The 2-parity conjecture for elliptic curves with isomorphic 2-torsion

Holly Green and Céline Maistret

1. Introduction

(a) Main results

For an abelian variety $A$ over a number field $K$, the Birch–Swinnerton-Dyer conjecture predicts that the algebraic rank of $A/K$ is given by the order of vanishing of its $L$-function $L(A/K, s)$ at $s = 1$. In addition, the completed $L$-function of $A/K$ is expected to satisfy a functional equation centred around $s = 1$, whose sign is given by the global root number of $A/K$. It then follows that the global root number should predict the parity of the order of vanishing of $L(A/K, s)$ at $s = 1$, which combined with the Birch–Swinnerton-Dyer yields the parity conjecture.
Conjecture 1.1 (Parity conjecture). For every abelian variety $A$ over a number field $K$,
\[ (-1)^{\text{rk}(A/K)} = w_{A/K}, \]
where $\text{rk}(A/K)$ and $w_{A/K}$ denote the rank and global root number of $A/K$, respectively.

The global root number is defined as a product of local root numbers which can be computed via the local Galois representations of $A/K$. The parity conjecture therefore offers an effective way to compute the parity of $\text{rk}(A/K)$.

There is no known successful approach to prove the parity conjecture unconditionally at present. However, assuming the finiteness of the Shafarevich–Tate group of $A/K$, several instances of the parity conjecture have been proven via the $p$-parity conjecture. Recall that, for each prime $p$, $\text{III}_{A/K}[p^\infty]$ decomposes as $(\mathbb{Q}_p/\mathbb{Z}_p)^\delta_p \times \Delta$, where $\Delta$ is a finite group and $\delta_p$ is a non-negative integer.

Define the $p^\infty$-Selmer rank as $\text{rk}_p(A/K) = \text{rk}(A/K) + \delta_p$. If $\text{III}_{A/K}$ is indeed finite then $\delta_p = 0$ for all $p$ so that $\text{rk}_p(A/K) = \text{rk}(A/K)$ for all $p$. This prompts the $p$-parity conjecture.

Conjecture 1.2 ($p$-parity conjecture). For every abelian variety $A$ over a number field $K$ and every prime $p$,
\[ (-1)^{\text{rk}_p(A/K)} = w_{A/K}. \]

In certain settings, the parity of the $p^\infty$-Selmer rank is computable and this can lead to a proof of the $p$-parity conjecture. Most notably the $p$-parity conjecture is known for elliptic curves over $\mathbb{Q}$ [1], for elliptic curves over number fields admitting a $p$-isogeny [2], for elliptic curves over totally real number fields when $p \neq 2$ (and in all non CM cases and some CM cases when $p = 2$) [3–7] and for quadratic twists of elliptic curves [8]. In particular, the $p$-parity conjecture is still open for elliptic curves over number fields in general. In higher dimensions, the $p$-parity conjecture is known for principally polarized abelian surfaces subject to local conditions [9], for Jacobians of hyperelliptic curves base-changed from a subfield of index 2 [10] and abelian varieties admitting a suitable isogeny [11]. In this paper, we consider two elliptic curves whose 2-torsion groups are isomorphic as Galois modules and prove the following.

Theorem 1.3 (Theorem 6.4). Let $E_1, E_2/K$ be elliptic curves over a number field. If $E_1[2] \cong E_2[2]$ as Galois modules, then the 2-parity conjecture holds for $E_1/K$ if and only if it holds for $E_2/K$.

Combining theorem 1.3 with the known results for the 2-parity conjecture for non-CM elliptic curves over totally real fields mentioned above, we prove the 2-parity conjecture for all CM curves over totally real fields.

Theorem 1.4 (Theorem 6.5). Let $E/K$ be an elliptic curve over a totally real number field with complex multiplication. The 2-parity conjecture holds for $E/K$.

In turn, we complete the proof of the $p$-parity conjecture for elliptic curves over totally real fields.

Theorem 1.5 (Corollary 6.6). Let $p$ be a prime and $K$ be a totally real field. The $p$-parity conjecture holds for all elliptic curves over $K$.

(b) Setup

The condition on the 2-torsion groups in theorem 1.3 provides us with a simple setup which we will use throughout this article.

Definition 1.6. Let $f(x)$ be a separable monic cubic polynomial such that $f(0) \neq 0$. We let
\[ E : y^2 = f(x) \quad \text{and} \quad E' : y^2 = xf(x). \]

Thanks to lemma 6.3, it is enough to work with $E$ and $E'$ to recover theorem 1.3 (see corollary 1.6 in [3] for results on 2-parity conjecture for elliptic curves over quadratic extensions). We therefore prove the following.
Theorem 1.7 (Theorem 6.1). Let $K$ be a number field. The 2-parity conjecture holds for $E/K$ if and only if it holds for $\text{Jac} E'/K$.

Lemma 2.3 also guarantees the existence of an isogeny $\phi : E \times \text{Jac} E' \to \text{Jac} C$, where $C : y^2 = f(x^2)$. It follows that theorem 1.7 yields

Theorem 1.8 (Theorem 6.2). Let $K$ be a number field, $c \in K^\times$ and $f(x) \in K[x]$ be a separable monic cubic polynomial such that $f(0) \neq 0$. The 2-parity conjecture holds for $\text{Jac} C/K$ where $C : y^2 = cf(x^2)$ is a genus 2 hyperelliptic curve.

Remark 1.9. Since no condition is imposed on the Galois group of the polynomial defining $C$, theorem 1.8 generalizes theorem 11.2 in [9] in the case of Jacobians of genus 2 curves which are isogenous to a product of elliptic curves.

As mentioned before, assuming finiteness of the Shafarevich–Tate group allows us to convert our results on the 2-parity conjecture into results on the parity conjecture.

Corollary 1.10. Let $K$ be a number field.

(1) If $E_1[2] \cong E_2[2]$ as Galois modules and both $\text{III}_{E_1/K}[2^\infty]$ and $\text{III}_{E_2/K}[2^\infty]$ are finite then the parity conjecture holds for $E_1/K$ if and only if it holds for $E_2/K$.

(2) If $\text{III}_{E/K}[2^\infty]$ and $\text{III}_{E'}[2^\infty]$ are finite then the parity conjecture holds for $E/K$ if and only if it holds for $E'/K$.

(3) If $\text{III}_{\text{Jac} C/K}[2^\infty]$ is finite then the parity conjecture holds for $\text{Jac} C/K$.

(c) Approach

Our approach relies on the existence of $\phi$ (lemma 2.3) which we use to express the parity of the $2^\infty$-Selmer rank of $E \times \text{Jac} E'$ as a product of local terms running over all places of $K$.

Definition 1.11. Let $\mathcal{K}$ be a local field. We write

$$
\lambda_{f,\mathcal{K}} = \mu_{C/\mathcal{K}} \cdot (-1)^{\dim_\mathcal{K} \ker \phi|_\mathcal{K} - \dim_\mathcal{K} \text{coker} \phi|_\mathcal{K}},
$$

where $\mu_{C/\mathcal{K}}$ is $-1$ if $C$ is deficient over $\mathcal{K}$ (as defined in [12, \S8]) and 1 otherwise. Here $\ker \phi|_\mathcal{K} = (E \times \text{Jac} E')(\mathcal{K})[\phi]$ and $\text{coker} \phi|_\mathcal{K} = [\text{Jac} C(\mathcal{K})/\phi((E \times \text{Jac} E')(\mathcal{K}))]$.

Theorem 1.12 (Theorem 2.4). Let $K$ be a number field. Then

$$
(-1)^{r_{K_e}E/K + r_{K_e}E'/K} \prod_v \lambda_{f,\mathcal{K}_v} = \prod_v w_{E/K_v} w_{\text{Jac} E'/K_v},
$$

where the product runs over all places of $K$.

Using this expression for the parity of the $2^\infty$-Selmer rank of $E \times \text{Jac} E'$, we prove that the 2-parity conjecture holds for $E \times \text{Jac} E'$ by comparing $\lambda_{f,\mathcal{K}_v}$ and $w_{E/K_v} w_{\text{Jac} E'/K_v}$ place by place and showing that

$$
\prod_v \lambda_{f,\mathcal{K}_v} = \prod_v w_{E/K_v} w_{\text{Jac} E'/K_v},
$$

in turn proving that

$$
(-1)^{r_{K_e}E/K + r_{K_e}E'/K} = w_{E/K\mathcal{K}} w_{\text{Jac} E'/K}.
$$

The point of this approach is that one can express each $\lambda_{f,\mathcal{K}_v}$ in terms of local arithmetic invariants of $E, \text{Jac} E'$ and $\text{Jac} C$ (lemmas 2.6 and 2.7). In most cases (when $v$ is an infinite or an odd place with semistable reduction), $\lambda_{f,\mathcal{K}_v}$ and the local root numbers $w_{E/K_v} w_{\text{Jac} E'/K_v}$ can be computed and compared locally. This leads to the most tricky part of the proof. It turns out that in general, $\lambda_{f,\mathcal{K}_v}$ and $w_{E/K_v} w_{\text{Jac} E'/K_v}$ do not agree locally. The bulk of the proof is then to find an expression $H_{f,\mathcal{K}_v}$ for that local discrepancy satisfying the product formula $\prod_v H_{f,\mathcal{K}_v} = 1$ and prove that

$$
w_{E/K_v} w_{\text{Jac} E'/K_v} = \lambda_{f,\mathcal{K}_v} H_{f,\mathcal{K}_v} \quad \text{for all } v.
$$

(†)

In this article, we propose an expression for $H_{f,\mathcal{K}_v}$ in the form of a product of Hilbert symbols (definition 2.8).
Finding the local error term $H_{f,K_v}$ is a common challenge in all instances of the proof of the $p$-parity conjecture listed in §1a. This is mainly due to the fact that no conceptual understanding of this local discrepancy exists at the moment. In particular, so far, each proof has exhibited a different ad hoc expression for the local error term with no obvious link to one another.

