conjecture is true for $p > 3$.*

1.15. Progress to date. Using the work of Breuil [Bre00, Theorem 2.1] on classification of finite flat group schemes, Coates, Fukaya, Kato, and Sujatha have proved both a version of Theorem 1.4 in [CFKS10] and a version of Conjecture 1.12 in [CFKS10, Theorem 2.7] for abelian varieties of arbitrary dimension. Unfortunately, their methods require a set of hypotheses that exclude some cases of Conjecture 1.12. For elliptic curves and $p > 3$ their results give

Theorem 1.16 ([CFKS10, Corollary 2.2]). *For $p > 3$, the p-parity conjecture holds for E/K if E has a (K-rational) p-isogeny, and if at each place v above p one of the following is true:*

(a) *E has potentially good ordinary reduction at v,*

(b) *E has potentially multiplicative reduction at v,*

(c) *E achieves good supersingular reduction after a finite abelian extension of K_v.*

We make essential use of both the results and the methods of Coates, Fukaya, Kato, and Sujatha in Section 5 to settle Conjecture 1.12 in the case of a place $v \mid p$ of additive reduction of Kodaira type III or III*. In all other cases the proof is independent of Theorem 1.16.

1.17. The contents of the paper. In Section 2 we recall known cases of Conjecture 1.12 and indicate how Theorem 1.4 was proved by T. and V. Dokchitser if $p \leq 3$ (see Sections 2.20 and 2.21). We prove in Section 3 that the p-isogeny conjecture is compatible with making a quadratic twist. The work of Section 3 is used in Section 4, where we settle all the remaining cases of Conjecture 1.12 except those of Kodaira types III or III*. These are taken up in Section 5 where we make use of the results and methods of Coates, Fukaya, Kato, and Sujatha to finish our proof. In Section 6 we prove Theorems 1.6 and 1.8 that concern elliptic curves with complex multiplication.

1.18. Conventions. (See also Section 2.1 for a notational setup that is valid from Section 2 on.) Whenever we work with algebraic extensions of a (global or local) field K, they are implicitly assumed to lie inside a *fixed* separable closure $\overline{K}$ of K. Given a global field K and a place v, we implicitly fix an embedding $\overline{K} \hookrightarrow \overline{K}_v$ and get the corresponding inclusion of a decomposition group $\mathrm{Gal}(\overline{K}_v/K_v) \hookrightarrow \mathrm{Gal}(\overline{K}/K)$. For a finite flat group scheme (such as $E[\phi]$) over a field K of characteristic 0, we confuse it with its associated Galois representation (such as $E[\phi](\overline{K})$) whenever it is convenient to do so. If E is an elliptic curve over a field K, we sometimes write E/K to emphasize the base; if L/K is a field extension, then E/L denotes the corresponding base change $E \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L$. We also make use of the subscript notation to denote base change: for instance, $E[\phi]$ is a K-scheme, and $E[\phi]_L$ denotes the base change $E[\phi] \times_{\mathrm{Spec}\, K} \mathrm{Spec}\, L$.

Acknowledgement. I thank my advisor Bjorn Poonen for his support and many helpful conversations and suggestions, as well as for reading the manuscript very carefully. I thank Tim Dokchitser for his lectures at the Postech Winter School 2012 in Pohang, South Korea which got me interested in the question answered by this paper, and for pointing out to me Theorem 4.6. Thanks are also due to POSTECH and the organizers of the winter school for an inspiring and hospitable atmosphere. I thank Karl Rubin for telling me that Theorem 1.6

follows from Theorem 1.4. I thank Douglas Ulmer for a very helpful conversation about the technique of twisting. I thank Tim Dokchitser, Jessica Fintzen, Jan Nekovář, and Bjorn Poonen for comments. I thank the anonymous referee for suggestions and a careful reading of the manuscript.

2. Known cases of the p-isogeny conjecture

We have seen in Section 1.13 that Theorem 1.4 follows once we establish the p-isogeny conjecture (Conjecture 1.12). In this section we recall some of the known cases of the latter (Sections 2.3–2.4, Sections 2.10–2.12, Sections 2.17–2.20), all of which are due to T. and V. Dokchitser [DD08, Section 5], [DD11]. In the cases of Section 2.11 and Section 2.19 minor simplifications are provided by Corollary 2.15 and the results of Section 3. Since for the rest of the paper we will be working in a local setting, we first change the notation of Section 1.11 slightly (see also Section 1.18 for other conventions). We also recall the classification of local root numbers of elliptic curves in Theorem 2.2. In Section 2.21 we discuss the case $p = 2$ which is excluded from Conjecture 1.12.

2.1. The setup. From now on, K denotes a local field of characteristic 0 (which is assumed to be nonarchimedean from Section 2.5 on). If K is nonarchimedean, we write v (or v_K) for its normalized discrete valuation, $\mathcal{O}_K$ for the ring of integers, $\mathfrak{m}_K$ for the maximal ideal, π_K for a uniformizer, and $\mathbb{F}_K$ for the residue field. If L/K is a finite extension of nonarchimedean local fields, we write $e_{L/K}$ and $f_{L/K}$ for the ramification index and the degree of the residue field extension, respectively. Let E/K be an elliptic curve with a (K-rational) p-isogeny $\phi\colon E \to E'$ for a prime $p \geq 3$. The map on K-points induced by ϕ is denoted by $\phi_K\colon E(K) \to E'(K)$. We write K_ψ for the fixed field of the kernel of the Galois character

$$\psi\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[\phi]) \cong \mathbb{F}_p^\times.$$

We write $(\psi, -1)_K$, instead of $(\psi, -1)_v$, for the Artin symbol (6). Conjecture 1.12 becomes

$$w(E/K) \stackrel{?}{=} (\psi, -1)_K \cdot \sigma_{\phi_K}. \tag{7}$$

Theorem 2.2 ([Roh96, Theorem 2], [Kob02, Theorem 1.1], reformulated in [DD10, Theorem 3.1]). *Let E be an elliptic curve over a local field K. Then*

(a) $w(E/K) = -1$ *if K is archimedean.*

If K is nonarchimedean, then:

(b) $w(E/K) = 1$ *if E has good or non-split multiplicative reduction,*

(c) $w(E/K) = -1$ *if E has split multiplicative reduction,*

(d) $w(E/K) = (\frac{-1}{\mathbb{F}_K})$ *if E has additive potentially multiplicative reduction and* $\mathrm{char}\,\mathbb{F}_K > 2$ *(here $(\frac{-1}{\mathbb{F}_K})$ is 1 if $-1 \in \mathbb{F}_K^{\times 2}$ and -1 otherwise),*

(e) $w(E/K) = (-1)^{\lfloor v(\Delta)\cdot \#\mathbb{F}_K/12 \rfloor}$ *if E has potentially good reduction and* $\mathrm{char}\,\mathbb{F}_K > 3$ *(here Δ is a minimal discriminant of E).*

We now begin the proof of (7).

2.3. The case $K = \mathbb{C}$. Since $E[\phi] \subset E(\mathbb{C})$ and $\operatorname{coker}\phi_K = 0$, one has $(\psi, -1)_K = 1$ and $\sigma_{\phi_K} = -1$. Since K is archimedean, $w(E/K) = -1$, and (7) holds.

2.4. The case $K = \mathbb{R}$. Since $\operatorname{coker}\phi_K$ is 2-torsion, $p \geq 3$, and $\#\ker\phi_K = 1$ or p, we have $\sigma_{\phi_K} = 1$ or $\sigma_{\phi_K} = -1$, respectively. Accordingly, $K_\psi = \mathbb{C}$ or $K_\psi = \mathbb{R}$, so by (6), $(\psi, -1)_K = -1$ or $(\psi, -1)_K = 1$. Since $w(E/K) = -1$, (7) holds in both cases.

Since the archimedean cases of (7) have been dealt with in Sections 2.3–2.4, we assume from now on that K is nonarchimedean.

2.5. If $f\colon A \to A'$ is a homomorphism of abelian groups, we write $\chi(f)$ for $\frac{\#\operatorname{coker} f}{\#\ker f}$. Whenever we do so, it is implicitly assumed that the quotient makes sense, i.e., that $\ker f$ and $\operatorname{coker} f$ are both finite. With this notation, $\sigma_{\phi_K} = (-1)^{\operatorname{ord}_p \chi(\phi_K)}$. We state several elementary properties of $\chi(f)$ that will be used later.

Proposition 2.6. *Given a morphism of short exact sequences*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0, \end{array}$$

one has $\chi(g) = \chi(f)\chi(h)$.

Proof. The proposition follows from the snake lemma. □

Proposition 2.7. *If $f\colon A \to A'$ and A, A' are finite, then $\chi(f) = \frac{\#A'}{\#A}$.* □

Lemma 2.8. *Let $f\colon K^\times \to K^\times$ be the p^{th} power map. Then*

$$\chi(f) = \begin{cases} p, & \text{if } \operatorname{char}\mathbb{F}_K \neq p, \\ p^{1+[K:\mathbb{Q}_p]}, & \text{if } \operatorname{char}\mathbb{F}_K = p. \end{cases}$$

Proof. A choice of a uniformizer π_K gives $K^\times \cong \mathbb{Z} \times \mathcal{O}_K^\times$, so

$$\chi(f) = p \cdot \chi\big(\mathcal{O}_K^\times \xrightarrow{f} \mathcal{O}_K^\times\big)$$

by Proposition 2.6. If one uses the filtration of $\mathcal{O}_K^\times$ by higher units together with the logarithm isomorphism $1 + \mathfrak{m}_K^n \cong \mathfrak{m}_K^n$ for big enough n, from Propositions 2.6 and 2.7 one gets

$$\chi\big(\mathcal{O}_K^\times \xrightarrow{f} \mathcal{O}_K^\times\big) = \chi(p),$$

where $p\colon \mathfrak{m}_K^n \to \mathfrak{m}_K^n$ is the multiplication by p map. Observe that the latter is an isomorphism if $\operatorname{char}\mathbb{F}_K \neq p$; if $\operatorname{char}\mathbb{F}_K = p$, one has $\chi(p) = p^{[K:\mathbb{Q}_p]}$. □

2.9. Another description of σ_{ϕ_K}. Let $E_0(K) \subset E(K)$ be the subgroup consisting of points whose reduction lies in the identity component $\widetilde{\mathcal{E}}^0$ of the special fiber $\widetilde{\mathcal{E}} := \mathcal{E} \times_{\mathcal{O}_K} \mathbb{F}_K$ of the Néron model $\mathcal{E}/\mathcal{O}_K$ of E/K. The reduction homomorphism

$$E(K) \cong \mathcal{E}(\mathcal{O}_K) \xrightarrow{r} \widetilde{\mathcal{E}}(\mathbb{F}_K)$$

is surjective because $\mathcal{E}/\mathcal{O}_K$ is smooth and $\mathcal{O}_K$ is henselian [BLR90, Section 2.3, Proposition 5], so

$$E(K)/E_0(K) \cong \widetilde{\mathcal{E}}(\mathbb{F}_K)/\widetilde{\mathcal{E}}^0(\mathbb{F}_K),$$

which is finite. The order of $E(K)/E_0(K)$ is the *local Tamagawa factor* $c_{E/K}$. The kernel of r is denoted by $E_1(K)$, so $E_0(K)/E_1(K) \cong \widetilde{\mathcal{E}}^0(\mathbb{F}_K)$. The cardinality of the latter is invariant with respect to K-rational isogenies: this can be seen, for instance, from the isogeny invariance of the local L-factor $L(E/K, s)$ which encodes $\#\widetilde{\mathcal{E}}^0(\mathbb{F}_K)$. Applying Propositions 2.6 and 2.7 to

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_0(K) & \longrightarrow & E(K) & \longrightarrow & E(K)/E_0(K) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi_0} & & \downarrow{\scriptstyle \phi_K} & & \downarrow & & \\ 0 & \longrightarrow & E_0'(K) & \longrightarrow & E'(K) & \longrightarrow & E'(K)/E_0'(K) & \longrightarrow & 0 \end{array}$$

and a similar diagram for $E_1(K) \subset E_0(K)$ gives

$$\chi(\phi_K) = \frac{c_{E'/K}}{c_{E/K}}\chi(\phi_0) = \frac{c_{E'/K}}{c_{E/K}}\chi(\phi_1).$$

If $p \neq \operatorname{char} \mathbb{F}_K$, then ϕ_1 is an isomorphism [Tat74, Corollary 1], so

$$\sigma_{\phi_K} = (-1)^{\operatorname{ord}_p \chi(\phi_K)} = (-1)^{\operatorname{ord}_p \frac{c_{E'/K}}{c_{E/K}}}. \tag{8}$$

If $\operatorname{char} \mathbb{F}_K = p$, one cannot use this formula. Instead one proceeds as follows: since $E_1(K)$ can be identified with the points of the formal group associated to E, one has the canonical exhaustive filtration $E_1(K) \supset E_2(K) \supset \cdots$ defined by $E_m(K) := \ker(\mathcal{E}(\mathcal{O}_K) \to \mathcal{E}(\mathcal{O}_K/\mathfrak{m}_K^m))$ (see the proof of Lemma 5.15 for another description). The subquotients of the filtration are $E_i(K)/E_{i+1}(K) \cong \mathbb{F}_K$ (see [Tat75, Section 4]). With this at hand, one applies Propositions 2.6 and 2.7 repeatedly to get $\chi(\phi_1) = \chi(\phi_m)$ for $m \geq 1$. Choose Néron differentials ω on $\mathcal{E}$ and ω' on $\mathcal{E}'$. Then $\phi^*\omega' = \alpha\omega$ for some $\alpha \in \mathcal{O}_K$. For m large enough, formal logarithm furnishes isomorphisms $E_m(K) \xrightarrow{\sim} \mathfrak{m}_K^m$ and $E_m'(K) \xrightarrow{\sim} \mathfrak{m}_K^m$, under which, by [Rub99, Proposition 3.14], ϕ_m corresponds to multiplication by α. The analogue of (8) is therefore

$$\sigma_{\phi_K} = (-1)^{v(\alpha) f_{K/\mathbb{Q}_p} + \operatorname{ord}_p \frac{c_{E'/K}}{c_{E/K}}}. \tag{9}$$

Formula (9) is a special case of a more general formula [Sch96, Lemma 3.8] valid for abelian varieties of any dimension.

