K. KRAMER

J. TUNNELL

Elliptic curves and local ε-factors

Compositio Mathematica, tome 46, nº 3 (1982), p. 307-352

<http://www.numdam.org/item?id=CM_1982__46_3_307_0>

COMPOSITIO MATHEMATICA, Vol. 46, Fasc. 3, 1982, pag. 307–352
© 1982 Martinus Nijhoff Publishers - The Hague
Printed in the Netherlands

ELLIPTIC CURVES AND LOCAL ϵ-FACTORS

K. Kramer and J. Tunnell

Introduction.

Let E be an elliptic curve over a local field F. Following Deligne and Langlands [10] we attach to E a complex two-dimensional representation σ_E of the Weil–Deligne group of F. By means of [4] we associate to σ_E a local factor $\epsilon(\sigma_E)$ which is ± 1. The purpose of this paper is to describe this "local sign" in geometric terms.

Given a quadratic character ω of F^*, there is a quadratic separable extension K of F such that the kernel of ω is precisely the image of the norm map from K^*. Let $\mathbb{N}$ be the norm homomorphism from $E(K)$ to $E(F)$ which assigns to P in $E(F)$ the sum $P + gP$, where g generates $\mathrm{Gal}(K/F)$. We consider the following

$$\text{CONJECTURE: } \epsilon(\sigma_E)\epsilon(\sigma_E \otimes \omega) = \omega(-\Delta)(-1)^{\dim(E(F)/NE(K))}.$$

Here Δ is the discriminant of any model of E over F, and $\dim(E(F)/\mathbb{N}E(K))$ is the $\mathbb{F}_2$-dimension of the two-group $E(F)/\mathbb{N}E(K)$.

In this paper we prove this conjecture in a large number of cases. These include all cases where F is archimedean or of odd residue characteristic. When F has even residue characteristic we prove the conjecture when ω is unramified or E has ordinary good reduction. The conjecture is motivated by consideration of the parity of the rank of the Mordell–Weil group of elliptic curves over quadratic extensions of global fields [8]. For an elliptic curve over $\mathbb{Q}$ with L-series given by the Dirichlet series associated to a modular form f, the ϵ-factor of the curve over $\mathbb{Q}_p$ is the negative of the eigenvalue of the Atkin–Lehner operator W_p on f. The sign in the functional equation for the L-series of the curve over $\mathbb{Q}$ is a product of ϵ-factors. We show that the conjecture above is a consequence of the standard conjectures about elliptic curves over global fields.

Research partially supported by grants from the National Science Foundation. The second author wishes to thank the I.H.E.S. for its hospitality in August, 1980, when a portion of this research was done.

0010–437X/82060307–46$00.20/0

The conjecture suggests many relations between the representation theoretic quantities on the left hand side and the geometric quantities on the right. Since σ_E depends only on the F-isogeny class of E, the conjecture implies that $\omega(\Delta)(-1)^{\dim(E(F)/NE(K))}$ is an F-isogeny invariant. On the other hand, the conjecture gives a geometric method to calculate ϵ-factors, which are originally defined in group-theoretic terms. This is similar to the results of [5] and [6] which give alternate interpretations for ϵ-factors of orthogonal representations. The representations σ_E are not necessarily orthogonal, even though they have real valued characters, since it is possible for the conductor exponent of σ_E to be odd. There seems to be no direct connection of our geometric results with the results of [5].

The first section of this paper recalls aspects of the theory of elliptic curves over local fields. In section 2 we review the local ϵ-factors attached to representations of the Weil–Deligne group and calculate these factors in some cases. Section 3 examines several compatibility statements involving the conjecture, showing that it follows from standard global conjectures. We prove the conjecture for curves with potential multiplicative reduction in section 4, and for curves over fields of odd residue characteristic in section 5. In section 6 the conjecture is proven for ω unramified, while section 7 gives the norm index in terms of Kodaira types of elliptic curves. The final sections contain a compendium of results and examples when the residue characteristic is two and some applications of our results to elliptic curves over global fields. The residue characteristic two fields are more troublesome due to the traditional problems of elliptic curves over such fields and the large number of possibilities for σ_E in that situation. For odd residue characteristics (sections 5 and those preceding) the possibilities for σ_E are rather limited.

The following notational conventions are employed throughout. The cardinality of a finite set S is denoted $|S|$. Attached to a nonarchimedean local field are its ring of integers $\mathcal{O}$, prime ideal $\mathcal{P}$, valuation v, and residue field k. These are indexed by the field when several fields are being considered. By abuse of terminology we sometimes refer to quadratic extensions which are in fact of degree 1 over the base. The $\mathbb{F}_2$-dimension of a 2-group A is denoted $\dim(A)$.

1. Elliptic curves over local fields

Let E be an elliptic curve over a local field F; that is a non-singular projective curve of genus 1 over F with a rational point 0. We refer to [16, §2] for the generalized Weierstrass equation of a model of E over

F and the definition of the discriminant Δ of the model. We recall that the isomorphism class of E determines Δ modulo $(F^*)^{12}$, and that $F(\sqrt{\Delta})$ is the unique quadratic extension of F contained in the field generated over F by the coordinates of the points of order 2 in the abelian group $E(\bar{F})$.

For each quadratic character ω of F^*, we obtain an elliptic curve E^ω over F, the *twist of E by ω*. The curve E^ω is isomorphic to E over the quadratic field K corresponding to ω, and is characterized by the fact that $E^\omega(F)$ is the group of points P in $E(K)$ where $g(P) = \omega(g) \cdot P$ for g in $\mathrm{Gal}(K/F)$.

When F is a nonarchimedean field we will utilize the Tate module of the elliptic curve E. Let ℓ be a prime number different from the residue characteristic of F, and let F_s be a separable closure of F. The $\mathrm{Gal}(F_s/F)$-module $T_\ell(E)$ is the projective limit of the groups of points in $E(F_s)$ of ℓ^n-power order. This is a free $\mathbb{Z}_\ell$-module of rank 2, and we let $V_\ell(E) = T_\ell(E) \otimes \mathbb{Q}_\ell$. For each g in $\mathrm{Gal}(F_s)$ it is known [16, §4] that the determinant of the endomorphism of $V_\ell(E)$ given by g is the unique element $\alpha(g) \in \mathbb{Q}_\ell^*$ such that $g(\xi) = \xi^{\alpha(g)}$ for all ℓ-power roots of unity in F_s.

Let W_F denote the absolute Weil group of F [18; §1]. Local class-field theory gives an isomorphism of F^* and W_F^{ab}. When F is nonarchimedean, W_F is the subgroup of $\mathrm{Gal}(F_s/F)$ which has image an integral power of the canonical generator of $\mathrm{Gal}(F^{\mathrm{nonram}}/F) \approx \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$, where the residue field of F is isomorphic to $\mathbb{F}_q$. We normalize the class field theory isomorphism so that if $w \in W_F$ projects to the canonical generator of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ (that is, raising to q^{th} powers), the corresponding element of $F^* \approx W_F^{ab}$ has valuation -1. We will systematically identify continuous quasicharacters of F^* and continuous 1-dimensional representation of W_F via the class field theory isomorphism.

The Weil–Deligne group W_F' is defined to be $W_F \times SL(2, \mathbb{C})$. By a representation of W_F' we will mean a continuous complex representation which is analytic on $SL(2, \mathbb{C})$. Every continuous representation of W_F provides one of W_F' by projecting the Weil–Deligne group on its first factor. We now associate to each elliptic curve E over F a representation σ_E of W_F'.

When $F = \mathbb{R}$, σ_E is the two-dimensional representation of W_F induced from the identity character $z \to z$ of $W_{\mathbb{C}} = \mathbb{C}^* \subset W_{\mathbb{R}}$. When $F \approx \mathbb{C}$, σ_E is the sum of the identity character and its complex conjugate. In these cases σ_E does not depend on E. See [4; §8.12].

When F is nonarchimedean, consider the inertia subgroup $I \subset W_F \subset \mathrm{Gal}(F_s/F)$. We will denote the representation of W_F on $V_\ell(E)$ by ρ_ℓ. Since W_F consists precisely of those elements which, considered modulo I, give an integral power of the canonical generator of the absolute Galois group of the residue field we have that $\rho_\ell(w)$ has a characteristic polynomial with rational coefficients independent of ℓ [15; Theorem 3]. When $\rho_\ell(I)$ is a finite subgroup of $\mathrm{Aut}(V_\ell(E))$ (potential good reduction in the sense of [15; §2]) we choose any imbedding $\mathbb{Q}_\ell \to \mathbb{C}$ and by means of this identify $\mathrm{Aut}(V_\ell(E)) \approx GL(2, \mathbb{Q}_\ell)$ with a subgroup of $GL(2, \mathbb{C})$. This gives a homomorphism $\sigma_E\colon W_F \to GL(2, \mathbb{C})$. Since the image of I is finite, σ_E is a semi-simple complex representation of W_F. Changing the imbedding $\mathbb{Q}_\ell \to \mathbb{C}$ does not alter the isomorphism class of σ_E since $\rho_\ell(w)$ has rational characteristic polynomial independent of ℓ.

When $\rho_\ell(I)$ is infinite we proceed as in [10; §4]. This is the case of potential multiplicative reduction, so that E is isomorphic to a Tate curve E_T (that is $E_T(F_s) \approx F_s^*/q^Z$ as a $\mathrm{Gal}(F_s/F)$ module for some $q \in F^*$) over a quadratic extension L. Let χ be the quadratic character of F^* corresponding to L, so that E is the twist E_T^χ ($\chi = 1$ if E is isomorphic to E_T over F).

Let $sp'(2)$ be the representation of W'_F given by projection onto $SL(2, \mathbb{C})$. Let $\|\cdot\|$ be the unramified quasicharacter of F^* for which $\|x\| = |k_F|^{-v(x)}$. Then we define the representation $sp(2)$ of W'_F to be $sp'(2) \otimes \|\ \|^{1/2}$ and we let $\sigma_E = sp(2) \otimes \chi$, where $\|\ \|^{1/2}$, χ are considered as 1-dimensional representations via the class-field theory isomorphism chosen earlier.

We have now associated to each elliptic curve E over a local field an isomorphism class of complex two-dimensional representations σ_E of W'_F. It is clear that this representation depends only on the F-isogeny class of E. Further, $\det \sigma_E$ is the 1-dimensional representation of W'_F corresponding to $\|\ \|$.

The symbol $a(\sigma)$ will denote the exponent of the Artin conductor of a representation σ of W_F, when F is nonarchimedean [14; Chap. VI]. We make the convention that $a(sp(2) \otimes \eta) = \max(1, 2a(\eta))$, when η is a 1-dimensional representation of W_F [4; 8.12.1]. The exponent of the conductor of E is by definition $a(E) = a(\sigma_E)$. This agrees with the usual definition [15; §3].

To conclude this section we consider the norm map on elliptic curves. Let L be a finite separable extension of F, and let L' be the Galois closure of L/F, with Galois group G and subgroup H stabilizing L. The norm homomorphism is the map

$$\begin{aligned} \mathbb{N}\colon E(L) &\to E(F) \\ P &\to \sum_{g \in G/H} g(P). \end{aligned}$$

We will show in (7.3) that $\mathbb{N}E(L)$ has finite index in $E(F)$. The following is a simpler version of that fact.

LEMMA 1.1: *The subgroup $\mathbb{N}E(L)$ has finite index in $E(F)$ when $[L:F]$ is not divisible by the residue characteristic of F. The index divides a power of $[L:F]$ in this case.*

PROOF: The group $E(F)/\mathbb{N}E(L)$ is annihilated by $[L:F]$, so the last statement follows once the index is known to be finite.

For F archimedean, the norm map is a continuous map of Lie groups, and $E(\mathbb{R})$ has at most two connected components. When F is nonarchimedean, it is well known [17; (4.7)] that $E(F)$ contains a finite index subgroup U which is profinite of order a power of the residue characteristic. If $[L:F]$ is not divisible by the residue characteristic, $[L:F]U = U$. Since $\mathbb{N}E(L)$ contains $[L:F]\ E(F)$ the result follows.

2. Local factors attached to representations of the Weil–Deligne group.

In this section we review the definition and properties of local ϵ-factors attached to complex linear representations of W'_F. For a detailed discussion see [18; §3] and the references there.

Choose a nontrivial additive character ψ and an additive Haar measure dx_F for F. Attach to each continuous linear representation σ of W_F a complex number $\epsilon(\sigma, \psi, dx_F)$ as follows. For σ one-dimensional, $\epsilon(\sigma, \psi, dx_F)$ is the factor appearing in the local functional equation in Tate's Thesis. For precise formulas, see [18; (3.2.1)]. In general $\epsilon(\sigma, \psi, dx_F)$ is the unique extension of this factor to a function on all representations which is additive and inductive in degree zero over F. The fact that such an extension exists has been verified by Langlands and Deligne [4]. The following properties [18; (3.4)] are used in the remainder of the paper. Let W, V be representations of the Weil group W_F.

$$\epsilon(V \oplus W, \psi, dx_F) = \epsilon(V, \psi, dx_F)\epsilon(W, \psi, dx_F). \qquad (2.1.1)$$

If V is a virtual representation of dimension zero of W_L, and L a finite extension of F

$$\epsilon(\mathrm{Ind}_{W_I}^{W_F}(V), \psi, dx_F) = \epsilon(V, \psi \circ tr_{L/F}, dx_L). \qquad (2.1.2)$$

$$\epsilon(V, \psi, r \cdot dx_F) = r^{\dim V} \epsilon(V, \psi, dx_F) \quad \text{for } r > 0. \tag{2.1.3}$$

Let $\psi_a(x) = \psi(ax)$. Then for $a \in F^*$

$$\epsilon(V, \psi_a, dx_F) = \det V(a) \cdot \|a\|^{-\dim V} \epsilon(V, \psi, dx_F). \tag{2.1.4}$$

If dx_F is self-dual with respect to ψ and V^* is the contragredient of V

$$\epsilon(V, \psi, dx_F)\epsilon(V^* \otimes \| \quad \|, \psi, dx_F) = \det V(-1) \tag{2.1.5}$$

Let F be nonarchimedean. There exists a choice of ψ so that

$$\epsilon(V \otimes W, \psi, dx_F) = \det W(\pi)^{a(V)} \epsilon(V, \psi, dx_F)^{\dim W} \tag{2.1.6}$$

when W is unramified. (π a generator of $\mathcal{P}_F$).

There are similar properties for representations of the Weil–Deligne group W_F'. (see [4, 8.12]). We will use only that when χ is a 1-dimensional representation of W_F

$$\epsilon(sp(2) \otimes \chi) = \begin{cases} \epsilon(\chi)^2 & \chi \text{ ramified} \\ -\chi(\pi)\epsilon(\chi)^2 & \chi \text{ unramified} \end{cases} \tag{2.1.7}$$

for suitable ψ and dx_F.

We now define the factor $\epsilon(\sigma_E)$ associated to the representation attached to an elliptic curve E over F in section 1.

DEFINITION 2.2: *$\epsilon(\sigma_E) = \epsilon(\sigma_E, \psi, dx_F)$ where ψ is arbitrary and dx_F is self-dual with respect to ψ.*

Since $\det(\sigma_E \otimes \| \quad \|^{-1/2})$ is trivial, property (2.1.4) shows that $\epsilon(\sigma_E)$ is independent of the choice of ψ. Further $\sigma_E \otimes \| \quad \|^{-1/2}$ is self-contragredient, so $\epsilon(\sigma_E)^2$ equals 1 by (2.1.5).

DEFINITION 2.3: *For each quadratic character ω of F^*, define $\epsilon(E, \omega)$ to be $\epsilon(\sigma_E)\epsilon(\sigma_E \otimes \omega)$.*

REMARK: The representation $\sigma_E \otimes \omega$ is attached to the twisted curve E^ω. Thus $\epsilon(E, \omega) = \pm 1$.

PROPOSITION 2.4: (*a*) *If F is archimedean, $\epsilon(E, \omega) = 1$.*

(*b*) *If* σ_E *is decomposable,* $\epsilon(E, \omega) = \omega(-1)$.

(*c*) *If* F *is nonarchimedean and* π *has valuation one, then* $\epsilon(E, \omega) = \omega(\pi)^{a(\sigma_E)}$ *for* ω *unramified.*

PROOF: (a) When F is archimedean, σ_E is independent of E, and the results of [18; (3.2)] shows that $\epsilon(\sigma_E) = \epsilon(\sigma_E \otimes \omega) = -1$.

For (b), suppose that $\sigma_E \approx \mu \oplus \nu$. Then det $\sigma_E = \mu\nu = \| \quad \|$, so that if dx is self dual with respect to ψ:

$$\epsilon(\sigma_E, \psi, dx) = \epsilon(\mu, \psi, dx)\epsilon(\mu^{-1}\| \quad \|, \psi, dx) = \mu(-1)$$

Similarly $\epsilon(\sigma_E \otimes \omega, \psi, dx) = \mu(-1)\omega(-1)$, so the result follows.

(c) This follows directly from the definition of $\epsilon(E, \omega)$ and property (2.1.6) of ϵ-factors.

The factors $\epsilon(E, \omega)$ can now be calculated in certain cases.

PROPOSITION 2.5: *Suppose that* $\sigma_E = sp(2) \otimes \chi$. *Then* $\epsilon(E, \omega)$ *is given by the following table*:

χ $\chi\omega$	ramified	unramified
ramified	$\omega(-1)$	$-\omega(-1)\chi(\pi)$
unramified	$-\chi(-\pi)\omega(\pi)$	$\omega(\pi)$

PROOF: From (2.1.7) and (2.1.5) we see that if η is a quadratic character of W_F we have for suitable ψ, dx:

$$\epsilon(sp(2) \otimes \eta, \psi, dx) = \begin{cases} -\eta(\pi) & \eta \text{ unramified} \\ \eta(-1) & \eta \text{ ramified} \end{cases} .$$

The result now follows from the definition of $\epsilon(E, \omega)$ and the above formula.