In appendix A, the first author conjectures an expression for a generalization of the error term defined in this paper for certain hyperelliptic curves, and observes that in the case of elliptic curves, it reduces to the error term presented in [13]. The appendix also explains what prompted our formulation of $H_{f,K_v}$.

(d) Overview

In §2, we establish the existence of $\phi$, prove a few of its properties, write $(-1)^{rk_{E/K}+rk_{\text{Jac}E/K}}$ as a product of local invariants (definition 1.11, lemmas 2.6 and 2.7), and introduce the local discrepancy $H_{f,K_v}$ (definition 2.8). Section 3 proceeds to prove that $\dagger$ holds over archimedean fields. This is followed by §4 which presents the theory of clusters that are used to prove $\dagger$ over non-archimedean local fields when $f(x)$ is integral, both $E$ and $E'$ have semistable reductions and $xf(x)$ has at most one double root. Section 5 then deals with the remaining cases by using a continuity argument in §5a, a few reduction steps and then a global–local argument in §5b. Lastly, §6 establishes our global results by taking the product of $\dagger$ over all places of $K$ and using the product formula for Hilbert symbols.

(e) Related work

We note that in a related work presented in [14], the authors compare the $p$-Selmer rank, global and local root numbers of two elliptic curves with equivalent mod $p$ Galois representations over number fields when the prime $p$ is odd.

2. Parity of the $2^\infty$-Selmer rank

In this section, we present how to control the parity of the $2^\infty$-Selmer rank of $E \times \text{Jac} E'$. The results here mimic those of [9, §3].

**Notation 2.1.** Let $K$ be a field of characteristic 0 and let $f(x) \in K[x]$ be a separable monic cubic polynomial with $f(0) \neq 0$. We write $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$.

**Remark 2.2.** Since $E' : y^2 = xf(x)$ has a rational point, the map $X = -(\alpha_1 \alpha_2 \alpha_3/x), Y = \alpha_1 \alpha_2 \alpha_3 y/x^2$ gives the following model for $\text{Jac} E'$.

$$\text{Jac} E' : y^2 = (x + \alpha_2 \alpha_3)(x + \alpha_1 \alpha_3)(x + \alpha_1 \alpha_2).$$

**Lemma 2.3.** Let $K$ be a field of characteristic 0 and let $f(x) \in K[x]$ be a separable monic cubic polynomial with $f(0) \neq 0$. There is an isogeny $\phi : E \times \text{Jac} E' \rightarrow \text{Jac} C$, where $C : y^2 = f(x^2)$, such that the dual isogeny $\phi^!$ satisfies $\phi \phi^! = [2]$, with

$$\ker \phi = \left\{ O, \left( (\alpha_i, 0), \left( -\frac{\alpha_1 \alpha_2 \alpha_3}{\alpha_i}, 0 \right) \right) \right\} \text{ for } i = 1, 2, 3.$$

**Proof.** This is theorem 14.1.1 in [15], where to recover $C : y^2 = f(x^2)$ we let $G_i = (x^2 - \alpha_i)$ in (ii) for $i = 1, 2, 3$. In our case the maps $C \rightarrow E$ and $C \rightarrow \text{Jac} E'$ are given in (14.1.4) and (14.1.5) respectively by

$$(x, y) \mapsto (x^2, y) \quad \text{and} \quad (x, y) \mapsto \left( \frac{-\alpha_1 \alpha_2 \alpha_3}{x^2}, \frac{\alpha_1 \alpha_2 \alpha_3}{x^3} \right).$$

Since $\ker \phi = \phi^!(\text{Jac} C[2])$ we use the explicit description of the isogeny $\phi^! : \text{Jac} C \rightarrow E \times \text{Jac} E'$ given in the footnote of theorem 14.1.1 to compute $\phi^!(\text{Jac} C[2])$. 

Fix a choice of square root for $\alpha_2$ and $\alpha_3$ and consider $P \in \text{Jac} C[2]$, given by $P = ((\sqrt{\alpha_2}, 0), (\sqrt{\alpha_3}, 0))$. Then

$$
\phi^1(P) = ((\alpha_2, 0) + (\alpha_3, 0), (-\alpha_1 \alpha_3, 0) + (-\alpha_1 \alpha_2, 0)) = ((\alpha_1, 0), (-\alpha_2 \alpha_3, 0)) \in E \times \text{Jac} E'.
$$

The result follows by permuting indices.

(a) Parity theorem

The isogeny $\phi$ allows us to express the parity of the $2\infty$-Selmer rank of $E \times \text{Jac} E'$ as a product of local terms.

**Theorem 2.4.** Let $K$ be a number field and let $f(x) \in K[x]$ be a separable monic cubic polynomial with $f(0) \neq 0$. Then

$$
(-1)^{\rho_{E/K} + \rho_{\text{Jac} E'}/K} = \prod_v \lambda_{f,K_v},
$$

where $\lambda_{f,K_v}$ is as definition 1.11 and the product runs over all places of $K$.

**Proof.** This follows from [9] theorem 3.2 with $A = E \times \text{Jac} E'$ and $A' = \text{Jac} C$.

(b) Kernel/Cokernel on local points

The local arithmetic data attached to the curves $E, E'$ and $C$ provide us with a practical way to compute the quantity $\lambda_{f,K_v}$.

**Notation 2.5.** For a curve $C/\mathbb{R}$ with Jacobian $A$, we write $n_{C/\mathbb{R}}$ for the number of connected components of $C(\mathbb{R})$. We write $A(\mathbb{R})^0$ for the connected component of $A$ containing the identity and $n_{A/\mathbb{R}} = |A(\mathbb{R})/A(\mathbb{R})^0|$ for the number of connected components.

For $K/\mathbb{Q}_p$ a finite extension, we denote by $c_{A/K}$ and $\omega_{A/K}$ the Tamagawa number and Néron exterior form for $A/K$.

**Lemma 2.6 ([9] lemma 3.4).** Let $K$ be a local field and let $f(x) \in K[x]$ be a separable monic cubic polynomial with $f(0) \neq 0$. Let $\phi$ be as in lemma 2.3. Then

$$
\frac{|\ker \phi|_{K_v}}{|\text{coker} \phi|_{K_v}} = \frac{|(E \times \text{Jac} E')(K)\phi|}{\prod_{v} n_{E/K} n_{\text{Jac} E'/K}}
$$

where $|x|_K$ denotes the normalized absolute value of $x$.

**Lemma 2.7 ([16] Prop. 3.2.2 and 3.3).** For a smooth projective curve $C$ over $\mathbb{R}$

$$
n_{\text{Jac} C/\mathbb{R}} = \begin{cases}
2^n_{C/R} & \text{if } n_{C/R} > 0, \\
1 & \text{if } n_{C/R} = 0 \text{ and } C \text{ has even genus}, \\
2 & \text{if } n_{C/R} = 0 \text{ and } C \text{ has odd genus}.
\end{cases}
$$

(c) The local discrepancy

We present here an expression for the local discrepancy between $\lambda_{f,K}$ and $\omega_{E/K} \omega_{\text{Jac} E'/K}$.

**Definition 2.8.** Let $K$ be a local field of characteristic 0 and let $f(x) = x^3 + ax^2 + bx + c \in K[x]$ be such that $c \neq 0$ and $\Delta_f := 18abc - 4a^3c + a^2b^2 - 4b^3 - 27c^2 \neq 0$. Let $L = ab - 9c$ and define $H_{f,K}$ as the following product of Hilbert symbols

$$
H_{f,K} = \begin{cases}
(b, -c)_K \cdot (-2L, \Delta_f)_K \cdot (L, -b)_K & b, L \neq 0, \\
(-c, -1)_K \cdot (2c, \Delta_f)_K & \text{otherwise}.
\end{cases}
$$
Remark 2.9. As \( b \) or \( L \) approach 0, both expressions for \( H_{f,K} \) agree. This can be seen in the proof of lemma 5.4.

Remark 2.10. The invariant \( L \) appearing in the definition of \( H_{f,K} \) can be written in terms of the roots of \( f \) as
\[
L = 8\alpha_1\alpha_2\alpha_3 - (\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_3).
\]

**Theorem 2.11 (Local theorem).** Let \( K \) be a local field of characteristic 0 and let \( f(x) \in K[x] \) be a separable monic cubic polynomial with \( f(0) \neq 0 \). Then
\[
w_{E/K}w_{\text{Jac}E/K} = \lambda_{f,K}H_{f,K}.
\]
The essential property of this description is that it explains why \( w_{E/K}w_{\text{Jac}E/K} \) and \( \lambda_{f,K} \) always differ at an even number of places, since, by the product formula for Hilbert symbols, \( \prod_v H_{f,K_v} = 1 \), where \( K \) is a number field and the product runs over all places of \( K \). Sections 3–5 will be dedicated to proving this statement.