If E has potentially good reduction, then the local Tamagawa factors are at most 4 (see, for instance, [Tat74, Addendum to Theorem 3]). If in addition $p > 3$, then (8) for the case $\operatorname{char} \mathbb{F}_K \neq p$ becomes

$$\sigma_{\phi_K} = 1,$$

and (9) for the case $\operatorname{char} \mathbb{F}_K = p$ becomes

$$\sigma_{\phi_K} = (-1)^{v(\alpha) f_{K/\mathbb{Q}_p}}. \tag{10}$$

2.10. The case $\operatorname{char} \mathbb{F}_K \neq p$, and E has good reduction. The local Tamagawa factors are 1, so (8) gives $\sigma_{\phi_K} = 1$. Also, $K_\psi \subset K(E[p])$, and the latter is an unramified extension of K by the criterion of Néron–Ogg–Shafarevich. Hence, so is K_ψ/K, and from (6) we get $(\psi, -1)_K = 1$. By Theorem 2.2 (b), $w(E/K) = 1$, and (7) holds.

2.11. The case $\operatorname{char}\mathbb{F}_K \neq p$, and E has potentially multiplicative reduction. If the reduction is not split multiplicative, it becomes so after a unique quadratic extension L/K which is unramified if and only if E has multiplicative reduction [Tat74, pp. 190–191]. The quadratic twist of E by L/K has split multiplicative reduction (this can be seen, for instance, from Proposition 3.8). By Theorem 3.12, we are therefore reduced to the case of split multiplicative reduction (see Remark 3.13).

Using Tate's theory of rigid analytic uniformization (loc. cit.) one has $E \cong \mathbb{G}_m/q^{\mathbb{Z}}$ for some $q \in K^\times$ with $v(q) > 0$ (and similarly for E'). Using rigid-analytic GAGA one sees that $\phi\colon E \to E'$ can be written as $\mathbb{G}_m/q^{\mathbb{Z}} \to \mathbb{G}_m/(q^p)^{\mathbb{Z}}$ induced by the p^{th} power map, or $\mathbb{G}_m/(q'^p)^{\mathbb{Z}} \to \mathbb{G}_m/(q')^{\mathbb{Z}}$ induced by the identity. By Proposition 2.6 and Lemma 2.8, in the first case $\chi(\phi_K) = p$; in the second $\chi(\phi_K) = 1/p$. In both cases $\sigma_{\phi_K} = -1$. In the first case $K_\psi = K(\zeta_p)$; in the second $K_\psi = K$. In both cases K_ψ/K is unramified, so $(\psi, -1)_K = 1$. Theorem 2.2 (c) gives $w(E/K) = -1$, and (7) holds.

2.12. The case $\operatorname{char}\mathbb{F}_K \neq p$, $p > 3$, and E has additive potentially good reduction. This is [DD08, Lemma 9].

2.13. Another description of the Artin symbol. For a continuous character

$$\theta\colon \operatorname{Gal}(\overline{K}/K) \to \mathbb{Q}/\mathbb{Z}$$

and $a \in K^\times$, let $(\theta, a)_K \in \mathbb{Q}/\mathbb{Z}$ be the corresponding symbol (cf. [Ser79, Chapter XIV, Section 1]). It can also be defined by setting

$$(\theta, a)_K := \theta(\operatorname{Art}_K(a))$$

where

$$\operatorname{Art}_K\colon K^\times \to \operatorname{Gal}(\overline{K}/K)^{\text{ab}}$$

is the local Artin homomorphism. Therefore, the pairing $(\theta, a)_K$ is bilinear, and if K_θ is the fixed field of $\ker\theta$, then $(\theta, a)_K$ vanishes if and only if a is a norm in K_θ/K. Since we are only interested in the case $a = -1$, we think of $(\theta, -1)_K$ as taking values in $\{\pm 1\}$.

Fix an injection $\mathbb{F}_p^\times \hookrightarrow \mathbb{Q}/\mathbb{Z}$. One possible choice for θ is ψ (Section 2.1). In this case one has $K_\psi = K(E[\phi])$, and we recover the Artin symbol $(\psi, -1)_K$ (cf. (6)). Another possible choice is the cyclotomic character $\omega : \operatorname{Gal}(\overline{K}/K) \to \mathbb{F}_p^\times$ described as follows: for ζ_p a primitive p^{th} root of unity $s(\zeta_p) = \zeta_p^{\omega(s)}$ (this is independent of ζ_p). In this case $K_\omega = K(\zeta_p)$.

Lemma 2.14. *For a finite extension L/K and every θ as above, one has*

$$(\theta, -1)_L = (\theta, -1)_K^{[L:K]}.$$

Proof. This follows from the bottom diagram of [Ser67, Section 2.4] applied to -1. □

Corollary 2.15. *Suppose that K is a finite extension of $\mathbb{Q}_p$. Then*

$$(\omega, -1)_K = (-1)^{[K:\mathbb{Q}_p]}.$$

Proof. Since $(\omega, -1)_{\mathbb{Q}_p} = -1$ (see, e.g., [Ser67, Section 3.1, Theorem 2 (2)]), one applies Lemma 2.14. □

To handle the cases of (7) when $\operatorname{char}\mathbb{F}_K = p$ we need to be able to compute symbols $(\theta, -1)_K$ for continuous characters $\theta\colon \operatorname{Gal}(\overline{K}/K) \to \mathbb{F}_p^\times$, in which case K_θ is a cyclic extension of K of degree dividing $p-1$. These symbols have been worked out by T. and V. Dokchitser:

Lemma 2.16 ([DD08, Lemma 12]). *Let K be a finite extension of $\mathbb{Q}_p$ with p odd, and fix a character $\theta\colon \operatorname{Gal}(\overline{K}/K) \to \mathbb{F}_p^\times$. Then*

$$(\theta, -1)_K = (-1)^{f_{K/\mathbb{Q}_p}(p-1)/e_{K_\theta/K}};$$

in other words, $(\theta, -1)_K = 1$ if and only if either $f_{K/\mathbb{Q}_p}$ or $\frac{p-1}{e_{K_\theta/K}}$ is even.

2.17. The case $\operatorname{char}\mathbb{F}_K = p > 3$, E has potentially good reduction, and $f_{K/\mathbb{Q}_p}$ is even. We show that all the terms in (7) are 1. Lemma 2.16 gives $(\psi, -1)_K = 1$, whereas formula (10) gives $\sigma_{\phi_K} = 1$. To compute $w(E/K)$ we use Theorem 2.2 (e): $\#\mathbb{F}_K$ is a square, so one gets $\#\mathbb{F}_K \equiv 1 \bmod 24$, whereas $v(\Delta) < 12$ because the reduction is potentially good. Hence, $w(E/K) = (-1)^{\lfloor v(\Delta)/12 \rfloor} = 1$.

2.18. The case $\operatorname{char}\mathbb{F}_K = p$, and E has good reduction. Because of Section 2.17, we assume that $f_{K/\mathbb{Q}_p}$ is odd. By Theorem 2.2 (b), $w(E/K) = 1$, so by Lemma 2.16 and (10), to check (7) one needs to argue that

$$(-1)^{(p-1)/e_{K_\psi/K}} = (-1)^{v(\alpha)},$$

where α defined in Section 2.9 is also the coefficient of T in the power series $f(T)$ giving the action of ϕ on formal groups. This is done in [DD08, Section 6] by a careful analysis of $f(T)$.

2.19. The case $\operatorname{char}\mathbb{F}_K = p$, and E has potentially multiplicative reduction. The argument is the same as in Section 2.11, and the second case there requires no modification. In the first case, by Proposition 2.6 and Lemma 2.8, $\chi(\phi_K) = p^{1+[K:\mathbb{Q}_p]}$, so

$$\sigma_{\phi_K} = (-1)^{1+[K:\mathbb{Q}_p]}.$$

We have $K_\psi = K(\zeta_p)$, so by (6) and Corollary 2.15, $(\psi, -1)_K = (\omega, -1)_K = (-1)^{[K:\mathbb{Q}_p]}$. By Theorem 2.2 (c), $w(E/K) = -1$, so (7) holds.

2.20. The case $p = 3$. The argument of [DD08, Lemma 9] used in Section 2.12 faces complications if $p = 3$. Calculations are still manageable if $\operatorname{char}\mathbb{F}_K \neq p$ (see [DD08, Lemma 10]), but get out of hand if $\operatorname{char}\mathbb{F}_K = p$. To treat these cases, and hence establish (7) if $p = 3$, T. and V. Dokchitser have used a global-to-local deformation argument with [Nek09, Theorem 1] as an input, see [DD11, Theorem 5.7].

2.21. The case $p = 2$. Formula (7) does not hold if $p = 2$. Indeed, the kernel of a 2-isogeny is always rational, so $K_\psi = K$, giving $(\psi, -1)_K = 1$. If $K = \mathbb{R}$ and ϕ_K is not surjective, then $\#\operatorname{coker}\phi_K = 2$ and $\sigma_{\phi_K} = 1$. This violates (7), because by Theorem 2.2 (a) one has $w(E/\mathbb{R}) = -1$.

In case $p = 2$, Theorem 1.4 was proved by T. and V. Dokchitser by finding an analogue [DD11, Conjecture 5.3] of formula (7), proving it in most cases by direct computations in [DD08, Section 7], and using a global-to-local deformation argument to handle the remaining ones in [DD11, Theorem 5.7].

2.22. Summary of the known cases. By Sections 2.3–2.4, Sections 2.10–2.12, and Sections 2.17–2.20, the p-isogeny conjecture (7) is true in all the cases, except possibly when $\operatorname{char} \mathbb{F}_K = p > 3$, $f_{K/\mathbb{Q}_p}$ is odd, and the reduction is additive potentially good. After some preparations in Section 3 we take up the remaining cases in Section 4.

3. Compatibility with making a quadratic twist

To verify that the p-isogeny conjecture (7) is compatible with making a quadratic twist (Theorem 3.12), we investigate how its individual terms change under this operation (Propositions 3.4, 3.6 and 3.11). The technique of twisting is standard but to fix ideas we begin by recalling the way in which we prefer to think about it. The setup is that of Section 2.1.

3.1. Twisting by a quadratic Galois character. Suppose that L/K is a quadratic extension and let

$$\tau\colon \operatorname{Gal}(\overline{K}/K) \to \{\pm 1\}$$

be the corresponding nontrivial character. Since $\{\pm 1\} \leq \operatorname{Aut}_{\overline{K}}(E)$, we can think of

$$\tau\colon \operatorname{Gal}(\overline{K}/K) \to \operatorname{Aut}_{\overline{K}}(E)$$

as a (crossed) homomorphism and therefore identify the character τ with the corresponding element of $H^1(K, \operatorname{Aut}_{\overline{K}}(E))$. The elements of the latter pointed set classify *twists* of E (cf. [Ser02, Chapter I, Section 5.3] or [BS64, Proposition 2.6]), i.e., elliptic curves over K that are $\overline{K}$-isomorphic to E. In particular, τ gives rise to the *twist* $\widetilde{E}/K$ of E/K by L/K.