The next result concerns the case when σ_E is induced from an index two subgroup of W'_F. By [3; Prop. 3.1.4] this always occurs if σ_E is irreducible when restricted to W_F and the residue characteristic is odd. The result depends on the following Theorem of Frohlich and Queyrut.

THEOREM 2.6[6]: *Let* θ *be a quasicharacter of a quadratic separable extension* L *of* F, *and suppose* θ *is trivial on* F^*. *Let* y *be an element of* L^* *such that* $\mathrm{tr}_{L/F}(y) = 0$. *Then* $\epsilon(\theta, \psi, dx_L) = c\,\theta(y)$, *where* c *depends only on* ψ *and* dx_L.

THEOREM 2.7: *Suppose that* $\sigma_E = \mathrm{Ind}_{W_L}^{W_F}\,\theta$, *where* L *is the unramified quadratic extension of* F. *Let* y *be a nonzero element of* L *with* $tr_{L/F}(y) = 0$. *Then*

$$\epsilon(E, \omega) = (-1)^{a(\theta)+a(\theta\omega\circ N_{L/F})}\omega(-y^2).$$

PROOF: Choose an additive character ψ and self dual measure dx. Since $\det\sigma_E(x) = \|x\|$, we have that $\theta|_{F^*} = \omega_L\|\ \ \|$, where ω_L is the unramified quadratic character. Let $\tilde{\omega}$ be the nontrivial unramified quadratic character of L^*, so that $\tilde{\omega}|_{F^*} = \omega_L$. Let α be the quasi-character $\theta\cdot\omega^{-1}\cdot\|\ \ \|^{-1}$ of L^*. Then α is trivial on F^*. Further $\epsilon(\sigma_E, \psi, dx) = \gamma\epsilon(\theta, \psi\circ\mathrm{tr}_{L/F}, dx_L)$ by (2.1.2), where γ depends only on L/F, dx, and ψ. Replacing $\psi\circ\mathrm{tr}_{L/F}$ by a suitable ψ' as in (2.1.6) and invoking (2.1.4), we notice that θ differs from α by an unramified character $\tilde{\omega}\|\ \ \|$, so that

$$\epsilon(\theta, \psi\circ\mathrm{tr}_{L/F}, dx_L) = \delta(-1)^{a(\alpha)}\epsilon(\alpha, \psi\circ\mathrm{tr}_{L/K}, dx_L)$$

where δ depends only on L/F, dx, ψ and ψ'. By (2.6), $\epsilon(\sigma_E, \psi, dx) = (-1)^{a(\alpha)}c'\alpha(y)$ for a constant c' depending only on L/F, y, dx, ψ and ψ'. Repeating the calculation with $\theta(\omega\circ N_{L/F})$ in place of θ and the same choice of y, dx, ψ and ψ' shows that $\epsilon(\sigma_E\otimes\omega, \psi, dx) = (-1)^{a(\alpha\cdot\omega\circ N_{L/F})}c'\alpha(y)\omega(N_{L/F}y)$. Hence

$$\epsilon(E, \omega) = (-1)^{a(\alpha)+a(\alpha\cdot\omega\circ N_{L/F})}\omega(-y)^2\alpha(y^2)(c')^2.$$

Notice that $y^2 = -Ny$, so $\alpha(y^2) = 1$. Also, $a(\alpha) = a(\theta)$ and $a(\alpha\cdot\omega\circ N_{L/F}) = a(\theta\cdot\omega\circ N_{L/F})$. The special case $\omega = 1$ shows that $(c')^2$ is 1. This proves the theorem.

COROLLARY 2.8: *Suppose that* σ_E *is irreducible and induced from the absolute Weil group of the quadratic unramified extension of* F. *If* $a(\omega) = 1$, *then* $\epsilon(E, \omega) = -\omega(-1)$.

PROOF: By assumption $\sigma_E = \mathrm{Ind}_{W_L}^{W_F}\,\theta$. The fact that σ_E is irreducible is equivalent (by Frobenius Reciprocity) to the fact that θ is not of the form $\eta\circ N_{L/F}$ for any quasicharacter η of F^*. In particular $a(\theta)\geq 1$, and hence $a(\theta\omega\circ N) = a(\theta)$. Since F has tamely ramified quadratic characters, the residue characteristic is odd, and $L = F(\sqrt{u})$ for some u in $\mathcal{O}_{F^*}$ which is not a square modulo the prime ideal. Take $y = \sqrt{u}$ in (2.6), so that $\omega(y^2) = \omega(u) = -1$, since $a(\omega) = 1$. The corollary results immediately from the preceding theorem.

3. Statement of the conjecture and motivation

Let E be an elliptic curve over a local field F, and let K be a quadratic extension of F corresponding by local class field theory to a quadratic character ω (when ω is trivial we take $K = F \oplus F$ and $\mathrm{N}E(K) = E(F)$). The group $E(F)/\mathrm{N}E(K)$ is a finite 2-group by (7.3). Let d be the dimension of this $\mathbb{F}_2$-vector space and define $\kappa(E, \omega)$ by $(-1)^d$. The discriminant Δ of a model of E is determined up to $(F^*)^{12}$-multiplication by the isomorphism class of E, so that $\omega(\Delta)$ is well-defined. Recall from (2.3) that $\epsilon(E, \omega)$ is a product of local signs for E and the twist E^{ω}.

CONJECTURE 3.1.: $\epsilon(E, \omega) = \omega(-\Delta)\kappa(E, \omega)$.

REMARKS: The conjecture is true when ω is trivial, as both sides equal 1.

When $F = \mathbb{R}$ and $K \approx \mathbb{C}$, the left hand side is 1 (2.4.a). The norm homomorphism maps the connected real Lie group $E(\mathbb{C})$ to the real Lie group $E(\mathbb{R})$. Hence $\kappa(E, \omega) = (-1)^{c-1}$, where c is the number of connected components of $E(\mathbb{R})$. It is well known that $\Delta > 0$ if and only if $E(\mathbb{R})$ has two components, which verifies the conjecture for F archimedean.

REMARK: Conjecture 3.1 is compatible with the standard conjectures for elliptic curves over global fields. In order to check this the formula developed in [8] for the parity of the rank of the Mordell–Weil group over a quadratic extension can be used as follows. Let F be a global field ($\mathrm{char}(F) \neq 2$) for this remark only, and K/F a quadratic extension. Let E be an elliptic curve over F. If the 2 primary component of the Tate–Shafarevitch group Ш(E, K) is finite, then

$$(-1)^{\mathrm{rank}\, E(K)} = \prod_v \kappa(E_v, \omega_v)$$

by Theorem 1 of [8]. On the other hand, if the L-function of E over F is given by an automorphic L-function such that the local ϵ-factors in the functional equation are $\epsilon(E_v, \omega_v)$, the Birch, Swinnerton–Dyer conjecture would imply that

$$(-1)^{\mathrm{rank}(E(K))} = \prod_v \epsilon(E_v, \omega_v).$$

Since $\prod_v \omega_v(-\Delta) = 1$, these two facts imply that $\prod_v \epsilon(E_v, \omega_v) = \prod_v \omega_v(-\Delta)\kappa(E_v, \omega_v)$. Thus, if conjecture 3.1 is known for all but one place F_v and quadratic character ω_v, it must be true for the remaining place. In [8] conjecture 3.1 was shown if E has good or multiplicative reduction. We show in section 6 that the conjecture is true for ω unramified. Using this, it is possible to derive the conjecture from global conjectures by choosing global fields with appropriate local behavior.

Two other compativility properties of $\epsilon(E, \omega)$ and $\kappa(E, \omega)$ will now be checked. The first is a symmetry result. It is clear that $\epsilon(E^\omega, \omega) = \epsilon(E, \omega)$, since $\sigma_{E^\omega} = \sigma_E \otimes \omega$. The ratio $\Delta_E/\Delta_{E^\omega}$ is in $(F^*)^6$. The conjecture suggests that $\kappa(E, \omega) = \kappa(E^\omega, \omega)$, which we now prove.

Proposition 3.3: *Let E be an elliptic curve over a local field F and let ω be a quadratic character of F^*. Then $|E(F)/\mathbb{N}E(K)| = |E^\omega(F)/\mathbb{N}E^\omega(K)|$ in particular $\kappa(E, \omega) = \kappa(E^\omega, \omega)$.*

Proof: The result is obvious if ω is trivial or F is archimedean. For ω nontrivial and F nonarchimedean, let K be the quadratic extension of F corresponding to ω, and let $G = \mathrm{Gal}(K/F)$. Then $H^0(G, E(K)) \approx E(F)/\mathbb{N}E(K)$ and $H^1(G, E(K)) \approx E^\omega(F)/\mathbb{N}E^\omega(K)$, so we must show that the Herbrand quotient $h(E(K))$ is trivial.

There is a finite index G-submodule U of $E(K)$ with $h(U) = 1$, see (7.3.1). (If the residue characteristic is odd, U may be taken to be the kernel of reduction modulo the prime ideal of K). Since the Herbrand quotient is an Euler–Poincaré characteristic trivial on finite G-modules [14; VIII, §4] we have $h(E(K)) = h(U) = 1$. This proves the symmetry result.

Remark: It is easy to see that $\epsilon(E, \omega_1)\epsilon(E, \omega_2) = \epsilon(E^{\omega_1}, \omega_1\omega_2)$. In other words, $\epsilon(E, \omega)$ may be considered as a 1-cocycle on the group of quadratic characters of F^* with values in the space of functions from elliptic curves of F to $\{\pm 1\}$. (The action of the group of quadratic characters is induced by the twisting action on elliptic curves). Since $\omega_1(-\Delta_E)\omega_2(-\Delta_E) = \omega_1\omega_2(-\Delta_E) = \omega_1\omega_2(-\Delta_E\omega_1)$ we see that a consequence of (3.1) is the prediction that $\kappa(E, \omega)$ satisfies the cocycle relation $\kappa(E, \omega_1)\kappa(E, \omega_2) = \kappa(E^{\omega_1}, \omega_1\omega_2)$. The case $\omega_2 = 1$ is the result of (3.3). We have not been able to show this cocycle relation in general.

A second compatibility stems from the behavior of conjecture (3.1) under change of base field. Let L be a finite Galois extension of F.

Denote by E_L the elliptic curve obtained by considering E over L and let $N_{L/F}$ be the norm map on fields.

PROPOSITION 3.4: *Let L be an odd degree Galois extension of F. Then $\epsilon(E, \omega) = \epsilon(E_L, \omega \circ N_{L/F})$.*

PROOF: Since the Galois groups of local fields are solvable, it suffices to treat the case L/F cyclic of odd order. Notice that $\sigma_{E_L} = \operatorname{Res}^{W_F}_{W_L} \sigma_E$. Since restriction is adjoint to induction, we can use the fact that ϵ factors are inductive in degree zero to compute the effect of restriction. We have

$$\epsilon(\operatorname{Ind}^{W_F}_{W_L}(\sigma\text{-dim}\ \sigma \cdot 1), \psi, dx_F) = \epsilon(\sigma\text{-dim}\ \sigma \cdot 1, \psi \circ \operatorname{tr}_{L/F}, dx_L).$$

Thus $\epsilon(\operatorname{Ind} \sigma, \psi, dx_F) = \epsilon(\sigma, \psi \circ \operatorname{tr}_{L/F}, dx_L)\lambda_{L/F}^{\dim \sigma}$ where $\lambda_{L/F} = \epsilon(\operatorname{Ind}^{W_F}_{W_L} 1, \psi, dx_F)/\epsilon(1, \psi \circ \operatorname{tr}_{L/F}, dx_L)$. When this is applied to $\sigma = \operatorname{Res}(\sigma_E)$ we obtain

$$\epsilon(\operatorname{Res} \sigma_E, \psi \circ \operatorname{tr}, dx_L) = \epsilon(\sigma_E, \psi, dx) \cdot \prod_{\chi \neq 1} \frac{\epsilon(\sigma_E \otimes \chi, \psi, dx)}{\epsilon(\chi, \psi, dx)^2} \lambda_{L/F}^2$$

where χ runs over the characters of G. By (2.1.5) and (2.1.6)

$$\epsilon(\sigma_E \otimes \chi, \psi, dx)\, \epsilon(\sigma_E \otimes \chi^{-1}, \psi, dx) = \chi^2(-1) = 1$$

and $\epsilon(\chi, \psi, dx)^2\ \epsilon(\chi^{-1}, \psi, dx)^2$ and $\lambda_{L/F}^2$ are positive. Since $[L:F]$ is odd, χ and χ^{-1} are distinct for nontrivial χ. Thus, $\epsilon(\operatorname{Res} \sigma_E, \psi \circ \operatorname{tr}_{L/F}, dx_L) = \epsilon(\sigma_E, \psi, dx)$. The same reasoning applied to $\sigma_E \otimes \omega$ shows that $\epsilon(\operatorname{Res} \sigma_E\omega, \psi \circ \operatorname{tr}_{L/F}, dx_L) = \epsilon(\sigma_E\omega, \psi, dx)$. Thus $\epsilon(E_L, \omega \circ N_{L/F}) = \epsilon(E, \omega)$.

The final theorem of this section is an analogous result for $\kappa(E, \omega)$. Notice that $\omega \cdot N_{L/F}(-\Delta) = \omega(-\Delta)^{[L:F]} = \omega(-\Delta)$ when $[L:F]$ is odd.

PROPOSITION 3.5: *Let L be an odd degree Galois extension of F. Then $\kappa(E, \omega) = \kappa(E_L, \omega \circ N_{L/F})$.*

PROOF: As before it suffices to treat the case that L is cyclic over F with Galois group G. The result is obvious if ω is trivial, so assume that ω is the quadratic character corresponding to the quadratic extension K. Consider the $\mathbb{F}_2[G]$-module $V = E(L)/\mathbb{N}E(KL)$. There is a norm map from $E(L)$ to $E(F)$ which induces a surjective map $\mathbb{N}^*$ of V to $E(F)/\mathbb{N}E(K)$ (since $[L:F]$ is odd). After tensoring with the algebraic closure $\bar{\mathbb{F}}_2$, we see that $V \otimes \bar{\mathbb{F}}_2$ is a direct sum of characters of the odd order group G, and the kernel of $\mathbb{N}^*$ is the direct sum of the nontrivial characters. Since V is an $\mathbb{F}_2[G]$-module, the character has values in $\mathbb{F}_2$. By linear independence of characters, this means that the kernel of $\mathbb{N}^*$ is even dimensional (if χ is nontrivial, the multiplicities of χ and χ^{-1} in $V \otimes \mathbb{F}_2$ have the same parity). Hence the dimension of $E(F)/\mathbb{N}E(K)$ is congruent modulo two to $\dim_{\mathbb{F}_2}(E(L)/\mathbb{N}E(LK))$.

REMARK: A further compatibility involves isogeny. Conjecture 3.1 predicts that $\omega(-\Delta_E)\kappa(E, \omega)$ is an isogeny invariant (since σ_E is). When E is replaced by a curve isogenous to E by an odd degree isogeny this is straightforward: the norm index remains the same, and odd isogenies do not alter the quadratic nature of the discriminant. An even isogeny may alter both the norm index and quadratic nature of Δ. Thus (3.1) predicts a factorization of the isogeny invariant $\epsilon(E, \omega)$ into the product of two geometric, but not isogeny invariant factors.

4. The case of potential multiplicative reduction.

In this section conjecture 3.1 is proved when E has potential multiplicative reduction over a nonarchimedean field F [16; §6]. The group of points of E in a separable closure F_s of F is isomorphic to $(F_s)^*/q^Z$, where q is an element of the prime ideal of the ring of integers of F. The action of $G_F = \mathrm{Gal}(F_s/F)$ on $E(F_s)$ is described by a homomorphism χ of G_F to $\mathrm{Aut}(E) \approx \{\pm 1\}$. Then E becomes a Tate curve over the quadratic extension L stabilized by the kernel of χ. When P in $E(F_s)$ is represented by x in F_s^*, the image $g(P)$ for g in G_F is represented by $g(x)^{\chi(g)}$.

Recall that $\Delta_E = q \prod_{n=1}^{\infty} (1-q^n)^{24}$, so that Δ/q is a square [16; §6].

For the remainder of this section let E be an elliptic curve over F with potential multiplicative reduction which becomes a Tate curve over the quadratic extension L (we take $L = F$ if E is a Tate curve over F). Let ω be a nontrivial quadratic character of F^* with corresponding quadratic extension K.

PROPOSITION 4.1: *If $LK = K$, then $E(F)/\mathbb{N}E(K)$ has order at most 2. Further, in this case $\kappa(E, \omega) = -\omega(q)$.*

PROOF: The description above shows that $E(K) \approx K^*/q^Z$ and $E(F) \approx \{z \in K^* \mid g(z) = z^{\chi(g)} q^i$ for all $g \in G_F$, some $i \in \mathbb{Z}\}/q^Z$. Alternately, $E(F)$ may be described as the elements of K^* with $g(z) \cdot z^{-\chi(g)}$ a power of q, modulo $q^{\mathbb{Z}}$. The norm map from $E(K)$ is represented by $z \mapsto z \cdot g(z)^{\chi(g)}$, where g generates $\mathrm{Gal}(K/F)$. If χ is trivial, this is the usual norm and the result is clear. If χ is nontrivial, let $E(F)' = \{z \in \mathcal{O}_K^* \mid N_{K/F}z = 1\}$. Then $E(F)' \hookrightarrow E(F)$ and Hilbert's Theorem 90 shows that $\mathbb{N}E(K) = E(F)'$. Hence $E(F)/\mathbb{N}E(K) = E(F)/E(F)'$. The latter group is cyclic, generated by an element $x \in K^*$ such that $N_{K/F}(x)$ is 1 or q. It is easy to see that $E(F)/E(F)'$ has order 2 if q is a norm from K^*, and has order 1 otherwise. This establishes the proposition.