3. Local theorem over archimedean fields

Here we prove that theorem 2.11 holds when \( K \) is an archimedean local field.

**Proposition 3.1.** Theorem 2.11 holds when \( K = C \).

**Proof.** Here \( w_{E/C} = w_{\text{Jac}E/C} = -1 \), \( H_{f,C} = 1 \) and by lemma 2.6 \( \lambda_{f,C} = (-1)^2 = 1 \).

**Proposition 3.2.** Theorem 2.11 holds when \( K = \mathbb{R} \).

**Proof.** We note first that \( w_{E/R}w_{\text{Jac}E/R} = +1 \) so we need only verify that \( \lambda_{f,R} = H_{f,R} \). Table 1 gives the values of \( n_{E/R}, n_{\text{Jac}E/R}, n_{\text{Jac}C/R}, |(E \times \text{Jac}E')(\mathbb{R}^0)\phi||, \mu_{C/R}, \lambda_{f,R} \) and \( H_{f,R} \) for each possible arrangement of the real roots of \( x^3f(x) \). In particular, column 2 lists the real roots of \( x^3f(x) \) from smallest to largest where the roots of \( f \) are denoted by red circles (\( \bullet \)), and the root 0 (of \( x \)) by a blue diamond (\( \bigcirc \)).

The contents of columns 3, 4 and 5 are determined using lemma 2.7 and observing that \( n_{E/R} = n_{E/R} = 2 \) when \( f \) has 3 real roots and 1 otherwise, and that \( n_{C/R} = 3 \) when \( f \) has 3 positive real roots, 2 when \( f \) has 2 positive real roots and 1 otherwise.

For column 6 we use the description of \( \ker \phi \) as given in lemma 2.3. We count how many elements belong to the identity component of \( (E \times \text{Jac}E')(\mathbb{R}) \) (i.e. each entry of the pair lies on the identity component of the corresponding curve). Clearly the point at infinity on \( (E \times \text{Jac}E') \) always satisfies these conditions. Let \( \alpha_3 \) be the largest real root of \( f \), so that \( (\alpha_3,0) \in E(\mathbb{R})^0 \) and \( (\alpha_1,0), (\alpha_2,0) \notin E(\mathbb{R})^0 \). Now \( |(E \times \text{Jac}E')(\mathbb{R}^0)\phi|| \) is 2 precisely when \( -\alpha_1\alpha_2,0 \in \text{Jac}E'(\mathbb{R})^0 \), i.e. when \( -\alpha_1\alpha_2 \) is the largest real element of \( S = \{-\alpha_1\alpha_2,-\alpha_2\alpha_3,-\alpha_1\alpha_3\} \), and 1 otherwise. In cases 1–4, \( \alpha_1,\alpha_2,\alpha_3 \in \mathbb{R} \) so \( S \subseteq \mathbb{R} \) and it can be observed that \( -\alpha_1\alpha_2 \) is the largest precisely when \( \alpha_1,\alpha_2 > 0 \). In cases 5 and 6, \( \alpha_1 = \bar{\alpha}_2 \) and so \( -\alpha_1\alpha_2 \) is the only real element of \( S \), in particular it is the largest real element.

Column 7 keeps track of the deficiency contribution from \( C/R \). As \( C(\mathbb{R}) \) is always non-empty, this is 1.

Column 8 gives the value of \( \lambda_{f,R} \) calculated using lemma 2.6.

We now justify the value of \( H_{f,R} \), as given in column 9, via a case by case analysis of the signs of the Hilbert symbol entries.

**Claim:** When \( b,L \neq 0 \), \( H_{f,R} = (\bar{L},\Delta_f)_R \cdot (L,-ac)_R \cdot (a,-c)_R \). This is true as \( (L,abc)_R = (ab,-c)_R \) by the standard Hilbert symbol identity \( (A + B, AB)_R = (A, B)_R \), thus \( (L,-b)_R = (L,-ac)_R \cdot (ab,-c)_R \).

Since the sign of \( a \) is easier to control than that of \( b \), we will use this equivalent expression for \( H_{f,R} \) whenever \( b,L \neq 0 \).
Here $\Delta_f, b, ac > 0$. Applying the AM-GM inequality gives that $\alpha_i + \alpha_j > 2\sqrt{\alpha_i \alpha_j}$ in case 1 and $\alpha_i + \alpha_j > -2\sqrt{\alpha_i \alpha_j}$ in case 4, for $i \neq j$. In particular, in case 1 we have $L < 0$ and $H_{f, R} = -1$ and in case 4 we have $L > 0$ and $H_{f, R} = 1$.

(2) Here $\Delta_f, c > 0$. If $b, L \neq 0$ then $H_{f, R} = (L, -a)_R \cdot (a, -1)_R$ which is $-1$ unless $a, L > 0$. Suppose $\alpha_1 < 0$, if $a > 0$ then $\alpha_1 + \alpha_2, \alpha_1 + \alpha_3 < 0$ and $\alpha_2 + \alpha_3 > 0$ so $L < 0$ using remark 2.10. If $bl = 0$ then clearly $H_{f, R}$ again evaluates to $-1$.

(3) Here $\Delta_f > 0, c < 0$. If $b, L \neq 0$ then $H_{f, R} = (L, a)_R$ which is $1$ unless $a, L < 0$. Suppose $\alpha_1, \alpha_2 < 0$, if $a < 0$ then $\alpha_1 + \alpha_3, \alpha_2 + \alpha_3 > 0$ and $\alpha_1 + \alpha_2 < 0$ so $L > 0$ using remark 2.10. If $bl = 0$ then clearly $H_{f, R}$ again evaluates to $1$.

(5) Here $\Delta_f, c < 0$. If $b, L \neq 0$ then $H_{f, R} = (-L, -a)_R$ which is $1$ unless $a > 0$, $L < 0$. Suppose $\alpha_2 = \bar{\alpha}_1$, if $a > 0$ then $\alpha_1 + \alpha_2 < 0$ so $L > 0$ using remark 2.10. If $bl = 0$ then clearly $H_{f, R}$ again evaluates to $1$.

(6) Here $\Delta_f < 0, c > 0$. If $b, L \neq 0$ then $H_{f, R} = (-L, a)_R$ which is $1$ unless $a < 0$, $L > 0$. Suppose $\alpha_2 = \bar{\alpha}_1$, if $a < 0$ then $\alpha_1 + \alpha_2 > 0$ so $L < 0$ using remark 2.10. If $bl = 0$ then clearly $H_{f, R}$ again evaluates to $-1$.

4. Local theorem over non-archimedean fields for nice reduction types

Here we prove that theorem 2.11 holds when $K/Q_p$ is a finite extension for an odd prime $p$ and the reduction of $E'$ is of a certain type. We write $\pi_K$ for a choice of uniformizer of $K$ and $v$ for the normalized valuation. We begin by recalling some useful terminology.

(a) Clusters: curves over local fields with odd residue characteristic

To keep track of the arithmetic invariants needed to compute $\lambda_{f, K}$ as in lemma 2.6, we use the machinery of ‘clusters’ [17,18]. Clusters allow us to extract arithmetic invariants of hyperelliptic curves over $p$-adic fields with $p$ odd from simple combinatorial data (see example 4.4 below for a worked out example).

**Definition 4.1 (Clusters).** Let $K$ be a finite extension of $Q_p$ where $p$ is an odd prime and $C : y^2 = cf(x)$ a hyperelliptic curve, where $c \in K^\times$ and $f(x) \in K[x]$ is monic with set of roots $\mathcal{R}$. A *cluster* is a non-empty subset $s \subset \mathcal{R}$ of the form $s = D \cap \mathcal{R}$ for some disc $D = \{x \in \bar{K} \mid v(x - z) \geq d\}$ for some $z \in \bar{K}$ and $d \in Q$.

For a cluster $s$ of size $> 1$, its depth $d_s$ is the maximal $d$ for which $s$ is cut out by such a disc, that is $d_s = \min_{r, r' \in s} v(r - r')$. If moreover $s \neq \mathcal{R}$, then its relative depth is $\delta_s = d_s - d_{P(s)}$, where $P(s)$ is the smallest cluster with $s \subseteq P(a)$ (the ‘parent’ cluster).

We refer to this data as the *cluster picture* of $C$, denoted $\Sigma_{C/K}$.

**Notation 4.2.** We draw cluster pictures by drawing roots $r \in \mathcal{R}$ as $\bullet$ and drawing ovals around roots to represent clusters (of size $> 1$). If we wish to specify which root is which, we instead draw
the roots of \( f \) as red circles \( \bullet \) and the root 0 (of \( x \)) as a blue diamond \( ◆ \). For example:

\[
\begin{array}{c}
\bullet \\
\circ \\
\end{array}
\text{or}
\begin{array}{c}
\circ \\
\bullet \\
\end{array}
\]

The subscript on the largest cluster \( \mathcal{R} \) is its depth; on the other clusters it is their relative depth.