For a K-scheme X, the X-valued points of $\widetilde{E}$ are the $X \times_K \overline{K}$-valued points of

$$E_{\overline{K}} := E \times_K \overline{K}$$

that are invariant under the twisted by τ Galois action, i.e., those $P \in E(X \times_K \overline{K})$ with

$$P = \tau(s) \cdot {}^s P \quad \text{for all } s \in \operatorname{Gal}(\overline{K}/K).$$

These are $P \in E(X \times_K L)$ on which the nontrivial element $t \in \operatorname{Gal}(L/K)$ acts as ${}^t P = -P$. This gives a description of the functor of points of $\widetilde{E}/K$; we also see that the isomorphism $E_{\overline{K}} \cong \widetilde{E}_{\overline{K}}$ is $\operatorname{Gal}(\overline{K}/L)$-equivariant, so E and $\widetilde{E}$ are L-isomorphic. Twisting being functorial in E (loc. cit.), $\widetilde{E}$ possesses a p-isogeny $\widetilde{\phi}\colon \widetilde{E} \to \widetilde{E'}$ defined over K.

Remark 3.2. If $L = K(\sqrt{d})$ and one wishes to think in terms of Weierstrass equations

$$E\colon y^2 = x^3 + Ax + B, \tag{11}$$

then the quadratic twist described above is the usual

$$\widetilde{E}\colon dy^2 = x^3 + Ax + B.$$

Indeed, since $[-1]_E$ in these coordinates is $(x, y) \mapsto (x, -y)$, multiplying the y-coordinate by $\sqrt{d}$ has the desired effect as far as the Galois action is concerned. By scaling the variables

one can bring the equation for $\widetilde{E}$ to

$$y^2 = x^3 + Ad^2x + Bd^3. \tag{12}$$

The discriminants Δ and $\widetilde{\Delta}$ of (11) and (12) are related by

$$\widetilde{\Delta} = d^6\Delta. \tag{13}$$

3.3. Implications for the p-isogeny. Consider the restriction of scalars $N_{L/K}E$ of E/L back to K. By definition, $(N_{L/K}E)(X) = E(X \times_K L)$ functorially in X and E. We have seen that $\widetilde{E}(X)$ identifies with the -1-eigenspace of $(N_{L/K}E)(X)$ for the action of t; similarly $E(X)$ identifies with the $+1$-eigenspace. These identifications being functorial, one gets a K-homomorphism of abelian varieties

$$f_E : E \times \widetilde{E} \to N_{L/K}E.$$

Since the intersection of the eigenspaces consists of 2-torsion points, so does the kernel of f_E. We conclude that f_E is an isogeny and that

$$\left(E(X) \otimes \mathbb{Z}\left[\frac{1}{2}\right]\right) \oplus \left(\widetilde{E}(X) \otimes \mathbb{Z}\left[\frac{1}{2}\right]\right) \xrightarrow{\sim} (N_{L/K}E)(X) \otimes \mathbb{Z}\left[\frac{1}{2}\right].$$

The latter being functorial in X and E, taking $X = \operatorname{Spec} K$ we get the commutative diagram

$$\begin{array}{ccc} (E(K) \otimes \mathbb{Z}[\frac{1}{2}]) \oplus (\widetilde{E}(K) \otimes \mathbb{Z}[\frac{1}{2}]) & \xrightarrow{\sim} & E(L) \otimes \mathbb{Z}[\frac{1}{2}] \\ \downarrow{\scriptstyle (\phi_K \otimes \mathbb{Z}[\frac{1}{2}]) \oplus (\widetilde{\phi}_K \otimes \mathbb{Z}[\frac{1}{2}])} & & \downarrow{\scriptstyle \phi_L \otimes \mathbb{Z}[\frac{1}{2}]} \\ (E'(K) \otimes \mathbb{Z}[\frac{1}{2}]) \oplus (\widetilde{E'}(K) \otimes \mathbb{Z}[\frac{1}{2}]) & \xrightarrow{\sim} & E'(L) \otimes \mathbb{Z}[\frac{1}{2}]. \end{array} \tag{14}$$

Since $- \otimes \mathbb{Z}[\frac{1}{2}]$ is exact and does not affect the p-primary parts ($p > 2$), (14) gives

Proposition 3.4. *One has*

$$\sigma_{\phi_K}\sigma_{\widetilde{\phi}_K} = \sigma_{\phi_L}.$$

3.5. The twist of ψ. Describing the character $\widetilde{\psi}\colon \operatorname{Gal}(\overline{K}/K) \to \mathbb{F}_p^\times$ that gives the Galois action on $\widetilde{E}[\widetilde{\phi}]$ is easy: $\widetilde{E}[\widetilde{\phi}](\overline{K})$ identifies with $E[\phi](\overline{K})$ with the Galois action twisted by τ, so $\widetilde{\psi} = \psi\tau$.

Proposition 3.6. *One has*

$$(\psi, -1)_L = 1 = (\psi, -1)_K(\widetilde{\psi}, -1)_K(\tau, -1)_K.$$

Proof. To deal with the left hand side one applies Lemma 2.14. The right hand side is taken care of by bilinearity (Section 2.13):

$$(\psi, -1)_K(\widetilde{\psi}, -1)_K(\tau, -1)_K = (\psi, -1)_K^2(\tau, -1)_K^2 = (\psi\tau, 1)_K = 1. \qquad \square$$

3.7. Implications for the l-adic Tate module. The isogeny f_E induces an isomorphism of l-adic Tate modules ($l \neq 2$)

$$V_l(E/K) \oplus V_l(\widetilde{E}/K) \cong V_l((E \times \widetilde{E})/K) \cong V_l((N_{L/K}E)/K) \cong \operatorname{Ind}_L^K V_l(E/L).$$

The last isomorphism is a general property of the restriction of scalars for abelian varieties (use [Mil72, Proposition 6 (b)] together with the formula $(\mathrm{Ind}_L^K \mathbf{1}_L) \otimes V_l(E/K) \cong \mathrm{Ind}_L^K V_l(E/L)$). Of course, this gives an isomorphism of the corresponding Weil–Deligne representations [Roh94, Sections 3, 4, and 13] (take $l \neq 2, \mathrm{char}\, \mathbb{F}_K$)

$$\sigma'_{E/K} \oplus \sigma'_{\widetilde{E}/K} \cong \mathrm{Ind}_L^K \sigma'_{E/L}. \tag{15}$$

Proposition 3.8. *The local L-factors are related by*

$$L(E/K, s)L(\widetilde{E}/K, s) = L(E/L, s).$$

Proof. This follows immediately from (15) and the multiplicativity and inductivity of the L-factor of a Weil–Deligne representation [Roh94, Section 8 and Section 17]. □

3.9. Properties of local root numbers. Let $\eta\colon K \to \mathbb{C}^\times$ be a nontrivial (continuous) additive character and let dx be a Haar measure on $(K, +)$. Let σ' be a Weil–Deligne representation and let $\epsilon(\sigma', \eta, dx)$ be its ϵ-factor (cf. [Roh94]). The *root number* of σ' is

$$w(\sigma', \eta) := \frac{\epsilon(\sigma', \eta, dx)}{|\epsilon(\sigma', \eta, dx)|}.$$

Standard properties of ϵ-factors show (op. cit.) that $w(\sigma', \eta)$ is independent of the choice of dx and is even independent of η if σ' is essentially symplectic, in which case we write $w(\sigma')$. Due to Weil pairing, this is the case for $\sigma'_{E/K}$ associated to an elliptic curve E (op. cit.); by definition $w(E/K) = w(\sigma'_{E/K})$. For use in the proof of Proposition 3.11 we record some basic properties of the root number, all of which follow from analogous properties of the ϵ-factor (op. cit.):

(a) Additivity:
$$w(\sigma'_1 \oplus \sigma'_2, \eta) = w(\sigma'_1, \eta)w(\sigma'_2, \eta).$$

(b) Inductivity in degree zero: if L/K is a finite extension and σ' is a virtual representation of degree 0 of the Weil–Deligne group $\mathcal{W}'(\overline{K}/L)$ of L, then
$$w(\mathrm{Ind}_L^K \sigma', \eta) = w(\sigma', \eta \circ \mathrm{tr}_{L/K}).$$

(c) Determinant formula:
$$w(\sigma', \eta)w(\sigma'^*, \eta) = (\det \sigma)(-1),$$
where σ'^* is the contragredient of σ', σ is the underlying representation of the Weil group $\mathcal{W}(\overline{K}/K)$, and, with the local Artin homomorphism Art_K from Section 2.13, $(\det \sigma)(-1) = \det \sigma \circ \mathrm{Art}_K(-1)$.

In particular, applying (c) to a self-contragredient character such as $\mathbf{1}_K$ or τ we get

$$w(\mathbf{1}_K, \eta)^2 = 1 \quad \text{and} \quad w(\tau, \eta)^2 = \tau(-1) = (\tau, -1)_K. \tag{16}$$

Lemma 3.10. *One has*

$$w(\mathrm{Ind}_L^K \mathbf{1}_L, \eta)^2 = (\tau, -1)_K.$$

Proof. Using decomposition $\operatorname{Ind}_L^K \mathbf{1}_L \cong \mathbf{1}_K \oplus \tau$, we compute

$$\begin{aligned} w(\operatorname{Ind}_L^K \mathbf{1}_L, \eta)^2 &= w(\mathbf{1}_K, \eta)^2 w(\tau, \eta)^2 && \text{by Section 3.9 (a)} \\ &= (\tau, -1)_K && \text{by (16).} \end{aligned}$$

□

Proposition 3.11. *The local root numbers are related by*

$$w(E/L) = w(E/K)w(\widetilde{E}/K)(\tau, -1)_K.$$

Proof. From (15) we get

$$\begin{aligned} w(E/K)w(\widetilde{E}/K) &= w(\operatorname{Ind}_L^K \sigma'_{E/L}, \eta) \\ &= \frac{w(E/L)}{w(\mathbf{1}_L \oplus \mathbf{1}_L, \eta \circ \operatorname{tr}_{L/K})} w(\operatorname{Ind}_L^K (\mathbf{1}_L \oplus \mathbf{1}_L), \eta) && \text{by Section 3.9 (b)} \\ &= w(E/L)w(\operatorname{Ind}_L^K \mathbf{1}_L, \eta)^2 && \text{by (16)} \\ &= w(E/L)(\tau, -1)_K && \text{by Lemma 3.10.} \end{aligned}$$

Since $(\tau, -1)_K \in \{\pm 1\}$, we can carry it to the other side, and the conclusion follows. □

Theorem 3.12. *Fix a prime $p \geq 3$. The p-isogeny conjecture* (7) *is compatible with quadratic twists: in the setup of Section* 2.1 *and Section* 3.1*,*

$$w(E/L) \cdot ((\psi, -1)_K \cdot \sigma_{\phi_K}) \cdot ((\widetilde{\psi}, -1)_K \cdot \sigma_{\widetilde{\phi}_K}) = ((\psi, -1)_L \cdot \sigma_{\phi_L}) \cdot w(E/K) \cdot w(\widetilde{E}/K).$$

In particular, if the p-isogeny conjecture holds for two of $E/K, E/L, \widetilde{E}/K$, then it holds for the third one.

Proof. Combine Propositions 3.4, 3.6 and 3.11. □

Remark 3.13. Note that Theorem 3.12 holds regardless of $\operatorname{char} \mathbb{F}_K$, and in its proof we have not used the case-by-case analysis of the p-isogeny conjecture from Section 2. In particular, it was legitimate to use it in Section 2.11 and Section 2.19.

4. The remaining cases of the p-isogeny conjecture

We have seen in Section 2.22 that the p-isogeny conjecture holds in most cases, including all cases when $\operatorname{char} \mathbb{F}_K \neq p$. In this section we prove it in all of the remaining cases except for Kodaira types III or III*, which are treated in Section 5.

4.1. The restricted setup. Since the p-isogeny conjecture is known in other cases (see Section 2.22), for the rest of the paper we make the following assumptions in addition to those of Section 2.1: the degree of the isogeny is equal to the residue characteristic $\operatorname{char} \mathbb{F}_K = p > 3$, the reduction of E is additive potentially good, and the degree of the residue field extension $f_{K/\mathbb{Q}_p}$ is odd. Let Δ be a minimal discriminant of E. Define Δ' similarly for E'. Since $\operatorname{char} \mathbb{F}_K > 3$ and the reduction is potentially good, we get $v(\Delta) < 12$ (see [Tat75, p. 46]). In fact, $v(\Delta) = 2, 3, 4, 6, 8, 9$, or 10, corresponding to Kodaira types II, III, IV, I_0^*, IV*, III*, or II*, respectively (loc. cit.).

Lemma 4.2. *Suppose that L/K is a finite extension of ramification index $e = e_{L/K}$, and that the degree $f_{L/K}$ of the residue field extension is odd. Write $ev(\Delta) = 12b + a$ with $0 \leq a < 12$, so that $b = \lfloor ev(\Delta)/12 \rfloor$. Define a', b' analogously using Δ'. Then:*

(a) *a and a' are the L-valuations of minimal discriminants of E/L and E'/L, respectively,*

(b) $\sigma_{\phi_L} = \sigma_{\phi_K}^{e} \cdot (-1)^{b+b'}$.