We now consider the case that LK has degree 4 over F. In this case

$$E(K) = \{z \in (LK)^* \mid N_{LK/K}z \in q^{\mathbb{Z}}\}/q^{\mathbb{Z}}$$

$$E(F) = \{z \in L^* \mid N_{L/F}z \in q^{\mathbb{Z}}\}/q^{\mathbb{Z}}.$$

The norm map from $E(K)$ to $E(F)$ is represented by $N_{KL/L}$. Let $E(F)'$ be the subgroup $\{z \in L^* \mid N_{L/F}z = 1\}$ of $E(F)$.

Lemma 4.2: $\mathbb{N}(E(K)) \subset E(F)'$.

Proof: Let x in $(LK)^*$ represent a point P of $E(K)$. Then $\mathbb{N}(P)$ is represented by $N_{LK/L}(x)$. Since x represents a point of $E(K)$ we have $N_{LK/K}(x) = q^i$ for some i. Hence $N_{L/F}(N_{KL/L}(x)) = q^{2i}$, which implies that $N_{KL/L}(x)/q^i$ has norm 1 to F, and so $N_{KL/L}(x)$ is in $E(F)'$.

Proposition 4.3: *With notation as above, when LK has degree* 4 *over F the order of* $E(F)/\mathbb{N}E(K)$ *divides* 4. *Further,* $\kappa(E, \omega) = \omega(q)$.

Proof: We first note that $E(F)/E(F)'$ has order dividing 2, and is a nontrivial group if and only if q is a norm from L (that is, if and only if $\chi(q) = 1$).

To determine $E(F)'/\mathbb{N}E(K)$ we consider $E(K)' = \{z \in (LK)^* \mid N_{LK/K}(z) = 1\} \subset E(K)$. Denote the generator of $\mathrm{Gal}(LK/K)$ by h, so that $E(K)' = \{x/h(x) \mid x \in (LK)^*\}$. Then $\mathbb{N}E(K)' = \{N_{LK/L}(x)/h \cdot N_{LK/L}(x) \mid x \in (LK)^*\}$. By Theorem 90 and the fact that $N_{LK/L}(LK)^*$ has index 2 in L^* we see that $\mathbb{N}E(K)'$ has index 2 in $E(F)'$. To determine $E(F)'/\mathbb{N}E(K)$ we note that $\mathbb{N}E(K) = \mathbb{N}E(K)'$ unless there exists an element z of $(LK)^*$ such that $N_{LK/K}(z) = q$ and $N_{LK/L}(z) = q\, y/hy$ for some y in L^* which is not a norm from LK.

Notice that if $y = N_{LK/L}(u)$, then $N_{LK/K}(z \cdot u/hu) = q$ and $N_{LK/L}(z \cdot u/hu) = q$, so that $q = z'h(z') = z'g(z')$ with $z' = zu/hu$. Hence $gh(z') = z'$ and $\omega\chi(q) = 1$. Conversely, if $\omega\chi(q) = 1$, $q = N_{KL/K}(z') = N_{KL/L}(z')$ for some z' fixed by gh. Then y is a norm from LK.

Thus $E(F)'/\mathbb{N}E(K)$ has order 1 or 2, and is trivial if and only if $\omega\chi(q) = -1$. Together with the first sentence of the proof this proves the claim.

THEOREM 4.4: *Let E be an elliptic curve over F with potential multiplicative reduction. Then $\epsilon(E, \omega) = \omega(-\Delta_E)\kappa(E, \omega)$.*

PROOF: The claim is true if $\omega = 1$. When ω is nontrivial and $\chi = \omega$ or $\chi = 1$ Proposition 4.1 applies to show that $\kappa(E, \omega)\omega(-\Delta) = -\omega(-1)$. Otherwise, 4.3 applies to show $\kappa(E, \omega)\omega(-\Delta) = \omega(-1)$. All that remains is to check the theorem using Proposition 2.5. We need only to notice that the unramified quadratic character has value -1 on a uniformizer to verify the result.

5. The case of potential good reduction in odd residue characteristic

Conjecture 3.1 has been established for archimedean fields and also for curves with potential multiplicative reduction. For this section only we assume that E is an elliptic curve with potential good reduction over a nonarchimedean field F with odd residue characteristic. This means that the image of the inertia subgroup in the ℓ-adic representation on the Tate module is finite [15; §2]. Since the residue characteristic is odd, we may utilize the representation of $\mathrm{Gal}(F_s/F)$ on the 2-adic Tate space $V_2(E)$. Let K be a quadratic extension of F, with corresponding quadratic character ω. Let $\lambda(E, \omega)$ equal $(-1)^d$, where d is the $\mathbb{F}_2$-dimension of the group $E(K)_2$ of elements of $E(K)$ of order dividing 2. In the first part of this section we show that $\epsilon(E, \omega) = \omega(-\Delta)\lambda(E, \omega)$. Proposition 5.11 will show that $\lambda(E, \omega) = \kappa(E, \omega)$ for curves with potential good reduction over fields of odd residue characteristic.

Let ρ be the representation of W_F on the 2-adic Tate module $T_2(E)$. Choose a basis to identify $\mathrm{Aut}(T_2(E))$ and $GL(2, \mathbb{Z}_2)$.

LEMMA 5.1: *The image $\rho(I)$ of the inertia subgroup in $GL(2, \mathbb{Z}_2)$ satisfies*

$$\rho(I) \cap (1 + 2M_2(\mathbb{Z}_2)) \subset \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

PROOF: The subgroup $1 + 4M_2(\mathbb{Z}_2)$ of $GL(2, \mathbb{Z}_2)$ contains no elements of finite order [15; pg. 479]. Thus $\rho(I)$ injects into

$GL(2, \mathbb{Z}_2)/1 + 4M_2(\mathbb{Z}_2)$. The elements of the 2-group $\rho(I) \cap (1 + 2M_2(\mathbb{Z}_2)/1 + 4M_2(\mathbb{Z}_2))$ are conjugate in $GL(2, \bar{\mathbb{Q}}_2)$ to matrices $\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$, with α and β equal to ± 1. Since $\det(\rho)$ is trivial on I, the elements of this 2-group must be scalars.

Let $\bar{\rho}$ denote the modulo 2 reduction of ρ, considered as a homomorphism of W_F to $GL(2, \mathbb{F}_2)$. Let q be the number of elements in the residue field k_F.

Lemma 5.2: *Suppose that $\rho(I)$ is cyclic.*

(a) *If $\bar{\rho}(I)$ is trivial, then σ_E is a reducible representation of W_F.*

(*b*)*If $\bar{\rho}(I)$ has order* 2, *then σ_E is a reducible if and only if $q \equiv 1$* (*modulo* 4).

Proof: The previous lemma shows that $\rho(I) \cap 1 + 2M_2(\mathbb{Z}_2)$ is central in $GL(2, \mathbb{Z}_2)$. In the case that $\bar{\rho}(I)$ is trivial, $\bar{\rho}(I) \subset 1 + 2M_2(\mathbb{Z}_2)$, so the image of I is central, and $\rho(W_F)$ is abelian. Thus σ_E has abelian image, and so is reducible.

When $\bar{\rho}(I)$ has order 2, $\rho(I)$ is a cyclic group contained in $GL(2, \mathbb{Z}/4\mathbb{Z})$ with modulo 2 reduction of order 2. All such groups have order 4. When σ_E is reducible, then in $GL(2, \bar{\mathbb{Q}}_2)$ the image of ρ is conjugate to diagonal matrices $\begin{pmatrix} \mu & 0 \\ 0 & \nu \end{pmatrix}$. The entries μ, ν are characters of W_F with values in $\bar{\mathbb{Q}}_2^*$ such that $\mu\nu$ is trivial on I. Hence $\rho(I)$ is a quotient of $\mathcal{O}_F^*/(1 + \mathcal{P}_F^i)$ for some i, and thus $\rho(I)$ has order dividing $(q-1)q^\infty$. Since q is odd, σ_E reducible implies that 4 divides $(q-1)$.

When σ_E is irreducible and $\rho(I)$ is cyclic there is a subgroup $H \subset W_F$ of index 2 such that $I \subset H$ and $\rho(H)$ is reducible. By Frobenius reciprocity ρ is induced from a 1-dimensional representation θ of H. By class field theory, $\rho(I)$ is a subquotient of $\mathcal{O}_L^*/(1 + \mathcal{P}_L^i)$ for some i, where L is the quadratic unramified extension of F. Since $\det \rho$ is trivial on I we see that θ is trivial on $\mathcal{O}_F^*$. Thus the order of $\rho(I)$ divides $(q+1)q^\infty$, a multiple of the order of $\mathcal{O}_L^*/\mathcal{O}_F^*(1 + \mathcal{P}_L^*)$. Thus σ_E irreducible implies that $(q+1)$ is divisible by 4.

In subsequent proofs it will be convenient to make an odd Galois extension L of F and work over L. The following proposition is analogous to (3.4) and (3.5).

Proposition 5.3: *Let E be an elliptic curve over a local field F. Let L be an odd degree Galois extension of F. Then $\lambda(E, \omega) = \lambda(E_L, \omega \circ N_{L/F})$ for each nontrivial quadratic character ω.*

PROOF: It suffices to notice that $\lambda(E, \omega) = -1$ if and only if $E(K)_2$ has order 2, where K corresponds to ω. Also $E(K)_2$ has order 2 if and only if $\bar{\rho}(W_K)$ has order 2. Since W_{LK} is a normal subgroup of odd index in W_K, $\bar{\rho}(W_K)$ has order 2 if and only if $\bar{\rho}(W_{LK})$ has order 2, that is if and only if $\lambda(E_L, \omega \circ N_{L/F}) = -1$.

LEMMA 5.4: *Suppose that $\bar{\rho}(I)$ is trivial. Then $\omega(-\Delta_E)\lambda(E, \omega) = \omega(-1)$.*

PROOF: By (5.3) we may make a degree 3 Galois change of base if necessary, and so we may assume $\bar{\rho}(W_F)$ has order dividing 2. The discriminant $\Delta = \Delta_E$ is a square if and only if $\bar{\rho}(W_F)$ is trivial, in which case $E(K)_2$ has 4 elements. If Δ is a nonsquare, $E(F(\sqrt{\Delta}))_2$ has four elements while $E(F)_2$ has 2. Since $\bar{\rho}$ is trivial on the inertia group I, $F(\sqrt{\Delta})$ is unramified. If K is unramified $K = F(\sqrt{\Delta})$ and $\omega(-\Delta)\lambda(E, \omega) = 1$. If K is ramified, ω is a tamely ramified character and $\omega(-\Delta) = -\omega(-1)$. Then $E(K)_2$ has 2 elements and $\omega(-\Delta)\lambda(E, \omega) = \omega(-1)$.

LEMMA 5.5: *Let $\bar{\rho}(W_F)$ be abelian, and $\bar{\rho}(I)$ of order 2. Then $\omega(-\Delta_E)\lambda(E, \omega) = 1$.*

PROOF: The discriminant Δ of E is not a square since the image of $\bar{\rho}$ is not in the alternating subgroup $A_3 \subset GL(2, \mathbb{F}_2)$. Since $\bar{\rho}(W_F)$ is an abelian subgroup of even order in S_3, it has order 2. Then $E(F(\sqrt{\Delta}))$ has order 4. For the quadratic unramified extension L (which is distinct from $F(\sqrt{\Delta})$ since $\bar{\rho}(I)$ is nontrivial) and the other quadratic extension M of F we have the following values:

K	$\omega(-\Delta)$	$\lambda(E, \omega)$
$F(\sqrt{\Delta})$	1	1
L	-1	-1
M	-1	-1

The lemma now follows.

THEOREM 5.6: *Let E be an elliptic curve over a local field of odd residue characteristic. Let K be a quadratic extension of F with character ω. Assume that $\rho(H)$ is abelian, where H is the unique index* *two subgroup of W_F containing I. Then*

$$\omega(-\Delta_E)\lambda(E,\omega)=\begin{cases}\omega(-1) & \sigma_E \textit{ reducible}\\ 1 & \omega \textit{ unramified}\\ -\omega(-1) & \sigma_E \textit{ irreducible and } \omega \textit{ ramified.}\end{cases}$$

Proof: Under the hypotheses $\rho(I)$ is diagonalizable in $GL(2,\bar{\mathbb{Q}}_2)$, and hence cyclic since the determinant of ρ is trivial on I. We distinguish two cases.

Case 1. The group $\bar{\rho}(W_F)$ is cyclic. By passing to the field stabilized by the 3-Sylow subgroup of $\bar{\rho}(W_F)$ we may assume $\bar{\rho}(W_F)$ has order 1 or 2, and (5.3) shows that $\omega(-\Delta_E)\lambda(E,\omega)$ is unchanged.

If $\bar{\rho}(I)$ is trivial, Lemma 5.2a shows that σ_E is reducible and $\omega(-\Delta)\lambda(E,\omega)$ equals $\omega(-1)$ by (5.4).

If $\bar{\rho}(I)$ has order 2, Lemma 5.2b shows that σ_E is reducible if and only if $q\equiv 1$ (modulo 4). By (5.5) $\omega(-\Delta)\lambda(E,\omega)=1$.

Case 2. The group $\bar{\rho}(W_F)$ is $GL(2,\mathbb{F}_2)$, in which case $\bar{\rho}(I)$ must be the unique subgroup of order 3. Clearly σ_E is irreducible in this case, since $\rho(W_F)$ has a nonabelian quotient. The field stabilized by the inverse image of $\bar{\rho}(I)$ in W_F is the quadratic unramified field $F(\sqrt{\Delta})$. Since I stabilizes $F(\sqrt{\Delta})$, $\omega(\Delta)=-1$ for each ramified quadratic character ω. For each quadratic extension K of F, $E(K)_2$ has order 1. Thus $\omega(-\Delta)\lambda(E,\omega)=1$ or $-\omega(-1)$ according to whether ω is unramified or ramified.

The theorem now follows by checking the two cases and recalling that a ramified quadratic character takes value 1 at -1 if and only if $q\equiv 1$ (modulo 4).

Corollary 5.7: *Suppose that σ_E is reducible when restricted to the index two subgroup H of W_F stabilizing the quadratic unramified extension. Then $\epsilon(E,\omega)=\omega(-\Delta_E)\lambda(E,\omega)$.*

Proof: The previous theorem applies to this situation. Notice that the exponent of the Artin conductor of σ_E is even, since $a(\sigma_E)=a(\mathrm{Res}_H\sigma_E)=a(\mu\oplus\nu)$, while $\mu\nu=\det\sigma_E\,|_H$ is unramified, so $a(\mu)=a(\nu)$. Further, if σ_E is irreducible and the restriction to H is reducible, σ_E is induced from a character of H. Statements (2.4) and (2.7) prove the claim of the theorem.

The only remaining case to consider is the case that σ_E is irreducible when restricted to the unique index two subgroup containing I.

Since the residue characteristic is odd, σ_E is induced from the subgroup W_L for some quadratic ramified extension L [4; (3.14)]. Then $\rho(I)$ is nonabelian, so that $\bar{\rho}(I)$ is not cyclic ($\bar{\rho}(I)$ is the quotient of $\rho(I)$ by the central subgroup $\rho(I) \cap (1 + 2M_2(\mathbb{Z}_2))$). Hence Δ is not a square in F^*, and $F(\sqrt{\Delta})$ is ramified and equal to L, since $\rho(W_L)$ is abelian. Let F_{nr}, $F(\sqrt{\Delta})$ and M be respectively the unramified quadratic extension of F and the remaining two quadratic extensions of F. Then

$$\omega_K(-\Delta)\lambda(E, \omega_K) = \begin{cases} 1 & K = F(\sqrt{\Delta}) \\ -1 & K = F_{nr} \quad \text{or } K = M. \end{cases}$$

Since σ_E is induced from $W_{F(\sqrt{\Delta})}$, we have $\sigma_E \approx \sigma_E \otimes \omega_{F(\sqrt{\Delta})}$, so $\epsilon(E, \omega_{F(\sqrt{\Delta})}) = 1$. By (2.4c) $\epsilon(E, \omega_{F_{nr}}) = (-1)^{a(\sigma_E)}$ and

$$\epsilon(E, \omega_M) = \epsilon(E, \omega_{F(\sqrt{\Delta})}\omega_{F_{nr}}) = \epsilon(E^{\omega_{F(\sqrt{\Delta})}}, \omega_{F(\sqrt{\Delta})})\epsilon(E, \omega_{F_{nr}}) = (-1)^{a(\sigma_E)}.$$

Proposition 5.8: *If σ_E is irreducible, but not induced from the subgroup stabilizing the quadratic unramified extension, then $a(\sigma_E)$ is odd, greater than* 2. *Thus,* (3.1) *is true in this case.*

Proof: The exponent of the Artin conductor of $\sigma_E = \operatorname{Ind}_{W_L}^{W_F} \theta$ is $a(\theta) + 1$ [14; VI§2, Prop. 4]. Since $\det \sigma_E = \|\ \ \|$, $\theta|_{K^*} = \omega_L\|\ \ \|$ [5; Prop. 1.2]. Thus θ is trivial on $(1 + \mathcal{P}_F)$. Since L is ramified, $(1 + \mathcal{P}_F)(1 + \mathcal{P}_L^{2j+1}) = (1 + \mathcal{P}_F)(1 + \mathcal{P}_L^{2j})$ for $j > 0$. Thus if $a(\theta) > 0$, we have that $a(\theta)$ is even, and hence $a(\sigma_E)$ is odd.

In the case $a(\theta) = 1$ ($a(\theta) = 0$ is impossible since irreducible representations have Artin conductor exponents at least equal to their dimensions) we let $\operatorname{Gal}(L/F) = \langle h \rangle$. Then θ^{h-1} is an unramified quadratic character (since $\theta|_{K^*} = \omega_L\|\ \ \|$). Thus $\sigma_E \otimes \omega \approx \sigma_E$ where ω is quadratic unramified. This would imply that σ_E was induced from the subgroup stabilizing the quadratic unramified extension, contrary to assumption. Thus, $a(\sigma_E)$ is odd and at least 3 under the hypotheses of the theorem.

Remark: The situation of (5.8) can only occur in residue characteristic 3 (or 2, if even residue characteristic is allowed). It is well known that conductor exponents for elliptic curves are less than or equal to 2 for residue characteristics 5 or greater.

