COMPOSITIO MATHEMATICA

Parity conjectures for elliptic curves over global fields of positive characteristic

Fabien Trihan and Christian Wuthrich

Compositio Math. **147** (2011), 1105–1128.

doi:10.1112/S0010437X1100532X

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

Compositio Math. 147 (2011) 1105–1128
doi:10.1112/S0010437X1100532X

Parity conjectures for elliptic curves over global fields of positive characteristic

Fabien Trihan and Christian Wuthrich

Abstract

We prove the p-parity conjecture for elliptic curves over global fields of characteristic $p > 3$. We also present partial results on the ℓ-parity conjecture for primes $\ell \neq p$.

1. Introduction

Let K be a global field and let E be an elliptic curve defined over K. The conjecture of Birch and Swinnerton-Dyer asserts that the rank of the Mordell–Weil group $E(K)$ is equal to the order of vanishing of the Hasse–Weil L-function $L(E/K, s)$ as $s = 1$. A weaker question is to know whether these two integers have at least the same parity. This seems more approachable because the parity of the order of vanishing on the analytic side can by expressed in more algebraic terms through local root numbers; at least when the L-function is known to have an analytic continuation. Let $w(E/K) \in \{\pm 1\}$ be the global root number of E over K which is equal to the product of local root numbers $\prod_v w(E/K_v)$ as v runs over all places in K. The local terms $w(E/K_v)$ were defined by Deligne without reference to the L-function, see [Roh94] for the definition. Hence we can formulate the following conjecture.

Full parity conjecture. We have $(-1)^{\operatorname{rank} E(K)} = w(E/K)$.

This conjecture is unproven except for specific cases. We will focus on the following easier question. Let $Ш(E/K)$ be the Tate–Shafarevich group defined as the kernel of the localisation maps $H^1(K, E) \to \prod_v H^1(K_v, E)$ in Galois cohomology. For a prime ℓ, the ℓ-primary Selmer group $\mathrm{Sel}_{\ell^\infty}(E/K)$ fits into an exact sequence

$$0 \to E(K) \otimes {}^{\mathbb{Q}_\ell}\!/\!_{\mathbb{Z}_\ell} \to \mathrm{Sel}_{\ell^\infty}(E/K) \to Ш(E/K)[\ell^\infty] \to 0. \qquad (1)$$

If the characteristic of K is prime to ℓ, we may define it as the preimage of $Ш(E/K)[\ell^\infty]$ under the map $H^1(K, E[\ell^\infty]) \to H^1(K, E)[\ell^\infty]$. If the characteristic is equal to ℓ, then one should use flat instead of Galois cohomology, see § 4 for definitions. The theorem of Mordell–Weil shows that the dual of $\mathrm{Sel}_{\ell^\infty}(E/K)$ is a finitely generated $\mathbb{Z}_\ell$-module, whose rank we will denote by r_ℓ. In particular, (1) is a short exact sequence of finite cotype $\mathbb{Z}_l$-modules for any prime ℓ. Since it is conjectured that rank $E(K) = r_\ell$, we can make the following conjecture, which seems more approachable as it links two algebraically defined terms.

ℓ-parity Conjecture. Let ℓ be a prime. We have $(-1)^{r_\ell} = w(E/K)$.

Received 15 January 2010, accepted in final form 10 December 2010, published online 4 May 2011.
2010 Mathematics Subject Classification 11G40 (primary), 11G05, 11G07 (secondary).
Keywords: parity conjecture, elliptic curves, function fields, Birch and Swinnerton-Dyer conjecture.
The first author is supported by EPSRC.

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

These conjectures have attracted much attention in recent years and the ℓ-parity conjecture is now known in many cases, in particular when the ground field is $K = \mathbb{Q}$ by work of the Dokchitser brothers [Dok05, DD08, DD09a, DD09b, DD10], Kim [Kim07], Mazur and Rubin [MR07], Nekovář [Nek01, Nek09, Nek10], Coates *et al.* [CFKS10] and others.

In this article, we restrict our attention to the case of positive characteristic. So, we suppose from now on that K is a global field of characteristic $p > 3$ with constant field $\mathbb{F}_q$. The main result of this article is the following theorem.

Theorem 1. *The p-parity conjecture holds for any elliptic curve E over a global field K of characteristic $p > 3$.*

The proof consists of two steps: first a local calculation linking the local root number to local data on the Frobenius isogeny on E, carried out in § 3; followed by the use of global duality in § 5. Luckily, we do not have to treat all individual cases of bad reduction for the local considerations, since we are able to use a theorem of Ulmer [Ulm05] to reduce to the semistable case. This is done in § 2.

The proof follows closely the arguments in [DD08] and Fisher's appendix of [Dok05]. We repeat it here in details, both for completeness and to make the reader aware of a few subtleties; for instance, it is to note that the Frobenius isogeny F and its dual V do not play an interchangeable role.

The hardest part concerns the global duality. The relevant dualities that we need for our conclusion have never appeared in the literature and we are forced to prove them. We think that it is worthwhile to include in § 8 a general formula for the parity of the corank of the p-primary Selmer group and a local formula for the root number in § 9.

Originally, global dualities have appeared in Cassels' work [Cas65] on the invariance under isogenies of the conjecture of Birch and Swinnerton-Dyer. It should be noted that one could use our duality statements to prove this in the case of characteristic $p > 0$, but there is no need for this. In fact it is known by [KT03] that the conjecture of Birch and Swinnerton-Dyer is equivalent to the finiteness of the Tate–Shafarevich group; and it is clear that the latter question is invariant under isogeny.

The second main result of this paper is a proof of the ℓ-parity conjecture when $\ell \neq p$ in some cases. Write μ_ℓ for the ℓth roots of unity.

Theorem 2. *Let E/K be an elliptic curve and let $\ell > 2$ be a prime different from p. Furthermore assume that both the following hold.*

(i) *The degree $a = [K(\mu_\ell) : K]$ is even.*

(ii) *The analytic rank of E does not grow by more than one in the constant quadratic extension $K \cdot \mathbb{F}_{q^2}/K$.*

Then the ℓ-parity conjecture holds for E/K.

The proof will be presented in § 10. Its main ingredients are the non-vanishing results of Ulmer in [Ulm05] and the techniques for proving the parity conjectures from representation theoretic considerations as explained in [DD09c, DD10].

Although the conditions will be fulfilled for many curves, the methods in this paper fail to give a complete proof of the ℓ-parity conjecture. See the remarks at the beginning of § 10 and the more detailed § 11 for an explanation of why we are not able to extend the proof any further.

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

1.1 Notations

The constant field of the global field K of characteristic $p > 3$ is the finite field $\mathbb{F}_q$ for some power q of p. Let C be a smooth, geometrically connected, projective curve over $\mathbb{F}_q$ with function field K. Let E/K be an elliptic curve, which we will assume to be non-isotrivial (i.e. the j-invariant of E is transcendental over $\mathbb{F}_q$). We fix a Weierstrass equation

$$E : y^2 = x^3 + Ax + B \tag{2}$$

with A and B in K and the corresponding invariant differential $\omega = dx/2y$. By $F : E \to E'$ we denote the Frobenius isogeny of degree p whose dual $V : E' \to E$ is the Verschiebung.

If $f : A \to B$ is a homomorphism of abelian groups, we write

$$z(f) = \frac{\#\mathrm{coker}(f)}{\#\mathrm{ker}(f)}$$

provided that the kernel and the cokernel of f are finite. For any abelian group (or group scheme) A and integer m, we denote by $A[m]$ the m-torsion part of it; and, for any prime ℓ, the ℓ-primary part will be denoted by $A[\ell^\infty]$.

The Pontryagin dual of an abelian group A is written $A^\vee$. If the Pontryagin dual of A is a finitely generated $\mathbb{Z}_\ell$-module for some prime ℓ, then we write $\mathrm{div}(A)$ for its maximal divisible subgroup and let A_{div} denote the quotient of A by $\mathrm{div}(A)$.

2. Reduction to the semistable case

Before, we start we should mention that the conjecture of Birch and Swinnerton-Dyer is known for isotrivial curves E by the work of Milne [Mil68]. Hence for the rest of the paper we will assume that E is not isotrivial as otherwise the parity conjectures are known. In particular, it follows from this assumption that E/K is ordinary. The parity conjecture is also known in the following cases.

Proposition 3. *Let A/K be an abelian variety over a function field of characteristic $p > 0$ and let ℓ be a prime ($\ell = p$ is allowed). The analytic rank of A/K is always greater or equal to the ℓ-corank of the Selmer group. If the analytic rank of A/K is zero, then the conjecture of Birch and Swinnerton-Dyer holds. If the analytic rank is one then it coincides with the $\mathbb{Z}_\ell$-corank of the ℓ-primary Selmer group.*

Note that if we restrict ourselves to elliptic curves and to the case $\ell \neq p$, then this result could already be deduced from the work of Artin and Tate [Tat95].

Proof. By [KT03, 3.2], the Hasse–Weil L-function of A/K can be expressed as an alternating product of characteristic polynomials of some operators ϕ_ℓ^i acting on a finite-dimensional $\mathbb{Q}_\ell$-vector space $H^i_{\mathbb{Q}_\ell}$, with $i = 0, 1, 2$. Then by [KT03, 3.5.1], the order at $s = 1$ of the Hasse–Weil L-function can be interpreted as the multiplicity of the eigenvalue 1 for the operator ϕ_ℓ^1 on $H^1_{\mathbb{Q}_\ell}$. Following the notations of 3.5 in [KT03], let $I_{3,\ell}$ denote the part of $H^1_{\mathbb{Q}_\ell}$ on which the operator $\mathrm{id} - \phi_\ell^1$ acts nilpotently and let $I_{2,\ell}$ denote the kernel of $\mathrm{id} - \phi_\ell^1$, such that we have the inclusions,

$$I_{2,\ell} \subset I_{3,\ell} \subset H^1_{\mathbb{Q}_\ell}.$$

Since by [KT03, 3.5.1] the operator $\mathrm{id} - \phi_\ell^i$ is an isomorphism for $i = 0, 2$, it follows that the analytic rank of A/K is equal to the dimension of $I_{3,\ell}$. On the other hand, it follows from [KT03, 3.5.5 and 3.5.6] that the ℓ-corank of the Selmer group of A/K is the dimension of $I_{2,\ell}$ so that we

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

deduce that the analytic rank of A/K is always greater or equal to the ℓ-corank of the Selmer group of A/K. If the analytic rank of A/K is trivial, so is the dimension of $I_{3,\ell}$. It implies that the dimension of $I_{2,\ell}$ is zero and by [KT03, 3.5.6], we conclude that the Mordell–Weil group is also of rank zero. We then conclude the proof of the assertion thanks to the main result 1.8 of [KT03]. If the analytic rank of A/K is one, then ϕ_ℓ^1 acts like the identity on $I_{3,\ell}$ and therefore $I_{2,\ell} = I_{3,\ell}$ and the second assertion immediately follows. □

The following proposition will be used at several places to reduce the conjecture to easier situations.

Proposition 4. *Let E/K be a non-isotrivial curve and L/K a separable extension. Let ℓ be a prime. Assume one of the following three conditions.*

(i) *The extension L/K is a Galois extension of odd degree and $\ell \neq p$.*

(ii) *The analytic rank of E does not grow in L/K.*

(iii) *The analytic rank of E does not grow by more than one in L/K and $\ell \neq p$.*

Then the ℓ-parity conjecture for E/K holds if and only if the ℓ-parity conjecture for E/L is known.