Proof. Choose minimal equations for E/K and E'/K to get associated minimal discriminants Δ and Δ', and Néron minimal differentials ω and ω'. When we pass from K to L, those equations might not be minimal anymore: one may need to make changes of coordinates to arrive at minimal equations over L. When making those changes of coordinates one will have some $u, u' \in L$ for which Δ, Δ' will get multiplied by $u^{-12}, (u')^{-12}$, respectively, and ω, ω' will get multiplied by u, u', respectively [Del75, (1.2) and (1.8)]. Since the reduction will stay potentially good, the L-valuations of new minimal discriminants will be < 12 and will therefore equal a and a', respectively, giving (a). Also, $v_L(u) = b$, $v_L(u') = b'$, and (b) follows from (10) because we are assuming that $f_{K/\mathbb{Q}_p}$ and $f_{L/\mathbb{Q}_p}$ are odd. □

Remark 4.3. The set $\{v(\Delta), v(\Delta')\}$ is a subset of one of the following: $\{2, 10\}$, $\{3, 9\}$, $\{4, 8\}$, or $\{6\}$. This is because E acquires good reduction over an extension L/K if and only if E' does, whereas Lemma 4.2 (a) tells us that the minimal ramification index of an extension over which E acquires good reduction is $\frac{12}{\gcd(v(\Delta),12)}$. Hence, $\gcd(v(\Delta), 12) = \gcd(v(\Delta'), 12)$.

Lemma 4.4. *Let L/K be a ramified quadratic extension and let $\widetilde{E}$ be the corresponding twist of E. Let $\widetilde{\Delta}$ be a minimal discriminant of $\widetilde{E}$. Then $v(\widetilde{\Delta}) \equiv v(\Delta) + 6 \bmod 12$.*

Proof. Since $\operatorname{char} \mathbb{F}_K > 3$ and the reduction of $\widetilde{E}$ is potentially good, we get $v(\widetilde{\Delta}) < 12$ (see [Tat75, p. 46]). But $L = K(\sqrt{\pi_K})$ for some uniformizer $\pi_K \in \mathcal{O}_K$, so the conclusion follows from (13). □

Proposition 4.5. *Under the assumptions of Section* 4.1*, the p-isogeny conjecture* (7) *is true if $v(\Delta) = 6$.*

Proof. Lemma 4.2 (a) shows that E acquires good reduction after a quadratic ramified extension L/K. The corresponding quadratic twist has good reduction by Lemma 4.4. The conclusion then follows from Theorem 3.12 and Section 2.18. □

The following relation between the discriminants of elliptic curves related by a p-isogeny has been communicated to me by Tim Dokchitser:

Theorem 4.6 ([Coa91, Appendix, Theorem 8], [DD12, Theorem 1.1])**.** *Let E and E' be elliptic curves over a field K of characteristic* 0*. Suppose that $\phi\colon E \to E'$ is a p-isogeny with $p > 3$. Let Δ and Δ' be discriminants of some Weierstrass equations for E and E', respectively. Then $\Delta'/\Delta^p \in (K^\times)^{12}$ regardless of the Weierstrass equations chosen.*

Lemma 4.7. *Under the assumptions of Section* 4.1*, suppose that $v(\Delta) = 4$ or $v(\Delta) = 8$. Then $v(\Delta) = v(\Delta')$ if and only if $\#\mathbb{F}_K \equiv 1 \bmod 6$.*

Proof. Theorem 4.6 tells us that $v(\Delta') - p \cdot v(\Delta) \equiv 0 \bmod 12$. Hence, if $v(\Delta) = v(\Delta')$, then $p - 1$ is divisible by 3, so $\#\mathbb{F}_K = p^{f_{K/\mathbb{Q}_p}} \equiv p \equiv 1 \bmod 6$.

Conversely, if $\#\mathbb{F}_K \equiv 1 \bmod 6$, then $p \equiv 1 \bmod 6$, and hence $v(\Delta') \equiv v(\Delta) \bmod 6$, so by Remark 4.3 we must have $v(\Delta) = v(\Delta')$. □

Proposition 4.8. *Under the assumptions of Section* 4.1*, the p-isogeny conjecture* (7) *is true if $v(\Delta) = 4$ or $v(\Delta) = 8$.*

Proof. Choose a cubic totally ramified extension L/K. By Lemma 4.2 (a), E/L has good reduction, so by Section 2.18 it satisfies the p-isogeny conjecture. We check how the terms change when passing from K to L:

(a) We have $(\psi, -1)_L = (\psi, -1)_K$ by Lemma 2.14.

(b) The valuation $v(\Delta)$ is 4 or 8, and Lemma 4.2 implies that b is 1 or 2 accordingly. By Remark 4.3, $v(\Delta')$ also is 4 or 8, so b' is 1 or 2 accordingly. Thus, by Lemma 4.2 (b), one has $\sigma_{\phi_L} \neq \sigma_{\phi_K}$ if and only if $v(\Delta) \neq v(\Delta')$. By Lemma 4.7, this is the case if and only if $\#\mathbb{F}_K \equiv 5 \bmod 6$.

(c) By Theorem 2.2 (e), we have $w(E/L) = 1$, whereas $w(E/K) = 1$ if $\#\mathbb{F}_K \equiv 1 \bmod 6$, and $w(E/K) = -1$ if $\#\mathbb{F}_K \equiv 5 \bmod 6$. Therefore, $w(E/L) \neq w(E/K)$ if and only if $\#\mathbb{F}_K \equiv 5 \bmod 6$.

We conclude that when passing from K to L both sides of (7) change sign if and only if $\#\mathbb{F}_K \equiv 5 \bmod 6$. Since (7) holds for E/L by Section 2.18, it must hold for E/K as well. □

Proposition 4.9. *Under the assumptions of Section* 4.1*, the p-isogeny conjecture* (7) *is true if $v(\Delta) = 2$ or $v(\Delta) = 10$.*

Proof. Choose a quadratic ramified extension L/K. By Lemma 4.2 (a), the valuation of a minimal discriminant of E/L is 4 or 8. By Lemma 4.4, the valuation of a minimal discriminant of the twist $\widetilde{E}$ is 8 or 4. In particular, the p-isogeny conjecture holds for both E/L and $\widetilde{E}/K$ by Proposition 4.8. By Theorem 3.12, it must hold for E as well. □

Remark 4.10. Another way to prove Proposition 4.9 is to choose a ramified cubic extension L/K and check that none of the terms in (7) change when passing from K to L. The argument is similar to that of Lemma 5.1.

5. The case of Kodaira type III or III*

As pointed out in Section 4.1, this is the case when $v(\Delta) = 3$ or $v(\Delta) = 9$. To study it we are going to use the work of Coates, Fukaya, Kato, and Sujatha [CFKS10] that settles the p-isogeny conjecture in many cases. We begin with a lemma that will be useful later in imposing additional assumptions in Lemma 5.4.

Lemma 5.1. *Under the assumptions of Section* 4.1*, suppose that $v(\Delta) = 3$ or $v(\Delta) = 9$ and let L/K be an extension of odd degree. The p-isogeny conjecture* (7) *holds for E/K if and only if it holds for E/L.*

Proof. In fact, none of the terms in (7) change when passing from K to L:

(a) We have $(\psi, -1)_L = (\psi, -1)_K$ by Lemma 2.14.

(b) We have $\sigma_{\phi_L} = \sigma_{\phi_K}$ because in Lemma 4.2 (b) one has $b \equiv b' \bmod 2$. Indeed, by Remark 4.3, $v(\Delta') \in \{3, 9\}$, so one only needs to check that

$$\left\lfloor \frac{3 \cdot e_{L/K}}{12} \right\rfloor \equiv \left\lfloor \frac{9 \cdot e_{L/K}}{12} \right\rfloor \bmod 2,$$

or equivalently that

$$\left\lfloor \frac{e_{L/K}}{4} \right\rfloor \equiv \left\lfloor \frac{3 \cdot e_{L/K}}{4} \right\rfloor \bmod 2.$$

This is confirmed after a short check of possibilities $e_{L/K} \in \{1, 3, 5, 7\} \bmod 8$.

(c) The valuation $v_L(\Delta_L)$ of a minimal discriminant of E/L is in $\{3, 9\}$ by Lemma 4.2 (a). Also, Theorem 2.2 (e) yields

$$w(E/L) = (-1)^{\lfloor v_L(\Delta_L) \cdot \#\mathbb{F}_L/12 \rfloor}.$$

The latter is $(-1)^{\lfloor v_L(\Delta_L) \cdot \#\mathbb{F}_K/12 \rfloor}$, because $\#\mathbb{F}_L \equiv \#\mathbb{F}_K \bmod 8$. Since

$$w(E/K) = (-1)^{\lfloor v(\Delta) \cdot \#\mathbb{F}_K/12 \rfloor},$$

to check that $w(E/L) = w(E/K)$ one needs to check that

$$\left\lfloor \frac{3 \cdot \#\mathbb{F}_K}{12} \right\rfloor \equiv \left\lfloor \frac{9 \cdot \#\mathbb{F}_K}{12} \right\rfloor \bmod 2,$$

which is the same computation as in (b). □

Theorem 5.2 ([CFKS10, Theorem 2.7, Proposition 2.8 (3)]). *Assume the setup of Section* 4.1. *The p-isogeny conjecture* (7) *holds if either E has potentially good ordinary reduction, or E achieves good supersingular reduction over a finite abelian extension of K.*

5.3. Consequences for the case at hand. Assume the setup of Section 4.1 and suppose that $v(\Delta) = 3$ or $v(\Delta) = 9$. Let F/K be a totally ramified extension of degree 4, so E/F has good reduction by Lemma 4.2 (a). If K contains a primitive 4^{th} root of unity, i.e., if $-1 \in \mathbb{F}_K^{\times 2}$, the extension F/K is abelian and we can apply Theorem 5.2 to deduce (7). If $-1 \notin \mathbb{F}_K^{\times 2}$, then $\#\mathbb{F}_K \equiv 3 \bmod 4$, and because of Theorem 5.2 we can assume in addition that E/K is potentially supersingular.

Lemma 5.4. *Under the assumptions of Section* 4.1*, suppose that $v(\Delta) = 3$ or $v(\Delta) = 9$, E/K has potentially supersingular reduction, and $\#\mathbb{F}_K \equiv 3 \bmod 4$. To prove the p-isogeny conjecture* (7) *for E/K it suffices to prove it assuming that $K(E[\phi]) = K$ (without losing other assumptions).*

Proof. Consider the subfield L of K_ψ/K fixed by the 2-Sylow subgroup of $\mathrm{Gal}(K_\psi/K)$. As $\mathrm{Gal}(K_\psi/K)$ is cyclic of order dividing $p - 1$, the degree $[K_\psi : L]$ is at most 2 and $[L : K]$ is odd. Using Lemma 5.1, we replace K by L (we do not lose any assumptions by doing this;

in particular, Lemma 4.2 (a) shows that E/L still has additive reduction of Kodaira type III or III*). If $K_\psi = L$, we are done, so assume that $[K_\psi : K] = 2$. The p-isogeny conjecture is already known for E/K_ψ: if K_ψ/K is unramified, this is Section 2.17, and if it is ramified, this follows from Lemma 4.2 (a) and Proposition 4.5. Using Theorem 3.12 we can therefore replace E by its quadratic twist $\widetilde{E}$ by K_ψ/K (without losing any assumptions). But the Galois action on $\widetilde{E}[\widetilde{\phi}]$ is trivial by construction, so we have reduced to the case $K(E[\phi]) = K$. □

5.5. Assumptions specific to the present case. In view of Section 5.3 and Lemma 5.4, for the rest of the paper we will be assuming in addition to Section 4.1 that $v(\Delta) = 3$ or 9, $\#\mathbb{F}_K \equiv 3 \bmod 4$, the reduction is potentially good supersingular, and $K(E[\phi]) = K$. In this case the Galois closure L of F/K from Section 5.3 is of degree 8 with $e_{L/K} = 4$, $f_{L/K} = 2$. Also, Lemma 4.2 (a) shows that E/L has good supersingular reduction. We set $G = \mathrm{Gal}(L/K)$ and let $I \lhd G$ be the index 2 inertia subgroup. The subfield of L/K fixed by I is denoted by M.