**Definition 4.3 (Twins and signs).** A twin is a cluster of size 2. For each twin \( t = \{r_1, r_2\} \) pick a square root \( \theta_t = \sqrt{\prod_{i=1}^{t} (r_1 + r_2)/2 - n} \) and define its sign \( \pm \) through the formula \( \text{Frob}_K(\theta_t)/\theta_{\text{Frob}_K(t)} \equiv \pm 1 \) in the residue field, where \( \text{Frob}_K \) denotes a Frobenius element in \( \text{Gal}(\bar{K}/K) \). Note that the sign depends on the choice of square root.

**Example 4.4.** Let \( K = \mathbb{Q}_{17} \) and \( E : y^2 = (x - 17)(x - 1)(x - 2) \). Then \( E' : y^2 = (x + 2)(x + 34)(x + 17) \). We see that both \( \Sigma_{E'/\mathbb{Q}_{17}} \) and \( \Sigma_{\text{Jac} E'/\mathbb{Q}_{17}} \) have a twin cluster \( t_1 = (0, 17) \) and \( t_2 = (-34, -17) \) respectively. To determine the sign on \( t_1 \) we compute \( \theta_{t_1} = \sqrt{(17/2 - 1)(17/2 - 2)} \) and find that \( \text{Frob}_{\mathbb{Q}_{17}}(\theta_{t_1})/\theta_{\text{Frob}_{\mathbb{Q}_{17}}(t_1)} \equiv 1 \) mod 17. It follows that both \( t_1 \) and \( t_2 \) have sign +1. Therefore

\[
\Sigma_{E'/\mathbb{Q}_{17}} = \begin{array}{c} 0 \end{array}, \quad \Sigma_{E'/\mathbb{Q}_{17}} = \begin{array}{c} 0 \end{array}, \quad \text{and} \quad \Sigma_{\text{Jac} E'/\mathbb{Q}_{17}} = \begin{array}{c} 0 \end{array}.
\]

Using [19, Theorems 3.1 & 3.3] with \( f_1(x) = x, f_2(x) = (x - 17)(x - 1)(x - 2) \) we find that \( \mathcal{Y}_{C/\mathbb{Q}_{17}} \) is where Frobenius fixes the loop. Following [18] table 1.1, \( C \) has type \( 1_2^+ \) so that we have \( c_{\text{Jac} C/\mathbb{Q}_{17}} = -1 \) and \( \mu_{C/\mathbb{Q}_{17}} = -1 \). Tamagawa numbers and local root numbers for both elliptic curves \( E \) and \( \text{Jac} E' \) are \( e_{E/\mathbb{Q}_{17}} = 1, c_{\text{Jac} E'/\mathbb{Q}_{17}} = 2, w_E/\mathbb{Q}_{17} = 1 \) and \( w_{\text{Jac} E'/\mathbb{Q}_{17}} = -1 \). By definition 1.11 and lemma 2.6 it follows that \( \lambda_{E'/\mathbb{Q}_{17}} = -1 \). A simple computation shows that \( H_f/\mathbb{Q}_{17} = +1 \) which proves theorem 2.11 for this particular choice of \( E \).

**Proposition 4.5.** Theorem 2.11 holds when \( K/\mathbb{Q}_p \) is a finite extension for some odd prime \( p \), \( f(x) \in O_K[x] \) and both \( E, E' \) are semistable with \( E' \) having cluster picture either \( \begin{array}{c} 0 \end{array} \) or \( \begin{array}{c} 0 \end{array} \).

**Proof.** The input of table 2 are the cluster pictures of \( E \) and \( E' \) (columns 2 and 3), coloured according to Notation 4.2, such that \( E' \) has at most one double root. Column 1 indexes the various cases using the reduction types of \( C/K \) as defined in [18], table 1.1.

**Table 2.** Local data for \( K/\mathbb{Q}_p \) when \( E' \) has at worst one double root.

| types | \( \Sigma_{E'/K} \) | \( \Sigma_{E/K} \) | \( \Sigma_{\text{Jac} E'/K} \) | \( \Sigma_{\text{Jac} E/K} \) | \( \mathcal{Y}_{C/K} \) | \( c_{\text{Jac} E'/K} \) | \( c_{\text{Jac} E/K} \) | \( \mu_{C/K} \) | \( \lambda_{E/K} \) | \( W_{E/K} \) | \( W_{\text{Jac} E/K} \) | \( H_{f/K} \) |
|-------|------------------|------------------|------------------|------------------|-----------------|------------------|------------------|------------------|-----------------|----------------|----------------|----------------|
| 2     | 0                | 0                | 0                | 0                | 1               | 1               | 1               | 1               | +1              | +1             | +1             | +1             |
| \( 1_2^- \) | 0                | 0                | 0                | 0                | 1               | 2               | 1               | -1              | -1              | -1             | 1              | -1             |
| \( 1_2^+ \) | 0                | 0                | 0                | 0                | 1               | 2               | \( n \)          | 1               | \( -1 \)       | +1             | \( -1 \)       | +1             |
| \( 1_{n,-}^+ \) | 0                | 0                | 0                | 0                | 1               | \( n \)          | \( n \)          | 1               | \( -1 \)       | +1             | \( -1 \)       | +1             |
| \( 1_{n,-}^- \) | 0                | 0                | 0                | 0                | 1               | \( n \)          | \( n \)          | 1               | \( -1 \)       | +1             | \( -1 \)       | +1             |

Notation: \( x = 2 \) if \( x \) and \( \bar{x} = 1 \) if \( \bar{x} \).
Column 4 gives the cluster picture for Jac \( E' \), which is easily determined from that of \( E' \) using remark 2.2.

Column 5 gives the dual graph of the minimal regular model of \( C \), denoted \( \gamma_{C/K} \), where an arrow is used to indicate the action of Frobenius. This is determined using [19, Theorems 3.1 & 3.3] with \( f_1(x) = x, f_2(x) = f(x) \) so that \( Y \) becomes \( C \).

Columns 6 and 7 list the Tamagawa numbers for \( E \) and Jac \( E' \), calculated from their respective cluster pictures using [20, table 15.1].

Similarly, column 8 contains the Tamagawa number for Jac \( C \) but this time calculated from \( \gamma_{C/K} \) using [18, Theorem 12.4].

Column 10 gives the value of \( \lambda_{f,K} \) calculated using lemma 2.6.

Column 11 gives \( \nu_{E/K} \nu_{jacE'/K} \) using that for a semistable elliptic curve \( E, \nu_{E/K} = -1 \) only when the curve has split multiplicative reduction, i.e. a twin with sign +.

It remains to compute the value of \( H_{f,K} \) via a case by case analysis of the valuations of \( b, c, L, \Delta_f \). Unless specified otherwise, equivalences are taken mod \( \pi_K \). By assumption \( a, b, c \in O_K \). Recall that \( \alpha_1, \alpha_2, \alpha_3 \) denote the roots of \( f \).

**Types 1**. We must show that \( H_{f,K} = 1 \). We have that \( v(c) = v(\Delta_f) = 0 \).

Suppose \( b, L \neq 0 \). Then \( H_{f,K} = (b, -L)_{K} \cdot (L, -b\Delta_f)_{K} \). If \( v(b) = v(L) = 0 \) we are done. Suppose that \( K/ \mathbb{Q}_p \) and \( p \neq 3 \). If \( b \equiv 0 \) then \( L \equiv -9c \) so \( H_{f,K} = 1 \). If \( L \equiv 0 \) then \( v(a) = v(b) = 0 \) and \( -b\Delta_f \equiv (4/b^2)(b^3 - 27c^2)^2 \) so again \( H_{f,K} = 1 \).

Now suppose that \( K/ \mathbb{Q}_3 \) and \( L \equiv 0 \). Write \( b = \pi_K^{\nu(b)} u_1, 3 = \pi_K^{\nu(3)} u_2 \) for units \( u_1, u_2 \) and assume that \( v(b) > 0 \) (if \( v(b) = 0 \) then we again observe that \( -b\Delta_f \) is a square). Note that \( \Delta_f \equiv -a^3 \) so \( v(a) = 0 \).

- If \( v(b) < 2v(3) \), then \( L = \pi_K^{\nu(b)} (au_1 - \pi_K^{2v(3)} v(b) cu_2^2) \) where \( au_1 - \pi_K^{2v(3)} v(b) cu_2^2 \equiv au_1 \). So \( H_{f,K} = 1 \) having used the standard Hilbert symbol identity \( (\pi_K, -\pi_K) = 1 \).
- If \( v(b) = 2v(3) \), then \( L = \pi_K^{\nu(b)} (au_1 - cu_2^2) \) and \( H_{f,K} = (au_1 - cu_2^2, u_1, \Delta_f)_{K} \), having used that \( v(b) \) is even. If \( v(au_1 - cu_2^2) = 0 \) then we are done, else \( -u_1\Delta_f \equiv u_2^2a^2c^2 \). So \( H_{f,K} = 1 \).
- If \( v(b) > 2v(3) \), then \( L = \pi_K^{2v(3)} (\pi_K^{\nu(b)} - 2v(3) au_1 - cu_2^2) \) where \( \pi_K^{\nu(b)} - 2v(3) au_1 - cu_2^2 \equiv -cu_2^2 \). So \( H_{f,K} = 1 \).

Suppose \( bL = 0 \). Clearly \( H_{f,K} = 1 \).