Proof. If condition (i) holds then the conclusion follows directly from [DD09c, Theorem 1.3]. Note already here that the complete paper [DD09c] and its proofs hold in our situation as long as $\ell \neq p$.

Suppose now as in condition (ii) that the analytic rank does not grow in L/K. Denote by A/K the Weil restriction of E under L/K and by B/K the quotient of A by the natural image of E in it. Since

$$L(E/L,s) = L(A/K,s) = L(E/K,s)\cdot L(B/K,s)$$

we see that the analytic rank of B/K is zero and therefore by Proposition 3, the full Birch and Swinnerton-Dyer conjecture holds. In particular, the Mordell–Weil rank of B/K is zero and its Selmer group is a finite group. Moreover, we have an exact sequence

$$\mathrm{Sel}_{\ell^\infty}(E/K) \to \mathrm{Sel}_{\ell^\infty}(A/K) \to \mathrm{Sel}_{\ell^\infty}(B/K), \tag{3}$$

and the kernel of the first map lies in $B(K)[\ell^\infty]$, which is a finite group. Hence we conclude that r_ℓ is equal to the corank of $\mathrm{Sel}_{\ell^\infty}(A/K)$ and, by [MR07, Proposition 3.1], this is the same as the corank of $\mathrm{Sel}_{\ell^\infty}(E/L)$. Hence we are able to deduce the ℓ-parity for E/K from the ℓ-parity for E/L.

Finally, suppose that $\ell \neq p$ and that the analytic rank grows exactly by one; so we are under condition (iii). Then we know by Proposition 3 that the rank of $\mathrm{Sel}_{\ell^\infty}(B/K)$ is less than or equal to one. We wish to exclude the possibility that it is zero, so assume by now that $\mathrm{Sel}_{\ell^\infty}(B/K)$ is finite. However, this means that $Ш(B/K)[\ell^\infty]$ is finite and hence the full conjecture of Birch and Swinnerton-Dyer holds by [KT03] again; so we reach a contradiction, since we would have $0 = \operatorname{rank} B(K) = \operatorname{ord}_{s=1} L(B/K,s) = 1$. Hence we have shown that the corank of $\mathrm{Sel}_{\ell^\infty}(B/K)$ is one.

Note that the left-hand map in (3) still has finite kernel. We will show now that right-hand map has finite cokernel, too. Let Σ be the finite set of places in K of bad reduction for E. Write $G_\Sigma(K)$ for the Galois group of the maximal separable extension of K which is unramified outside Σ. Note that from the definition of the Selmer group, we find the following diagram with

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

exact rows and columns.

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] & & \\
\mathrm{Sel}_{\ell^\infty}(A/K) \arrow[r] \arrow[d] & \mathrm{Sel}_{\ell^\infty}(B/K) \arrow[d] & & \\
H^1(G_\Sigma(L), A[\ell^\infty]) \arrow[r] \arrow[d] & H^1(G_\Sigma(K), B[\ell^\infty]) \arrow[r] \arrow[d] & H^2(G_\Sigma(K), E[\ell^\infty]) \arrow[r, "r"] & H^2(G_\Sigma(K), A[\ell^\infty]) \\
\bigoplus_{v\in\Sigma} H^1(K_v, A)[\ell^\infty] \arrow[r] & \bigoplus_{v\in\Sigma} H^1(K_v, B)[\ell^\infty] & &
\end{tikzcd}$$

We know that the bottom groups are finite as they are dual to $\varprojlim A(K_v)/\ell^k$ and $\varprojlim B(K_v)/\ell^k$ respectively. Hence we see from the snake lemma that we only have to prove that the kernel of r is finite. Shapiro's lemma shows that $H^2(G_\Sigma(K), A[\ell^\infty])$ is isomorphic to $H^2(G_\Sigma(L), E[\ell^\infty])$ and hence the map r is simply the restriction map. As its kernel will only get larger when increasing L, we may assume that L/K is Galois. Then the kernel of the restriction is contained in the part of $H^2(G_\Sigma(K), E[\ell^\infty])$ that is killed by $[L:K]$. Hence it is finite, because $H^2(G_\Sigma(K), E[\ell^\infty])$ is a discrete abelian group with finite $\mathbb{Z}_\ell$-corank.

Therefore, we conclude again that the corank of the ℓ-primary Selmer group increased by exactly one in L/K. □

Corollary 5. *If the ℓ-parity conjecture holds for all semistable elliptic curves, then it holds for all elliptic curves.*

Proof. Theorem 11.1 in [Ulm05] proves that there is a separable extension L/K such that the reductions of E becomes semistable and the analytic rank does not grow in L/K. □

The same argument also reduces the full parity conjecture to the semistable case.

3. Local computations

The following computations are purely local and we change the notations for this section. Let K be a local field of characteristic $p>3$ with residue field $\mathbb{F}_q$. The ring of integers is written $\mathcal{O}$, the maximal ideal $\mathfrak{m}$ and the normalised valuation by v. The elliptic curve E/K is given by the Weierstrass equation (2). By changing the equation, if necessary, we may suppose for this section that A and B are in $\mathcal{O}$.

Define L to be the minimal extension of K such that $E'(L)[p] = {}^{\mathbb{Z}}\!/\!{}_{p\mathbb{Z}}$, or equivalently that $E[F]$ is isomorphic to $\mu[p]$ as a group scheme over L. There is a representation

$$\rho : \mathrm{Gal}(L/K) \to \mathrm{Aut}(E'(L)[p]) \cong ({}^{\mathbb{Z}}\!/\!{}_{p\mathbb{Z}})^\times$$

which shows that $[L:K]$ divides $p-1$. Define $(-1/(L/K)) \in \{\pm 1\}$ to be the image of -1 under the composition of the reciprocity map and ρ

$$K^\times \to \mathrm{Gal}(L/K) \to ({}^{\mathbb{Z}}\!/\!{}_{p\mathbb{Z}})^\times.$$

Hence $(-1/(L/K)) = +1$ if and only if -1 is a norm from $L^\times$ to $K^\times$.

We will also consider $z_V = z(V : E'(K) \to E(K))$, which is a certain power of p. Put

$$\sigma = \sigma(E/K) = \begin{cases} +1 & \text{if } z_V \text{ is a square and} \\ -1 & \text{otherwise.} \end{cases}$$

It is important to note that we cannot define $z(F : E(K) \to E'(K))$ since its cokernel will never be finite.

Finally, as in the introduction, we let $w = w(E/K)$ be the local root number of E over K, as defined by Deligne and well explained in [Roh94]. The aim of this section is to show the following theorem.

Theorem 6. *Let K be a local field of characteristic $p > 3$. For any non-isotrivial elliptic curve E/K whose reduction is not additive and potentially good, we have $w(E/K) = (-1/(L/K)) \cdot \sigma(E/K)$.*

We will prove this theorem by treating each type of reduction separately. In the last section of this paper, we will prove this local theorem without the assumption on the reduction using global methods. See [DD09b, Conjecture 5.3] for the analogue in characteristic zero. In particular, the following computations show that the analogy should take places above p in characteristic zero to supersingular places in characteristic p.

Recall the definition of the Hasse invariant $\alpha = A(E, \omega)$ associated to the given integral equation (2). Write $\mathcal{F}$ for the formal group of E over $\mathcal{O}$, and similarly $\mathcal{F}'$ for the formal group for the isogenous curve E' given by the integral equation

$$E' : y'^2 = x'^3 + A^p x' + B^p.$$

Choose $t = -x'/y'$ as the parameter of the formal group $\mathcal{F}'$. Then the formal isogeny V_1 of the Verschiebung V is of the form

$$\begin{tikzcd} V_1 : \mathcal{F}'(\mathfrak{m}) \arrow[r, tail] & \mathcal{F}(\mathfrak{m}) \\ t \arrow[r, mapsto, tail] & \alpha \cdot G(t) + H(t^p) \end{tikzcd}$$

for some $G(t) = t + \cdots \in \mathcal{O}[\![t]\!]$ and $H(t) = u \cdot t + \cdots \in \mathcal{O}[\![t]\!]$ with u in $\mathcal{O}^\times$. See [KM85, § 12.4] for other descriptions of the Hasse invariant α.

We begin now the proof of Theorem 6. For the computation of the local root number w, we can simply refer to [Roh94, Proposition 19], where we find that $w = -1$ if the reduction is split multiplicative and $w = +1$ if it is good or non-split multiplicative.

3.1 Good reduction

Proposition 7. *Suppose E/K has good reduction. Then $w = +1$. The quantities σ and $(-1/(L/K))$ are $+1$ if and only if $q^{v(\alpha)}$ is a square. In particular, if the reduction is ordinary then $\sigma = (-1/(L/K)) = +1$.*

Proof. We may suppose that the Weierstrass equation (2) is minimal, i.e. that it has good reduction. We then have the diagram

$$\begin{tikzcd} 0 \arrow[r, tail] & \mathcal{F}'(\mathfrak{m}) \arrow[r, tail] \arrow[d, "V_1"'] & E'(K) \arrow[r, tail] \arrow[d, "V"'] & \tilde{E}'(\mathbb{F}_q) \arrow[r, tail] \arrow[d] & 0 \\ 0 \arrow[r, tail] & \mathcal{F}(\mathfrak{m}) \arrow[r, tail] & E(K) \arrow[r, tail] & \tilde{E}(\mathbb{F}_q) \arrow[r, tail] & 0 \end{tikzcd}$$

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

where $\tilde{E}$ denotes the reduction of E. The isogenous curves $\tilde{E}$ and $\tilde{E}'$ over $\mathbb{F}_q$ have the same number of points, so the kernel and cokernel of this map have the same size. Hence $z_v = z(V_1)$.

For any $N \geqslant 1$,

$$\frac{\mathcal{F}(\mathfrak{m}^N)}{\mathcal{F}(\mathfrak{m}^{N+1})} \cong \frac{\mathfrak{m}^N}{\mathfrak{m}^{N+1}} \cong \frac{\mathcal{F}'(\mathfrak{m}^N)}{\mathcal{F}'(\mathfrak{m}^{N+1})}$$

and so the same argument shows that $z_v = z(V_1) = z(V_N : \mathcal{F}'(\mathfrak{m}^N) \to \mathcal{F}(\mathfrak{m}^N))$.

We claim that if $N > \upsilon(\alpha)$ then V_N maps $\mathcal{F}'(\mathfrak{m}^N)$ bijectively onto $\mathcal{F}(\mathfrak{m}^{N+\upsilon(\alpha)})$. If t has valuation at least N, then the valuation of αt is smaller than the valuation of $u \cdot t^p$. Therefore $\upsilon(V_N(t)) = \upsilon(\alpha) + \upsilon(t)$. This shows that V_N maps $\mathcal{F}'(\mathfrak{m}^N)$ injectively to $\mathcal{F}(\mathfrak{m}^{N+\upsilon(\alpha)})$. In particular, the kernel $\ker(V_N)$ is trivial.