The assumption $K(E[\phi]) = K$ gives in particular that $(\psi, -1)_K = 1$, so (7) in this case is

$$w(E/K) \stackrel{?}{=} \sigma_{\phi_K}. \tag{17}$$

5.6. A convenient Weierstrass equation. Assume the setup of Section 5.5 and pick a minimal Weierstrass equation for E/K with associated quantities $a_1, a_2, \ldots, c_4, c_6, \Delta$ and $j = c_4^3/\Delta$ (cf. [Tat75, Section 1]). Then

$$y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$$

is another minimal equation for E/K since it has integral coefficients and the same valuation of the discriminant (we are assuming $p > 3$) [Tat75, (1.7)]. If one considers it as an equation for E/L, it is no longer minimal but after a change of coordinates

$$x = u^2 X,$$
$$y = u^3 Y,$$

with $u = \pi_L^{v(\Delta)/3}$ one arrives at a minimal equation

$$Y^2 = X^3 - \frac{c_4}{48u^4}X - \frac{c_6}{864u^6} \tag{18}$$

for E/L. Indeed, its discriminant has valuation 0 and it has integral coefficients because the relations $3v(c_4) \geq v(\Delta)$ (i.e., $v(j) \geq 0$) and $1728\Delta = c_4^3 - c_6^2$ show that $v(c_4) \geq v(\Delta)/3$ and $v(c_6) \geq v(\Delta)/2$.

5.7. The formal group of E/L. With the choice of a minimal equation (18),

$$T = -X/Y$$

is a parameter for the formal group $\mathcal{F}$ of E/L. Similarly, $t = -x/y$ is a parameter for the formal group of E/K, and

$$T = ut. \tag{19}$$

Since E/L has good supersingular reduction, it follows that $\mathcal{F}$ is of height 2. In other words, in $[p]_{\mathcal{F}}(T) = pT + V_2T^2 \cdots + V_pT^p + \cdots + V_{p^2}T^{p^2} + \cdots$ the first coefficient which is a unit is V_{p^2}. Let $\mathfrak{m}_0^+ \subset \overline{K}$ consist of all elements of positive valuation after uniquely extending v to $\overline{K}$ (see also Section 5.22). The $\mathrm{Gal}(\overline{K}/L)$-module $E[p]$ is isomorphic to the kernel $N_p \subset \mathfrak{m}_0^+$ of $[p]_{\mathcal{F}}$ via the map $T(P) = -X(P)/Y(P)$ (one puts $T(O) = 0$).

Lemma 5.8. *The L-valuation of a nonzero $\beta \in T(E[\phi])$ is an odd integer independent of β.*

Proof. For a nonzero $P \in E[\phi]$, (19) shows that

$$v_L(T(P)) = v_L(t(P)) + v_L(u) = 4 \cdot v(t(P)) + \frac{v(\Delta)}{3}$$

is an odd integer, because $v(t(P))$ is an integer due to our assumption that $E[\phi] \subset E(K)$. But since $E[\phi]$ and $T(E[\phi])$ are cyclic of order p, and the formal group law is

$$T_1 + T_2 + \text{higher order terms},$$

all nonzero elements of $T(E[\phi])$ have the same valuation. □

5.9. The actions of G. Let $\mathcal{E}/\mathcal{O}_L$ be the Néron model of E/L, and let $\mathcal{E}'/\mathcal{O}_L$ be that of E'/L. For each $\sigma \in G = \mathrm{Gal}(L/K)$ we have a commutative diagram

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{\sigma} & \mathcal{E} \\ \downarrow & & \downarrow \\ \operatorname{Spec} \mathcal{O}_L & \xrightarrow{\sigma} & \operatorname{Spec} \mathcal{O}_L. \end{array} \tag{20}$$

Here $\sigma\colon \operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathcal{O}_L$ is a morphism corresponding to $\mathcal{O}_L \xrightarrow{\sigma^{-1}} \mathcal{O}_L$ and $\sigma\colon \mathcal{E} \to \mathcal{E}$ is the unique morphism making the square commute, obtained by invoking the Néron property. Uniqueness gives us actions of G on both $\operatorname{Spec} \mathcal{O}_L$ and $\mathcal{E}$ which are compatible with the morphism $\mathcal{E} \to \operatorname{Spec} \mathcal{O}_L$. Analogous statements are true for $\mathcal{E}'/\mathcal{O}_L$.

Since $\mathcal{E}/\mathcal{O}_L$ is an abelian scheme, [BLR90, Section 7.3, Proposition 6] shows that the isogeny $\phi\colon E \to E'$ extends to an isogeny $\phi\colon \mathcal{E} \to \mathcal{E}'$, whose kernel is a finite flat commutative $\mathcal{O}_L$-group scheme $\mathcal{E}[\phi]$ of order p with generic fiber $\mathcal{E}[\phi]_L = E[\phi]_L$. The diagram (20) being functorial, we get an action of G on $\mathcal{E}[\phi]$ which is compatible with its action on $\operatorname{Spec} \mathcal{O}_L$. Restricting this action to I and reducing to the special fiber $\mathcal{E}[\phi]_{\mathbb{F}_L}$, we get an action of I on $\mathcal{E}[\phi]_{\mathbb{F}_L}$ preserving the morphism to $\operatorname{Spec} \mathbb{F}_L$.

Following [CFKS10, Remark after Lemma 2.20] we define the $\mathcal{O}_L/p\mathcal{O}_L$-module (or the $\mathcal{O}_L$-module):

$$\mathrm{Lie}(\mathcal{E}[\phi]) := \mathrm{Ker}(\mathcal{E}[\phi]((\mathcal{O}_L/p\mathcal{O}_L)[\epsilon]/(\epsilon^2)) \to \mathcal{E}[\phi](\mathcal{O}_L/p\mathcal{O}_L)). \tag{21}$$

(One could more accurately call this $\mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_L/p\mathcal{O}_L})$.) The action of G on $\mathcal{E}[\phi]$ gives an $\mathcal{O}_L$-semilinear action of G on $\mathrm{Lie}(\mathcal{E}[\phi])$.

Since E/L is a base change of E/K, one also has an action of G on $E(L) \cong \mathcal{E}(\mathcal{O}_L)$ for which ϕ_L is G-equivariant, being defined over K. Let $\phi_{\mathcal{O}_L}\colon \mathcal{E}(\mathcal{O}_L) \to \mathcal{E}'(\mathcal{O}_L)$ be the map induced by $\phi\colon \mathcal{E} \to \mathcal{E}'$ on $\mathcal{O}_L$-points; it is G-equivariant as well. Since $E(L)^G = E(K)$, and similarly for E', we get

$$\chi(\phi_K) = \chi(\mathcal{E}(\mathcal{O}_L)^G \xrightarrow{\phi_{\mathcal{O}_L}} \mathcal{E}'(\mathcal{O}_L)^G). \tag{22}$$

Theorem 5.10 ([TO70, pp. 14–16, Remarks 1 and 5]). *Let A be $\mathcal{O}_L$, L, $\mathbb{F}_L$, or $\overline{\mathbb{F}}_L$. There is a bijective correspondence between isomorphism classes of finite flat group schemes G of order p over A and equivalence classes of factorizations $p = ac$ with $a, c \in A$, where $p = ac$ and $p = a'c'$ are said to be equivalent if there is a $u \in A^\times$ such that $a' = u^{p-1}a$ and $c' = u^{1-p}c$. As an A-scheme, the group scheme corresponding to $p = ac$ is isomorphic to* $\operatorname{Spec} A[s]/(s^p - as)$ *(c appears in the description of the group law).*

Remark 5.11. Theorem 5.10 is part of a more general Oort–Tate classification of finite flat group schemes of order p, cf. [TO70]. The version stated here will be sufficient for our purposes. In Theorem 5.10 the factorization corresponding to the constant group scheme $\underline{\mathbb{Z}/p\mathbb{Z}}$ is $p = 1 \cdot p$ (see [TO70, pp. 8–10 and Remarks on pp. 14–15]). (With our choices for $\underline{A}$, this can also be seen from Theorem 5.10 directly, because if $\operatorname{Spec} A[s]/(s^p - as)$ has a nontrivial A-point, then $a = u^{p-1}$ for some $u \in A$, $u \neq 0$.)

Lemma 5.12. *As finite $\mathbb{F}_L$-group schemes, $\mathcal{E}[\phi]_{\mathbb{F}_L} \cong \alpha_p$. Its corresponding factorization is $p = 0 \cdot 0$.*

Proof. The kernel of a p-isogeny between supersingular elliptic curves in characteristic p is local-local. Therefore, one has $\mathcal{E}[\phi]_{\mathbb{F}_L} \cong \alpha_p$, because α_p has no twists and is the only local-local group scheme of order p over $\overline{\mathbb{F}}_L$. Also, α_p is isomorphic to its own Cartier dual, so the second claim follows, because by [TO70, p. 15, Remark 2] in characteristic p Cartier duality has the effect $ac \leftrightarrow (-c)(-a)$. □

5.13. The kernel of $\phi\colon \mathcal{E} \to \mathcal{E}'$ as a scheme. Let $p = ac$ with $a, c \in \mathcal{O}_L$ be a factorization corresponding to $\mathcal{E}[\phi]$. Since $\mathcal{E}[\phi]_L \cong E[\phi]_L$ is the constant group scheme, it follows from Remark 5.11 that its corresponding factorization is $p = 1 \cdot c_0$. Theorem 5.10 therefore gives $a = a_0^{p-1}$ for some $a_0 \in \mathcal{O}_L$. Moreover, by Lemma 5.12 the factorization of $\mathcal{E}[\phi]_{\mathbb{F}_L}$ is $p = 0 \cdot 0$. We conclude that a_0 and c are of positive valuation, and as a scheme $\mathcal{E}[\phi]$ is isomorphic to $\operatorname{Spec} \mathcal{O}_L[s]/(s^p - a_0^{p-1}s)$ with $0 < v_L(a_0) < v_L(p)/(p-1)$.

Lemma 5.14. *We have* $\operatorname{length}_{\mathcal{O}_L} \operatorname{Lie}(\mathcal{E}[\phi]) = (p-1)v_L(a_0)$.

Proof. Interpreting (21) on rings, $\operatorname{Lie}(\mathcal{E}[\phi])$ consists of $\mathcal{O}_L$-algebra homomorphisms

$$\mathcal{O}_L[s]/(s^p - a_0^{p-1}s) \to (\mathcal{O}_L/p\mathcal{O}_L)[\epsilon]/(\epsilon^2)$$

whose composite with

$$\begin{aligned}(\mathcal{O}_L/p\mathcal{O}_L)[\epsilon]/(\epsilon^2) &\to \mathcal{O}_L/p\mathcal{O}_L,\\ \epsilon &\mapsto 0,\end{aligned}$$

sends s to 0. Such are given by $s \mapsto b\epsilon$ with $a_0^{p-1}b = 0$, or equivalently with

$$b \in \pi_L^{v_L(p)-(p-1)v_L(a_0)}\mathcal{O}_L/\pi_F^{v_L(p)}\mathcal{O}_L.$$ □

Lemma 5.15. *For any nonzero element $\beta \in T(E[\phi])$,*

$$v_L(a_0) = v_L(\beta)$$

(cf. Lemma 5.8*).*

Proof. One way to define the filtration $E_1(L) \supset \cdots \supset E_m(L) \supset \cdots$ discussed in Section 2.9 is as follows (cf. [LS10, Lemma 5.1]): for $z \in E_1(L)$ let $S_z = \overline{\{z\}}$ be the closure of z in $\mathcal{E}$; if $z \neq 0$, then $S_0 \cap S_z$ is a local Artin scheme, whose length we denote by $l(z)$; now let $E_m(L)$ consist of all $z \in E_1(L)$ with $l(z) \geq m$ (one sets $l(0) = \infty$).

One nonzero L-point of the group scheme $\mathcal{E}[\phi]$ is $s \mapsto a_0$, its closure in $\mathcal{E}[\phi]$ (and hence $\mathcal{E}$) is $\operatorname{Spec} \mathcal{O}_L[s]/(s - a_0)$, the intersection with the zero section is $\operatorname{Spec} \mathcal{O}_L[s]/(s, s - a_0)$, and the length of this local Artin scheme is $v_L(a_0)$. On the other hand, every nonzero point of $E[\phi]_L$ belongs to the filtration level $v_L(\beta)$ by definition. □

Lemma 5.16. *If N is a finite length $\mathcal{O}_M$-module equipped with an $\mathcal{O}_M$-semilinear action of G/I, then*

$$\operatorname{length}_{\mathcal{O}_K} N^{G/I} = \operatorname{length}_{\mathcal{O}_M} N.$$

Proof. This is clear if $N = \mathbb{F}_M \times \cdots \times \mathbb{F}_M$ by classical Galois descent for vector spaces. The general case follows by induction on the number of nonzero terms in the (G/I)-stable filtration $N \supset \pi_K N \supset \pi_K^2 N \supset \cdots$ using Hilbert's Theorem 90. □

Corollary 5.17. *One has*

$$\operatorname{length}_{\mathcal{O}_K} \operatorname{Lie}(\mathcal{E}[\phi])^G = \operatorname{length}_{\mathcal{O}_M} \operatorname{Lie}(\mathcal{E}[\phi])^I.$$

Proof. Observe that both lengths are finite by Lemma 5.14 and apply Lemma 5.16 with $N = \operatorname{Lie}(\mathcal{E}[\phi])^I$. □

Lemma 5.18. *One has*

$$\operatorname{ord}_p \chi(\phi_K) \equiv \operatorname{ord}_p \#(\operatorname{Lie}(\mathcal{E}[\phi])^G) \equiv \operatorname{length}_{\mathcal{O}_M} \operatorname{Lie}(\mathcal{E}[\phi])^I \bmod 2.$$

Proof. The second congruence holds because $f_{K/\mathbb{Q}_p}$ is assumed to be odd: indeed, by Corollary 5.17,

$$\operatorname{ord}_p \#(\operatorname{Lie}(\mathcal{E}[\phi])^G) = f_{K/\mathbb{Q}_p} \operatorname{length}_{\mathcal{O}_K} \operatorname{Lie}(\mathcal{E}[\phi])^G \equiv \operatorname{length}_{\mathcal{O}_M} \operatorname{Lie}(\mathcal{E}[\phi])^I \bmod 2.$$

The first congruence is [CFKS10, Lemma 2.20 (4) and (5)] together with (22). The proof given there does not use the assumption (iii) of [CFKS10, Theorem 2.1] and therefore extends to the situation considered here. We recall the argument of op. cit. below.