**Types 1^+_n** or \( 1^-_n **. Suppose that \( \alpha_1 \equiv 0 \) with \( v(\alpha_1) = n \). Since \( \theta_{l,E} = \sqrt{\frac{1}{2}(\alpha_1 - 2\alpha_2)(\alpha_1 - 2\alpha_3)} \), it can be observed that we are in type \( 1^+_n \) when \( \alpha_2\alpha_3 \in (K^*)^2 \) (when \( \theta_{l,E} \in K^* \)), and type \( 1^-_n \) otherwise. We are required to show that \( H_{f,K} = -1 \) precisely when \( n \) is odd and \( \alpha_2\alpha_3 \notin (K^*)^2 \), i.e. that \( H_{f,K} = (\pi_K^{\nu(b)}, \alpha_2\alpha_3)_{K} \). We have that \( v(b) = v(\Delta_f) = 0 \) and \( v(c) = n \).

Suppose \( L \neq 0 \). Then \( H_{f,K} = (b, \pi_K^{\nu(b)})_{K} \cdot (L, -b\Delta_f)_{K} \) and as \( b \equiv \alpha_2\alpha_3 \) it remains to show that \( (L, -b\Delta_f)_{K} = 1 \). If \( v(L) = 0 \) we are done. If not, then since \( L \equiv -\alpha_2\alpha_3(2\alpha_1 + 2\alpha_2 + 2\alpha_3) \) we have that \( \alpha_1 \equiv -\frac{1}{4}(\alpha_2 + \alpha_3) \) and \( -cL \equiv \frac{3}{2} \frac{9}{2}(\alpha_2 + \alpha_3)^6 \).

Suppose \( b \neq 0 \). Then \( H_{f,K} = (b, -cL)_{K} \cdot (2L, \pi_K^{\nu(b)} \alpha_1) \) and as \( \equiv -(\alpha_2 + \alpha_3)(\alpha_1 - \frac{1}{2}(\alpha_2 + \alpha_3)^2) \) it remains to show that \( (b, -cL) = 1 \). If \( v(b) = 0 \) we are done. If not, since \( b \equiv \frac{1}{2}(\alpha_2 + \alpha_3)(2\alpha_1 + \frac{1}{2}(\alpha_2 + \alpha_3)) \) we have that \( \alpha_1 \equiv -\frac{1}{4}(\alpha_2 + \alpha_3) \) and \( -cL \equiv \frac{9}{2}(\alpha_2 + \alpha_3)^6 \).

Suppose \( b = 0 \). Then \( H_{f,K} = (2c, \pi_K^{\nu(b)})_{K} \) where \( 2c = 2\alpha_1(\alpha_2 + \alpha_3) \).
5. Local theorem in all remaining cases

Here we prove that theorem 2.11 holds in all remaining cases using a global–local argument. In summary, so far we have proved the following:

**Proposition 5.1.** Let $K$ be a local field of characteristic 0 and let $f(x) \in K[x]$ be a separable monic cubic polynomial with $f(0) \neq 0$. Theorem 2.11 holds when

1. $K = \mathbb{C}$,
2. $K = \mathbb{R}$, or
3. $K/\mathbb{Q}_p$ is a finite extension for an odd prime $p$, $f(x) \in \mathbb{O}_K[x]$, $E, E'/K$ are both semistable and $xf(x)$ has at least one double root mod $\pi_K$.

**Proof.** These are propositions 3.1, 3.2 and 4.5 respectively.

(a) Continuity of local invariants

**Lemma 5.2 ([3] lemma 3.2).** Let $K$ be a local field of characteristic 0. The Hilbert symbol $(A, B)_K$ is a continuous function of $A, B \in K^\times$.

**Lemma 5.3.** Let $K$ be a local field of characteristic 0 and $f(x) = x^3 + ax^2 + bx + c \in K[x]$ a separable cubic. The invariants $b, c, L := ab - 9c, \Delta_f, w_{E/K}, w_{E'/K}$ and $\lambda_{f,K}$ are continuous in the coefficients of $f(x)$.

**Proof.** This can be seen from [9, Lemma 9.2].

**Lemma 5.4.** Let $K$ be a local field of characteristic 0 and $f(x) \in \mathbb{O}_K[x]$ be a separable monic cubic. If $\tilde{f}(x) \in \mathbb{O}_K[x]$ is a separable monic cubic with coefficients close enough to those of $f$ then theorem 2.11 holds for $f$ if and only if it holds for $\tilde{f}$.

**Proof.** Write $f(x) = x^3 + ax^2 + bx + c$, $\tilde{f}(x) = x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c}$. If $b, L \neq 0$ then, ensuring that $\tilde{b}, \tilde{L} \neq 0$, this is clear from lemmas 5.2 and 5.3. If $b = \tilde{b} = 0$ or $L = \tilde{L} = 0$ then again this is clear. When we are not in either of these cases, lemma 5.3 still asserts that the root numbers are unchanged and that $\lambda_{f,K} = \lambda_{\tilde{f},K}$, but showing that $H_{f,K} = H_{\tilde{f},K}$ is more delicate.

Suppose that $K$ is non-archimedean. Let $\pi_K$ be a choice of uniformizer and $v$ a normalized valuation. We write $\Box$ for a non-zero square element in $K$.

Suppose that $b = 0$ and $\tilde{b} \neq 0$. Let $N = v(c) + v(36) + 1$ and pick $a \equiv \tilde{a}, b \equiv \tilde{b}, c \equiv \tilde{c}$ mod $\pi_K^N$. Then $\tilde{L} = \tilde{a}\tilde{b} - 9\tilde{c} \equiv -9\tilde{c} \neq 0$ mod $\pi_K^N$ and so $\tilde{L} = \tilde{c} \cdot 6$. Therefore $H_{f,K} = (\tilde{b}, -\tilde{c}) \cdot (2\tilde{c}, \Delta_f) \cdot (\tilde{c}, -1)_K$ and by lemma 5.2 this is equal to $H_{\tilde{f},K}$.

Now suppose that $L = 0$ and $\tilde{L} \neq 0$. Let $N = v(b) + 2v(a^2 - 3b) + v(16) + 1$ and pick $a \equiv \tilde{a}, b \equiv \tilde{b}c \equiv \tilde{c}$ mod $\pi_K^N$, $b \equiv \tilde{b}c \equiv \tilde{c}$ mod $\pi_K^N$. We have that $\tilde{a} \equiv 9\tilde{c} \mod \pi_K^N$, therefore $9\Delta_f \equiv -4\tilde{b}(a^2 - 3\tilde{b}) \neq 0$ mod $\pi_K^N$ and $\Delta_f = -\tilde{b} \cdot 6$. So, $H_{f,K} = (\tilde{b}, -\tilde{c}) \cdot (2\tilde{L}, -\tilde{b}) \cdot (\tilde{L}, -\tilde{b}) = (\tilde{b}, -\tilde{c}) \cdot (\tilde{L}, -\tilde{b})_K$ and by lemma 5.2 this is equal to $H_{\tilde{f},K}$ since $\Delta_f = -\tilde{b} \cdot 6$.

The case when $K$ is archimedean and $bL = 0$ follows from table 1 since $f$ and $\tilde{f}$ will have the same number of positive and negative real roots.

(b) Reduction steps

**Lemma 5.5.** Let $K$ be a non-archimedean local field of characteristic 0. It is sufficient to prove theorem 2.11 for $f(x) \in \mathbb{O}_K[x]$.

**Proof.** Let $g(x) = x^3 + ax^2 + bx + c \in K[x]$ and choose $d \in K^\times$ such that $d^3a, d^4b, d^6c \in \mathbb{O}_K$. Define $f(x) = x^3 + dx^2 + bx + d^6c \in \mathbb{O}_K[x]$. Since $y^2 = g(x) \equiv y^2 = f(x)$, $y^2 = xg(x) \equiv y^2 = xf(x)$ and $H_{g,K} = H_{f,K}$ (the Hilbert symbol entries have been scaled by squares), theorem 2.11 holds for $g(x)$ if and only if it holds for $f(x)$.
Lemma 5.6. Let \( K \) be a number field and \( f(x) = x^3 + ax^2 + bx + c \in O_K[x] \) a separable cubic such that \( a^2 - 3b, b, a^2 - 4b, ab - 9c, c \neq 0 \). Fix a prime \( p \mid 2, 3 \) and suppose that the following conditions are satisfied:

1. if \( p \mid a^2 - 3b \) then \( 9c \not\equiv ab \mod p \)
2. if \( p \mid b(a^2 - 4b) \) then \( c \not\equiv 0 \mod p \)

then \( xf(x) \) has either distinct roots or no worse than 1 double root modulo \( p \).

Proof. We must prove that (1) and (2) guarantee that \( xf(x) \) has at least three distinct roots mod \( p \).

Suppose that three roots of \( xf(x) \) are congruent mod \( p \). This happens when either (i) all three roots of \( f(x) \) are congruent, or (ii) two roots of \( f(x) \) are congruent to 0. Situation (i) occurs if \( f(x), f'(x) = 3x^2 + 2ax + b, f''(x) = 6x + 2a \) share a root mod \( p \), i.e. when \( f(-(a/3)) \equiv f'(-(a/3)) \equiv 0 \mod p \). Condition (1) ensures that this does not happen. We are in situation (ii) whenever \( f(0) \equiv f'(0) \equiv 0 \mod p \). Condition (2) ensures that this does not happen.