For elliptic curves E having potential good reduction we need to know that $\dim E(F)/\mathbb{N}E(K) \equiv \dim E(K)_2 \pmod 2$ if $\operatorname{char}(k_F) \neq 2$. To prepare for the proof of this fact, we recall the following filtration on

$E(F)$. Let E_0 be the connected component of the identity in the Néron model for E over $\mathcal{O}_F$. Then $E(F)/E_0(F)$ is a finite group and $E_0(F)$ corresponds to the points having non-singular reduction in a minimal generalized Weierstrass model for E over $\mathcal{O}_F$ [17; p. 41]. Let $E_1(F)$ be the kernel of reduction, so that it fits into the exact sequence:

$$0 \to E_1(F) \to E_0(F) \to \bar{E}_0(k_F) \to 0$$

where $\bar{E}_0$ denotes the reduction of E_0. There is a formal group structure on the prime ideal $\mathcal{P}_F$ giving rise to an isomorphism $\mathcal{P}_F \to E_1(F)$. In particular $E_1(F)$ is uniquely divisible by 2 if $\operatorname{char}(k_F) \neq 2$.

Lemma 5.9: *Let ω be a quadratic character of F^* corresponding to the extension K/F. Suppose that E has potential good reduction over F and good reduction over K. Then E or E^ω has good reduction over F.*

Proof: Since E attains good reduction over the quadratic extension K, the image of inertia has order at most 2 in the ℓ-adic representation ($\ell \neq$ residue characteristic). If the image of inertia is nontrivial, then the ℓ-adic representation on E^ω is trivial on inertia. This proves the result.

Lemma 5.10: *Suppose that* $\operatorname{char}(k_F) \neq 2$. *Then E has reduction of Kodaira type I_ν^* over F, with $\nu > 0$, if and only if for each ramified quadratic character ρ of F^* there is a curve $\mathscr{E}$ with reduction of type I_ν over F such that $E = \mathscr{E}^\rho$.*

Proof: Choose a prime π of F such that $\pi^{1/2}$ generates the quadratic extension corresponding to ρ. Suppose that E has reduction of type I_ν^* over F. Choose a minimal model for E over F in generalized Weierstrass from (7.0.1) satisfying the conditions $\pi \mid a_1$, $\pi \mid a_2$, $\pi^2 \mid a_3$, $\pi^3 \mid a_4$, $\pi^4 \mid a_6$ of Tate's algorithm [17, case 7]. By a translation of y, we obtain the model

$$E:\ y^2 = x^3 + \tfrac{1}{4}b_2x^2 + \tfrac{1}{2}b_4x + \tfrac{1}{4}b_6 \tag{5.10.1}$$

with b_i as in [17, p. 36]. Now $\pi \mid b_2$, $\pi^2 \mid b_4$, $\pi^4 \mid b_6$. Let $\mathscr{E}$ be the curve with b_i replaced by $b_i' = b_i\pi^{-1/2i}$. The algorithm [17, case 2] shows that $\mathscr{E}$ has multiplicative reduction, type $I_{\nu'}$. To see that in fact $\nu = \nu'$, recall that $a_F(\mathscr{E}) = 1$. Hence $a_F(E) = \max\{a_F(\mathscr{E}), 2a(\rho)\} = 2$. Let Δ_E and $\Delta_{\mathscr{E}}$

denote the discriminant of E and $\mathscr{E}$. By the algorithm, these discriminants are minimal and by [17, p. 38, (2.3)] $\Delta_E = \Delta_{\mathscr{E}}\pi^6$. Now the conductor-discriminant formula [13] shows that $v_F(\Delta_E) = 6 + \nu$ while $v_F(\Delta_{\mathscr{E}}) = v'$. Hence $\nu = \nu'$.

The converse can be treated similarly, as can the case $\nu = 0$. We do not use this information later on.

REMARK: If $\operatorname{char}(k_F) = 2$, curves of type I_ν^* need not have potential multiplicative reduction. Consider for example the curve $y^2 = x^3 - x^2 - 4x + 4$ of conductor 24 over $\mathbb{Q}$ and type I_1^* over $\mathbb{Q}_2$ (see [2, p. 83]). It has integral j-invariant $j = 2^4 \cdot 13^3 \cdot 3^{-2}$ over $\mathbb{Q}_2$.

PROPOSITION 5.11: *Suppose that E has potential good reduction over F, with* $\operatorname{char}(k_F) \neq 2$. *Let K be a quadratic extension of F. Then* $\dim E(F)/\mathsf{N}E(K) \equiv \dim E(K)_2 (\operatorname{mod} 2)$.

PROOF: Suppose first that E has good reduction over K. By Lemma 5.9 and symmetry, Proposition 3.3, we may assume that E has good reduction over F. In particular, the minimal discriminant Δ of E is a unit. If K/F is unramified, Δ therefore is a square in K and $\dim E(K)_2$ must be even. By [11, Corollary 4.4] $E(F)/\mathsf{N}E(K)$ is trivial as desired. If K/F is ramified, then by [11, Corollary 4.6] and the fact that N: $E_1(K) \to E_1(F)$ is surjective because E_1 is divisible by 2, $E(F)/\mathsf{N}E(K)$ is isomorphic to $\bar{E}(k_F)/2\bar{E}(k_F)$. Hence $\dim E(F)/\mathsf{N}E(K) = \dim \bar{E}(k_F)_2$. But the 2-division field of E is unramified because E has good reduction and $\operatorname{char}(k_F) \neq 2$. Hence $\bar{E}(k_F)_2 \approx E(F)_2 = E(K)_2$ as desired.

Next suppose that E has potential good reduction, but not good reduction over K. Then $E_0(K)/E_1(K) \approx k_K$. Since $E_1(K)$ is uniquely divisible by 2, so is $E_0(K)$. Let M be the subgroup of $E(K)$ generated by $E_0(K)$ and representatives for the cosets of odd order in $E(K)/E_0(K)$. Since the curve E has additive reduction over K, not type I_ν^* with $\nu > 0$, the table of possibilities [17, p. 46] shows that $E(K)/E_0(K)$ is annihilated by 2. Hence $E(K)_2 \approx E(K)/M$. Let $G = \operatorname{Gal}(K/F)$. In reduced Galois cohomology we have $H^i(G, M) = 0$. Hence $E(F)/\mathsf{N}E(K) \approx H^0(G, E(K)) \approx H^0(G, E(K)_2) \approx E(F)_2/\mathsf{N}E(K)_2$. We have the exact sequence:

$$0 \to E^{\omega}(F)_2 \to E(K)_2 \to E(F)_2 \to E(F)_2/\mathsf{N}E(K)_2 \to 0.$$

But $E^{\omega}(F)_2 \approx E(F)_2$. Hence $\dim E(F)_2/\mathsf{N}E(K)_2 \equiv \dim E(K)_2 \pmod 2$ as desired.

6. Unramified extensions.

Let E be an elliptic curve having minimal discriminant Δ over the local field F, with finite residue field k_F. Let K/F be an unramified quadratic extension with corresponding character ω. We now verify conjecture (3.1) that $\epsilon(E, \omega) = \omega(-\Delta)(-1)^{\dim E(F)/\mathsf{N}E(K)}$. In view of the previous section, we could assume that $\mathrm{char}(k_F) = 2$. However, we present a uniform proof.

Let E_0 be the connected component of the identity in the Neron minimal model for E. It follows from Lang's theorem [9] that N: $E_0(K) \to E_0(F)$ is surjective. Let X be the 2-Sylow subgroup of $E(K)/E_0(K)$. Let $G = \mathrm{Gal}(K/F)$. Then

$$E(F)/\mathsf{N}E(K) \approx H^0(G, E(K)) \approx H^0(G, E(K)/E_0(K)) \approx H^0(G, X).$$

Lemma 6.1: *Let M be the maximal unramified extension of F and let n be the number of components in the singular fiber of E over M. Then* $\dim E(F)/\mathsf{N}E(K) \equiv n - 1 \pmod 2$.

Proof: The table [17, p. 46] gives n and $c = |E(M)/E_0(M)|$. For reductions of type I_0, I_ν with $v_F(\Delta) = \nu$ odd, II, II*, IV, IV*, c is odd and n is odd. Since X must be trivial, $\dim E(F)/\mathsf{N}E(K) = 0$. Hence $\dim E(F)/\mathsf{N}E(K) \equiv n - 1 \pmod 2$.

For reduction of type III or III*, $X \approx \mathbb{Z}/2\mathbb{Z}$ and n is even. Hence $\dim H^0(G, X) = 1 \equiv n - 1$ as desired. For reduction of type I_ν, $E(K)/E_0(K) \approx \mathbb{Z}/n\mathbb{Z}$ and $\nu = n = v_M(\Delta) = v_F(\Delta)$. Moreover, if we choose for E the curve which has rational tangents at the node in its reduction over k_F and for E^ω the unramified twist of E over F, as we may do without changing the norm index by Proposition 3.3, then the points of E/E_0 already are rational over F. Hence G acts trivially on X and $H^0(G, X) \approx X/2X$. Then $\dim E(F)/\mathsf{N}E(K) = \dim X \equiv n - 1$ (mod 2).

Next consider type I_ν^* for $\nu \geq 0$. If ν is odd, the points of E/E_0 may not be defined over F, but certainly are over K. Hence $X = \mathbb{Z}/4\mathbb{Z}$. Then G acts either trivially or by inversion. Hence $H^0(\mathfrak{G}, X) \approx \mathbb{Z}/2\mathbb{Z}$. Furthermore $n = 5 + \nu$ is even, as desired. If ν is even, X is annihilated by 2. Let g generate G. Then $g - 1 = g + 1$ on X. Hence $\dim H^0(G, X) = \dim[\mathrm{Kernel}\, g - 1] - \dim[\mathrm{Image}\, g - 1] \equiv \dim X \pmod 2$. If $\nu > 2$, all of E/E_0 need not be defined over F, but is defined over K. Hence $X = \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$ is even dimensional. If $\nu = 0$, then $|X| = 1 +$ number of roots of a cubic. The cubic is defined over F and has distinct roots in M. Hence its discriminant is a square in K and

$|X| = 1$ or 4. Again $\dim X$ is even. Furthermore $n = 5 + \nu$ is odd, as desired.

THEOREM 6.2: *Let ω be the unramified quadratic character of F. Then $\epsilon(E, \omega) = \omega(-\Delta) \cdot \kappa(E, \omega)$.*

PROOF: By the previous Lemma, $\kappa(E, \omega) = (-1)^{n-1}$, where n is the number of connected components of the Néron fibre. From (2.4.c), $\epsilon(E, \omega) = (-1)^{a(\sigma_E)}$. The value of $\omega(-\Delta)$ is $(-1)^{v(\Delta)}$. The theorem then follows from the Ogg relation [13] between the conductor and discriminant:

$$v(\Delta) = n + a(\sigma_E) - 1.$$

REMARK: The theorem depends on the validity (modulo 2) of Ogg's conductor relation. In [13] the proof of this relation is given for odd residue characteristic and the case when F has characteristic 2.

7. The norm index and the Néron model

Let E be an elliptic curve defined over a local field F with finite residue field k_F, ring of integers $\mathcal{O}_F$ and maximal ideal $\mathcal{P}_F$. Let v_F be the additive valuation of F. Let K be a quadratic extension of F. The object of this section is to express the norm index $E(F)/\mathbb{N}E(K)$ in terms of information available from the Néron model.

Let E_0 be the connected component of the identity in the Néron minimal model for E over $\mathcal{O}_F$ and let $\bar{E}_0$ denote the reduction over k_F. We may identify $E_0(F)$ with the group of points on a minimal generalized Weierstrass model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{7.0.1}$$

for E over $\mathcal{O}_F$ with non-singular reduction. For $n > 0$ we have the filtration $E_n(F)$ consisting of the zero element together with $\{(x, y) \in E_0(F) \mid v_F(x) \leq -2n\}$.

It will be convenient for us to work with the same filtration on a possibly non-minimal model A for E over $\mathcal{O}_F$. The following lemma gives the relation between the two models. Those aspects not explicitly mentioned in [16] are clear.

LEMMA 7.1: (1) *There is an isomorphism for Weierstrass models*

$E(F) \to A(F)$ given by $(x', y') \to (x, y)$ with $x = u^2x' + r$, $y = u^3y' + su^2x' + t$ and u, r, s, $t \in \mathcal{O}_F$. Let $\Delta_F(E)$ be the (minimal) discriminant of E and Δ the discriminant of A. Then $\Delta = u^{12}\Delta_F(E)$. For future use, write $u = u_F(E, A)$.

(2) *For $n \geqslant 1$, both $A_n(F)/A_{n+1}(F)$ and $E_n(F)/E_{n+1}(F)$ are isomorphic to k_F. Furthermore $E(F)/E_{n+v_F(u)}(F) \approx A(F)/A_n(F)$.*

(3) $|A(F)/A_n(F)| = |E(F)/E_0(F)| \cdot |\bar{E}_0(k_F)| \cdot |k_F|^{n+v_F(u)-1}$.

We shall study the norm mapping N on the filtration A_n. To do so we need some information on the trace map Tr: $\mathcal{O}_K \to \mathcal{O}_F$, especially for use when K/F is ramified and $\mathrm{char}(k_F) = 2$. However, we give a uniform description of the situation. For the moment we assume only that K/F is a separable, finite extension of local fields with finite residue fields.

LEMMA 7.2: *Let K/F be a finite, separable extension of local fields and let $\mathcal{D}$ be the corresponding different ideal. Let $\alpha = v_k(\mathcal{D})$. Define $\psi(n)$ by* $\mathrm{Tr}(\mathcal{P}_K^n) = \mathcal{P}_F^{\psi(n)}$. *Then $\psi(n) = \left[\dfrac{n+\alpha}{e(K/F)}\right]$ where $e(K/F)$ is the ramification index of K/F and $[\quad]$ is the greatest integer function.*

PROOF: Clearly $\mathrm{Tr}(\mathcal{P}_K^n)$ is an ideal of F, so has the form $\mathcal{P}_F^{\psi(n)}$. By [14; III, §3, Proposition 7] we have $\mathcal{P}_K^n \dot{\subseteq} \mathcal{P}_F^{\psi(n)}\mathcal{D}^{-1}$ and $\mathcal{P}_K^n \not\subseteq \mathcal{P}_F^{\psi(n)+1}\mathcal{D}^{-1}$. But $\mathcal{P}_F\mathcal{O}_K = \mathcal{P}_K^{e(K/F)}$ and $\mathcal{D} = \mathcal{P}_K^{\alpha}$. Therefore

$$e(K/F)\psi(n) - \alpha \leq n < e(K/F)[\psi(n) + 1] - \alpha.$$

The resulting inequalities on $\psi(n)$ are

$$\frac{n+\alpha}{e(K/F)} - 1 < \psi(n) \leq \frac{n+\alpha}{e(K/F)}$$

so that $\psi(n) = \left[\dfrac{n+\alpha}{e(K/F)}\right]$ as desired.

The next proposition determines the norm image in filtration groups with large index. In section 8 we analyze the norm map on the full filtration by formal group methods.

PROPOSITION 7.3: *Let K/F be a finite separable extension of local fields with different $\mathcal{D}$ and ramification index $e(K/F)$. Let $\alpha = v_K(\mathcal{D})$. Assume that $n + \alpha + 1 \equiv 0 \pmod{e(K/F)}$ and $n \geqslant \alpha + 1$. Then N:*

$A_n(K) \to A_{\psi(n)}(F)$ and is surjective. Furthermore, the quotient $A(F)/\mathbb{N}A(K)$ is finite.

Proof: There is a formal group law on $\mathcal{P}_K^n$ providing us with an isomorphism $\mathcal{P}_K^n \to A_n(K)$ which we denote by $z \mapsto P(z)$. This isomorphism is defined over F, since A is. See [16; §3] for explicit formulas. We now validate the following commutative square:

$$\begin{tikzcd}
\mathcal{P}_K^n/\mathcal{P}_K^{n+1} \arrow[r, "\mathcal{T}"] \arrow[d, "\wr"] & \mathcal{P}_F^{\psi(n)}/\mathcal{P}_F^{\psi(n)+1} \arrow[d, "\wr"] \\
A_n(K)/A_{n+1}(K) \arrow[r, "N"'] & A_{\psi(n)}(F)/A_{\psi(n)+1}(F).
\end{tikzcd}$$

The congruence $n + \alpha + 1 \equiv 0(e(K/F))$ implies that $\psi(n+1) = \psi(n) + 1$. Hence the horizontal arrow $\mathcal{T}$ above induced by trace is well-defined, and is surjective by definition of ψ.

Let L be the Galois closure of K over F and let $\sigma_1 = 1, \sigma_2, \ldots, \sigma_\ell$ be a complete set of distinct coset representatives for $\mathrm{Gal}(L/F)/\mathrm{Gal}(L/K)$. For $z \in K$, let $z_i = \sigma_i(z)$ with $i = 1, \ldots, \ell$. Thus $Tz = z_1 + \cdots + z_\ell$.

Suppose that $z, z' \in \mathcal{P}_K^n$. By the explicit addition formulas [16; (16)] $P(z) + P(z') = P(z + z' + zz'\omega) = P(z + z') + P(\omega')$ where $\omega, \omega' \in \mathcal{O}_K$ and $v_K(\omega') = v_K(zz'\omega) \geq 2n$. Repeated use of this formula shows that

$$\mathbb{N}P(z) = P(z_1) + \cdots + P(z_\ell) = P(Tz) + P'$$

where $P' \in A_{2n}(K) \cap A(F)$. That is $P' = P(\omega')$ with $\omega' \in \mathcal{O}_F$ and $v_F(\omega') \geq 2n/e(K/F)$. Our hypotheses on n imply that $2n/e(K/F) \geq \psi(n) + 1$. Hence $P' \in A_{\psi(n)+1}(F)$.