Let $\mathcal{E}_{\mathbb{F}_L}$ and $\mathcal{E}'_{\mathbb{F}_L}$ denote the reductions of E/L and E'/L.

Claim 5.18.1. *One has*

$$\chi(\phi_K) = \frac{\#\mathcal{E}'(\mathbb{F}_L)^G}{\#\mathcal{E}(\mathbb{F}_L)^G} \cdot \frac{\#(\operatorname{Lie} \mathcal{E}_{\mathbb{F}_L})^G}{\#(\operatorname{Lie} \mathcal{E}'_{\mathbb{F}_L})^G} \cdot \chi\big(\operatorname{Lie}(\mathcal{E})^G \xrightarrow{\operatorname{Lie}(\phi)} \operatorname{Lie}(\mathcal{E}')^G\big).$$

Proof. Let $\mathfrak{m}_L \subset \mathcal{O}_L$ be the maximal ideal and choose a large $n \in \mathbb{Z}_{>0}$ such that the G-equivariant

$$\mathfrak{m}_L^n \operatorname{Lie} \mathcal{E} \to \operatorname{Ker}\big(\mathcal{E}(\mathcal{O}_L) \xrightarrow{r} \mathcal{E}(\mathcal{O}_L/\mathfrak{m}_L^n)\big)$$

and

$$\mathfrak{m}_L^n \operatorname{Lie} \mathcal{E}' \to \operatorname{Ker}\big(\mathcal{E}'(\mathcal{O}_L) \xrightarrow{r'} \mathcal{E}'(\mathcal{O}_L/\mathfrak{m}_L^n)\big)$$

induced by the exponential maps of $\mathcal{E}$ and $\mathcal{E}'$ are isomorphisms. By Hensel's lemma, r and r' are surjective, so [Ser67, Section 1.2, Lemma 3] and the coprimality of $\#G$ and p ensure the exactness of

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (\mathfrak{m}_L^n \operatorname{Lie} \mathcal{E})^G & \longrightarrow & \mathcal{E}(\mathcal{O}_L)^G & \xrightarrow{r} & \mathcal{E}(\mathcal{O}_L/\mathfrak{m}_L^n)^G & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \phi_{\mathcal{O}_L}} & & \downarrow & & \\ 0 & \longrightarrow & (\mathfrak{m}_L^n \operatorname{Lie} \mathcal{E}')^G & \longrightarrow & \mathcal{E}'(\mathcal{O}_L)^G & \xrightarrow{r'} & \mathcal{E}'(\mathcal{O}_L/\mathfrak{m}_L^n)^G & \longrightarrow & 0 \end{array}$$

in spite of the presence of G-invariants. Therefore, (22) together with Propositions 2.6 and 2.7 give

$$\chi(\phi_K) = \frac{\#\mathcal{E}'(\mathcal{O}_L/\mathfrak{m}_L^n)^G}{\#\mathcal{E}(\mathcal{O}_L/\mathfrak{m}_L^n)^G} \cdot \frac{\#(\operatorname{Lie}\mathcal{E}/\mathfrak{m}_L^n \operatorname{Lie}\mathcal{E})^G}{\#(\operatorname{Lie}\mathcal{E}'/\mathfrak{m}_L^n \operatorname{Lie}\mathcal{E}')^G} \cdot \chi\big(\operatorname{Lie}(\mathcal{E})^G \xrightarrow{\operatorname{Lie}(\phi)} \operatorname{Lie}(\mathcal{E}')^G\big).$$

To conclude it remains to argue that one has G-equivariant isomorphisms

$$\operatorname{Ker}\big(\mathcal{E}(\mathcal{O}_L/\mathfrak{m}_L^{i+1}) \to \mathcal{E}(\mathcal{O}_L/\mathfrak{m}_L^i)\big) \cong \frac{\mathfrak{m}_L^i \operatorname{Lie}\mathcal{E}}{\mathfrak{m}_L^{i+1} \operatorname{Lie}\mathcal{E}} \quad \text{for } i \geq 1, \text{ and similarly for } \mathcal{E}'.$$

These are supplied by deformation theory: e.g., invoke [Ill05, Theorem 8.5.9 (a) and (the analogue of) Remark 8.5.10 (b)] and use the zero lift to get a canonical trivialization of the appearing torsor. □

Claim 5.18.2. *One has*

$$\#(\operatorname{Lie}\mathcal{E}_{\mathbb{F}_L})^G = \#(\operatorname{Lie}\mathcal{E}'_{\mathbb{F}_L})^G.$$

Proof. Let D be the covariant Dieudonné module of the p-divisible group of $\mathcal{E}_{\mathbb{F}_L}$, let V be the Verschiebung operator of D, and let D' and V' be the corresponding objects for $\mathcal{E}'_{\mathbb{F}_L}$. The G-equivariant isomorphism $\operatorname{Lie}\mathcal{E}_{\mathbb{F}_L} \cong D/VD$ and [Ser67, Section 1.2, Lemma 3] give

$$(\operatorname{Lie}\mathcal{E}_{\mathbb{F}_L})^G \cong D^G/VD^G.$$

Consequently, since D^G is a free $\mathbb{Z}_p$-module of finite rank and V is $\mathbb{Z}_p$-linear,

$$\#(\operatorname{Lie}\mathcal{E}_{\mathbb{F}_L})^G = \det(V \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \colon D^G \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to D^G \otimes_{\mathbb{Z}_p} \mathbb{Q}_p). \tag{23}$$

It remains to note that $D^G \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong (D \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^G$, so the right hand side of (23) is the same for $\mathcal{E}'_{\mathbb{F}_L}$ because ϕ induces a G-isomorphism

$$(D \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, V \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \cong (D' \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, V' \otimes_{\mathbb{Z}_p} \mathbb{Q}_p).$$ □

Claim 5.18.3. *One has*

$$\operatorname{ord}_p \#\mathcal{E}(\mathbb{F}_L)^G = \operatorname{ord}_p \#\mathcal{E}'(\mathbb{F}_L)^G.$$

Proof. Since the action of the inertia $I \lhd G$ preserves the morphism $\mathcal{E}_{\mathbb{F}_L} \to \operatorname{Spec}\mathbb{F}_L$, the subgroup $(\mathcal{E}(\overline{\mathbb{F}}_L)[p^\infty])^I \subset \mathcal{E}(\overline{\mathbb{F}}_L)[p^\infty]$ is $\operatorname{Gal}(\overline{\mathbb{F}}_L/\mathbb{F}_L)$-stable. Let $\operatorname{Frob}_K \in \operatorname{Gal}(\overline{K}/K)$ be a geometric Frobenius. On the one hand, the action of Frob_K on $(\mathcal{E}(\overline{\mathbb{F}}_L)[p^\infty])^I$ lifts the action of the generator of G/I. On the other hand, the action of Frob_K^2 is that of the geometric Frobenius in $\operatorname{Gal}(\overline{\mathbb{F}}_L/\mathbb{F}_L)$. In conclusion,

$$\mathcal{E}(\mathbb{F}_L)^G[p^\infty] = \operatorname{Ker}\big(1 - \operatorname{Frob}_K \colon (\mathcal{E}(\overline{\mathbb{F}}_L)[p^\infty])^I \to (\mathcal{E}(\overline{\mathbb{F}}_L)[p^\infty])^I\big).$$

Since $(\mathcal{E}(\overline{\mathbb{F}}_L)[p^\infty])^I \subset \mathcal{E}(\overline{\mathbb{F}}_L)[p^\infty]$ is cut out by an idempotent of $\mathbb{Z}_p[I]$, it inherits p-divisibility. Set $T_p := \varprojlim(\mathcal{E}(\overline{\mathbb{F}}_L)[p^n])^I$ and $V_p := T_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Since $\mathcal{E}(\mathbb{F}_L)^G$ is finite, $1 - \mathrm{Frob}_K$ is injective on T_p, and hence also on V_p. Consequently, the snake lemma applied to

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_p & \longrightarrow & V_p & \longrightarrow & (\mathcal{E}(\overline{\mathbb{F}}_L)[p^\infty])^I & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1-\mathrm{Frob}_K} & & \downarrow{\scriptstyle 1-\mathrm{Frob}_K} & & \downarrow{\scriptstyle 1-\mathrm{Frob}_K} & & \\ 0 & \longrightarrow & T_p & \longrightarrow & V_p & \longrightarrow & (\mathcal{E}(\overline{\mathbb{F}}_L)[p^\infty])^I & \longrightarrow & 0 \end{array}$$

gives the first equality in

$$\mathrm{ord}_p \#\mathcal{E}(\mathbb{F}_L)^G = \mathrm{ord}_p \#\left(\frac{T_p}{(1-\mathrm{Frob}_K)T_p}\right) = \mathrm{ord}_p \det(1 - \mathrm{Frob}_K \colon V_p \to V_p). \tag{24}$$

The claim follows from (24): indeed, similar reasoning applies to $\mathcal{E}'$, so, denoting by V_p' the analogue of V_p, one notes that ϕ induces a Frob_K-equivariant isomorphism $V_p \cong V_p'$. □

Claim 5.18.4. *One has*

$$\begin{aligned} \chi\big(\mathrm{Lie}(\mathcal{E})^G \xrightarrow{\mathrm{Lie}(\phi)} \mathrm{Lie}(\mathcal{E}')^G\big) &= \#\,\mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_L/p\mathcal{O}_L})^G \\ &= \#(\mathrm{Lie}(\mathcal{E}[\phi])^G) \qquad \textit{by Section } 5.9. \end{aligned}$$

Proof. The Lie algebras $\mathrm{Lie}(\mathcal{E})$ and $\mathrm{Lie}(\mathcal{E}')$ are free $\mathcal{O}_L$-modules of rank 1. Consideration of the isogeny dual to ϕ shows that

$$\mathrm{Lie}(\mathcal{E}) \xrightarrow{\mathrm{Lie}(\phi)} \mathrm{Lie}(\mathcal{E}')$$

is injective and its cokernel Q is killed by p.

Consider the short exact sequence

$$0 \to \mathcal{E}[\phi]_{\mathcal{O}_L/p\mathcal{O}_L} \to \mathcal{E}_{\mathcal{O}_L/p\mathcal{O}_L} \to \mathcal{E}'_{\mathcal{O}_L/p\mathcal{O}_L} \to 0 \tag{25}$$

of $\mathcal{O}_L/p\mathcal{O}_L$-group schemes. Forming Lie algebras commutes with base change, so (25) gives the exact

$$0 \to \mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_L/p\mathcal{O}_L}) \to \mathrm{Lie}(\mathcal{E}) \otimes_{\mathcal{O}_L} \mathcal{O}_L/p\mathcal{O}_L \xrightarrow{\mathrm{Lie}(\phi)\otimes_{\mathcal{O}_L}\mathcal{O}_L/p\mathcal{O}_L} \mathrm{Lie}(\mathcal{E}') \otimes_{\mathcal{O}_L} \mathcal{O}_L/p\mathcal{O}_L.$$

Consequently, the snake lemma applied to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Lie}(\mathcal{E}) & \xrightarrow{\mathrm{Lie}(\phi)} & \mathrm{Lie}(\mathcal{E}') & \longrightarrow & Q & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle 0} & & \\ 0 & \longrightarrow & \mathrm{Lie}(\mathcal{E}) & \xrightarrow{\mathrm{Lie}(\phi)} & \mathrm{Lie}(\mathcal{E}') & \longrightarrow & Q & \longrightarrow & 0 \end{array}$$

of G-modules gives $Q \cong \mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_L/p\mathcal{O}_L})$. Since $(\#G, p) = 1$, the resulting

$$0 \to \mathrm{Lie}(\mathcal{E}) \xrightarrow{\mathrm{Lie}(\phi)} \mathrm{Lie}(\mathcal{E}') \to \mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_L/p\mathcal{O}_L}) \to 0$$

remains short exact after taking G-invariants, and the desired conclusion follows. □

In conclusion, Claims 5.18.1 to 5.18.4 provide an equality underlying the first congruence of Lemma 5.18. □

5.19. Vector space structures. Let $M_0 := \widehat{M^{\mathrm{ur}}}$ be the completion of the maximal unramified extension of M, and let and L_0 be a compositum of M_0 and L. The field L_0 is complete, and L_0/M_0 is Galois with Galois group identified with I. In particular, $[L_0 : M_0] = 4$. The rings of integers of L_0 and M_0 will be denoted by $\mathcal{O}_{L_0}$ and $\mathcal{O}_{M_0}$.