Let s have valuation $\upsilon(s) \geqslant N + \upsilon(\alpha)$. Put $t_0 = s/\alpha$. Then t_0 is close to a zero of $g(t) = V_N(t) - s$. Namely $g(t_0) = \alpha a t_0^2 + \cdots + u t_0^p + \cdots$ has valuation at least $2\upsilon(s) - \upsilon(\alpha) \geqslant 2N + \upsilon(\alpha) > 2\upsilon(\alpha)$, if we write $G(t) = t + at^2 + \cdots$ for some $a \in \mathcal{O}$. Since $g'(t_0) = \alpha + 2\alpha a t_0 + \cdots$ has valuation $\upsilon(\alpha)$, Hensel's lemma shows that there is a t close to t_0 such that $g(t) = 0$, i.e. such that $V_N(t) = s$.

We conclude that the cokernel of V_N is equal to the index of $\mathcal{F}(\mathfrak{m}^{N+\upsilon(\alpha)})$ in $\mathcal{F}(\mathfrak{m}^N)$. Hence $z_v = z(V_N) = q^{\upsilon(\alpha)}$. In particular $z_v = 1$ if the reduction is ordinary, i.e. when α is a unit in $\mathcal{O}$.

Let $e_{L/K}$ be the ramification index of L/K. If the reduction is good ordinary, then the inertia group acts trivially on T_pE', which is a $\mathbb{Z}_p$-module of rank one. Hence L/K is unramified and we have immediately that $(-1/(L/K)) = +1$.

Lemma 8. *The parity of $\upsilon(\alpha)$ is equal to the parity of $(p-1)/e_{L/K}$.*

Proof. If E has good ordinary reduction, then $\upsilon(\alpha) = 0$, $e_{L/K} = 1$ and $p-1$ is even so that the assertion is true. If E has good supersingular reduction, then since $E'(L)[p]$ contains a non-trivial point $P = (x'_P, y'_P)$, but the reduction does not contain a point of order p, there exist a $t_P = -x'_P/y'_P$ in the maximal ideal $\mathfrak{m}_L$ of L such that $V_1(t_P) = 0$. From $V_1(t_P) = \alpha t_P + \cdots + u t_P^p + \cdots$, we see that the valuations of αt_P and $u t_P^p$ must cancel out. Hence $\upsilon_L(\alpha) = e_{L/K} \cdot \upsilon(\alpha) = (p-1) \cdot \upsilon_L(t_P)$, where υ_L denotes the normalised valuation in L; so if the valuation of t_P is odd, we have proved the assertion.

Assume that $\upsilon_L(t_P)$ is even. Then $\upsilon(\alpha)$ is also even and we have to show that $(p-1)/e_{L/K}$ is even. The extension $L/K(x'_P)$ is generated by t_P whose square belongs to $K(x'_P)$; so this extension is either unramified quadratic or trivial. If $L = K(x'_P)$, then $\mathrm{Gal}(L/K)$ acts on the set of $\{x'_P \mid O \neq P \in E'(L)[p]\}$ and hence $[L:K]$ divides $(p-1)/2$, so $(p-1)/[L:K]$ is even. Otherwise, if L is an unramified quadratic extension of $K(x'_P)$, then $e_{L/K} = e_{K(x'_P)/K}$ and $p-1$ is divisible by $[L:K] = 2e_{L/K} f_{K(x'_p)/K}$. Hence $(p-1)/e_{L/K}$ is even. □

Now we can conclude the proof of Proposition 7. Lemma 12 in [DD08], whose proof is valid even if the characteristic of K is not zero, says that $(-1/(L/K)) = +1$ if and only if q is a square or if $(p-1)/e_{L/K}$ is even. The previous lemma suffices now to conclude. □

In the good supersingular case, L/K may or may not be totally ramified. We illustrate this with two examples.

We take $p = 5$, $w > 0$ any integer, and the curve E given by the minimal Weierstrass equation

$$y^2 = x^3 + T^w \cdot x + 1$$

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

over $\mathcal{O}=\mathbb{F}_5[[T]]$. The Hasse invariant is $\alpha=2\cdot T^w$. The reduction is good, but supersingular. The division polynomial f_V associated to the isogeny V can be computed to be equal to

$$f_V(x)=2T^w x^2+4T^{2w}x+(4+3T^{3w}+T^{6w}).$$

First we take the case $w=2m$ is even. Then we can make the substitution $X=T^m\cdot x$ to get

$$f_V(x)=2X^2+4T^{3m}X+(4+3T^{6m}+T^{12m}).$$

We see that $K(x_P)$ is a quadratic unramified extension of K. The quantity $(p-1)/e_{L/K}$ will certainly be even.

Now, take $w=2m-1$ to be odd with $m>1$. This time the substitution $X=T^m\cdot x$ gets us to

$$T\cdot f_V(x)=2X^2+4T^{3m-2}X+T\cdot(4+3T^{6m-3}+T^{12m-6}).$$

Therefore $K(x_P)/K$ will be a ramified extension of degree two. The valuation of x_P over $K(x_P)$ is odd, so we have to make a further extension $L/K(x_P)$, again ramified of degree two, to have a p-torsion point in $E'(L)$. Hence $e_{L/K}=4$ and $(p-1)/e_{L/K}$ is odd.

3.2 Split multiplicative

Proposition 9. *Suppose E/K has split multiplicative reduction. Then $w(E/K)=-1$, $(-1/(L/K))=+1$, and $\sigma(E/K)=-1$.*

Proof. Let $q_E\in K^\times$ be the parameter of the Tate curve which is isomorphic to E over K. Then the isogenous curve E' has parameter ${q_E}^p$ and the Frobenius map

$$V:\frac{K^\times}{({q_E}^p)^{\mathbb{Z}}}\longrightarrow\frac{K^\times}{(q_E)^{\mathbb{Z}}}$$

is induced by the identity on $K^\times$. Hence V has a kernel with p elements and is surjective, so $z_V=1/p$ and $\sigma=-1$.

Since E' has already a p-torsion point over K, we have $L=K$ and $(-1/(L/K))=+1$. □

3.3 Non-split multiplicative

Proposition 10. *Suppose E/K has non-split multiplicative reduction. Then*

$$w(E/K)=\left(\frac{-1}{L/K}\right)=\sigma(E/K)=+1.$$

Proof. There is a quadratic extension K' over which E has split multiplicative reduction. Hence either $L=K$ or $L=K'$. Let $E^\dagger$ be the quadratic twist of E over K'. Up to 2-torsion groups, we have $E(L)=E(K)\oplus E^\dagger(K)$. Since $E^\dagger$ has split multiplicative reduction over K there is a p-torsion point in $E^\dagger(K)$. Hence $L=K'$.

From the previous section, we know that z_V for E/L and $E^\dagger/K$ both are equal to $1/p$. Therefore, by the above formula for $E(L)$ up to 2-torsion, we get that z_V for E/K is 1. Hence $\sigma=+1$. Since L/K is unramified, $(-1/(L/K))=+1$. □

3.4 Additive potentially multiplicative

Proposition 11. *Suppose E/K has additive, potentially multiplicative reduction. Let $\chi: K^\times\to\{\pm1\}$ be the character associated to the quadratic ramified extension over which E has split multiplicative reduction. Then $w(E/K)=(-1/(L/K))=\chi(-1)$ and $\sigma(E/K)=+1$.*

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

Proof. The root number is computed by Rohrlich [Roh94, 19.ii]. The proof that $\sigma = +1$ is the same as in the non-split multiplicative case. The formula $(-1/(L/K)) = \chi(-1)$ is clear, too. □

4. Selmer groups

We return to the global situation and we wish to define properly the Selmer groups involved in p-descent in characteristic p using flat cohomology.

From now on, K is again a global field with field of constants $\mathbb{F}_q$ and E/K is a semistable, non-isotrivial elliptic curve. We denote by $\mathcal{E}$ the Néron model of E/K over C and $\mathcal{E}^0$ its connected component containing the identity. Let U be a dense open subset of C such that $\mathcal{E}$ has good reduction on U. The group schemes $\mathcal{E}$ and $\mathcal{E}^0$ coincide over U and we define for any $v \notin U$ the group of connected components Φ_v in the fibre above v. Hence we have the following short exact sequence:

$$0 \to \mathcal{E}^0 \to \mathcal{E} \to \bigoplus_{v \notin U} \Phi_v \to 0.$$

Following [KT03, 2.2], the discrete p^∞-Selmer group of E/K is defined as

$$\mathrm{Sel}_{p^\infty}(E/K) := \ker\left[H^1_{\mathrm{fl}}(K, E[p^\infty]) \to \prod_v H^1_{\mathrm{fl}}(K_v, E)\right]$$

where $E[p^\infty]$ is the p-divisible group associated to E and H_{fl} stands for flat cohomology. It is known that $\mathrm{Sel}_{p^\infty}(E/K)$ fits into the following exact sequence:

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

This follows from the fact that the Tate–Shafarevich group can also be computed using flat cohomology as the kernel of $H^1_{\mathrm{fl}}(K, E) \to \prod_v H^1_{\mathrm{fl}}(K_v, E)$ since for the elliptic curve E over K or K_v, the étale and flat cohomology groups coincide (see [Mil80, Theorem 3.9]). Note also that the dual of $\mathrm{Sel}_{p^\infty}(E/K)$ is a finitely generated $\mathbb{Z}_p$-module by the theorem of Mordell–Weil and the finiteness of $Ш(E/K)[p]$ (see e.g. [Ulm91]).

Let $\phi : E \to E'$ be an isogeny of elliptic curves. The map ϕ induces a short exact sequence of sheaves in the flat topology

$$\begin{tikzcd} 0 \arrow[r] & E[\phi] \arrow[r] & E \arrow[r, "\phi"] & E' \arrow[r] & 0. \end{tikzcd} \tag{5}$$

The Selmer group $\mathrm{Sel}_\phi(E/K)$ is defined to be the set of elements in $H^1_{\mathrm{fl}}(K, E[\phi])$ whose restrictions to $H^1_{\mathrm{fl}}(K_v, E[\phi])$ lie in the image of the connecting homomorphism $E(K_v) \to H^1_{\mathrm{fl}}(K_v, E[\phi])$ for all v. If U is any open subset of C where E has good reduction, we can also describe $\mathrm{Sel}_\phi(E/K)$ as the kernel of the composed map

$$\begin{tikzcd} H^1_{\mathrm{fl}}(U, \mathcal{E}[\phi]) \arrow[r] & \prod_{v \notin U} H^1_{\mathrm{fl}}(K_v, E[\phi]) \arrow[r] & \prod_{v \notin U} H^1_{\mathrm{fl}}(K_v, E)[\phi]. \end{tikzcd}$$

Passing to cohomology, the short exact sequence (5) induces the short exact sequence of finite groups

$$\begin{tikzcd} 0 \arrow[r] & E'(K)/\phi(E(K)) \arrow[r] & \mathrm{Sel}_\phi(E/K) \arrow[r] & Ш(E/K)[\phi] \arrow[r] & 0, \end{tikzcd} \tag{6}$$

where $Ш(E/K)[\phi]$ is the kernel of the induced map $\phi_Ш : Ш(E/K) \to Ш(E'/K)$.

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

5. Global Euler characteristics

We prove in the next three sections a few results on global dualities for the p-primary part of the Tate–Shafarevich group in characteristic p using flat cohomology. The main reference will be [Mil06], but we wish to point the reader to related results in [Gon09, GT07].

Note that most results in these three sections do not need any condition on the reduction. Also, except where mentioned, the characteristic p can be any prime.