Now suppose that \( xf(x) \) has two double roots mod \( p \), so that two roots of \( f(x) \) are (nonzero and) congruent mod \( p \) with the remaining root congruent to zero. Here \( f(0) \equiv 0 \) and \( \Delta_f \equiv 0 \). By definition of \( \Delta_f \), these happen simultaneously when \( c \equiv 0 \) and \( a^2b^2 - 4b^3 \equiv 0 \), so again condition (2) ensures that this does not happen.

Remark 5.7. Using cluster pictures (see §4a), lemma 5.6 says that \( \Sigma_{E/K_p} \) is either \( \bullet \circ \circ \circ \) or \( \circ \circ \bullet \circ \circ \circ \). In particular, proposition 4.5 holds for such a choice of \( f \).

Lemma 5.8. Let \( K/\mathbb{Q}_3 \) be a finite extension and let \( f(x) = x^3 + x + 1 \in K[x] \) then theorem 2.11 holds.

Proof. \( E \) and \( \text{Jac} E' \) have good reduction at primes \( p \mid 3 \) so \( w_{E/K} = w_{\text{Jac} E/K} = 1 \) and \( \lambda_{f,K} = 1 \). That \( H_{f,K} = 1 \) follows by definition since \( H_{f,K} = (1, -1)_K \cdot (18, -31)_K \cdot (-9, -1)_K \).

Proof of theorem 2.11. We first prove that the theorem holds for \( K/\mathbb{Q}_2 \). Pick a totally real number \( K \) so that \( F_p \cong K \) (to see that such a field exists, if \( K = \mathbb{Q}_2(\theta) \) and \( h(x) \in \mathbb{Q}_2[x] \) is the minimal polynomial for \( \theta \) then approximate \( h(x) \) by some \( \tilde{h}(x) \in \mathbb{Q}[x] \) which has all real roots; then take \( F = \mathbb{Q}[x]/\tilde{h}(x) \)). Fix another prime \( p \neq p' \mid 2, 3 \). By lemma 5.5, we may assume that \( f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}_K[x] \). We will approximate \( f(x) \) by \( \tilde{f}(x) = x^3 + a\tilde{x}^2 + \tilde{b}x + \tilde{c} \in \mathbb{Q}_F[x] \) subject to the following:

1. pick \( \tilde{a} \) to be \( p \)-adically close to \( a \), \( p' \)-adically close to \(-1 \) and \( q \)-adically close to \( 0 \) for all \( q \mid 3 \);
2. pick \( \tilde{b} \neq 0, \frac{1}{2}\tilde{a}^2, \frac{1}{3}\tilde{a}^2\) so that \( \tilde{b} \) is \( p \)-adically close to \( b \), \( p' \)-adically close to \(-1 \) and \( q \)-adically close to \( 1 \) for all \( q \mid 3 \);
3. pick \( \tilde{c} \neq 0, \frac{1}{2}\tilde{a} \tilde{b} \) so that \( \tilde{c} \) is \( p \)-adically close to \( c \), \( p' \)-adically close to \( 1 \), \( q \)-adically close to \( 1 \) for all \( q \mid 3 \), and such that if \( q \mid 2, 3, p' \) then conditions (1) and (2) of lemma 5.6 are satisfied (namely: \( 9\tilde{c} \equiv \tilde{a} \tilde{b} \mod q \) for all \( q \mid \tilde{a}^2 - 3\tilde{b} \), and \( \tilde{c} \equiv 0 \mod q \) for all \( q \mid \tilde{b}(\tilde{a}^2 - 4\tilde{b}) \)).

Let \( \bar{E} : y^2 = \tilde{f}(x) \) and \( \bar{E}' : y^2 = xf(x) \). By construction, \( \tilde{f}(x) \) is \( p \)-adically close to \( f(x) \), \( p' \)-adically close to \( x^3 - x^2 - x + 1 \), \( q \)-adically close to \( x^3 + x + 1 \) when \( q \mid 3 \), and \( q \)-adically close to a monic cubic for which proposition 4.5 holds when \( q \mid 2, 3, p' \). Invoking lemma 5.4, this means that theorem 2.11 holds for \( \tilde{f} \in F_p[x] \) whenever \( v \neq p \), and proving it for \( \tilde{f} \in F_p[x] \) is equivalent to proving it for \( f \in F_p[x] \).

Since \( \text{ord}_p((j(E))), \text{ord}_p((j(E')))) < 0 \), and the 2-parity conjecture holds for elliptic curves over totally real number fields with non-integral \( j \)-invariant \([3, \text{Theorem } 2.4]\), it holds for \( E \) and \( E' \).
Therefore

\[
1 = (-1)^{rk_2 E/F + rk_2 \text{Jac} E/F} w_{E/F} w_{\text{Jac} E/F} \\
= \prod_v \lambda_{f,F_v} w_{E/F_v} w_{\text{Jac} E/F_v} \quad (= \text{theorem } 2.4) \\
= \lambda_{f,F_p} w_{E/F_p} w_{\text{Jac} E/F_p} \prod_{p \neq v} H_{f,F_v} \quad (= \text{theorem } 2.11) \\
= \lambda_{f,F_p} w_{E/F_p} w_{\text{Jac} E/F_p} H_{f,F_p} \quad (= \text{Hilbert symbol product law})
\]

where the products range over all places of \( F \). In conclusion, we now know that theorem 2.11 holds for \( f \in F_p[x] \) and so it must also hold for \( f \in F_p[x] \) where \( F_p \cong K \).

Using that theorem 2.11 now holds for \( K/\mathbb{Q}_2 \), we can prove it for \( K/\mathbb{Q}_p \) (\( p \) odd) by repeating the above argument after replacing 2 by \( p \) (when \( p = 3 \) we also replace the condition ‘\( q \mid 3 \)’ by ‘\( q \mid 3 \) and \( q \neq p \)’).

6. Global results

Here we present the 2-parity results we obtain as consequences to theorem 2.11.

**Theorem 6.1.** Let \( K \) be a number field and let \( f(x) \in K[x] \) be a separable monic cubic polynomial with \( f(0) \neq 0 \). The 2-parity conjecture holds for \( E/K \) if and only if it holds for \( \text{Jac} E'/K \).

**Proof.** Theorem 2.11 says that for each place \( v \) of \( K \), \( w_{E/K,v} w_{\text{Jac} E/K_v} = \lambda_{f,K_v} H_{f,K_v} \). Taking the product over all such \( v \) then invoking theorem 2.4 and the product formula for Hilbert symbols, we see that

\[
w_{E/K} w_{\text{Jac} E/K} = (-1)^{rk_2 E/K + rk_2 \text{Jac} E/K}.
\]

**Theorem 6.2.** Let \( K \) be a number field. The 2-parity conjecture holds for \( \text{Jac} C/K \) whenever \( C \) is a genus 2 hyperelliptic curve of the form \( C : y^2 = cf(x^2) \) with \( c \in K^\times \) and \( f(x) \in K[x] \) a separable monic cubic polynomial with \( f(0) \neq 0 \).

**Proof.** Let \( E_0 : y^2 = cf(x) \), \( E_0' : y^2 = cf(x^2) \). Adapting the proof of lemma 2.3 to incorporate the leading term \( c \in K^\times \) in \( C : y^2 = cf(x^2) \), shows that there is an isogeny \( E_0 \times \text{Jac} E_0' \to \text{Jac} C \). It follows that proving the 2-parity conjecture for \( \text{Jac} C/K \) is equivalent to proving it for \( E_0 \times \text{Jac} E_0'/K \). Define \( E : y^2 = f(x) \) and \( E' : y^2 = xf(x) \). Observe that the 2-parity conjecture for quadratic twists \([3, \text{Corollary 1.6}]\) says that the 2-parity conjecture holds for \( E_0/K \) (resp. \( \text{Jac} E_0'/K \)) if and only if it holds for \( E/K \) (resp. \( \text{Jac} E'/K \)). This reduces proving the 2-parity conjecture for \( \text{Jac} C/K \) to proving it for \( E \times \text{Jac} E'/K \), which is precisely theorem 6.1.