As observed in Section 5.9, I acts on $\mathcal{E}[\phi]$ compatibly with its action on $\operatorname{Spec} \mathcal{O}_L$. With the identification above, I therefore acts on $\mathcal{E}[\phi]_{\mathcal{O}_{L_0}}$ compatibly with its action on $\operatorname{Spec} \mathcal{O}_{L_0}$, and we get an $\mathcal{O}_{L_0}$-semilinear action of I on $\operatorname{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}}) \cong \operatorname{Lie}(\mathcal{E}[\phi]) \otimes_{\mathcal{O}_L} \mathcal{O}_{L_0}$.

By definition, $\operatorname{Lie}(\mathcal{E}[\phi])$ is an $\mathcal{O}_L/p\mathcal{O}_L$-module. In particular, denoting by $W(\mathbb{F}_L)$ the ring of Witt vectors, we can regard $\operatorname{Lie}(\mathcal{E}[\phi])$ as a vector space over

$$\mathbb{F}_L \cong W(\mathbb{F}_L)/pW(\mathbb{F}_L) \subset \mathcal{O}_L/p\mathcal{O}_L$$

equipped with an $\mathbb{F}_L$-linear action of I. In other words, $\operatorname{Lie}(\mathcal{E}[\phi])$ is a finite-dimensional $\mathbb{F}_L$-representation of I with

$$\operatorname{length}_{\mathcal{O}_L} \operatorname{Lie}(\mathcal{E}[\phi]) = \dim_{\mathbb{F}_L} \operatorname{Lie}(\mathcal{E}[\phi]), \tag{26}$$

and also

$$\operatorname{length}_{\mathcal{O}_M} \operatorname{Lie}(\mathcal{E}[\phi])^I = \dim_{\mathbb{F}_L} \operatorname{Lie}(\mathcal{E}[\phi])^I. \tag{27}$$

On the other hand,

$$\operatorname{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}}) \cong \operatorname{Lie}(\mathcal{E}[\phi]) \otimes_{\mathbb{F}_L} \overline{\mathbb{F}}_L,$$

and also

$$\operatorname{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}})^I \cong \operatorname{Lie}(\mathcal{E}[\phi])^I \otimes_{\mathbb{F}_L} \overline{\mathbb{F}}_L.$$

Therefore

$$\operatorname{length}_{\mathcal{O}_L} \operatorname{Lie}(\mathcal{E}[\phi]) \overset{(26)}{=} \dim_{\mathbb{F}_L} \operatorname{Lie}(\mathcal{E}[\phi]) = \dim_{\overline{\mathbb{F}}_L} \operatorname{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}}), \tag{28}$$

and also

$$\operatorname{length}_{\mathcal{O}_M} \operatorname{Lie}(\mathcal{E}[\phi])^I \overset{(27)}{=} \dim_{\mathbb{F}_L} \operatorname{Lie}(\mathcal{E}[\phi])^I = \dim_{\overline{\mathbb{F}}_L} \operatorname{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}})^I. \tag{29}$$

Corollary 5.20. *One has*

$$\operatorname{ord}_p \chi(\phi_K) \equiv \dim_{\overline{\mathbb{F}}_L} \operatorname{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}})^I \bmod 2.$$

Proof. Combine Lemma 5.18 and (29). □

5.21. The Dieudonné module of the special fiber. The special fiber of $\mathcal{E}[\phi]_{\mathcal{O}_{L_0}}$ is $\mathcal{E}[\phi]_{\overline{\mathbb{F}}_L}$, which by Section 5.9 carries the action of I preserving the morphism to $\operatorname{Spec} \overline{\mathbb{F}}_L$. By Lemma 5.12, $\mathcal{E}[\phi]_{\overline{\mathbb{F}}_L} \cong \alpha_p$, so the (covariant) Dieudonné module $D(\mathcal{E}[\phi]_{\overline{\mathbb{F}}_L}) \cong D(\alpha_p)$ is especially easy to describe:

$$D(\mathcal{E}[\phi]_{\overline{\mathbb{F}}_L}) \cong \overline{\mathbb{F}}_L$$

with vanishing Frobenius and Verschiebung. By functoriality, $D(\mathcal{E}[\phi]_{\overline{\mathbb{F}}_L})$ is an $\overline{\mathbb{F}}_L$-representation of I. The latter is cyclic of order 4, so it acts on $D(\mathcal{E}[\phi]_{\overline{\mathbb{F}}_L})$ via scaling by some 4^{th} roots of unity.

5.22. $\overline{\mathbb{F}}_M$-representations of inertia. Let $I_M \lhd \mathrm{Gal}(\overline{K}/M)$ be the inertia subgroup, and let $P_M \lhd I_M$ be the wild inertia. We are interested in continuous irreducible $\overline{\mathbb{F}}_M$-representations V of I_M. Since $\mathrm{char}\,\overline{\mathbb{F}}_M = p$, and P_M is pro-p, one has $V^{P_M} \neq 0$ (see [Ser77, Proposition 26]). Moreover, P_M is normal in I_M, so V^{P_M} is I_M-stable, hence $V^{P_M} = V$. In other words, V is the inflation of a continuous irreducible representation of the tame inertia I_M/P_M. Tame inertia is abelian, so V is 1-dimensional; it must, therefore, be isomorphic to some V_a, $a \in \mathbb{Q}$, constructed as follows (cf. [Ser72, Sections 1.7–1.8]). The valuation v on K extends uniquely to a (no longer discrete) valuation on $\overline{K}$, which we continue to denote v. Let $\mathfrak{m}_a$ be the set of $x \in \overline{K}$ with valuation $v(x) \geq a$. Let $\mathfrak{m}_a^+ \subset \mathfrak{m}_a$ be the set of $x \in \overline{K}$ with $v(x) > a$. The quotient $\mathfrak{m}_a/\mathfrak{m}_a^+$ is a 1-dimensional $\mathfrak{m}_0/\mathfrak{m}_0^+ \cong \overline{\mathbb{F}}_M$-linear representation of I_M, which we call V_a. In addition, $V_a \cong V_b$ if and only if $a - b \in \mathbb{Z}[1/p]$ (loc. cit.), and we conclude that the Grothendieck group of continuous $\overline{\mathbb{F}}_M$-representations of I_M is isomorphic to the group ring $R := \mathbb{Z}[\mathbb{Q}/\mathbb{Z}[1/p]]$. Multiplication in R corresponds to tensor product of representations (loc. cit.).

In fact, since I_M identifies with $\mathrm{Gal}(\overline{M_0}/M_0)$, we can think of R as the Grothendieck group of continuous $\overline{\mathbb{F}}_M$-linear representations of $\mathrm{Gal}(\overline{M_0}/M_0)$. The representations that will interest us most are $\mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}})$ and $D(\mathcal{E}[\phi]_{\overline{\mathbb{F}}_L})$; they factor through the finite quotient $\mathrm{Gal}(\overline{M_0}/M_0)/\mathrm{Gal}(\overline{M_0}/L_0) = I$ of order 4.

5.23. Maps related to R. Following [CFKS10, Section 7.2] let us supplement the ring

$$R = \mathbb{Z}[\mathbb{Q}/\mathbb{Z}[1/p]]$$

of Section 5.22 with

(a) the notation $\gamma(a)$ for the standard $\mathbb{Z}$-basis element of R corresponding to $a \in \mathbb{Q}/\mathbb{Z}[1/p]$,

(b) the automorphism $\varphi\colon R \to R$ induced by sending $\gamma(a)$ to $\gamma(pa)$,

(c) the $\mathbb{Z}$-linear map $\alpha\colon R \to \mathbb{Q}/\mathbb{Z}[1/p]$ which sends $\gamma(a)$ to a,

(d) the $\mathbb{Z}$-linear map $\widetilde{\alpha}\colon R \to \mathbb{Q}$ defined by sending $\gamma(a)$ to the unique element of $\mathbb{Z}_{(p)} \cap (0, 1]$ whose class mod $\mathbb{Z}[1/p]$ is a,

(e) the $\mathbb{Z}$-linear map $\delta_0\colon R \to \mathbb{Z}$ such that $\delta_0(\gamma(0)) = 1$ and $\delta_0(\gamma(a)) = 0$ for $a \neq 0$,

(f) the $\mathbb{Z}$-linear map $\deg\colon R \to \mathbb{Z}$ which sends each $\gamma(a)$ to 1.

Thinking in terms of representations of $\mathrm{Gal}(\overline{M_0}/M_0)$, one observes that deg (resp., δ_0) is nothing else than the $\overline{\mathbb{F}}_M$-dimension of the representation space (resp., the fixed subspace).

Proposition 5.24. *Denoting by $[V]$ the class in the ring R of an $\overline{\mathbb{F}}_M$-representation V of $\mathrm{Gal}(\overline{M_0}/M_0)$, we have the following relations:*

(a)
$$\widetilde{\alpha}(\varphi^{-1}([D(\mathcal{E}[\phi]_{\overline{\mathbb{F}}_L})])) - \widetilde{\alpha}([D(\mathcal{E}[\phi]_{\overline{\mathbb{F}}_L})]) = \frac{\deg([\mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}})])}{4} - \delta_0([\mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}})]) \quad \text{in } \mathbb{Q}$$

and

(b)
$$-\alpha([D(\mathcal{E}[\phi]_{\overline{\mathbb{F}}_L})]) = \frac{p \cdot \deg([\mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}})])}{4(p-1)} \quad \text{in } \mathbb{Q}/\mathbb{Z}[1/p].$$

Proof. This is [CFKS10, Proposition 7.3] applied to $P = \mathcal{E}[\phi]_{\mathcal{O}_{L_0}}$; their K is our M_0, their L is our L_0, their k is our $\overline{\mathbb{F}}_M$ $(= \overline{\mathbb{F}}_L)$, and their Δ is our I. Since $E[\phi] \subset E(K)$, the Galois representation on geometric points of the generic fiber of $\mathcal{E}[\phi]_{\mathcal{O}_{L_0}}$ is trivial, which allows us to discard the first summand in [CFKS10, Proposition 7.3 (2)]. □

Proposition 5.25. *Under the assumptions of Section* 5.5*, the p-isogeny conjecture* (17) *is true.*

Proof. From Section 5.21 we get that $[D(\mathcal{E}[\phi]_{\overline{\mathbb{F}}_L})]$ is $\gamma(i)$, where $i = 0, \frac{1}{4}, \frac{1}{2}$, or $\frac{3}{4}$. Moreover,

$$\begin{aligned}
\deg([\mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}})]) &= \dim_{\overline{\mathbb{F}}_L} \mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}}) && \text{by Section 5.23} \\
&= \mathrm{length}_{\mathcal{O}_L} \mathrm{Lie}(\mathcal{E}[\phi]) && \text{by (28)} \\
&= (p-1)v_L(a_0) && \text{by Lemma 5.14} \\
&= (p-1)(2m+1), &&
\end{aligned}$$

for some $m \geq 0$, where the last equality follows from Lemma 5.15 and Lemma 5.8. Proposition 5.24 (b) gives

$$-i = \frac{p(2m+1)}{4} \quad \text{in } \mathbb{Q}/\mathbb{Z}[1/p].$$

Since $p \equiv 3 \bmod 4$, this means that $i = \frac{1}{4}$ if m even, and $i = \frac{3}{4}$ if m is odd. Therefore, we have $\varphi^{-1}(\gamma(i)) = \gamma(\frac{3}{4})$ if m is even, and $\varphi^{-1}(\gamma(i)) = \gamma(\frac{1}{4})$ if m is odd. The left hand side of Proposition 5.24 (a) is therefore $\frac{1}{2}$ if m is even, and $-\frac{1}{2}$ if m is odd.