We give a short review of the Oort–Tate classification of finite flat group schemes of order p (see [TO70] for details). Let X be a scheme of characteristic $p>0$. The data of a finite flat group scheme N of order p over X is equivalent to the data of an invertible sheaf $\mathcal{L}$, a section $a\in H^0(C,\mathcal{L}^{\otimes(p-1)})$ and a section $b\in H^0(C,\mathcal{L}^{\otimes(1-p)})$ such that $a\otimes b=0$. We use the notation $N_{\mathcal{L},a,b}$. If N is of height 1, then $a=0$. The Cartier dual of $N_{\mathcal{L},a,b}$ is $N_{\mathcal{L}^{-1},b,a}$.

For a scheme S of characteristic $p>0$ and a finite flat group scheme N/S we define the Euler characteristic of N/S as

$$\chi(S,N):=\prod_i (\#H^i_{\mathrm{fl}}(S,N))^{(-1)^i}$$

whenever the groups $H^i_{\mathrm{fl}}(S,N)$ are finite.

Lemma 12. *Assume that the prime p is odd. Let N be a finite flat group scheme of order p over C. Assume that the Cartier dual N^D of N is of height 1. Then the groups $H^i_{\mathrm{fl}}(C,N)$ are finite and $\chi(C,N)$ is a square in $\mathbb{Q}^\times$.*

Proof. The cohomology is finite by [Mil06, Lemma III.8.9] since N is finite flat. If N^D has height 1 then N corresponds to a group scheme $N_{\mathcal{L},a,b}$ with $b=0$. Now we follow the explanation after [Mil06, Problem III.8.10]. Since N is the dual of a group scheme of height 1, we have that there is a sequence

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] & \mathcal{L} \arrow[r] & \mathcal{L}^{\otimes p} \arrow[r] & 0, \\ & & z \arrow[r, mapsto] & z^{\otimes p}-a\otimes z & \end{tikzcd}$$

which is exact by the definition of $N_{\mathcal{L},a,b}$. See also [Mil06, Example III.5.4]. Hence we have that $\chi(C,N)=q^{\chi(\mathcal{L})-\chi(\mathcal{L}^{\otimes p})}$. Using Riemann–Roch, we get

$$\chi(\mathcal{L})=\deg(\mathcal{L})+1-g,$$
$$\chi(\mathcal{L}^{\otimes p})=p\cdot\deg(\mathcal{L})+1-g$$

and therefore we find the formula

$$\chi(C,N)=q^{(p-1)\deg\mathcal{L}}.$$

Hence the lemma follows from the fact that p is odd. □

For any place v in K, we denote by $|\cdot|_v$ the normalised absolute value of the completion K_v. In particular the absolute value of a uniformiser is q_v^{-1} where q_v denotes the number of elements in the residue field.

Lemma 13. *Let $N=N_{\mathcal{L},a,b}$ be a finite flat group scheme of order $p>2$ over the ring O_v of integers in K_v. Assume that N_{K_v} is étale. Then the Euler characteristic of N is well defined and we have*

$$\chi(O_v,N)\equiv|a|_v^{-1}$$

modulo squares in $\mathbb{Q}^\times$.

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

Proof. The invertible sheaf $\mathcal{L}$ is $c^{-1} \cdot O_v$ for some $c \in K_v^\times$. Then by [Mil06, III.0.9.(c)], we have $N_{\mathcal{L},a,b} \cong N_{O_v, ac^{p-1}, bc^{1-p}}$. Using Remark III.7.6 and the Example after Theorem III.1.19 on page 244 of [Mil06], we have $\chi(O_v, N) = |a \cdot c^{p-1}|_v^{-1} \equiv |a|_v^{-1}$ modulo squares in $\mathbb{Q}^\times$. □

For a scheme S of characteristic $p > 0$ and a scheme X/S, we denote by X' the fibre product $X \times_S S$ where the map $S \to S$ in this product is the absolute Frobenius of S. By the universal property of the fibre product, we have a map $F : X \to X'$ called the relative Frobenius. If moreover X/S is a flat group scheme, then there exists a map $V : X' \to X$ called the Verschiebung such that $V \circ F$ and $F \circ V$ induce $[p]$, the multiplication by p (see [GD70, VII]). In particular, $F : E \to E'$ is a p-isogeny of elliptic curves which extends to the Néron models of E and E' by its universal property. Since the Néron model of E' is $\mathcal{E}'$, this map is just the relative Frobenius $F : \mathcal{E} \to \mathcal{E}'$.

Over the field K, or more generally over any open subset U in C where E has good reduction, [Ulm91, Proposition 2.1] shows that $E[F] = N_{\underline{\omega}^{-1},0,\alpha}$ and $E[V] = N_{\underline{\omega},\alpha,0}$, where α is the Hasse invariant of E and where $\underline{\omega}$ is the invertible sheaf $\pi_* \Omega^1_{E/K}$ with $\pi : E \to \operatorname{Spec}(K)$ being the structure morphism.

Proposition 14. *Let E/K be a non-isotrivial elliptic curve. There exists a dense open subset U of C such that E has everywhere good ordinary reduction and $\chi(U, \mathcal{E}[F])$ is a well-defined square in $\mathbb{Q}^\times$.*

Proof. By the Oort–Tate classification, $E[F]/K$ is isomorphic to $N_{\underline{\omega}^{-1},0,\alpha}$. By [Mil06, Proposition B.4] and its proof, it extends to a finite flat group scheme $\mathcal{N}/C$ of order p of the form $N_{\mathcal{O}_C(W),0,\alpha}$ for some Weil divisor $W \leqslant 0$ such that $(\alpha) \geqslant W$. Let U_1 be a dense open subset of C over which $\mathcal{E}$ has good reduction. As in [Mil06, proof of Theorem III.8.2] on page 291, we replace U_1 by a smaller open set U_2, over which $\mathcal{N}|_{U_2} \simeq \mathcal{E}[F]|_{U_2}$. Finally, we set U equal to the open subset of U_2 where we have removed all places v for which E/K has good supersingular reduction.

Write $\mathcal{N}^D$ for the Cartier dual of $\mathcal{N}$. By [Mil06, Proposition III.0.4(c) and Remark III.0.6(b)], we have a long exact sequence

$$\cdots \longrightarrow H^i_{\mathrm{fl},c}(U, \mathcal{N}^D) \longrightarrow H^i_{\mathrm{fl}}(C, \mathcal{N}^D) \longrightarrow \textstyle\prod_{v \notin U} H^i_{\mathrm{fl}}(O_v, \mathcal{N}^D) \longrightarrow \cdots.$$

Global duality [Mil06, Theorem III.8.2] shows that

$$H^i_{\mathrm{fl},c}(U, \mathcal{N}^D) = H^i_{\mathrm{fl},c}(U, \mathcal{E}'[V]) \text{ is dual to } H^i_{\mathrm{fl}}(U, \mathcal{E}[F]).$$

By the multiplicative property of the Euler characteristic, we get

$$\chi(U, \mathcal{E}[F]) = \frac{\chi(C, \mathcal{N}^D)}{\prod_{v \notin U} \chi(O_v, \mathcal{N}^D)}.$$

Since $\mathcal{N}^D = N_{\mathcal{O}_C(-W),\alpha,0}$ is finite flat of order p over C, Lemma 12 shows that $\chi(C, \mathcal{N}^D)$ is a square. Furthermore, Lemma 13 yields

$$\chi(U, \mathcal{E}[F]) \equiv \prod_{v \notin U} \chi(O_v, \mathcal{N}^D)^{-1} \equiv \prod_{v \notin U} |\alpha|_v \pmod{\square}.$$

Since the places of U are places of good ordinary reduction where $|\alpha|_v$ is a square by Proposition 7, we have, using the product formula,

$$\chi(U, \mathcal{E}[F]) \equiv \prod_{v \notin U} |\alpha|_v^{-1} \equiv \prod_{v} |\alpha|_v^{-1} = 1 \pmod{\square}.$$ □

6. The Cassels–Tate pairing

Recall that there exist a pairing [Mil06, proof of Theorem II.5.6] called the Cassels–Tate pairing

$$\langle\!\langle \cdot, \cdot \rangle\!\rangle : \text{Ш}(E/K) \times \text{Ш}(E/K) \to {}^{\mathbb{Q}}\!/\!_{\mathbb{Z}}.$$

As claimed in [Mil06, Proposition III.9.5] its left and right kernels are the divisible part $\mathrm{div}(\text{Ш}(E/K))$ of the Tate–Shafarevich group. We are calling the attention of the reader to the fact that the initial proof in [Mil06] is wrong, as noticed by Harari and Szamuely in [HS09]. The first correct published proofs that the Cassels–Tate pairing of [Mil06, Theorem II.5.6(a)], annihilates only maximal divisible subgroups appear in [HS09] (for prime-to-p primary components) and in [Gon09] (for p-primary components) when the 1-motive considered in these references is taken to be $(0 \to E)$. This pairing is alternating and hence the order of $\text{Ш}(E/K)_{\mathrm{div}}$ is a square. This last fact is not always true if we consider general abelian varieties.

Lemma 15. *Let $\phi : E \to E'$ be an isogeny of elliptic curves and $\hat{\phi}$ the dual isogeny. Then the induced map $\phi_{\text{Ш}} : \text{Ш}(E/K) \to \text{Ш}(E'/K)$ and $\hat{\phi}_{\text{Ш}} : \text{Ш}(E'/K) \to \text{Ш}(E/K)$ are adjoints with respect to the Cassels–Tate pairings, i.e.*

$$\langle\!\langle \phi_{\text{Ш}}(\eta), \xi \rangle\!\rangle_{E'} = \langle\!\langle \eta, \hat{\phi_{\text{Ш}}}(\xi) \rangle\!\rangle_{E}$$

for every $\eta \in \text{Ш}(E/K)$ and $\xi \in \text{Ш}(E'/K)$.

Proof. The proof is analogous to the proof in the number field case (see [Mil06, Remark I.6.10] or [Cas65, § 2]) and is deduced from the functoriality of the local pairings in flat cohomology. □

Proposition 16. *The orthogonal complement of $\text{Ш}(E'/K)[V]$ in $\text{Ш}(E'/K)[p^\infty]$ under the Cassels–Tate pairing*

$$\text{Ш}(E'/K)[p^\infty] \times \text{Ш}(E'/K)[p^\infty] \to {}^{\mathbb{Q}}\!/\!_{\mathbb{Z}}$$

is the image of $F : \text{Ш}(E/K)[p^\infty] \to \text{Ш}(E'/K)[p^\infty]$.