**Lemma 6.3.** Let \( K \) be a number field and \( E_1, E_2/K \) be elliptic curves. If \( E_1[2] \cong E_2[2] \) as Galois modules, then either \( E_2 \) is a quadratic twist of \( E_1 \) or there exists separable monic \( f(x) \in K[x] \) with \( f(0) \neq 0 \) and \( d \in K \) such that we have the following isomorphisms of curves

\[
E_1 \cong y^2 = f(x) \quad \text{and} \quad E_2 \cong dy^2 = xf(x).
\]

**Proof.** Write \( E_1 : y^2 = g_1(x) \), \( E_2 : y^2 = g_2(x) \) for monic cubics \( g_1, g_2 \in K[x] \) and \( \psi : E_1[2] \to E_2[2] \) for a Galois module isomorphism. Let \( \alpha_1, \alpha_2, 3 \) and \( \beta_1, \beta_2, \beta_3 \) be the roots of \( g_1 \) and \( g_2 \) respectively, labelled so that \( \psi((\alpha_i, 0)) = (\beta_i, 0) \). Let

\[
A = \alpha_1 \alpha_2 (\beta_1 - \beta_2) + \alpha_3 \alpha_1 (\beta_3 - \beta_1) + \alpha_2 \alpha_3 (\beta_2 - \beta_3), \\
B = \alpha_1 \alpha_2 \beta_3 (\beta_2 - \beta_1) + \alpha_3 \alpha_1 \beta_2 (\beta_1 - \beta_3) + \alpha_2 \alpha_3 \beta_1 (\beta_3 - \beta_2), \\
C = \beta_1 (\alpha_2 - \alpha_3) + \beta_2 (\alpha_3 - \alpha_1) + \beta_3 (\alpha_1 - \alpha_2) \\
\]

and

\[
D = \beta_1 \beta_2 (\alpha_1 - \alpha_2) + \beta_2 \beta_3 (\alpha_2 - \alpha_3) + \beta_3 \beta_1 (\alpha_3 - \alpha_1),
\]
permutes the roots of $g_1$ and the roots of $g_2$ in the same way, one can readily check that $h(z)$ is defined over $K$. Observing that $h(x) - h(\alpha) = ((AD - BC)/(A - Cx))(x - \alpha)$ gives

$$g_2(h(x)) = \frac{(AD - BC)^3}{(A - Cx)^3(A - C\alpha_1)(A - C\alpha_2)(A - C\alpha_3)}g_1(x).$$

Clearly, $E_2 \cong y^2 = g_2(h(x))$ and hence also,

$$E_2 \cong y^2 = \begin{cases} \frac{A(\alpha - C\alpha_1)(\alpha - C\alpha_2)(\alpha - C\alpha_3)}{AD - BC} \left(1 - \frac{C}{A}x\right)g_1(x) & A \neq 0, \\ \frac{C_1}{B}xg_1(x) & A = 0. \end{cases}$$

If $A, C \neq 0$, set $x' = 1 - (C/A)x$ then $E_1 \cong y^2 = f(x')$ and $E_2 \cong y^2 = dx'f(x')$ where $f(x') = g_1((A/C)(1 - x'))$ and $d \in K^\times$. If $A \neq 0$ and $C = 0$, then $E_2$ is just a quadratic twist of $E_1$. Finally, if $A = 0$ then the result is clear.

**Theorem 6.4.** Let $K$ be a number field and $E_1, E_2/K$ be elliptic curves. If $E_1[2] \cong E_2[2]$ as Galois modules, then the 2-parity conjecture holds for $E_1/K$ if and only if it holds for $E_2/K$.

**Proof.** By lemma 6.3, either $E_2$ is a quadratic twist of $E_1$ and this is just [3, Corollary 1.6], or $E_1 \cong y^2 = f(x)$ and $E_2 \cong dy^2 = xf(x)$ (as curves) for some separable monic $f(x) \in K[x]$ with $f(0) \neq 0$ and $d \in K$. Since $E_2 \cong \text{Jac} E_2 \cong \text{Jac}(dy^2 = xf(x))$, [3, Corollary 1.6] tells us that the 2-parity conjecture holds for $E_2/K$ if and only if it holds for $\text{Jac}(y^2 = xf(x))/K$. Theorem 6.1 says that the 2-parity conjecture holds for $\text{Jac}(y^2 = xf(x))/K$ if and only if it holds for $E_1/K$.

When working with elliptic curves over totally real number fields, the $p$-parity conjecture is known in most cases thanks to the work of Nekovář ([7, Theorem E], [5, Theorem A]) and Dokchitser–Dokchitser ([3, Theorem 2.4]). When $p = 2$ and $E$ does have complex multiplication some cases are proved in ([6, (5.9)]) but this setting is unsolved in general. Theorem 6.4 allows us to prove the missing cases, completing the proof of the $p$-parity conjecture for elliptic curves over totally real fields.

**Theorem 6.5.** Let $E/K$ be an elliptic curve over a totally real number field with complex multiplication. The 2-parity conjecture holds for $E/K$.

**Proof.** Suppose $E : y^2 = f(x)$ where $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. For $\gamma \in K$, set $f_\gamma(x) = f(x - \gamma)$ and define $E_\gamma = \text{Jac}(y^2 = xf_\gamma(x))$. By remark 2.2, a model for $E_\gamma$ is given by

$$y^2 = (x + (\alpha_1 + \gamma)(\alpha_2 + \gamma))(x + (\alpha_1 + \gamma)(\alpha_3 + \gamma))(x + (\alpha_2 + \gamma)(\alpha_3 + \gamma)).$$

Clearly $E[2] \cong E_\gamma[2]$ as Galois modules. The $j$-invariant for $E_\gamma$ is a non-constant rational function in $\gamma$, so for some $y_0 \in K$ it will hold that $j(E_{\gamma_0}) \notin \mathcal{O}_K$, therefore $E_{\gamma_0}$ does not have CM. In particular, the 2-parity conjecture holds for $E_{\gamma_0}/K$ by [3, Theorem 2.4], and applying theorem 6.4 gives that the 2-parity conjecture holds for $E/K$.

**Corollary 6.6.** Let $p$ be a prime and $K$ be a totally real field. The $p$-parity conjecture holds for all elliptic curves over $K$.

**Proof.** When $p$ is odd, this is [7, Theorem E] and [5, Theorem A]. When $p = 2$ and the elliptic curve does not have complex multiplication, this is [3, Theorem 2.4]. When $p = 2$ and the elliptic curve has complex multiplication, this is theorem 6.5.

Data accessibility. This article has no additional data.

Conflict of interest declaration. We declare that we have no competing interests.

Authors’ contributions. H.M.G.: conceptualization, data curation, formal analysis, funding acquisition, investigation, methodology, project administration, resources, software, supervision, validation, visualization, writing—original draft, writing—review and editing; C.M.: conceptualization, data curation, formal analysis, funding acquisition, investigation, methodology, project administration, resources, software, supervision, validation, visualization, writing—original draft, writing—review and editing.
All authors gave final approval for publication and agreed to be held accountable for the work performed therein.

**Funding.** The first author is supported by University College London and the EPSRC studentship grant no. EP/R513143/1. The second author is supported by a Royal Society Dorothy Hodgkin Fellowship and was supported by the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation (Simons Foundation grant no. 550023) during part of this work.

**Acknowledgements.** We would like to warmly thank Vladimir Dokchitser and Adam Morgan for helpful discussions and suggestions. We also thank the anonymous referee for suggesting to look into proving theorem 6.5.

**Appendix A. Local Conjecture for a family of hyperelliptic curves (by HOLLY GREEN)**

As mentioned in §1, finding the correct local discrepancy using the above approach is very challenging due to the current lack of a conceptual understanding for it. In fact, there are instances where one can give local formulae for the parity of the $2^n$-Selmer rank of varieties but where we do not know an expression for the local error term (see [21] for a local formula in the case of Jacobians of genus 2 or 3 curves with a $K$-rational 2-torsion point, and remark 1.8 for a discussion on the error term).

The error term found in this article stands out as it can be generalized in the settings presented below and it recovers the error term found in [13] when proving the 2-parity conjecture for elliptic curves admitting a 2-isogeny. Here we motivate and present the generalization, providing references for additional details on some of the results.

**(a) Setup**

Let $K$ be a number field. For a separable monic polynomial $f(x) \in K[x]$ such that $f(0) \neq 0$ we consider the hyperelliptic curves

$$C_1 : y^2 = f(x), \quad C_2 : y^2 = xf(x) \quad \text{and} \quad C : y^2 = f(x^2).$$

As in §2, we can control the parity of the $2^n$-Selmer rank of $\text{Jac} C_1 \times \text{Jac} C_2$ using an isogeny.

**Lemma A.1.** Let $K$ be a field of characteristic 0 and let $f(x) \in K[x]$ be separable, monic and such that $f(0) \neq 0$. Then there is an isogeny $\phi : \text{Jac} C_1 \times \text{Jac} C_2 \to \text{Jac} C$, such that $\phi \phi^t = [2]$.

**Proof.** This is similar to the proof of lemma 2.3. In particular, it can be shown that the maps $C \to C_1 : (x, y) \mapsto (x^2, y)$ and $C \to C_2 : (x, y) \mapsto (x^2, xy)$ induce an isogeny $\text{Jac} C_1 \times \text{Jac} C_2 \to \text{Jac} C$ with the required properties. ■

**Definition A.2.** Let $K$ be a local field and let $f(x) \in K[x]$ be separable, monic and such that $f(0) \neq 0$. We write

$$\lambda_{f, K} = \mu_{C_1/K} \mu_{C_2/K} \mu_{C/K} \cdot (-1)^{\dim_{\mathbb{Q}_2} \ker \phi|_{K} - \dim_{\mathbb{Q}_2} \coker \phi|_{K}},$$

where for a curve $X/K$, $\mu_X/K$ is $-1$ if $X$ is deficient over $K$ (as defined in [12, § 8]) and 1 otherwise. Here $\ker \phi|_{K} = (\text{Jac} C_1 \times \text{Jac} C_2)(K)\phi$ and $\coker \phi|_{K} = [\text{Jac} C(K)/\phi((\text{Jac} C_1 \times \text{Jac} C_2)(K))]$.

**Theorem A.3.** Let $K$ be a number field and let $f(x) \in K[x]$ be separable, monic and such that $f(0) \neq 0$. Then

$$(-1)^{\text{rk}_{\text{Jac} C_1/K + \text{rk}_{\text{Jac} C_2/K}} = \prod_{\nu} \lambda_{f, K_{v}},$$

where the product runs over all places of $K$.