It follows that the horizontal arrow N above induced by $\mathbb{N}$ is well-defined and that the diagram commutes. Hence N is surjective, and so must $\mathbb{N}$ be using successive approximations. The quotient $A(F)/\mathbb{N}A(K)$ is finite because $A_{\psi(n)}(F)$ has finite index in $A(F)$.

Corollary 7.3.1: *Let K be a quadratic separable extension of F, and E an elliptic curve over F. There is a finite index subgroup U of $E(K)$ such that $|H^0(\mathrm{Gal}(K/F), U)| = |H^1(\mathrm{Gal}(K/F), U)|$.*

Proof: For n as in 7.3, $[A_n(K) \cap A(F)]/\mathbb{N}A_n(K)$ is isomorphic to $A_{\{n/e(K/F)\}}(F)/A_{\psi(n)}(F)$, and has order dependent only on K/F. Apply this for A equaling E and E^ω to compute that the order of H^0 and H^1 agree for $U = A_n(K)$.

As a computational device, we introduce some choices of models for E and E^{ω}. Let A be a possibly non-minimal model for E over $\mathcal{O}_F$, in generalized Weierstrass form (7.0.1). If $\mathrm{ch}(k_F) \neq 2$ we obtain by translation of y the integral model

$$A^{\mathrm{trans}}\colon\ y^2 = x^3 + \tfrac{1}{4}b_2x^2 + \tfrac{1}{2}b_4x + \tfrac{1}{4}b_6 \qquad (7.4.1)$$

with b_i as in [17; (1.2)] and discriminant Δ preserved. If $K = F(\sqrt{d})$ and ω is the quadratic character of F^* corresponding to K, then

$$A'\colon y^2 = x^3 + \tfrac{1}{4}b_2dx^2 + \tfrac{1}{2}b_4d^2x + \tfrac{1}{4}b_6d^3 \qquad (7.4.2)$$

is a model for E^{ω} over $\mathcal{O}_F$ with discriminant $\Delta' = \Delta d^6$. The inclusion i: $A'(F) \to A(K)$ is given by the composition of the map $(x, y) \to (x/d, y/d^{3/2})$ to $A^{\mathrm{trans}}(K)$ with translation of y back to $A(K)$.

If $\mathrm{char}(k_F) = 2$ the following construction serves in both the equal and unequal characteristic cases. Suppose that $K = F(\theta)$ where θ is a root of the Artin–Schreier equation $x^2 - x + \gamma = 0$ with $\gamma \in F$. Again assume that A is given in generalized Weierstrass form (7.0.1) over $\mathcal{O}_F$. Let g generate $\mathrm{Gal}(K/F)$. The condition for $P = (x, y) \in A(F)$ to be in $E^{\omega}(F)$ is that $P^g = -P$ or equivalently $x \in F$ and $y + y^g = -a_1x - a_3$. Write $y = y_0 + y_1\theta$ with y_0, $y_1 \in F$. Then $P \in E^{\omega}(F)$ if and only if $y_1 = -2y_0 - a_1x - a_3$ and, from substituting y in (7.0.1),

$$\begin{aligned}(1 - 4\gamma)(y_0^2 + a_1xy_0 + a_3y_0) &= x^3 + (a_2 + \gamma a_1^2)x^2 + (a_4 + 2\gamma a_1a_3)x \\ &\quad + (a_6 + \gamma a_3^2). \end{aligned}\qquad (7.4.3)$$

Further stretching may now be required to obtain an integral model. To do so, let $\delta = 1 - 4\gamma$ If $\mathrm{char}(F) \neq 2$, we see that as δ ranges over the discriminants of quadratic extensions of F, γ provides the corresponding Artin–Schreier equations. Hence all quadratic extensions K/F are in this form and we may assume $v_F(\delta) = 0$ or 1. Choose minimal $r \geq 0$ such that $\pi_F^{2r}\gamma \in \mathcal{O}_F$. From the integral equation $x^2 - \pi_F^rx + \pi_F^{2r}\gamma = 0$ for K over F we see that $d = \pi_F^{2r}(1 - 4\gamma) = \pi_F^{2r}\delta$ is the discriminant of K/F determined up to the square of a unit of F. It follows from (7.4.3) that a model for E^{ω} over $\mathcal{O}_F$ is

$$\begin{aligned}A'\colon\ y^2 + (\pi_F^r\delta)a_1XY + (\pi_F^{3r}\delta^2)a_3Y \\ = X^3 + d(a_2 + \gamma a_1^2)X^2 + d^2(a_4 + 2\gamma a_1a_3)X + d^3(a_6 + \gamma a_3^2)\end{aligned} \qquad (7.4.4)$$

with discriminant $\Delta' = d^6\Delta$. The map i: $A'(F) \to A(K)$ is given by

$$(X, Y) \to (X/d, [Y - \theta(2Y + a_1X + a_3)]/\delta^2\pi_F^{3r}).$$

The following Lemma summarizes those aspects of the above discussion which we shall need later.

LEMMA 7.5: *Let A be a possibly non-minimal Weierstrass model for E over $\mathcal{O}_F$ having discriminant Δ. Let ω be a quadratic character of F^* and let K be the corresponding extension. There is a model A' for E^ω over $\mathcal{O}_F$ having discriminant $\Delta' = \Delta d^6$, where d is the discriminant of K/F, determined up to the square of a unit of F. The map i: $A'(F) \to A(K)$ has the form $i(x', y') = (x, y)$ with $x = x'/d$.*

We now come to the formula for the norm index in terms of the group of components of multiplicity one of the singular fiber in the Néron models of E and its twist. Let $\|a\|_F = |k_F|^{-v_F(a)}$ be the absolute value on F. Let $\| \quad \|_K$ be the corresponding absolute value on the quadratic extension K, and let ω be the quadratic character of F^* corresponding to K/F.

THEOREM 7.6: *Choose a Weierstrass model A for E over $\mathcal{O}_F$ and use the same model for E over K. Choose a model A' for E^ω over $\mathcal{O}_F$ as in the above Lemma. In the notation of Lemma* 7.1, *let the "stretching factors" from minimality be given by $u_F = u_F(E, A)$, $u_K = u_K(E, A)$, $u_F^\omega = u_F(E^\omega, A')$. Let $c_F = |E(F)/E_0(F)|$, $c_K = |E(K)/E_0(K)|$, $c_F^\omega = |E^\omega(F)/E_0^\omega(F)|$. Then*

$$|E(F)/\mathbb{N}E(K)| = \frac{c_F c_F^\omega}{c_K} \cdot \frac{\|u_K\|_K}{\|u_F u_F^\omega\|_F}.$$

PROOF: We produce the following exact sequence, as explained below.

$$0 \to A'(F)/A'_q(F) \overset{i}{\to} A(K)/A_n(K) \overset{\mathbb{N}}{\to} A(F)/A_{\psi(n)}(F) \to E(F)/\mathbb{N}E(K) \to 0 \tag{7.6.1}$$

Clearly $E(F)/\mathbb{N}E(K)$ is isomorphic to $A(F)/\mathbb{N}A(K)$. Choose n as in Proposition 7.3. Exactness to the right of the map $\mathbb{N}$ follows from surjectivity of $\mathbb{N}$: $A_n(K) \to A_{\psi(n)}(F)$. Moreover, if $\mathbb{N}P \in A_{\psi(n)}(F)$ we may correct P by an element of $A_n(K)$ so that $\mathbb{N}P = 0$. But then $P = i(Q)$ for some $Q \in A'(F)$. Since the other inclusion is trivial, $\operatorname{Ker} \mathbb{N} = \operatorname{Image} i$. To compute q and verify exactness on the left, note first that if $(x', y') = P \in A'(F)$ then by (7.5), $i(P) = (x'/d, \ldots)$ is in $A_n(K)$ if and only if $v_K(x'/d) \leq -2n$. Recall the notation $\alpha = v_K(\mathcal{D})$

where $\mathscr{D}$ is the different of K/F. Hence $v_K(d) = 2\alpha$ and $i(P) \in A_n(K)$ if and only if $v_K(x') \leq -2n + 2\alpha$.

Now $n \geq \alpha + 1$. Hence $v_F(x')$ is negative, so must be even. It follows that $i(P) \in A_n(K)$ if and only if $P \in A'_q(F)$ with $q = \left\{\frac{n-\alpha}{e(K/F)}\right\}$ where $\{I\}$ is the smallest integer not smaller than I.

From the Euler characteristic of exact sequence (7.6.1) and Lemma (7.1.3) we see that

$$|E(F)/\mathbb{N}E(K)| = \frac{c_F c_F^{\omega}}{c_K} \cdot \frac{|\bar{E}_0(k_F)|\,|\bar{E}_0^{\omega}(k_F)|}{|\bar{E}_0(k_K)|} \cdot \frac{|k_F|^{\psi(n)+q-2+v_F(u_F u_F^{\omega})}}{|k_K|^{n+v_K(u_K)-1}}. \tag{7.6.2}$$

Let L_F (resp. L_F^{ω}, L_K) be the L-function for E over F (resp. E^{ω} over F, E over K). Then $L_F(1) = |k_F|/|\bar{E}_0(k_F)|$ by [17; (5.2)]. But $L_K = L_F \cdot L_F^{\omega}$. Hence

$$\frac{|\bar{E}_0(k_F)|\,|\bar{E}_0^{\omega}(k_F)|}{|\bar{E}_0(k_K)|} = \frac{|k_F|^2}{|k_K|}.$$

Furthermore, $q + \psi(n) = \left\{\frac{n-\alpha}{e(K/F)}\right\} + \left\{\frac{n+\alpha}{e(K/F)}\right\}$ is obviously $2n$ if $e(K/F) = 1$ and is n if $e(K/F) = 2$ since $n \equiv \alpha + 1 \pmod 2$ by the hypothesis of Proposition 7.3. Substituting in (7.6.2) yields the desired formula.

Remark: Clearly the norm index $E(F)/\mathbb{N}F(K)$ is independent of the choice of model A. To see that the right side of the formula in Theorem 7.6 is independent of A, let Δ_F, Δ_F^{ω}, Δ_K be the minimal discriminants for E over F, E^{ω} over F and E over K. Then

$$u_F^{12} = \Delta/\Delta_F, \quad (u_F^{\omega})^{12} = \Delta'/\Delta_F^{\omega} = \Delta d^6/\Delta_F^{\omega}, \quad u_K^{12} = \Delta/\Delta_K.$$

Hence

$$\|u_K\|_K/\|u_F u_F^{\omega}\|_F = [\|\Delta_F \Delta_F^{\omega} d^{-6}\|_F/\|\Delta_K\|_K]^{1/12}.$$

We leave it to the reader to express this in terms of conductors and numbers of components in the singular fibers of the Néron models.

Example: We apply the previous results to the curve E with model $y^2 = x^3 - x^2 + x$ over $\mathbb{Q}_2$. This is the curve $24A$ of Table 1 of [2] (E is isogenous over $\mathbb{Q}$ to the modular curve X_0 (24)). Over $\mathbb{Q}_2$ E has Kodaira type III, discriminant $\Delta_E = -2^4 \cdot 3$, and $c_F = 2$. It is easy to check that over a ramified quadratic extension K this model remains minimal and the type is I_1^* with $c_K = 4$. The curves $48A$, $144E$, $192E$ and $192K$ are the twists of E by the quadratic fields $\mathbb{Q}_2(\sqrt{-1})$, $\mathbb{Q}_2(\sqrt{3})$, $\mathbb{Q}_2(\sqrt{-2})$, $\mathbb{Q}_2(\sqrt{2})$ respectively (the other ramified twists have conductors outside the range of the table). Then formula (7.6) and the remark above can be applied to compute that $E(F)/\mathbb{N}E(K)$ has order 1 for the first two fields listed, and order 2 for the remaining two.

To complete verification of (3.1) in these cases we notice that $\omega(-\Delta) = \omega(3) = \omega(-1)(-1)^{a(\omega)}$ (see 8.16.1). Then $\omega(-\Delta)(-1)^{\dim E(F)/\mathbb{N}E(K)}$ is 1 for the field $\mathbb{Q}_2(\sqrt{-2})$ and -1 otherwise. The value of $\epsilon(\sigma_E)$ is the negative of the eigenvalue of the operator W_2, given in Table 3 of [2]. Using this it is easy to see $\epsilon(\sigma_E)\epsilon(\sigma_E \otimes \omega) = \omega(-\Delta)(-1)^{\dim E(F)/\mathbb{N}E(K)}$ in all cases above.

We remark that $\epsilon(E, \omega)$, $\omega(-\Delta_E)$ and the parity of $\dim_{\mathbb{F}_2}(E(F)/\mathbb{N}E(K))$ are locally constant functions of the coefficients of E. Hence the above example can be perturbed to yield infinitely many nonisomorphic curves over $\mathbb{Q}_2$ for which conjecture (3.1) is true for the quadratic extension considered.

Similar computations apply to other examples. Conjecture 3.1 would imply that there is an algorithmic method for computing $\epsilon(E, \omega)$, which is completely divorced from the definition of ϵ-factors in group theory terms.

COROLLARY 7.6: *If K/F is unramified or if* $\mathrm{char}(k_F) \neq 2$ *then* $\|u_K\|_K/\|u_F u_F^{\omega}\|_F = 1$ *and* $|E(F)/\mathbb{N}E(K)| = c_F c_F^{\omega}/c_K$.

PROOF: Let Δ_F (resp. Δ_F^{ω}) be the minimal discriminants for E (resp. E^{ω}) over $\mathcal{O}_F$. By symmetry we may assume $v_F(\Delta_F) \leq v_F(\Delta_F^{\omega})$. Let A in Theorem 7.6 be the minimal model for E over $\mathcal{O}_F$. We claim that the model A' also is minimal over $\mathcal{O}_F$. Otherwise, since the discriminant changes by a twelfth power, $v_F(\Delta_F^{\omega}) \leq v_F(A') - 12 = v_F(\Delta_F d^6) - 12$. But our hypotheses imply $v_F(d) \leq 1$, contradicting the inequality $v_F(\Delta_F) \leq v_F(\Delta_F^{\omega})$.

Furthermore, the model A remains minimal over K. We show this first in $\mathrm{char}(k_F) \neq 2$. If A is not minimal over K and if π_K is a prime of K, we have $\pi_K^i \mid b_i$ in the model (5.10.1) using the algorithm [17]. Choose $\pi_K = \pi_F$ if K/F unramified and $\pi_K^2 = \pi_F$ if K/F ramified. Then $\pi_F^i \mid b_i d^{i/2}$, contradicting minimality of the model (7.4.2) for E^{ω}.

Finally, if $\mathrm{char}(k_F) = 2$ and K/F is unramified similar arguments apply to the models A and A' coming from the Artin–Schreier equations as described above. Alternatively, the terms in the conductor-discriminant formula [13] are not changed upon unramified base-change. Hence $v_K(\Delta_F) = v_F(\Delta_F)$ is already minimal.

8. The case of residue characteristic 2.

Throughout this section F is a local field with finite residue field k_F such that $\mathrm{char}(k_F) = 2$. Let U_F denote the units of F and $\mathcal{O}_F$ the ring of integers. Let E be an elliptic curve defined over F, with discriminant Δ determined modulo $(F^*)^{12}$. Let K be a separable quadratic extension of F corresponding to the character ω of F^*. Let $\kappa(E, \omega) = (-1)^{\dim E(F)/\mathbb{N}E(K)}$. In this section we shall examine the conjecture that $\epsilon(E, \omega) = \omega(-\Delta)\kappa(E, \omega)$ in various cases, including those for which E has good reduction and for which the exponent of the Artin conductor of E is 2. When K/F is unramified, the conjecture is valid by Theorem 6.2. Hence we assume that K/F is ramified. The arguments below could also be used in the unramified case after slight modification, which we leave to the reader.

Suppose that E has good reduction over F. Recall the notation $\bar{E}$ for the reduction of E and E_1 for the kernel of reduction.

LEMMA 8.1: *Suppose that E has good reduction over F and that K/F is ramified. Then $\mathbb{N}E(K) = 2E(F) + \mathbb{N}E_1(K)$ and the following sequence is exact:*

$$0 \to [E_1(F) + \mathbb{N}E(K)]/\mathbb{N}E(K) \to E(F)/\mathbb{N}E(K) \to \bar{E}(k_F)/2\bar{E}(k_F) \to 0.$$

PROOF: The map $E(F)/E_1(F) \to E(K)/E_1(K)$, which obviously is injective, must be surjective because domain and codomain are isomorphic to the finite group $\bar{E}(k_F)$. Hence $E(K) = E(F) + E_1(K)$ and $\mathbb{N}E(K) = 2E(F) + \mathbb{N}E_1(K)$. It follows that $\mathbb{N}$ induces multiplication by 2 upon reduction and the rest of the desired exact sequence is clear. See also [11, Corollary 4.6].

Now suppose further that E has ordinary good reduction. Then $|\bar{E}(k_F)/2\bar{E}(k_F)| = |\bar{E}(k_F)_2| = 2$ and we shall analyze the norm $\mathbb{N}$ on E_1 by relating it to the field-theoretic norm. Recall that multiplication by 2 on $\bar{E}$ is the product of dual isogenies of degree 2 defined over k_F, the Frobenius $\bar{\pi}$ which is inseparable, and a separable isogeny $\bar{\psi}$. If $\mathrm{char}(F) = 2$, the same applies over F. If $\mathrm{char}(F) = 0$ there is a unique point of order 2 which reduces trivially. It must therefore be fixed by

Galois($\bar{F}/F$) and hence be in $E_1(F)$. If we form the isogeny whose kernel is $E_1(F)_2$, it reduces to Frobenius. It follows that in general, multiplication by 2 on E is the product of dual isogenies of degree 2 defined over F, say $2 = \pi \circ \psi$, where π: $E \to E'$ reduces to Frobenius $\bar{\pi}$ while ψ: $E' \to E$ is separable and reduces to the separable isogeny $\bar{\psi}$.