Proof. Note that the proposition follows immediately from the previous lemma if the pairing is perfect. Else, by the previous Lemma 15, it is immediate that $F(\text{Ш}(E/K)[p^\infty])$ is contained in the orthogonal of $\text{Ш}(E'/K)[V]$. Let ξ be an element in $\text{Ш}(E'/K)[p^\infty]$ orthogonal to the kernel of V. Let D' denote the maximal divisible subgroup of $\text{Ш}(E'/K)[p^\infty]$ and D the maximal divisible subgroup of $\text{Ш}(E/K)[p^\infty]$. Then there is a perfect paring on the quotients $\text{Ш}(E'/K)[p^\infty]/D'$ and $\text{Ш}(E/K)[p^\infty]/D$. Since V and F map divisible elements to divisible elements, they induce maps between these quotients, as follows.

$$\begin{tikzcd}
0 \arrow[r] & D' \arrow[r] \arrow[d, shift left, "V"] & \text{Ш}(E'/K)[p^\infty] \arrow[r] \arrow[d, shift left, "V"] & \text{Ш}(E'/K)[p^\infty]/D' \arrow[r] \arrow[d, shift left, "V"] & 0 \\
0 \arrow[r] & D \arrow[r] \arrow[u, shift left, "F"] & \text{Ш}(E/K)[p^\infty] \arrow[r] \arrow[u, shift left, "F"] & \text{Ш}(E/K)[p^\infty]/D \arrow[r] \arrow[u, shift left, "F"] & 0
\end{tikzcd}$$

The element $\xi + D'$ in the quotient $\text{Ш}(E'/K)[p^\infty]/D'$ is orthogonal to the kernel of V. Since the pairing is perfect there, we have an element η in $\text{Ш}(E/K)[p^\infty]$ such that F maps $\eta + D$ to $\xi + D'$ in the quotients. Hence $F(\eta) = \xi + \delta$ for some $\delta \in D'$. However, since the map $F \circ V = [p]$ is surjective on D', the map F maps D onto D'. Hence δ is in the image of F and so is ξ. □

The short exact sequence of finite flat group schemes

$$0 \to E[F] \to E[p] \to E'[V] \to 0, \tag{7}$$

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

induces, when passing to flat cohomology, the top row of the following exact commutative diagram.

$$\begin{tikzcd}
\cdots \arrow[r] & E'(K)[V] \arrow[r] & H^1_{\mathrm{fl}}(K, E[F]) \arrow[r] \arrow[d] & H^1_{\mathrm{fl}}(K, E[p]) \arrow[r, "F"] \arrow[d] & H^1_{\mathrm{fl}}(K, E'[V]) \arrow[d] \\
& 0 \arrow[r] & \prod_v H^1_{\mathrm{fl}}(K_v, E)[F] \arrow[r] & \prod_v H^1_{\mathrm{fl}}(K_v, E)[p] \arrow[r, "F"] & \prod_v H^1_{\mathrm{fl}}(K_v, E')[V]
\end{tikzcd}$$

From the above diagram, we obtain an exact sequence

$$\begin{gathered}
0 \longrightarrow E(K)[F] \longrightarrow E(K)[p] \xrightarrow{F} E'(K)[V] \longrightarrow \\
\longrightarrow \mathrm{Sel}_F(E/K) \longrightarrow \mathrm{Sel}_p(E/K) \xrightarrow{F} \mathrm{Sel}_V(E'/K) \longrightarrow T \longrightarrow 0,
\end{gathered} \tag{8}$$

where T is the cokernel of the map induced by F on the Selmer groups. Parallel to this, we have a long exact (kernel-cokernel) sequence

$$\begin{gathered}
0 \longrightarrow E(K)[F] \longrightarrow E(K)[p] \xrightarrow{F} E'(K)[V] \longrightarrow \\
\longrightarrow E'(K)/F(E(K)) \xrightarrow{V} E(K)/pE(K) \longrightarrow E(K)/V(E'(K)) \longrightarrow 0.
\end{gathered} \tag{9}$$

We may quotient the exact sequence (8) by the exact sequence (9), using Kummer maps in the short exact sequence (6). We get an alternative description of T by an exact sequence:

$$0 \longrightarrow \text{Ш}(E/K)[F] \longrightarrow \text{Ш}(E/K)[p] \xrightarrow{F} \text{Ш}(E'/K)[V] \longrightarrow T \longrightarrow 0. \tag{10}$$

Corollary 17. *Let E/K be an elliptic curve. The order of T is a square. In other words,*

$$\#\text{Ш}(E/K)[F] \cdot \#\text{Ш}(E'/K)[V] \equiv \text{Ш}(E/K)[p] \pmod{\square}.$$

Proof. By restriction the Cassels–Tate pairing induces a pairing on $\text{Ш}(E'/K)[V]$ with values in ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$. By the previous proposition the right and left kernels of this pairing are equal to the intersection of $F(\text{Ш}(E/K)[p^\infty])$ and $\text{Ш}(E'/K)[V]$, which is equal to $F(\text{Ш}(E/K)[p])$. Therefore the pairing induces a non-degenerate alternating pairing on T; hence the order of T is a square. □

Lemma 18. *We have*

$$p^{r_p} \equiv \frac{\#E(K)[F] \cdot \#\mathrm{Sel}_V(E'/K)}{\#E'(K)[V] \cdot \#\mathrm{Sel}_F(E/K)} \pmod{\square}.$$

Of course, we have $\#E(K)[F] = 1$, but we include it here so as to make the formula resemble the symmetric formula in the classical case, like that in Fisher's appendix to [Dok05].

Proof. By the short exact sequence (4), $r_p = r + \mathrm{corank}_{\mathbb{Z}_p} \text{Ш}(E/K)[p^\infty]$, where $r = \mathrm{rank}_{\mathbb{Z}}(E(K))$ and r_p is the $\mathbb{Z}_p$-rank of the dual of $\mathrm{Sel}_{p^\infty}(E/K)$. Now, since $\text{Ш}(E/K)[p^\infty]$ is cofinitely generated as a $\mathbb{Z}_p$-module, we have

$$\dim_{\mathbb{F}_p} \text{Ш}(E/K)[p] = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{div}\, \text{Ш}(E/K)[p^\infty]) + \dim_{\mathbb{F}_p}(\text{Ш}(E/K)_{\mathrm{div}}[p]).$$

As noticed at the beginning of § 6, $\#\text{Ш}(E/K)_{\mathrm{div}}$ (and therefore $\#\text{Ш}(E/K)_{\mathrm{div}}[p]$) is a square. We deduce that

$$r_p \equiv r + \dim_{\mathbb{F}_p} \text{Ш}(E/K)[p] \pmod{2}.$$

On the other hand, the short exact sequence (6) applied to $[p]$ implies that

$$\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K) = r + \dim_{\mathbb{F}_p} E(K)[p] + \dim_{\mathbb{F}_p} \text{Ш}(E/K)[p],$$

since $E(K)/pE(K) \simeq E(K)[p] \oplus (\mathbb{Z}/p\mathbb{Z})^r$. Hence we get the formula

$$r_p \equiv \dim_{\mathbb{F}_p} E(K)[p] + \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K) \pmod 2.$$

The assertion results then from the exact sequence (8) and Corollary 17. □

7. Global duality

Proposition 19. *Let E/K be a non-isotrivial elliptic curve and let U be an open subset of C over which E has good reduction. Then we have*

$$\frac{\#E(K)[F]\cdot\#\mathrm{Sel}_V(E'/K)}{\#E'(K)[V]\cdot\#\mathrm{Sel}_F(E/K)} = \frac{1}{\chi(U,\mathcal{E}[F])}\cdot\prod_{v\notin U} z(V_{E'(K_v)}).$$

We insist once more that the roles of F and V here are not interchangeable, e.g. the terms $z(F_{E(K_v)})$ in the product would not be finite.

Proof. The long exact sequence for flat cohomology deduced from the definition of $H^i_{\mathrm{fl},c}$ in [Mil06, Proposition III.0.4(a)] reads

$$\begin{tikzcd} \cdots \arrow[r] & H^i_{\mathrm{fl},c}(U,\cdot) \arrow[r] & H^i_{\mathrm{fl}}(U,\cdot) \arrow[r] & \bigoplus_{v\notin U} H^i_{\mathrm{fl}}(K_v,\cdot) \arrow[r] & H^{i+1}_{\mathrm{fl},c}(U,\cdot) \arrow[r] & \cdots . \end{tikzcd}$$

The global duality in [Mil06, Theorem III.8.2] implies that the group $H^i_{\mathrm{fl},c}(U,\mathcal{E}[F])$ is dual to $H^{3-i}_{\mathrm{fl}}(U,\mathcal{E}'[V])$ since $\mathcal{E}[F]$ is finite and flat over U. We find the following long exact sequence:

$$\begin{tikzcd} & H^1_{\mathrm{fl}}(U,\mathcal{E}[F]) \arrow[r] & \bigoplus_{v\notin U} H^1_{\mathrm{fl}}(K_v,E[F]) \arrow[r] & H^1_{\mathrm{fl}}(U,\mathcal{E}'[V])^\vee \arrow[r] & {} \\ {} \arrow[r] & H^2_{\mathrm{fl}}(U,\mathcal{E}[F]) \arrow[r] & \bigoplus_{v\notin U} H^2_{\mathrm{fl}}(K_v,E[F]) \arrow[r] & H^0_{\mathrm{fl}}(U,\mathcal{E}'[V])^\vee \arrow[r] & 0. \end{tikzcd}$$

Local duality as in [Mil06, Theorem III.6.10] shows that $H^2_{\mathrm{fl}}(K_v,E[F])$ is dual to $E'(K_v)[V]$. Our aim is to replace the local term $H^1_{\mathrm{fl}}(K_v,E[F])$ by the cokernel of the map from $E'(K_v)/F(E(K_v))$. By local duality ([Mil06, Theorem III.7.8] and the functoriality of biextensions), this term is dual to $H^1_{\mathrm{fl}}(K_v,E')[V]$. Hence we will quotient the term $H^1_{\mathrm{fl}}(U,\mathcal{E}'[V])^\vee$ by the image of the map on the right-hand side in the following commutative diagram.

$$\begin{tikzcd} & \bigoplus_{v\notin U} E'(K_v)/F(E(K_v)) \arrow[r, "\cong"] \arrow[d] & \bigoplus_{v\notin U} (H^1_{\mathrm{fl}}(K_v,E')[V])^\vee \arrow[d] & \\ H^1_{\mathrm{fl}}(U,\mathcal{E}[F]) \arrow[r] & \bigoplus_{v\notin U} H^1_{\mathrm{fl}}(K_v,E[F]) \arrow[r] & H^1_{\mathrm{fl}}(U,\mathcal{E}'[V])^\vee \arrow[r] & \cdots \end{tikzcd} \tag{11}$$

Because of the exact Kummer sequence

$$\begin{tikzcd} 0 \arrow[r] & E'(K_v)/F(E(K_v)) \arrow[r] & H^1_{\mathrm{fl}}(K_v,E[F]) \arrow[r] & H^1_{\mathrm{fl}}(K_v,E)[F] \arrow[r] & 0 \end{tikzcd}$$

the cokernel of the map on the left in (11) is $\bigoplus_{v\notin U} H^1_{\mathrm{fl}}(K_v,E)[F]$, which, again by local duality, is dual to $\bigoplus_{v\notin U} E(K_v)/V(E'(K_v))$. By definition the cokernel of the map on the right in (11) is the dual of the Selmer group $\mathrm{Sel}_V(E'/K)$.