**Proof.** This is argued as in [9, Theorem 3.2] with $A = \text{Jac} C_1 \times \text{Jac} C_2$ and $A' = \text{Jac} C$. ■
(b) Sturm polynomials

As in lemma 2.6, computing the quantity \( \lambda_{f, R} \) boils down to counting connected components of \( \text{Jac} C_1, \text{Jac} C_2 \) and \( \text{Jac} C \) over the reals. These numbers can be determined from the number of real roots of \( f(x) \) and \( f(x^2) \). To count the latter we use Sturm’s theorem to determine the number of real roots of \( f(x) \) greater than 0.

**Definition A.4.** Let \( f(x) \in \mathbb{R}[x] \). The Sturm sequence for \( f \) is a sequence of polynomials \( P_0, P_1, \ldots \) defined via

\[
P_0 = f(x), \quad P_1 = f'(x), \quad P_{i+1} \equiv -P_{i-1}(\text{mod } P_i) \text{ for } i \geq 1,
\]

where either \( \deg P_{i+1} < \deg P_i \) or \( P_{i+1} = 0 \). The sequence terminates once one of the \( P_i \) is zero.

**Definition A.5.** Let \( f(x) \in \mathbb{R}[x] \) have Sturm sequence \( P_0, P_1, \ldots \). We write \( \sigma(x_0) \) for the number of sign changes (ignoring zeros) in the sequence of real numbers

\[
P_0(x_0), P_1(x_0), \ldots.
\]

**Theorem A.6 (Sturm’s theorem).** Let \( f(x) \in \mathbb{R}[x] \) have Sturm sequence \( P_0, P_1, \ldots \). The number of roots of \( f \) in the interval \((a, b) \subset \mathbb{R}\) is \( \sigma(a) - \sigma(b) \).

In practice, the Sturm sequence for a polynomial provides us with a way to compute the number of roots it has in any half-open interval. Therefore, the Sturm polynomials evaluated at 0 and \( \infty \) were good candidates for the entries of the Hilbert symbol of our error term.

(c) Conjecture based on experimental data

**Definition A.7.** Let \( K \) be a local field of characteristic 0 and let \( f(x) \in K[x] \) be separable and monic. Let \( P_0, P_1, \ldots \) denote the Sturm sequence for \( f \), write \( c_i \) for the lead coefficient of \( P_i \) and assume that \( \deg P_i = \deg f - i \) for \( i = 0, \ldots, \deg f \). Whenever \( \prod_{i=0}^{\deg f - 1} P_i(0) \neq 0 \), we define \( H_{f,K} \) to be the following product of Hilbert symbols

\[
H_{f,K} = \prod_{i=0}^{\deg f - 2} (-P_i(0), P_{i+1}(0))_K \cdot (c_i, -c_{i+1})_K.
\]

**Remark A.8.** When \( f \) is a quadratic, this recovers the error term given in [13] (the isogeny \( \phi \) given in lemma A.1 becomes a 2-isogeny of elliptic curves) and when \( f \) is a cubic, this is precisely \( H_{f,K} \) as defined in 2.8 (when \( b, L \neq 0 \)).

**Conjecture A.9 (Local conjecture).** Let \( K \) be a local field of characteristic 0 and let \( f(x) \in K[x] \) be separable monic and such that \( f(0) \neq 0 \). Define hyperelliptic curves over \( K \) by

\[
C_1 : y^2 = f(x) \quad \text{and} \quad C_2 : y^2 = xf(x).
\]

Let \( P_0, P_1, \ldots \) denote the Sturm sequence for \( f \). If \( \deg P_i = \deg f - i \) for \( i = 0, \ldots, \deg f \) and \( \prod_{i=0}^{\deg f - 1} P_i(0) \neq 0 \), then

\[
\omega_{\text{Jac} C_1/K} \omega_{\text{Jac} C_2/K} = \lambda_{f,K} H_{f,K}.
\]

**Remark A.10.** If \( P_i(0) = 0 \) or \( \deg P_{i+1} < \deg P_i - 1 \) for some \( i \), then \( H_{f,K} \) is no longer well-defined. It is expected that a different Hilbert symbol expression can be found so that the conjecture still holds, as in definition 2.8.

**Remark A.11.** We have proved the conjecture whenever \( K \cong \mathbb{C} \) or \( K \cong \mathbb{R} \). Proving it when \( K \) is a non-archimedean field is work in progress. When \( f \) is a quartic and \( K/Q_p \) is a finite extension for odd \( p \), we have an analogue of proposition 4.5, namely the conjecture is known to hold when the cluster picture for \( C_2 \) is \( \bullet \bullet \bullet \bullet \), or \( \bullet \bullet \bullet \bullet \), or \( \bullet \bullet \bullet \bullet \).

**Remark A.12.** Supposing that conjecture A.9 is true, the 2-parity conjecture holds for \( \text{Jac} C_1 \) if and only if it holds for \( \text{Jac} C_2 \). This is argued identically to theorem 6.1.
Remark A.13. Applying remark A.12 repeatedly proves the 2-parity conjecture for hyperelliptic curves over a number field $K$ with defining polynomial $f_1, f_2, \ldots, f_n$, where each $f_i \in K[x]$ is linear (subject to the usual conditions on the Sturm sequence for each product $f_i, \ldots, f_n$ for $i = 1, \ldots, n - 3$).

References

1. Dokchitser T, Dokchitser V. 2010 On the Birch–Swinnerton-Dyer quotients modulo squares. *Ann. Math.* 172, 567–596. (doi:10.4007/annals.2010.172.567)
2. Česnavičius K. 2016 The $p$-parity conjecture for elliptic curves with a $p$-isogeny. *J. Reine Angew. Math.* 2016, 45–73. (doi:10.1515/crelle-2014-0040)
3. Dokchitser T, Dokchitser V. 2011 Root numbers and parity of ranks of elliptic curves. *J. Reine Angew. Math.* 658, 39–64. (doi:10.1515/crelle.2011.060)
4. Nekovář J. 2009 On the parity of ranks of Selmer groups IV. With an appendix by Jean-Pierre Wintenberger. *Composit. Math.* 145, 1351–1359. (doi:10.1112/S0010437X09003959)
5. Nekovář J. 2013 Some consequences of a formula of Mazur and Rubin for arithmetic local constants. *Algebra Number Theory* 7, 1101–1120. (doi:10.2140/ant.2013.7.1101)
6. Nekovář J. 2015 Compatibility of arithmetic and algebraic local constants (the case $\ell \neq p$). *Compos. Math.* 151, 1626–1646. (doi:10.1112/S0010437X14008069)
7. Nekovář J. 2018 Compatibility of arithmetic and algebraic local constants, II: the tame abelian potentially Barsotti-Tate case. *Proc. Lond. Math. Soc.* 116, 378–427. (doi:10.1112/plms.12085)
8. Kramer K, Tunnell J. 1982 Elliptic curves and local $\epsilon$-factors. *Compos. Math.* 46, 307–352.
9. Dokchitser V, Maistret C. 2019 Parity conjecture for abelian surfaces. (https://arxiv.org/abs/1911.04626)
10. Morgan A. 2015 2-Selmer parity for hyperelliptic curves in quadratic extensions. (https://arxiv.org/abs/1504.01960)
11. Coates J, Fukaya T, Kato K, Sujatha R. 2010 Root numbers, Selmer groups and non-commutative Iwasawa theory. *J. Alg. Geom.* 19, 19–97. (doi:10.1090/S1056-3911-09-00504-9)
12. Poonen B, Stoll M. 1999 The Cassels-Tate pairing on polarized abelian varieties. *Ann. Math.* 150, 1109–1149. (doi:10.2307/121064)
13. Dokchitser T, Dokchitser V. 2008 Parity of ranks for elliptic curves with a cyclic isogeny. *J. Number Theory* 128, 662–679. (doi:10.1016/j.jnt.2007.02.008)
14. Ahmed S, Aribam C, Shekhar S. 2016 Root numbers and parity of local Iwasawa invariants. (https://arxiv.org/abs/1608.08078)
15. Cassels JWS, Flynn EV. 1996 *Prolegomena to a middlebrow arithmetic of curves of genus 2*, vol. 230. London Mathematical Society. Lecture Note Series. Cambridge, UK: Cambridge University Press.
16. Gross B, Harris J. 1981 Real algebraic curves. *Ann. Sci. Ec. Norm. Super.* 14, 157–182. (doi:10.24033/asens.1401)
17. Best A et al. 2021 A user’s guide to the local arithmetic of hyperelliptic curves. (https://arxiv.org/abs/2007.01749)
18. Dokchitser T, Dokchitser V, Maistret C, Morgan A. 2018 Arithmetic of hyperelliptic curves over local fields. (https://arxiv.org/abs/1808.02936)
19. Faraggi O. 2021 Models of bihyperelliptic curves. (https://arxiv.org/abs/2103.09730)
20. Silverman JH. 2009 *The arithmetic of elliptic curves*, vol. 106. Berlin, Germany: Springer.
21. Docking J. 2021 $2^\infty$-Selmer rank parities via the Prym construction. (https://arxiv.org/abs/2108.09564)