Lemma 8.2: *Let L be a separable extension of F. Then ψ induces an isomorphism $E_1'(L) \xrightarrow{\sim} E_1(L)$. Let F^s be the separable closure of F and $\mathcal{G} = \mathrm{Gal}(F^s/F)$. There is an exact sequence*

$$0 \to E'(F)_\psi \to E'(F) \xrightarrow{\psi} E(F) \xrightarrow{\lambda_\psi} H^1(\mathcal{G}, E'_\psi).$$

The image of λ_ψ has order 2 and corresponds by Kummer theory to the unique unramified quadratic extension of F. More precisely, if char(F) = 0 *then $H^1(\mathcal{G}, E'_\psi) = F^*/F^{*2}$ and Image $\lambda_\psi = (1 + 4\mathcal{O}_F)F^{*2}/F^{*2}$. If* char($F$) = 2, *then $H^1(\mathcal{G}, E'_\psi) = F/\mathcal{P}F$, where $\mathcal{P}$ is the Artin–Schreier function $\mathcal{P}(x) = x^2 + x$, and* Image $\lambda_\psi = (k_F + \mathcal{P}F)/\mathcal{P}F$.

Proof: Since ψ is separable, we have a surjection ψ: $E_1'(F^s) \to E_1(F^s)$, which is an injection because Ker $\psi \cap E_1' = \{0\}$. Taking fixed points under Gal(F^s/L) provides the isomorphism $E_1'(L) \xrightarrow{\sim} E_1(L)$.

The desired exact sequence above arises from the Kummer theory of elliptic curves, with the map λ_ψ obtained as follows: Given $P \in E(F)$, choose $Q \in \psi^{-1}(P)$. Form the cocycle which sends $g \in \mathcal{G}$ to $(g-1)(Q)$ in E'_ψ. The identification of $H^1(\mathcal{G}, E'_\psi)$ with F^*/F^{*2} if char $(F) = 0$ (respectively, with $F/\mathcal{P}F$ if char$(F) = 2$) is obtained by associating to P a Kummer (respectively Artin–Schreier) generator for the separable extension of degree at most 2 over F containing Q.

We now determine the image of λ_ψ. Let $\bar{\psi}$: $\bar{E}'(k_F) \to \bar{E}(k_F)$ be the reduction of ψ. Since $|\text{Coker } \bar{\psi}| = |\text{Ker } \bar{\psi}| = 2$ is not trivial, the cokernel of ψ cannot be trivial. Let $P \in E(F)$ reduce to $\bar{P} \in \bar{E}(k_F)$. Choose $\bar{Q}$ defined over at most a quadratic extension of k_F, such that $\bar{\psi}(\bar{Q}) = \bar{P}$. Let L be the unramified quadratic extension of F. Since ψ: $E_1'(L) \to E_1(L)$ is surjective we may choose $Q \in E(L)$ such that $\psi(Q) = P$. Since Image λ_ψ is not trivial it corresponds by Kummer theory exactly to the extension L as desired.

Lemma 8.3: *There is an exact sequence*

$$0 \to E(F)_\pi \to E(F) \xrightarrow{\pi} E'(F) \xrightarrow{\lambda_\pi} U_F/U_F^2 \to 0.$$

Let T' be the point of order 2 generating $E'(F)_\psi$. Then $\lambda_\pi(T') = \operatorname{coset}\{\Delta\}$ where Δ is the minimal discriminant of E.

Proof: If $\operatorname{char}(F) = 0$ then $H^1(\mathcal{G}, E_\pi) = F^*/F^{*2}$ and we obtain the exact sequence

$$0 \to E(F)_\pi \to E(F) \xrightarrow{\pi} E'(F) \xrightarrow{\lambda_\pi} F^*/F^{*2}$$

again by Kummer theory, or by the cohomology of the short exact sequence $0 \to E(\bar{F})_\pi \to E(\bar{F}) \to E'(\bar{F}) \to 0$ where $\bar{F} = F^s$ is the algebraic closure of F. By local duality theory (J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Inter. Congress Math. at Stockholm, 1962, 288–295) the image of λ_π and the image of λ_ψ are orthogonal complements in the perfect pairing

$$H^1(\mathcal{G}, E_\pi) \times H^1(\mathcal{G}, E_\psi) \to \mu_2.$$

It follows that Image $\lambda_\pi = U_F/U_F^2$. If $\operatorname{char}(F) = 2$ there is a similar cohomological argument via the duality theory [12], or else the Lemma can be checked by explicit computation [7, Proposition 1.1(b) and Proposition 2.2].

To determine $\lambda_\pi(T')$ note that Ker π is defined over F. Hence the 2-division field of E is $M = F(\Delta^{1/2})$. Let T be a point of order 2 in $E(M)$ not in Ker π. Then $T' = \pi(T)$. By our exact sequence, $\lambda_\pi(T')$ is trivial if and only if $T' \in F$; that is, if and only if $M = F$ and $\Delta \in F^2$. It follows that $\lambda_\pi(T') = \operatorname{coset}\{\Delta\}$.

Lemma 8.4: *If E has ordinary good reduction over F then $[E_1(F) + 2E(F)]/2E(F)$ is isomorphic to $U_F/U_F^2 \cdot \Delta^Z$ where Δ is the minimal discriminant of E and Δ^Z is the cyclic group generated by Δ.*

Proof: Let us first show that $\psi[E'(F)] = E_1(F) + 2E(F)$. Given $P \in E'(F)$, pass to $\bar{P} \in \bar{E}'(k_F)$. Since the Frobenius $\bar{\pi}$ is inseparable while k_F is perfect we have $\bar{P} = \bar{\pi}(\bar{Q})$ for some $\bar{Q} \in \bar{E}(k_F)$. Choose $Q \in E(F)$ which reduces to $\bar{Q}$. Then $P - \pi(Q) \in E_1'(F)$. Hence $\psi(P) = \psi(P - \pi Q) + 2Q$ is in $E_1(F) + 2E(F)$. Conversely, since $E_1(F) = \psi E_1'(F)$ and $2E(F) = (\psi \circ \pi)[E(F)]$ we obtain the reverse inclusion, $\psi E'(F) \supseteq E_1(F) + 2E(F)$, and hence equality. Now we clearly have isomorphisms

$$U_F/U_F^2 \cdot \Delta^Z \xleftarrow[\lambda_\pi]{} E'(F)/[E'(F)_\psi + \pi E(F)] \xrightarrow[\psi]{} [E_1(F) + 2E(F)]/2E(F).$$

Corollary 8.5: *Let E have ordinary good reduction over F and let K be a ramified quadratic extension of F. Then*

$$[E_1(F)+\mathsf{N}E(K)]/\mathsf{N}E(K)\xrightarrow{\sim} U_F/(N\,U_K)\Delta^Z.$$

Proof: From the above Proposition we obtain the commutative diagram

$$\begin{tikzcd}
{[E_1(K)+2E(K)]/2E(K)} \arrow[r, "\sim"] \arrow[d, "\mathsf{N}"'] & U_K/U_K^2\cdot\Delta^Z \arrow[d, "N"] \\
{[E_1(F)+2E(F)]/2E(F)} \arrow[r, "\sim"] & U_F/U_F^2\cdot\Delta^Z.
\end{tikzcd}$$

In particular, N induces corestriction in cohomology and hence field-theoretic norm N on U_K. By Lemma 8.1, $2E(F)+\mathsf{N}E_1(K)=\mathsf{N}E(K)$. Hence the cokernel of N is $[E_1(F)+2E(F)]/[\mathsf{N}E_1(K)+2E(F)]=[E_1(F)+\mathsf{N}E(F)]/\mathsf{N}E(F)$ and is isomorphic to $U_F/(NU_K)\cdot\Delta^Z$, the cokernel of N.

Proposition 8.6: *Suppose that E has ordinary good reduction over F and that K/F is a quadratic extension corresponding to the character ω of F^*. Then*

$$|E(F)/\mathsf{N}E(K)| = \begin{array}{r} 1 \\ 2 \\ 4 \end{array}\left\{\begin{array}{l} \textit{if } K/F \textit{ is unramified,} \\ \textit{if } K/F \textit{ ramified and } \omega(\Delta)=-1, \\ \textit{if } K/F \textit{ ramified and } \omega(\Delta)=+1. \end{array}\right.$$

Furthermore, $\kappa(E,\omega)=\omega(\Delta)$ and $\epsilon(E,\omega)=\omega(-\Delta)\kappa(E,\omega)$.

Proof: If K/F is unramified, than $E(F)=\mathsf{N}E(K)$ for example by [11, Corollary 4.4]. Since Δ is a unit, $\omega(\Delta)=1$. By (2.4), $\epsilon(E,\omega)=1$ as desired.

If K/F is ramified, then by Lemma 8.1 $|E(F)/\mathsf{N}E(K)|=|\bar{E}(k_F)/2\bar{E}(k_F)|\cdot|[E_1(F)+\mathsf{N}E(K)]/\mathsf{N}E(K)|$. But $|\bar{E}(k_F)/2\bar{E}(k_F)|=2$ and $|[E_1(F)+\mathsf{N}E(K)]/\mathsf{N}E(K)|=|U_F/(NU_K)\cdot\Delta^Z|=1$ or 2, according to whether $\omega(\Delta)=-1$ or $\omega(\Delta)=+1$, by local class field theory. Finally, $\epsilon(E,\omega)=\omega(-1)$ by 2.4b as desired.

We now turn our attention to curves with supersingular good reduction. Supersingular reduction implies that $\bar{E}(k_F)$ has odd order, so that (8.1) shows that $E(F)/\mathsf{N}E(K)$ is isomorphic to $E_1(F)/\mathsf{N}E_1(K)$. We will use the formal group law on the prime ideal $\mathcal{P}_K$ to study the norm map. Our method is exactly analogous to the treatment of the norm map for multiplicative groups of fields [14; chap. V]; for the formal group associated to elliptic curves it does not appear to be in the literature.

We recall a few facts about quadratic extensions of local fields. If ω is a quadratic character of F^* and K is ramified quadratic

$$\mathrm{Tr}_{K/F}(\mathcal{P}_K^n) = \mathcal{P}_F^{[(n+a(\omega))/2]} \tag{8.7.1}$$

$$a(\omega) \leq 2v(2)+1, \text{ and } a(\omega) \leq 2v(2) \text{ implies } a(\omega) \text{ even.} \tag{8.7.2}$$

Since E has supersingular reduction it has a minimal Weierstrass model (7.0.1) with $v(a_1) \geq 1$. Further, since F does not have characteristic 3, we may arrange that $a_2 = 0$ [17; (5.2)]. Then the formal group law [16; (16)] is

$$\begin{aligned} F(z_1, z_2) = z_1 + z_2 - a_1 z_1 z_2 - 2a_3(z_1^3 z_2 + z_1 z_2^3) - 3a_3 z_1^2 z_2^2 \\ + \text{terms of total degree} \geq 5. \end{aligned} \tag{8.8.1}$$

We may now compute the Norm map $\mathbb{N}$: $E_1(K) \to E_1(F)$ explicitly. When $z \in \mathcal{P}_K^n$, we have

$$\mathbb{N}(z) = \mathrm{Tr}(z) - a_1 Nz - 3a_3 N^2 z - 2a_3 Nz(\mathrm{Tr} z)^2 (\mathrm{mod}\ \mathcal{P}_K^{5n}) \tag{8.8.2}$$

when Tr and N are the trace and norm for K/F. Since $\mathbb{N}(z)$ and the right side of (8.8.2) are both in F, we have

$$\mathbb{N}(z) = \mathrm{Tr}(z) - a_1 Nz - 3a_3 N^2 z - 2a_3 Nz(\mathrm{Tr}(z))^2 (\mathrm{mod}\ \mathcal{P}_F^{2n+[n+1/2]}). \tag{8.8.3}$$

From the explicit formula for the discriminant in [16, (2)] we see that

$$\Delta = -3a_3^4 + a_3^2 a_1^2(a_1 a_3 + 2a_4) - a_1^4(a_1^2 a_6 - a_1 a_3 a_4 - a_4^2) \quad \text{modulo } \mathcal{P}_F^{2v(2)+1}. \tag{8.8.4}$$

The goal of this section is to compute $\omega(-\Delta)(-1)^{\dim E(F)/\mathbb{N}E(K)}$ when $v(a_1)$ is sufficiently large with respect to $a(\omega)$. Notice that when E has supersingular good reduction, $v(a_1) \geq 1$ and $v(a_3) = 0$. Assume $a(\omega) \geq 2$.

LEMMA 8.9: *When $n \geq a(\omega) - 1$, $\mathbb{N}(\mathcal{P}_K^{2n-a(\omega)+1}) = \mathcal{P}_F^n$.*

PROOF: It is easy to see from (8.8.3) that $\mathbb{N}(\mathcal{P}_K^{2n-a(\omega)+1}) \subset \mathcal{P}_F^n$ for $n \geq a(\omega)-1$. The map induced on the quotients $\mathcal{P}_K^{2n-a(\omega)+1}/\mathcal{P}_K^{2n-a(\omega)+3} \to \mathcal{P}_F^n/\mathcal{P}_F^{n+1}$ is given by $z \mapsto \operatorname{Tr} z$, and hence is surjective. This shows that $\mathbb{N}(\mathcal{P}_K^{2n-a(\omega)+1}) = \mathcal{P}_F^n$ (see [14, V.1 Lemma 2]).

LEMMA 8.10: *Let $n \leqslant a(\omega)-1$. For $z \in \mathcal{P}_k^n$, $\mathbb{N}(z) = \operatorname{Tr} z - a_1 Nz + a_3 Nz^2$ modulo $\mathcal{P}_F^{2n+[n+1/2]}$.*

PROOF: This follows from the fact that $2a_3Nz(\operatorname{Tr} z)^2$ and $4\,\mathcal{P}_F^{2n}$ are contained in $\mathcal{P}_F^{2n+[n+1/2]+1}$ when $n \leq a(\omega)-1$.

LEMMA 8.11: *Suppose that $3n \leqslant a(\omega)-2$. Then for z in $\mathcal{P}_K^n$ $\mathbb{N}(z) = -a_1Nz + a_3Nz^2 \bmod \mathcal{P}_F^{2n+1}$. Further, if $v(a_1) \geqslant n+1$ then the induced map $\mathbb{N}_n$: $\mathcal{P}_K^n/\mathcal{P}_K^{n+1} \to \mathcal{P}_F^{2n}/\mathcal{P}_F^{2n+1}$ is bijective.*

PROOF: For $3n \leq a(\omega)-2$ we have $\operatorname{Tr}(\mathcal{P}_K^n) \subset \mathcal{P}_F^{2n+1}$. When $v(a_1) \geq n+1$, $\mathbb{N}(z) = a_3Nz^2 (\bmod\ \mathcal{P}_F^{2n+1})$, so that the induced map on the quotients (which are isomorphic to k) is a nonzero multiple of squaring, and hence bijective.

LEMMA 8.12: *Suppose that $3(a(\omega)-1) \geq 3n > a(\omega)+1$. Then for z in $\mathcal{P}_K^n$, $\mathbb{N}(z) = \operatorname{Tr} z - a_1Nz \bmod \mathcal{P}_F^{[n+a(\omega)/2]+1}$. Further, if $v(a_1) \geqslant \left[\dfrac{a(\omega)-n}{2}\right]+1$, then $\mathbb{N}(\mathcal{P}_K^n) = \mathcal{P}_F^{[(n+a(\omega))/2]}$.*

PROOF: For such n, $2n \geq \dfrac{n+a(\omega)}{2}+1$. When $v(a_1) \geq \left[\dfrac{a(\omega)-n}{2}\right]+1$, $\mathbb{N}(z) = \operatorname{Tr} z \bmod \mathcal{P}_F^{[(n+a(\omega))/2]+1}$. Then $\mathbb{N}$ induces the trace map on quotients $\mathcal{P}_K^n/\mathcal{P}_K^{n+1} \to \mathcal{P}_F^{[(n+a(\omega))/2]}/\mathcal{P}_F^{[n+a(\omega)/2]+1}$ when $n+a(\omega)$ is odd. By the same reasoning as above $\mathbb{N}(\mathcal{P}_K^n) = \mathcal{P}_F^{[(n+a(\omega))/2]}$.

LEMMA 8.14: *Let $A_0 \supset A_1 \supset \cdots \supset A_n$ and $B_0 \supset B_1 \supset B_2 \supset \cdots \supset B_n$ be two filtered abelian groups, and let ϕ: $A \to B$ be a homomorphism with finite cokernel which preserves the filtration. Let ϕ_i: $A_i/A_{i+1} \to B_i/B_{i+1}$. If ϕ_n is surjective and ϕ_i is injective for $i \leqslant n-2$, then $[A: \phi(B)] = \sum_{i=0}^{n-1} |\operatorname{coker} \phi_i|$.*

PROOF: By replacing A_0 by A_0/A_n and B_0 by B_0/B_n we may assume that $A_n = B_n = 0$. The result is clear if $n = 0$, 1 and we proceed by induction. Apply the Snake Lemma [14; V.1 Lemma 1] to the exact sequences

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r] & A_0 \arrow[r] \arrow[d, "\phi"] & A_0/A_1 \arrow[r] & 0 \\
0 \arrow[r] & B_1 \arrow[r] & B_0 \arrow[r] & B_0/B_1 \arrow[r] & 0.
\end{tikzcd}$$

Since ϕ_0 is injective, we have that $|\text{coker } \phi| = [B_1 \colon \phi(A_1)] + |\text{coker } \phi_0|$. The result now follows by induction.

Proposition 8.15: *Let E be an elliptic curve with supersingular good reduction over a local field F of residue characteristic 2. Assume that the valuation $v(a_1)$ of the coefficient a_1 in a minimal model satisfies $3v(a_1) \geq a(\omega) - 1$. Then*

$$\dim_{\mathbb{F}_2} E(F)/\mathbb{N}E(K) = \left[\frac{a(\omega)+1}{3}\right] \dim(k_F) + \dim(\text{coker } \mathbb{N}_n),$$

where $n = \left[\frac{a(\omega)+1}{3}\right]$ and $\mathbb{N}_n \colon \mathcal{P}_K^n/\mathcal{P}_K^{n+1} \to \mathcal{P}_F^{2n-1}/\mathcal{P}_F^{2n}$ if 3 does not divide $a(\omega) - 1$ and $\mathbb{N}_n \colon \mathcal{P}_K^n/\mathcal{P}_K^{n+1} \to \mathcal{P}_F^{2n}/\mathcal{P}_F^{2n+1}$ when 3 divides $a(\omega) - 1$.