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

Putting all these results together, we obtain the long exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_F(E/K) \arrow[r] & H^1_{\mathrm{fl}}(U,\mathcal{E}[F]) \arrow[r] & \bigoplus_{v\notin U}\left({}^{E(K_v)}\!/\!{}_{V(E'(K_v))}\right)^\vee \arrow[r] & {} \\
{} \arrow[r] & \mathrm{Sel}_V(E'/K)^\vee \arrow[r] & H^2_{\mathrm{fl}}(U,\mathcal{E}[F]) \arrow[r] & \bigoplus_{v\notin U}(E'(K_v)[V])^\vee \arrow[r] & {} \\
{} \arrow[r] & (E(K)[V])^\vee \arrow[r] & 0.
\end{tikzcd}$$

Since all other terms in the sequence are finite, the groups $H^i_{\mathrm{fl}}(U,\mathcal{E}[F])$ are finite, too. The alternating product of its orders gives the result. □

If E/K_v is a non-isotrivial, semistable elliptic curve then one can show that the group scheme $\mathcal{E}[F]$ is finite and flat. Hence the result of Proposition 19 can be extended to any open subset U such that E has semistable reduction over all places in U. In particular U can be taken to be equal to C, if E/K is semistable.

8. The proof of the p-parity

We now pass to the proof of Theorem 1. We return now to our running assumptions. K has characteristic $p>3$ and E/K is not isotrivial. We present first the main results coming from global duality and the local computations and then we just have to put them together. However, both these statements are interesting in their own right.

Theorem 20. *Let E/K be a non-isotrivial elliptic curve. We have*

$$p^{r_p} \equiv \prod_v z(V_{E'(K_v)} : E'(K_v) \to E(K_v)) \pmod{\square}$$

where the product runs over all places v in K.

Proof. Proposition 14 provides us with an open subset U in C such that E has good ordinary reduction at all places in U. It follows from Lemma 18, Propositions 19 and 14 that

$$\begin{aligned}
p^{r_p} &\equiv \frac{\#E(K)[F]\cdot\#\mathrm{Sel}_V(E'/K)}{\#E'(K)[V]\cdot\#\mathrm{Sel}_F(E/K)} \pmod{\square}\\
&= \frac{1}{\chi(U,\mathcal{E}[F])}\cdot\prod_{v\notin U} z(V_{E'(K_v)} : E'(K_v)\to E(K_v))\\
&\equiv \prod_{v\notin U} z(V_{E'(K_v)} : E'(K_v)\to E(K_v)) \pmod{\square}.
\end{aligned}$$

Finally from Proposition 7, we know that $z(V_{E'(K_v)})$ is a square for all places $v\in U$ as E has good ordinary reduction there. □

Next, we collect from § 3 the following result.

Proposition 21. *Let E/K be a semistable elliptic curve. Then the root number is $w(E/K) = (-1)^s$ where s is the number of split multiplicative primes for E/K. Furthermore s has the same parity as the p-adic valuation of*

$$\prod_v \frac{c_v(E/K)}{c_v(E'/K)}$$

where c_v are Tamagawa numbers.

Proof. From Theorem 6 we deduce that

$$w(E/K) = \prod_v w(E/K_v) = \prod_v \sigma(E/K_v) \cdot \left(\frac{-1}{L_w/K_v}\right) = \prod_v \sigma(E/K_v)$$

by the product formula for the norm symbols $\prod_v(-1/(L_w/K_v))$ with L being the extension of K over which $E[F] = \mu_p$ and w is any place above v. Using the Propositions 7, 9 and 10, we see that $\sigma(E/K_v)$ is -1 if and only if E has split multiplicative reduction at v.

If the reduction at v is split multiplicative, then we have $c_v(E'/K) = p \cdot c_v(E/K)$ since the parameters in the Tate parametrisation satisfy $q_{E'} = q_E{}^p$. If the reduction is non-split multiplicative then the Tamagawa numbers can only be 1 or 2. □

Note that we could have used the known modularity and the Atkin–Lehner operators to prove this statement without the computations in § 3, at least if E has at least one place of split multiplicative reduction.

Proof of Theorem 1. First, we use Corollary 5 which allows us to assume that E/K is semistable. Then by the previous Proposition 21 we have $w(E/K) = \prod_v \sigma(E/K_v)$ and Theorem 20 states that $(-1)^{r_p} = \prod_v \sigma(E/K_v)$. □

9. Local root number formula

We now prove Theorem 6 without any hypothesis on the reduction. We use, without repeating the definitions, the notations from § 3.

Theorem 22. *Let K be a local field of characteristic $p > 3$. For any non-isotrivial elliptic curve E/K, we have $w(E/K) = (-1/(L/K)) \cdot \sigma(E/K)$.*

As mentioned in § 3 this answers positively a conjecture in [DD09b] for the isogeny V. This theorem could certainly be shown by local computations only, but they would tend to be very tedious for additive potentially supersingular reduction. We can avoid this here by using a global argument. This is a similar idea as in [DD09b, proof of Theorem 5.7].

Proof. By Theorem 6, we may assume that E/K has additive, potentially good reduction. Let $n \geqslant 12$. We can find a minimal integral equation $y^2 = x^3 + Ax + B$ for E/K. Choose a global field $\mathcal{K}$ of characteristic p with a place v_0 such that $\mathcal{K}_{v_0} = K$. Choose another place $v_1 \neq v_0$ in $\mathcal{K}$ and choose a large even integer N such that $(N-1) \cdot \deg(v_1) > 2g - 1 + n \deg(v_0)$, where g is the genus of $\mathcal{K}$. For a divisor D on the projective smooth curve $\mathcal{C}$ corresponding to $\mathcal{K}$, we write $L(D)$ for the Riemann–Roch space $H^0(\mathcal{C}, \mathcal{O}_C(D))$. The inequality on N guarantees that the dimensions of the Riemann–Roch spaces in the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & L(N(v_1) - n(v_0)) \arrow[r] & L(N(v_1)) \arrow[r] & \mathcal{O}_{v_0}/\mathfrak{m}_{v_0}^n \arrow[r] & 0 \end{tikzcd}$$

are positive; e.g. equal to $N\deg(v_1) - n\deg(v_0) + 1 - g > g + \deg(v_1)$ for the smaller space. Choose an element a in $L(N(v_1))$ which maps to $A + \mathfrak{m}_{v_0}^n$ on the right. We can even impose that it does not lie in $L((N-1)(v_1))$, since this is a subspace of codimension $\deg(v_1) > 0$ in $L(N(v_1))$. Then a has a single pole of order N at v_1 and it satisfies $v_0(A - a) \geqslant n$. Next, we use that N is even and we choose an element b in $\mathcal{K}$ such that $v_1(b) = -\frac{3}{2}N$, and $v_0(B - b) \geqslant n$. We can also impose that $v_1(4a^3 + 27b^2) > -3N$. Furthermore we impose that the zeroes of b are distinct from the zeroes of a; this excludes, at worst, $N\deg(v_1)$ subspaces of codimension one in $L((3N/2)(v_1))$.

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

Let $\mathcal{E}/\mathcal{K}$ be the elliptic curve given by $y^2 = x^3 + ax + b$. By the congruences on a and b at v_0 and the continuity of Tate's algorithm, the reduction of $\mathcal{E}$ at v_0 is additive, potentially good. At the place v_1 the valuation of the j-invariant $j(\mathcal{E}) = 2^8 \cdot 3^3 \cdot a^3/(4a^3 + 27b^2)$ will be negative by our choices. Hence the reduction is either multiplicative or potentially multiplicative. For any other place v with $v(a) > 0$, we have $v(4a^3 + 27b^2) = 0$ and hence the curve has good reduction at v, and for any other place v with $v(a) = 0$, either the reduction is good or $v(j(\mathcal{E})) < 0$.

Therefore we have constructed an elliptic curve $\mathcal{E}/\mathcal{K}$ with a single place v_0 of additive, potentially good reduction. Hence for all other places Theorem 6 applies. Let $\mathcal{L}$ be the extension of $\mathcal{K}$ such that $E[F] \cong \mu_p$ over $\mathcal{L}$. Now we use the results of Theorem 20 and the proven p-parity in Theorem 1 to compute

$$\begin{aligned} w(\mathcal{E}/K) &= \frac{w(\mathcal{E}/\mathcal{K})}{\prod_{v\neq v_0} w(\mathcal{E}/\mathcal{K}_v)} = \frac{(-1)^{r_p}}{\prod_{v\neq v_0}(-1/(\mathcal{L}_w/\mathcal{K}_v))\sigma(\mathcal{E}/\mathcal{K}_v)} \\ &= \frac{(-1/(\mathcal{L}_{w_0}/K))}{\prod_{\text{all } v}(-1/(\mathcal{L}_w/\mathcal{K}_v))} \cdot \frac{\prod_{\text{all } v}\sigma(\mathcal{E}/\mathcal{K}_v)}{\prod_{v\neq v_0}\sigma(\mathcal{E}/\mathcal{K}_v)} = \left(\frac{-1}{\mathcal{L}_{w_0}/K}\right) \cdot \sigma(\mathcal{E}/K). \end{aligned}$$

Once again we used the product formula for the norm symbol. Now we argue that the three terms are all continuous in the topology of K as a and b varies: for the local root number this is exactly the statement of [Hel09, Proposition 4.2]. The field $\mathcal{L}_{w_0}$ and the order of the kernel $E'(K)[V]$ of Verschiebung are locally constant because they are defined by continuously varying separable polynomials. Finally, the order of the cokernel of $V : E'(K) \to E(K)$ is locally constant, because the group of connected components and the reduction and the induced map V on them will not change and on the formal group the cokernel is determined by the valuation of the Hasse invariant (which again is a polynomial in a and b) by the argument in the proof of Proposition 7. Since all three terms take value ±1, they will eventually, for big enough n, be equal to the corresponding values for E. □

10. On the ℓ-parity conjecture

We switch now to investigating the ℓ-parity conjecture when $\ell \neq p$. As mentioned in the introduction, we have only a partial result in this case. Recall that $p > 3$ is a prime and that K is a global field of characteristic p with constant field $\mathbb{F}_q$.

For any n and any extension L of K, we denote by L_n the field $L \cdot \mathbb{F}_{q^n}$. The aim of this section is to show the following partial result (given as Theorem 2 in the introduction).

Theorem 23. *Let E/K be an elliptic curve and let ℓ be an odd prime different from p. Furthermore assume that both the following hold.*

(i) *The degree $a = [K(\mu_\ell) : K]$ is even.*

(ii) *The analytic rank of E does not grow by more than one in the extension K_2/K.*

Then the ℓ-parity conjecture holds for E/K.

Note first that we believe that condition (i) holds for roughly two thirds of the ℓ as a is also the order of q in the group $(\mathbb{Z}/\ell\mathbb{Z})^\times$. The second condition should hold quite often as it says that the analytic rank of the twist of E by the unramified quadratic character is less or equal to 1. Hence, for instance, if b as in [Ulm05, Lemma 11.3.1] is odd, then condition (ii) holds.

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

See the next section for a discussion about why we were not able to extend the proof here to any situation without these hypotheses.

Proof. Corollary 5 allows us to assume that E is semistable and we may assume that E is not isotrivial as for isotrivial curves even the conjecture of Birch and Swinnerton-Dyer is known. First we use a non-vanishing result, to produce from the analytic information a useful extension of K, which we want to link to the algebraic side later.