Write $p = 4k + 3$. If m is even, Proposition 5.24 (a) gives

$$\delta_0([\mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}})]) = \frac{(p-1)(2m+1)}{4} - \frac{1}{2} = k(2m+1) + m \equiv k \bmod 2.$$

If m is odd, it gives

$$\delta_0([\mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}})]) = \frac{(p-1)(2m+1)}{4} + \frac{1}{2} = k(2m+1) + (m+1) \equiv k \bmod 2.$$

We conclude that in all cases $\delta_0([\mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}})]) \equiv k \bmod 2$. On the other hand,

$$\begin{aligned}
\delta_0([\mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}})]) &= \dim_{\overline{\mathbb{F}}_L} \mathrm{Lie}(\mathcal{E}[\phi]_{\mathcal{O}_{L_0}})^I && \text{by Section 5.23} \\
&\equiv \mathrm{ord}_p\, \chi(\phi_K) \bmod 2 && \text{by Corollary 5.20,}
\end{aligned}$$

so $\sigma_{\phi_K} = (-1)^k$.

To compute the root number, note that by Theorem 2.2 (e),

$$w(E/K) = (-1)^{\lfloor v(\Delta) \cdot \#\mathbb{F}_K/12 \rfloor}.$$

The latter is $(-1)^{\lfloor v(\Delta) \cdot p/12 \rfloor}$, because $\#\mathbb{F}_K = p^{f_{K/\mathbb{Q}_p}} \equiv p \bmod 24$, since $f_{K/\mathbb{Q}_p}$ is odd. Because $v(\Delta) \in \{3, 9\}$, one checks that $w(E/K) = 1$ if $p \equiv 3 \bmod 8$, and $w(E/K) = -1$ if $p \equiv 7 \bmod 8$. The former occurs if k is even, the latter if k is odd. □

Theorem 5.26. *The p-isogeny conjecture is true for $p > 3$.*

Proof. Indeed, we have settled all the remaining cases: see Section 2.22, Propositions 4.5, 4.8 and 4.9, Section 5.3, Lemma 5.4, Section 5.5, and Proposition 5.25. □

6. The p-parity conjecture for elliptic curves with complex multiplication

In this section E denotes an elliptic curve over a number field K such that E/K has complex multiplication by an order of the imaginary quadratic field $F := (\mathrm{End}_K E) \otimes \mathbb{Q}$. The ring of integers of F will be denoted by $\mathcal{O}_F$. We set

$$\mathcal{X}_p(E/K) := \mathrm{Hom}_{\mathbb{Z}_p}(\varinjlim \mathrm{Sel}_{p^n}(E/K), \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

and note that by definition $\mathrm{rk}_p(E/K) = \dim_{\mathbb{Q}_p} \mathcal{X}_p(E/K)$.

In Theorem 6.4 we prove the p-parity conjecture for such elliptic curves; I thank Karl Rubin for pointing out to me that this result follows from Theorem 1.4. In Proposition 6.3 we prove that the global root number of E/K is 1, which gives Theorem 1.8. We begin by recalling two well-known results that will be used in the proofs.

Proposition 6.1. *There is an elliptic curve E'/K such that $\mathrm{End}_K E' \cong \mathcal{O}_F$ and there is an isogeny $\lambda\colon E \to E'$ defined over K.*

Proof. See, for instance, [Rub99, Proposition 5.3]. □

Proposition 6.2. *If E and E' are two elliptic curves defined over a number field K and $\lambda\colon E \to E'$ is an isogeny defined over K, then*

$$\mathrm{rk}_p(E/K) = \mathrm{rk}_p(E'/K) \quad \textit{and} \quad w(E/K) = w(E'/K).$$

Proof. If λ' is the dual isogeny, then one notes that the composition $\lambda' \circ \lambda$ induces automorphisms of $\mathcal{X}_p(E/K)$ and $V_l(E/K)$, and similarly for $\lambda \circ \lambda'$. Hence the maps induced by λ are isomorphisms. This gives the claim about rk_p. The local root numbers at finite places are defined in terms of $V_l(E/K)$ and at infinite places are -1 by Theorem 2.2 (a), so the conclusion follows. □

Proposition 6.3. *If E has complex multiplication defined over K, then $w(E/K) = 1$. More precisely, if $\psi_{E/K} = \prod_v' \psi_v\colon \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$ is the Hecke character associated to E/K (cf., for instance,* [Rub99, Theorem 5.15]*), then $w(E/K_v) = \psi_v(-1)$ for every place v.*

Proof. It is clear that the first claim follows from the second by taking the product over all places:

$$\prod_v \psi_v(-1) = \psi_{E/K}(-1) = 1.$$

Let v be a finite place of K and choose a rational prime p such that $v \nmid p$ and p splits in F. The Galois representation $V_p(E/K_v)$ is a direct sum $\psi_v \oplus \psi_v$ (see [Rub99, Corollary 5.6 and Theorem 5.15 (ii)]) (here we engage in the usual abuse of local class field theory by identifying characters of $K_v^\times$ and of $\mathcal{W}(\overline{K}_v/K_v)$). If $\omega_v\colon \mathcal{W}(\overline{K}_v/K_v) \to \mathbb{C}^\times$ is the cyclotomic character, then, because of the Weil pairing, $\psi_v\omega_v^{-1/2}$ squares to the trivial character, and hence is self-contragredient. The determinant formula (c) from Section 3.9 applies, giving

$$w(\psi_v\omega_v^{-1/2}, \eta)^2 = \psi_v(-1).$$

Since a twist by $\omega_v^{-1/2}$ does not affect the root number [Roh94, Section 11, Proposition (iii)], we conclude that $w(E/K_v) = w(\psi_v, \eta)^2 = \psi_v(-1)$.

The formula $w(E/K_v) = \psi_v(-1)$ holds at an archimedean place v as well. Indeed, we have $w(E/K_v) = -1$ by Theorem 2.2 (a), while $\psi_v(-1) = -1$ by construction of $\psi_{E/K}$, see the proof of [Rub99, Theorem 5.15] (the $\psi_{E/K}$ constructed there is unique because (ii) there determines its finite component uniquely, and then the infinite component is uniquely determined because $\psi_{E/K}$ is a Hecke character). □

Theorem 6.4. *If E has complex multiplication defined over K, then the p-parity conjecture holds for E/K.*

Proof. Due to Propositions 6.1 and 6.2, we assume that E has complex multiplication by the maximal order $\mathcal{O}_F$. If p is inert or ramifies in F, then $F_{\mathfrak{p}} := \mathcal{O}_F \otimes \mathbb{Q}_p$ is a quadratic extension of $\mathbb{Q}_p$. Since $\mathcal{X}_p(E/K)$ is an $F_{\mathfrak{p}}$-vector space, $\mathrm{rk}_p(E/K) = \dim_{\mathbb{Q}_p} \mathcal{X}_p(E/K)$ is even and the conclusion follows from Proposition 6.3. On the other hand, if p ramifies or splits in F and $\mathfrak{p}$ is a prime of F above p, then $E[\mathfrak{p}] := \bigcap_{\alpha \in \mathfrak{p}} \{P \in E(\overline{K}) : \alpha P = 0\}$ is a subgroup of $E[p]$ of order p defined over K (see [Rub99, Proposition 5.4] for instance). In other words, the subgroup $E[\mathfrak{p}]$ is the kernel of a p-isogeny defined over K, and the conclusion follows from Theorem 1.4. □

References

[BS64] *A. Borel* and *J.-P. Serre*, Théorèmes de finitude en cohomologie galoisienne, Comment. Math. Helv. **39** (1964), 111–164.

[BLR90] *S. Bosch*, *W. Lütkebohmert* and *M. Raynaud*, Néron models, Ergeb. Math. Grenzgeb. (3) **21**, Springer-Verlag, Berlin 1990.

[Bre00] *C. Breuil*, Groupes p-divisibles, groupes finis et modules filtrés, Ann. of Math. (2) **152** (2000), no. 2, 489–549.

[Cas62] *J. W. S. Cassels*, Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung, J. reine angew. Math. **211** (1962), 95–112.

[Coa91] *J. Coates*, Elliptic curves with complex multiplication and Iwasawa theory, Bull. Lond. Math. Soc. **23** (1991), no. 4, 321–350.

[CFKS10] *J. Coates*, *T. Fukaya*, *K. Kato* and *R. Sujatha*, Root numbers, Selmer groups, and non-commutative Iwasawa theory, J. Algebraic Geom. **19** (2010), no. 1, 19–97.

[Del75] *P. Deligne*, Courbes elliptiques: formulaire d'après J. Tate, in: Modular functions of one variable. IV (Antwerp 1972), Lecture Notes in Math. **476**, Springer-Verlag, Berlin (1975), 53–73.

[DD08] *T. Dokchitser* and *V. Dokchitser*, Parity of ranks for elliptic curves with a cyclic isogeny, J. Number Theory **128** (2008), no. 3, 662–679.

[DD09] *T. Dokchitser* and *V. Dokchitser*, Regulator constants and the parity conjecture, Invent. Math. **178** (2009), no. 1, 23–71.

[DD10] *T. Dokchitser* and *V. Dokchitser*, On the Birch–Swinnerton-Dyer quotients modulo squares, Ann. of Math. (2) **172** (2010), no. 1, 567–596.

[DD11] *T. Dokchitser* and *V. Dokchitser*, Root numbers and parity of ranks of elliptic curves, J. reine angew. Math. **658** (2011), 39–64.

[DD12] *T. Dokchitser* and *V. Dokchitser*, Local invariants of isogenous elliptic curves, Trans. Amer. Math. Soc., to appear.

[Ill05] *L. Illusie*, Grothendieck's existence theorem in formal geometry, in: Fundamental algebraic geometry, Math. Surveys Monogr. **123**, American Mathematical Society, Providence (2005), 179–233.

[Kim07] *B. D. Kim*, The parity conjecture for elliptic curves at supersingular reduction primes, Compos. Math. **143** (2007), no. 1, 47–72.

[Kob02] *S. Kobayashi*, The local root number of elliptic curves with wild ramification, Math. Ann. **323** (2002), no. 3, 609–623.

[LS10] *C. Liedtke* and *S. Schröer*, The Néron model over the Igusa curves, J. Number Theory **130** (2010), no. 10, 2157–2197.

[MR10] *B. Mazur* and *K. Rubin*, Ranks of twists of elliptic curves and Hilbert's tenth problem, Invent. Math. **181** (2010), no. 3, 541–575.
[Mil72] *J. S. Milne*, On the arithmetic of abelian varieties, Invent. Math. **17** (1972), 177–190.
[Nek06] *J. Nekovář*, Selmer complexes, Astérisque **310**, Société Mathématique de France, Paris 2007.
[Nek09] *J. Nekovář*, On the parity of ranks of Selmer groups. IV, Compos. Math. **145** (2009), no. 6, 1351–1359.
[Nek12] *J. Nekovář*, Some consequences of a formula of Mazur and Rubin for arithmetic local constants, Algebra Number Theory **7** (2013), no. 5, 1101–1120.
[Nek14] *J. Nekovář*, Compatibility of arithmetic and algebraic local constants (the case $l \neq p$), preprint 2014, `http://www.math.jussieu.fr/~nekovar/pu/loc.pdf`.
[Roh94] *D. E. Rohrlich*, Elliptic curves and the Weil–Deligne group, in: Elliptic curves and related topics, CRM Proc. Lecture Notes **4**, American Mathematical Society, Providence (1994), 125–157.
[Roh96] *D. E. Rohrlich*, Galois theory, elliptic curves, and root numbers, Compos. Math. **100** (1996), no. 3, 311–349.
[Rub99] *K. Rubin*, Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer, in: Arithmetic theory of elliptic curves (Cetraro 1997), Lecture Notes in Math. **1716**, Springer-Verlag, Berlin (1999), 167–234.
[Sch96] *E. F. Schaefer*, Class groups and Selmer groups, J. Number Theory **56** (1996), no. 1, 79–114.
[Ser67] *J.-P. Serre*, Local class field theory, in: Algebraic number theory (Brighton 1965), Thompson, Washington (1967), 128–161.
[Ser72] *J.-P. Serre*, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), no. 4, 259–331.
[Ser77] *J.-P. Serre*, Linear representations of finite groups, Grad. Texts in Math. **42**, Springer-Verlag, New York 1977.
[Ser79] *J.-P. Serre*, Local fields, Grad. Texts in Math. **67**, Springer-Verlag, New York 1979.
[Ser02] *J.-P. Serre*, Galois cohomology, Springer Monogr. Math., Springer-Verlag, Berlin 2002.
[Tat74] *J. T. Tate*, The arithmetic of elliptic curves, Invent. Math. **23** (1974), 179–206.
[Tat75] *J. Tate*, Algorithm for determining the type of a singular fiber in an elliptic pencil, in: Modular functions of one variable. IV (Antwerp 1972), Lecture Notes in Math. **476**, Springer-Verlag, Berlin (1975), 33–52.
[TO70] *J. Tate* and *F. Oort*, Group schemes of prime order, Ann. Sci. Éc. Norm. Supér. (4) **3** (1970), 1–21.

Kęstutis Česnavičius, Department of Mathematics, Massachusetts Institute of Technology,
Cambridge, MA 02139, USA
e-mail: kestutis@math.mit.edu

Eingegangen 3. September 2012, in revidierter Fassung 10. März 2014