Proof: When $3i \leq a(\omega) - 2$, (8.11) shows that the induced map $\mathbb{N}$: $\mathcal{P}_K^i/\mathcal{P}_K^{i+1} \to \mathcal{P}_F^{2i}/\mathcal{P}_F^{2i+1}$ is injective. When $3i > a(\omega) + 1$, (8.12) shows that $\mathbb{N}(\mathcal{P}_K^i) = \mathcal{P}_F^{[(i+a(\omega))/2]}$. Thus Lemma 8.14 applies to this situation to compute $E_1(F)/\mathbb{N}E_1(K)$. Notice that $n = \left[\frac{a(\omega)+1}{3}\right]$ is the unique integer such that $a(\omega) - 2 < 3n < a(\omega) + 1$. Application of (8.10) and straightforward calculation yield the proposition.

It will be necessary to compute $\omega(-\Delta)$ in order to check (3.1). From (8.8.4) we see that when $3v(a_1) \geq a(\omega) - 1$ and $v(a_3) = 0$:

$$\omega(\Delta) = \omega(-3 + a_1^3/a_3) \tag{8.15.1}$$

Lemma 8.16: *Let ω be a ramified quadratic character of F^* of conductor exponent $a(\omega)$. For x in $\mathcal{P}_F^{a(\omega)-1}$, $\omega(1+x)$ equals $(-1)^{\text{tr}(\gamma x)}$, where $\gamma = (N_{K/F}\pi)^{a(\omega)-1}/(\text{Tr}_{K/F}(\pi^{a(\omega)-1}))^2$ for π a generator of $\mathcal{P}_K$ and* tr *is the trace from $\mathcal{O}/\mathcal{P} \approx k_F$* to $\mathbb{F}_2$.

Proof: The maps $x \mapsto (-1)^{\text{tr}(\gamma x)}$ and $x \mapsto \omega(1+x)$ are quadratic characters of $\mathcal{P}_F^{a(\omega)-1}/\mathcal{P}_F^{a(\omega)}$, so it suffices to check that the kernels agree. The kernel of ω consists of norms from K^*. By [14; Chap. V] we see that the kernel of ω on $\mathcal{P}_F^{a(\omega)-1}/\mathcal{P}_F^{a(\omega)}$ is

$$\{\text{Tr}_{K/F}(z) + N_{K/F}(z) \mid z \in \mathcal{P}_K^{a(\omega)-1}\}/\mathcal{P}_K^{a(\omega)}.$$

By parameterizing $\mathcal{P}_K^{a(\omega)-1}/\mathcal{P}_K^{a(\omega)}$ by elements of $\mathcal{O}_F/\mathcal{P}_F$ via choice of an element of K of valuation $a(\omega)-1$, we see that the kernel is $((\mathrm{Tr}_{K/F}\pi^{a(\omega)-1})^2/N_{K/F}\pi^{a(\omega)-1})\{w+w^2 \mid w \in \mathcal{O}/\mathcal{P}\}$. This is clearly the kernel of $x \mapsto \mathrm{tr}(\tau x)$.

Example 8.16.1: We may compute $\omega(1-4y)$ for $v(y) \geq 0$ by use of (8.16). The result is

$$\omega(1-4y) = (-1)^{a(\omega)\cdot \mathrm{tr}(y)}.$$

This is clear if $a(\omega)$ is even by (8.7.2). If $a(\omega)$ is odd, we have $a(\omega)-1 = 2v(2)$ and appropriate choice of π in the previous Lemma shows 4γ is congruent to 1 modulo $\mathcal{P}$. In particular, $\omega(-3) = (-1)^{(\dim k)a(\omega)}$.

In order to utilize (8.15) we must compute the map induced on $\mathcal{P}_K^n/\mathcal{P}_K^{n+1}$ by the norm map for elliptic curves. When $3v(a_1) \geq a(\omega)$ we see easily from (8.10) that N_n is the zero map when $a(\omega)$ is divisible by 3 and is surjective otherwise. Further, under this condition on $v(a_1)$, $\omega(\Delta) = \omega(-3)$.

Theorem 8.17: *Let E be a supersingular curve with good reduction over the local field F of residue characteristic two. Let ω be a quadratic character of F^*. If in some minimal Weierstrass model for E, $3v(a_1) \geq a(\omega)$, then $\omega(\Delta) = (-1)^{\dim(E(F)/\mathsf{N}E(K))}$. In particular, conjecture* 3.1 *is true in this case.*

Proof: For a curve of good reduction, $\epsilon(E, \omega) = \omega(-1)$. Hence conjecture 3.1 follows from the claimed value of $\omega(\Delta)$ in the theorem statement. For unramified ω, the result is known from section 6. If ω is ramified, we apply the result of (8.15) together with the remarks on N_n preceeding the theorem. Then $\dim(E(F)/\mathsf{N}E(K))$ is congruent to $a(\omega)\cdot \dim_{\mathbb{F}_2}(k_F)$ in all cases. From the example following (8.16) we see that the statement of the theorem results.

The only remaining case to which these methods apply is when $3v(a_1) = a(\omega)-1$. If $v(a_1)$ is smaller, with respect to $a(\omega)$, more terms in the formal group law are necessary to analyze the norm map.

To analyze N_n in this final case we need the following Lemma. It can be easily shown using the modification of discriminants for polynomials over characteristic 2 fields, but we give a proof in the spirit of the preceeding investigation.

LEMMA 8.18: *Let k be a finite extension of $\mathbb{F}_2$. Consider the endomorphism $\phi(w) = \alpha w + \beta w^2 + w^4$ of k, where $\beta \in k$ and $\alpha \in k^*$. Then* $\dim_{\mathbb{F}_2}(\ker(\phi)) \equiv \mathrm{tr}_{k/\mathbb{F}_2}(1 + \beta^3/\alpha^2)$ *modulo* 2.

PROOF: The cardinality of Ker (ϕ) is 1 plus the number of roots of the separable cubic $Q(w) = \alpha + \beta w + w^3$. Let ℓ/k be the extension obtained by adjoining the roots of $Q(w) = 0$ to k. Thus the dimension of $\mathrm{Ker}(\phi)$ is odd if and only if $[\ell : k]$ is even. By Hensel's lemma there exist unramified extensions L and K of $\mathbb{Q}_2$ with residue fields ℓ and k respectively such that L is obtained by adjoining the roots of the cubic $\tilde{Q}(w) = A + Bw + w^3$ to K, and $\tilde{Q}$ reduces modulo the prime ideal of K to Q. Hence $[\ell : k] = [L : K]$, and we discover if $[L : K]$ is even by examining the discriminant $-4B^3 - 27A^2$. Thus $[\ell : k]$ is even if and only if $-4B^3/A^2 - 27$ is not a square in K. Since $-4B^3/A^2 - 27 = 1 - 4(7 + B^3/A^2)$, this discriminant is a nonsquare if and only if there is a quadratic character taking nontrivial value on it. All characters of conductor exponent less than or equal to twice the K-valuation of 2 clearly are trivial on this quantity. For the quadratic characters of K^* of maximal conductor exponent, example (8.16.1) shows that the value is $(-1)^{\mathrm{tr}(1+B^3/A^2)}$. Since the trace is computed from the residue field k to $\mathbb{F}_2$, we see that $\dim \mathrm{Ker}(\phi)$ is odd if and only if $\mathrm{tr}_{k/\mathbb{F}_2}(1 + \beta^3/\alpha^2)$ is odd.

THEOREM 8.19: *Let E be a supersingular elliptic curve with good reduction over F. Let ω be a quadratic character such that in a minimal Weierstrass model $3v(a_1) = a(\omega) - 1$. Then $\omega(\Delta) = (-1)^{\dim(E(F)/\mathsf{N}E(K))}$, and conjecture* (3.1) *is true in this case.*

PROOF: We notice from (8.15.1) that in this case $\omega(\Delta) = \omega(1 - 4 + a_1^3/a_3) = \omega(-3)\omega(1 + a_1^3/a_3) = \omega(-3) \cdot (-1)^{\mathrm{tr}(\gamma a_1^3/a_3)}$ for γ as in (8.16). On the other hand, the map N_n of (8.15) is given by $\mathsf{N}_n(z) = \bar{z} \cdot \mathrm{tr}(\pi^n) + \bar{z}^2 \cdot a_1 N(\pi)^n + \bar{z}^4 \cdot a_3 N\pi^{2n}$, where $z = \bar{z} \cdot \pi^n \in \mathcal{P}_K^n$ with $\bar{z} \in \mathcal{O}_F$. Identifying $\mathcal{P}_K^n/\mathcal{P}_K^{n+1}$ and $\mathcal{P}_F^{2n}/\mathcal{P}_F^{2n+1}$ with k_F, we may apply (8.18) with $\alpha = \mathrm{tr}(\pi^n)/(a_3 N\pi^{2n})$, $\beta = a_1/(a_3 N\pi^n)$. Hence the cokernel of N_n has $\mathbb{F}_2$-dimension congruent mod 2 to $\mathrm{tr}_{k/\mathbb{F}_2}(a_1^3 N\pi^n/a_3(\mathrm{tr}\pi^n)^2 + 1)$ by (8.18).

Recall that $\gamma = N\pi^{a(\omega)-1}/(\mathrm{tr}\ \pi^{a(\omega)-1})^2$, and notice that $\gamma a_1^3/a_3$ and $a_1^3 N\pi^n/a_3(\mathrm{tr}\pi^n)^2$ are units congruent modulo the prime ideal of $\mathcal{O}_K$ (since $\mathrm{tr}\ \pi^{a(\omega)-1} = \mathrm{tr}(\pi^{a(\omega)-1} - (N\pi^n)\pi^n) + \mathrm{tr}(\pi^n)N\pi^n$ and $(N\pi^n)\pi^n = \pi^{a(\omega)-1} \cdot \epsilon$ with $\epsilon - 1 \in \mathcal{P}_F^{a(\omega)-1}$ [14; Chap IV.2 Prop. 5]).

Thus the $\mathbb{F}_2$-dimension of the cokernel of N_n is congruent to

$\mathrm{tr}_{k/\mathbb{F}_2}(\gamma a_1^3/a_3+1)$. Since $\dfrac{a(\omega)-1}{3} \equiv a(\omega)-1$ modulo 2, we have

$$\begin{aligned}(-1)^{\dim(E(F)/NE(K))} &= (-1)^{(a(\omega)-1)\dim(k)+\mathrm{tr}(\gamma a_1^3/a_3+1)}\\ &= (-1)^{a(\omega)\dim k}(-1)^{\mathrm{tr}(\gamma a_1^3/a_3)}\\ &= \omega(-3)\,\omega(1+a_1^3/a_3)\\ &= \omega(\Delta).\end{aligned}$$

To provide further evidence for the conjecture (3.1) we examine the case in which the exponent of the Artin conductor is 2.

PROPOSITION 8.20: *Let F be a local field whose residue field k_F has characteristic 2. Then the exponent of the Artin conductor of the elliptic curve E defined over F is $a(E)=2$ if and only if E has reduction of Kodaira type IV or IV*.*

PROOF: Since conductor and Kodaira type are invariant of unramified base change, we may replace F by its unramified closure M. By [15; §3] $a(E)=2$ if and only if E has additive reduction and, for each prime $\ell \neq 2$, the ℓ-division field of E is tamely ramified. Let L be the 3-division field of E over M. Since $\mathrm{Gal}(L/M)$ can be represented in $GL_2(\mathbb{F}_3)$ and $|GL_2(\mathbb{F}_3)| = 48$ we have $a(E) = 2$ if and only if E has additive reduction and $|\mathrm{Gal}(L/M)|$ divides 3. In fact $|\mathrm{Gal}(L/M)| = 3$, since L must ramify by [15].

If indeed $|\mathrm{Gal}(L/M)|=3$, let g be a generator for $\mathrm{Gal}(L/M)$ represented as a matrix in $GL_2(\mathbb{F}_3)$. Then 1 is an eigenvalue of g. Hence E has a point of order 3 defined over M. Conversely, if E has a point of order 3 defined over M, then by choosing suitable basis for E_3, $\mathrm{Gal}(L/M)$ is contained in $\begin{pmatrix}1 & *\\ 0 & 1\end{pmatrix}$, using the fact that $\mu_3 \subset M$ to get determinant 1. Hence $a(E)=2$ if and only if E has additive reduction and a point of order 3 over M.

Suppose E has additive reduction. Then $E_0(M)/E_1(M) \approx k_M$ and $E_1(M)$ are divisible by 3. Hence $E(M)$ contains a point of order 3 if and only if $[E(M): E_0(M)]$ is divisible by 3. Equivalently, by the table, [17, pg. 46], E has reduction of Type IV or IV*.

REMARK: It follows from the discussion above that if k_F does not contain the cube roots of unity the image of the ℓ-adic representation for $\ell = 3$ is nonabelian when $a(E) = 2$. Thus σ_E is irreducible under these circumstances.

REMARK 8.21: One can see from the algorithm [17] that E has reduction of type IV over F if and only if there is a generalized Weierstrass model (7.0.1) for E over $\mathcal{O}_F$ whose coefficients satisfy $\pi_F \mid a_1, a_2$; $\pi_F \parallel a_3$; $\pi_F^2 \mid a_4, a_6$. If we pass to a ramified cubic extension R of F and take for E over $\mathcal{O}_R$ the Weierstrass model with coefficients $A_i = a_i \pi_R^{-i}$ then it is easy to see that E has supersingular good reduction over R. Similarly, E has reduction of type IV* over F if and only if we have $\pi_F \mid a_1$, $\pi_F^2 \mid a_2$, $\pi_F^2 \parallel a_3$, $\pi_F^3 \mid a_4$, $\pi_F^4 \mid a_6$. We then obtain a model for E over $\mathcal{O}_R$ with supersingular reduction by taking coefficients $A_i = a_i \pi_R^{-2i}$. By the formula for the discriminant we have modulo $\mathcal{P}_F^{2v_F(2)+4v_F(a_3)+1}$

$$\Delta_F \equiv -3a_3^4 + a_1^2 a_3^2(a_1 a_3 + 2a_4) - a_1^4(a_1^2 a_6 - a_1 a_3 a_4 - a_4^2 + a_2 a_3^2) \qquad (8.21.1)$$

COROLLARY 8.22: *Suppose that E has reduction of type IV or IV* over F and that in a generalized Weierstrass model for E we have* $v_F(a_1^3/a_3) \geq a(\omega) - 1$, *where* $a(\omega)$ *is the exponent of the Artin conductor of the quadratic character* ω *of F*. If the cube roots of unity are contained in F then Conjecture* 3.1 *is valid for E and* ω.

PROOF: There exists a ramified Galois cubic extension R of F. The curve E has supersingular reduction over R by the above Remark. Moreover, from our hypotheses on $v_F(a_1^3/a_3)$ and the fact that $a_R(\omega) = 3a_F(\omega) - 2$ we find that $3v_R(A_1) \geq a_R(\omega) - 1$. Hence the conjecture is valid for E and ω over R by Theorems 8.17 and 8.19. It then holds over F by Propositions 3.4 and 3.5, which show that odd Galois change of base doesn't change the quantities in the conjecture.

To cover the case in which F does not contain the cube roots of unity we resort to an argument using the formula of Theorem 7.6.

LEMMA 8.23: *Suppose that E has reduction of type IV or IV* over F and that K is a ramified quadratic extension of F corresponding to the character* ω *of F*. Then* $|E(F)/\mathrm{N}E(K)| = c_F^\omega |k_F|^t$ *where* $c_F^\omega = [E^\omega(F) : E_0^\omega(F)]$ *and t is an integer.*

We have the following possibilities for t according to types of *reduction of E and E^ω:*

$E \backslash E^\omega$	II	II^*	$I_\nu^*,\ \nu \equiv 0(4)$
IV	$\frac{1}{3}(a(\omega)+1)$	$\frac{1}{3}(a(\omega)-1)$	$\frac{1}{3}\left(a(\omega)-\frac{\nu}{4}\right)$
IV*	$\frac{1}{3}(a(\omega)-1)$	$\frac{1}{3}(a(\omega)+1)$	$\frac{1}{3}\left(a(\omega)-2-\frac{\nu}{4}\right)$

Moreover,

$$\kappa(E, \omega) = (-1)^{\dim E(F)/\mathrm{N}E(K)} = \begin{cases} \omega(-3)(-1)^{\dim k_F} & E^\omega \text{ type II, II}^*, \\ \omega(-3)(-1)^{[\mathrm{ord}_2(c_F^\omega)]+\frac{\nu}{4}(\dim k_F)} & E^\omega \text{ type } \quad \mathrm{I}_\nu^*. \end{cases}$$

Proof: Using the fact that E has conductor 2 by Proposition 8.20 and the conductor-discriminant formula, or else from the above Remark, we see that $v_F(\Delta_F) = 4$ or 8 according to whether E has reduction of type IV or IV*. Here Δ_F is a minimal discriminant for E over F and in the notation of Theorem 7.6, $v_F(u_F) = 0$. Over K, the exponent of the Artin conductor of E remains $a_K(E) = 2$, for example because the 3-division field remains tamely ramified. By Proposition 8.20, E has reduction of type IV or IV* over K, and the same constraints apply to $v_K(\Delta_K)$, where Δ_K is the minimal discriminant of E over K. Thus $v_K(\Delta_K) = v_K(\Delta_F) - 12v_K(u_K) = 2v_F(\Delta_F) - 12v_K(u_K)$. The only possibilities are either that E has type IV over F, type IV* over K and $v_K(u_K) = 0$ or else that E has type IV* over F, type IV over K and $v_K(u_K) = 1$. Let Δ_F^ω be the minimal discriminant for E^ω over F. Then

$$v_F(\Delta_F^\omega) = v_F(\Delta_F d^6) - 12v_F(u_F^\omega)$$

wnere d is the discriminant of K over F and hence $v_F(d) = a(\omega)$. Moreover $a_F(E^\omega) = \max(a_F(E), 2a(\omega)) = 2a(\omega)$ by an argument along the lines of [14, Chap. VI, §2, Proposition 5]. The conductor-discriminant formula gives

$$n_F^\omega + 4a(\omega) + 12v_F(u_F^\omega) = \begin{cases} 5 & E \text{ type IV over } F, \\ 9 & E \text{ type IV* over } F. \end{cases} \tag{8.23.1}$$

In particular, $n_F^\omega \equiv 1 \pmod 4$ and by the table [17, p. 46] the only possibilities are

$$n_F^\omega = \begin{cases} 1 & E^\omega \quad \text{type II}, \\ 9 & E^\omega \quad \text{type II}^*, \\ 5+\nu & E^\omega \quad \text{type } I_\nu^*, \nu \equiv 0(4). \end{cases}$$

From these values, we recalculate $v_F(u_F^\omega)$ in (8.23.1) and determine $t = v_F(u_F^\omega) - v_K(u_K)$ as given above.