We write $\mathfrak{n}$ for the conductor of E/K. The degree of $\mathfrak{n}$ is linked to the degree of the polynomial $L(E/K,T)$ in $T=q^{-s}$ by the formula of Grothendieck–Ogg–Shafarevich (as used in [Ulm04, Formula (5.1)]):

$$\deg(\mathfrak{n}) = \deg(L(E/K,T)) - 2(2g_K-2).$$

We can factor the polynomial to

$$L(E/K,T) = (1-qT)^r \cdot (1+qT)^{r'} \cdot \prod_i (1-\alpha_i T)(1-\bar{\alpha}_i T)$$

where α_i are non-real, complex numbers of absolute value q. By definition r is the analytic rank of E/K and it is easy to see that $r+r'$ is the analytic rank of E/K_2 since the analytic rank of E/K_2 is the number of inverse zeroes α of $L(E/K,T)$ such that $\alpha^2=q^2$. Hence we get

$$\sum_{v \text{ bad}} \deg(v) = \deg(\mathfrak{n}) \equiv \deg(L(E/K,T)) \equiv r+r' = \operatorname{ord}_{s=1} L(E/K_2,s) \pmod 2. \qquad (12)$$

We are now going to use [Ulm05, Theorem 5.2] to construct suitable extensions of K. The argument is very similar to [Ulm05, proof of Step 2 in 11.4.2]. The following is a very special case of this very general and powerful theorem.

Theorem 24 (Ulmer). *Let K be a global field of characteristic $p>3$, let S be a finite non-empty set of places in K, let $\ell \neq p$ be an odd prime, and let E/K be a semistable elliptic curve. Assume that $a=[K(\mu_\ell):K]$ is even and suppose that the sum of the degree of the bad places not belonging to S is even. Then there exists an integer n coprime to a and a element $z \in K_n^\times$ such that the extension $K_n(\sqrt[\ell]{z})/K_n$ is totally ramified at all places above S and unramified at all bad places not in S and such that the analytic rank of E does not grow in it.*

Proof. All notations and results in this proof refer to [Ulm05]. We use Theorem 5.2(1) with $F=K$, $\alpha_n=q^n$, $d=\ell$, $S_r=S$ and ρ the symplectically self-dual representation of weight $w=1$ attached to E on the Tate module $V_\ell(E)$ as in § 11. We can choose the sets S_s and S_i arbitrarily as long as we make sure that S, S_s, and S_i are disjoint. The conditions (especially from his § 3.1) are satisfied. Let o be an orbit in $({}^{\mathbb{Z}}/_{\ell\mathbb{Z}})^\times$ for the multiplication by q. Then $d_o=\ell$ and $a_o=a$. Hence we can conclude the existence of n and z such that $L(\rho\otimes\sigma_{o,z},K_n,T)$ does not have α_n as an inverse root in 5.2(1) unless we are in the exceptional cases (i)–(iv) in 5.1.1.1. Now, case (iv) cannot hold because ρ is not orthogonally self-dual and cases (i) and (ii) are impossible because $d=\ell$ is odd. However, all the conditions in case (iii) are satisfied apart from maybe the condition 4.2.3.1. (In particular, we know that $-o=o$ because a is even.)

We now have to show that the hypothesis on S imposes that the condition 4.2.3.1 fails. Since E is semistable, the local exponent of the conductor $\operatorname{cond}_v(\rho)$ is 1. Let v be a bad place in S and χ_v be a totally ramified character of the decomposition group D_v which has exact order ℓ. Then the conductor $\operatorname{cond}_v(\rho\otimes\chi_v)=2$ again because E has multiplicative reduction at v. Hence the first condition in 4.2.3.1 saying that this has constant parity as χ_v varies is always fulfilled.

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

In order to make the condition 4.2.3.1 fail, we must have that

$$\sum_{\text{bad } v\in S} \mathrm{cond}_v(\rho\otimes\chi_v)\deg(v)+\sum_{\text{bad } v\notin S}\mathrm{cond}_v(\rho)\deg(v)$$

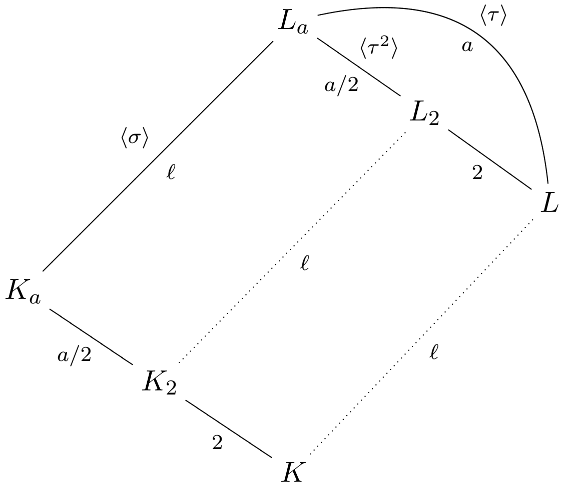
is even. That is exactly what the hypothesis in the theorem imposes. □

Lemma 25. *To prove Theorem 23, we may assume that there exists a non-constant Kummer extension L/K of degree ℓ in which the analytic rank does not grow and such that one of the following holds.*

- *If the analytic rank of E/K_2 is even then no place of bad reduction ramifies in L/K.*
- *If the analytic rank of E/K_2 is odd then exactly one place of bad reduction ramifies. Moreover, in the latter case, the degree of this place is odd.*

Proof. If the analytic rank is even we choose the finite non-empty set of places S to be disjoint from the set of bad places. If the analytic rank is odd, then the congruence (12) shows that there is at least one bad place v of odd degree. Therefore we choose S to contain this as the only bad place. Then (12) shows that the hypothesis in Theorem 24 with the above choice for S holds. Hence we have an integer n and an element $z\in K_n^{\times}$. Now we use the first item in Proposition 4 to replace K by its odd Galois extension K_n. Hence $L=K(\sqrt[\ell]{z})$ is the requested extension. □

We now come to the algebraic part of the argument. Using the previous two lemmata, we have now a Kummer extension L/K of degree ℓ in which the analytic rank does not grow. The Galois closure of L/K is L_a containing L_2. We have the following picture of extensions.



The dotted lines are non-Galois extensions. We have written the degree under each inclusion. The Galois group $G=\mathrm{Gal}(L_a/K)$ is a meta-cyclic group generated by elements σ and τ of order ℓ and a respectively, with $L=(L_a)^{\tau}$. We have

$$G=\langle\sigma,\tau\mid\tau^a=\sigma^\ell=1,\tau\sigma\tau^{-1}=\sigma^q\rangle.$$

We list the irreducible $\mathbb{Q}_\ell[G]$-modules. By $\mathbb{1}$ we denote the trivial representation. Fix a primitive character $\chi:\langle\tau\rangle\cong{}^{\mathbb{Z}}\!/_{a\mathbb{Z}}\cdot\tau\to\mathbb{Q}_\ell^{\times}$ that we can view as a character of G by setting $\chi(\sigma)=1$. (Note that a divides $\ell-1$, so χ is indeed realisable over $\mathbb{Q}_\ell$.) The non-trivial one-dimensional representations of G are exactly the χ^i for $1\leqslant i\leqslant a-1$. There is only one non-trivial irreducible $\mathbb{Q}_\ell[\langle\sigma\rangle]$-module. It is of degree $\ell-1$. We can represent it as $\rho=\mathbb{Q}_\ell[\xi]$ where ξ

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

is a primitive ℓth root of unity and σ acts on ρ by multiplication with ξ. (Over $\bar{\mathbb{Q}}_\ell$ it would split into the $\ell-1$ non-trivial characters of $\langle\sigma\rangle \cong {}^{\mathbb{Z}}\!/\!_{\ell\mathbb{Z}}$.) We make ρ into a G-module by defining the $\mathbb{Q}_\ell$-linear action of τ by $\tau(\xi^j) = \xi^{qj}$ for all $0 \leqslant j \leqslant \ell-2$. It is easy to see that ρ is an irreducible $\mathbb{Q}_\ell[G]$-module of degree $\ell-1$ and in fact it is the only higher dimensional irreducible $\mathbb{Q}_\ell[G]$-module. (Note that $\rho\otimes\overline{\mathbb{Q}}_\ell$ decomposes into $(\ell-1)/a$ irreducibles of degree a corresponding to the orbits of the multiplication by q on $({}^{\mathbb{Z}}\!/\!_{\ell\mathbb{Z}})^\times$.) We have

$$\mathbb{Q}_\ell[G] = \mathbb{1} \oplus \bigoplus_{i=1}^{a-1} \chi^i \oplus \rho^a.$$

For convenience we will denote $\chi^{a/2}$ by ε. The fixed field of the kernel of ε is K_2.

To announce the next lemma, we need to introduce the corrected product of Tamagawa numbers. Fix the invariant 1-form ω on E/K corresponding to the fixed Weierstrass equation. For each place v, write $c_v(E/K)$ for the Tamagawa number and define

$$C_v(E/K,\omega) = c_v(E/K)\cdot\left|\frac{\omega}{\omega_v^o}\right|_v$$

where ω_v^o is a Néron differential for E/K_v. The global product over all places v of K

$$C(E/K) = \prod_v C_v(E/K,\omega)$$

is no longer dependent on the choice of ω by the product formula.

For any irreducible $\mathbb{Q}_\ell[G]$-module ψ, write m_ψ for the multiplicity of the ψ-part of the ℓ-primary Selmer group $\mathrm{Sel}_{\ell^\infty}(E/L_2)$.

Lemma 26. *We have*

$$m_{\mathbb{1}} + m_\varepsilon + m_\rho \equiv \mathrm{ord}_\ell\left(\frac{C(E/L_2)}{C(E/K_2)}\right) \pmod 2.$$

Proof. We are interested in the following relation between permutations representations (in the terminology of the Dokchitser brothers' work, say [DD10, 2.3])

$$\Theta = 2\cdot G + \langle\tau^2\rangle - 2\cdot\langle\tau\rangle - \langle\sigma,\tau^2\rangle$$

corresponding to the equality of L-functions

$$L(E/K,s)^2\cdot L(E/L_2,s) = L(E,\mathbb{1},s)^3\cdot L(E,\varepsilon,s)\cdot L(E,\rho,s)^2 = L(E/K_2,s)\cdot L(E/L,s)^2.$$

It can be seen that the regulator constants (as defined in [DD10, 2.11]) satisfy

$$C_\Theta(\mathbb{1}) \equiv C_\Theta(\varepsilon) \equiv C_\Theta(\rho) \equiv \ell \pmod{\square}$$

in $\mathbb{Q}^\times$ modulo squares. For $\mathbb{1}$ and ε this is straightforward; for ρ we best use [DD09a, Theorem 4(4)] with $D = \langle\tau\rangle$, implying that

$$C_\Theta(\rho)\cdot C_\Theta(\mathbb{1}) = C_\Theta(\mathbb{Q}_\ell[G/\langle\tau\rangle]) = 1.$$

Hence $S_\Theta = \{\mathbb{1},\varepsilon,\rho\}$ in the notation of the Dokchitser brothers in [DD09c].

In short everything looks just like if L_2/K were a dihedral extension (which it is not unless $a=2$). For $a=2$ this is computed in [DD09a, Example 1] and [DD10, Example 4.5] and [DD09c, Example 3.5]. For $a=\ell-1$, this is [DD10, Example 2.20] and [DD09c, Example 3.6].

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

Now, [DD09c, Theorem 1.6] shows that

$$m_{\mathbb{1}} + m_\varepsilon + m_\rho \equiv \operatorname{ord}_\ell\left(\frac{C(E/K)^2 \cdot C(E/L_2)}{C(E/L)^2 \cdot C(E/K_2)}\right) \pmod 2$$

which proves the lemma. □

LEMMA 27. *Suppose that no bad place ramifies in L/K, then the ℓ-adic valuation of the integer $C(E/L_2)/C(E/K_2)$ is even. If there is only one bad place that ramifies in L/K and this place is of odd degree, then the ℓ-adic valuation of $C(E/L_2)/C(E/K_2)$ is odd.*

The more general statement for $a = 2$ can be found in [DD10, Remark 4.18].