Now c_F, $c_K \in \{1, 3\}$, while $E(F)/\mathbb{N}E(K)$ is a 2-group. Hence by Theorem 7.6 $|E(F)/\mathbb{N}E(K)| = c_F^\omega |k_F|^t$. The sign $\kappa(E, \omega)$ can then be determined using the fact that $a(\omega) \cdot \dim k_F$ is even or odd according to whether $\omega(-3) = 1$ or -1, and that $c_F^\omega = 1$ if E^ω has reduction of type II or II*.

Proposition 8.24: *Suppose that E has reduction of type IV or IV* and that in the minimal model of* Remark 8.21, $v_F(a_1^3/a_3) \geq a(\omega) - 1$. *Then Conjecture* 3.1 *is valid for E and* ω.

Proof: In view of Theorem 6.2, we may assume that ω is a ramified character. Hence $2 \leq a(\omega) \leq 2v_F(2) + 1$. It follows from our hypothesis on $v_F(a_1^3/a_3)$ and the inequalities on $v_F(a_i)$ in Remark 8.21 that $\Delta_F \equiv -3a_3^4 + a_1^3 a_3^3 \pmod{\mathscr{P}_F^{a(\omega)+4v_F(a_3)}}$. Hence $\omega(\Delta_F) = \omega(1 + a_1^3 a_3^{-1}) \cdot \omega(-3)$.

Next we obtain a model for E^ω over F by putting $X = x_0 \delta \pi_F^{2s}$, $Y = y_0 \delta^2 \pi_F^{3s}$ in (7.4.3), with s chosen as the smallest integer such that the coefficients in the resulting generalized Weierstrass model are in $\mathcal{O}_F$. These coefficients are

$$a_1' = \delta \pi_F^s a_1, \quad a_3' = \delta^3 \pi_F^{3s} a_3, \quad a_2' = \delta \pi_F^{2s}(\gamma a_1^2 + a_2)$$
$$a_4' = \delta^2 \pi_F^{4s}(2ya_1a_3 + a_4), \quad a_6' = \delta^3 \pi_F^{6s}(\gamma a_3^2 + a_6).$$

Recall that $\delta = 1 - 4\gamma$, $v_F(\delta)$ is 0 or 1 according to whether $a(\omega)$ is even or odd, and $v_F(\gamma) = 1 - a(\omega)$.

One now checks that from the conditions on $v_F(a_1^3/a_3)$ and on $v_F(a_i)$ in Remark 8.21, s is determined by consideration of a_6', so that $v_F(\delta^3 \pi_F^{6s} \gamma a_3^2) \geq 0$. Using the inequality $a(\omega) \geq 2$ we find that $v_F(\delta \pi_F^{2s}) \geq 0$ and then in fact $v_F(a_i') \geq 1$ for all $i = 1, 2, 3, 4, 6$. Furthermore, consideration modulo 2 and 3 shows that the only possibilities are

$$v_F(\delta^3\pi_F^{6s}\gamma a_3^2) = \begin{cases} 1 & a(\omega) \equiv 2v_F(a_3) \quad (3), \\ 3 & a(\omega) \equiv 2v_F(a_3) + 1\ (3), \\ 5 & a(\omega) \equiv 2v_F(a_3) - 1\ (3). \end{cases} \tag{8.24.1}$$

In the first case above, it follows that $v_F(a_6') = 1$ and that E has reduction of type II by the algorithm [17]. Hence $\kappa(E, \omega) = \omega(-3)(-1)^{\dim k_F}$ by Lemma 8.23. But $a(\omega) \equiv 2v_F(a_3)$ (mod 3) together with $v_F(a_1^3/a_3) \geq a(\omega) - 1$ forces $v_F(a_1^3/a_3) \geq a(\omega)$. Hence $\omega(-\Delta_F) = \omega(3)$, and $\omega(-\Delta)\kappa(E, \omega) = \epsilon(E, \omega)$ by Lemma 8.24.2 below.

In the second (respectively, third) case of (8.24.1) one checks further that $v_F(a_3') \geq 2$, $v_F(a_4') \geq 3$, $v_F(a_6') = 3$ (respectively, 5). [To do this it must be observed that now $v_F(\delta\pi_F^{2s}) \geq 1$ if E has reduction of type IV; that is, if $v_F(a_3) = 1$]. If in fact $v_F(a_6') = 5$, we arrive at type II* for E^ω in the algorithm [17], and $\omega(-\Delta)\kappa(E, \omega) = \epsilon(E, \omega)$ as above.

If $v_F(a_6') = 3$, then E^ω has reduction of type I_0^* and $c_F^\omega - 1$ is the number of roots in k_F of reduction of $P(T) = T^3 + a_{2,1}'T^2 + a_{4,2}'T + a_{6,3}'$, in the notation of [17, (8.1)]. Modulo π_F, the following congruences hold:

$$a_{2,1}' \equiv \delta\pi_F^{2s-1}\gamma a_1^2, \quad a_{4,2}' \equiv 0, \quad a_{6,3}' \equiv \delta^3\pi_F^{2s-3}\gamma a_3^2 \not\equiv 0.$$

By making the change of variables $U = T^{-1}$, we may apply Lemma 8.18 to conclude that $\mathrm{ord}_2(c_F^\omega) \equiv \mathrm{Tr}(1 + b) \equiv \mathrm{Tr} b + \dim k_F$ (mod 2), where b is the residue in k_F of $(a_{2,1}')^3/a_{6,3}'$ and hence of $\gamma^2 a_1^6 a_3^{-2}$. But $\mathrm{Tr}(\gamma^2 a_1^6 a_3^{-2}) = \mathrm{Tr}(\gamma a_1^3 a_3^{-1})$. Hence $(-1)^{c_F^\omega} = \omega(1 + a_1^3 a_3^{-1})(-1)^{\dim k_F}$ by Lemma 8.16, and therefore $(-1)^{c_F^\omega} = \omega(-3\Delta)(-1)^{\dim k_F}$. Hence by Lemma 8.23, $\kappa(E, \omega) = \omega(\Delta)(-1)^{\dim k_F}$. Conjecture 3.1 now holds by the Lemma below.

LEMMA 8.24.2: *Suppose that σ_E has conductor exponent 2 and F has even residue characteristic. Then $\epsilon(E, \omega) = \omega(-1)\,(-1)^{\dim k_F}$ when ω is ramified.*

PROOF: If σ_E is irreducible and has conductor exponent 2 it is in fact induced from a character θ of conductor exponent 1 of the unramified quadratic extension L (see, for example, *On the Local Langlands Conjecture for $GL(2)$*, Inv. Math. 46 (1979), Proposition 3.5). An application of 2.7 then shows that $\epsilon(E, \omega) = (-1)^{1+a(\omega)}\,\omega(-y^2)$ where y is a nonzero element of L such that $\mathrm{tr}_{L/F}(y) = 0$.

When $\dim k_F$ is odd we may take $y = \sqrt{-3}$ or $y = 1$ according to F having characteristic 0 or 2. In either case, $\dim k_F$ odd implies $\epsilon(E, \omega) = \omega(-3)(-1)^{(1+a(\omega))\dim(k)}$, which is precisely $\omega(-1)(-1)^{\dim k_F}$ by the previous computation of $\omega(-3)$. To conclude, recall the remark that $\dim k_F$ odd implies σ_E is irreducible, so the above applies. In case $\dim k_F$ is even, make a Galois cubic change of base, so that E attains good reduction and $\epsilon(E, \omega)$ is unchanged. For curves of good reduction the product of local signs is $\omega(-1)$, verifying the lemma.

9. Applications.

In this section we consider some applications of the results of previous sections. The first application deals with the relation of Kodaira types [17; §6] and the corresponding ℓ-adic representations. For example, it is well known that type I_0 implies that the image of the inertia subgroup is trivial, while type I_ν for $\nu > 0$ implies that the image of inertia is infinite.

THEOREM 9.1: *Let E be an elliptic curve of conductor exponent* 2 *and potential good reduction over a nonarchimedean local field F. The representation σ_E is irreducible if and only if $\epsilon(E, \omega) = -\omega(-1)$ for ramified quadratic characters ω.*

PROOF: When the residue characteristic is odd this follows from (2.8) and (2.4b). For even residue characteristic we apply (8.24.2) and obtain $\epsilon(E, \omega) = \omega(-1)(-1)^{\dim(k_F)}$. As pointed out in the proof of that result, σ_E is irreducible when $\dim(k_F)$ is odd. When $\dim(k_F)$ is even, σ_E is reducible (and of conductor exponent zero) after restriction to a normal subgroup of index 3. By Frobenius reciprocity this implies that σ_E is reducible.

COROLLARY 9.1.1: *Let E be an elliptic curve of conductor exponent* 2 *and Kodaira type III or III* over a local field F of residue field cardinality q. Then σ_E is irreducible if $q \equiv 3$ (modulo* 4) *and is reducible if $q \equiv 1$ (modulo* 4).

PROOF: The algorithm and table of [17] show that type III or III* curves have $E(F)/E_0(F)$ order 2 and odd discriminant valuation. If the residue characteristic is odd, $E(F)_2$ has order 2 and the number of points in $E(K)_2$ for a ramified quadratic extension K is 4 when $K = F(\sqrt{\Delta})$ and 2 otherwise. Thus $\lambda(E, \omega_K) = \omega_K(-\Delta)$ in these cases.

From the results of section 5 we have $\epsilon(E, \omega) = \lambda(E, \omega)\omega(-\Delta) = 1$. The result now follows from (9.1).

The remaining applications are of a global nature. They involve the main formula of [8] which we restate here. In the sequel F will denote a global field and K a separable quadratic extension described by a character $\omega = \Pi\, \omega_v$ of the idele class group of F.

THEOREM 9.2 [8]: *Let E be an elliptic curve over a global field F* (char $F \neq 2$). *Let K be a quadratic extension of F. If the 2-primary component of the Tate–Shafarevitch group* Ш(E, K) *is finite, then*

$$(-1)^{\operatorname{rank} E(K)} = \prod_v \kappa(E_v, \omega_v).$$

REMARK: The product is taken over all places v of F. The hypotheses are conjecturally always true (Ш should be finite) and are checkable by descent in many cases.

THEOREM 9.3: *Let E be an elliptic curve over the global field F* (char $F \neq 2$) *with integral j-invariant and cube-free conductor. If K is a quadratic extension of F such that* Ш$_{2^\infty}(E, K)$ *is finite, then* rank $E(K)$ *is congruent* modulo 2 *to the number of places v of F ramified in K such that σ_{E_v} is irreducible.*

PROOF: We apply (9.2) to conclude $(-1)^{\operatorname{rank} E(K)} = \Pi\, \kappa(E_v, \omega_v)$. Since ω is an idele class character, $\omega(-\Delta) = 1$. Thus $(-1)^{\operatorname{rank} E(K)} = \Pi\, \kappa(E_v, \omega_v)\omega_v(-\Delta) = \Pi\, \epsilon(E_v, \omega_v)$, by the known cases of (3.1). By (2.4) we have $\epsilon(E_v, \omega_v) = \omega_v(-1)$ if v is not ramified in K or σ_{E_v} is reducible. By (2.4a) and (9.1) we have $\epsilon(E_v, \omega_v) = -\omega_v(-1)$ when v is ramified and σ_{E_v} is irreducible. This establishes the result.

As a final application we study a compatibility of the Birch, Swinnerton–Dyer conjecture under twisting. Let E be an elliptic curve over a global field F which has an L-series given by an automorphic L-function $L(s, \pi)$ for some representation π of $GL(2)$. When $F = \mathbb{Q}$ this just means that the L-series is the Dirichlet series of a modular form. Further assume that $\epsilon(\pi_v) = \epsilon(\sigma_v)$, where $\pi = \bigotimes \pi_v$. This has been checked (by Deligne, unpublished) when E is a quotient of the Jacobian of a modular curve and v has odd residue characteristic. A consequence of the Birch, Swinnerton–Dyer conjecture is the

PARITY CONJECTURE: rank $E(F) \equiv \operatorname{ord}_{s=1} L(E, s)$ (modulo 2).

We now check that under assumptions as in (9.2), the parity conjecture is simultaneously true or false for all twists of E.

THEOREM 9.4: *Let E be an elliptic curve satisfying the assumptions and hypothesis above. Then the parity conjecture for E implies the parity conjecture for E^{ω}, assuming the truth of conjecture* 3.1.

PROOF: The parity of the order of zero at $s = 1$ of $L(E, s)$ may be determined from the functional equation $L(E, s) = \epsilon(E) L(E, 1 - s)$. Under the above assumptions, $\epsilon(E) = \prod_v \epsilon(\sigma_{E_v})$. Hence the parity conjecture is equivalent to $(-1)^{\operatorname{rank} E(F)} = \prod_v \epsilon(\sigma_{E_v})$. Since rank $E(K) =$ rank $E(F) +$ rank $E^{\omega}(F)$ we have that $(-1)^{\operatorname{rank} E(K)} = \prod_v \epsilon(E_v, \omega_v)$ if and only if the parity conjecture is simultaneously true (or false) for E and E^{ω}. Conjecture (3.1) allows $\epsilon(E_v, \omega_v)$ to be replaced by $\kappa(E_v, \omega_v)\, \omega_v(-\Delta)$, and then the equation is a consequence of (9.2).

COROLLARY: *Let E be an elliptic curve over a global field F* (char $F \neq 2$) *with good or potential multiplicative reduction above all places v of F of even residue characteristic. Then if the order of zero of $L(E, s)$ at $s = 1$ has the same parity as* rank $E(F)$, *the same is true for the twisted curve E^{ω} if $Ш_{2^{\infty}}(E, K)$ is finite.*

PROOF: Conjecture 3.1 will be true for all places of F under the hypotheses, so this follows from (9.4).

REMARK: Additive reduction may be allowed at places of even residue characteristic under certain circumstances. This results from the same proof as above, taking into account (8.24).

REFERENCES

[1] A. BRUMER and K. KRAMER: The rank of elliptic curves. *Duke Math J. 44(4)* (1972) 715–743.

[2] B. BIRCH and W. KUYK Editors: Modular functions of one variable IV. *Lecture Notes in Math. 475*, Springer–Verlag 1975.

[3] P. DELIGNE: Formes modulaires et representations de $GL(2)$, in Modular functions of one variable II. *Lecture Notes in Math. 349*, Springer-Verlag 1973, 55–106.

[4] P. DELIGNE: Les constantes des equations fonctionelles des fonctions L, in Modular functions of one variable II. *Lecture Notes in Math. 349*, Springer-Verlag 1973, 501–579.

[5] P. DELIGNE: Les constantes locales de l'equation fonctionelle de la fonction L d'Artin d'une representation orthogonale. *Inv. Math. 35* (1976) 299–316.

[6] A. FROHLICH and J. QUEYRUT: On the functional equation of the Artin L-function for characters of real representations. *Inv. Math. 20* (1973) 125–138.

[7] K. KRAMER: Two descent for elliptic curves in characteristic two. *Trans. AMS 232* (1977) 279–295.

[8] K. KRAMER: Arithmetic of elliptic curves upon quadratic extension. *Trans. AMS. 264* (1981) 121–135.

[9] S. LANG: Algebraic groups over finite fields. *Amer. J. Math. 78*, no. 3 (1956) 555–563.

[10] R. LANGLANDS: Modular forms and ℓ-adic representations, in Modular functions of one variable II. *Lecture Notes in Math. 349*, Springer-Verlag 1973, 361–500.

[11] B. MAZUR: Rational poims of Abelian varieties with values in towers of number fields. *Inv. Math. 18* (1972) 183–266.

[12] J. MILNE: Weil-Châtelet groups over local fields. *Ann. Sci. Ecole Norm. Sup. 4* (1970) 273–284.

[13] A. OGG: Elliptic curves and wild ramification. *Amer. J. Math.* (1967) 1–21.

(14) J-P. SERRE: *Corps Locaux*, 2nd Edition, Hermann, Paris 1968.

[15] J-P. SERRE and J. TATE: Good reduction of abelian varieties. *Annals of Math. 88* (1968) 492–517.

[16] J. TATE: The arithmetic of elliptic curves. *Inv. Math. 23* (1974) 179–206.

[17] J. TATE: Algorithm for determining the type of a singular fiber in an elliptic pencil, in Modular functions of one variable IV. *Lecture Notes in Math. 476*, Springer-Verlag 1975.

[18] J. TATE: Number theoretic background, in Automorphic Forms, Representations and L-functions, *Proc. Symp. in Pure Math. XXXIII* Part 2 (1979) 3–26.

K. Kramer
Department of Mathematics
Queens College (CUNY)
Flushing, N.Y. 11367
U.S.A.

J. Tunnell
Department of Mathematics
Princeton University
Princeton,N.J. 08544
U.S.A.