Proof. Let v be a place of K_2. Write y for ω/ω_v^o. Then

$$\frac{\prod_{w|v} C_w(E/L_2, \omega)}{C_v(E/K_2, \omega)} = \frac{\prod_{w|v} c_w(E/L_2)}{c_v(E/K_2)} \cdot \frac{\prod_{w|v} |y|_w}{|y|_v} \equiv \frac{\prod_{w|v} c_w(E/L_2)}{c_v(E/K_2)} \pmod \square$$

because $\prod_{w|v} |y|_w/|y|_v = |y|_v^{\ell-1}$ is a square. If the place v is unramified, then the type of reduction and the Tamagawa number do not change and we have

$$\frac{\prod_{w|v} c_w(E/L_2)}{c_v(E/K_2)} = \begin{cases} c_v(E/K_2)^{\ell-1} & \text{if } v \text{ decomposes in } L_2/K_2 \text{ and} \\ 1 & \text{if } v \text{ is inert.} \end{cases}$$

In either case it is a square. If the reduction is good at v then $c_w(E/L_2) = c_v(E/K_2) = 1$. This proves the first case.

Suppose now v is a place in K_2 which lies above a place of odd degree in K and which ramifies in L_2/K_2. Then the place is inert in K_2/K and hence the reduction of E/K_2 at v is necessarily split multiplicative. Let q be the Tate parameter of E at v. Then $c_v(E/K_2) = v(q)$ and $c_w(E/L_2) = w(q) = \ell \cdot v(q)$ for the place w above v. Hence the quotient is ℓ which has odd ℓ-adic valuation. This proves the second statement. □

Finally we can finish the proof of Theorem 23. By construction, we have $\operatorname{ord}_{s=1} L(E, \rho, s) = 0$. As in the proof of Proposition 4, this implies that $m_\rho = 0$; in fact $L(E, \rho, s)$ is $L(B/K, s)$ for the extension L/K. Hence the last two lemmata show that $m_{\mathbb{1}} + m_\varepsilon$, which is the corank of the ℓ-primary Selmer group $\mathrm{Sel}_{\ell^\infty}(E/K_2)$, has the same parity as the analytic rank of E/K_2. This proves the ℓ-parity conjecture for E/K_2. Assumption (ii) and Proposition 4 prove that the ℓ-parity holds over K, too. □

11. Failure to extend

Although it is not usual to write in a mathematical article about unsuccessful attempts to prove a result, we wish to include in this last section a short explanation of why we were unable to extend the proof in the previous section. We hope this might be the starting point for a complete proof of the ℓ-parity conjecture. We try to outline here the missing non-vanishing result for L-functions, which might be accessible using automorphic methods.

The main ingredient for proving Theorem 23 was the existence of a Kummer extension of degree ℓ in which the analytic rank does not grow. Moreover this extension was linked in a 'non-commutative way' to an even abelian extension. The machinery using representation theory set up by Tim and Vladimir Dokchitser is then sufficient to prove the parity.

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

First, if condition (ii) in Theorem 23 does not hold but condition (i) still holds, then there is no hope that a Kummer extension will do. In order to obtain a Galois extension of K from a Kummer extension, we need to make the extension K_2/K. However, without any control about the growth of the analytic rank in this quadratic extension, we do not know how to prove the ℓ-parity over K. With some extra work, one can conclude that the ℓ-parity conjecture holds for E/K_2. In this case, we would need a non-vanishing result for an extension of K of degree dividing ℓ which is not a Kummer extension.

Suppose now that the condition (i) does not hold. Then we would need to find the 'dihedral' extension somewhere else. The Proposition 28 below formulates this in a positive way.

PROPOSITION 28. *Suppose E/K is semistable and non-isotrivial. Let F/K be a quadratic extension such that the analytic rank of E grows at most by one in F/K and the analytic rank of E/F is even. Assume both the following.*

(i) *The degree $a = [F(\mu_\ell) : F]$ is odd.*

(ii) *There exists an odd $n \geqslant 1$ and a $z \in F_n^\times$ with the property that $L = F_n(\sqrt[\ell]{z})$ is an extension of degree ℓ of F_n such that L_a/K_{an} is a dihedral extension, no bad place of E/F_n ramifies in L/F_n, and the analytic rank of E does not grow in L/F_n.*

Then the ℓ-parity conjecture holds for E/K.

Remark that there is a large supply of quadratic extensions F/K by [Ulm05, Theorem 11.2]. The main problem here seems to find the extension L_a/F_{an}. Theorem 5.2 in [Ulm05] provides us with many extensions that satisfy all the properties except that we can not guarantee that L_a/K_{an} is dihedral. We first had hopes that Ulmer's proof could be adapted to enforce that L/K_n is dihedral. In the notations of [Ulm05], we may sketch the problem. Let D be a divisor of large degree as in § 6.2. Then the density (as n grows) of elements in the Riemann–Roch space $H^1(\mathcal{C} \times \mathbb{F}_{q^n}, \mathcal{O}(D))$ which give rise to a dihedral extension of F_n with respect to the fixed quadratic extension F/K will be tending very fast to 0. So we would need to modify the parameter space X and it is not clear how to find a nice variety parametrising such dihedral extensions.

Proof. This is very similar to the proof of Theorem 23. By Proposition 4, we may assume that $a = 1$ and $n = 1$. So L/K is a dihedral extension with group G. Let ρ be the irreducible $\mathbb{Q}_\ell[G]$-module of degree $\ell - 1$ and let ε the character corresponding to the quadratic extension F/K. The usual relation of induced representation Θ for G, as in [DD09c, Example 3.5], yields the congruence

$$m_{\mathbb{1}} + m_\varepsilon + m_\rho \equiv \operatorname{ord}_\ell\left(\frac{C(E/L)}{C(E/F)}\right) \pmod 2.$$

We have $m_\rho = 0$ and, from Lemma 27, we know that the assumption that no bad place ramifies in L/K implies that $C(E/L)/C(E/F)$ has even ℓ-adic valuation. This implies that $m_{\mathbb{1}} + m_\varepsilon$ is even, i.e. the ℓ-parity is valid for E/F. By Proposition 4 this implies that the ℓ-parity also holds for E/K.

ACKNOWLEDGEMENTS

We express our gratitude to Tim and Vladimir Dokchitser, Jean Gillibert, Christian Liedtke, James S. Milne, Takeshi Saito, Ki-Seng Tan, Douglas Ulmer, and the anonymous referee for useful comments on the preliminary versions of this paper.

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

References

Cas65 J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–199.

CFKS10 J. Coates, T. Fukaya, K. Kato and R. Sujatha, *Root numbers, Selmer groups, and non-commutative Iwasawa theory*, J. Algebraic Geom. **19** (2010), 19–97.

Dok05 V. Dokchitser, *Root numbers of non-abelian twists of elliptic curves*, Proc. Lond. Math. Soc. (3) **91** (2005), 300–324, with an appendix by Tom Fisher.

DD08 T. Dokchitser and V. Dokchitser, *Parity of ranks for elliptic curves with a cyclic isogeny*, J. Number Theory **128** (2008), 662–679.

DD09a T. Dokchitser and V. Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178** (2009), 23–71.

DD09b T. Dokchitser and V. Dokchitser, *Root numbers and parity of ranks for elliptic curves*, J. Reine Angew. Math., to appear, Preprint (2009) available at http://arxiv.org/abs/0906.1815.

DD09c T. Dokchitser and V. Dokchitser, *Self-duality of Selmer groups*, Math. Proc. Cambridge Philos. Soc. **146** (2009), 257–267.

DD10 T. Dokchitser and V. Dokchitser, *On the Birch–Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) **172** (2010), 567–596.

Gon09 C. D. González-Avilés, *Arithmetic duality theorems for 1-motives over function fields*, J. Reine Angew. Math. **632** (2009), 203–231.

GT07 C. D. González-Avilés and K.-S. Tan, *A generalization of the Cassels–Tate dual exact sequence*, Math. Res. Lett. **14** (2007), 295–302.

GD70 A. Grothendieck and M. Demazure (ed), *Schémas en groupes. I: Propriétés générales des schémas en groupes*, in *Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck*, Lecture Notes in Mathematics, vol. 151 (Springer, Berlin, 1970).

HS09 D. Harari and T. Szamuely, *Corrigenda for: arithmetic duality theorems for 1-motives*, J. Reine Angew. Math. **632** (2009), 233–236.

Hel09 H. A. Helfgott, *On the behaviour of root numbers in families of elliptic curves*, Preprint (2009), available at http://arxiv.org/abs/math.NT/0408141.

KT03 K. Kato and F. Trihan, *On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$*, Invent. Math. **153** (2003), 537–592.

KM85 N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108 (Princeton University Press, Princeton, NJ, 1985).

Kim07 B. D. Kim, *The parity conjecture for elliptic curves at supersingular reduction primes*, Compositio Math. **143** (2007), 47–72.

MR07 B. Mazur and K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), 579–612.

Mil68 J. S. Milne, *The Tate–Šafarevič group of a constant abelian variety*, Invent. Math. **6** (1968), 91–105.

Mil80 J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33 (Princeton University Press, Princeton, NJ, 1980).

Mil06 J. S. Milne, *Arithmetic duality theorems*, second edition (BookSurge, LLC, Charleston, SC, 2006).

Nek01 J. Nekovář, *On the parity of ranks of Selmer groups. II*, C. R. Math. Acad. Sci. Paris Sér. I **332** (2001), 99–104.

Nek09 J. Nekovář, *On the parity of ranks of Selmer groups. IV*, Compositio Math. **145** (2009), 1351–1359, with an appendix by Jean-Pierre Wintenberger.

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press

Nek10 J. Nekovář, *Some consequences of a formula of Mazur and Rubin for arithmetic local constants*, Preprint (2010).

Roh94 D. E. Rohrlich, *Elliptic curves and the Weil–Deligne group*, in *Elliptic curves and related topics*, CRM Proceedings Lecture Notes, vol. 4 (American Mathematical Society, Providence, RI, 1994), 125–157.

Tat95 J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, vol. 9 (Soc. Math. France, Paris, 1995), Exp. No. 306, 415–440.

TO70 J. Tate and F. Oort, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21.

Ulm91 D. L. Ulmer, *p-descent in characteristic p*, Duke Math. J. **62** (1991), 237–265.

Ulm04 D. Ulmer, *Elliptic curves and analogies between number fields and function fields*, in *Heegner points and Rankin L-series*, Mathematical Sciences Research Institute Publications, vol. 49 (Cambridge University Press, Cambridge, 2004), 285–315.

Ulm05 D. L. Ulmer, *Geometric non-vanishing*, Invent. Math. **159** (2005), 133–186.

Fabien Trihan fabien.trihan@nottingham.ac.uk
School of Mathematical Sciences, University Nottingham, Nottingham NG7 2RD, UK

Christian Wuthrich christian.wuthrich@gmail.com
School of Mathematical Sciences, University Nottingham, Nottingham NG7 2RD, UK

https://doi.org/10.1112/S0010437X1100532X Published online by Cambridge University Press